With funding from the:

Federal Ministry
of Research, Technology
and Space

ConnRAD – Connectivity and Resilience for Automated Driving

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany

Final Presentation 23.10.2025

Safety Analysis and Results (UC1 & 3)

Peter Engel & Alexander Geraldy, Robert Bosch GmbH (CR/APC2)

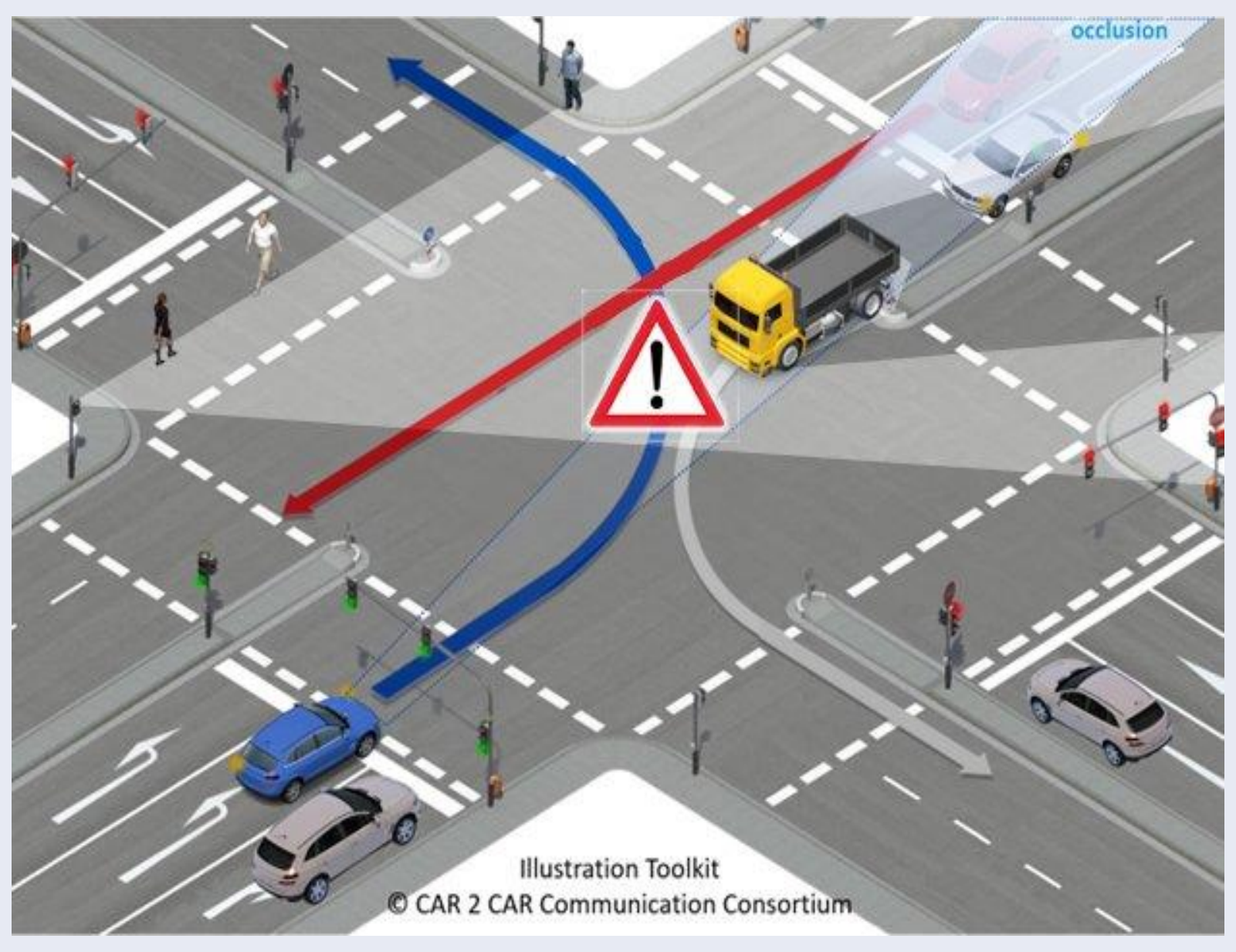
Goals

- Enable safe driving functions among diverse dynamic subsystems of a distributed V2X system,
- assuming that the collaboration partner does not a-priori fulfill all assumptions & requirements,
- assuming that specifying all requirements for one function in rigid standards is not the ideal solution.

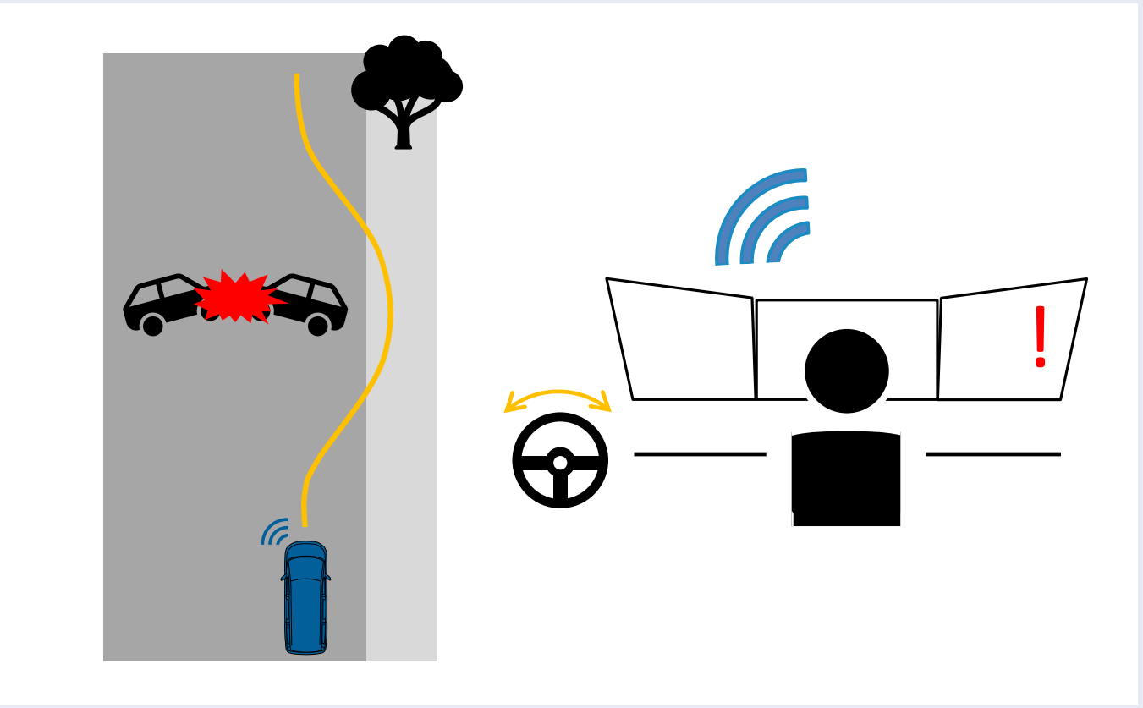
- Identify the challenges and possible gaps of a dynamic, distributed V2X system
- Shine a light on solution methods to be applied
  - to identify unmatched requirements at runtime,
  - to adapt dynamically and safely to the options given by surrounding V2X partners
- To derive possibilities for a independent approval of one vehicle or infrastructure without limiting the set of possible V2X partners.

Use Cases

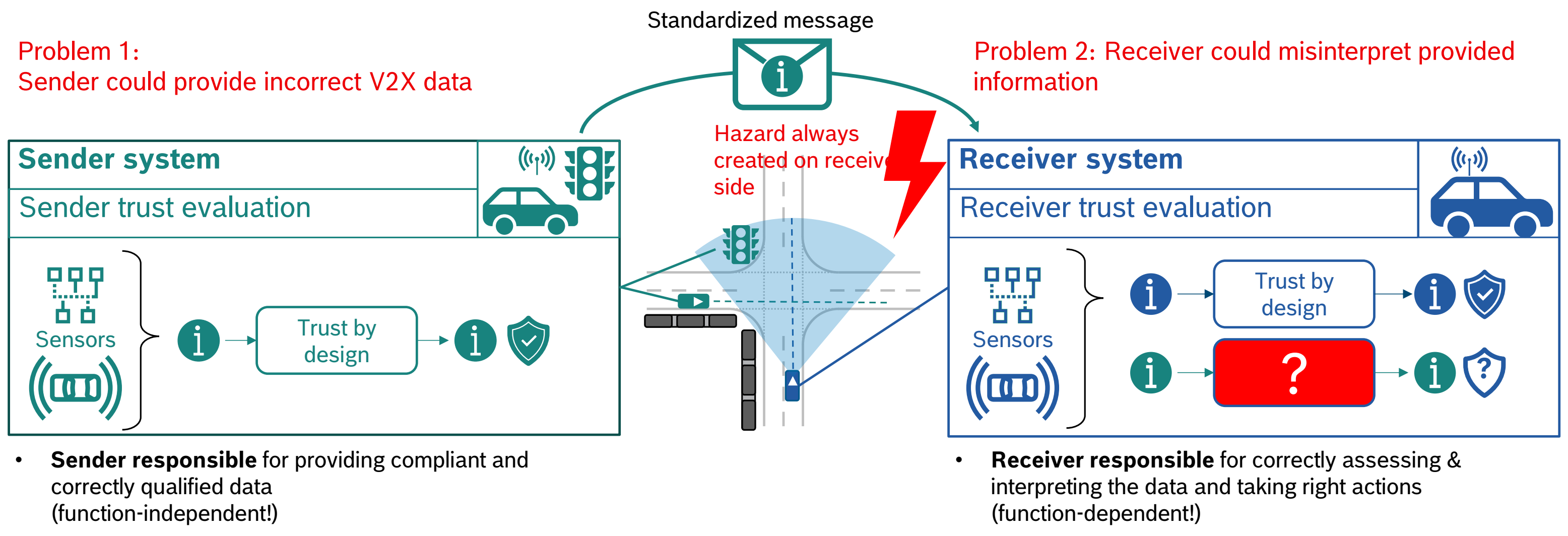
UC1 "Urban Intersection"



UC3 "Tele-operation"



Main Challenge



Standardized message

Problem 1:
Sender could provide incorrect V2X data

Problem 2: Receiver could misinterpret provided information

Hazard always created on receiver side

Sender system
Sender trust evaluation
Sensors
Trust by design

Receiver system
Receiver trust evaluation
Sensors
Trust by design
?

- **Sender responsible** for providing compliant and correctly qualified data (function-independent!)
- **Receiver responsible** for correctly assessing & interpreting the data and taking right actions (function-dependent!)

Safety Goals
- The sender shall not provide faulty information
- The receiver shall not misinterpret received information

Safety Goal 1: The sender shall not provide faulty information

- The sender must be **approved for delivery of correct meta data** to describe the payload
- The approval must be **certified** by 3rd party (e.g., TÜV) as trust anchor

Safety Goal 2: The receiver shall not misinterpret received information

- The receiver needs **meta data**, which describes the payload and **enables rating usability of information**
  → Quality of information
  → Service Specification containing
    – Capability of information generation
    – Qualification of safety assurance

Standardization
- Format and protocol of data exchange
- Interpretation rules of data

Safety Analysis Method

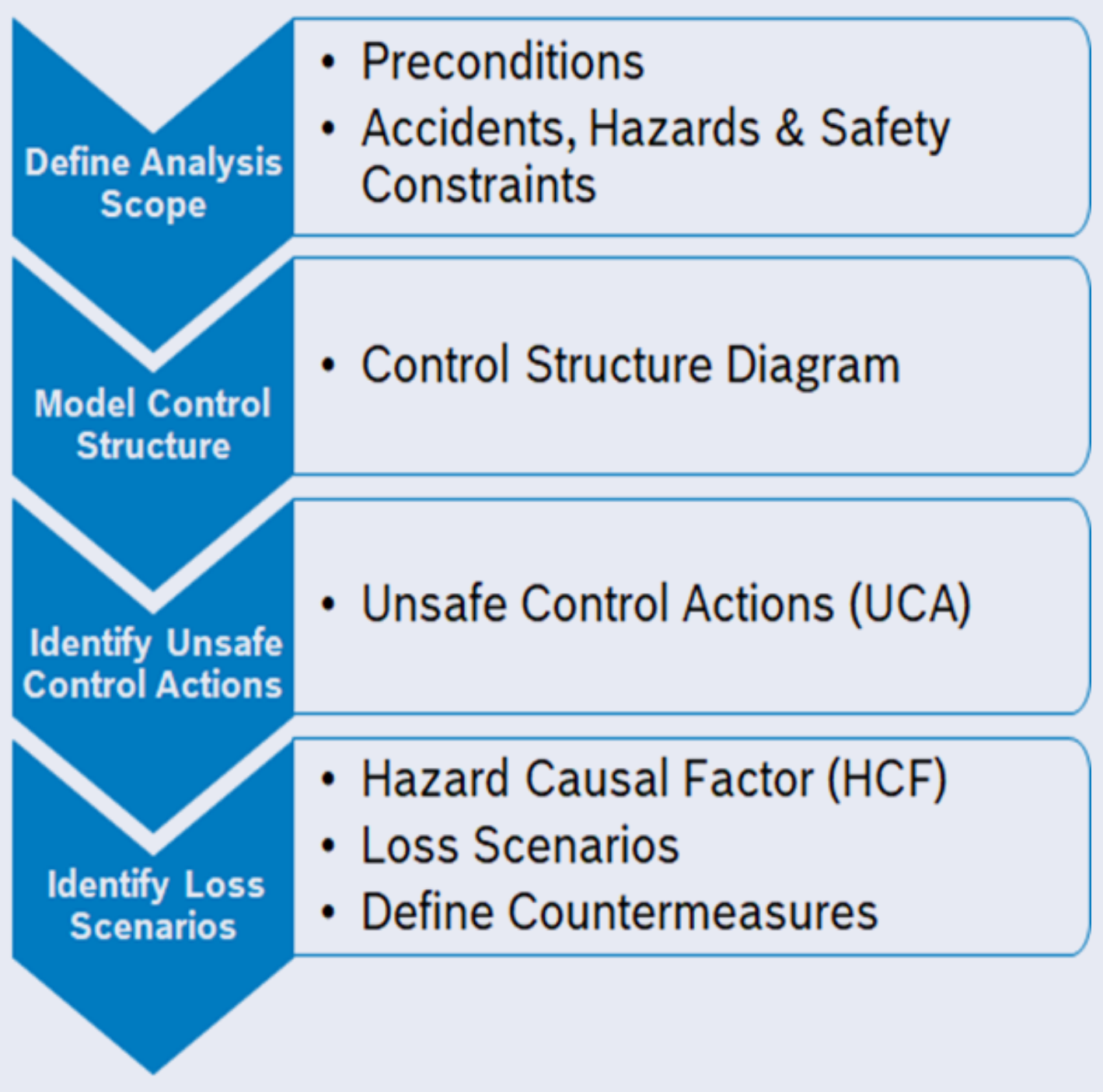
Approach

- Strong focus on **SOTIF***
  - Start with UC3 and use **STPA*** method
  - Gather experience with STPA
  - Learn about pitfalls and gaps
  - Transfer method and learnings to UC1

* SOTIF: Safety of the Intended Functionality (ISO 21448);
STPA: System-Theoretic Process Analysis

STPA Analysis Steps

1. Define purpose of analysis
   - "only" traditional safety goals or more broadly to security, privacy, performance, …
   - system boundaries
2. Build up model of system → control structure
   - relationships and interactions as feedback loops
3. Analysis of control actions
   - identify unsafe control actions (UCA)
4. Identify the reasons of UCA occurrence
   - causal scenario identification
   - define countermeasures



Define Analysis Scope
- Preconditions
- Accidents, Hazards & Safety Constraints

Model Control Structure
- Control Structure Diagram

Identify Unsafe Control Actions
- Unsafe Control Actions (UCA)

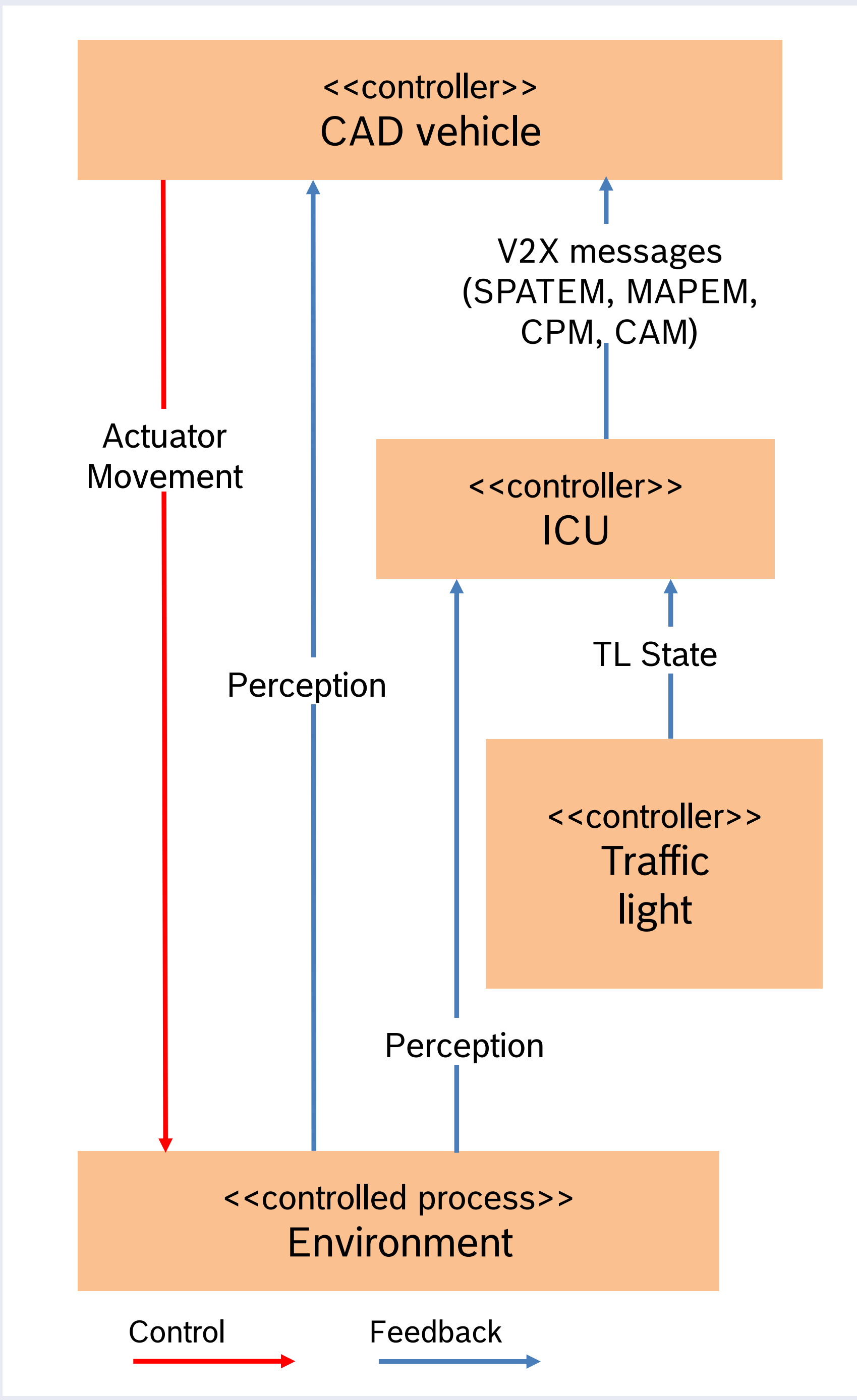
Identify Loss Scenarios
- Hazard Causal Factor (HCF)
- Loss Scenarios
- Define Countermeasures

Challenges

- Analyze SOTIF challenges in **distributed V2X** driving functions
  - Identify control model (control loops, components, controls)
  - Define Preconditions/Assumptions
  - Identify "Unsafe Control Actions (UCA)"
  - Identify "Hazard Causal Factors (HCF)"
  - Identify "Counter Measures (CM)"

Safety Analysis of UC3 &/ UC1: Control Model

UC1 "Urban Intersection"



<<controller>>
CAD vehicle

V2X messages (SPATEM, MAPEM, CPM, CAM)

Actuator Movement

<<controller>>
ICU

Perception

TL State

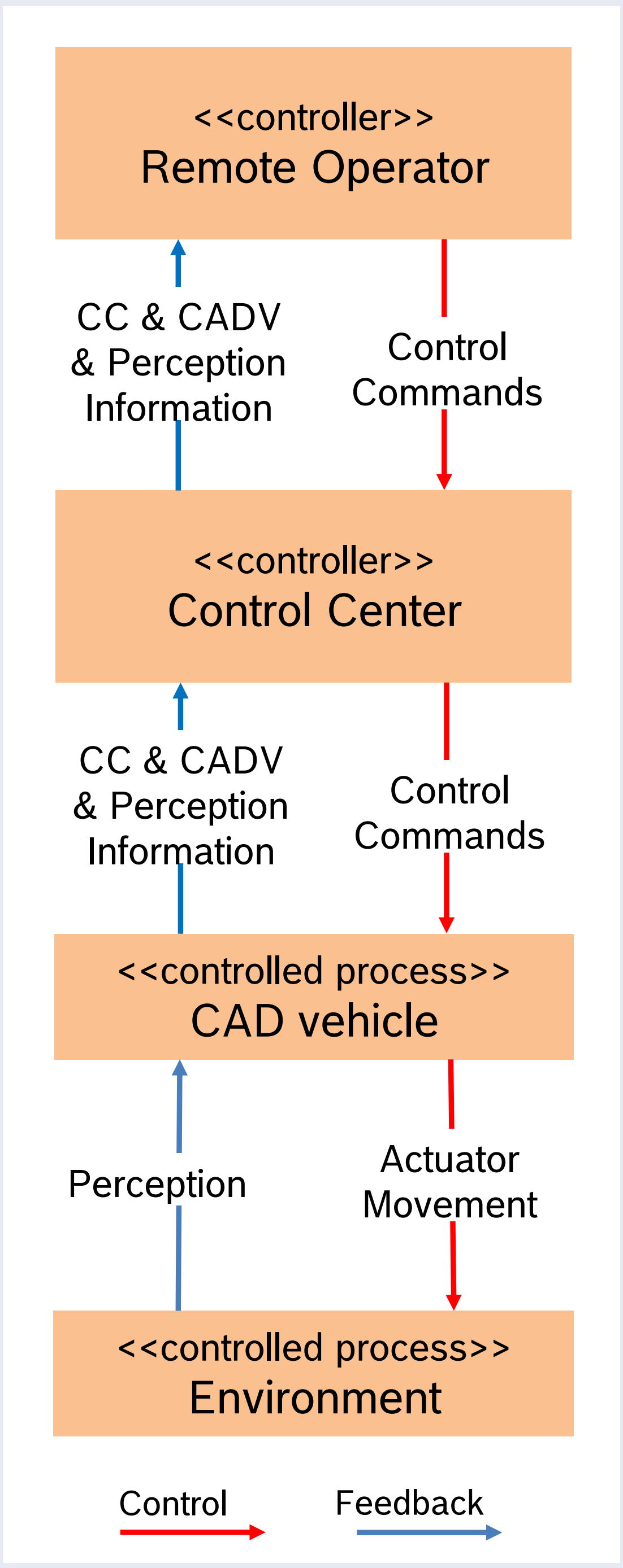
<<controller>>
Traffic light

Perception

<<controlled process>>
Environment

Control → Feedback →

UC3 "Tele-operation"



<<controller>>
Remote Operator

CC & CADV & Perception Information

Control Commands

<<controller>>
Control Center

CC & CADV & Perception Information

Control Commands

<<controlled process>>
CAD vehicle

Perception

Actuator Movement

<<controlled process>>
Environment

Control → Feedback →

General Safety Analysis Results

- **Completeness:** All objects in the announced perception area must be detected and transmitted by the infrastructure
- **Correct definition of perception area:** The infrastructure must transmit the current perception area to the vehicle
- **Consistency:** All data processed by infrastructure and vehicle must be consistent. Deviation must be detected and signaled to trigger needed actions (e.g. degradation, MRM)
- **Freshness:** The age of each data must be known (→ time synchronization & timestamps). Older data may be discarded or discounted in usability.

Required Countermeasures

- **Alignment of Safety Related Assumptions,** E.g., are passengers allowed inside the ToD vehicle?
- **Dynamic ODD / Ability Evaluation & Alignment:** under which condition are the CADV and the CC designed to drive?
- **Trust** in Env. Sensing & Remote-Control Commands: E.g., reflects the environment representation the reality and is not manipulated?
- **Clarification of responsibilities:** E.g., is the CADV or the RO responsible? → Exclusion of conflicting controls
- **Time synchronization:** E.g., what are the exact ages of message & measurements?
- **Map** correctness & alignment & evaluation: E.g., in which area ToD is allowed (under which constraints)?

BOSCH · [ˌdiːsɪ aɪˈtiː] Daimler Center for Automotive IT Innovations · Fraunhofer FOKUS · Fraunhofer IEM · htw saar Forschungsgruppe Verkehrstelematik · infineon · TUM Technische Universität München · TÜV SÜD · universität uulm