Towards Scenario-Based Certification of Highly Automated Railway Systems

RSSRail 2023, October 10th, Berlin

Michael Wild, Jan Steffen Becker,
Günter Ehmen, and Eike Möhlmann

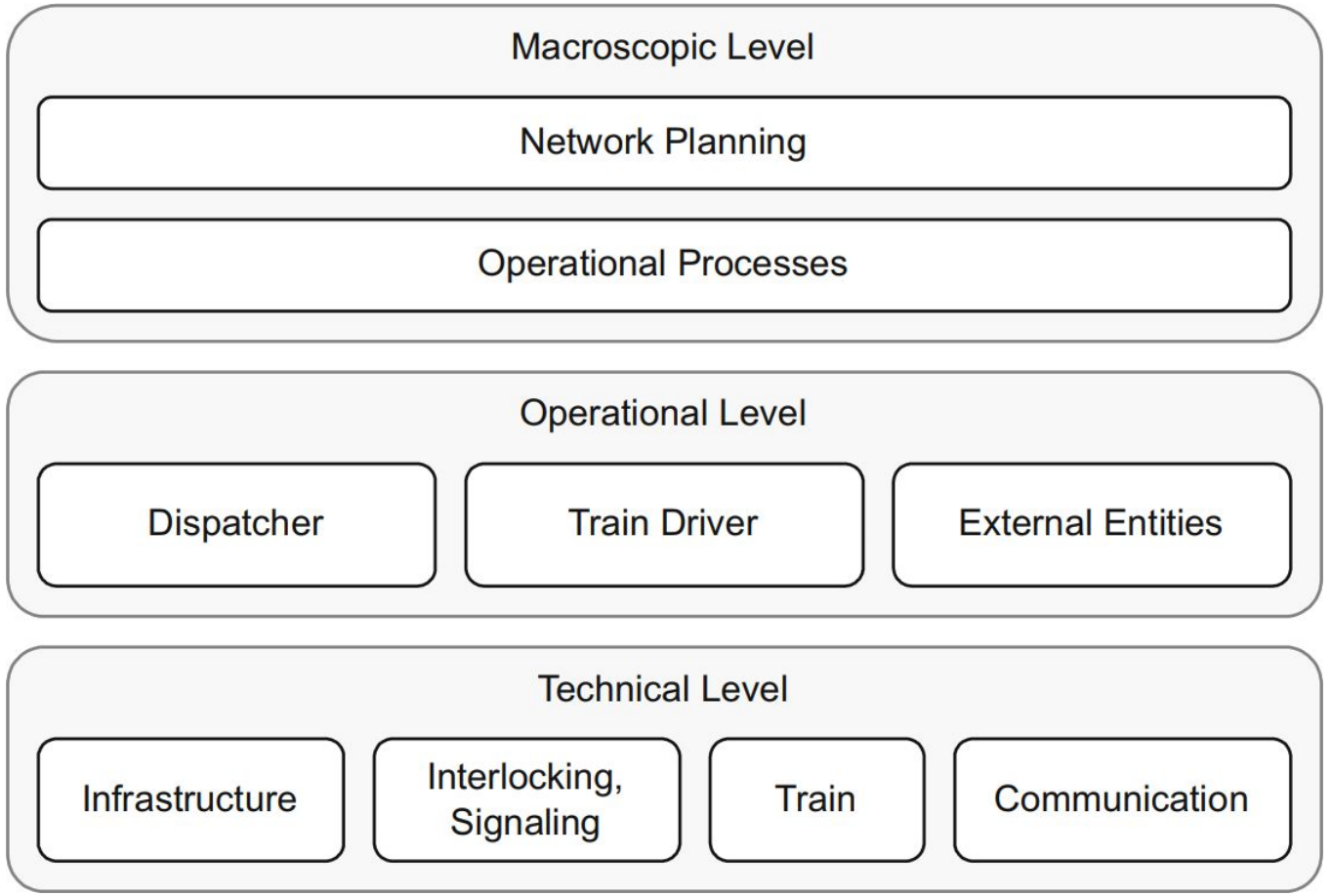
DLR Institute for Systems Engineering
for Future Mobility (DLR-SE),
Oldenburg, Germany

Outline

- Operations in the Railway Domain are Safeguarded at Various Levels
- Motivation for a Scenario-Based Simulation Supported Approach
- Deriving Characteristic Properties of Railway Scenarios | Method
- Characteristic Properties of Railway Scenarios
- List of Concepts and Tasks of the Train Driver
- Future Work:
  - Extending Traffic Sequence Charts (TSCs) to the Railway Domain
  - Testcase Evaluation
- Conclusion

Operations in the Railway Domain are Safeguarded at Various Levels

- Currently GoA-2 can be achieved via ATO over ETCS (AoE). ETCS acts as a safety envelope.
- Automation in the macroscopic and technical levels are widely covered by existing technology such as AoE
- For higher levels of automation the greatest challenges lie in the Operational Level [2, 3]
- This includes tasks currently done by the train driver, like recognizing immediate hazards along the route and acting accordingly.



[2] Flamm et al. Regulatorischer anpassungsbedarf für das automatische fahren im bahnbetrieb (2019)
[3] Hagemeyer et al. Automatisiertes Fahren auf der Schiene https://doi.org/10.1007/978-3-658-32328-8

Motivation for a Scenario-Based Simulation Supported Approach

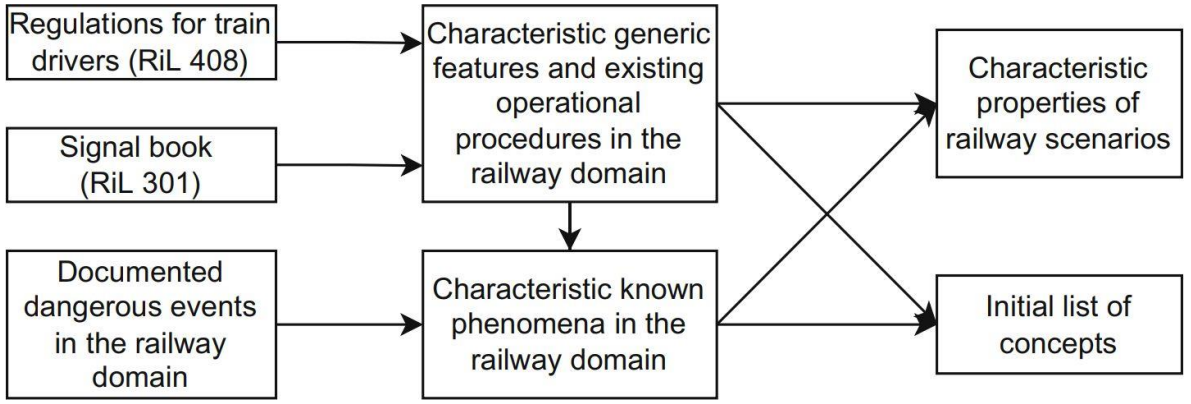
- In order to allow for certification of an highly automated system, we first need to **gather evidence for its abilities and performance**, i.e. allowing for assessment of the system. Based on the assessment results a certification may happen.
- The technical systems required for automated operation range from sensor and data processing systems for **environment perception** to **maneuver planning** and **fail-safe communication** between trains and control centers. --> A wide variety of local risks exist, some of which are difficult to predict and which, by their very nature, have a **very low probability of occurrence** (unrealistic many kilometers needed when testing in reality).
- With the scenario-based approach, one has a tool to **generate critical situations in a targeted manner** and thus validate the behavior of the system.

- In the **automotive domain** relevant critical scenarios are gathered from real world observations, and used for risk assessment, requirement specification and testing [6].
- It can be assumed that in the railway domain the scenarios are less complex and fewer in number, but the scope of automation is larger.

[6] Leitner et al. Enable-s3: Project introduction. Validation and Verification of Automated Systems. (2020)

Deriving Characteristic Properties of Railway Scenarios | Method

- We start with an analysis of the **operational processes** as they are currently realized in Germany (RiL 408, RiL 301), and documented dangerous events in the railway domain [43]
- These sources yield the **characteristic known phenomena of the railway domain**, which in turn are a source for the **characteristic properties of the railway scenarios**, and the **initial list of concepts**.
- The **tasks of the train driver** are of special interest, since these tasks will have to be executed one way or another in highly automated railway systems as well



[43]Bundesstelle für Eisenbahnunfalluntersuchung: Untersuchungsberichte. https://www.eisenbahn-unfalluntersuchung.de. Accessed Mai 02, 2023

Characteristic Properties* of Railway Scenarios

- **P1:** The spatial, relative arrangement of objects is relevant in rail scenarios. Here, the rail network can be viewed as a graph, where the position of an object in this graph can be characterized by the distance along an edge. Furthermore:
  - **P1.1:** The position, velocity and acceleration of a train is usually given in the direction of travel.
  - **P1.2:** Branches (switches, crossings, etc.) shall be taken into account.
  - **P1.3:** For non-rail objects (e.g. external traffic participants), the distance, or relative position, to the track is also relevant.
  - **P1.3a:** A non-rail object can also be located at or behind the end of a track.
  - **P1.4:** For dynamic rail-bound objects, the affiliation to a sequence of track section must be unique (they can change their sections and can be present in more than one sections at the same time).
  - **P1.5:** For static track-side equipment, the affiliation to a track section must be unique.
- **P2:** Properties and states of the track system are relevant. These include:
  - **P2.1:** Physical states and properties (e.g., setting of railroad switches).
  - **P2.2:** Logical states and properties (e.g., route).
  - **P2.3:** Links of trains and their route (occupation of which track section at which time). Notably, these are not constant, but can change dynamically over the course of a scenario.

P3: Signals and other infrastructure (platforms, level crossing, trackside train control equipment, etc.) are relevant, including:

P3.1: their logical affiliation to a track.

P3.2: their logical and physical properties, as well as dynamic states (e.g., shown signals or disturbances). Signals include in particular:

P3.3: audible signals and hand signals.

P3.4: Markings (e.g., pole signs (German "Mastschild")) and signal combinations.

P4: Message exchanges (including type, time, content, sender and receiver of messages) are relevant.

P5: Environmental characteristics/weather effects are relevant.

P6: The condition of trains is relevant. This includes ETCS level, speed, damage/hazards (e.g. fire).

P7: Train parts and their states are relevant, e.g. doors, pantographs, ETCS displays.

P8: External objects (e.g. obstacles, animals) and road users (e.g. pedestrians) are relevant.

P9: Staff members of the railroad operation are relevant, in particular:

P9.1: the mental state of staff members.

P9.2: their physical position (within the scenario).

P9.3: including remotely working operators (e.g. dispatcher, potentially remote train operator).

P10: The timetable is relevant for scenarios.

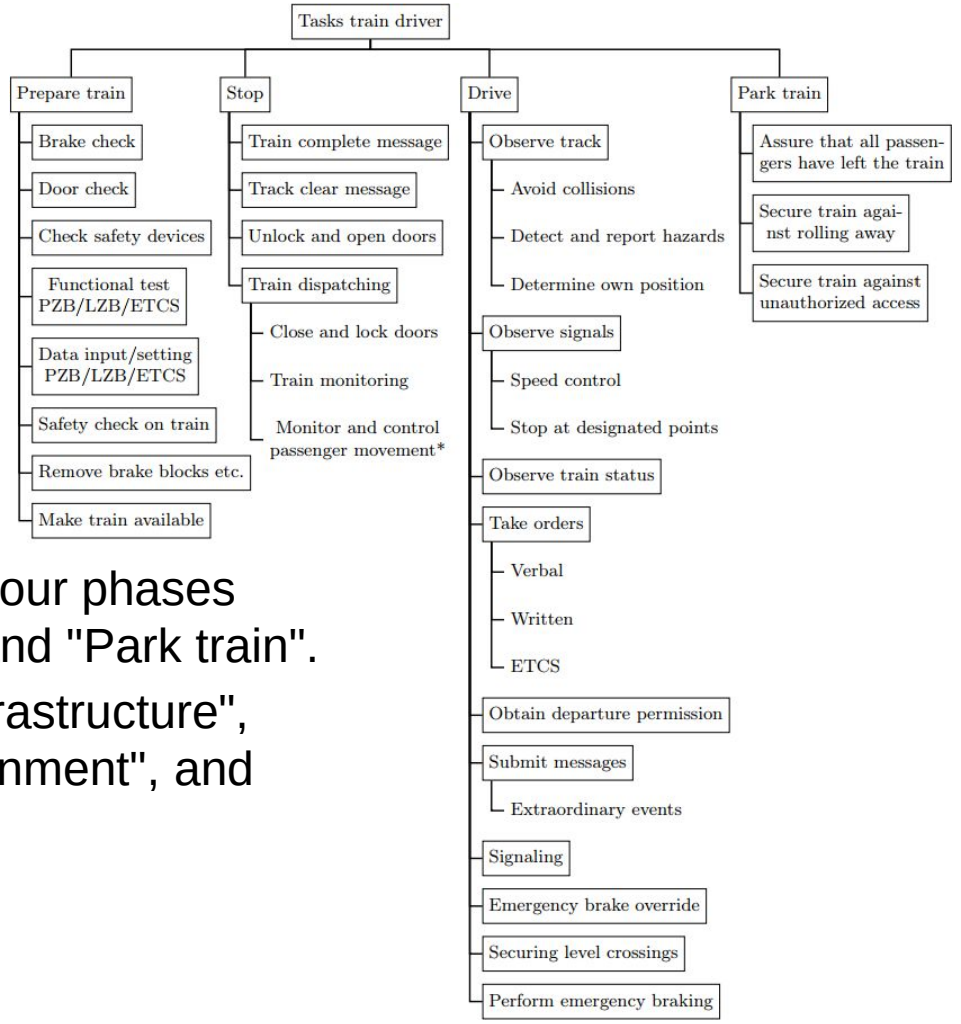
P11: The clearance profile is relevant.

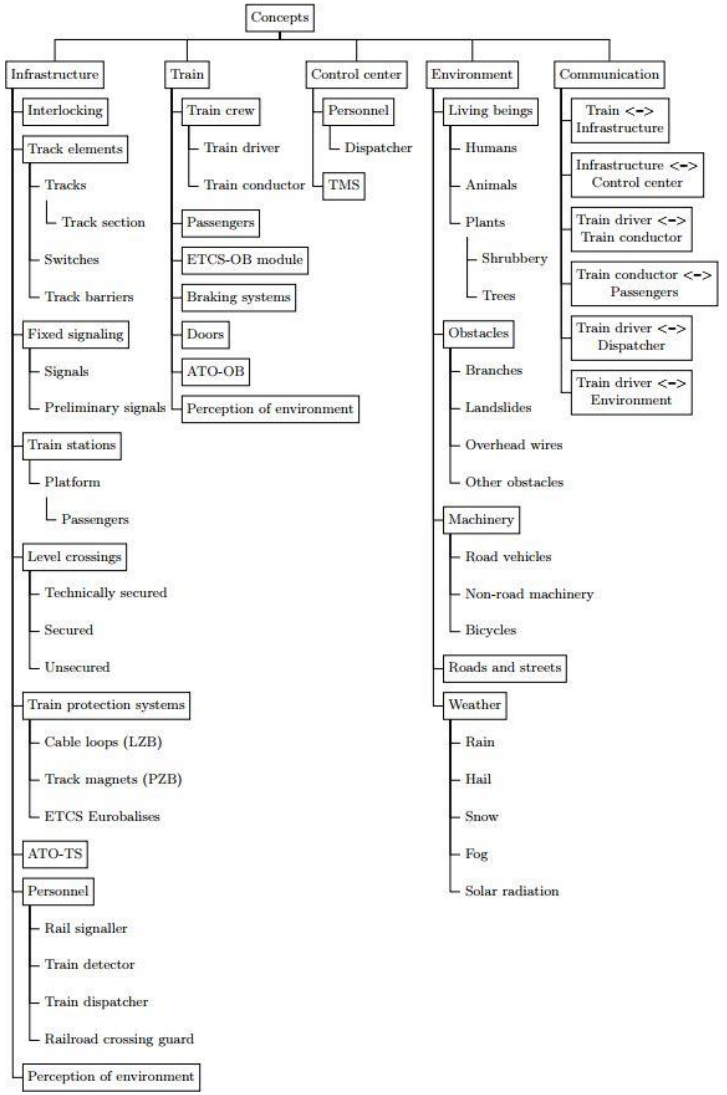
P12: Deviations from planned operations are relevant. In addition to the representation of the occurred, actual, situation, it must therefore be possible to represent the planned (but not occurred) situation in scenarios.

P13: (Virtually) coupled train formations are relevant. In particular, such formations can be formed, modified, and disbanded during a scenario.

* we understand properties as concepts and their relations, where a concept is understood as the underlying “thing” that shall be represented by a symbol. Those symbols are used for capturing scenarios, where scenario is understood as a sequence of situations.

List of Concepts and Tasks of Train Driver





- The train driver has tasks in the four phases "Prepare train", "Stop", "Drive", and "Park train".
- Concepts are structured into "Infrastructure", "Train", "Control Center", "Environment", and "Communication".

Short Explanation of Traffic Sequence Charts (TSCs) [9]

- Description language that combines:
  - Intuitiveness of depicting traffic situations graphically
  - Well-defined semantics required for the application of formal methods
- *Invariant nodes* graphically depict traffic situations (or combinations of situations)
- A *requirement TSC* consists of three parts
  - *Bulletin board* declaring symbols referring to global object variables
  - *Pre-chart* describing a triggering condition split into history (left part) and future (right part)
  - *Consequence* defining a reaction to the trigger that is synced with the future.
- TSCs are always interpreted with respect to a *world model* and a *symbol dictionary*. The world model defines the domain ontology for the specification. At least, it defines the *object types* that a TSC may speak about together with the attributes.

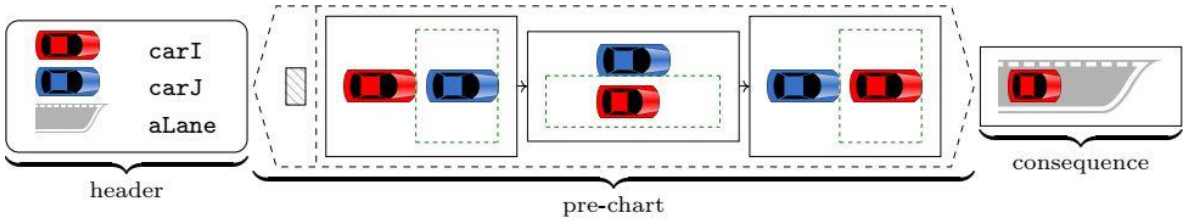


Fig. 1: A TSC and its parts

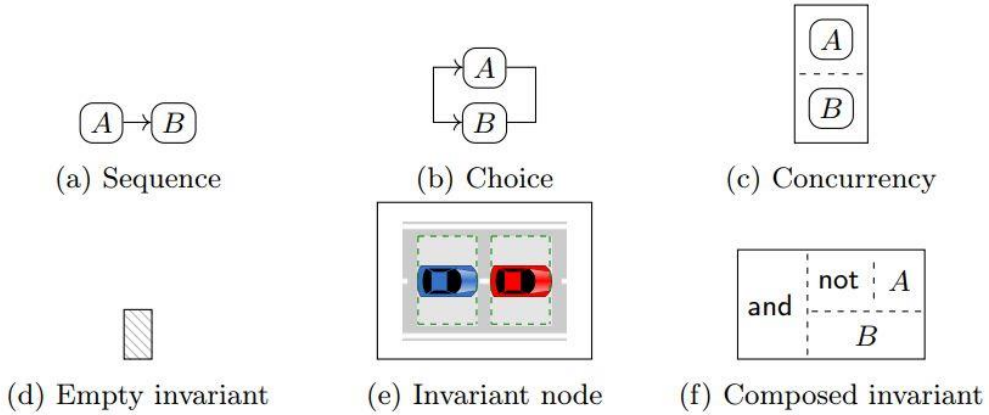
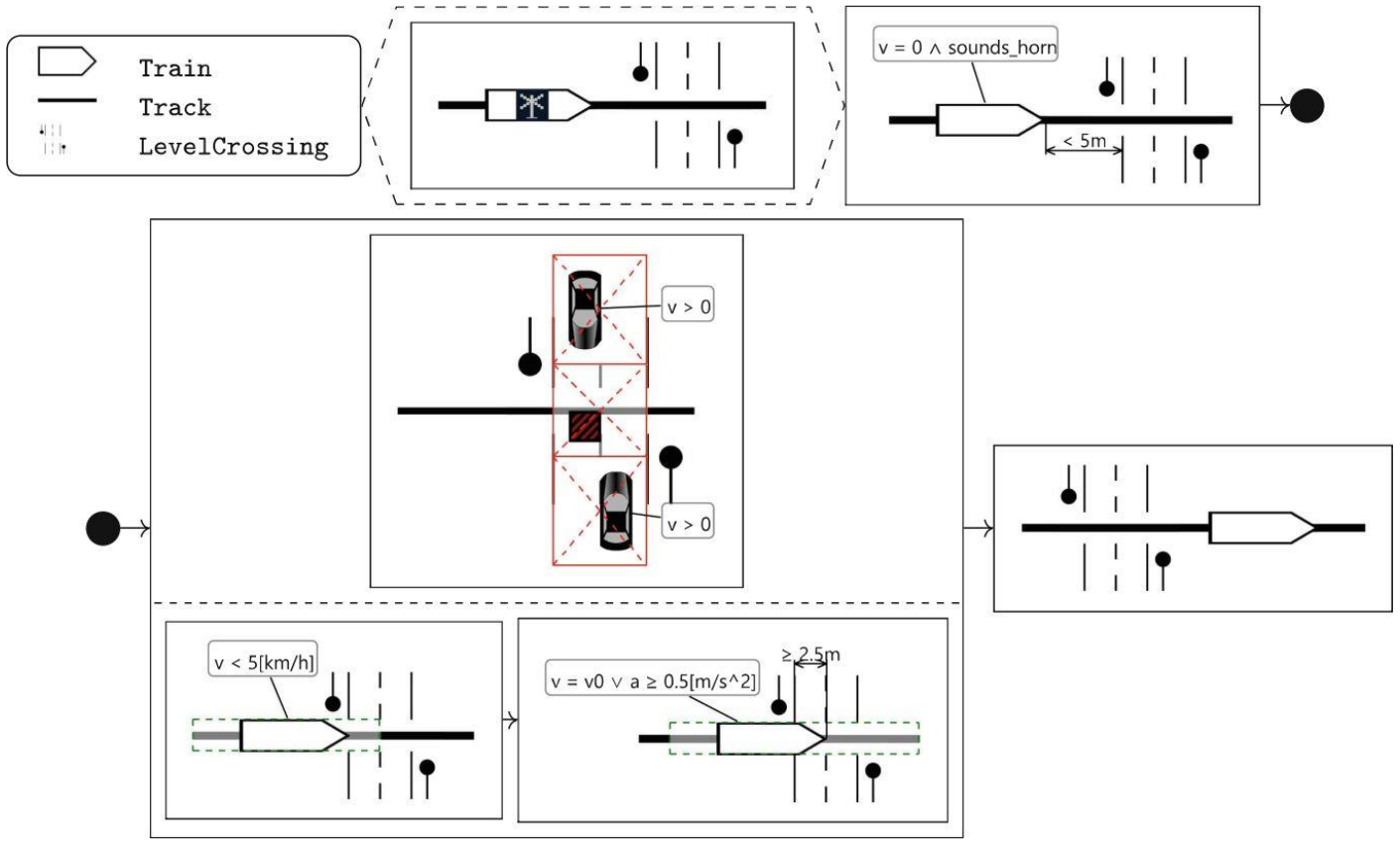


Fig. 2: Basic charts

[9] W. Damm et al. Traffic Sequence Charts for the ENABLE-S_3 Test Architecture, 2019, https://doi.org/10.1007/978-3-030-14628-3_6

Extending Traffic Sequence Charts (TSCs) to the Railway Domain

- The TSC on the right shows a simple test scenario which is relevant, when irregularities are encountered at a level crossing
- A seamless sequence of the situations is depicted in invariant nodes (rectangular boxes):
    1. Level crossing not protected symbol (LX01) is displayed on the DMI
    2. Train Driver needs to come to a complete stop, warn potential entities by giving the signal ZP 1 (sounding the horn)
    3. Continue the journey over the crossing and vacate the crossing as quickly as possible
    4. Parallel to that, the driver needs to observe the crossing and make sure that there are no obstacles on the tracks.



Testcase Evaluation

- Concrete test cases for a specific system under test (SUT), e.g. a **perception system** or a system that executes other tasks previously allocated to the train driver, can be derived by **sampling concrete scenarios** from TSCs and then simulating them.
- We are currently working with the OpenRails [28] simulator to demonstrate the concept.
- A threshold on **criticality metrics** (CM) as used in the automotive domain could serve as **pass/fail criteria**. CM are used to quantify the criticality of a specific scenario. Some examples from [54] that can serve as a starting point:
  - Time to Collision (TTC). Minimum time until two entities E1 and E2 collide
  - Proportion of Stopping Distance (PSD). PSD = RD/MSD, with Minimal Stopping Distance (MSD) and RD (remaining distance). One needs a PSD value of 1 or greater to stop safely.
  - Brake Threat Number (BTN). Defined as the necessary acceleration that is imposed on entity E1 as a consequence of a movement of another entity E2, divided by the maximum possible acceleration of E1. This CM seems to be particularly relevant for train sequences.
  - Post Encroachment Time (PET). Time between leaving a conflict area (CA) of E1 and entering the same CA of E2. This CM is particularly relevant at level crossings.

[54] Westhofen et al.: Criticality metrics for automated driving: a review and suitability analysis of the state of the art (2022). https://doi.org/10.1007/s11831-022-09788-7
[10] Open Rails (2023). https://www.openrails.org/. Accessed 11 Apr 2023

Conclusion

- We gave a summary how a scenario-based, simulation supported approach fits in an safety argument which could be used in the future to virtually certify highly automated railway systems.
- We derived 13 characteristic properties of the railway domain that scenario specifications shall be able to address.
- The collections of properties and concepts are a starting point for building critical railway scenarios, which may be specified as TSCs.
- This helps to fulfill the requirements on systems with AI components, especially those related to completeness and representativeness.
- The derived list of concepts, which shall be included in an ontology, can be used to instantiate concrete tests that shall be simulated.
- Thresholds on criticality metrics can serve as pass/fail criteria in those tests

Thanks!

Are there any questions?