Integrity of autonomous train: safety requirements analysis

Insaf Sassi, El-Miloudi El-Koursi

Integrity of autonomous train: safety requirements analysis

Insaf Sassi[1], El-Miloudi El-Koursi[2]

[1] *Institut de Recherche Technologique Railenium, F-59300, Famars, France.*
E-mail: insaf.sassi@railenium.eu
[2] *IFSTTAR, COSYS, ESTAS, Villeneuve d'Ascq Cedex, France.*
E-mail: el-miloudi.el-koursi@ifsttar.fr

abstract

The evolution of the European Rail Traffic Management System (ERTMS) to level 3 enables increasing the capacity on the lines thanks to continuous supervision and communication, moving block and virtual block. It relies on the autonomous position and integrity information reported by the train to determine if it is safe to issue to movement authority. The aim of our paper is to present a short preview of the train integrity monitoring system and its safety challenges. A methodology to maintain traceability of safety requirements to cover the hazards, identified from the system functions, is proposed based on the standard EN 50126.
Keywords: autonomous train, ERTMS, integrity, safety, requirements traceability.

1. Introduction

The existing railway signalling systems have been progressed to cover the customer needs and to provide a safe system. The European railway contributors have defined and evolved the standard European Rail Traffic Management System (ERTMS) to improve the onboard and trackside subsystems to cope with the evolution of the railway industry. The key motivation for the evolution from the ERTMS level 2 to level 3 is to find a solution that increases the capacity in the European railway networks in a cost effective way and guarantees the safety. The ERTMS level 3 has an important impact on the railway industry. It enables reducing rail infrastructure costs by removing the trackside equipment, increasing the capacity, improving the reliability and the punctuality (6). It is a common aim raised by the railway stakeholders creating the partnership project *Shift2Rail* to facilitate the cooperation and to define a road map for different objectives. This project consists of five Innovation Programs (IPs) that cover all the railway subsystems in order to provide demonstration activities and dissemination of relevant results. Under the IP2 *Advanced Traffic Management and Control Systems*, strategies are being set up in order to increase the functionalities of the existing ERTMS. The ERTMS evolution to level 3 implies continuous supervision of train speed and communication, moving block and virtual block. It uses radio communication to pass the movement authorities to the train. It also utilizes the autonomous position and integrity information reported by the train to determine if it is safe to issue to movement authority as specified in (2). Consequently, there is no need for fixed blocks nor trackside equipment (track circuit, axle encounters) for train integrity monitoring and detection.
To answer this new challenges, the work package untitled On-board Train Integrity

Proceedings of the 29th European Safety and Reliability Conference.

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_output

(OTI) of the X2Rail-2 project aims to design an autonomous OTI monitoring system that must be compliant to a set of safety requirements. One of the main contribution of our project is to reach a safe OTI. The OTI main goal is to autonomously verify the completeness of the train in operation. The OTI system must respect safety requirements defined by the European Railways standard EN 50126 (3) and the common safety method (1). It must implement requirements that permit the achievement of the Safety Integrity Level SIL 4. The certification of a railway system requires an important amount of work for safety demonstration. One of the high recommended measure for SIL 4 systems is capturing safety requirement and maintain their traceability which is primordial for safety certification inspections (3). In fact, performing traceability is establishing consistency among project artifacts of the product life cycle. It also consists in providing evidence that the system specifications and implementations address the identified hazards and their mitigations. Safety requirements should be traced to architecture elements that are responsible for the implementation of the measures preventing safety critical failures. A poor traceability impacts the completeness and consistency of safety requirements.
In this paper, we start with defining the traceability activities and a brief review of related works in section 2. A set of safety requirements must be considered in the development of the OTI Monitoring System. For this purpose, we propose in section 3 a set of steps to perform traceability of safety requirements over the design flow according to the standard En 50126 (3). Section 4 is devoted for describing the OTI monitoring system and its safety challenges. It also presents a preview of the implementation of the traceability model. A conclusion and perspectives are given in section 5.

2. Traceability and Related Work

Traceability is the ability to describe and follow the life cycle of a product artifact as defined in (9). It is a technique to relate the produced data during the product development cycle to ensure the completeness of the specification and to manage changing requirements. The requirements are expressed by natural text. Graphical notations like the Systems Modeling Language (SysML) (4) and the Goal Structuring Notation (GSN) (10) are also used to obtain a structured view to represent the requirements. Some other graphical approach have been produced independently of SysML and GSN using a Conceptual Model of Traceability (11) or a Traceability Information Model (TIM) (7).
The traceability is represented by two main concepts constituting a traceability model (11):

- **artifact**: it is the identifiable units of data managed (used, modified, and/or produced) throughout the product life cycle.
- **trace**:it is the traceability link that expresses the relationship between the artifacts.

The main data categories provided from the product life-cycle according to (4) and (11) are requirement, design/implementation, test case. The requirement, specified from the system functions, is satisfied if it is fulfilled by a design element and an implementation. A test case should verify if a requirement is satisfied. A requirement could be decomposed into multiple requirements or derived from another require-

ment in another abstraction level.
For safety Critical systems, many standards include a phase of risk analysis and evaluation in the product life cycle (see (3)). A safety analysis produces specific type of data such as hazards, faults that contribute to the hazards occurrence, and safety requirements that mitigate these faults as explained in the work of (12). The study of (12) analyzes traceability models for safety critical projects and establishes a list of recommendations and a ”typical” traceability model taking into account the safety artifacts. However, this model does not take into account the refinements and the new requirements that can be determined at the technical level.
Assuring the traceability between the functional and technical requirements and safety analysis is essential in order to prepare safety cases. The standards recommend to develop a well structured methodology to provide evidence that the system specifications and implementation cover the identified hazard and their mitigations. The authors in (10) uses the GSN in order to represent the safety concepts hierarchically. The basic elements of their graphical notation are safety goal (requirement), solutions and strategies. The safety goal is decomposed into sub-goals. However, no apportionment and decomposition process of safety requirements is represented in their approach. The work of (11) proposes a conceptual model that encloses all the levels of the development process. It starts from system concept development to system installation. The set of artifacts defined in their model covers the system functional analysis, architecture specification, system requirements, software and hardware requirements which are the elements from the system development process. From the safety assessment process, it includes objects such as hazards, mitigations, safety requirements, safety integrity level (SIL), common cause failures. The model of (11) can be adapted for safety requirements specification and traceability in our work. Unfortunately, it does not give details about the decomposition process of safety requirements and their apportionment to components level. The safety requirements decomposition pattern developed by (7) covers the shortcomings of the aforementioned traceability models. It specifies separately the safety requirements and defines the associated architecture element that addresses them at functional and technical level. It also represents a decomposition policy that consists in determining the composite and atomic safety requirement by providing a refinement argument. Our Traceability model is build on the models of (11), (12), (7) and (8) by maintaining regulatory compliance to the standard EN 50126. Unlike the contribution of (7), we present a justification to the existence of a safety requirement according to the standard. Our approach represents a TIM that shows a view for safety requirements management. It is independent from graphical approach like SysML or GSN. It also sets a procedure for Safety requirements decomposition.

3. Traceability Information Model for Safety Requirements Management

The Traceability Information Model (TIM) is useful for information management in a safety critical project. It is recommended to create a TIM early in a project to ensure consistency throughout the system life-cycle and to specify traceability links manually for ”critical” requirements, i.e. safety related requirements. The relationships between the artifacts, the change information in artifacts relationships for further impact analysis and traceability maintenance, guarantee this consistency.
We propose the TIM of figure 1 according to these recommendations. This model

gives an overview of the generated data, resulted from the product life-cycle and the performed safety analysis, and the links that represent the relationship between them. The data are represented by a rectangle in figure 1. An identifier ID and a description are the main two properties of every artifact. The trace between the artifacts are visualized as a line. Two types of traces or relationships are defined:

- The intra-traceability link depicts the traceability within a set of artifacts belonging to the same family such as the *"compose"* and the *"heritage"* links.
- The inter-traceability trace represents the traceability among the different artifacts.

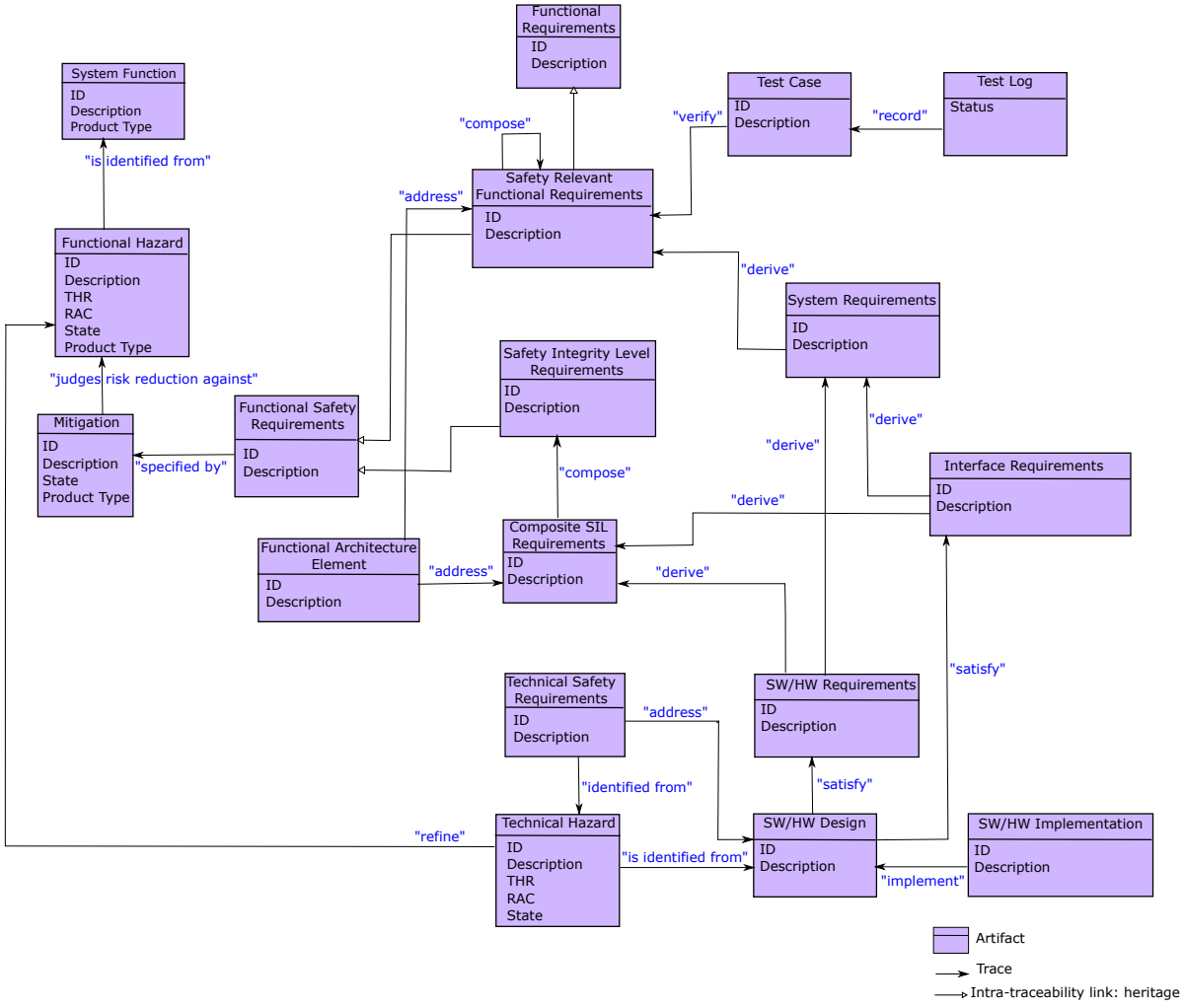

Fig. 1. Traceability Information Model

The first step consists in defining the system functions which become safety related

functions whose failures affect the safety of the system by the phase of risk analysis and evaluation. In the next step of the definition of the TIM, a list of hazards is *"identified from"* the safety-related functions by performing a Preliminary Hazard Analysis (PHA). A hazard probability level is also defined. The hazard state can be open, deleted, solved, covered or closed, depending on the progress state of the mitigation implementation to cover this hazard. The risk analysis and evaluation aim to set a Tolerable Hazard Rate (THR) for every hazard that should be agreed with the railway authority. To achieve an accepted risk level, a set of mitigations is defined to reduce the risk severity or frequency. These mitigations should then be *"specified"* or implemented by the functional safety requirements at the functional abstraction level. If a mitigation is covered by a safety requirement, its state becomes *"resolved"* and then *"implemented"*. It is considered *"open"* when it is not linked to any requirements unless it is transferred to be implemented by another system.

The safety requirements, as represented in figure 1, are categorized as safety relevant functional requirements if they are functional requirements that implement the mitigations. A compound safety relevant functional requirement is decomposed into sub-requirements that can be realized in the technical level. Thus, a set of system and interface requirements and software and hardware requirements are derived to implement the functional requirements. A design and an implementation code are used to *"satisfy"* a requirement in the one hand. In the other hand, a test case, whose result is recorded in a test log, is established to "verify" that the requirement is covered and implemented (see figure 1).

To justify the existence of a safety requirement, unlike (7), our specification takes into consideration the implementation of safety-related functions, safety-related assumptions, the THR and the Tolerable Functional Failure Rate (TFFR) as quantitative requirements, legal safety requirements, environmental conditions and a set of operational, organisational and maintenance rules. The SIL requirements are thus considered as functional safety requirements that associate qualitative measures to a range of TFFR (3). A common causal analysis (CCA) is performed in this level using Fault Tree Analysis (FTA) to apportion the SIL requirements based on the quantified targets in terms of THR as recommended by the standard and detailed in (13). It consists in assigning TFFR and SIL for functions by analysing the functional architecture and allocating them to subsystems in the fifth phase of the product life-cycle. At the design and implementation or technical level, safety tactics, such as software checking, redundancy and barriers, are defined to be compliant to the Software/hardware requirements. These requirements are obtained by the apportionment of integrity to the components level: software and hardware integrity level. A technical hazard analysis, related to the design and implementation solution, should be carried out in this phase to refine the functional hazard analysis as depicted in figure 1. A CCA is used to investigate the causes deriving from the technical solutions taking into consideration environmental, functional, interface, hardware, software, human factors and failure rates of the components. A set of technical safety requirements are defined to address technical design and implementation of the system.

The proposed TIM of figure 1 is implemented in Excel in section 4 for the train integrity monitoring system to show its relevance.

4. On-board Train Integrity

4.1. *System definition*

The train integrity monitoring system is an essential component of the ERTMS level 3 architecture which must be performed safely. 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 integrity status information must be transferred to the European Train Control System Train Interface Unit (ETCS TIU) as shown in figure 2. The provided integrity information has three possible values: confirmed, lost or unknown. The train integrity monitoring system consists of the following modules as depicted in figure 2:

- **OTI Slave (OTI-S)**: It is the tail OTI device. It determines the status of the train tail and communicates it to the OTI Master.
- **OTI Master (OTI-M)**: It is the head OTI device. It acquires the information of train integrity status from the OTI-S and sends it to the ETCS TIU module.
- **OTI Intermediate (OTI-I)**: It is the intermediate device optionally installed along the vehicle.
- **On-board Communication Network (OCN)**: It is the communication channel for information exchanging between OTI monitoring system devices. It can be wired or wireless and it is bidirectional between the OTI modules.

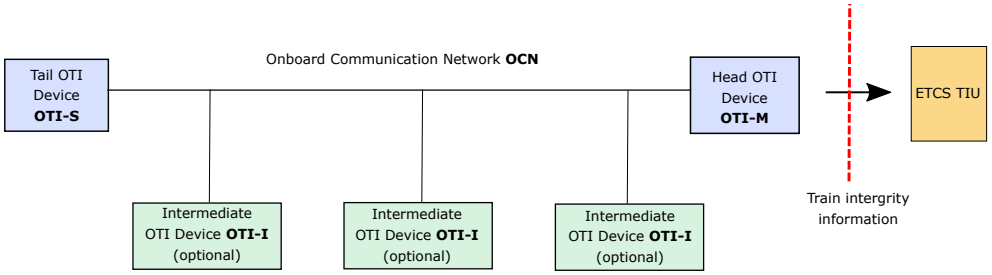

Fig. 2. System definition (5)

The type of the communication channel is a key characteristic to define the integrity criteria and the three product types or classes. The first product class refers to train with wired communication network where the integrity criteria is evaluated based on the communication liveliness between an OTI Slave module located at train tail and OTI Master module located in front cabin. The application domains of this type of products are Inter-city High Speed, Regional, Urban and Sub-Urban, and Freight. The second product class encompasses the trains with wireless communication channel and the integrity is determined based on comparing kinematic data of train tail and front cabin (e.g. position, speed, acceleration). Product class three is designed to enhance safety in train length and composition determination by installing OTI devices in every wagon. The freight train is the main application of the last two product classes.

The train integrity monitoring system is used to safely detect the train interruption and mainly for two functional scenarios: train joining and splitting. Moreover, the

OTI modules should perform basic functionalities before starting any of the aforementioned scenarios. The OTI slave and master functional modules shall safely carry out the mastership, inauguration and monitoring phases. The mastership consists in identifying the OTI module role (e.g. master or slave). The inauguration phase aims at identifying the OTI modules connected to the OCN where the OTI-M shall send identification request messages to all OTI Slave modules. The OTI-M shall activate a pairing procedure with OTI Slave module located at train tail. Finally, the monitoring phase objective is to perform train integrity monitoring where the OTI-M shall receive train tail status from OTI-S. The results of the qualitative risk analysis detailed in (5) show that OTI-M module, OTI-S module and the OCN of figure 2 shall be SIL 4.

4.2. *TIM implementation*

In Safety related project, generating trace queries or trace slices permit to visualize the hazard and its related artifacts. Visualizing the trace slices is an important safety related task and helps to understand how a hazard has been mitigated from a regulator point of view. The TIM of figure 1 is implemented using Excel. A part of the implementation is shown in figure 3. For every identified hazard, a list of its properties are enumerated. Two fields are added to realise the traceability link between the functional hazard and the mitigations in the one hand and between the functional and the technical hazards in the other hand. The mitigation OTI_MIT_017, highlighted in red, has the state open because no safety functional requirements are specified to implement this mitigation. The Risk Acceptance Principle (RAP) shall be carried out if the risk is not acceptable. The three risk acceptance principles are: Code of Practice (CoP), Similar Reference System, Explicit Risk Estimation (ERE). In case of Explicit Risk Estimation, one of the following Risk Acceptance Criteria (RAC) must be defined to establish the acceptability of the risk: As Low As Reasonably Practicable (ALARP), Globalement Au Moins Equivalent (GAME) and Minimum Endogenous Mortality (MEM). The field *Notes* is used to add any comments. The *Product type* field specifies the applicability of the hazard for the product class.
This Excel sheet must be completed until filling all the gaps to cover all the hazards identified in the functional level.

Hazard ID	Description	Mitigation ID(judges risk reduction against)	State(covered by a safety related requirement)	THR	Risk Acceptance Principle	Technical hazard	Notes	Product Type
OTI_HZ_002	The ERTMS/ETCS On-board equipment receives inappropriate Train Integrity Confirmation (incorrect or earlier information)	OTI_MIT_003 OTI_MIT_006 OTI_MIT_009 OTI_MIT_010 OTI_MIT_016	yes	(to be defined according to standard EN 50126)	☐ Code of Practice ☐ Similar Reference System ☐ Explicit Risk Estimation ☐ ALARP ☐ GAME ☐ MEM	(to be defined)		all product types
OTI_HZ_003	OTI Slave is not installed on the last car/waggon but it localizes itself on the last waggon/car or the OTI Master receives an incorrect identification message from OTI Slave ("TAIL" instead of "Non TAIL")	OTI_MIT_001 OTI_MIT_002 OTI_MIT_004 OTI_MIT_005 OTI_MIT_010 OTI_MIT_017 OTI_MIT_019 OTI_MIT_022 OTI_MIT_023		(to be defined according to standard EN 50126)	☐ Code of Practice ☐ Similar Reference System ☐ Explicit Risk Estimation ☐ ALARP ☐ GAME ☐ MEM	(to be defined)		

Fig. 3. Traceability view hazards

5. Conclusion

The train integrity monitoring system is an important part of the realization of the ERTMS level 3. It must be comply with safety targets. This requirement implies a set of constraints and approaches to be considered. Traceability of safety requirements starts from the specification of safety related functions to the validation step. These requirements should be implemented, tested and validated. The proposed TIM is build on the inter/intra-traceability approach to guarantee the consistency in accordance with the standard EN 50126. The TIM covers the data that should be taken into consideration as recommended in the standard. It maintains the links between the data in order to show the achievement of the implementation of safety requirements.

Acknowledgement

This work is supported by the X2RAIL-2 project, part of the Shift2Rail Innovation Program 2. We would like to thank our X2RAIL-2 WP4 partners, Ansaldo STS, Alstom Transport Sa, AZD Praha Sro, Bombardier Transportation Sweden, CAF Signalling S.L., Asociacion Centro Tecnologico Ceit-IK4, Deutsche Bahn AG, Deutsches Zentrum Fuer Luft-Und Raumfahrt Ev, Schweizerische Bundesbahnen SBB Ag, INDRA SISTEMAS SA, IRT Railenium, Mermec Spa, Network Rail Infrastructure Limited, Siemens Aktiengesellschaft, Trafikverket.

References

[1] Common safety method for risk evaluation and assessment and repealing regulation (ec)352/2009, document regulation (eu) 402/2013, 30th commission implementing regulation. April 2013.
[2] Subset 026 ertms/etcs-system requirement specification-rev.3.6.0. 2016.
[3] En 50126: Railway applications-the specification and demonstration of reliability, availability, maintainability and safety (rams). 2017.
[4] Omg systems modeling language, version 1.5, 2017.
[5] Deliverable d 4.1 train integrity concept and functional requirements specifications. 2018.
[6] Shift2rail, shift2rail multi-annual action plan. `https://shift2rail.org`, December 2018.
[7] P. O. Antonino, M. Trapp, P. Barbosa, E. C. Gurjão, and J. Rosário. The safety requirements decomposition pattern. In *International Conference on Computer Safety, Reliability, and Security*, pages 269–282. Springer, 2014.
[8] P. Barbosa, F. Leite, D. Santos, A. Figueiredo, and K. Galdino. Introducing traceability information models in connected health projects. In *2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS)*, pages 18–23. IEEE, 2018.
[9] O. C. Gotel and C. Finkelstein. An analysis of the requirements traceability problem. In *Requirements Engineering, 1994., Proceedings of the First International Conference on*, pages 94–101. IEEE, 1994.
[10] I. Habli, I. Ibarra, R. S. Rivett, and T. Kelly. Model-based assurance for justifying automotive functional safety. Technical report, SAE Technical Paper, 2010.
[11] V. Katta and T. Stålhane. A conceptual model of traceability for safety systems. In *Poster session at 2nd International Conference on Complex Systems Design & Management (CSD&M11)*, 2011.
[12] P. Mader, P. L. Jones, Y. Zhang, and J. Cleland-Huang. Strategic traceability for safety-critical projects. *IEEE software*, 30(3):58–66, 2013.
[13] K. A. Ouedraogo, J. Beugin, E.-M. El-Koursi, J. Clarhaut, D. Renaux, and F. Lisiecki. Toward an application guide for safety integrity level allocation in railway systems. *Risk Analysis*, 2018.