Formalizing Rulebooks for Railway Operations

Eduard Kamburjan, Prof. Dr. Reiner Hähnle
Software Engineering Group, TU Darmstadt

Railways: Managing Safety in Distributed Systems since 1825!

The FormbaR project aims to model and analyze the Deutsche Bahn rulebooks for railway operations with the methods and tools developed in computer science for distributed software systems.

Can railway operations benefit from the theory of concurrency in Computer Science?

Reduce infrastructure with new procedures – prove same level of safety

Integration for Usability

We integrate available techniques and tools into a framework for designers of cyber-physical distributed systems:

Modeled in the Abstract Behavioral Specification Language (ABS):
- Based on active objects: object-oriented actors with futures
- Designed with usability and analyzability in mind
- Executable models: allows simulation and testing
- Extensive tool support with e.g., the SACO toolsuite for static analysis and the KeY tool for deductive verification

Multiple approaches for functional specification:
- Top-Down with session types for protocols
- Bottom-Up with method contracts for critical subroutines
- Trace Logic for formalization of subsystems and partial protocols

Abstraction: Model Rulebooks – Not Physical Systems

Analysis focuses on scenarios described in the rulebooks
- Simplifies physical train driving
- Enables simulation of large networks
- Reduces infrastructure to a layered model of information flow
- Reduces communication to abstract message passing:

A railway signal is abstracted away from its construction form (e.g., shape or light) and treated only as an information transmitter for “Go”, “Slow”, “Halt” and “unclear(broken)”:...