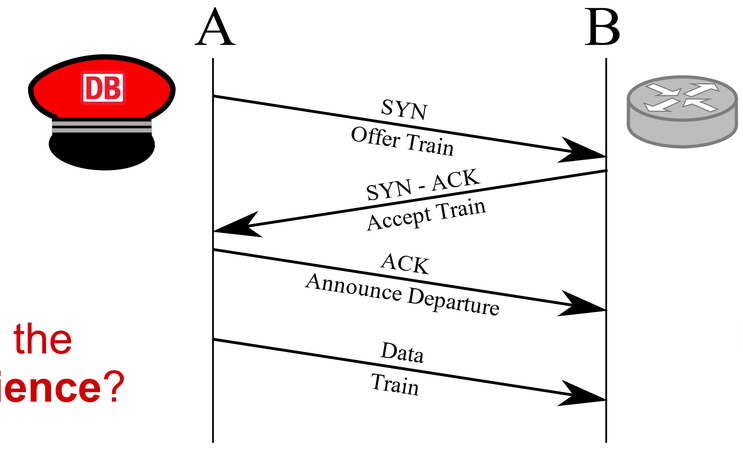
Formalizing Rulebooks for Railway Operations

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

TECHNISCHE UNIVERSITÄT DARMSTADT

Railways: Managing Safety in Distributed Systems since 1825!

Railways deal with **safety in distributed systems** since the 19th century with procedures that prefigure modern solutions: Departing a train from a station *A* to *B* is the same as a TCP handshake.



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:

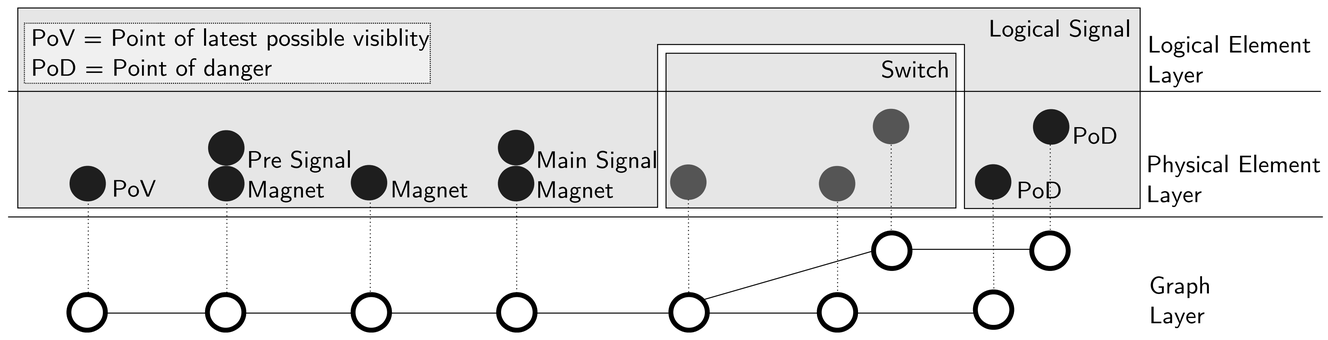
Modeled in the **Abstract Behavioral Specification** Language (ABS):
- Based on active objects: object-oriented **actors** with futures
- Designed with **usability** and **analyzability** in mind
- Executable models: allows **simulation** and testing
- Extensive tool support with e.g., the SACO toolsuite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

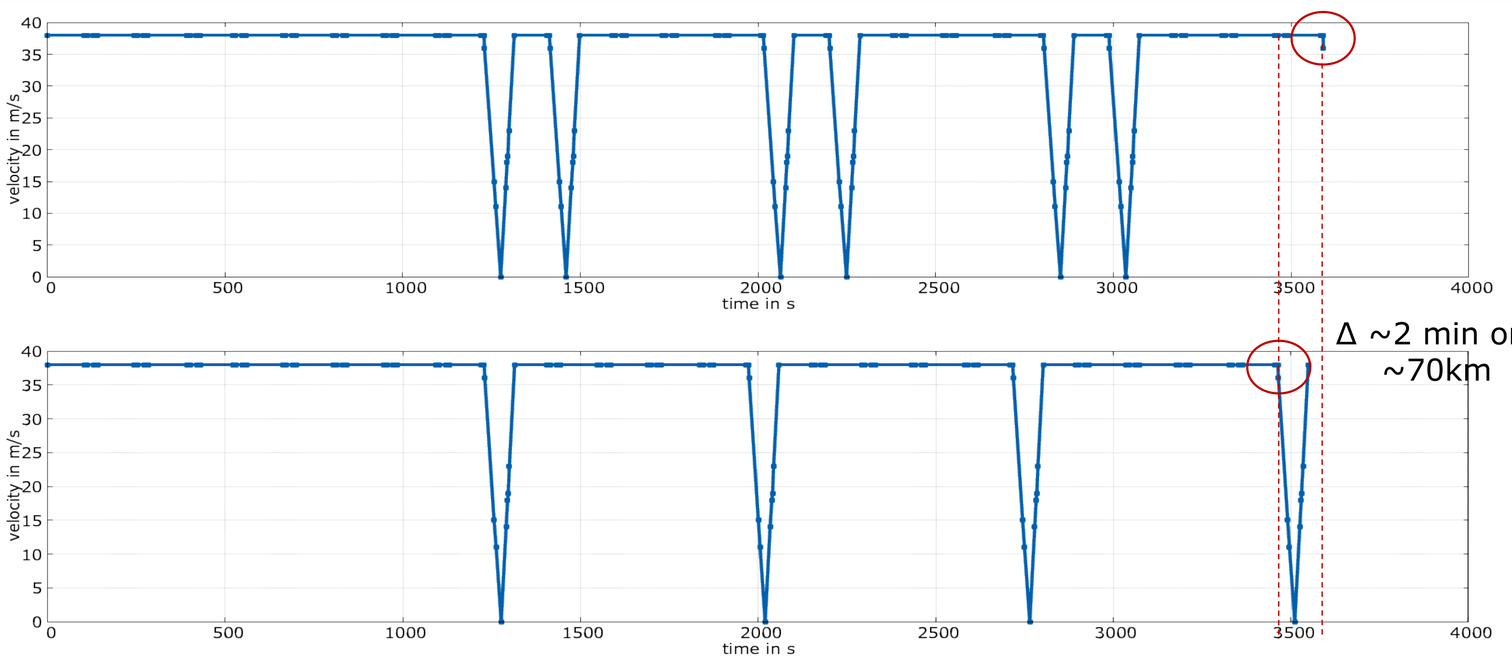
Abstraction: Model Rulebooks – Not Physical Systems

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:**

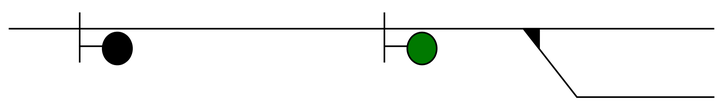
A railway signal is abstracted away from its construction form (e.g., shape or light) and treated only as a information transmitter for “Go”, “Slow”, “Halt” and “unclear(broken)”.



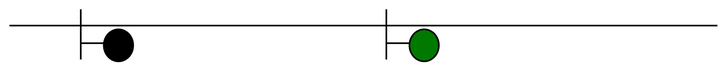
Static Safety – Dynamic Capacity



Simulation of original procedure with 2 stops before a faulty signal



Simulation of changed procedure with only 1 stop if faulty signal covers no switch



- Critical systems require **high level of confidence** in safety proofs
- Safety of rulebook is statically proven for **every well-formed infrastructure**
- Real infrastructure may be imported and used as **test case** for calibration

- Effects on **capacity** depend on possible schedules
- Capacity is analyzed by **simulation on one concrete infrastructure**
- Allows to compare with existing capacity simulation tools for railways

References

- ABS: A Core Language for Abstract Behavioral Specification,
- *E. B. Johnsen, R. Hähnle, J. Schäfer et al., FMCO 2010*
- *Uniform Modeling of Railway Operations, E. Kamburjan, R. Hähnle, FTSCS 2016*
- *Deductive Verification of Railway Operations, E. Kamburjan, R. Hähnle, RSSRail 2017*

Short Facts

- Cooperation project between the chairs of Software Engineering and Railway Engineering at TU Darmstadt and DB Netz AG
- Modeling Railway Operations with Methods from Distributed Systems

Try out the model: formbar.raillab.de

Innovationsallianz DB & TU Darmstadt
DB RailLab | AG Signalling