Constructing an Event-B Model using Promise-Driven Modeling *

Felix Schaber[1,2]

[1]Hitachi Rail, Austria
[2]Heinrich Heine University Düsseldorf, Germany

Abstract

This workshop presentation describes the construction of an Event-B model for a novel type of train protection system, called the moving block system, which is currently being investigated as part of Europe's Rail Joint Undertaking. The moving block system allows for more dynamicity than the fixed block approach traditionally used in railways. The Event-B model is constructed in Rodin using promise-driven modeling. The core idea behind promise-driven modeling is to prioritize modeling those parts of the system requirements that are least likely to change in later stages, hence supporting early validation through animation. Experiences and lessons learned when constructing the Event-B model of the moving block system using promise-driven modeling are described.

1 Introduction to Promise-Driven Modeling

It is well known that errors discovered in the early stages of system development are significantly less costly to fix than those found later [1]. Modeling is often promoted as a way to catch errors early, thereby reducing overall costs. However, as system complexity grows, so does the complexity of the model.

Consequently, errors introduced in early modeling stages can also become increasingly expensive. Getting this right on the first attempt is a known challenge, particularly for cyber-physical systems, where it is often unclear which part of the system should be modeled first and at what level of detail.

When the system is safety-critical, the model must also support reasoning about safety properties. To address this, we use System Theoretic Process Analysis (STPA) to decompose the system into individual controllers and identify the safety constraints associated with each controller.

This presentation introduces promise-driven modeling as a solution to the challenges mentioned above.

Promise-driven modeling is based on the principle that behaviors least likely to change during model evolution are modeled first. Prioritizing design decisions by their likelihood of change is a generally considered best practice [2].

*Partly funded by the European Union Grant Agreement # 101102001.

This reduces the risk of discovering the need for high-level changes late in the modeling process. High-level changes often ripple through the refinement chain, making them resource-intensive.

The promise-driven modeling approach is used to construct an Event-B [3] model in Rodin [4]. The model is visualized in ProB2-UI using VisB [5]. This allows experts to validate model behavior, even with no prior experience with or knowledge of Event-B.

2 Moving Block System

The moving block system (MBS) controls the movement authorities (MAs) sent to trains [6]. An MA limits how fast and how far a train may run safely. These MAs are enforced by an on-board-unit (OBU) on the train. The OBU calculates the braking curve and enforces the onset of braking if the train driver brakes too late to keep the train within the limits of the MA.

The MAs are proposed to MBS from an external system. MBS can decide to grant or reject the proposal for an MA. Only granted MAs are sent to the train. MAs contain mode profiles describing the responsibility split between MBS, OBU, and the train driver for avoiding collisions. For this workshop, we'll focus on the full-supervision European Train Control System (ETCS) mode, where the MBS is solely responsible for ensuring that the track is and stays clear of trains and obstacles (known at the time of the request). The OBU can request a new MA from the MBS (MA request).

The OBU sends train data (TrainData) to MBS, estimates the physical train position, and periodically sends train position reports (TPRs). Trackside train detection systems (TTDs), installed at fixed sections along the tracks, also detect physical train presence, and information about train presence is sent to MBS.

The Event-B Model model for a selected part of this system is constructed using promise-driven modeling.

3 Conclusion

Using promise-driven modeling, an Event-B model for the moving block system was constructed and the associated Proof Obligations were discharged. During the modeling process, a number of open points and potential gaps were discovered. Animation in ProB2-UI using VisB allowed to discuses associated behaviors with domain experts who had no previous exposure to Event-B or formal modeling.

The promise log contained all promises from which the Event-B model was constructed, closely linking Event-B model with the expected behavior described by the promises. For unexpected model behavior, this promise log was helpful for fostering a discussion between domain experts, who are typically familiar with descriptions of behavior than formal modeling details.

References

[1] N. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety.* 2012.

[2] Nancy G. Leveson. "Design and Assurance of Control Software". In: *IEEE Transactions on Software Engineering* 51.3 (Mar. 2025), pp. 666–672. ISSN: 0098-5589, 1939-3520, 2326-3881. DOI: 10.1109/TSE.2025.3539975. URL: https://ieeexplore.ieee.org/document/10877915/ (visited on 03/30/2025).

[3] Jean-Raymond Abrial. *Modeling in Event-B - System and Software Engineering.* Cambridge University Press, 2010. DOI: 10.1017/CBO9781139195881.

[4] Jean-Raymond Abrial et al. "Rodin: An Open Toolset for Modelling and Reasoning in Event-B". In: *International journal on software tools for technology transfer* 12 (2010), pp. 447–466.

[5] Michelle Werth and Michael Leuschel. "VisB: A Lightweight Tool to Visualize Formal Models with SVG Graphics". In: *Rigorous State-Based Methods.* Ed. by Alexander Raschke, Dominique Méry, and Frank Houdek. Vol. 12071. Cham: Springer International Publishing, 2020, pp. 260–265. DOI: 10.1007/978-3-030-48077-6_21.

[6] Nina D. Versluis et al. "Real-Time Railway Traffic Management under Moving-Block Signalling: A Literature Review and Research Agenda". In: *Transportation Research Part C: Emerging Technologies* 158 (Jan. 2024), p. 104438. DOI: 10.1016/j.trc.2023.104438.