Theories, Techniques and Tools for Engineering Heterogeneous Railway Networks

Paulius Stankaitis and Alexei Iliasov

Centre for Software Reliability, Newcastle University, UK

RSSRail Conference '17

November 16th, Pistoia

Railway Signalling

Formal Methods for Railway

Developing Distributed Interlocking Model

Formal Verification of Hybrid (Event-B) Models

Conclusions and Future Work

Railway Signalling

Railway Signalling

- Low rolling resistance makes railway efficient for heavy load transportation.
- A train cannot be stopped at a short notice (spatial/temporal separation).
- Railway signalling (interlocking) ensures a safe railway operation.
  - Route-based fixed block signalling.
  - Route-based moving block signalling.

Railway Signalling

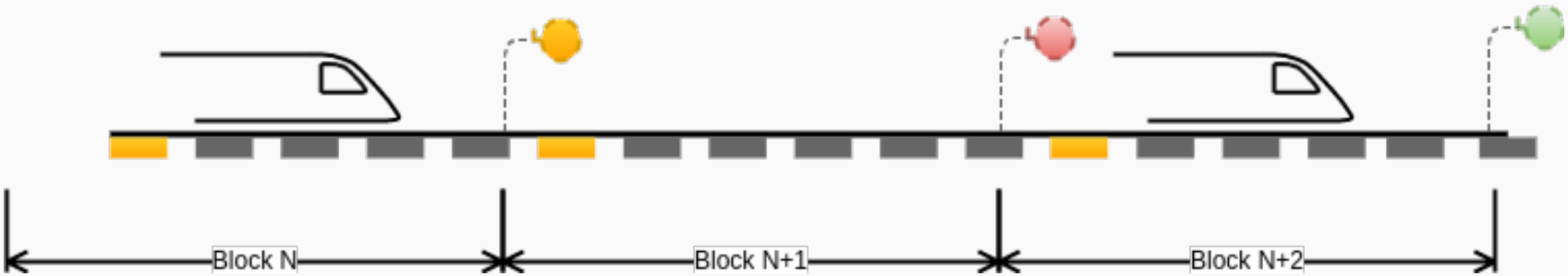


Figure 1: Route-based fixed block signalling. National Signalling Systems, European Train Control System (ETCS) Level 0 - 2.

Railway Signalling

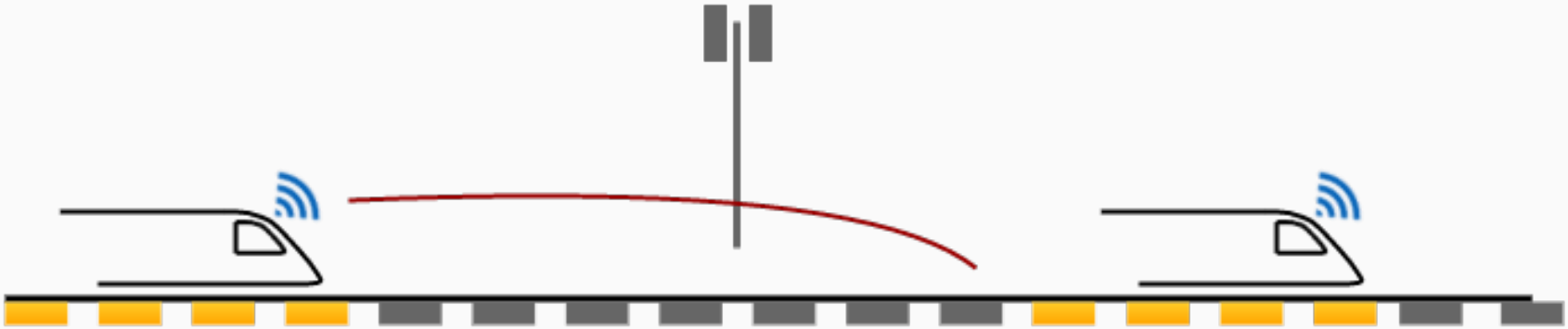


Figure 2: Route-based moving block signalling. Communication Based Train Control (CBTC) System, ETCS Level 3.

Railway Signalling - New Challenges

- Replacing national signalling systems.
- Integrating mainline services with urban networks.
  - Crossrail Network (ETCS, CBTC and TPWS).
  - Thameslink Network (ETCS and TPWS).
- RBC/RBC Handover.
- Trains transition at a line speed.

Railway Signalling - New Challenges

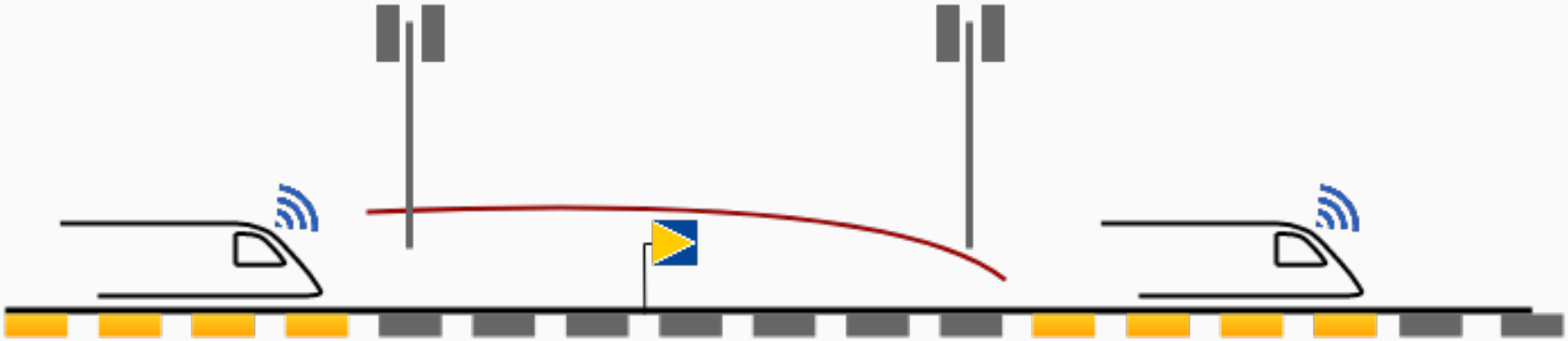


Figure 3: Level Transition. RBC-RBC Handover, ETCS/CBTC Handover.

Formal Methods for Railway

Formal Methods for Railway Domain

- Railway data verification.
  - topology verification;
  - control table verification;
- Distributed nature of railway (larger railway networks).
  - Multiple interlocking communication;
- Cyber-physical nature of railway. ‘
  - Communication, computation and control aspects;
  - Discrete and continuous system behaviour;

Formal Methods for Railway Domain

- Railway data verification.
  - topology verification;
  - control table verification;
- Distributed nature of railway (larger railway networks).
  - Multiple interlocking communication.
- Cyber-physical nature of railway. ‘
  - Communication, computation and control aspects;
  - Discrete and continuous system behaviour;

PhD Objective.

To develop a practical formal verification framework for reasoning about safety of (distributed-hybrid) heterogeneous railway networks.

Developing Distributed Interlocking Model

Generic Safe Railway Model

- A generic safe railway model.
- Automatic mathematical model extraction from the source data.
- Matching dataset against the assumptions of a formal model.
- Counter-example on a schema layout.

Extending Generic Safe Railway Model - Requirements

System Requirement 1. Cross boundary route locking and releasing system must ensure that a cross boundary route has been reserved only to a single train at a time.

Extending Generic Safe Railway Model - Requirements

System Requirement 2. Cross boundary route locking system must ensure that a locked cross boundary route has points properly positioned and signals sets.

Extending Generic Safe Railway Model - Requirements

System Requirement 3. Cross boundary route locking system must ensure that train will cross to the next interlocking zone only if connection with the following interlocking has been established.

Extending Generic Safe Railway Model

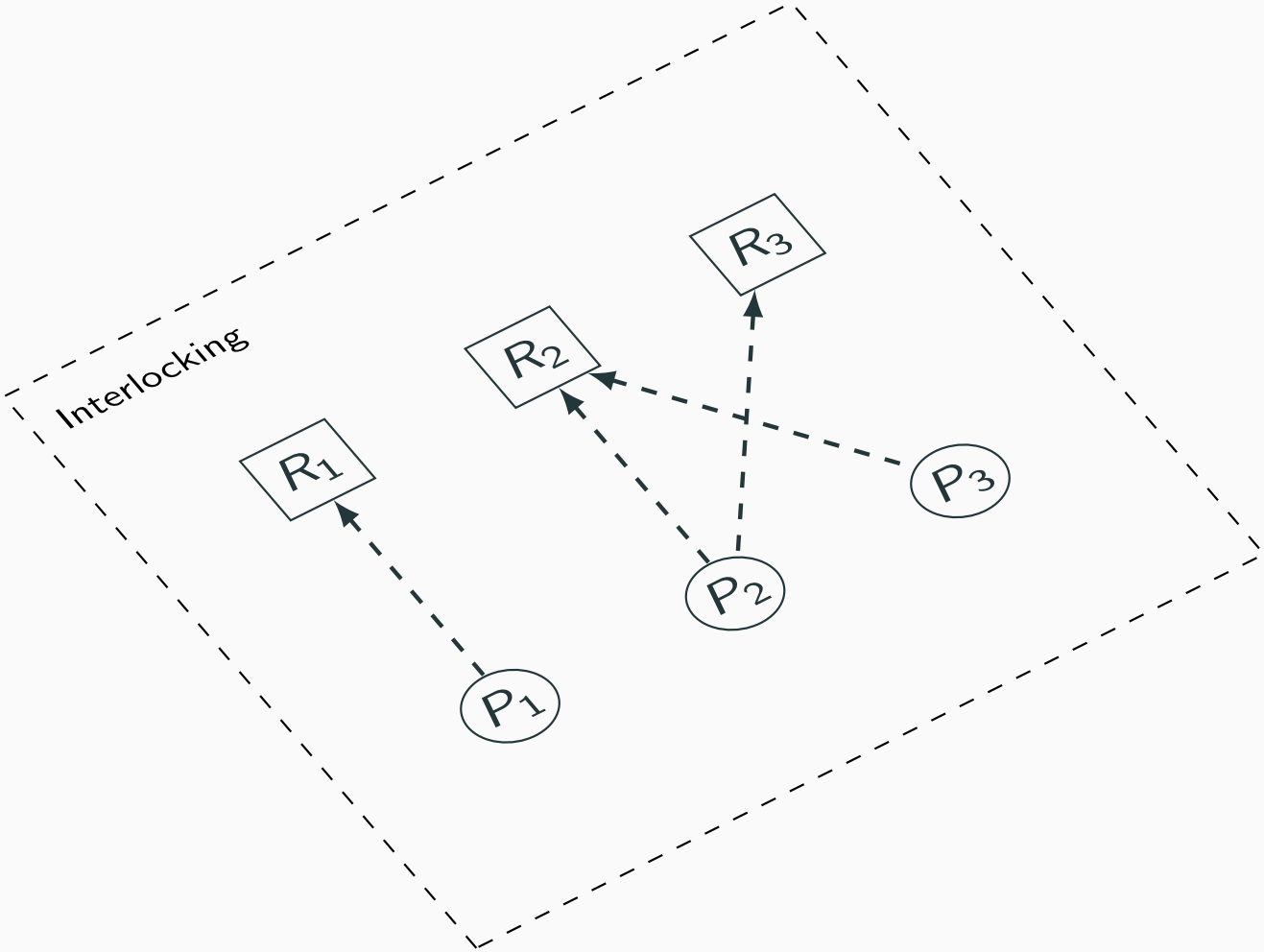
- Event-B modelling to develop the theory of safe railway.
- Theory describes route locking and releasing mechanism.
  - Abscence of collisions;
  - Derailment;
  - Protection of flanks;
- The proof of Event-B model is a one time effort.
- The model is automatically instatiated for a particular schema.
- The control table and topology of a concrete railway is safe if instantiated model is an instant of a generic.

Extending Generic Safe Railway Model - Refinement Plan

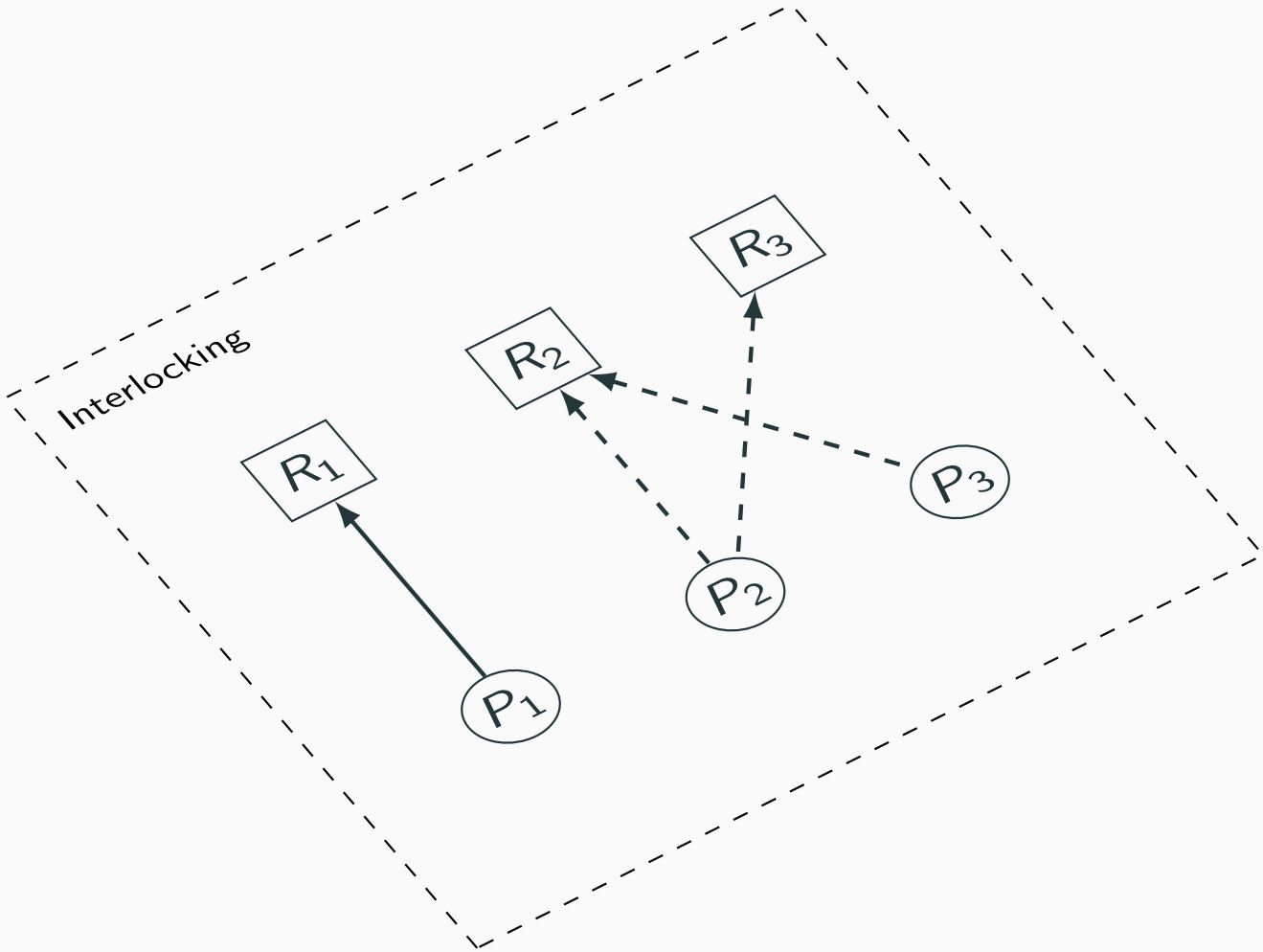
Event-B model refinement plan.

1. Abstract model of processes capturing resources.
    - Global controller and a shared-resource problem.
    - Distributing controllers.
    - Introducing graph into the model.
2. Introducing railway related information.
    - Routes, lines, points, signals.
    - Route locking mechanism.
3. Including a hybrid part for level transition.

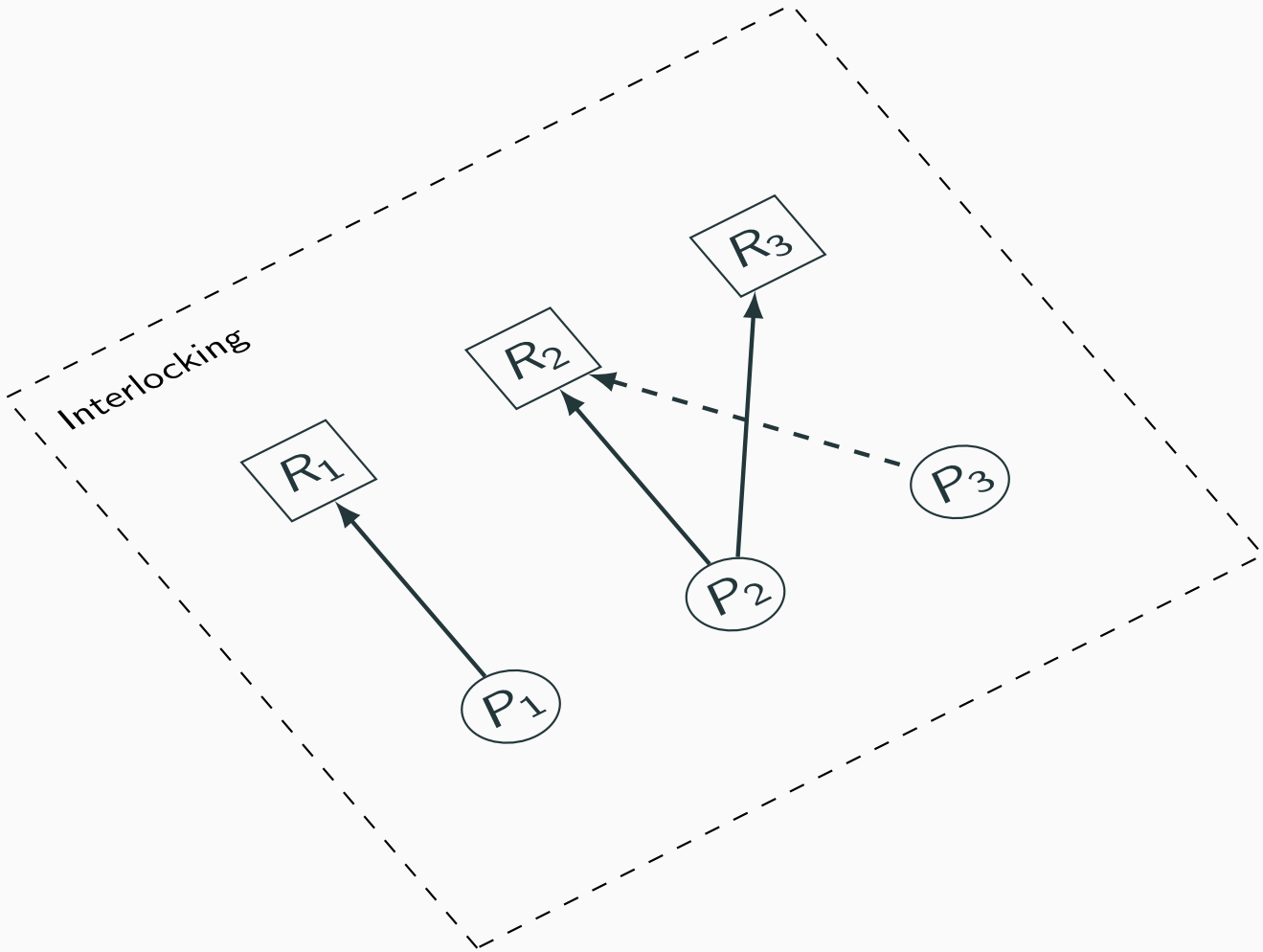
Extending Generic Safe Railway Model - Abstract Model



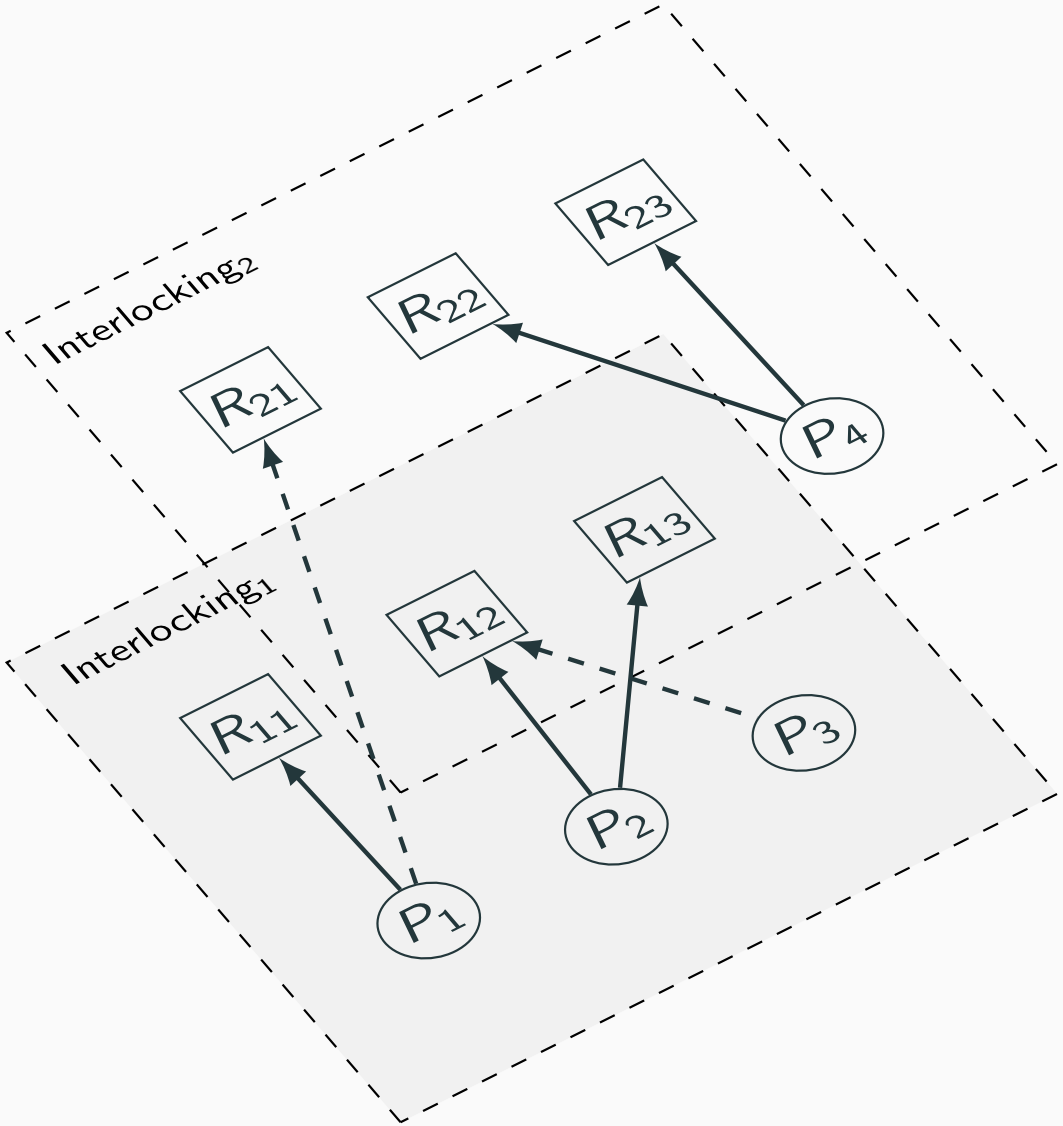
Extending Generic Safe Railway Model - Abstract Model



Extending Generic Safe Railway Model - Abstract Model



Extending Generic Safe Railway Model - Abstract Model

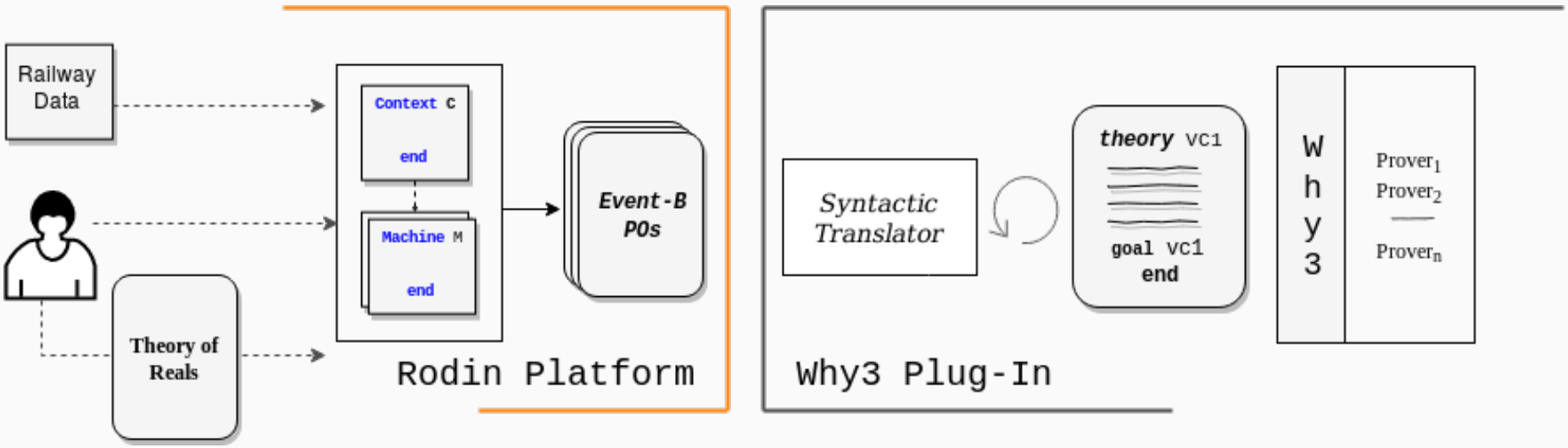


Formal Verification of Hybrid (Event-B) Models

Automated Theorem Proving and Cloud Technology

- In recent years a lot automated theorem provers were developed.
  - SMT based provers (e.g. Z3, CVC3)
  - Umbrella proves (e.g. Why3)
- Automated theorem proving is computationally intensive exercise.
- Cloud technology offers:
  - cheap computational power,
  - flexibility,
  - process parallelism.
- Reasoning about continuous behaviour is difficult (interactive).

Automated Theorem Proving and Cloud Technology



Conclusions and Future Work

Conclusions and Future Work

Practical outcomes.

- Safety invariants for cross boundary transition.
- Improved verification automation of hybrid models.

Future work.

- Hybrid framework.