Standardisation Consideration for Autonomous Train Control

Jan Peleska – peleska@uni-bremen.de,
Anne E. Haxthausen aeha@dtu.dk and Thierry Lecomte thierry.lecomte@clearsy.com

ISoLA 2022
DisCo Rail 2022

2022-10-25

Motivation

Certifiable autonomous train control systems

- A couple of years ago, a suitable set of standards serving as certification basis for autonomous trains was not available
- **Today, we advocate to combine**
  - **the existing standards CENELEC EN 50126, 50128, 50129 with**
  - **the new pre-standard ANSI/UL 4600 for assuring system-level safety**
- We present a “thought experiment” how verification and validation (V&V) could be performed for autonomous freight trains and metro trains,
  - based on the standards above and
  - a specific “conservative” architectural approach

Motivation

Certifiable autonomous train control systems

- A couple of years ago, a suitable set of standards serving as certification basis for autonomous trains was not available
- Today, we advocate to combine
  - the existing standards CENELEC EN 50126, 5012
  - the new pre-standard ANSI/UL 4600 for assuring syst

In open environments with today's railway infrastructure

- We present a "thought experiment" how verification and validation (V&V) could be performed for autonomous freight trains and metro trains,
  - based on the standards above and
  - a specific "conservative" architectural approach

Side Remark

Autonomous versus Automatic

- **GoA 4 – Grade 4 of Automation**
  - Unattended train operation, neither the driver nor the staff are required
- Flammini et al. present a detailed discussion of **“real autonomy” versus “just automation”** in automated train control (ATC) systems

  Flammini, F., Donato, L.D., Fantechi, A., Vittorini, V.: A vision of intelligent train control. In: Dutilleul, S.C., Haxthausen, A.E., Lecomte, T. (eds.) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - 4th International Conference, RSSRail 2022, Paris, France, June 12, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13294, pp. 192–208. Springer (2022), https://doi.org/10.1007/978-3-031-05814-1_14
- **In this talk, we are addressing truly autonomous systems, though with a “mild” and very concisely defined degree of autonomy**

Overview

- Reference architecture for autonomous trains
- Sample evaluation according to ANSI/UL 4600
- Conclusion and future work

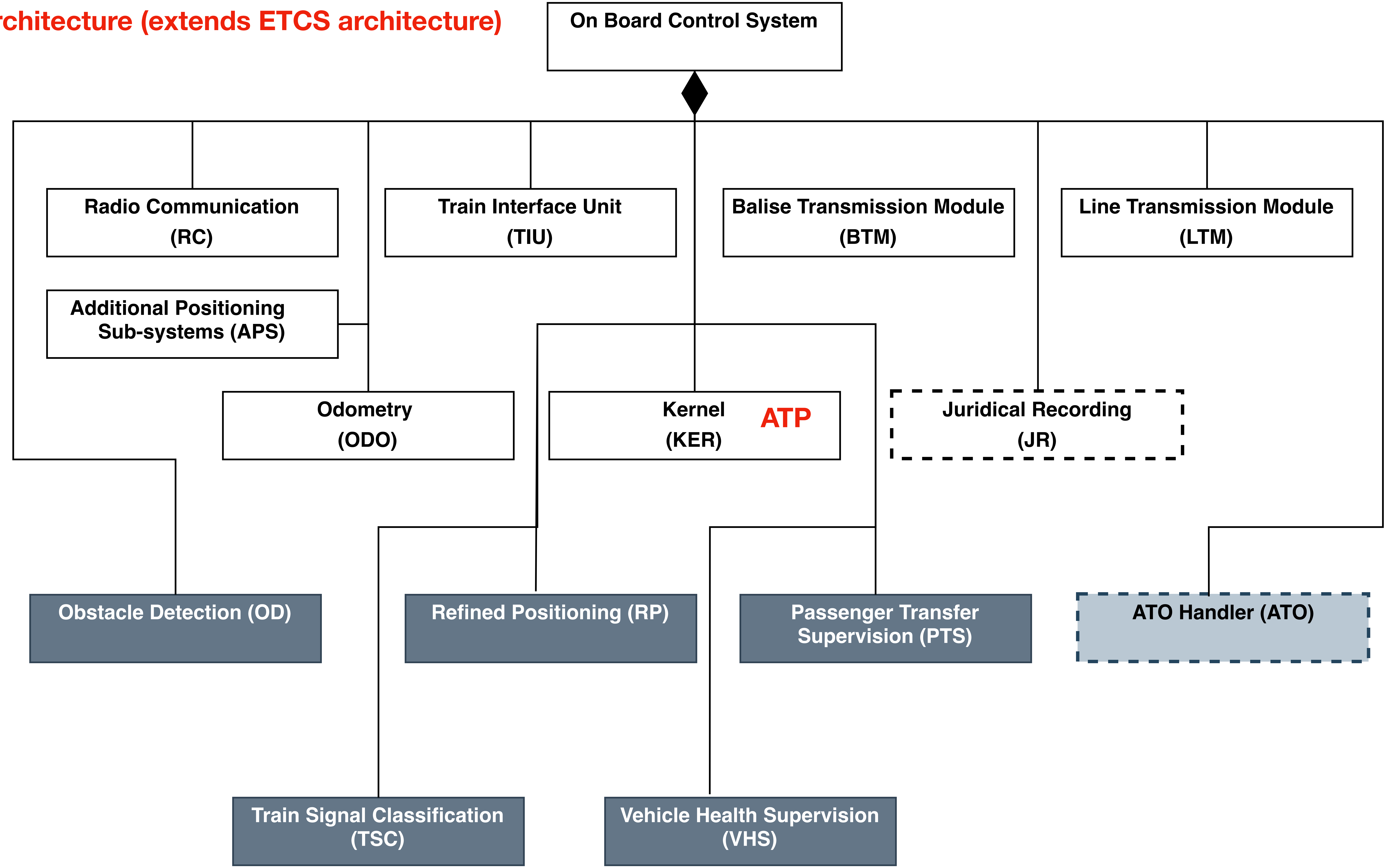
Reference architecture for autonomous trains

Reference architecture

for autonomous trains

- The existing ETCS reference architecture can be extended to incorporate **components supporting automated train control (ATC)** in autonomous operation
    - Obstacle detection (OD)
    - Refined positioning (RP)
    - Passenger transfer supervision (PTS)
    - Train signal classification (TSC)
    - Vehicle health supervision (VHS)

ATC Architecture (extends ETCS architecture)

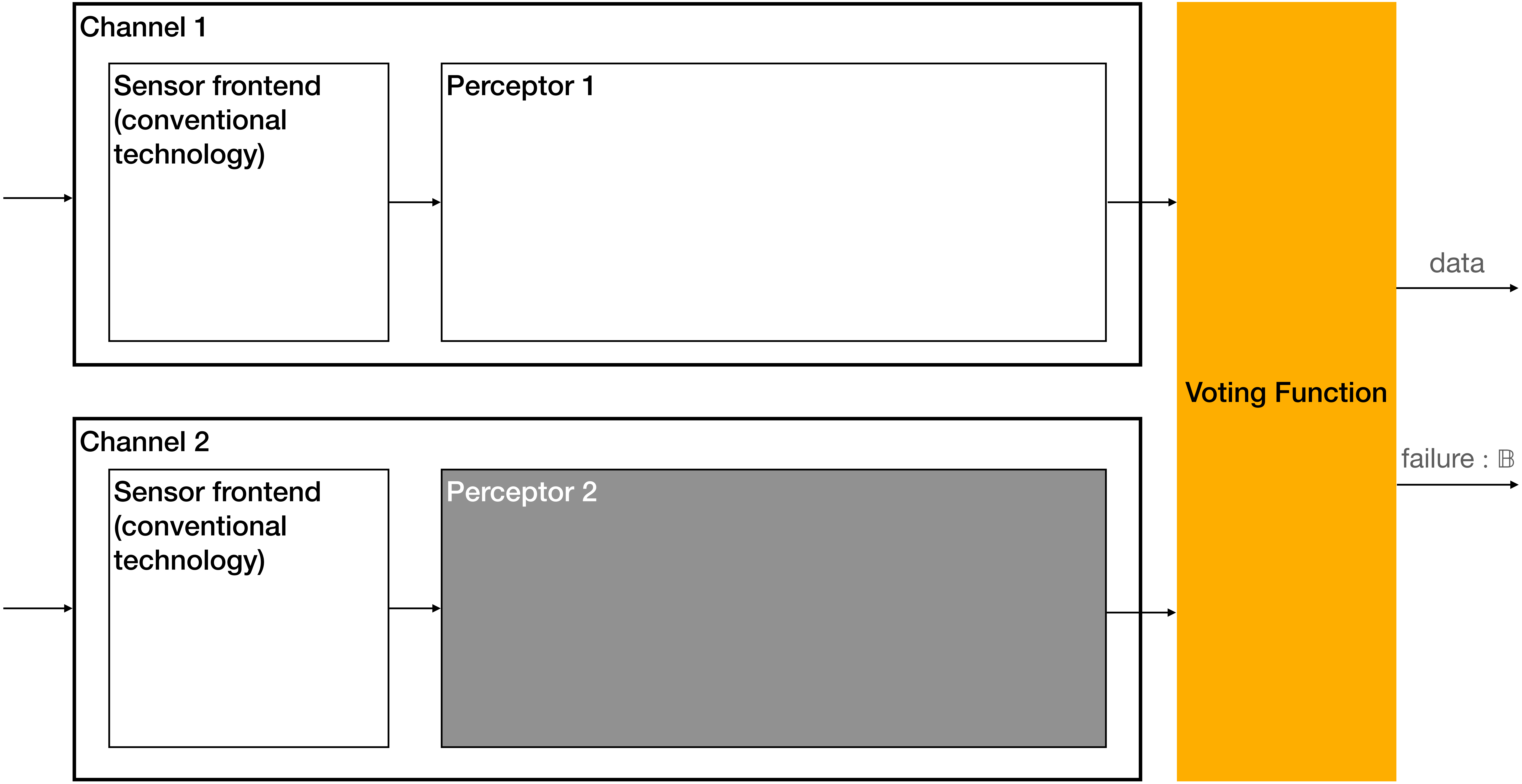


ATC Architecture (extends ETCS architecture)

Increase trustworthiness of AI-based support functions

A 2-out-of-2 channel architecture

- 2-Channel system consists of
  - Redundant, stochastically independent power supplies and wiring
  - Redundant, stochastically independent sensors (e.g. cameras, radars)
  - **Redundant, stochastically independent perceptors, for example,**
    - **Perceptor 1 – conventional image processing technology**
    - **Perceptor 2 – trained neural network**
  - **Voter performing decisions to the safe side**



Channel 1
Sensor frontend (conventional technology)
Perceptor 1
Channel 2
Sensor frontend (conventional technology)
Perceptor 2
Voting Function
data
failure : $\mathbb{B}$

Operational modes

Switching between autonomous, degraded, and manual operation

- Any failure of sensors and perceptors supporting autonomous operation leads to
  - **degraded autonomous operation** (e.g. low speed until train position is determined again with high confidence), or
  - **remotely controlled or manual operation** in case of unrecoverable failures in ATP and/or supporting functions (e.g. permanent disagreement of obstacle detection perceptors)

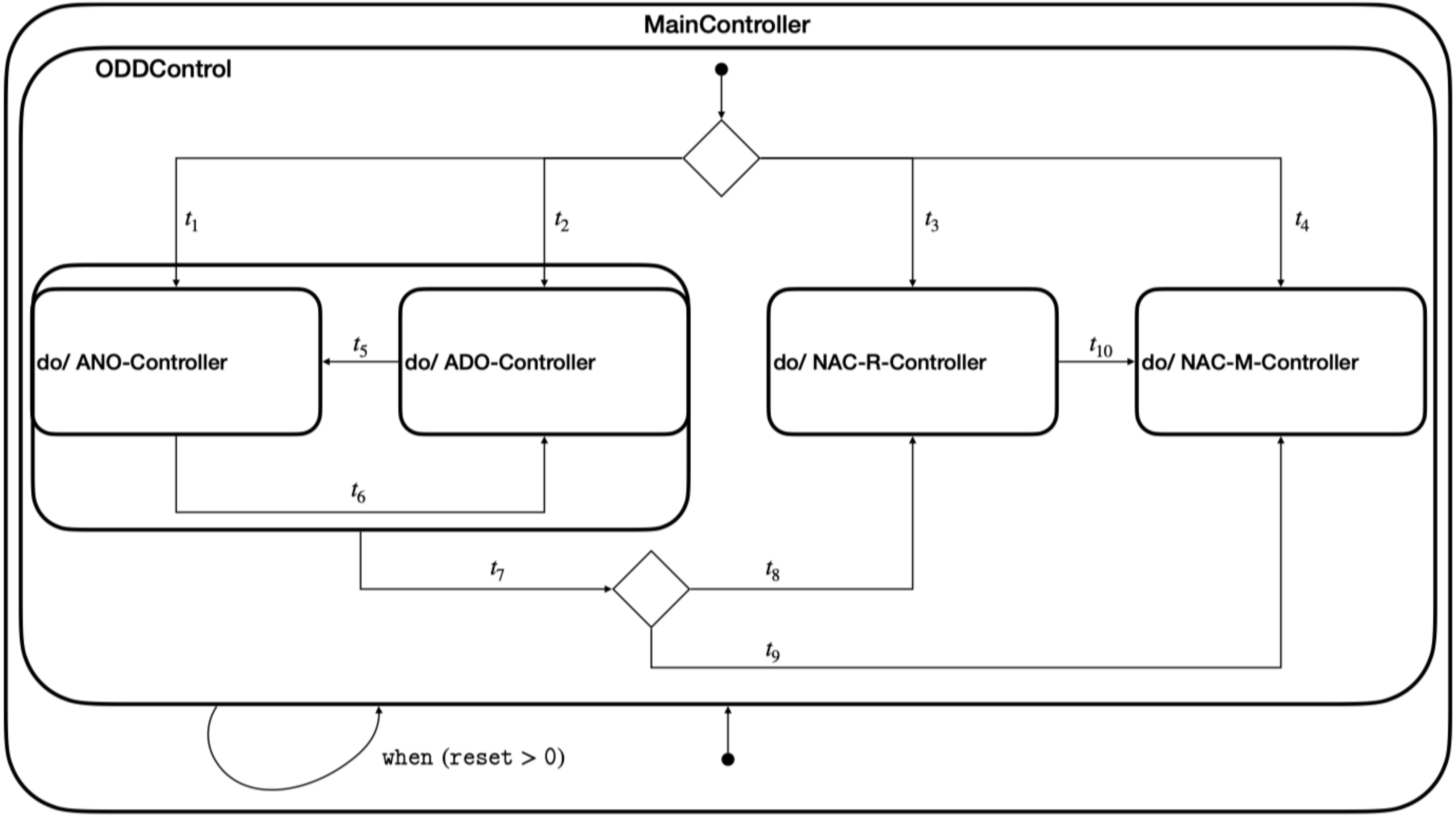


Fig. 2. Operational modes for train protection in autonomous trains.

Table 1. Mapping of architectural components to SIL 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	

Design characteristic facilitating assurance

Strict separation of safety-critical components from components implementing application logic

Sample evaluation according to ANSI/UL 4600

Step 1. Hazard analysis

Autonomy functions – related hazards – mitigations

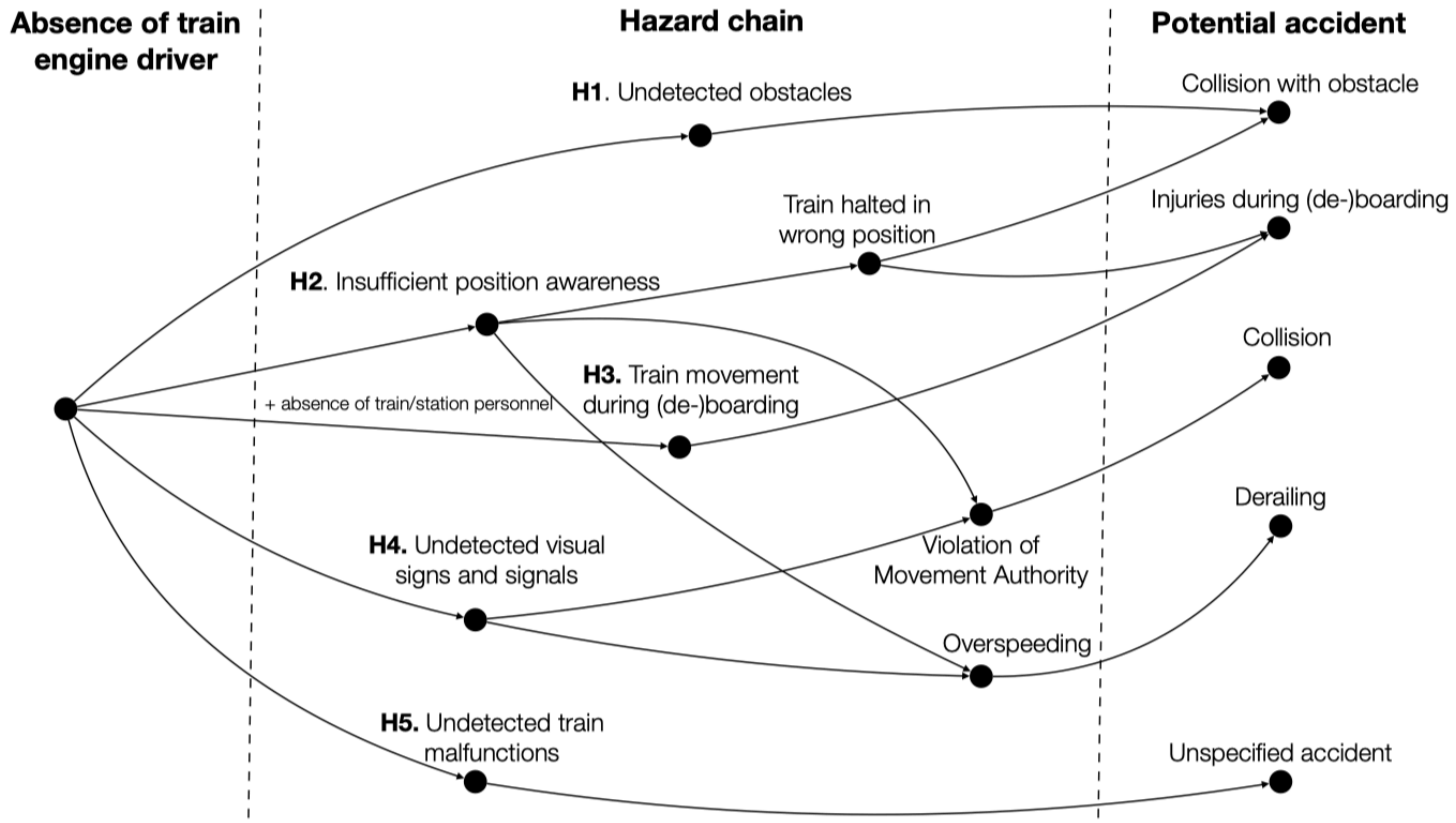


Table 2. Hazard mitigations to enable autonomy.

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. Elaborate Operational Design Domain (ODD)

and relate safety cases to ODD

ODD

- **Scenery**
  - Train station
  - Open track
  - Tunnel
  - Level crossing
  - Maintenance site
  - . . .
- **Environmental conditions**
  - Weather
  - Lighting conditions
  - Infrastructure availability
  - . . .
- **Dynamic elements**
  - Train and its speed
  - Obstacle occurrence
  - . . .

Step 2. Elaborate Operational Design Domain (ODD)

and relate safety cases to ODD

This serves as a coverage basis for system tests

ODD

- **Scenery**
  - Train station
  - Open track
  - Tunnel
  - Level crossing
  - Maintenance site
  - . . .
- **Environmental conditions**
  - Weather
  - Lighting conditions
  - Infrastructure availability
  - . . .
- **Dynamic elements**
  - Train and its speed
  - Obstacle occurrence
  - . . .

Step 3. Evaluation of the autonomy pipeline

Perception

- **Main goal: perceptor performance ensures safety of the intended functionality (SOTIF)**
  - Show that false negative rate is acceptable (safety critical)
  - Show that false positive rate is acceptable (to ensure availability)
  - Justify that
    - training and V&V data sets are sufficiently independent from each other
    - perceptor results are correctly mapped to ontology
    - equivalence classes have been adequately chosen
    - perceptor is sufficiently robust (absence of brittleness and overfitting)

Step 3. Evaluation of the autonomy pipeline

sensing – planning – prediction – control – actuation

- These pipeline components are based on conventional design and can be evaluated according to CENELEC standards

Conclusion and future work

Conclusion

- **Evaluation and certification on the basis of CENELEC and ANSI/UL 4600 seems feasible for slow freight trains and metro trains**
- The certifiability strongly relies on the very conservative architecture presented here
- For freight trains running on modern railway networks with line transmission of signal aspects or ETCS infrastructure, the architectural components depending on AI and machine learning are reduced to obstacle detection
- The evaluation presented here was qualitative – quantitative risk assessment still pending
- **Remark**. Obstacle detection can be made even safer by track-side detection equipment at danger points (e.g. lighting and cameras installed at level crossings)

Future Work

- Create **stochastic world model** to obtain quantitative risk values
  - Based on stochastic model checking with PRISM
- Trustworthiness of qualitative risk assessment depends on two other research foci based on sound stochastic arguments and associated statistical tests
  - Ensure that two classification methods (e.g. for obstacle detection) are **stochastically independent**
  - Ensure that the residual **probability for misclassifications** of such a method is less than some low probability p and that this statement is true with high confidence γ

Future Work

Mario Gleirscher, Radu Calinescu, James A. Douthwaite, Benjamin Lesage, Colin Paterson, Jonathan M. Aitken, Rob Alexander, James Law:
Verified synthesis of optimal safety controllers for human-robot collaboration. Sci. Comput. Program. 218: 102809 (2022)

- Create stochastic world model to obtain quantitative risk values
  - Based on stoc

Hana Chockler, Daniel Kroening, Youcheng Sun:
Compositional Explanations for Image Classifiers.
CoRR abs/2103.03622 (2021)

- Trustworthiness … two other research foci based on sound stochastic arguments and associated statistical tests
  - Ensure that two classification methods (e.g. for obstacle detection) are stochastically independent
  - Ensure that the residual probability for misclassifications of such a method is less than some low probability p and that this statement is true with high confidence γ

Philippe Flajolet, Daniele Gardy, and Loys Thimonier. Birthday paradox, coupon collectors, caching algorithms and self-organizing search. Discrete Applied Mathematics, 39(3):207{229, 1992. ISSN 0166-218X. doi: https://doi.org/10. 1016/0166-218X(92)90177-C.

Supporting R&D Projects and Organisations

UNIVERSITY of York

Assuring Autonomy International Programme

RoboStar*

HiDyVe

Universität Bremen

UKRI Verifiability Node

UKRI

Trustworthy Autonomous Systems UK Verifiability Node

CLEARSY

Safety Solutions Designer

SafeTRANS

SAFETY IN TRANSPORTATION SYSTEMS

Further Reading

Related to this presentation

1. Flammini, F., Donato, L.D., Fantechi, A., Vittorini, V.: A vision of intelligent train control. In: Dutilleul, S.C., Haxthausen, A.E., Lecomte, T. (eds.) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - 4th International Conference, RSSRail 2022, Paris, France, June 12, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13294, pp. 192–208. Springer (2022), https://doi.org/10.1007/978-3-031-05814-1_14

2. Trentesaux, D., Dahyot, R., Ouedraogo, A., Arenas, D., Lefebvre, S., Sch¨on, W., Lussier, B., Ch´eritel, H.: The Autonomous Train. In: 2018 13th Annual Conference on System of Systems Engineering (SoSE). pp. 514–520 (Jun 2018)

3. Risti´c-Durrant, D., Franke, M., Michels, K.: A Review of Vision-Based On-Board Obstacle Detection and Distance Estimation in Railways. Sensors (Basel, Switzerland) 21(10), 3452 (May 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/ PMC8156009/

4. Kerstin I. Eder, Wen-ling Huang, and Jan Peleska. Complete agent-driven model-based system testing for autonomous systems. In Marie Farrell and Matt Luckcuck, editors, Proceedings Third Workshop on Formal Methods for Autonomous Systems, FMAS 2021, Virtual, 21st-22nd of October 2021, volume 348 of EPTCS, pages 54–72, 2021b. doi: 10.4204/EPTCS.348.4. URL https://doi.org/10.4204/EPTCS.348.4

5. Mario Gleirscher and Jan Peleska. Complete test of synthesised safety supervisors for robots and autonomous systems. In Marie Farrell and Matt Luckcuck, editors, Proceedings Third Workshop on Formal Methods for Autonomous Systems, FMAS 2021, Virtual, 21st-22nd of October 2021, volume 348 of EPTCS, pages 101–109, 2021. doi: 10.4204/EPTCS.348.7. URL https://doi. org/10.4204/EPTCS.348.7

THANK YOU VERY MUCH FOR YOUR ATTENTION!