STPA at Europe’s Rail
Felix Schaber, STAMP Workshop 2024

Hitachi Rail
Goals of Europe’s Rail

Mission statement

- To deliver, via an integrated system approach, a high capacity, flexible, multi-modal, sustainable and reliable *integrated European railway network* by eliminating barriers to interoperability and providing solutions for full integration, for European citizens and cargo.
Europe’s Rail Landscape

System Pillar

Task 1

Task 2

Innovation Pillar

FA 1

FA 2

WP 13.3

...
Our Use Case – Moving Block System

- **OBU**
- **Radio Block Center**
- **Interlocking**
- **Track Data**
- **Train Position**
- **Point**
- **Level Crossing**

---

**Trackside**

**Train Detection**

---

**Eurobalise**

---

**TTD**

---
Hazard Analysis for Moving Block System

High level of safety assurance
→ Need for comprehensive hazard analysis

Component interaction important for safety

Early stages of design
→ use STPA
System Evolution

Shift2Rail

EULYNX

Europe's Rail

A BODY OF THE EUROPEAN UNION
Existing requirements

**Difference in**
- System scope
- Assumptions about system requirements

**Strategy**
- Perform STPA
- Extract solution concepts from requirements
- Match loss scenarios to solution concepts
- Identify Gaps
Example UCAs

Unsafe Control Action:
[UCA-MBS-16] MBS provides FS MA to OBU when the area reserved for train is not clear of other trains or obstacles

[UCA-MBS-17] MBS provides MA to OBU when other train or obstacles have insufficient distance from the flank of the area reserved for train movement

Operational context
Type of collision (head-on/rear-on/flank)
Type of vehicle (controlled vehicle/rollaway train)
ETCS mode (full supervision/on sight/staff responsible)
Track occupation (occupied/free/unknown)
Collision speed

…
Relevant solution concepts

**Location of controlled trains**
- Reported Train Position
- Reported Track Occupation

→ Train Location

**Permitted location of controlled trains**
- Movement Authority

→ Area Reserved for Train

**Location of unknown origin**
- Reported Track Occupation

→ Unresolved Trackbound Object
Linking Scenarios to Solution Concepts

- Loss Scenario
  - Operational context
  - Unsafe Control Action

- Scenario simulation

- Document used solution concepts

- Loss Scenario prevented?
  - No → Document safety gap
  - Yes → Next loss scenario
Linked loss scenarios

Leads to loss scenarios with causal factors including:
- Coupling of trains
- Incorrect train lengths
- Train separation
- Roll-away after parking of trains

Prevention of loss scenarios linked to assumptions
- Detection of roll-away trains by trackside train detectors
- Received information about the infrastructure (geographical position of tracks, points, etc.) correctly represent physical reality
Validating Assumptions

Explicit sources
Assumptions stated within requirements
Assumptions stated within STPA

Implicit sources
Design of solution concepts
Responsibilities of other controllers

Differences in stakeholder viewpoints
Example Assumption

Assumption:
Received information about the infrastructure (geographical position of tracks, points, etc.) correctly represent physical reality

Viewpoints:
Moving block system: cannot validate physical correctness of position
Digital register: relies on infrastructure management data validation
IM data validation: exact process not specified as part of the analysis

→ Potentially gap regarding data validation
Lessons learned

**Context of solution concepts is essential**
Implicit assumptions may require reverse engineering
Domain experts greatly help guiding the search for loss scenarios

**Operational procedures are critical**
Covers areas where feedback is insufficient/too late automated controllers to prevent hazards
→ importance increases with automation

**STPA fosters dialog between stakeholders**
Makes context and associated assumptions explicit
Helps synchronize viewpoints early in the design process
Questions?