Universität Bremen

Standardisation and Certification Considerations for Autonomous Train Control

Joint work with Kerstin Eder (University of Bristol), Anne. E. Haxthausen (Denmark Technical University), Wen-ling Huang (University of Bremen), and Thierry Lecomte (CLEARSY, France)

Jan Peleska, University of Bremen – 2022-06-03

SafeTRANS
INDUSTRIAL DAY

Background

HiDyVe – Highly Dynamic Virtual and Hybrid Validation and Verification

Grant agreement 20X1908E HiDyVe

HiDyVe Project Objectives

V&V for the following application scenarios

- Formation flight – similar to platooning of trucks
- Autonomous taxi, take-off, and landing ATTOL
- Future urban mobility – combined autonomous cars and drones

HiDyVe

More general project background indicating the need for new V&V approaches

- Four main trends to be observed in cyber-physical systems in general
  - **Growing system complexity** which can no longer be captured anymore in monolithic, comprehensive models and specifications.
  - **Evolving system behaviour** after type certification.
  - Use of **multi agent systems** elaborating plans changing their behaviour at runtime
  - Use of **trained neural networks** whose true behaviour at runtime can be specified neither deterministically, nor within the logic concepts of the application domain.

In this talk: overview

Standardisation and certification of autonomous train control systems

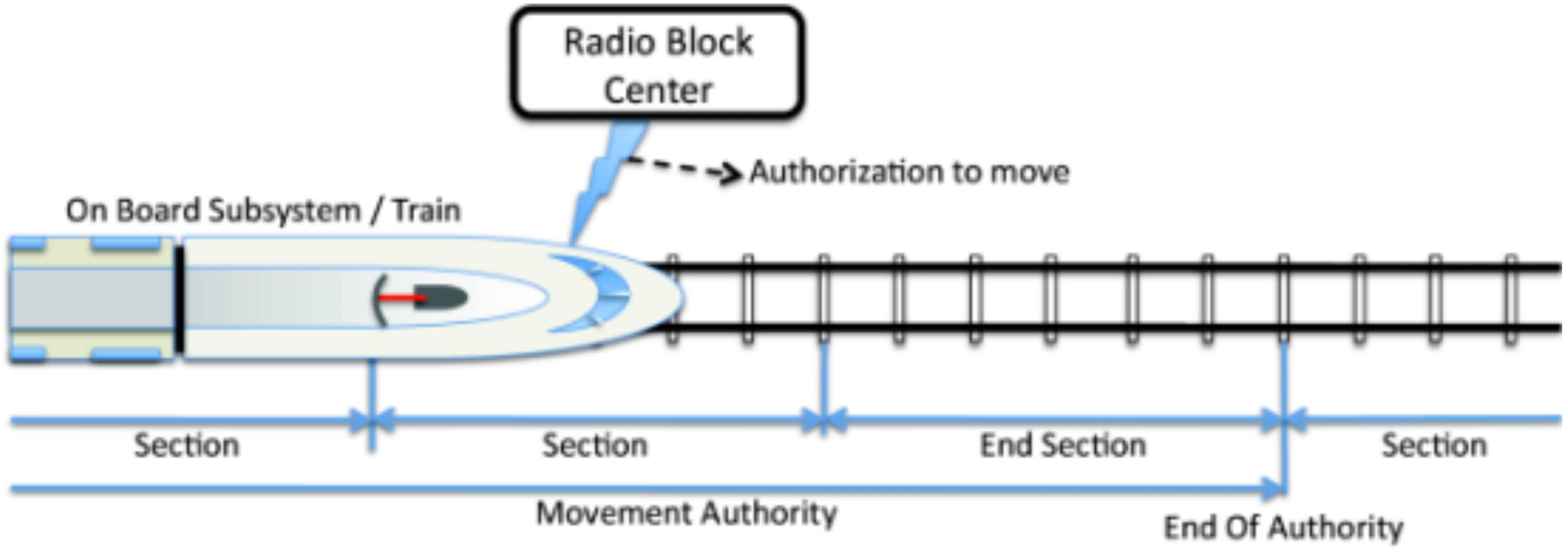
- Suggest and analyse a **"moderate" architectural change** of existing train control systems, **to allow for autonomous operation** with grade of automation GoA 4 (unattended train operation)
  - Do not require changes in today's track-side infrastructure
- Investigate **system-level certifiability and associated evaluation effort** according to novel pre-standard **ANSI/UL 4600**
  - Re-use of certification credit obtained for "conventional" sub-systems certified on the basis of existing CENELEC standards EN 50126, 50128, 50129
- Investigate **hybrid testing strategy** on module level and system level
  - Obtain certification credit for tests performed partially with original equipment, and partially in cloud-based simulation environments

Train Control System Architecture

Assumptions

about the operational environment of an autonomous train

- Assume only track-side equipment as available today in Europe
  - The available equipment varies, depending on the specific train routes
- Assume existing interlocking/radio block stations
  - These ensure elementary train protection, so that an autonomous train with movement authority will be safe from collisions with other trains an derailing caused by wrong point positions within the boundaries of the movement authority

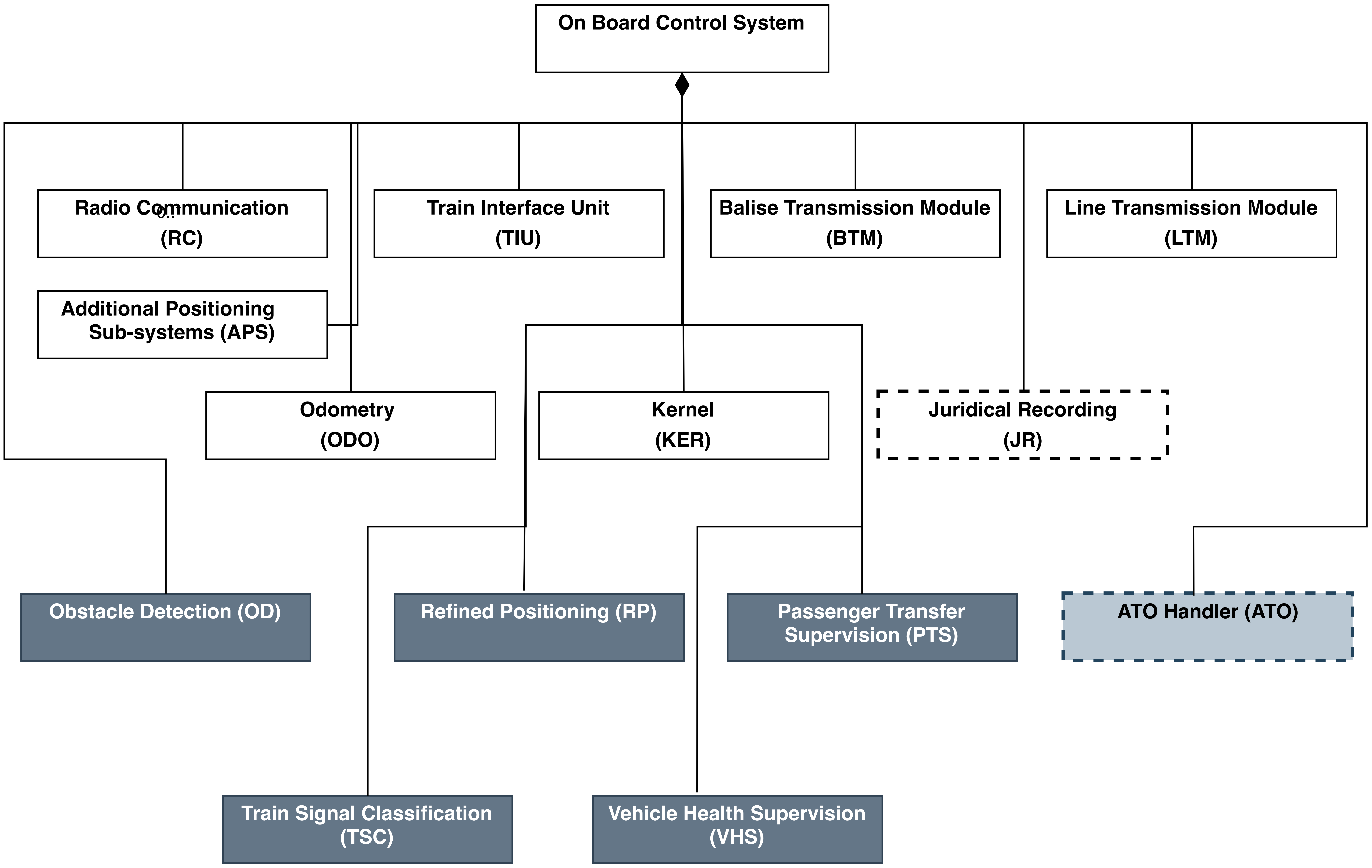


Source: https://es-static.fbk.eu/projects/eurailcheck/

Architecture for Autonomous Train Control

A “moderate” approach

- **Re-use generic architecture for ETCS train control**, as deployed on the European Vital Computer EVC
- Extend architecture by **new modules enabling autonomy**
- **Separate modules** using AI-based technologies from those using conventional technology
- Careful separation of modules for
  - **Automated train protection (ATP)** – this is the safety-critical part (SIL-4)
  - **Automated train operation (ATO)** – this can be certified as a sub-system according to a lower SIL (probably SIL-3), if the design ensures that ATP overrules ATO decisions



On Board Control System
Radio Communication (RC)
Train Interface Unit (TIU)
Balise Transmission Module (BTM)
Line Transmission Module (LTM)
Additional Positioning Sub-systems (APS)
Odometry (ODO)
Kernel (KER)
Juridical Recording (JR)
Obstacle Detection (OD)
Refined Positioning (RP)
Passenger Transfer Supervision (PTS)
ATO Handler (ATO)
Train Signal Classification (TSC)
Vehicle Health Supervision (VHS)

Main Controller

Deployed in kernel module

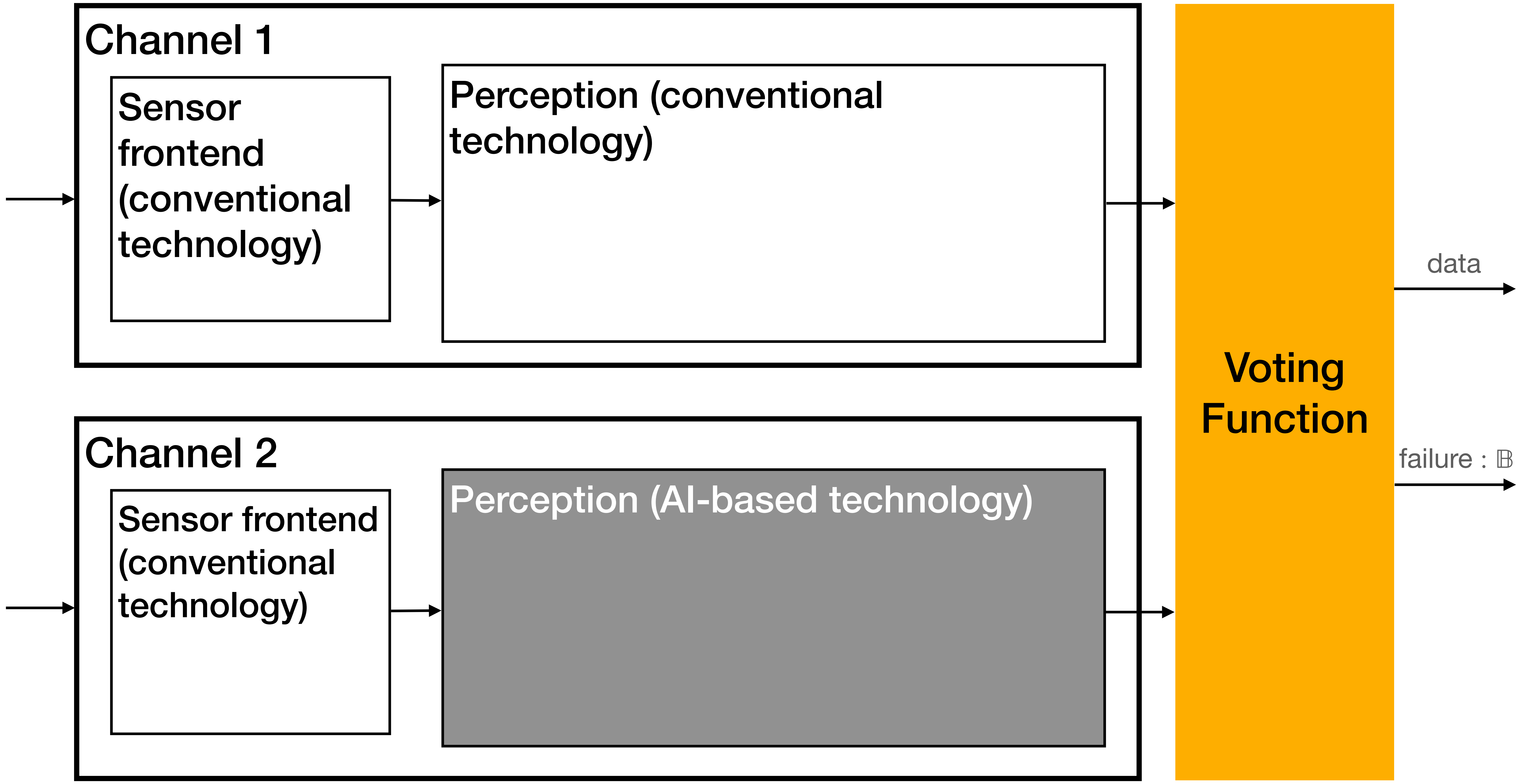
- Conventional control module (state machine model)
- Switches between autonomous and non-autonomous modes
- Provides automated train protection (ATP)
- Depends on data provided by
  - **modules with conventional technology**:
    radio communication, odometry, …
  - **modules with AI-based technology**:
    obstacle detection, train signal classification …


Main Controller (Kernel)
switch between operational modes
ODDControl
t_1
t_2
t_3
t_4
Autonomous normal operation
t_5
Autonomous degraded operation
Non-autonomous operation - remotely controlled
t_{10}
Non-autonomous operation - manual control
t_6
t_7
t_8
t_9
when (reset > 0)

Sensor/perceptor architecture

Redundancy increases safety

- Combine conventional technology with AI-based technology for various classification tasks – this ensures **stochastic independence of failure modes**



Mapping of architectural components

to safety integrity level and autonomy pipeline

	Sensing	Perception	Planning	Prediction	Control	Actuation
SIL-4	OD, TSC, RP, PTS, VHS	RC, ODO, APS, BTM, LTM	KER	KER	KER	TIU
SIL-4 +AI		OD, TSC, RP, PTS, VHS				
lower SIL +AI			ATO	ATO	ATO	

Evaluation According to ANSI/UL 4600

Evaluation Steps

according to ANSI/UL 4600

- **Step 1.** Identify all hazards related to autonomy and specify suitable mitigations
- **Step 2.** Specify the autonomy-related implications on the operational design domain ODD
- **Step 3.** Specify how each part of the autonomy pipeline contributes to the identified hazards and specify the mitigations designed to reduce the risks involved to an acceptable level


Absence of train engine driver
Hazard chain
Potential accident
H1. Undetected obstacles
Collision with obstacle
Train halted in wrong position
Injuries during (de-)boarding
H2. Insufficient position awareness
Collision
H3. Train movement during (de-)boarding
+ absence of train/station personnel
Derailing
Violation of Movement Authority
H4. Undetected visual signs and signals
Overspeeding
H5. Undetected train malfunctions
Unspecified accident
Step 1

Step 1. Hazard mitigations to enable autonomy

Id.	Hazard	Mitigations by pipeline
H1	Undetected obstacles	OD $\rightarrow$ KER $\rightarrow$ TIU
H2	Insufficient position awareness	{ODO,APS,BTM,RP} $\rightarrow$ KER $\rightarrow$ TIU
H3	Train movement during (de-)boarding	PTS $\rightarrow$ KER $\rightarrow$ TIU
H4	Undetected visual signs and signals	{LTM,TSC} $\rightarrow$ KER $\rightarrow$ TIU
H5	Undetected train malfunctions	VHS $\rightarrow$ KER $\rightarrow$ TIU

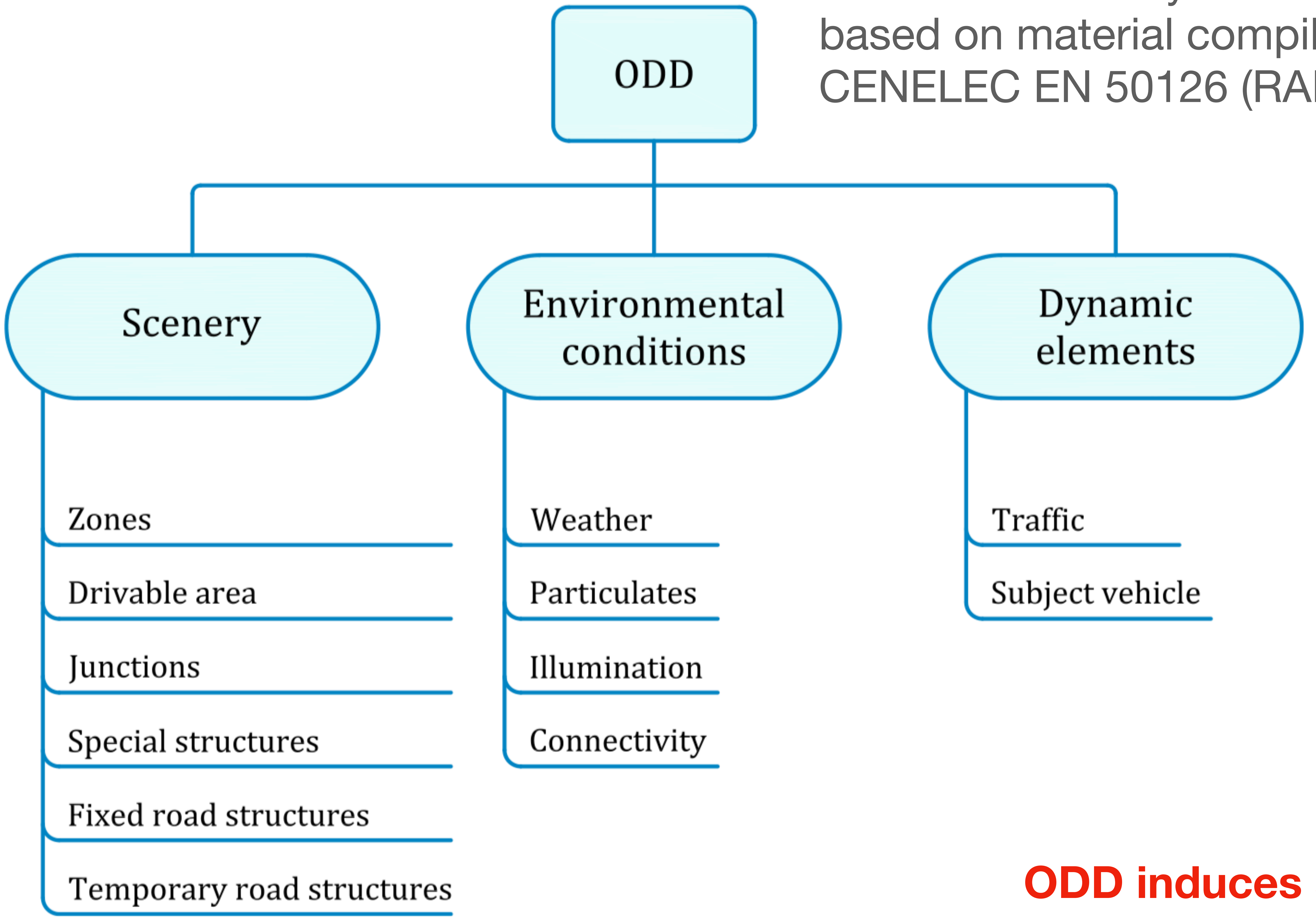
Step 2

ODD and autonomy-related implications

- **Operational Design Domain (ODD)**. The set of environments and situations the item is to operate within.
- Show that **system operation is safe within the limits of the ODD**

Original ODD taxonomy according to PAS 1883:2020 has been revised for the railway domain

Creation of railway ODD model can be based on material compiled for CENELEC EN 50126 (RAMS)



ODD induces system-level V&V objectives

Step 3

Evaluation of the autonomy pipeline

- Evaluation according to *ANSI/UL 4600, Section 8: Autonomy Functions and Support*
- Separate performance evaluation is required for each hazard mitigation pipeline
- **Step 3a.** Sensor evaluation
  - Covers redundancy management, mitigations for sensor performance degradation

Step 3
Evaluation of the autonomy pipeline

- **Step 3b.** Perceptor evaluation, covers
  - functional performance (acceptable false negative rate)
  - ontology-based evaluation of classification results
  - Justification of equivalence classes used during V&V
  - For perceptor channels based on trained neural networks
    - show diversity of training and evaluation data sets
    - show that correct classification results have been achieved *"for the correct reasons"*
    - show robustness, absence of brittleness

Step 3

Evaluation of the autonomy pipeline

- **Step c.** Evaluation of conventional sub-pipelines:
  planning → prediction → control → actuation
  - There is **no discrepancy between safety of the specified functionality and safety of the intended functionality**
  - Evaluation according to CENELEC EN 50128 suffices

Certifiable Hybrid Testing Approach

A new Strategy to Perform Testing for ATC

An approach to solve the test suite size problem for ATC

- On the module level, use **complete model-based testing strategies** with guaranteed fault coverage
- On the system level, use novel **scenario-based end-to-end testing strategy** and novel **strategy to assess system test coverage**, exploiting knowledge about complete module tests and their models
- Optimise the system test execution by
  - Multiple concurrent system **test executions on target systems and in the cloud**
  - Change of system test case objectives on-the-fly (**online testing**), driven by **continuous coverage assessment**
  - Coordination of system test executions by means of multi-agent system (**agent-based system testing**)

Kerstin I. Eder, Wen-ling Huang, Jan Peleska:
Complete Agent-driven Model-based System Testing for Autonomous Systems.
FMAS 2021: 54-72

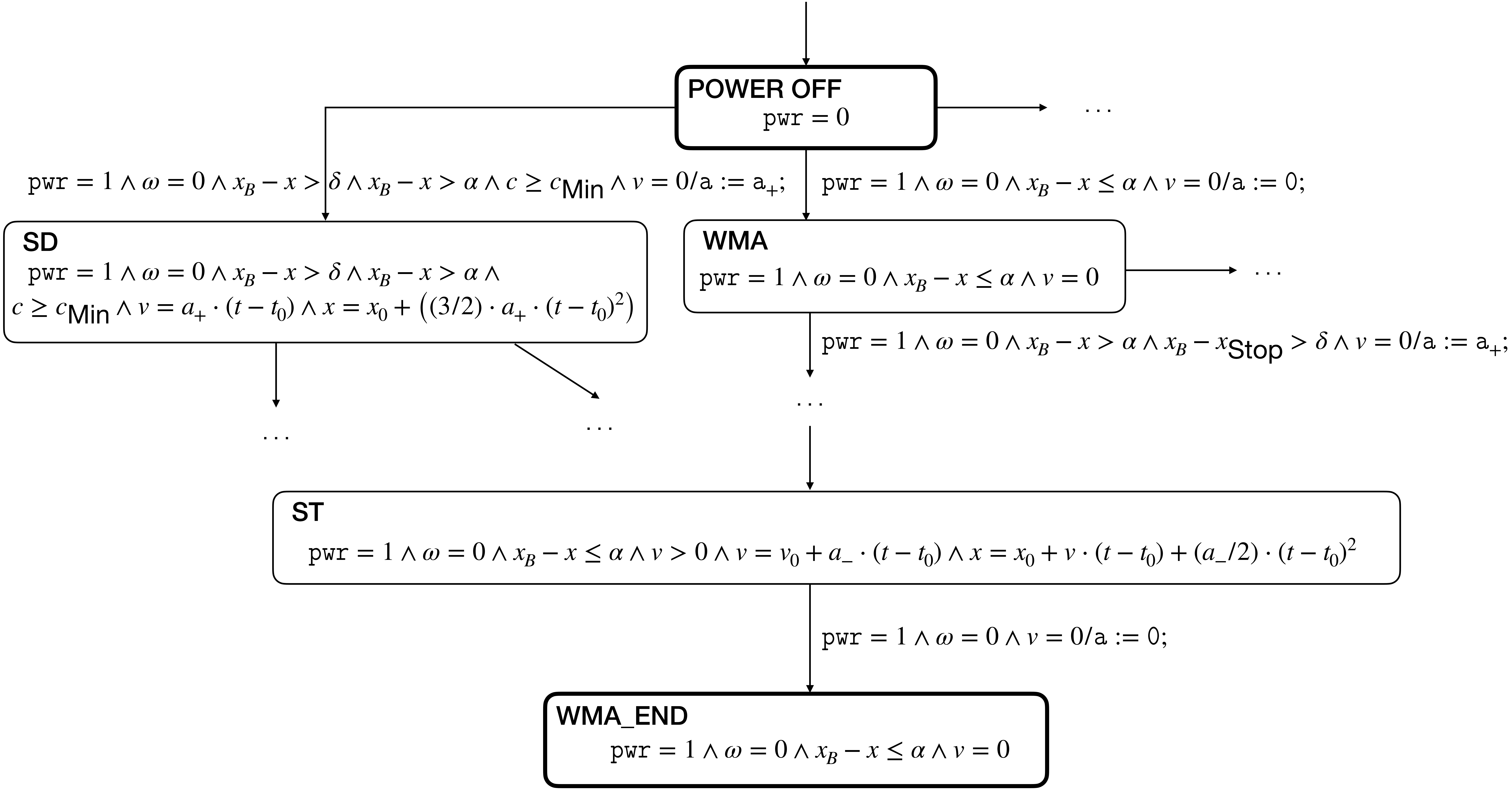
Test Execution of the System Level

Testing in the cloud

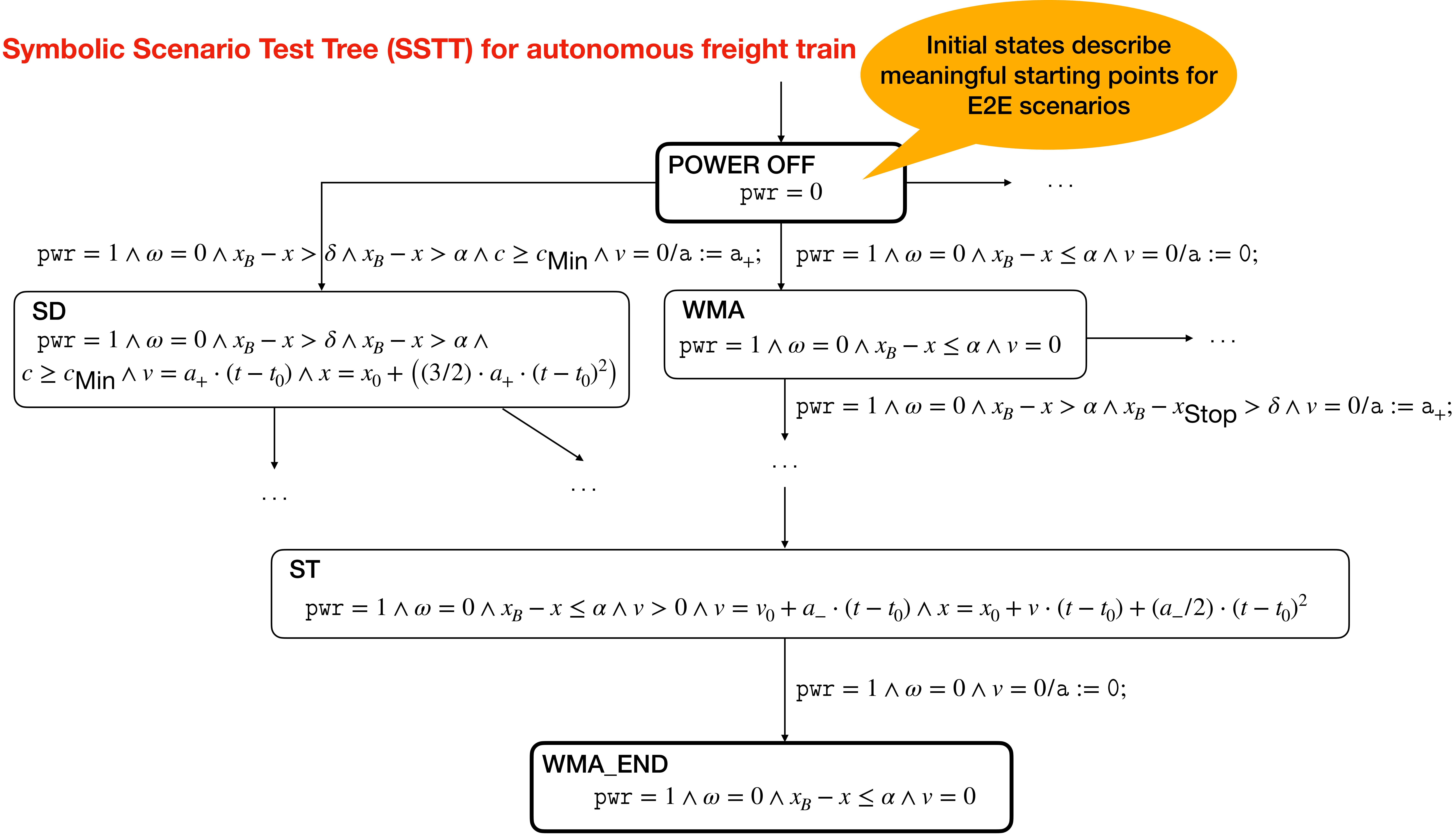
- Majority of tests have to be executed in the cloud, to ensure timely completion of test campaigns
- Prerequisites to obtain certification credit for test results obtained in the cloud
  - Trustworthy simulation of the “real” operational environment
  - Execution of the SUT software in trustworthy simulator (virtual prototype) modelling the target hardware (registers, address maps, …)

Vladimir Herdt, Daniel Große, Pascal Pieper & Rolf Drechsler (2020): **RISC-V based virtual prototype: An extensible and configurable platform for the system-level.** J. Syst. Archit. 109, p. 101756, doi:10.1016/j.sysarc.2020.101756.

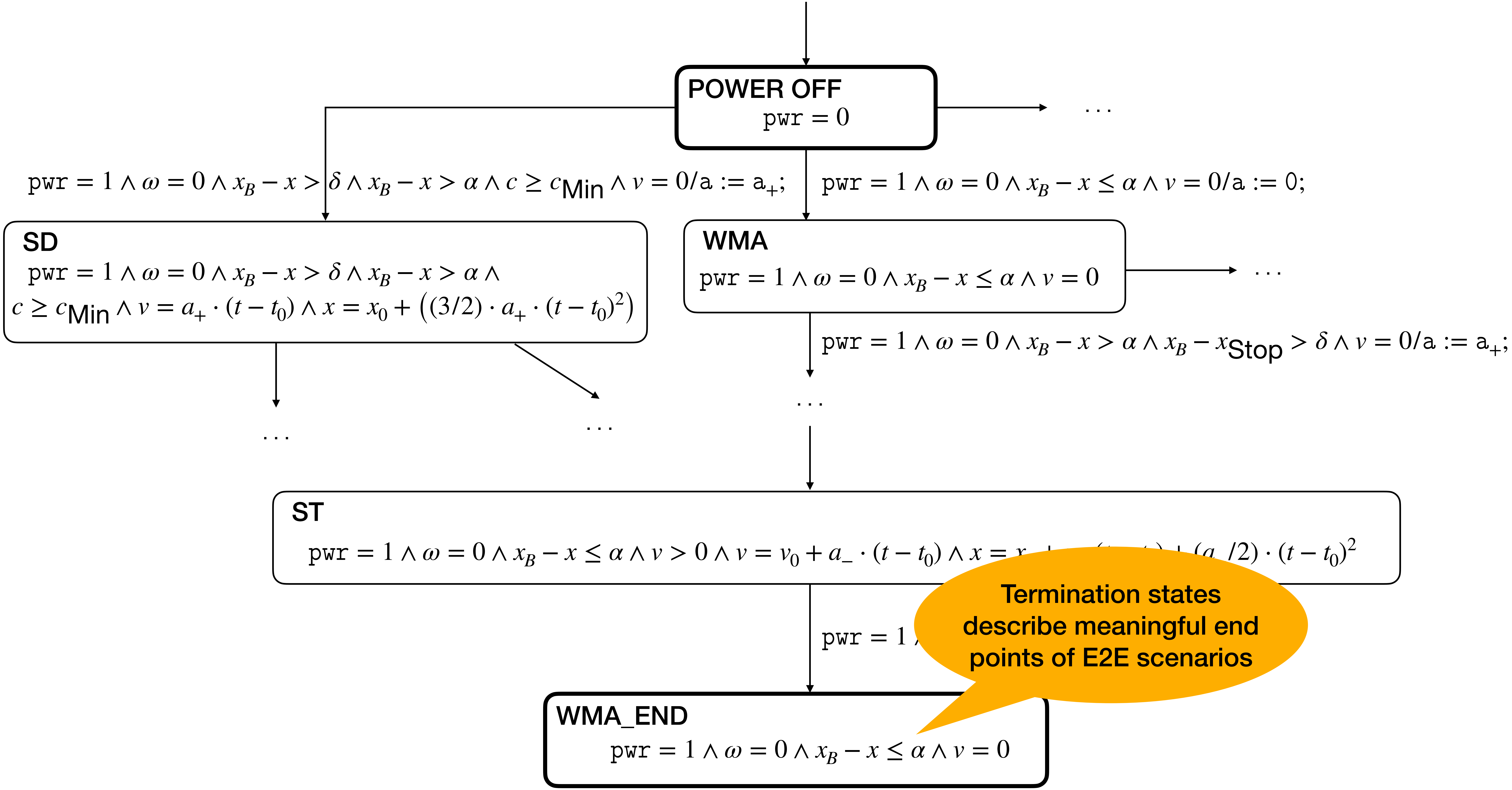
Symbolic Scenario Test Tree (SSTT) for autonomous freight train



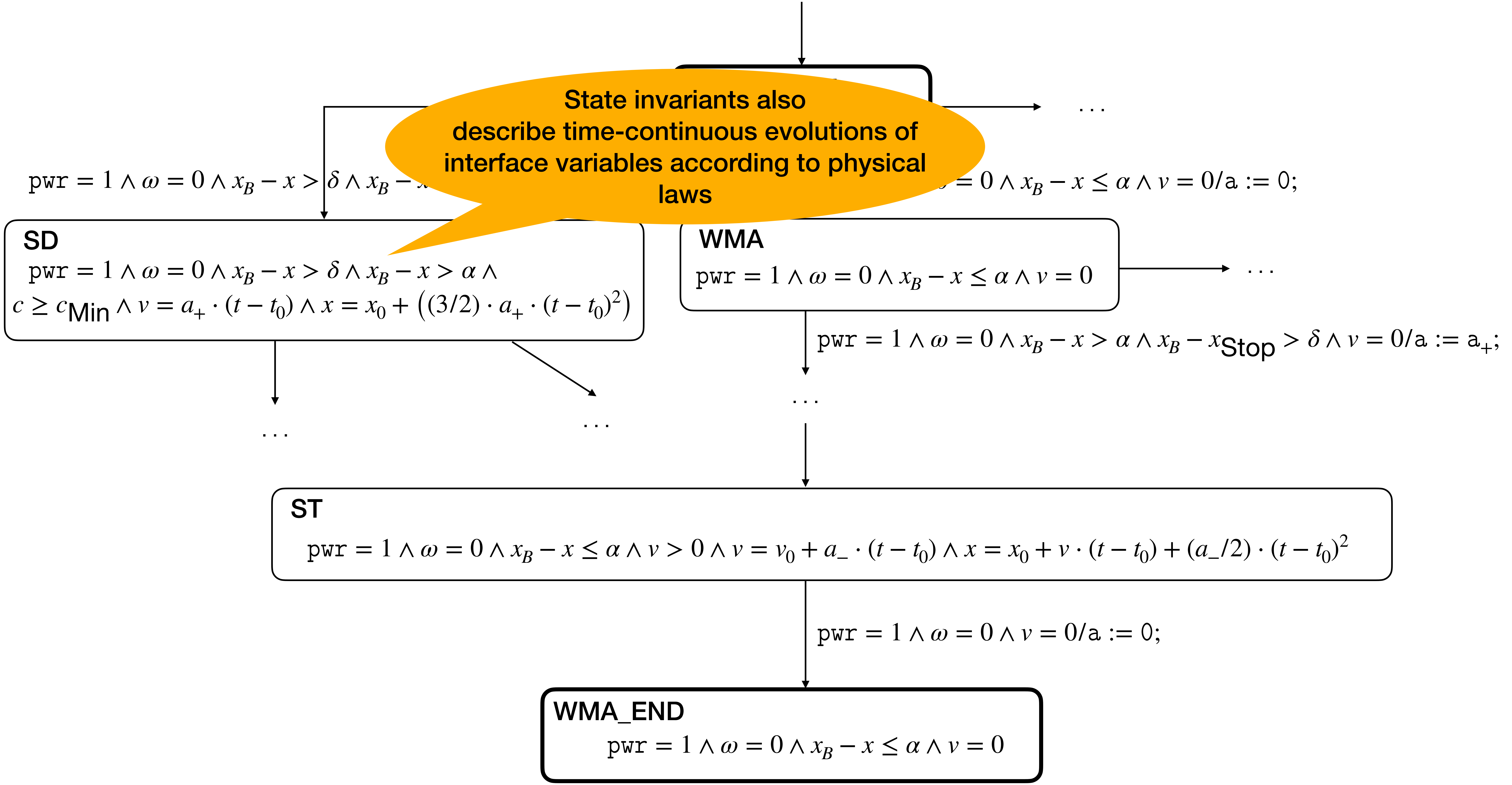
Symbolic Scenario Test Tree (SSTT) for autonomous freight train



Symbolic Scenario Test Tree (SSTT) for autonomous freight train



Symbolic Scenario Test Tree (SSTT) for autonomous freight train



Conclusion

Conclusion

Summary

- An architecture for on-board train control of autonomous trains has been presented
- As a thought experiment, an evaluation according to ANSI/UL 4600 has been performed
- Certifiability seems feasible for trains with low velocity (metro trains, freight trains)
  - This restriction is necessary since there is no evidence that obstacle detection and visual signal evaluation could work for speeds above 120km/h
- ANSI/UL 4600 addresses V&V objectives related to autonomous control and AI-based technologies in a rather comprehensive way
- Combined system tests performed with original equipment in cloud simulation environments could achieve certification credit, based on formally justified coverage criteria

Conclusion

Future work

- Perform quantitative risk analysis based on stochastic model checking
- Implement architecture on model train
- Perform proof of concept of combined module test/system test strategy for model train

THANK YOU VERY MUCH FOR YOUR ATTENTION!