Verification Framework for Moving Block System Safety: application on the Loss of Train Integrity Use Case

Rim Saddem-Yagoubi[a,*], Julie Beugin[a] and Mohamed Ghazel[a]

[a] Univ Gustave Eiffel, COSYS-ESTAS, F-59650 Villeneuve d'Ascq, France
rim.saddem@univ-eiffel.fr, julie.beugin@univ-eiffel.fr, mohamed.ghazel@univ-eiffel.fr
* Corresponding author

Extended abstract submitted for presentation at the 11th Triennial Symposium on Transportation Analysis conference (TRISTAN XI)
June 19-25, 2022, Mauritius Island

April 6, 2022

Keywords: Railway safety; Requirement engineering, Semi-formal modelling; ERTMS/ETCS; Moving block, Verification & validation

1 INTRODUCTION

Railway signalling is a system that is responsible for managing railway traffic and maintaining a safe distance between trains at all times. The traditional signalling system is based on the concept of fixed blocks; namely the railway line is divided into sections of track, named blocks, which are separated by lineside signals controlling their clearness. A block can be occupied only by one train at a given time [Alikoc *et al.* (2013)]. Among other drawbacks, this system lacks of flexibility in the sense that the block size is fixed regardless of the actual speed and braking performance of the running trains. In other terms, the long safety distances required by fast trains are imposed to slower trains as well. Certainly, this reduces track capacity unnecessarily. Nowadays, rail transport systems constitute an important mode of transport for both freight and passengers and the demand for rail transport is growing very fast. Therefore, traditional signalling systems become insufficient to meet this significantly increasing demand. For example, in 2019, the statistics show approximately 643 billion passenger kilometers on European railways, making Europe the second-largest market for rail passenger traffic in the world[1]. To cope with this increasing demand, the European railway industry is looking into next-generation signalling systems able to manage train traffic more optimally. In particular, Moving Block systems (MB) are control-command and signalling systems that are introduced in this context. They can reduce train headway in order to maximise capacity utilisation of existing networks. The third application level of ETCS (European Train Control System) is based on the MB principle. ETCS is the automatic train protection (ATP) part of the European Rail Traffic Management System standard (ERTMS). ERTMS aims to replace the different national train Control-Command and Signaling systems (CCS) in Europe with an interoperable European CCS system [Hoang *et al.* (2018)]. Compared to ETCS Levels 1 and 2 that are based on traditional signalling system, ETCS Level 3 introduces the original concept of moving-block as follows: trains could just be separated by an absolute or a relative braking distance (i.e. the distance needed to reach a stopping point or the speed of the train ahead) plus a safety margin (see Figure 1). Lineside signals (used in ETCS L1) and train detectors (used in ETCS L1 and L2) are not required anymore. In so doing, ETCS L3 allows for substantial capacity gains, cost reduction (e.g. removal of trackside elements) and a higher reliability due to fewer equipment on the trackside [Furness *et al.* (2017)].

[1] https://www.statista.com/topics/8282/rail-passenger-transport-in-europe/#dossierKeyfigures

Figure 1 – *Full Moving Block*

One of the crucial issues to be tackled towards implementing ETCS L3, is related to the Verification and Validation (V&V) of the safety and functional specifications of MB that have been generated in the framework of previous European projects (X2Rail-1, X2Rail-3, MovingRail, Astrail). These specifications are constituted of an important number of interrelated requirements that need to be consistent with each other while tackling all the safety and performance aspects of railway operation. Due to the critical nature of railway CCS, railway safety standards recommend the use of formal modelling and verification techniques for the engineering of such systems.

The work presented here is part of the activities undertaken in the framework of PERFORMINGRAIL project, which aims, among other objectives, to develop semi-formal/formal models for moving block systems. Such models will serve as a basis for the V&V of ETCS L3 operation. In the present paper, we aim to give an overview on the modelling process. Namely, we will first introduce the generic developed methodology for building structural and behavioural models for moving block systems. Then, we will illustrate our approach through a representative use case related to the train integrity monitoring onboard function.

2 Generic Methodology & Illustration Use Case

In order to design verifiable models for Moving Block systems, we established a generic methodology that will serve as a guide for the modelling activities in the framework of PERFORMINGRAIL project. In the sequel, we will firstly outline this methodology and then, we will focus on the Loss of Train Integrity Use Case to illustrate the SysML models issued on the basis our modelling approach.

2.1 Methodological process

The proposed methodology aims to produce generic semi-formal and formal models for Moving Block (MB) systems. In fact, the semi-modelling activity is an intermediary step towards achieving workable formal models that can be used for actual V&V activities. Namely, since the MB requirements that we need to handle are mainly written in literal language, we will adopt a stepwise process to eventually elaborate the MB formal models. The defined methodological process comprises a number of iterative steps that need to be implemented with the aim to producing such formal models. This process (workflow) is composed of a number of interrelated activities, which exchange various inputs/outputs. Figure 2 presents a high-level view of the workflow, while the main outputs of the workflow are represented by a number of blue bold items.

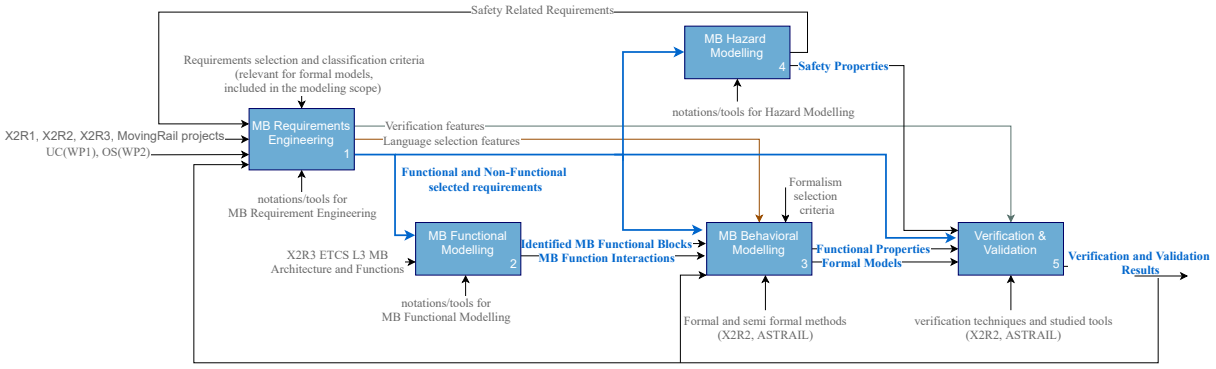

Figure 2 – *Workflow structure*

The first step *"MB Requirement Engineering"* aims to identify and classify the most relevant requirements for the MB system. The selected requirements can be presented using SysML requirement diagram. The second step *"MB Functional Modelling"* aims to identify, from the selected requirements, the various functions within the MB scope, as well as the interaction between them. The identified functions can be modelled by means of SysML state machines and the interactions they induce, by using SysML sequence diagrams. The step *"MB Behavioral Modelling"* aims to develop parameterizable formal models for the different MB functions and to identify functional properties. The step *"Hazard Modelling"* aims to model the identified hazards that are related to the MB system and to identify the safety properties to be checked. Finally, the *"Verification & Validation"* step aims to verify and validate the produced formal models.

In order to define the scope of the modeling activities, a survey has been conducted in [Seceleanu *et al.* (2021)] to evaluate the industrial relevance of the various available operational scenarios. Four Operational Scenarios (OSs) that allow for delineating the MB behavior have been selected. These selected OSs are covered by eight Use Cases (UCs). Among them, Loss of train integrity is a worth analyzing UC, given the safety hazards related to such a situation. In fact, the loss of integrity corresponds to the situation where some wagons are unintentionally unleashed from the convoy, which may induce severe accidents if not timely detected. In the sequel, we will focus on this UC.

2.2 Illustration with SysML models for Loss of Train Integrity

As mentioned above, the Loss of Train Integrity (LTI) UC is a hazardous scenario. This may occur for different reasons, but in the event that a train splits unintentionally, the dispatcher needs to take appropriate measures, in particular to prevent the collision of dislocated part of the train with some following trains. When trains moving in ETCS L3, the train integrity information have a significant impact on the performance of the line.

Following the generic methodology described above, in the first step related to MB requirement engineering, 10 requirements related to LTI use case were identified and are represented by a SysML requirement diagram, as shown in Figure 3.

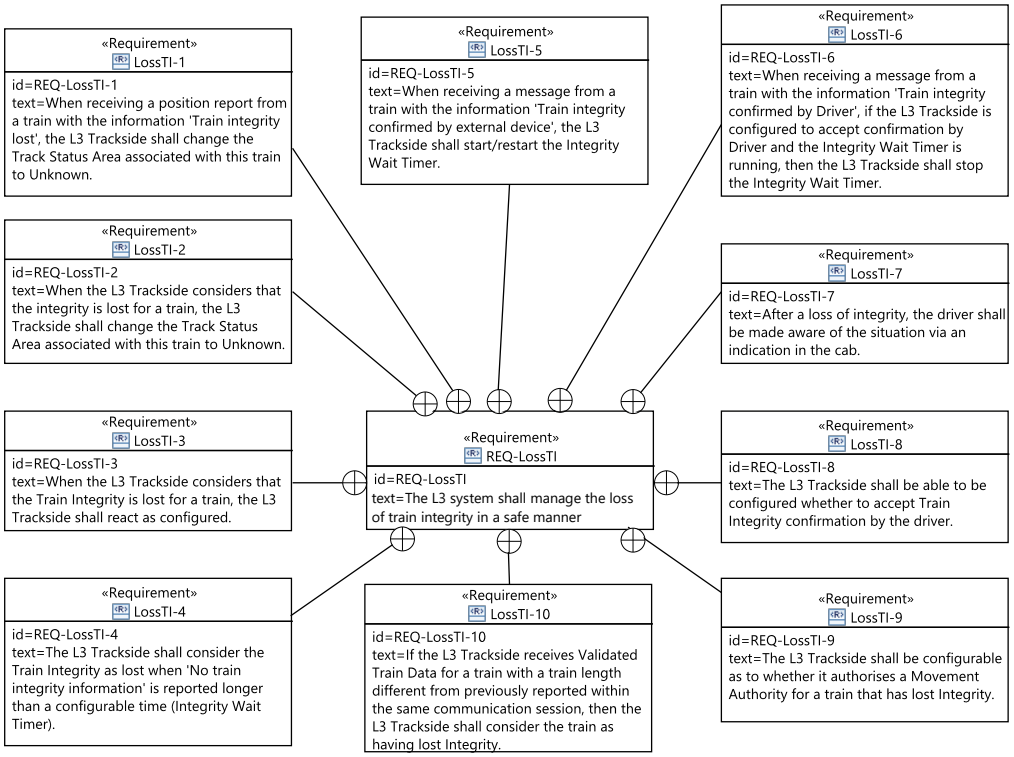

Figure 3 – *Loss of train integrity SysML requirement diagram*

In the second step, from the identified LTI related requirements, the interaction between LTI UC and ETCS L3 actors is depicted using a SysML sequence diagram (see Figure 4). In this figure, TPR stands for Train Position Report which is sent by the train onboard to ETCS trackside, and MA stands for Movement Authority which corresponds to a detailed authorization to run sent from the trackside to the train onboard.

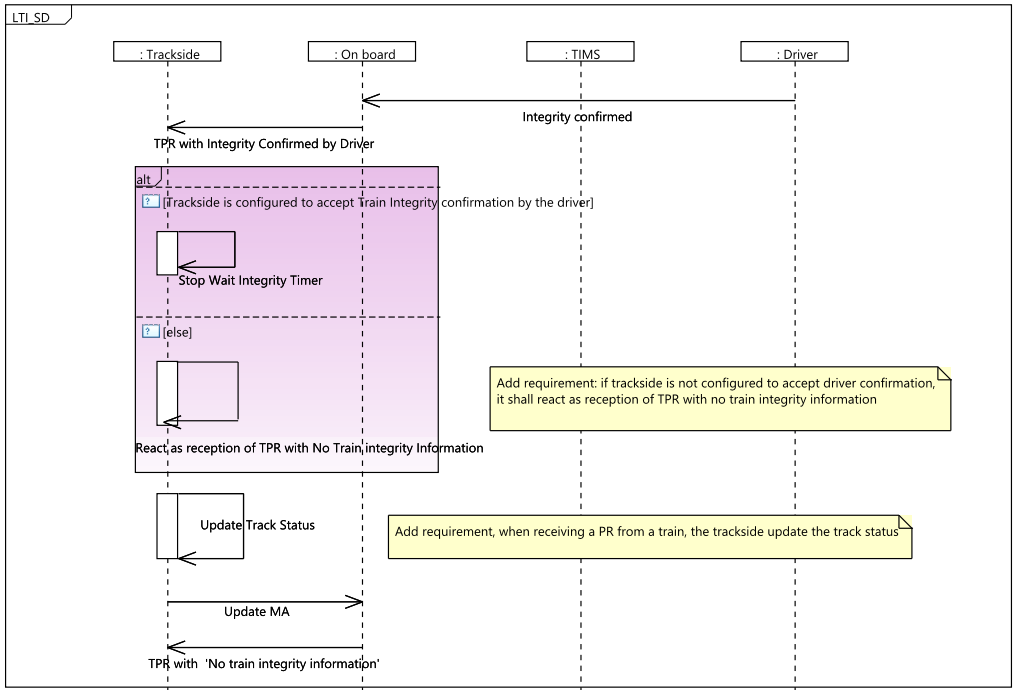

Figure 4 – *Loss of train integrity SysML sequence diagram*

While modelling the various interactions through the SysML sequence diagram, some missing requirements have been identified. For instance, if the trackside is not configured to accept train integrity from the driver, then its reaction is not explicitly defined. To fix this issue, we proposed to add a requirement such that if the trackside is not configured to accept a confirmation of the train integrity by the driver, then it shall react as if the received TPR does not hold any train integrity information. It is worth noticing that identifying such lacking requirements as early as from the requirement engineering step is crucial, since this allows a substantial gain during the subsequent engineering activities [Ghazel (2014)].

In the next step, we will proceed with checking the correctness, robustness and completeness of the LTI UC requirements.

3 Conclusion and future works

In this paper, we introduce a methodology framework aiming to produce generic semi-formal and formal models for the Moving Block system in order to ensure that the ERTMS/ETCS Level 3 requirements are safely defined. Illustrations through the loss of train integrity use case are also presented. In the future work, further operational scenarios and use cases will be considered, before proceeding with the formal modelling activity, per se, and the V&V process that will allow us to check the various safety and functional properties on the L3 MB system.

References

Alikoc, Baran, Mutlu, Ilhan, & Ergenc, Ali Fuat. 2013. Stability Analysis of Train Following Model with Multiple Communication Delays. vol. 1.

Furness, Nicola, van Houten, Henri, Arenas, Laura, & Bartholomeus, Maarten. 2017. ERTMS Level 3: the game-changer. *IRSE News*, **232**, 2–9.

Ghazel, Mohamed. 2014. Formalizing a subset of ERTMS/ETCS specifications for verification purposes. **42**, 60–75.

Hoang, Thai Son, Butler, Michael, & Reichl, Klaus. 2018. The hybrid ERTMS/ETCS level 3 case study. *Pages 251–261 of: Int. Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z.*

Seceleanu, Cristina, Flammini, Francesco, Marrone, Stefano, Mogavero, Fabio, Nardone, Roberto, Starace, Luigi, Vittorini, Valeria, Beugin, Julie, Ghazel, Mohamed, Saddem, Rim, Goverde, Rob, Versluis, Nina, Janssen, Bob, Garcia, Miquel, Samra, Mohamed, & Mazini, Achila. 2021. *Deliverable D 2.1 Modelling Guidelines and Moving Block Use Cases Characterization.*