Rodin in the field of railway system engineering

Tomas Fischer

Thales Austria GmbH, Handelskai 92, 1200 Vienna, Austria,
tomas.fischer@thalesgroup.com

Abstract. Railway signaling systems are required to provide the highest safety level due to the risk of loss of human life. Formal methods can contribute to the reliability and robustness of specification, design and implementation of such systems and support their verification and validation. Moreover, the CENELEC standards [1–3], which define the certification process of safety critical applications in the railway domain, qualify the use of formal methods as highly recommended.
However, the application of formal methods is very labor intensive, and thus expensive. A formal model of the respective system has to be created, maintained over the long product lifespan (25+ years) and reasoned about not only during the development phase, but recurringly at each modification of the evolving specification. Qualified experts with versatile skills are inevitable for this job. These experts are required to transform a semi-formal domain model (as understood by the domain experts) into the mathematical one and keep both of them aligned. They are also expected to interpret the verification and validation results and to communicate them to experts from other domains. These tasks demand a good tool support assisting users in all development phases with the aim to reduce manual efforts and thus decrease overall costs (see also [4]).
In the industrial context formal methods can be used as a one-time shot (e.g. prove the correctness of one particular algorithm) or continuously, as an integral part of the development process and therefore integrated into the development toolchain. Whilst the former usage has already been studied well and there are some very promising results available, the latter one encounters several obstacles.
At the workshop we present our experiences with introducing formal methods (in particular Event-B with the Rodin toolset) for the development of a railway interlocking system and discuss our current technical maturity assessment of the Event-B tools. On a small model we demonstrate the identified mismatch between the engineering demands and business needs on one side and current state of the Rodin toolset on the other side. Finally we propose some measures how to increase Rodin's usability (and hence the productivity) without sacrificing its profound theoretical foundation.

References

1. CENELEC, E.N.: 50126-Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization (1999)

2. CENELEC, E.N.: 50129-Railway Applications: Communication, signalling and processing systems - Safety related electronic systems for signalling. European Committee for Electrotechnical Standardization (2003)
3. CENELEC, E.N.: 50128-Railway Applications: Software for Railway Control and Protection Systems. European Committee for Electrotechnical Standardization (2011)
4. Romanovsky, A., Thomas, M.: Industrial deployment of system engineering methods. Springer (2013)