

Translating Event-B models into Elisa - A Case Study in Railway Automation

Tibor Kiss, Florin Craciun, Bazil Parv

Department of Computer Science, Faculty of Mathematics and Computer Science
Babes-Bolyai University, Cluj-Napoca

{kisst, craciunf,bparv}@cs.ubbcluj.ro

Automatic translation of the verified formal models into programming languages is the foundation of the correct-by-construction approach, used to develop safety critical systems. Making connection between a formal method, like Event-B and a modern programming language, like Elisa, can open new research areas, and also can improve the software development of safety critical systems. We have made a deep analysis of this translation process, taking into account different aspects of translation, like software maintainability and human understandability. For this reason we tried different translation approaches to improve the translation process. We analysed the opportunity to generate the verification code, to prove the translation correctness, and also to give the opportunity to the developer to modify the source code and to check the modification correctness corresponding to the Event-B invariants.

References

- [1] Abrial, Jean-Raymond: Modeling in Event-B: System and Software Engineering (2010)
- [2] Dominique Mery and Rosemary Monahan: Transforming EVENT B Models into Verified C# Implementations(2013)
- [3] Dominique Mery and Neeraj Kumar Singh: Automatic code generation from event-B models(2011)
- [4] Jan Klunder: Elisa & Domain Orientation(2014)