HITACHI

Constructing an Event-B Model using Promise-Driven Modeling

Felix Schaber, Rodin Workshop, 10.06.2025

HITACHI

Motivation

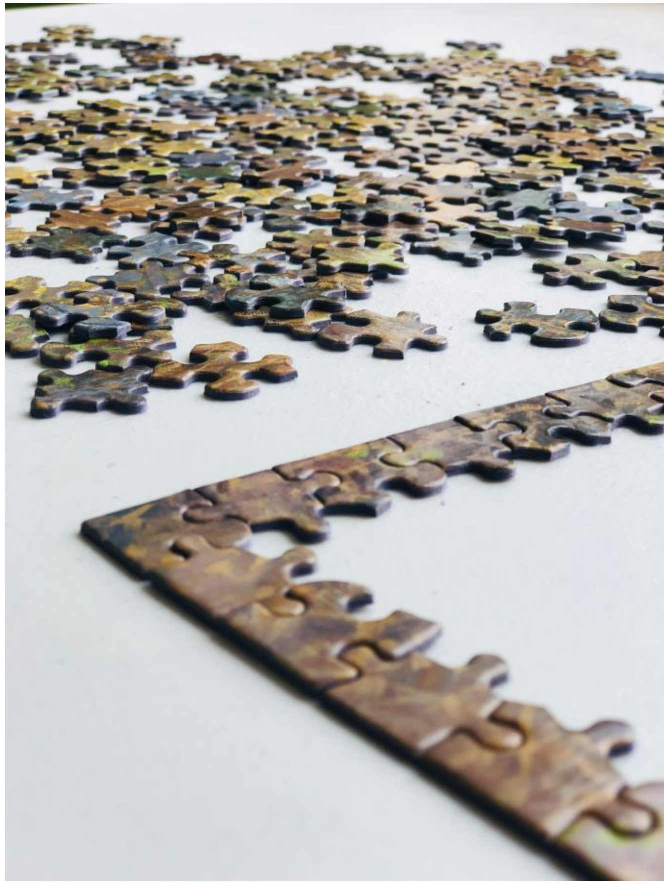
Formal modeling can provide strong safety assurances

→ But resource intensive to perform

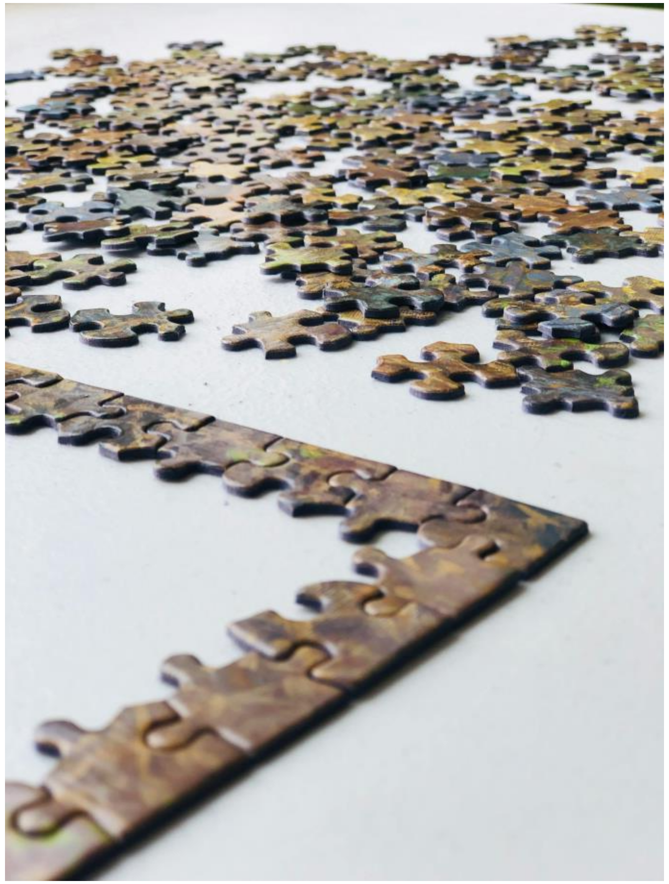
Breaking changes to initial assumptions are typically more resource intensive the later they are performed

→ Getting the initial modeling decisions right is important

The Challenge



Where to start?



Types of complexity

Domain Complexity

Modeling Complexity

HITACHI

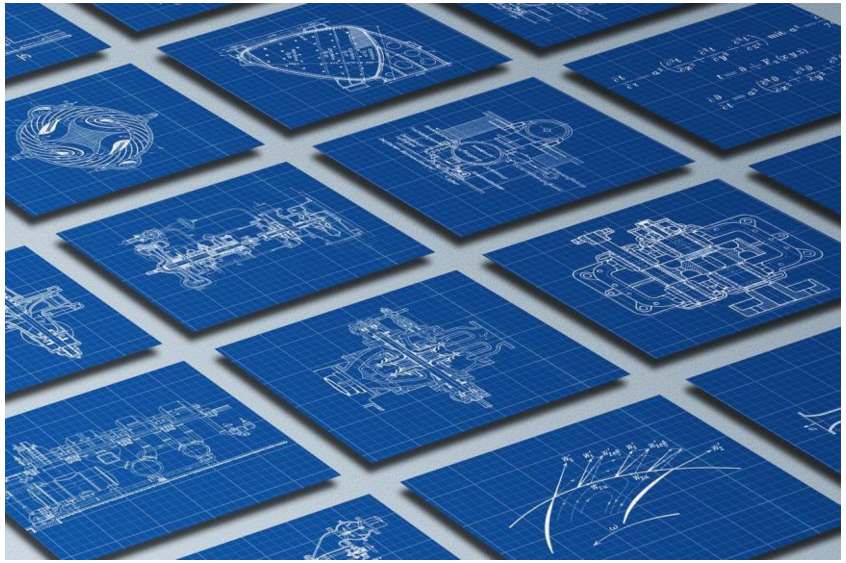
Incremental model development in Event-B

Event-B Refinement

- Helps to build and verify the model step-by-step
- Refinement structure is influenced by the order of modeling
  → can strongly affect required effort to discharge Proof Obligations

→ ordering heuristic desirable

→ increase chances that early modeling decision do not require incompatible changes later



Goals

Derive Event-B Model from domain description

→ Heuristic when to model what parts of the domain

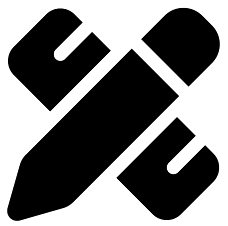
→ Minimize likelihood that model decisions need to revisited later

Apply approach to case study from the railway domain

Methods

System Theoretic Process Analysis (STPA) for hazard analysis
→ Find which safety constraints the model shall keep
→ Focus on parts with the greatest immediate benefit from formal modeling

Promise modeling for domain description and prioritization
→ Domain knowledge are expressed as promises
→ Also describes dependencies on other parts of the system
→ Prioritization heuristic



Promise Theory

HITACHI

Promise

- Promise (π_n) represents intended behaviour
- Made between Sender (S) and Receiver (R)
- Promise body (p) represents formalized content
- Can be (partially) kept or broken

Stability

- Dependable cooperation requires matching promises

Dependencies

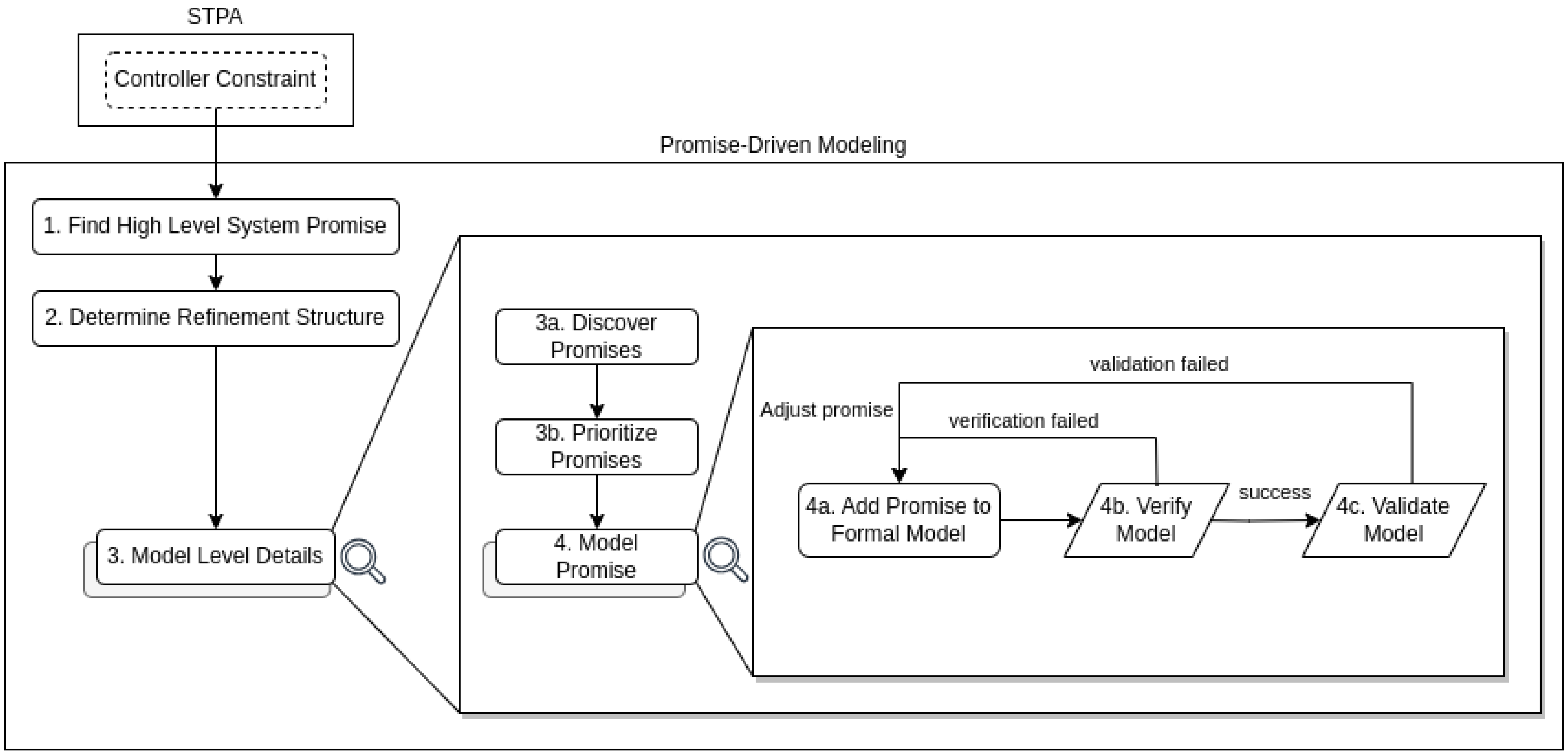
- Body can be conditional on keeping of promise by another agent (c)

$$\pi_n : S \xrightarrow{\pm p|c} R$$

Prioritization heuristic

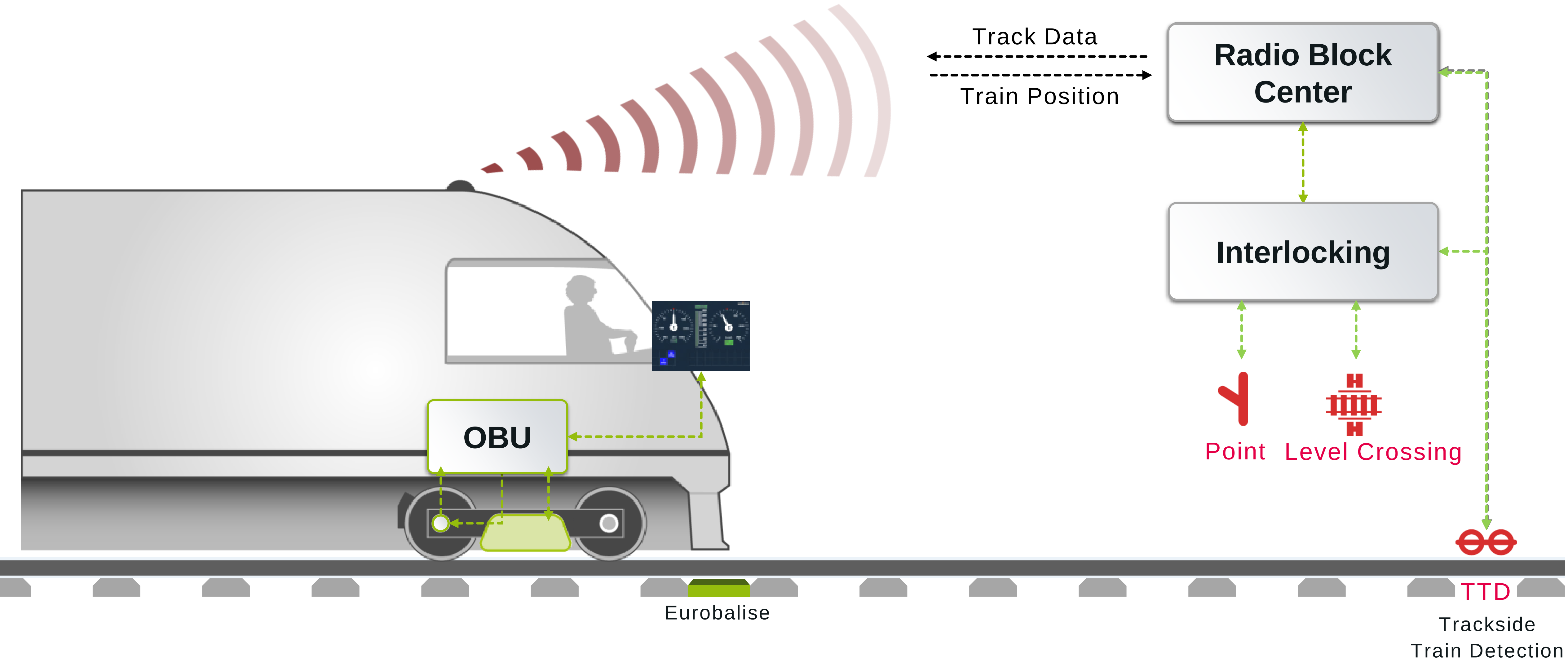
Model parts least likely to require breaking changes first

Promise Driven Development

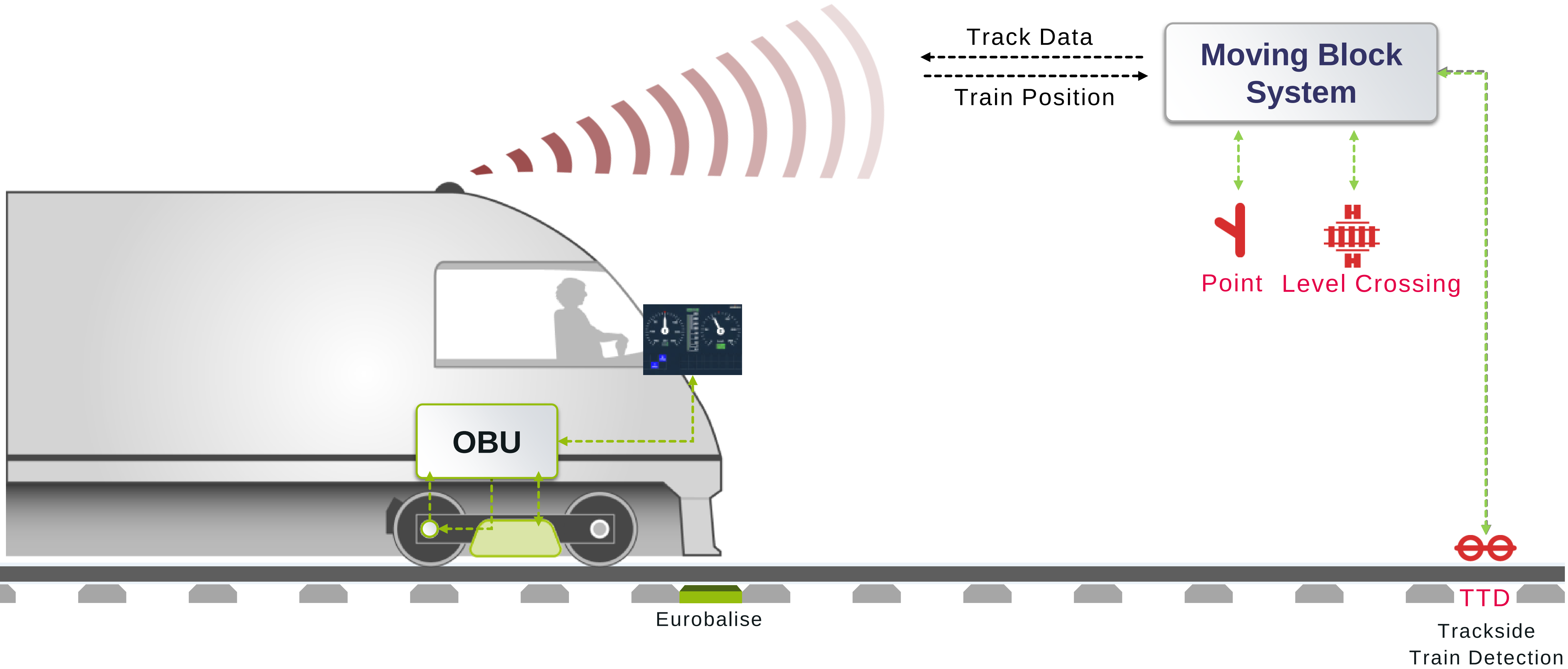


HITACHI

Moving Block System



Moving Block System



Case Study Overview

Train protection
- Simplified model of the European train control system (ETCS)
- Moving Block System (MBS) allow train movements by issuing movement authorities (MA)
- Train On-board-unit (OBU) applies brakes to keep train within MA

System goal
- Prevent the collision of trains
- → Need to detect presence of trains

Train presence
- Detected by fixed trackside train detectors (TTD)
- Reported by train position reports

Focus on the system ability to enforce the movement authority

Findings during the case study

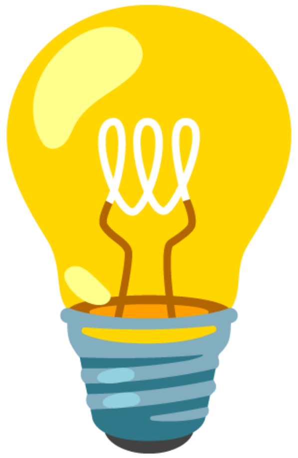
Which promises are modelled first?

→ mainly physical promises

→ often in turn have less reliable dependencies (e.g. physical braking conditions on the track)

→ typically leads to modelling promises not directly observable by MBS first

- Decisions how to represent the domain concepts within Event-B remains
  - e.g. model individual train cars?
  - e.g. create new trains or modify existing trains when splitting or joining trains?



HITACHI

Event-B model

Successfully constructed event-B model using this approach

Promises are traced the parts they affect in the Event-B Code

→ Can simulate the effects of promise braking

→ Facilitates model re-use, as it is immediately clear which parts of the model depend on a given promise

All Proof obligations could be discharged even when the model process lead to target properties being introduced late in the modelling process

Conclusion

– Likelihood of change provided a useful heuristic to decide when to model what part of the system

– Promises allowed to reason about stability and likelihood of change

– Representation and encoding of concepts in Event-B remains an important task of the modeller

More information

Questions?

Felix Schaber, Atif Mashkoor and Michael Leuschel
„Promise-Driven Modeling: A Structured Approach for Modeling Cyber-Physical Systems“
To appear in FMICS 2025