Formal Verification of EULYNX Models Using Event-B and RODIN

Abdul Rasheeq[1,2] and Shubhangi Salunkhe[1,2]

DB Netz AG[1], Neovendi GmBH[2]

{shubhangi.salunkhe-extern, abdul.rasheeq-extern}@deutschebahn.com
{s.salunkhe, a.rasheeq}@neovendi.com

Abstract

Advancements in technology have improved the safety of railway transportation systems. However, railway operators face challenges when constructing and maintaining systems that use components from a variety of suppliers. Obsolescence may result in the need to replace complex components with equivalent parts while ensuring that the operation and safety of the overall system are not compromised.

This abstract presents a model-based systems engineering (MBSE) approach for the specification of Deutsche Bahn's railway interlocking system (RIS) to address two issues: The first issue is the separation of the life cycles of the interlocking core and the field elements to reduce the vendor lock-in risks when upgrading or renewing railway field elements such as a level crossing, point machine etc. The second issue is achieving the required assurance that safety properties are preserved by the specification.

In the EULYNX consortium, European railway infrastructure managers develop standard interfaces and subsystems for the next generation command, control and signaling (CCS) architecture. Model-based systems engineering (MBSE) is used to ensure soundness and completeness of the specified interfaces. In order to achieve this, we propose a diagrammatic MBSE framework so that safety compliant standardized models of the interface specifications can be handed over to the railway suppliers. In this framework, Infrastructure managers define the appropriate use case descriptions and modelling experts convert the use cases into executable SysML models using the Windchill Modeler3 tool. Subsequently, infrastructure managers evaluate whether the specified interfaces are sound regarding their intended use applying simulation-based testing. Modelling of the interlocking system interfaces using SysML which is a semi-formal language has already led to significant improvements in the quality of created specifications but does not allow formal verification of system properties. Our proposed framework enables the transformation of SysML models into the Event-B formal language to prove the safety requirements. Figure 1 depicts the overall verification and validation approach.

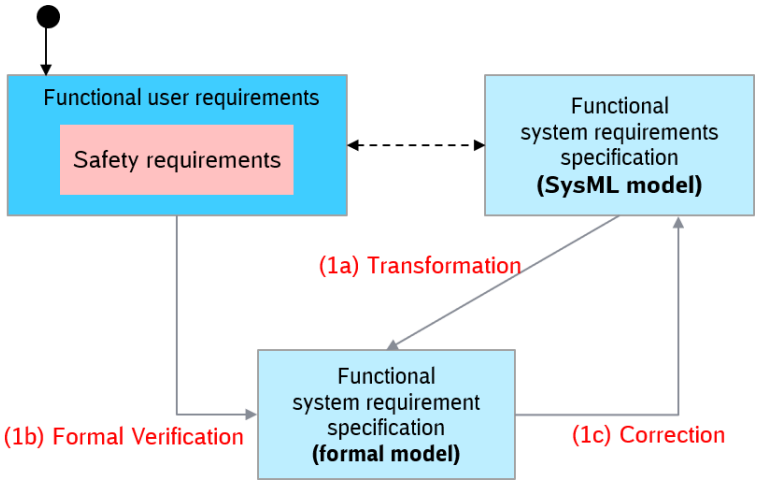
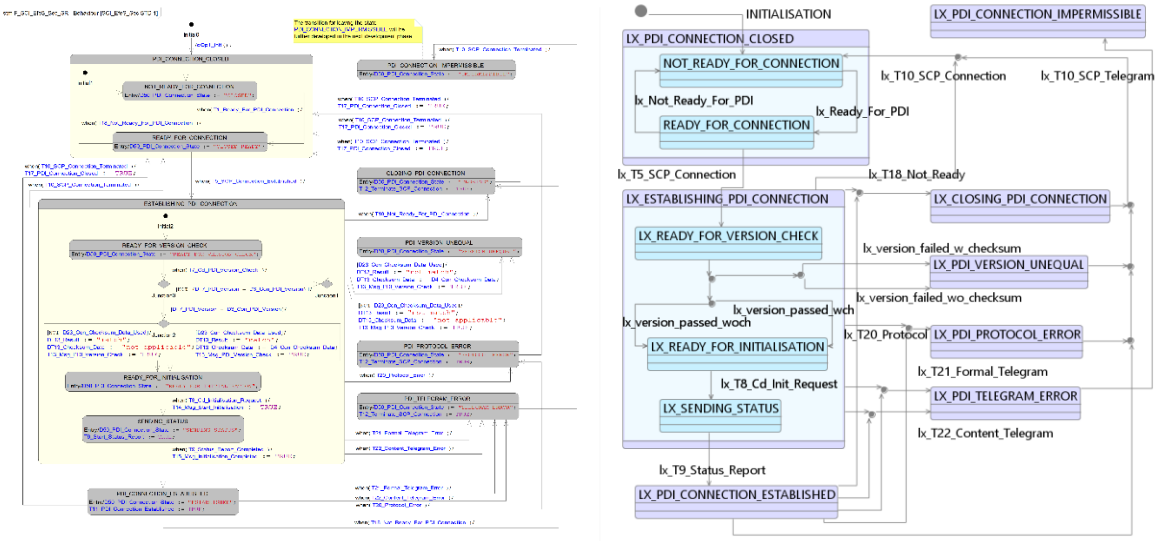


Figure 1: The principle behind formal modelling and verification

Initially, we achieved the transformation in step (1a) manually using UML-B which is a UML-like front end for Event-B and performed the formal verification of safety requirements. This transformation was applied on multiple EULYNX interface models. The following Use Case 1 shows one of the equivalent UML-B model of SysML model achieved using manual transformation.



Use Case 1: SysML Model and equivalent UML-B Model

During this formal transformation and verification, we observed that, the manual transformation of models is time consuming especially when the complexity of models increase (as we can see in Use Case 1). This led to the idea of having the automatic transformation, which will reduce the efforts require for manual transformation and makes the overall V&V approach more efficient.

The objectives of the automatic transformation are as follows: (1) The main objective is to propose a methodology and tool-chain to automate the transformation of SysML specification models into formal models (Event-B). (2) The traceability should be maintained between informal requirements and the modeled system, specifically for the safety properties. (3) The model should be verified against such safety

requirements using formal methods with some tool support. (4) Reduce the efforts involved in the manual transformation of the SysML semi-formal model to a formal model. This approach proposes a transformation using Triple Graph Grammars (TGG) between SysML and Event-B. The automatic transformation is an advancement of the approach explained in Figure 1.

In the manual transformation from SysML to UML-B we were able to identify and rectify the errors in SysML model, which were not detected during simulation-based testing and subsequently able to prove the safety requirements for EULYNX models. In the automatic transformation approach, we are able to successfully implement a prototype that acquire elementary constructs of the SysML state machine. We plan to extend the transformation for more complex state machine constructs to provide the practical applicability of the transformation to the real-world models (e.g., EULYNX models). The proposed MBSE framework for Verification and Validation has changed the perspective of Infrastructure managers like Duetsche Bahn and ProRail for the standardization of railway interfaces.