

Legal, regulatory and normative aspects and requirements

Udo Steininger, TÜV SÜD Rail GmbH

Scope of work

Regulatory and organizational aspects and requirements for scalable safeguarding and approval of external, distributed safety-critical driving functions are examined. The status quo and the state of the art are evaluated and the relevant regulatory and normative requirements are derived.

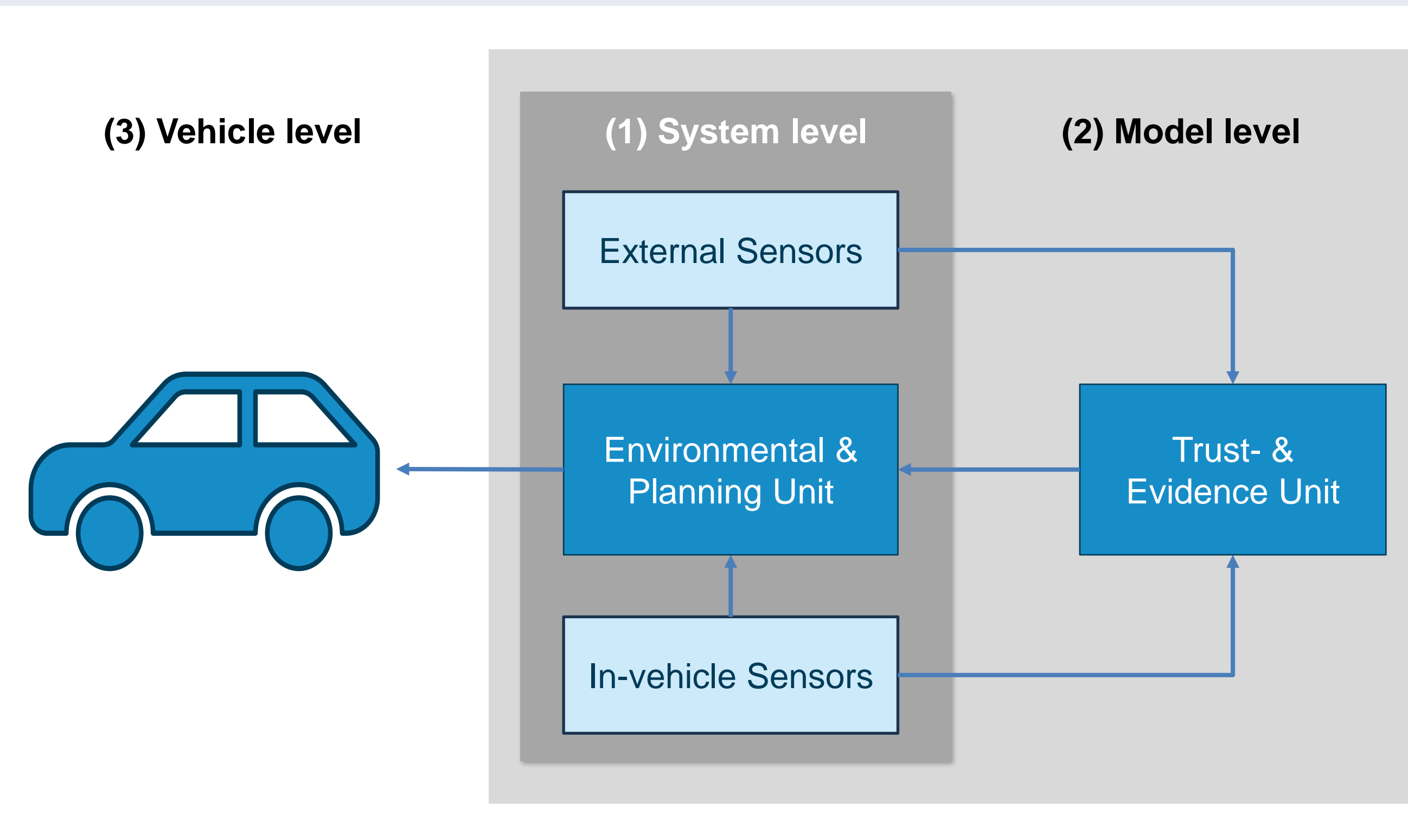
The current regulatory and normative framework is refined and new concepts and approaches for distributed safeguarding and approval are being evaluated.

For scalability, the safeguarding and approval process covers 3 levels, building on each other

- (1) "System level": Requirements for in-vehicle and external systems & V2X and resulting basic driving functions
- (2) "Model level": Requirements for evaluation of trust & evidence and resulting extended driving functions
- (3) "Vehicle level": Requirements for safe, resilient longitudinal and lateral vehicle control

Note: This is a specific nomenclature only for safeguarding and approval, other project partners use other designations and other / more detailed elements

Levels for scalable safeguarding & approval



Concept for scalable safeguarding & approval

General regulations

- UN-R155 (cyber-security), 156 (software updates) & 157 (ALKS)
- Implementing Regulation (EU) 2022/1426
- Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV)

Standards

- Regulations require - to varying degrees - compliance with
- ISO 26262 for functional safety,
 - ISO 21448 for the safety of the intended functionality (SOTIF) and
 - ISO/SAE 21434 for cyber security

Basic requirements

- Not to harm other road users or to endanger, obstruct or inconvenience them more than unavoidable (§30(1) StVZO)
- "Safety and ease" of traffic (AFGBV), "dependability" (ISO TR 4804 - voluntary)
- Scale: Human driver → positive risk balance and avoidance of unreasonable risks

(1) Integration of external systems & V2X

- AFGBV, Annex 1, clause 6: Transmission and processing of data from external technical units for autonomous management of the driving task in autonomous operation
- Implementing Regulation (EU) 2022/1426, Annex 1, point 17.2.1.2: External functions relevant to the ADS safety concept
- UN-R155 and 156: Manufacturers' obligations regarding cybersecurity and OTA updates

It could be demonstrated exemplarily which data from external sensors are required and which protocols and rules are needed for V2X → safeguarding & approval on system level ✓

(2) Integration of trust & evidence

- UN Regulation No. 157, Annex 4, Section 3.4, Manufacturer's safety concept, provides for "fallback to a subsystem" with resulting functional restrictions
- Analogously in Implementing Regulation (EU) 2022/1426)

Extended system architecture

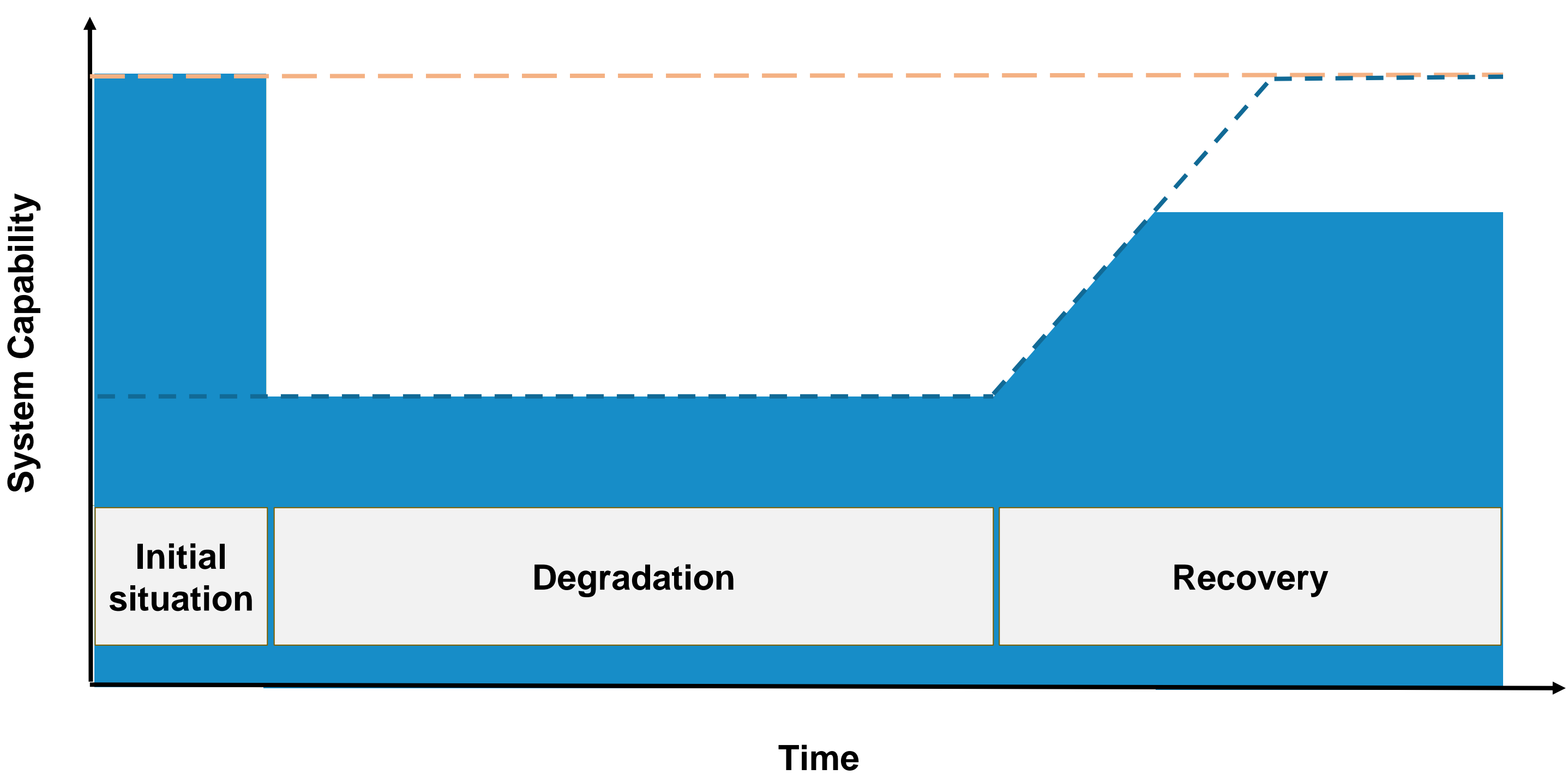
- offers extended driving functions and higher reliability if data from external systems is available and sufficiently trusted
- falls back to basic driving functions if there is a lack of or insufficient trust in this data

It could be demonstrated exemplarily how trust and evidence in data from in-vehicle and external sensors are evaluated → safeguarding & approval on model level ✓

(3) Integration of longitudinal & lateral vehicle control (capability of driving functions)

- Prerequisite: Description & evaluation of system capability depending on trust & evidence
- Easy for min. or max. capability, i.e., basic or extended driving functions
- Challenge: Description & evaluation of system capability during degradation & recovery
- Solution: Controllable degree of complexity of degraded & recovered system capability & resulting driving functions

It could be demonstrated exemplarily what effects trust & evidence evaluation has on the capability of driving functions → safeguarding & approval on vehicle level ✓



(1) Safeguarding and approval of external, distributed safety-critical driving functions fundamentally possible with available regulation and standards

(2) Helpful for practical implementation:

- Joint "model procedures" with applicants, authorities & technical services
- Procedural certainty through common guideline