Chapter 9
Conclusion

Simon Collart-Dutilleul

Starting from the fact that railway high-speed trains running at a speed higher than 300 km/h are becoming common, the first part of this book has presented a context integrating various parameters.

The first one is the diversity of safety national rules that must be considered while crossing borders. The second one is the economical interest of international passenger lines that correspond to a societal need. The third one is the technological framework provided by the European community, namely the ERTMS framework. The corresponding chapter of this book presents not only a current state of the ERTMS specification, but a strategic choice of preserving a stable kernel during a given amount of time in order to allow a commercial use. Moreover, the specification of retrocompatibility properties is presented too. It provides the possibility to use more recent ERTMS released rolling stocks on an older released infrastructure for example. These two properties are raising the specification to a life cycle compatible one. ERTMS specification is a living specification, made for accompanying future technological innovations, like moving blocks for instance, toward a commercial efficient use.

The ERTMS chapter is followed by a description of CTCS, which can be seen as an equivalent proposition in China. This proposition is aligned with the assumption that the ERTMS proposition is an alive specification that may be instantiated and may evolve differently, taking into account various contexts including specific needs or new technologies.

The last section of the first part devoted to the background of transnational high-speed railway lines is a short state of the art. It presents tools and approaches that have been successfully experimented. Perspectives associated with several European projects are explained. This section provides the core material that is used

S. Collart-Dutilleul (✉)
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_9

to build a systematic proposition to be used for designing a safe border crossing solution. This is the focus of the second part of this book. Moreover, the state of the art opens to future tooled approaches that promise more efficiency. Actually, it leads to the identification of the next scientific challenges.

Building on the technological and scientific fundamentals of the first part of the book, the second part argues and details a scientific and technological framework allowing addressing the border crossing problem while running ERTMS.

The problem is broken out into two different dimensions: the vertical one and the horizontal one. By vertical, we mean the problem of aligning the operating rule with the ERTMS specification while respecting national lines that are based on a safe interlocking layer.

The horizontal point is common to many cyber-physical systems : trains do not cross instantaneously the border, because they have a given length and because they move with a finite speed. Beyond this physical layer, trains crossing the border need to comply with the countries safety and technical laws. Commpliance with these laws is performed by automation and software services, which cannot simply be switched from one set of rules to another. Therefore, a transient mode must be implemented.

The first chapter provides a synthetic presentation of the global strategy. Then, it proposes a UML-centered approach to integrate UML models of national operating rules into the global railway system. The model engineering is presented as a key technology, as various models are well adapted to describe various types of knowledge. An example of relay-based specification corresponding to a real industrial system is presented. Then, the specification is translated in abstract B machines.

Formal methods-based proofs correspond to the second main proposition of this chapter: checking the global consistency using the B method. It leads us to introduce a systematic translation of UML models of operating rules in abstract B machines using the B4Msecure tools. One of the advantages of this framework is that it separates the functional part and the safety part in the model.

Nevertheless, Event B for system modelling seems to be more adapted. A new version of the tool proposes to translate the UML profile into Event B. Today, safety requirements are introduced at this stage in the model by the mean of safety invariants. Using the goal engineering tools to build these safety invariants independently from technical choices should be more appropriate.

The global safety approach assumes that the interlocking layer behaves correctly, while collaborating fairly with the ERTMS layer (by the mean of the RBC in ERTMS level 2). A whole chapter focuses on this subject. It mainly proposes a generic high-level Petri net model of a railway infrastructure that can be instantiated on a wide variety of infrastructures. This generic pattern embedded the classical French signaling rules to be respected as well as constraints for route forming or train itinerary tracing.

In this particular case, the safety constraints are well known, and they can be checked using the associated model-checking tools, when the corresponding model is not too large.

The translation of high-level Petri nets model into B machines is not presented in this chapter, while there are substantial works in the state of the art devoted to this task. This translation is needed in an approach based on the definition of a global model of the system fulfilling global safety invariants. The last chapter of the book details the border crossing. A proposition is to formalize the problem using a system of system approaches where various functioning modes can be applied when common functioning modes exist. The ERTMS structures use a quite compatible design philosophy, allowing an easy implementation of the approach. Nevertheless, a specific transient mode has to be introduced, fulfilling an intersection of the set of constraints imposed by the first and second countries. A high-level Petri net-based modelling approach is proposed, and some elementary properties insuring the global safe functioning of the system can be checked. A translation of the Petri net model is needed in order to allow proving global invariants while integrating the corresponding operating rule, but it is not presented in this book.

Even if all models are not presented or detailed, a global modelling approach that aims at specifying the problem of international railway lines is presented in this book. The proposed framework allows the use of specific dedicated formalisms when there exists a way of translating the model into abstract B machines.

Nevertheless, a lot of modelling works have to be performed by the experts in the current proposition. Using the BIM implementation provided by the initiative IFC-Rail will deliver a huge amount of structured data that may allow avoiding some repetitive modeling tasks. Moreover, through the OntoRail project, IFC-Rail is aligned with a functional model of the railway topology (this is the RailTopoModel contribution). This functional specification is to be used to feed the building process of formal models analyzed for safety assessment. The more promising element is the project to make RailTopoModel evolve to RailSYS, providing a global functional ontology of the railway system. When this goal will be achieved, a lot of difficult alignment tasks are avoided. Moreover, it will be possible to propose the automation of the formal modelling task.