Self-Driving Cars: Challenging Reliable Distributed Systems

SRDS, Vienna, Sep/22, 2022

Wilfried Steiner

TTTech Computertechnik AG

Our vision

Advancing safe technologies, improving human lives

TTTech Group
Key facts

Founded in **1998**, headquartered in Vienna, Austria, with **19** offices in **14** countries worldwide

Products in **1173** production programs

Connected companies: TTTech Auto, TTTech Industrial, TTControl, RT-RK

2,300
Employees/ subcontractors

60
Nations represented by our workforce

380
R&D/ENG/ADMIN

50
TTTech Industrial

490
RT-RK Classic

100
TTControl

1,170
TTTech Auto

90
TTTech Aerospace

Numbers as of March 2022

TTTech

Market overview

TTTechAuto

- Digital platforms for highly automated vehicles

TTControl
HYDAC INTERNATIONAL

- Construction
- Agriculture
- Material handling
- Municipal vehicles
- Special vehicles

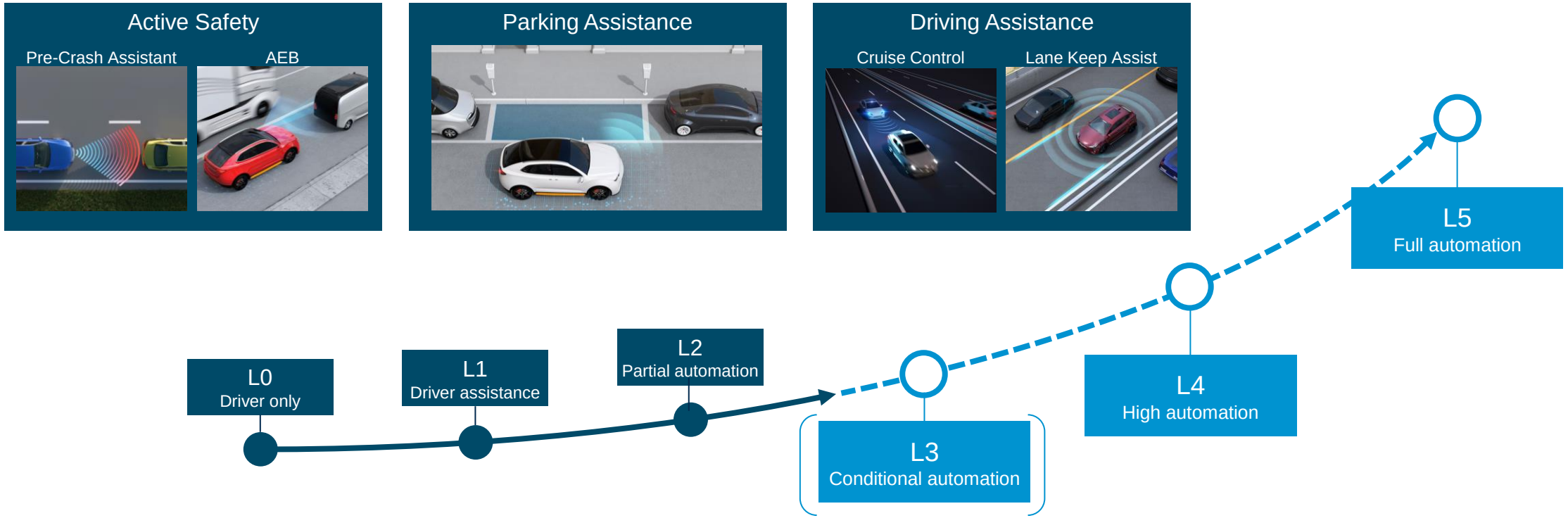
TTTech industrial

- Discrete manufacturing
- Process automation
- Energy production
- Smart grid
- Logistics

TTTech Aerospace

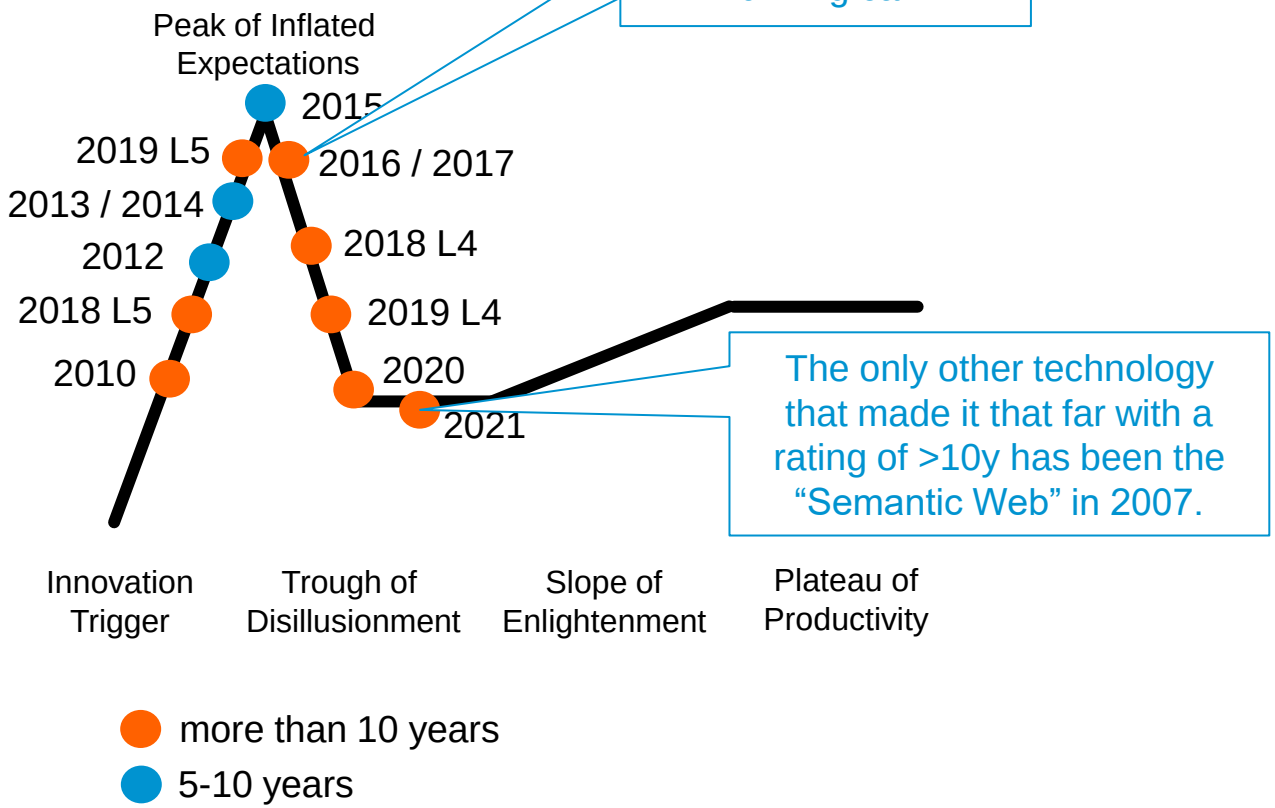
- Fixed wing aircraft
- Rotorcraft
- Human space flight
- Space: launcher, robotics, satellites
- UAV / UAM

From fail-safe to fail-operational systems



Where do we stand?
Hype Cycle on Autonomous Systems 2010-2021

Why is it so hard?



Safety is the grand challenge to introduce Level 4 Automated Driving

TTTech

Perception and the “World Model”

Fail-Operational Safety Architecture

System Verification & Validation

Safety is the grand challenge to introduce Level 4 Automated Driving

TTTech

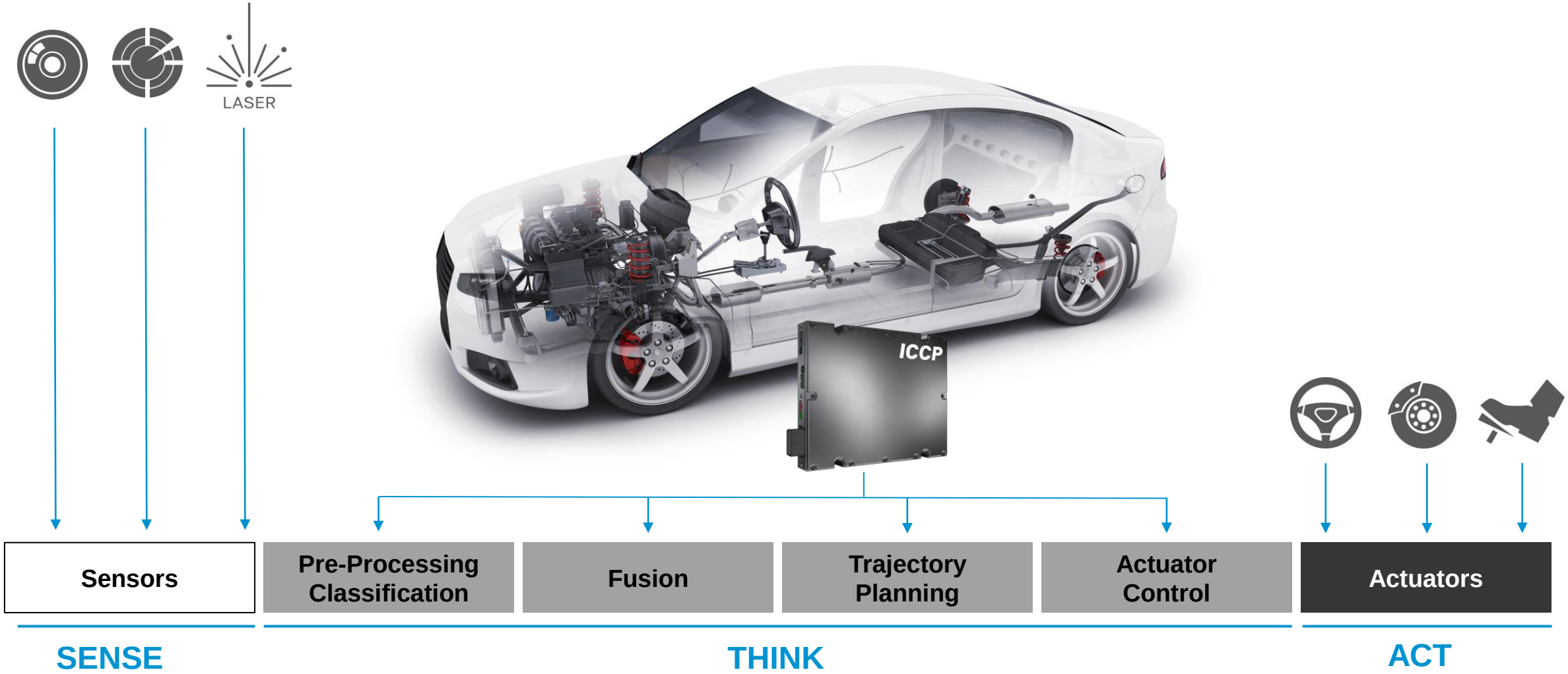
Perception and the “World Model”

Fail-Operational Safety Architecture

System Verification & Validation

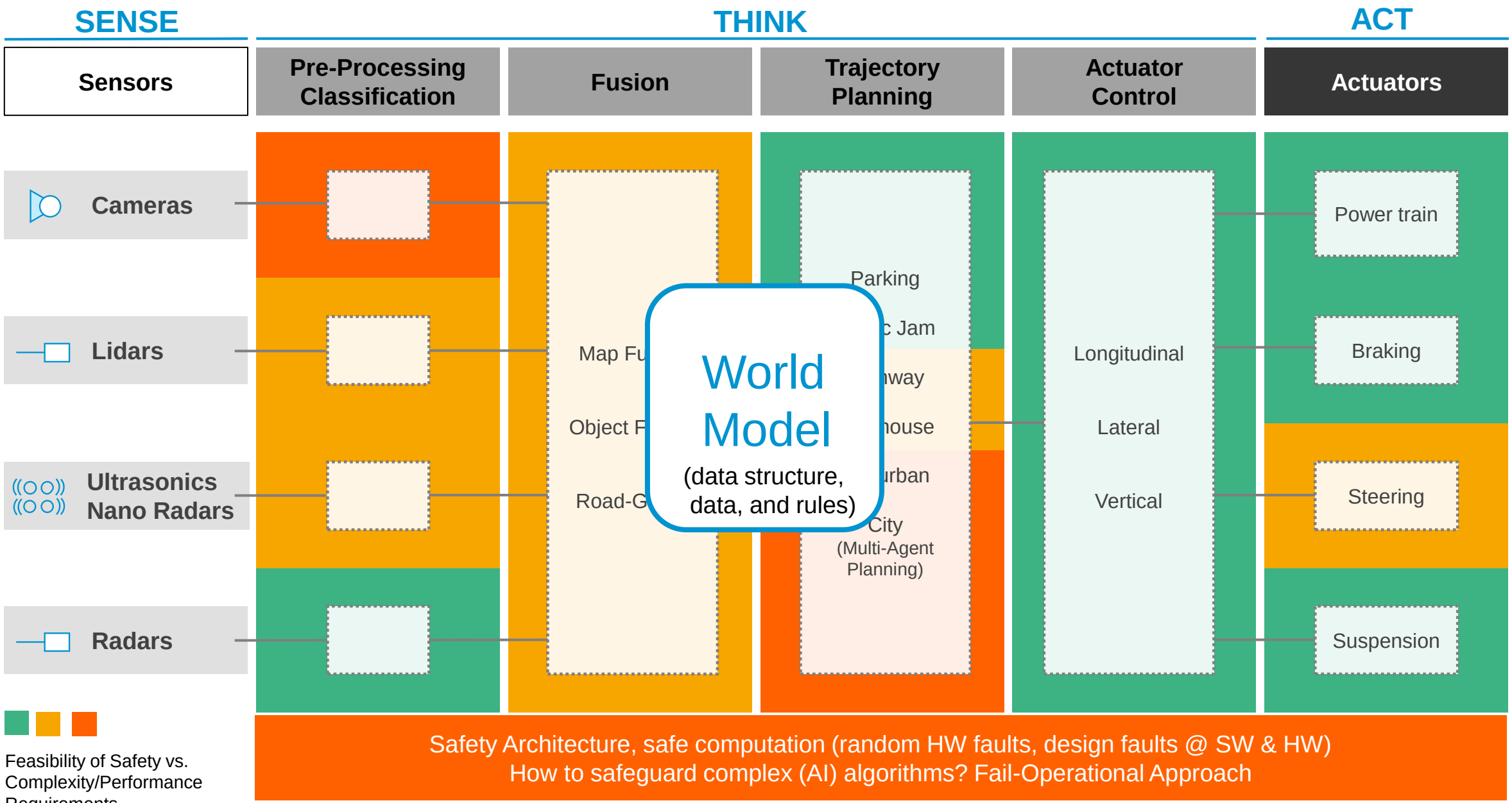
Automated Driving as Closed-Control Loop

TTTech

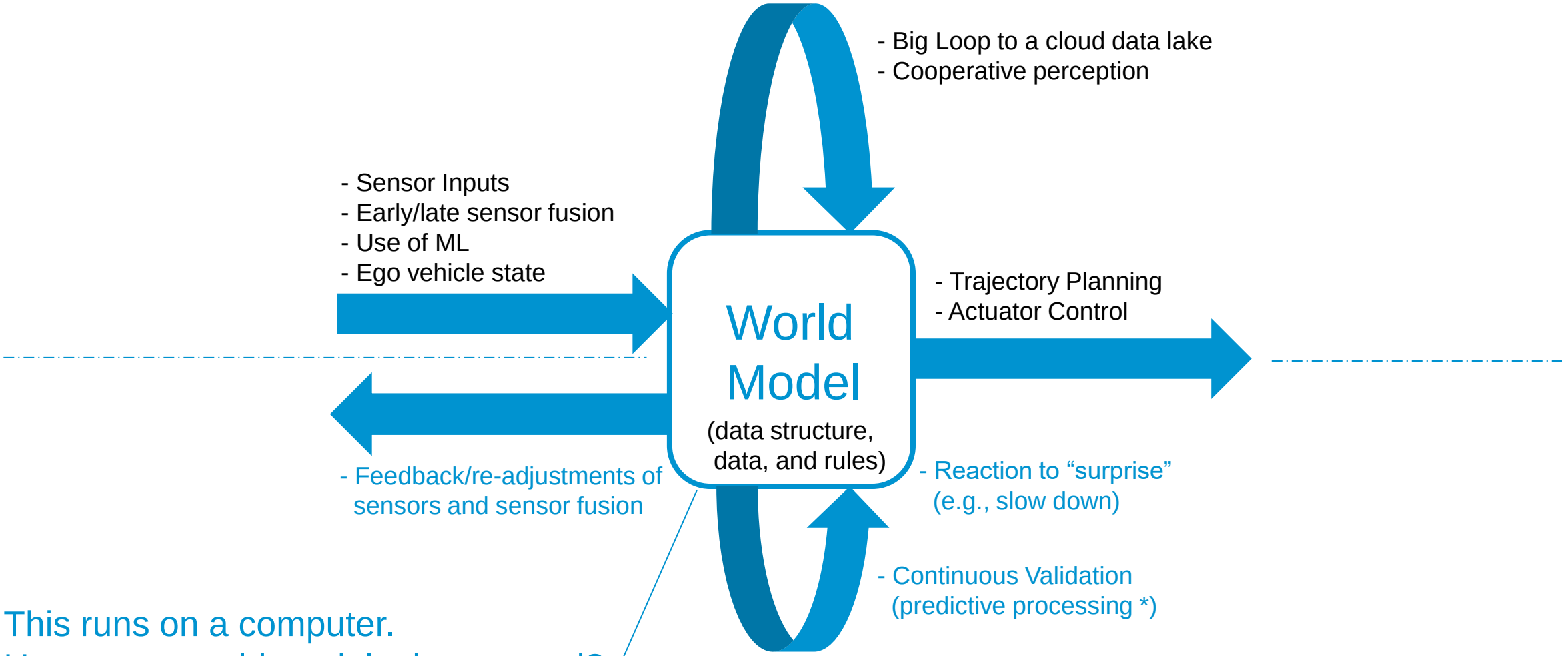


The Automated Driving Challenge Heatmap

TTTechAuto



World Model as a Centerpiece for Assurance



This runs on a computer.
How many world models do we need?

* Rushby, J. (2022). *Models and their Validation and their Role in Perception And in Safe Autonomous Vehicles*. IFIP WG10.4 Virtual Meeting. URL: http://www.csl.sri.com/users/rushby/abstracts/ifip-11may22

Safety is the grand challenge to introduce Level 4 Automated Driving

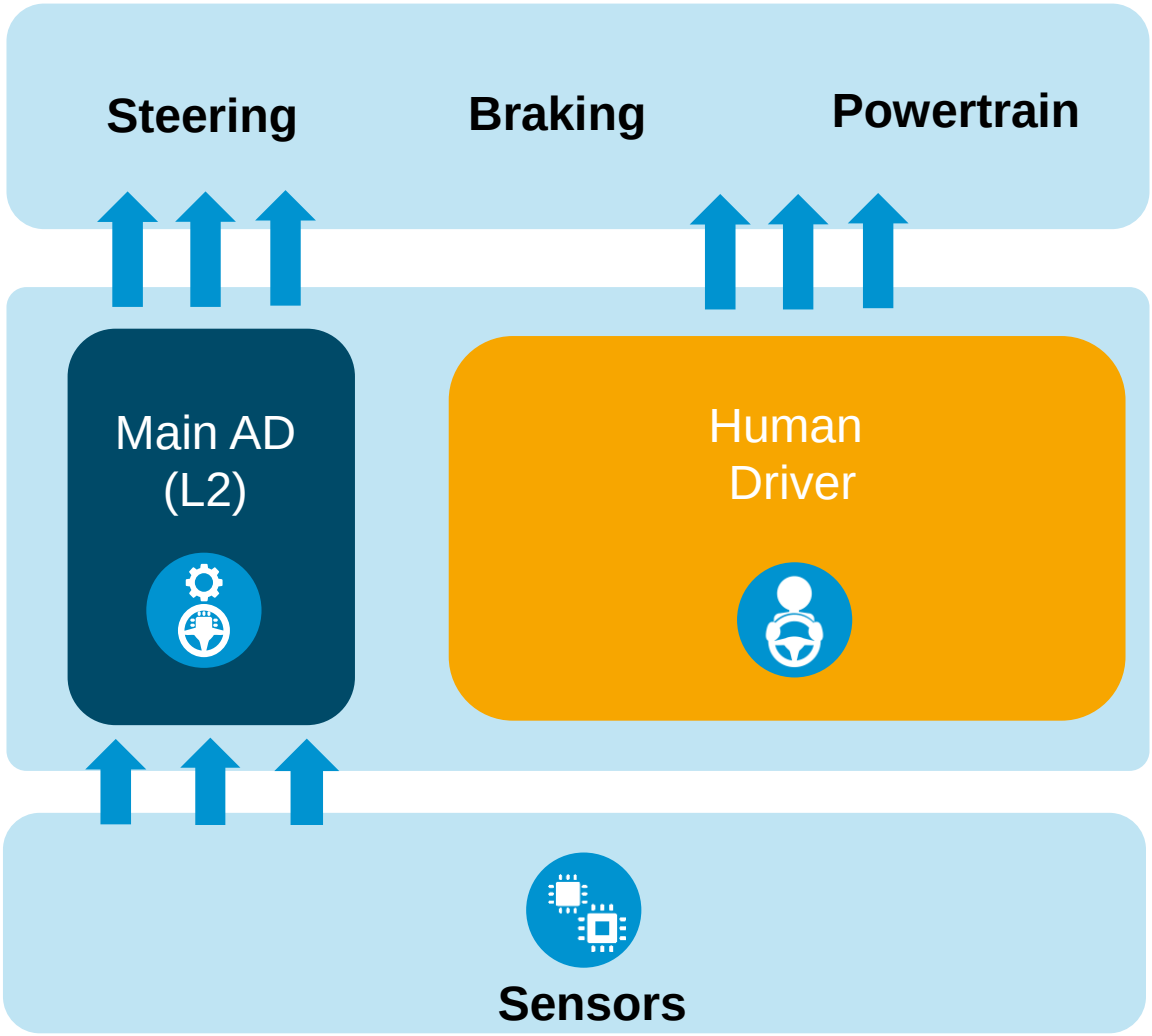
TTTech

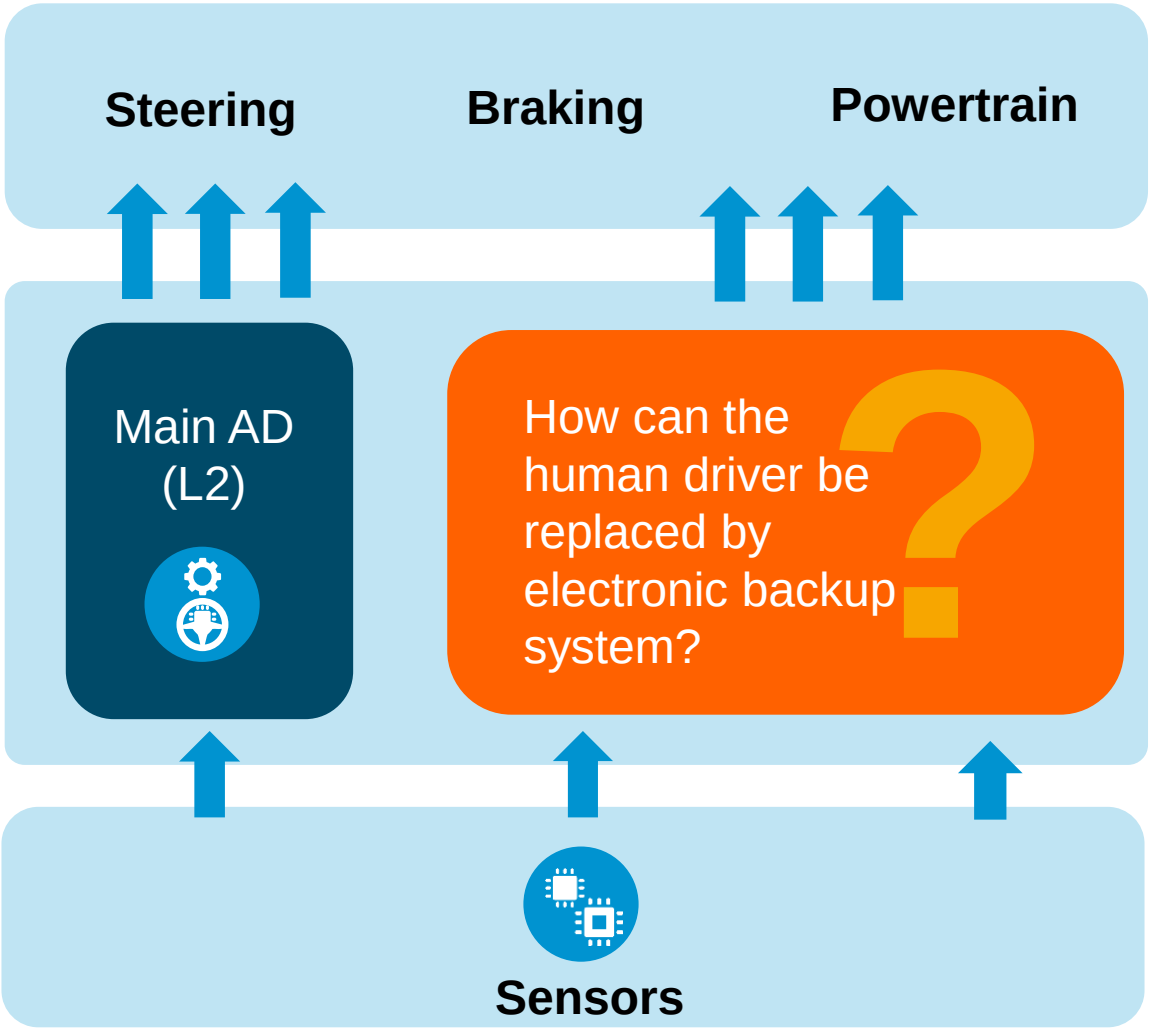
Perception and the “World Model”

Fail-Operational Safety Architecture

System Verification & Validation

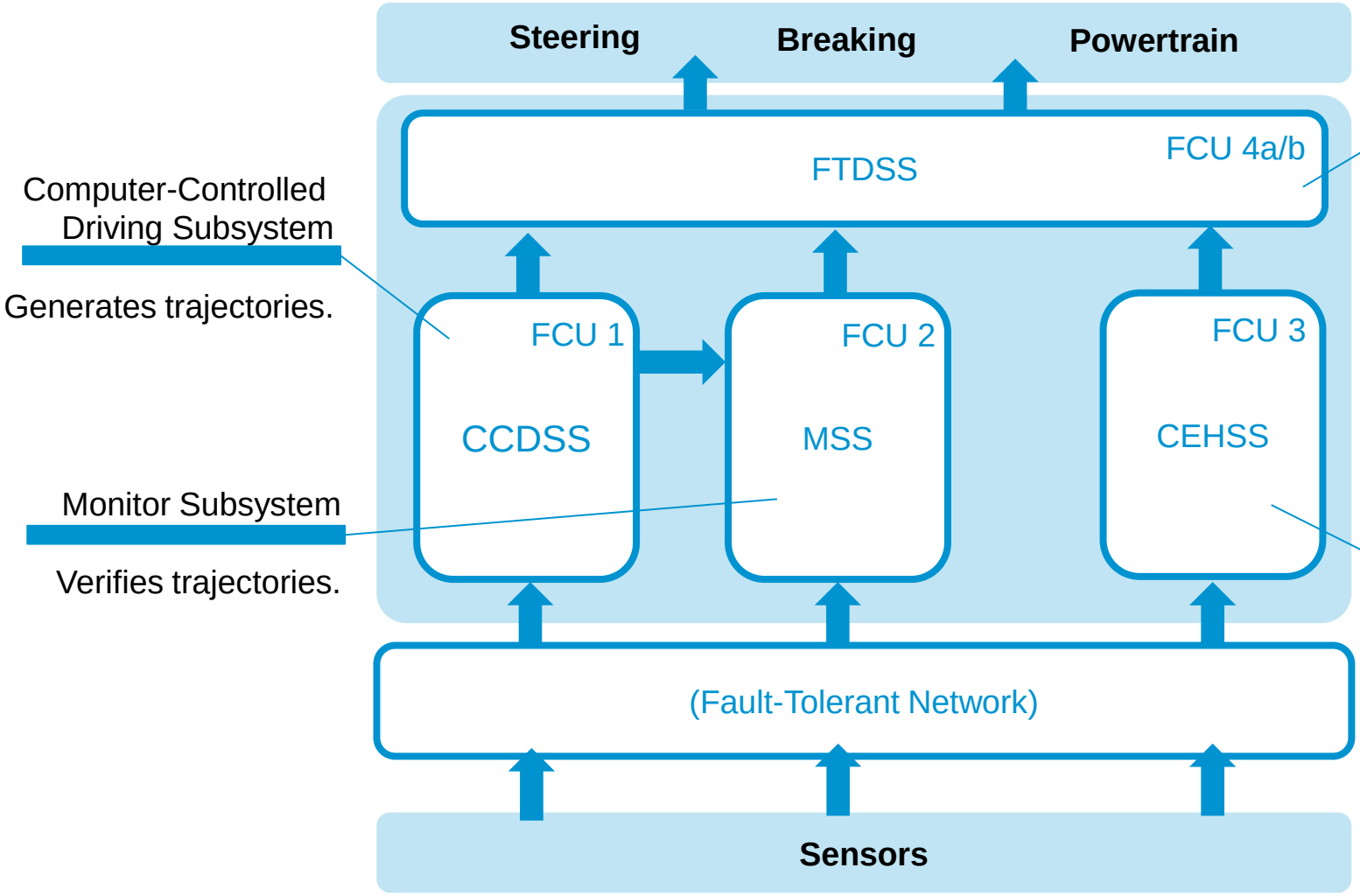
Moving from Level 2 to Level 4 System





Conceptual Architecture for Safe Autonomous Systems

Kopetz, H. (2021). *An Architecture for Driving Automation*.
URL: https://www.the-autonomous.com/news/an-architecture-for-driving-automation



Computer-Controlled Driving Subsystem

Generates trajectories.

Monitor Subsystem

Verifies trajectories.

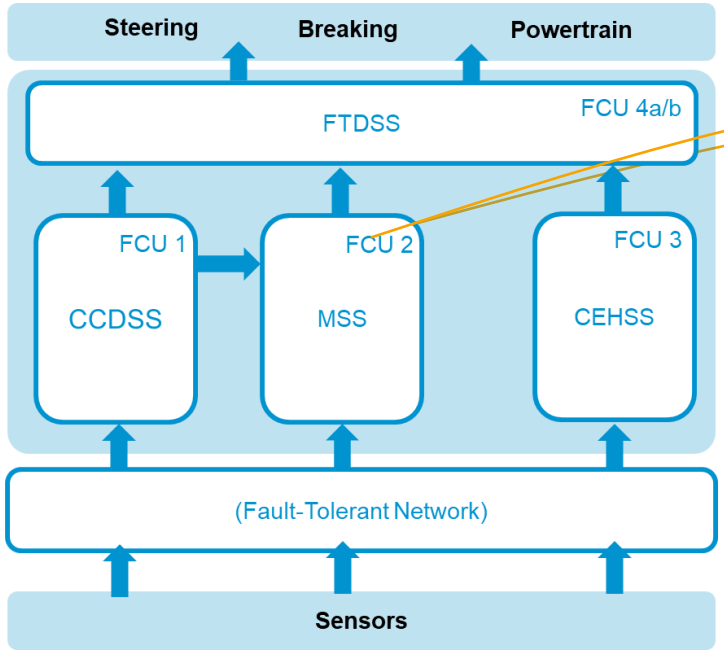
Fault-Tolerant Decision Subsystem

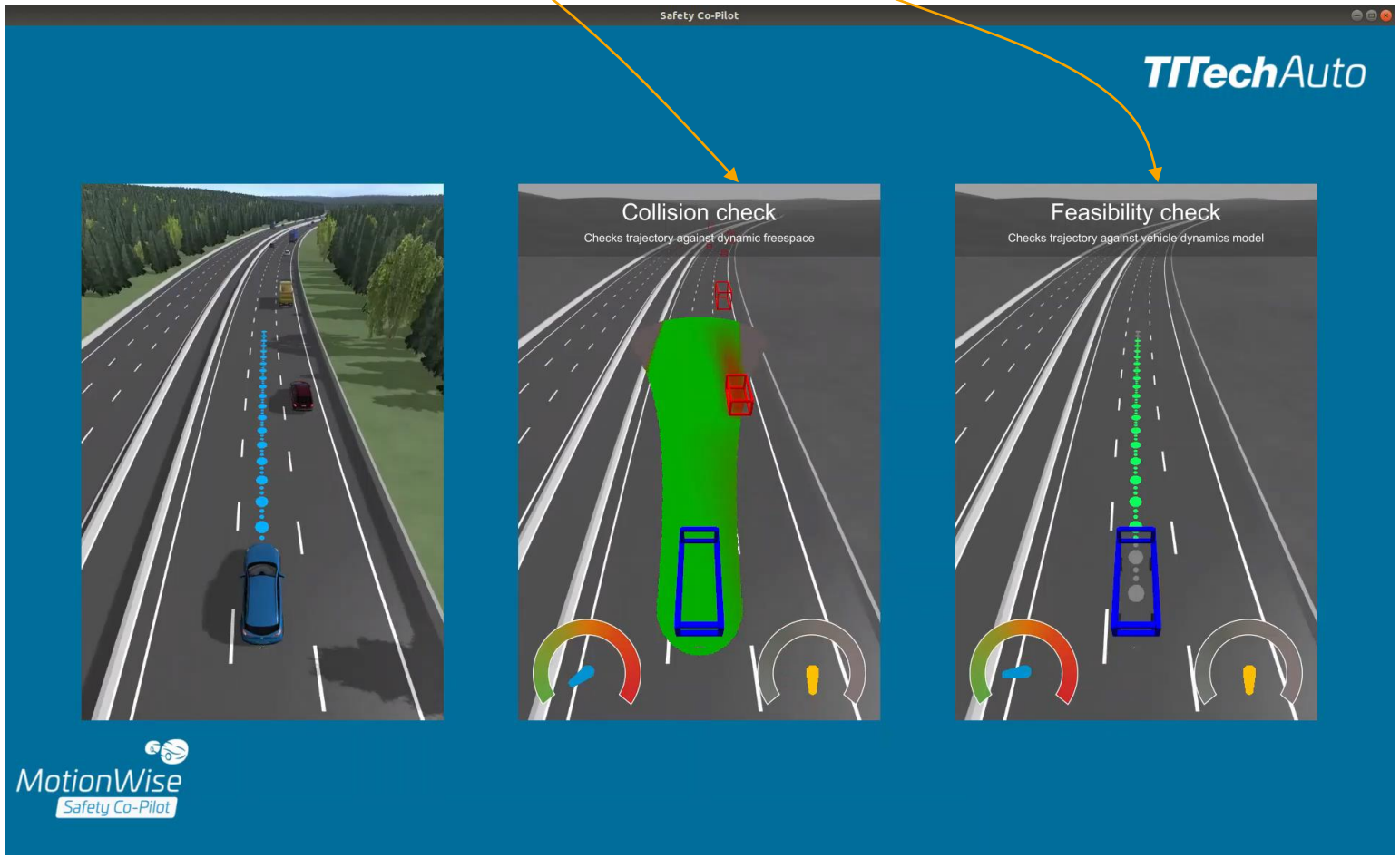
Decides whether the CCDSS or the CEHSS output is forwarded to the actuators.

Critical Event Handling Subsystem

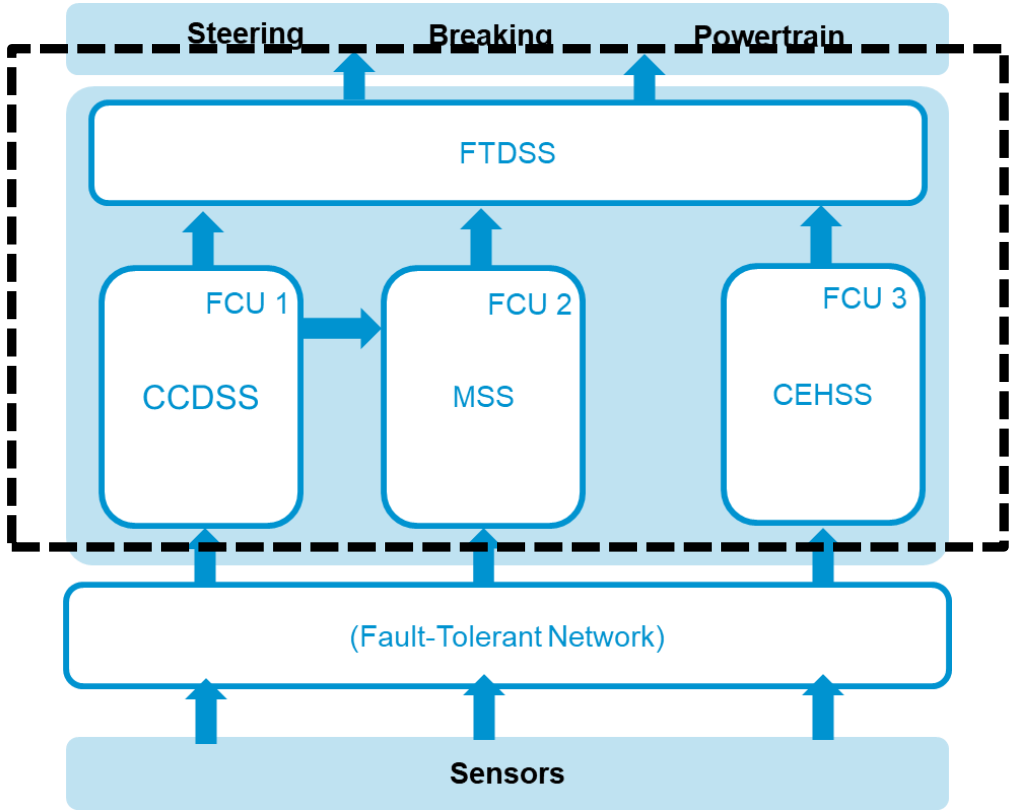
Generates trajectories including minimum risk maneuvers.
Designed to operate in any ODD.

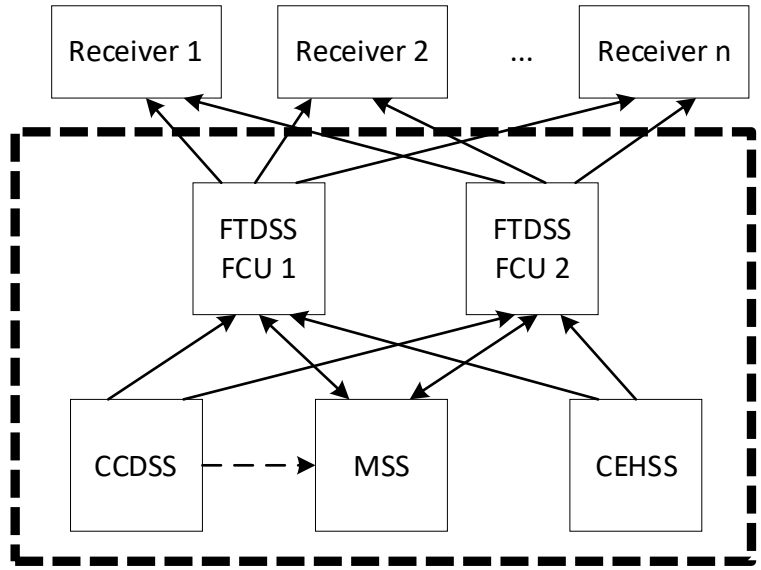
Monitor – Example Trajectory Verification Procedures





One more detailed level of abstraction



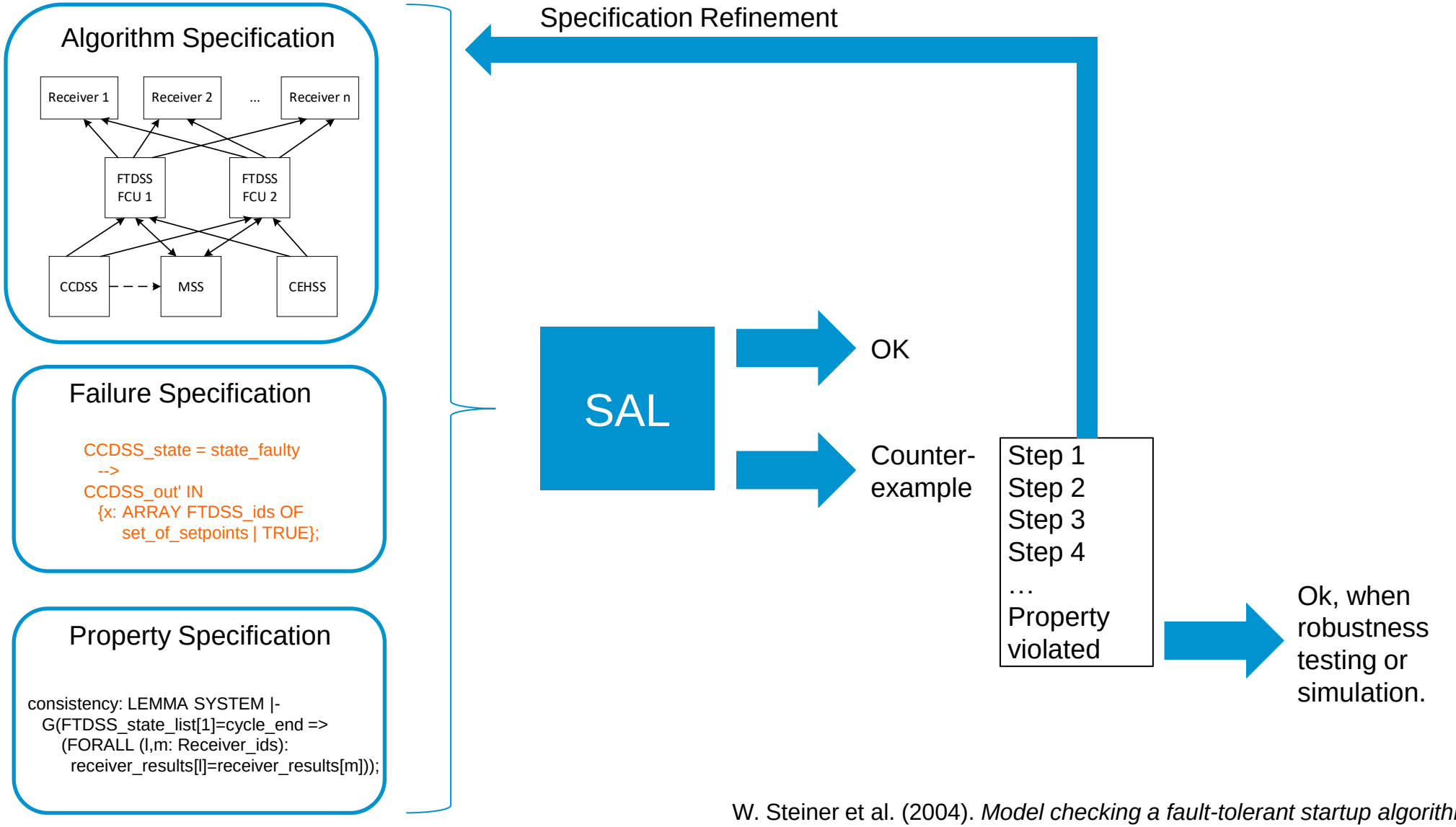


Hybrid failure assumption *
- FTDSS FCUs are simple FCUs and ~ fail silently
- CCDSS, MSS, CEHSS are complex FCUs and fail arbitrarily

* Verissimo, P. et al. (2003). *Intrusion-tolerant architectures: Concepts and design*. In Architecting dependable systems (pp. 3-36). Springer, Berlin, Heidelberg.

Exhaustive Fault Simulation (Qualitative Study)

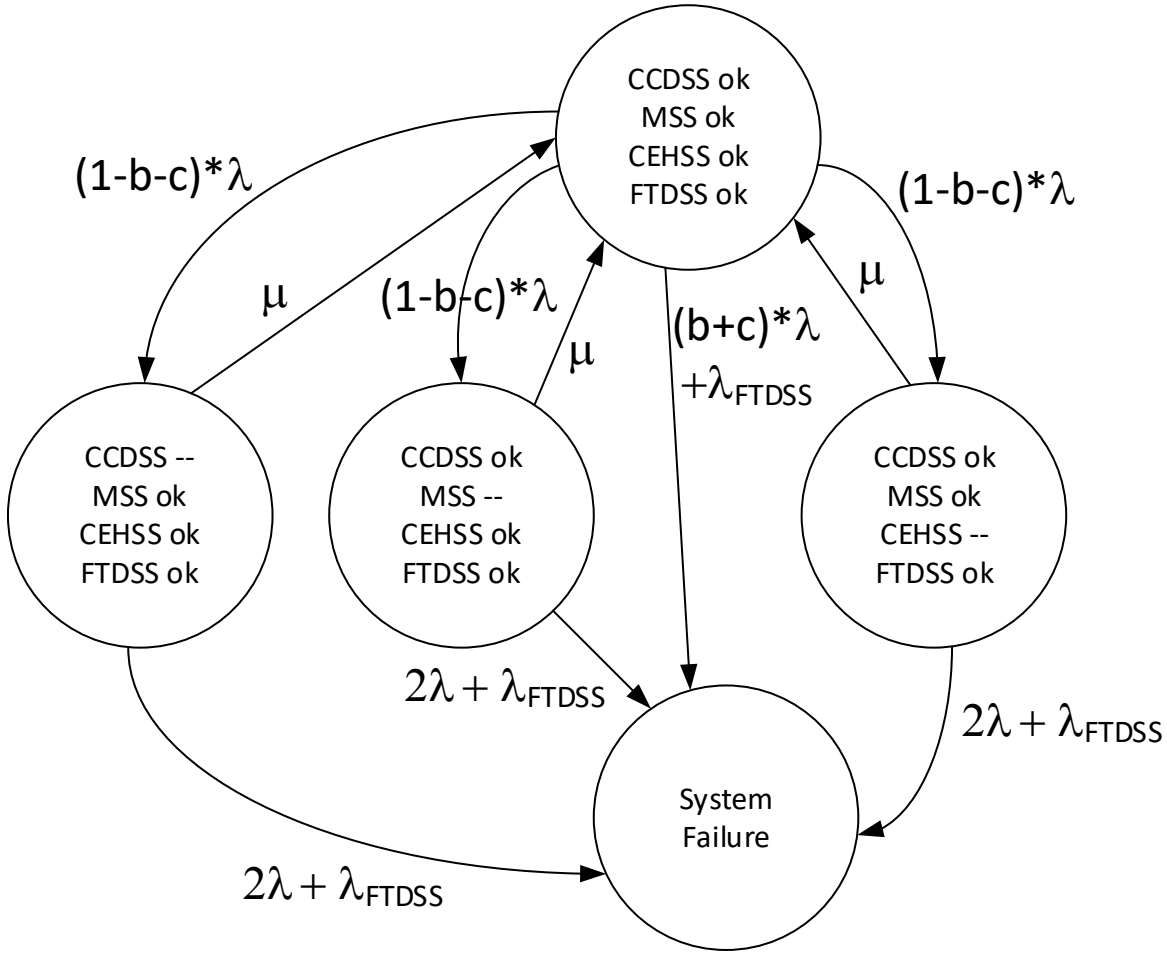
TTTech



W. Steiner et al. (2004). *Model checking a fault-tolerant startup algorithm: From design exploration to exhaustive fault simulation*. Proc. of the International Conference on Dependable Systems and Networks. IEEE. pp. 189-198.

Formalization of Assumptions in PRISM (Quantitative Study)

TTTechAuto



Kopetz, H. (2021). *An Architecture for Driving Automation*. URL: https://www.the-autonomous.com/news/an-architecture-for-driving-automation

Safety is the grand challenge to introduce Level 4 Automated Driving

TTTech

Perception and the “World Model”

Fail-Operational Safety Architecture

System Verification & Validation

System Verification and Validation

- “Classical” and more recent automotive standards
  - ISO 26262: Functional Safety
    - Automotive Safety Integrity Levels (ASIL)
  - ISO 21448: Safety Of The Intended Functionality (SOTIF)
  - ANSI/UL 4600: Standard for Safety for the Evaluation of Autonomous Products
    - Includes also anomaly detection, called “Safety Performance Indicators”
- Big Loop, e.g., https://www.youtube.com/watch?v=2Acx6W5Totg
- Street testing-only seems implausible
  - Kalra, N. & S.M. Paddock. (2016). *Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?.* Transportation Research Part A: Policy and Practice 94 (2016): 182-193.
- Composable V&V would be ideal: system V&V follows from independent subsystem V&V
  - How can common mode failures of the different subsystems be addressed?
  - Terrosi, F., L. Strigini, & A. Bondavalli. *Impact of machine learning on safety monitors.* In International Conference on Computer Safety, Reliability, and Security, pp. 129-143. Springer.

Conclusion

Conclusion

- Self-driving cars are the future of automotive mobility.
- Making them safe still is a challenge.
- Three safety challenges:
  - Perception and the “World Model”
  - Fail-Operational Safety Architecture
  - System Verification & Validation
- Three safety challenges are not independent.
  - How many world models are necessary?
  - Big loop validation has an impact on world model and the fail-operational safety architecture (which FCUs must connected to the cloud, which ones must be isolated?)

References:

- Kopetz, H. & W. Steiner. (2022). *Real-Time Systems: Design Principles for Distributed Embedded Applications*. 3rd Edition. Springer.
- Rushby, J. (2022). *Models and their Validation and their Role in Perception and in Safe Autonomous Vehicles*. IFIP WG10.4 Virtual Meeting. URL: http://www.csl.sri.com/users/rushby/abstracts/ifip-11may22
- Jah, S., J. Rushby, & N. Shankar. (2020). *Model-Centered Assurance for Autonomous Systems*. In International Conference on Computer Safety, Reliability, and Security, pp. 228-243. Springer.
- Kopetz, H. (2021). *An Architecture for Driving Automation*. URL: https://www.the-autonomous.com/news/an-architecture-for-driving-automation
- Miner, P.S., M. Malekpour & W. Torres (2002). *A Conceptual Design for a Reliable Optical Bus (ROBUS).* Proc. of the 21st Digital Avionics Systems Conference. IEEE press. (pp 13D3–13D3).
- Verissimo, P. et al. (2003). *Intrusion-tolerant architectures: Concepts and design*. In Architecting dependable systems (pp. 3-36). Springer, Berlin, Heidelberg.
- W. Steiner et al. (2004). *Model checking a fault-tolerant startup algorithm: From design exploration to exhaustive fault simulation*. Proc. of the International Conference on Dependable Systems and Networks. IEEE. pp. 189-198.
- Kalra, N. & S.M. Paddock. (2016). *Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?*. Transportation Research Part A: Policy and Practice 94 (2016): 182-193.
- Terrosi, F., L. Strigini, & A. Bondavalli. (2022). *Impact of machine learning on safety monitors*. In International Conference on Computer Safety, Reliability, and Security, pp. 129-143. Springer.
- SAL https://sal.csl.sri.com/ PRISM https://www.prismmodelchecker.org/

Meet us outside at our booth!

Contact us

VIENNA, AUSTRIA
(HEADQUARTERS)

+43 1 585 34 34-0
office@tttech.com

JAPAN

+81 52 485 5898
office@tttech.jp

USA

+1 978 933 7979
usa@tttech.com

CHINA

+86 21 5015 2925-0
china@tttech.com

www.tttech.com