Abstract

This thesis focuses on the modeling and the safety requirements verification of a communication system in the railway signaling domain where the use of standard interfaces and formal methods is increasing and is also expanding at the industrial level.

The adoption of formal methods and standard interfaces can favor the interoperability between systems provided by different suppliers, thus increasing the market competition while ensuring higher safety standards.

To promote the use of these two key aspects in the European signaling area, the Eulynx and the 4SECURail initiatives were conceived with the specific aim of standardizing the interfaces and the elements of the signaling systems, and contributing to the widespread diffusion of the formal methods in the industrial applications, respectively.

In particular, this thesis takes into account the same railway signaling subsystem identified by the 4SECURail project to exercise a formal methods demonstrator, providing a formal analysis of the system starting from its safety requirements. The selected case study concerns the RBC/RBC handover protocol specified in natural language through a public standardized interface.

One of the aims of this work is to contribute to the 4SECURail evaluation of the cost-benefit analysis for the adoption of formal methods by providing some useful data on the efforts made to reach the results we are about to describe in this thesis. For the formal modeling and verification of the system, we chose to use Stochastic Timed Automata and Statistical Model Checking, and in particular the UPPAAL SMC toolbox has been used.

The resulting artifacts can provide a further contribution for the definition of unambiguous system requirements, enriching the documentation with consistent and formally verified model-based specifications as promoted by the Eulynx project.