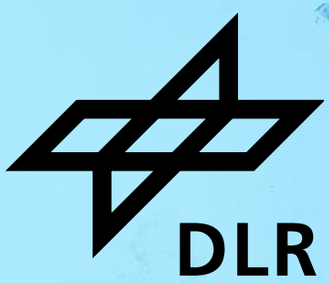
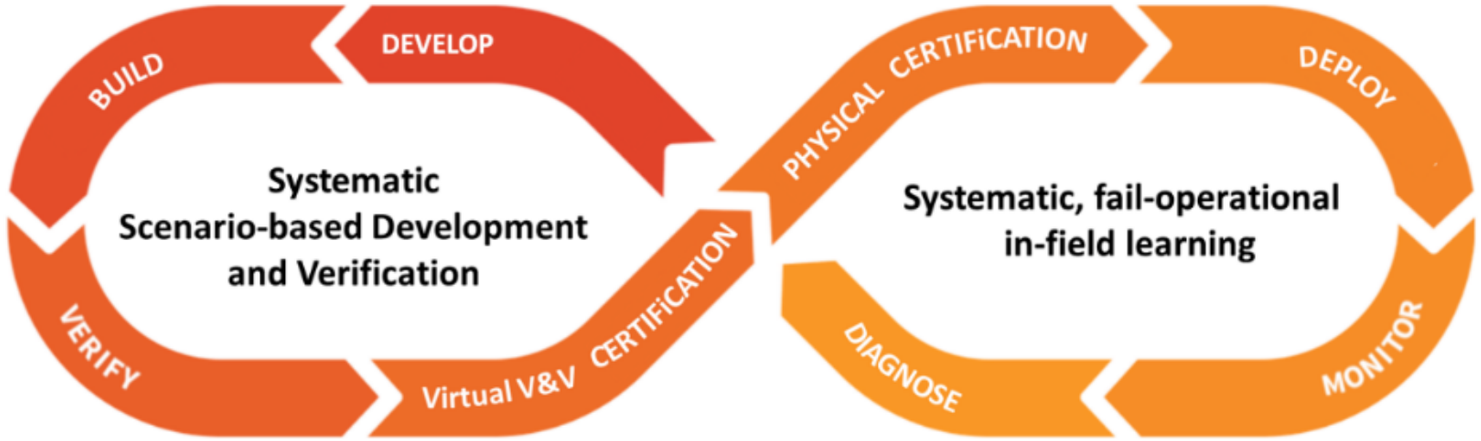
Safety in Dev and Ops – The Case of Automated Driving Functions.

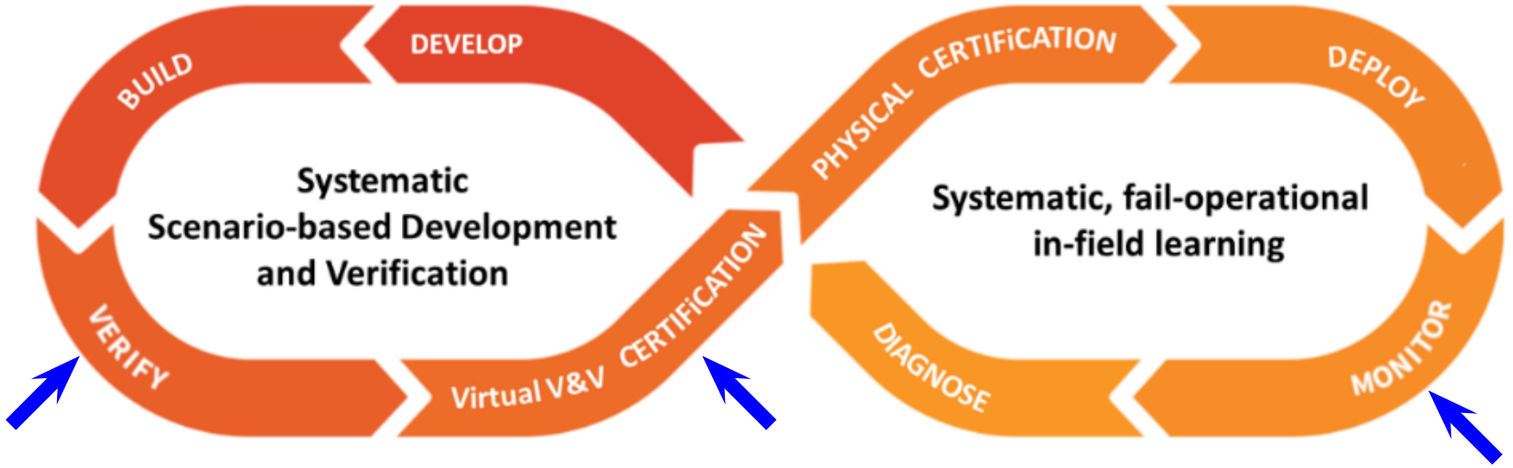
MCS Workshop / HiPEAC'23



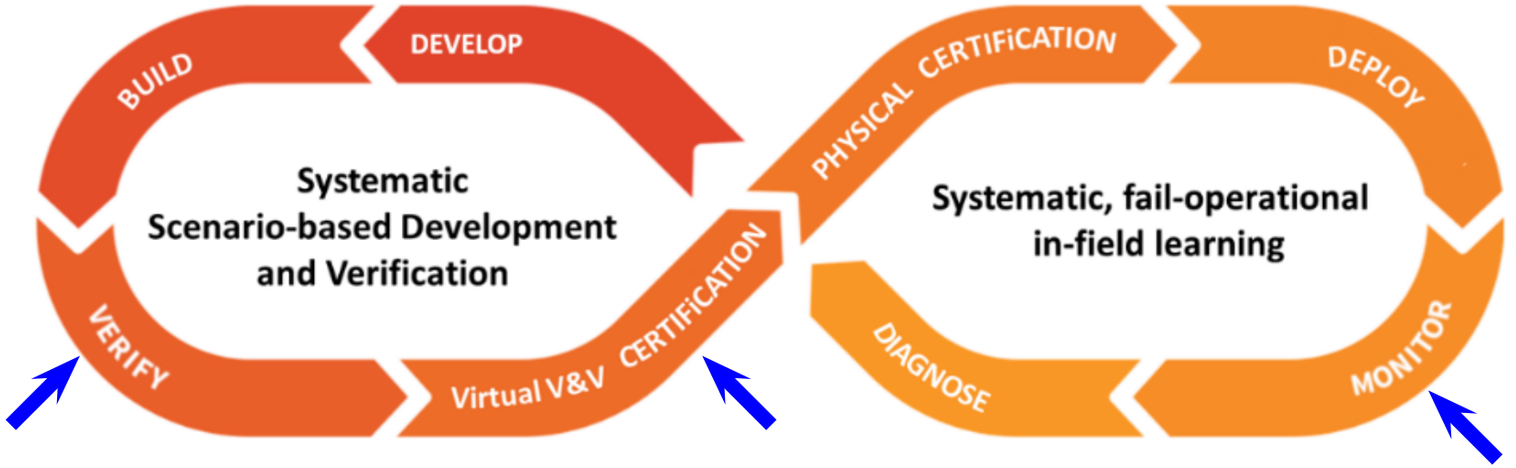
Bernd Westphal , Institute of Systems Engineering for Future Mobility , 2023-01-16



DLR, CC-BY 3.0, https://verkehrsforschung.dlr.de/de/projekte/vv4ngc-methoden-prozesse-und-werkzeugketten-fuer-die-validierung-verifikation-von-next

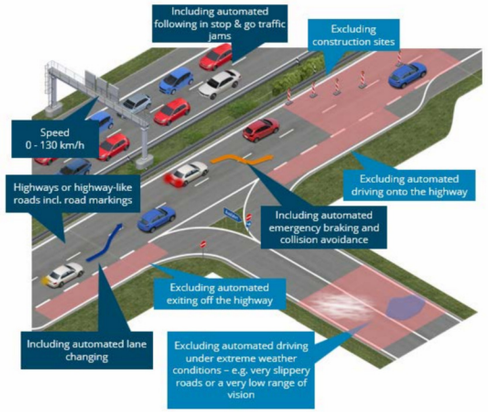


DLR, CC-BY 3.0, https://verkehrsforschung.dlr.de/de/projekte/vv4ngc-methoden-prozesse-und-werkzeugketten-fuer-die-validierung-verifikation-von-next

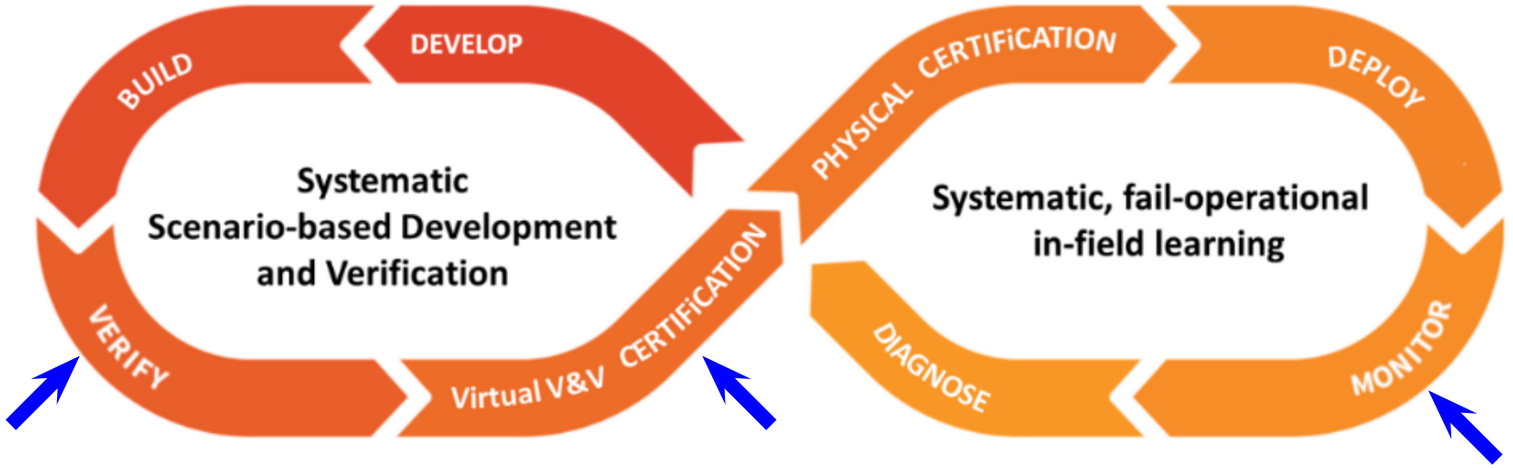


DLR, CC-BY 3.0, https://verkehrsforschung.dlr.de/de/projekte/vv4ngc-methoden-prozesse-und-werkzeugketten-fuer-die-validierung-verifikation-von-next

DLR, CC-BY 3.0



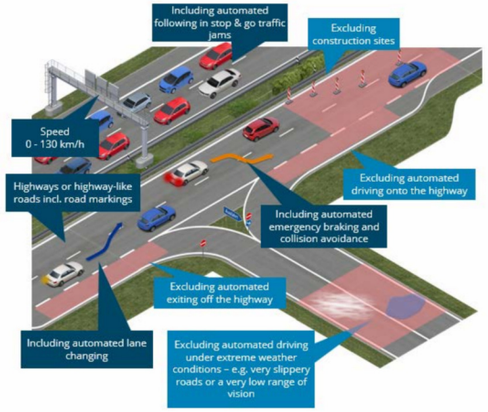
U. Eberle, VVM mid-term presentation, 2022. https://www.vvm-projekt.de/midterm-docs



DLR, CC-BY 3.0, https://verkehrsforschung.dlr.de/de/projekte/vv4ngc-methoden-prozesse-und-werkzeugketten-fuer-die-validierung-verifikation-von-next

- Main challenge:
  vehicles operate in **open context**. [1]
  - to prove their trustworthiness to potential users as well as regulation authorities it is necessary to show they **operate safely in all (relevant) environments** and **under all circumstances**
  - established approaches (e.g., distance based testing) are no longer feasible

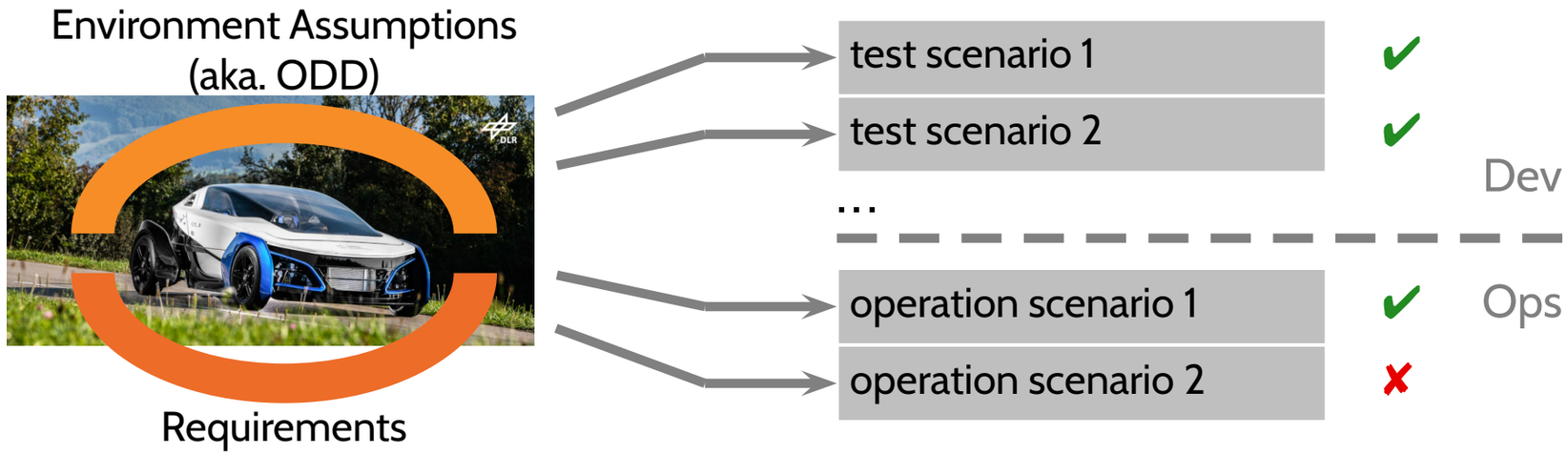
DLR, CC-BY 3.0



U. Eberle, VVM mid-term presentation, 2022. https://www.vvm-projekt.de/midterm-docs

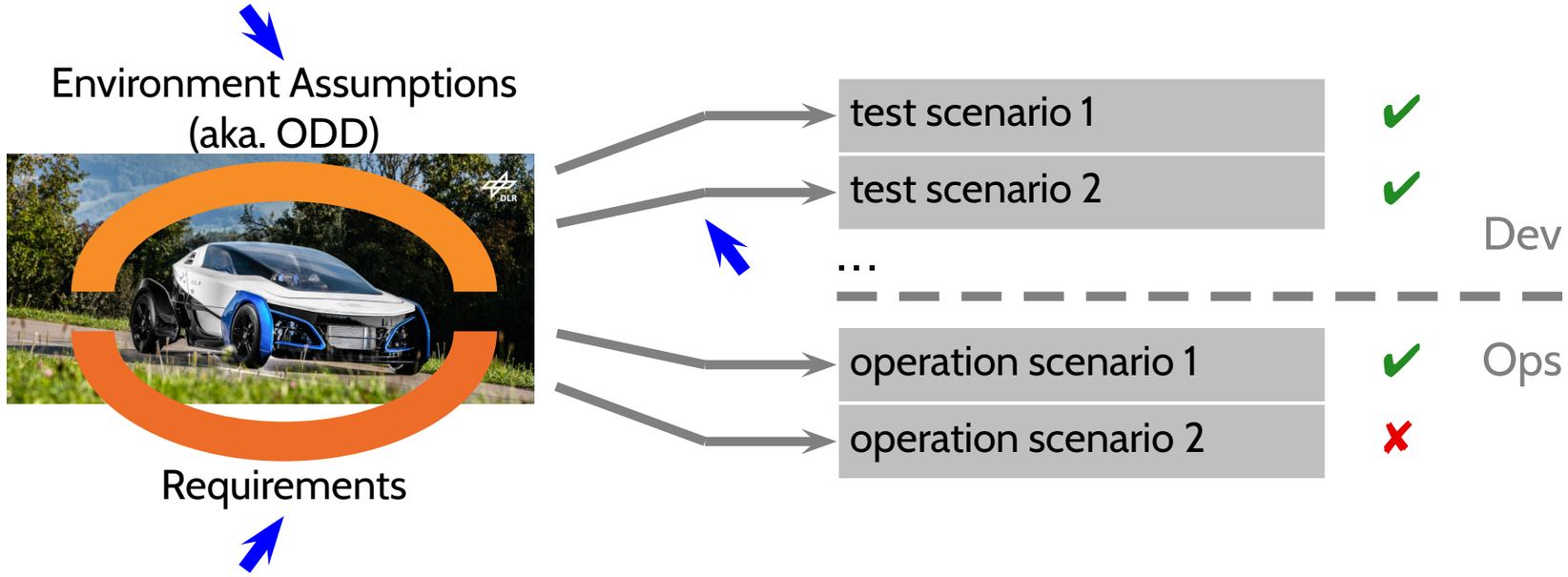
Scenario-based Verification & Validation of Driving Functions

- Main goals: (R. Galbas, VVM mid-term presentation, 2022. https://www.vvm-projekt.de/midterm-docs)
  - (i) Systematic control of the test space.
  - (ii) Consistent interfaces for systems and components.
  - (iii) Significant shift from real-world testing to simulation.



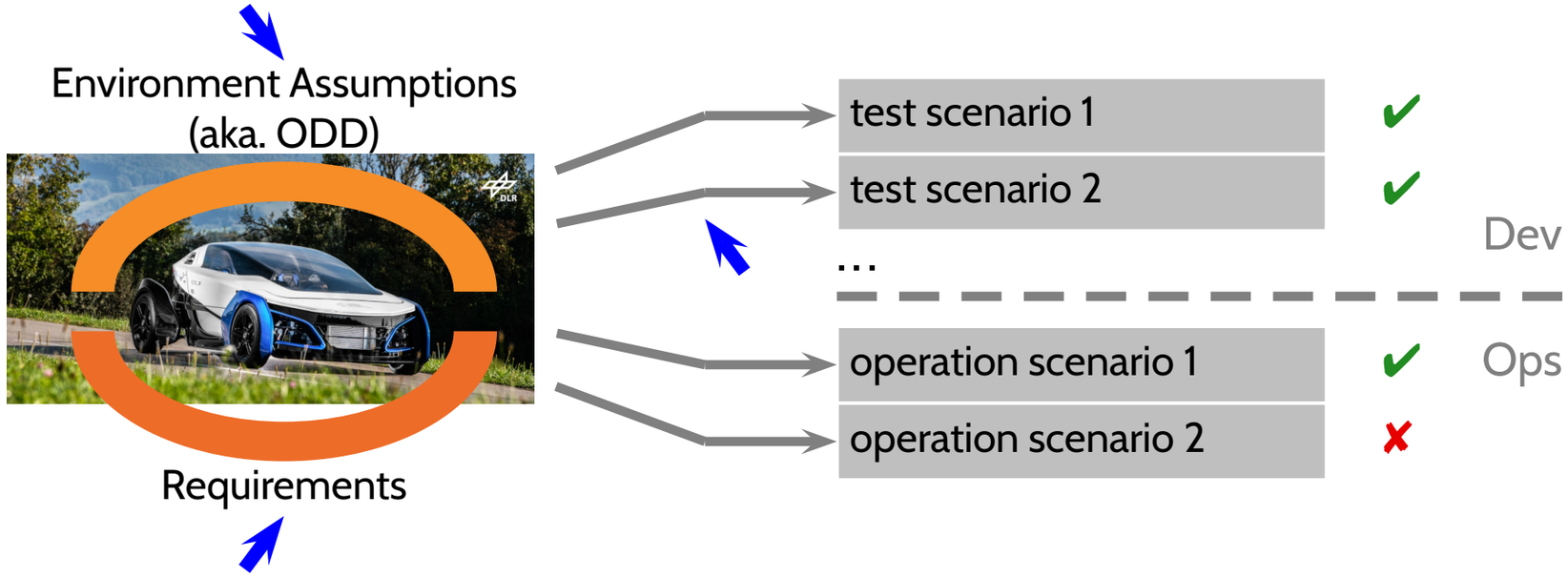
Scenario-based Verification & Validation of Driving Functions

- Main goals: (R. Galbas, VVM mid-term presentation, 2022. https://www.vvm-projekt.de/midterm-docs)
  - (i) Systematic control of the test space.
  - (ii) Consistent interfaces for systems and components.
  - (iii) Significant shift from real-world testing to simulation.



Scenario-based Verification & Validation of Driving Functions

- Main goals: (R. Galbas, VVM mid-term presentation, 2022. https://www.vvm-projekt.de/midterm-docs)
  - (i) Systematic control of the test space.
  - (ii) Consistent interfaces for systems and components.
  - (iii) Significant shift from real-world testing to simulation.

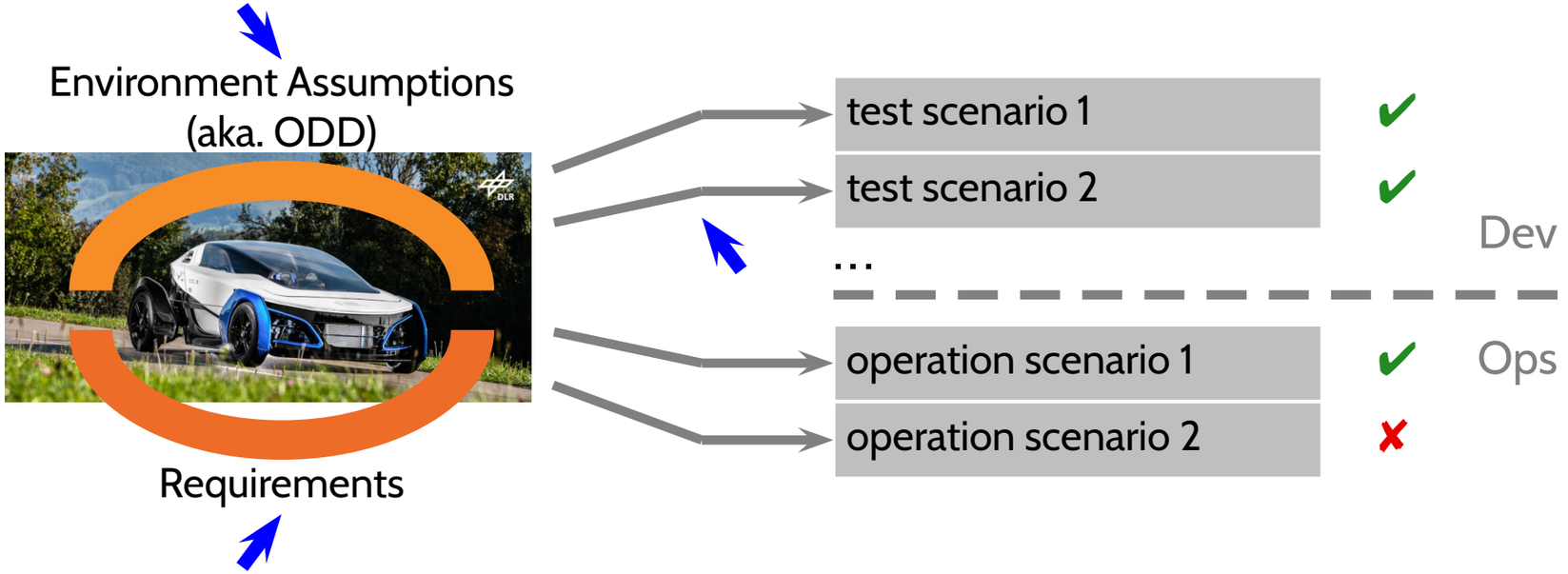


This talk:

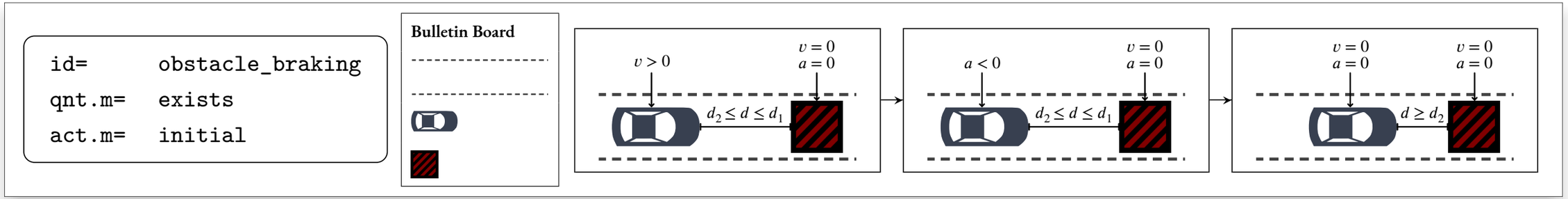
- How do we **formally specify** scenarios for testing?
- How do we **formally specify** requirements and ODDs?

Overview

- How do we **formally specify** scenarios for testing?
- How do we **formally specify** requirements and ODDs?

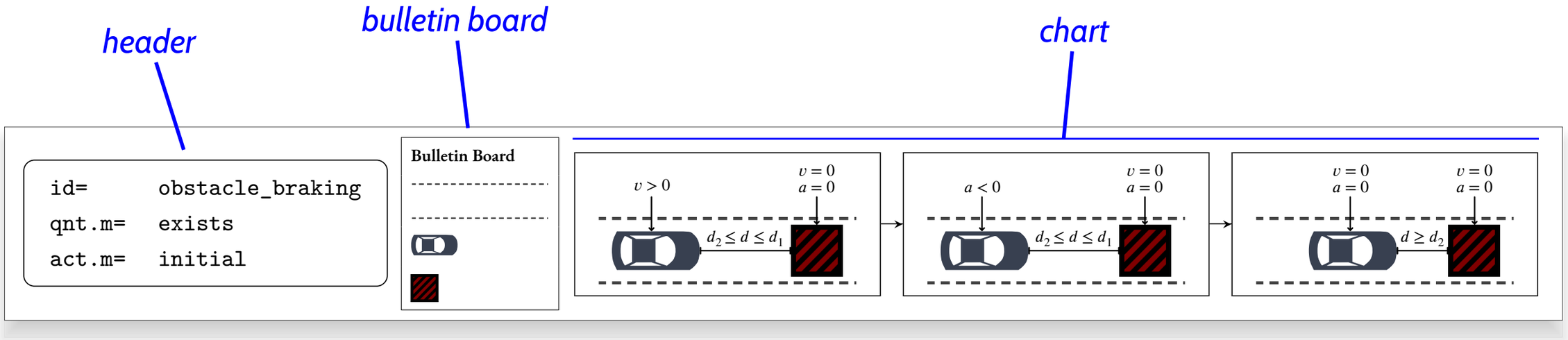


Excursion: Traffic Sequence Charts — Syntax



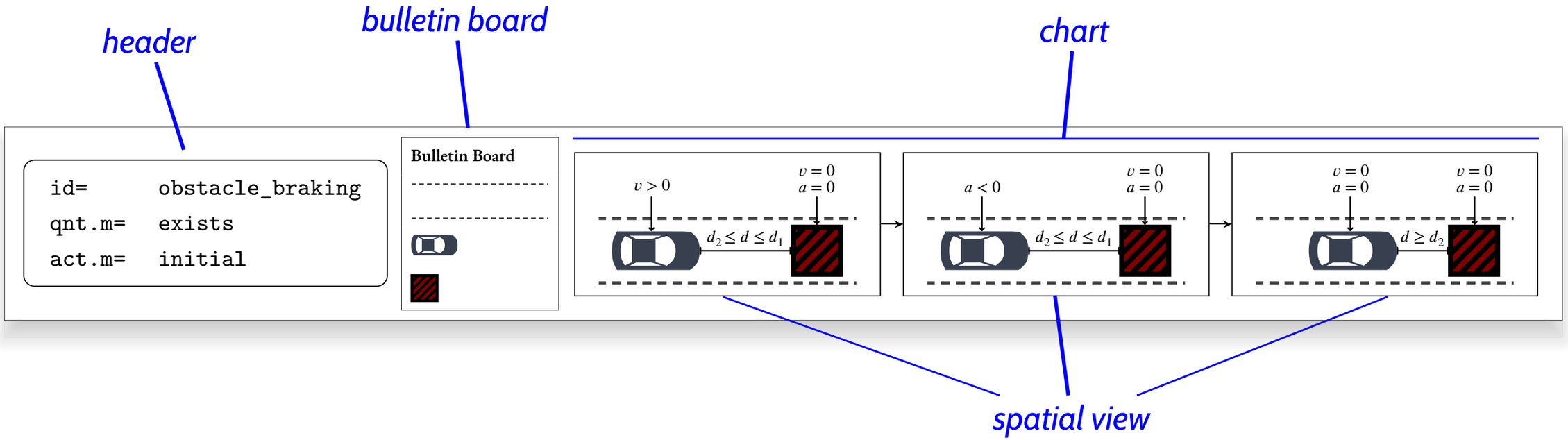
TSC source: J. Hakemann, Automated Monitoring of Traffic Sequence Chart Specifications for Simulated Driving Scenarios, MSc, 2022.

Excursion: Traffic Sequence Charts — Syntax



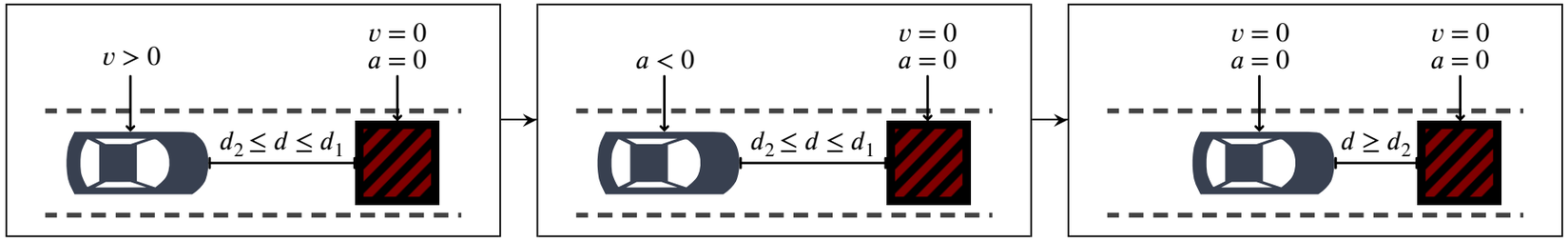
TSC source: J. Hakemann, Automated Monitoring of Traffic Sequence Chart Specifications for Simulated Driving Scenarios, MSc, 2022.

Excursion: Traffic Sequence Charts — Syntax

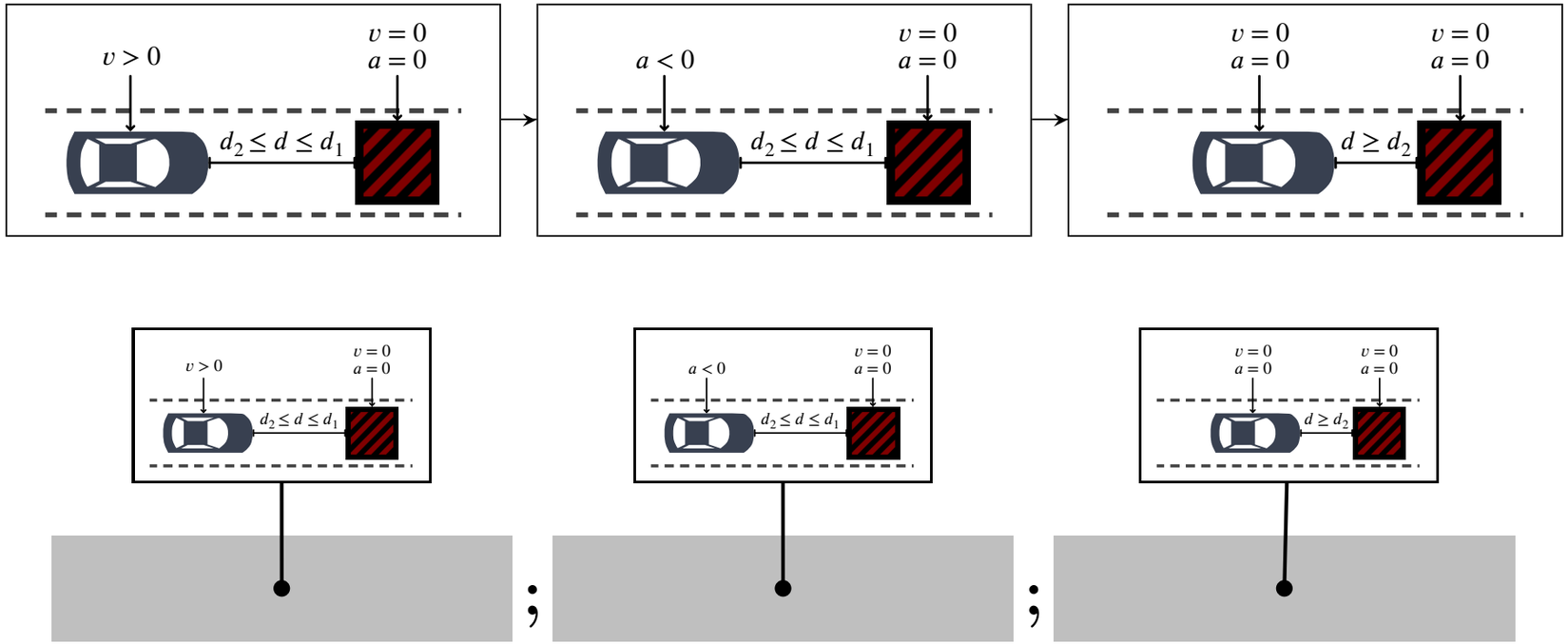


TSC source: J. Hakemann, Automated Monitoring of Traffic Sequence Chart Specifications for Simulated Driving Scenarios, MSc, 2022.

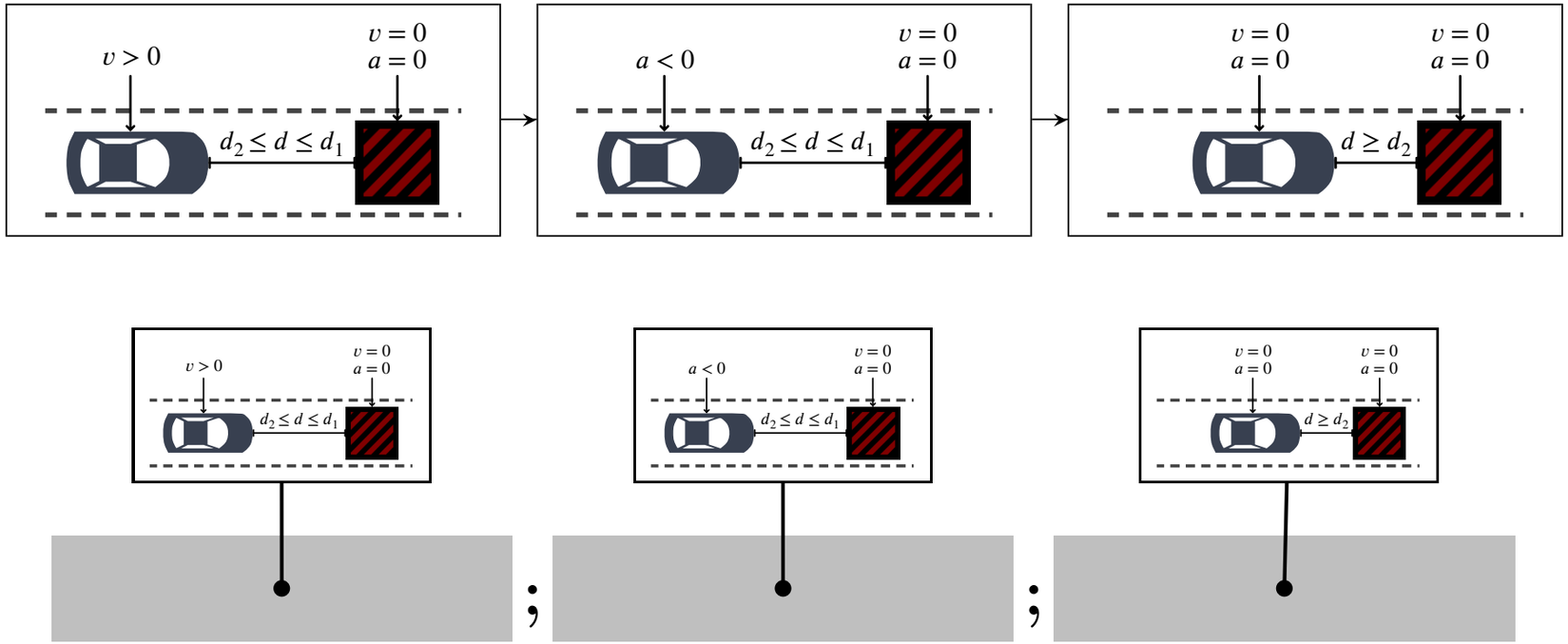
Excursion: Traffic Sequence Charts — Semantics

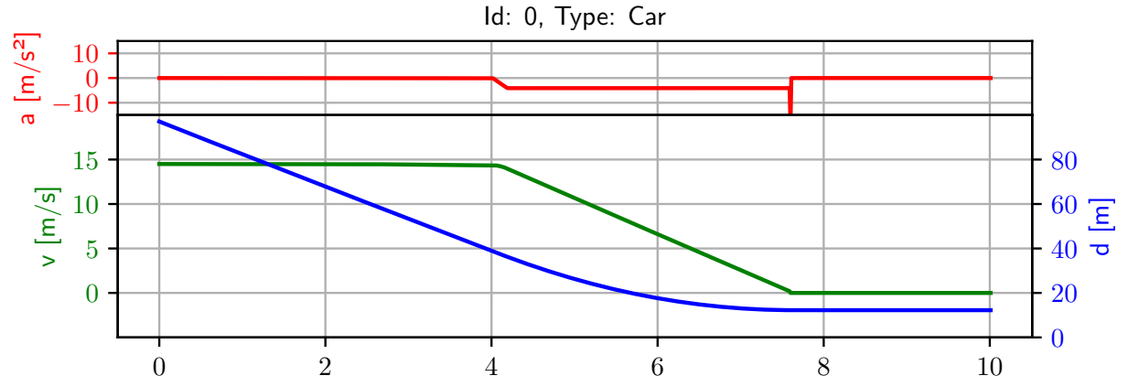


Excursion: Traffic Sequence Charts — Semantics



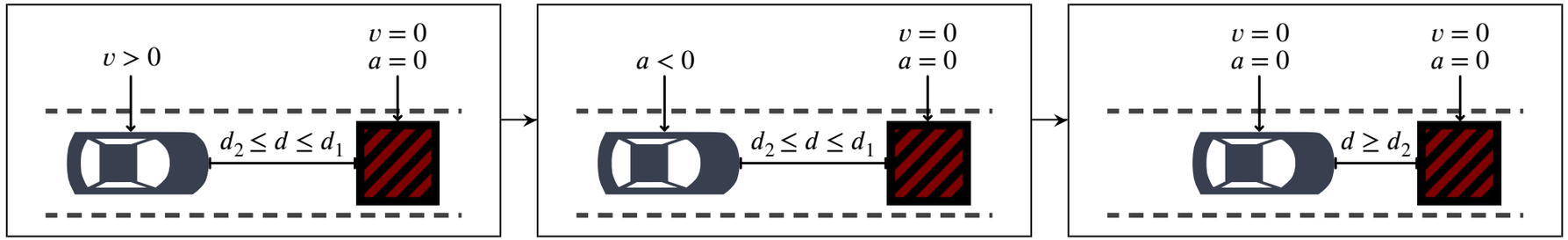
Excursion: Traffic Sequence Charts — Semantics

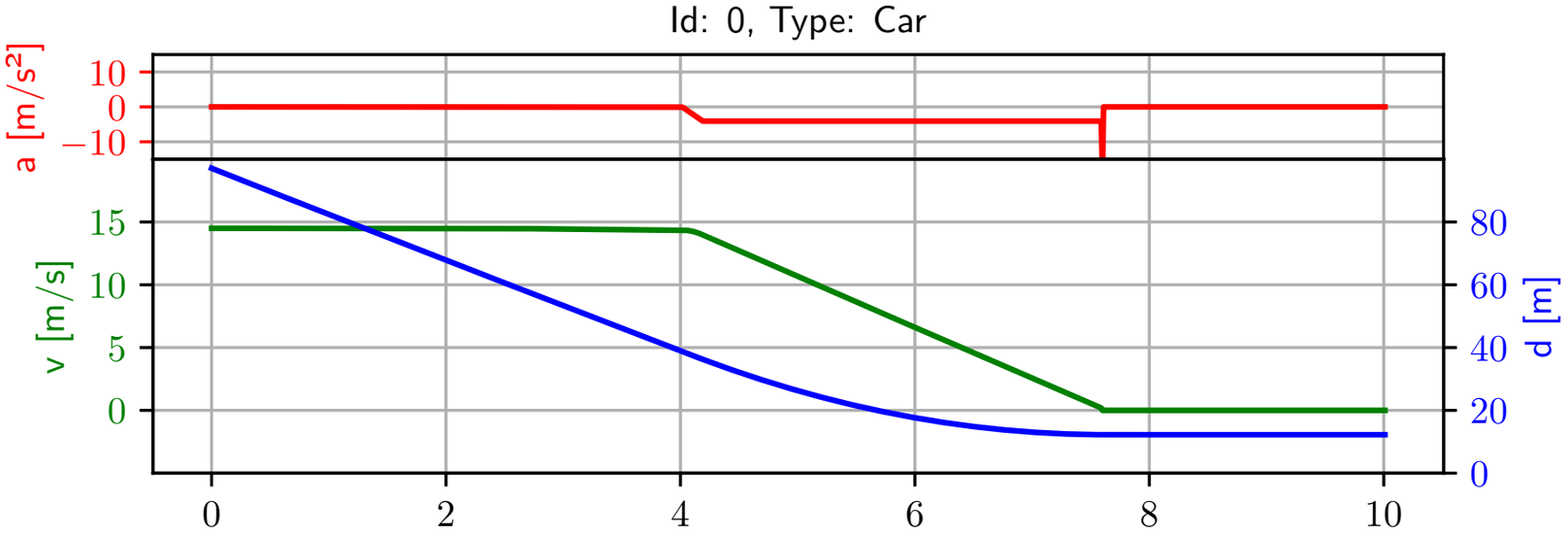




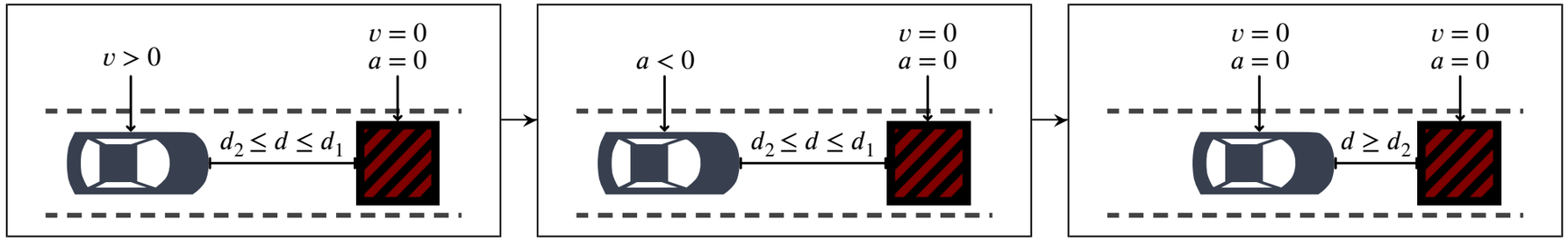
source: J. Hakemann, Automated Monitoring …, MSc, 2022.

Excursion: Traffic Sequence Charts — Stop in Front of Obstacle

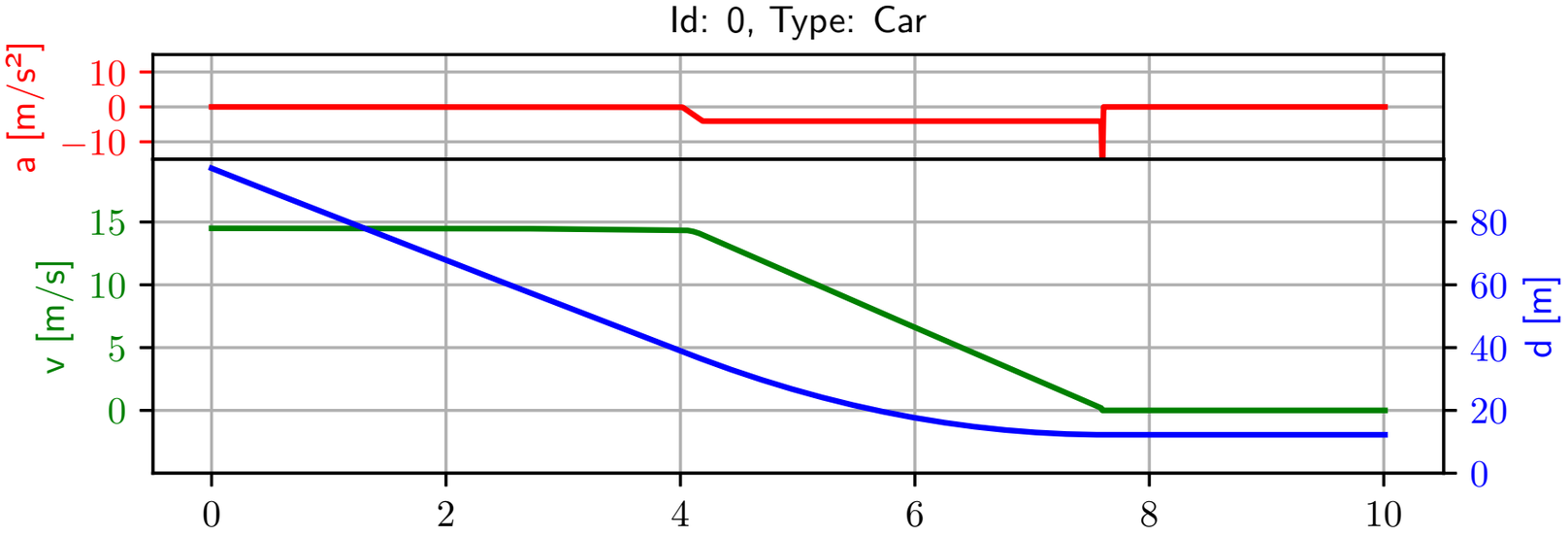




Excursion: Traffic Sequence Charts — Stop in Front of Obstacle

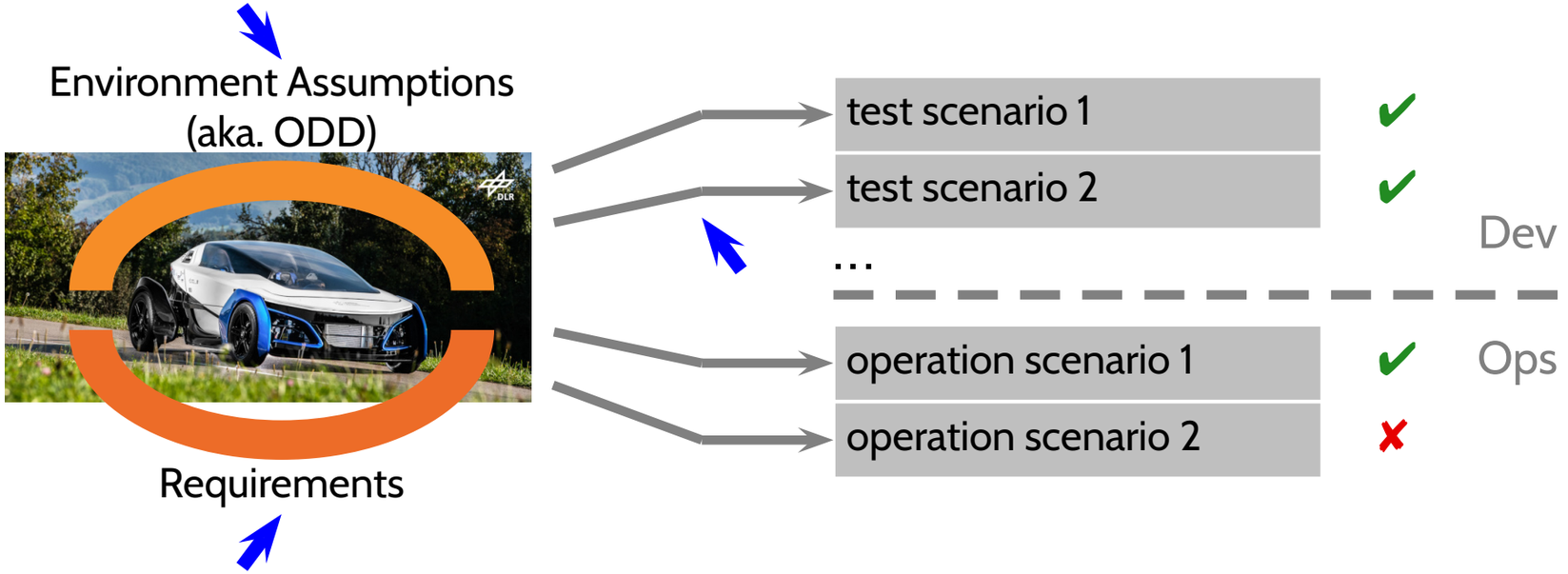


"does this evolution satisfy the TSC?" ↑ ↓ "pls. synthesize an evolution that satisfies the TSC"



Overview

- How do we **formally specify** scenarios for testing?
- How do we **formally specify** requirements and ODDs?



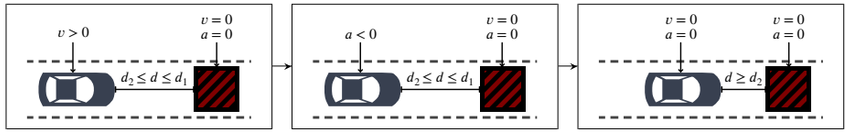
Notions of Scenario Descriptions

Ch. Neurohr, L. Westhofen, M. Butz et al.: Criticality Analysis for the Verification and Validation of Automated Vehicles, IEEE Access, 9/2021.

Functional
- non-formal, human readable
- behavior-based description of a traffic scenario
- possibly containing a visualization

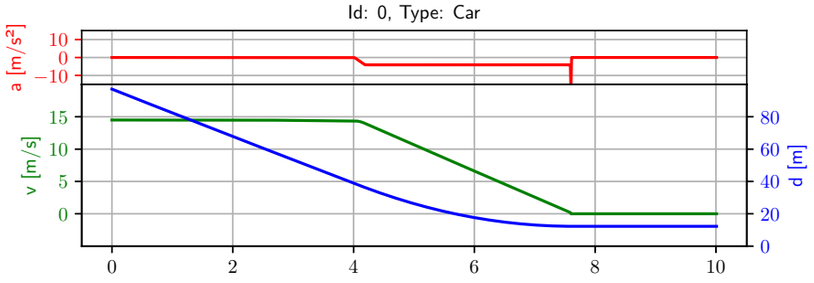
"car stops in front of obstacle"

Abstract
- formalized, machine readable, and declarative description (i.e. constraints on the happenings)
- closely tied to an ontology (or rather family of ontologies)
- efficient description of relations (e.g. cause-effect).

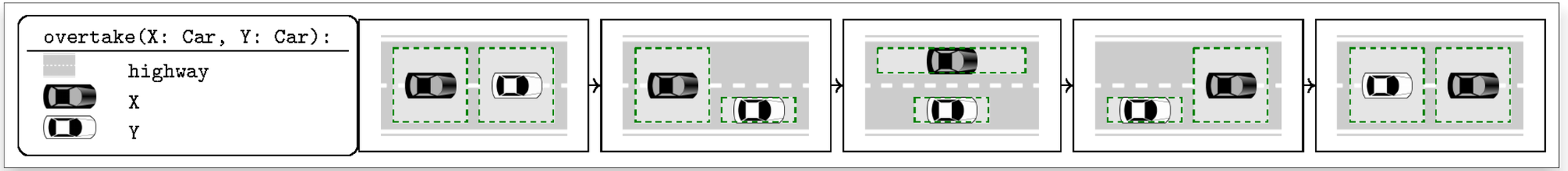


Logical
- parameterized representation of a set of scenarios, where
- influencing factors are described by means of parameter ranges and distributions
- enables parameter variation

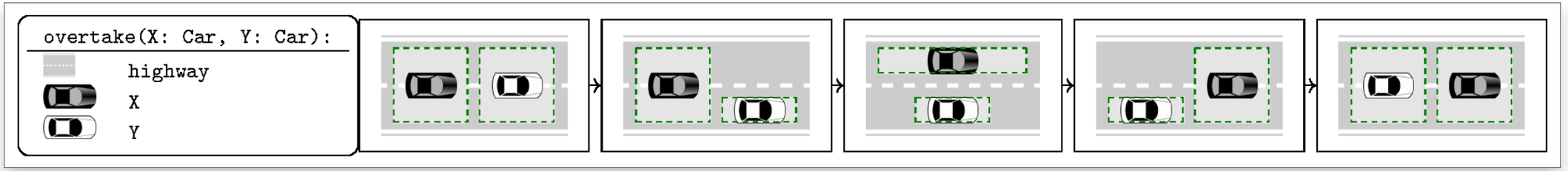
Concrete
- a single scenario, describing exactly one specific scenery and chain of events with fixed parameters
- can, for example, be written as OpenDRIVE + OpenSCENARIO

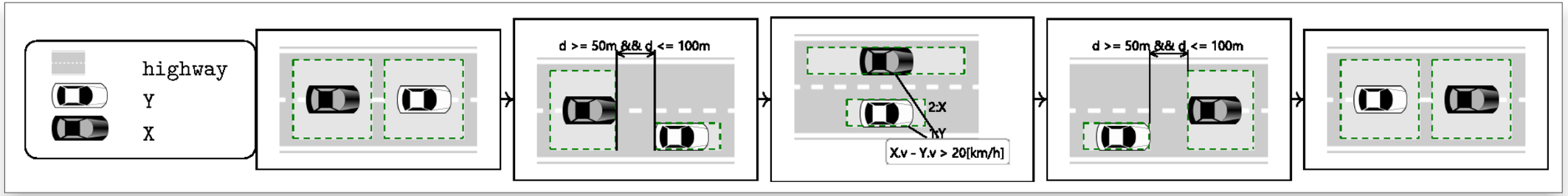


J. Becker, T. Koopmann, et al.: Simulation of Abstract Scenarios, 2022

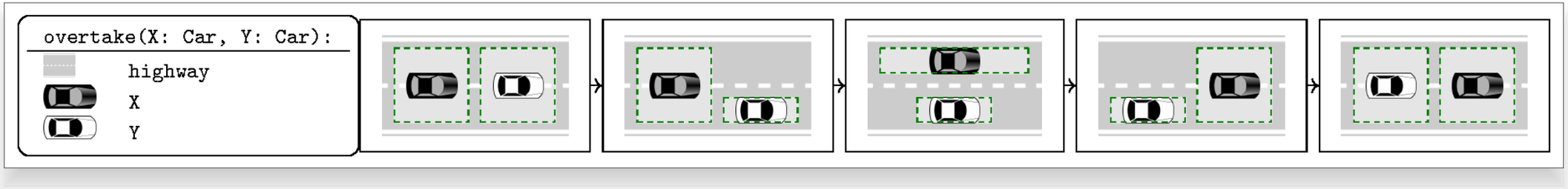


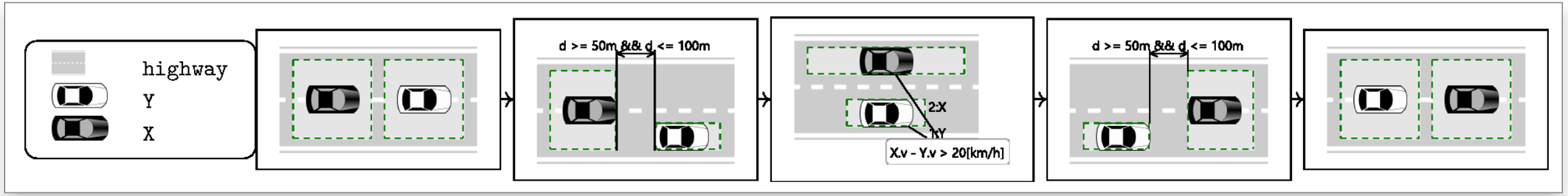
J. Becker, T. Koopmann, et al.: Simulation of Abstract Scenarios, 2022

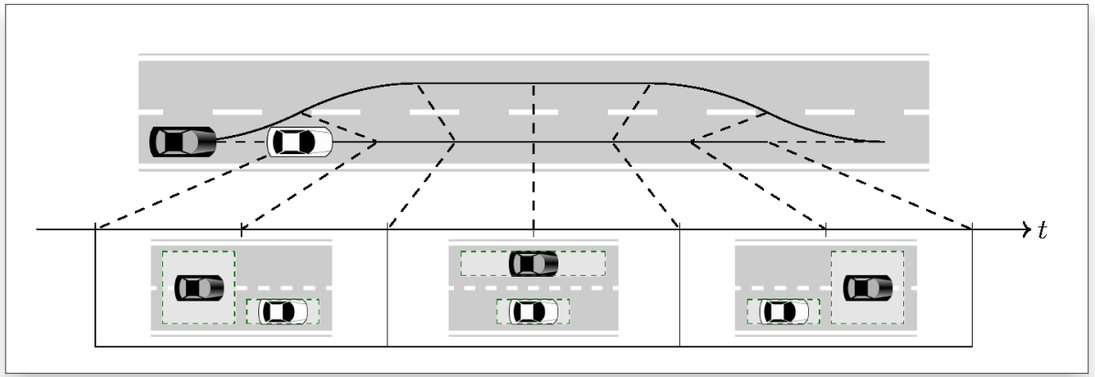




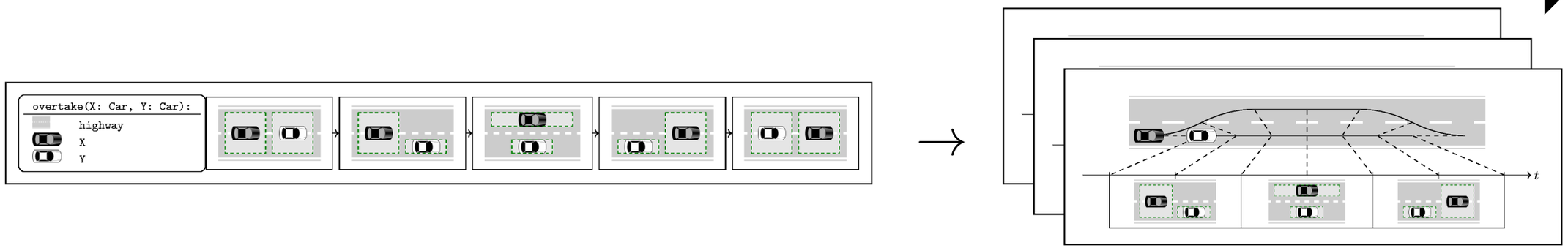
J. Becker, T. Koopmann, et al.: Simulation of Abstract Scenarios, 2022







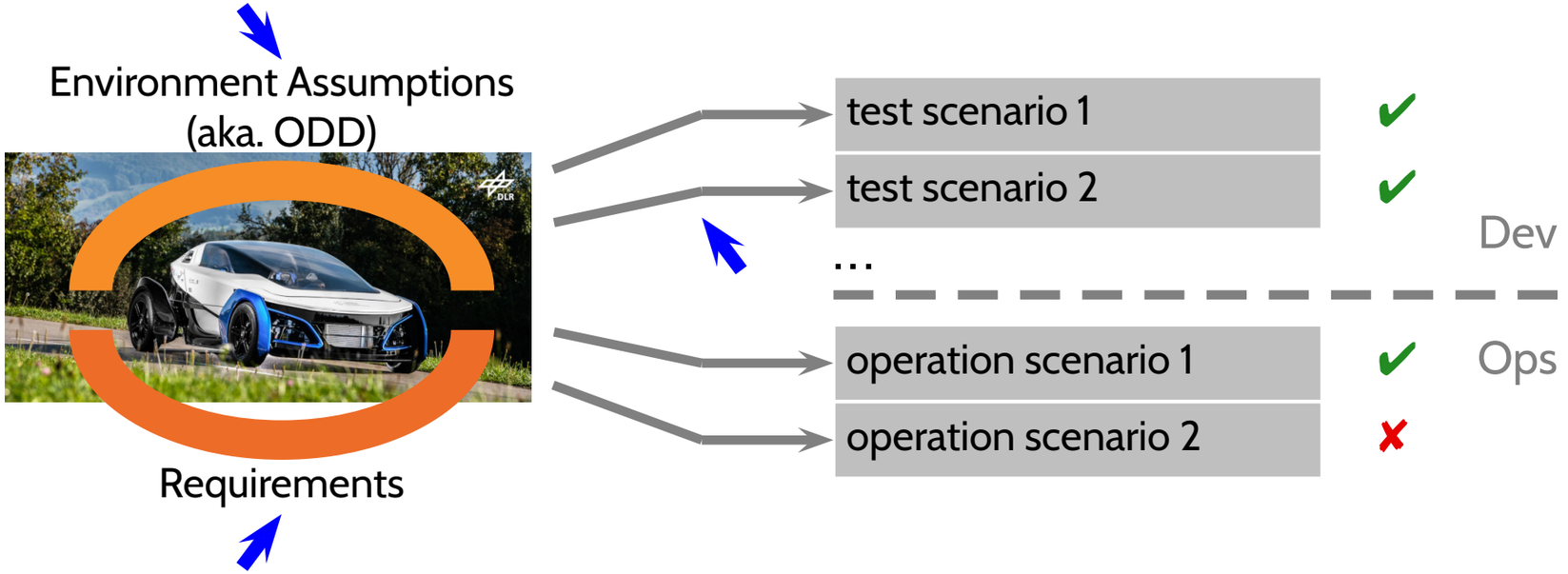
Automatic Generation of Concrete from Abstract Scenarios



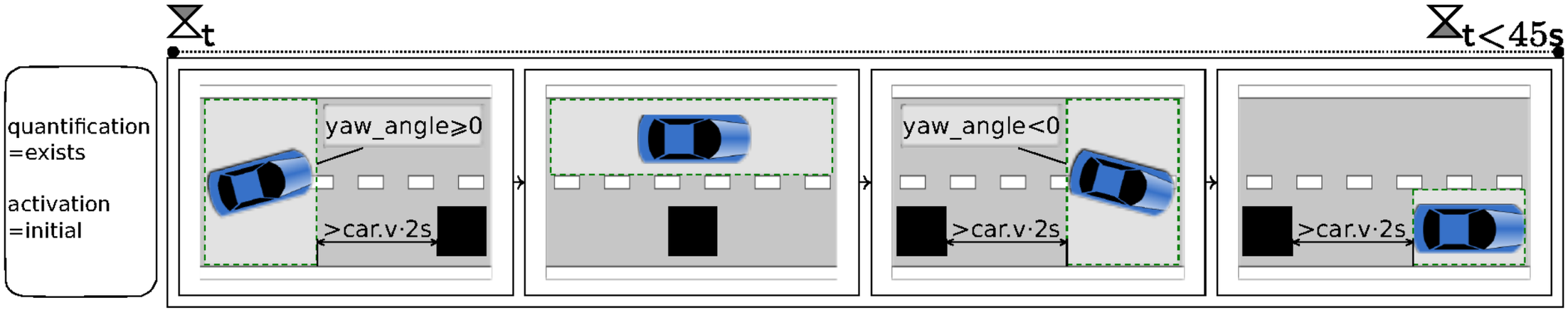
- not mentioned so far: synthesis needs so-called **world model** — a formal model of car physics ("cars do not teleport")
- concrete scenario shown here is **very concrete**: "these two cars drive these particular trajectories"
- useful for:
  - **validation** of formalisation
  - analysis of **criticality phenomena**
  - study of **certain** driving function aspects
- getting useful **test cases** is work in progress

Overview

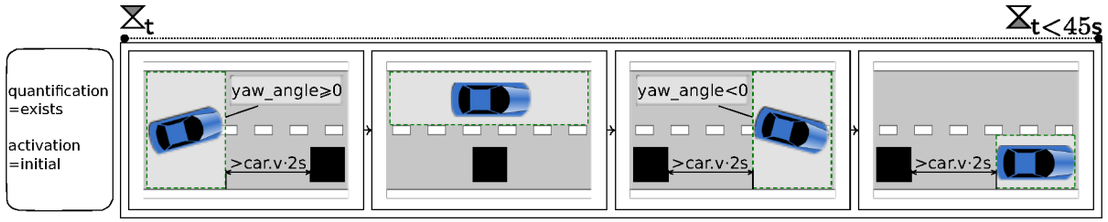
- How do we **formally specify** scenarios for testing?
- How do we **formally specify** requirements and ODDs?



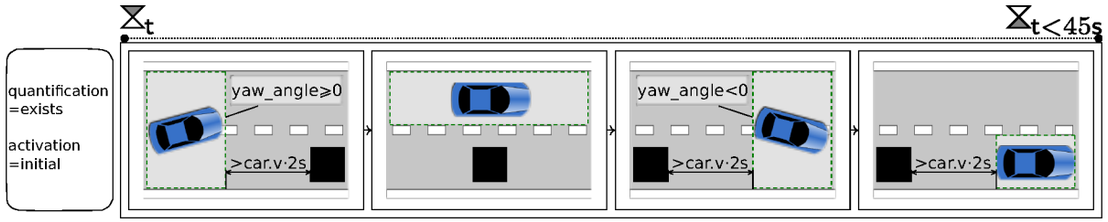
D. Grundt, A. Köhne, et al.: Towards Automated Monitoring, FMAS, 2022

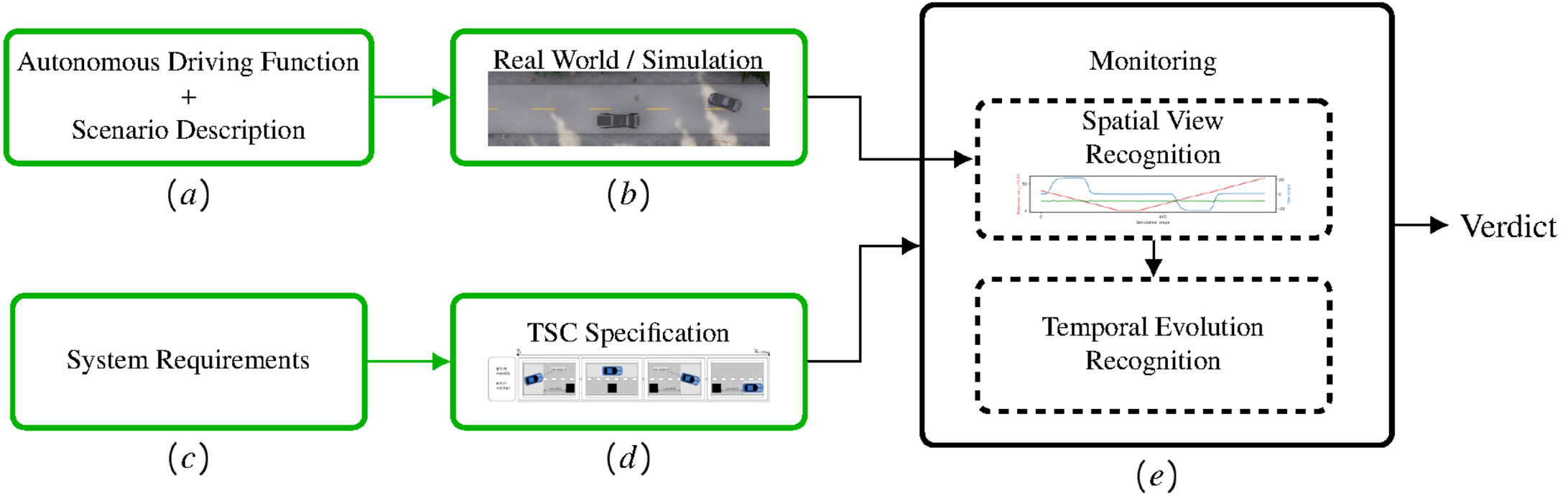


D. Grundt, A. Köhne, et al.: Towards Automated Monitoring, FMAS, 2022



D. Grundt, A. Köhne, et al.: Towards Automated Monitoring, FMAS, 2022





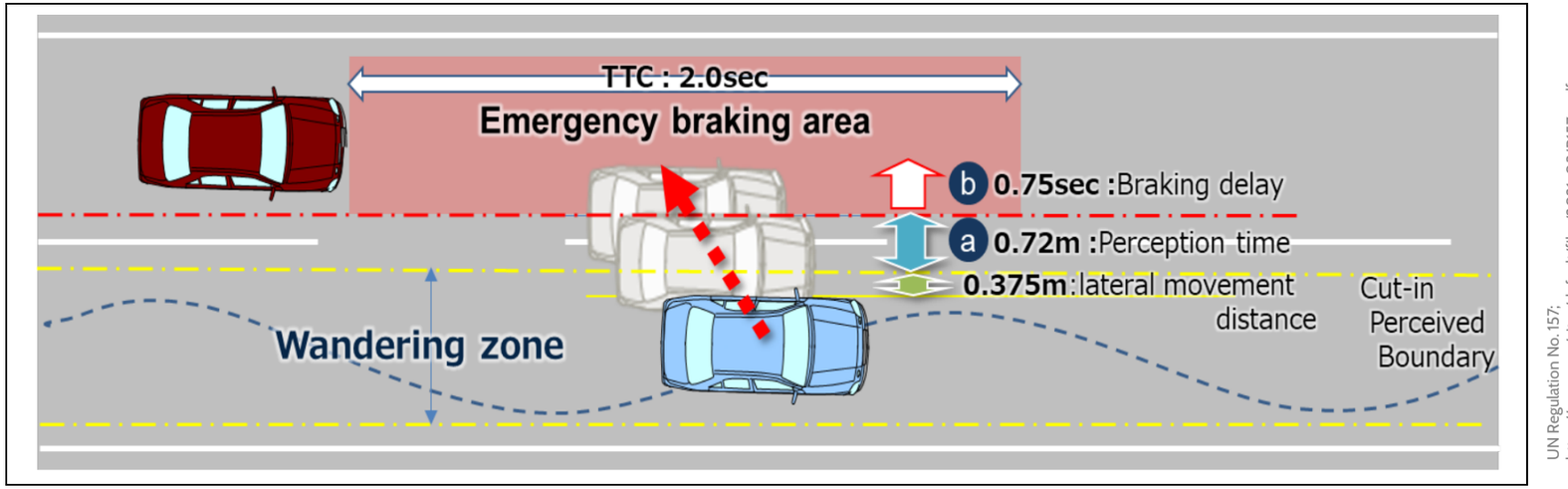
Outlook: Dynamic ODD Aspects

- ODD (Operational Design Domain) $\sim$ the environment conditions that a system was **designed** for, under which the system can be/is expected to provide its intended functionality.
  And what it will be certified/approved for.
- In driving functions for example:
  - Lighting conditions, rain vs. dryness, etc.
  - To me also: „healthiness“ of sub-systems.

Outlook: Dynamic ODD Aspects

- ODD (Operational Design Domain) ~ the environment conditions that a system was **designed** for, under which the system can be/is expected to provide its intended functionality.
  And what it will be certified/approved for.
- In driving functions for example:
  - Lighting conditions, rain vs. dryness, etc.
  - To me also: „healthiness“ of sub-systems.

- ODD may also refer to dynamic behaviour of other traffic participants, e.g., ALKS (Automated Lane Keeping System) in UN ECE 157 has the following illustration:



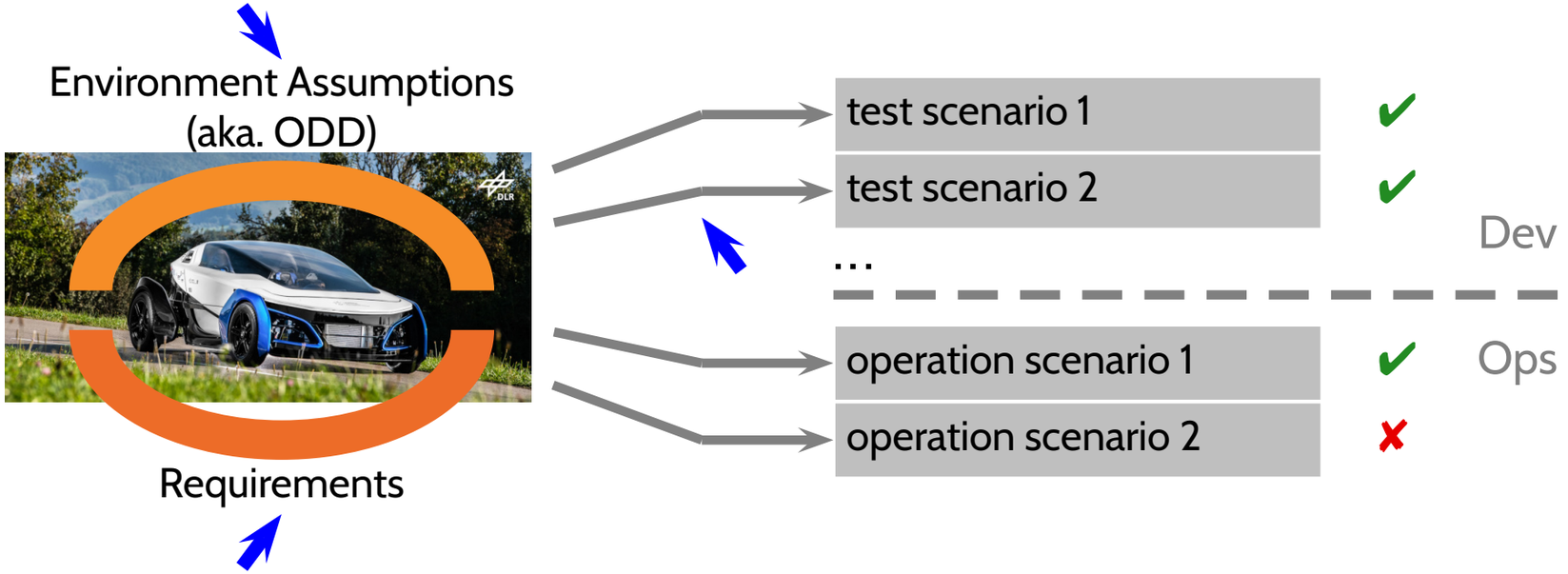
UN Regulation No. 157; https://unece.org/sites/default/files/2021-03/R157e.pdf

Related Work

- ASAM OpenScenario 2.0:
  `https://www.asam.net/project-detail/asam-openscenario-v20-1/`
- ASAM OpenODD (under construction):
  `https://www.asam.net/standards/detail/openodd/`
- Vendor-specific solutions…
- etc.

Thank You!

- How do we **formally specify** scenarios for testing?
- How do we **formally specify** requirements and ODDs?



References

[1] Jan Steffen Becker, Tjark Koopmann, Birte Neurohr, Christian Neurohr, Lukas Westhofen, Boris Wirtz, Eckard Böde, and Werner Damm. Simulation of abstract scenarios: Towards automated tooling in criticality analysis. In *Autonomes Fahren. Ein Treiber zukünftiger Mobilität*, pages 42–52. Zenodo, 2022.

[2] Werner Damm, Eike Möhlmann, Thomas Peikenkamp, and Astrid Rakow. A formal semantics for traffic sequence charts. In Marten Lohstroh, Patricia Derler, and Marjan Sirjani, editors, *Principles of Modeling - Essays Dedicated to Edward A. Lee on the Occasion of His 60th Birthday*, volume 10760 of *Lecture Notes in Computer Science*, pages 182–205. Springer, 2018.

[3] Dominik Grundt, Anna Köhne, Ishan Saxena, Ralf Stemmer, Bernd Westphal, and Eike Möhlmann. Towards runtime monitoring of complex system requirements for autonomous driving functions. In Matt Luckcuck and Marie Farrell, editors, *FMAS*, number 371 in EPTCS, pages 53–61, 2022.

[4] Jan Hakemann. Automated monitoring of traffic sequence chart specifications for simulated driving scenarios. Master's thesis, Carl von Ossietzky Universität Oldenburg, 2022.

[5] Christian Neurohr, Lukas Westhofen, Martin Butz, Martin Herbert Bollmann, Ulrich Eberle, and Roland Galbas. Criticality analysis for the verification and validation of automated vehicles. *IEEE Access*, 9:18016–18041, 2021.