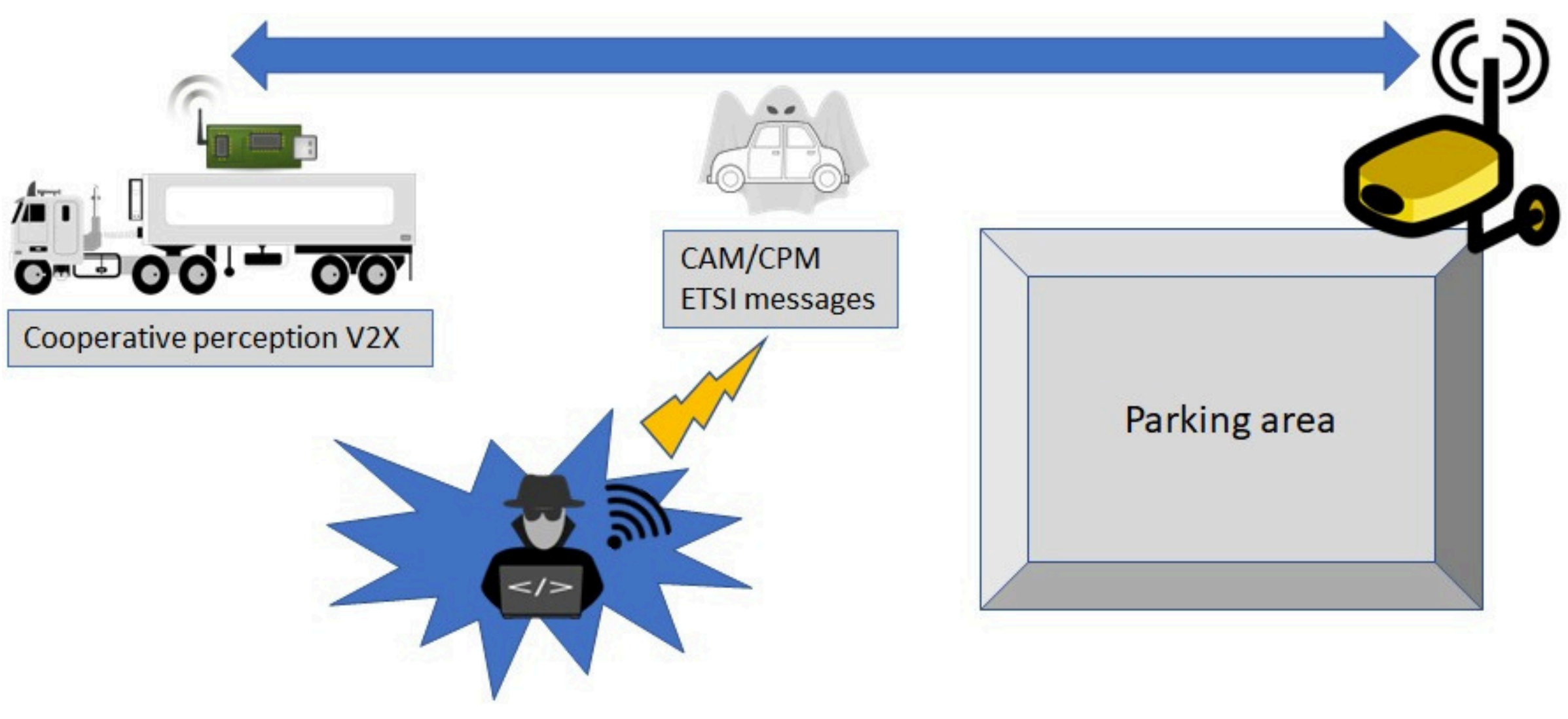
UC4.2 - TRUCK LOW-SPEED CONNECTED PERCEPTION CYBER-SECURITY

UC4 - FREIGHT VEHICLE AUTOMATED PARKING

SAFETY ASSURANCE FRAMEWORK FOR CONNECTED, AUTOMATED MOBILITY SYSTEMS

Anastasia Bolovinou

Use case overview



UC4.2 builds on top of the CCAM system of UC4.1 and the perception system of UC1.3, and deals with a connected perception AD subsystem that is compromised by cyber-security attacks.

Objectives

In virtual simulation, combine several aspects simultaneously (environment, perception, V2X connectivity, cyber-attacks) and study the effects of remotely executed cyber attacks on collective environment awareness.

SAF blocks demonstrated

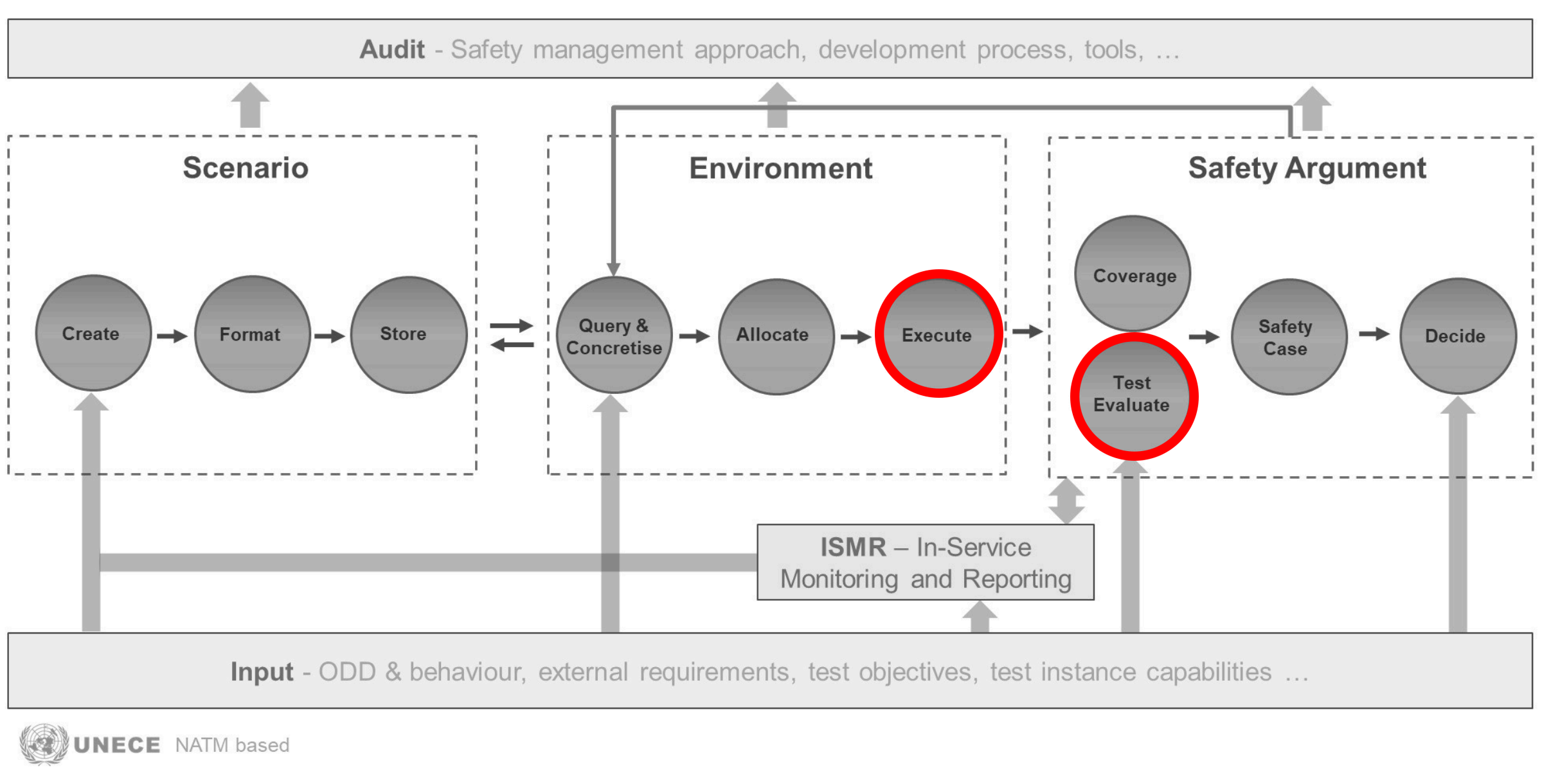


Figure 2. Overview of demonstrated SAF blocks

Test case setup

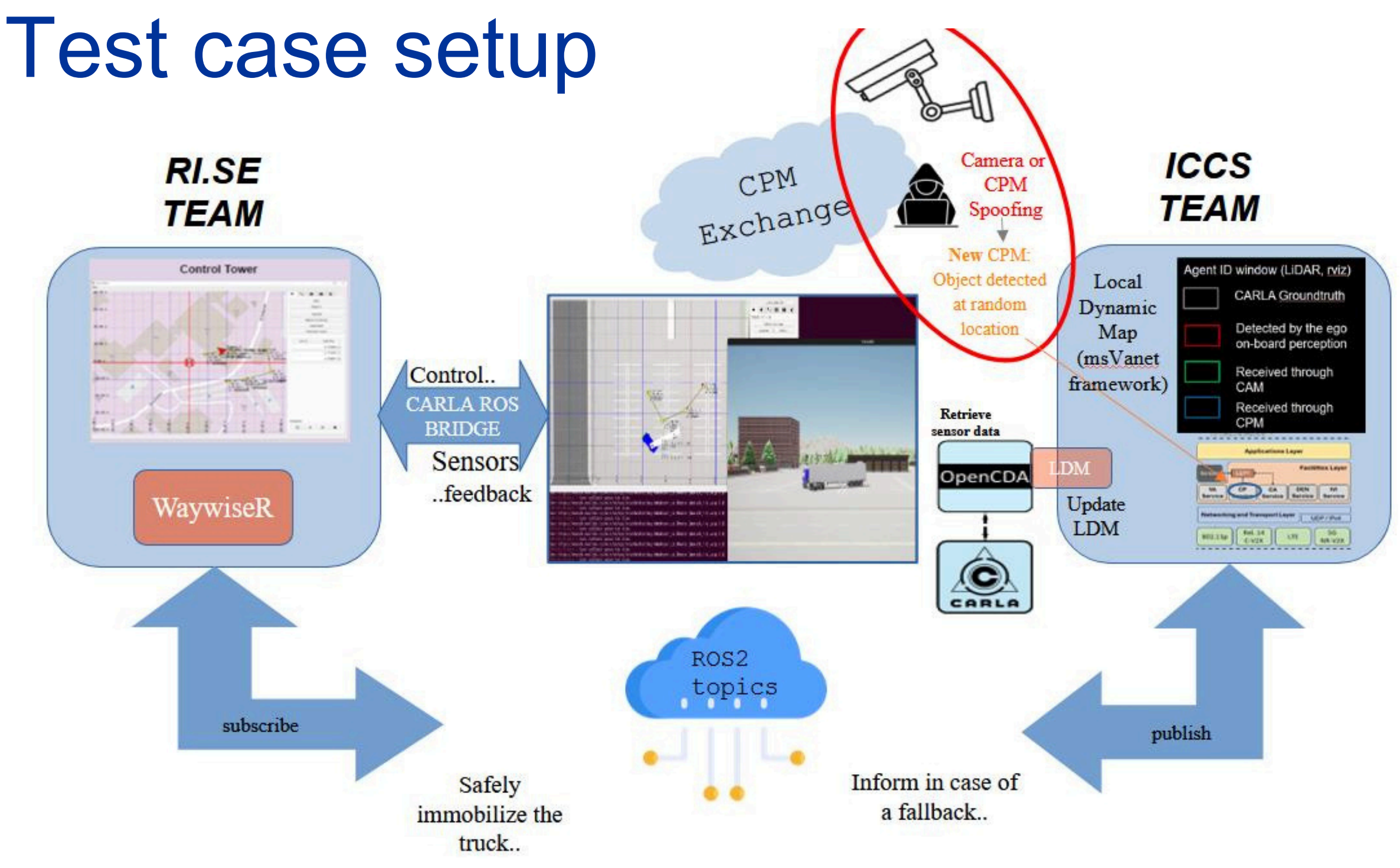


Figure 3. Test case setup

In UC4.2, two partners spoof the Road Side Unit (RSU) camera and falsify Cooperative Perception Messages (CPMs) while controlling a virtual truck in a parking manoeuvre in a CARLA simulation. A virtual camera-based RSU module is assumed to provide information about the scene through CPMs. Considered pass/fail criteria are similar to the truck parking system of UC4.1.

CCAM = Cooperative, Connected and Automated Mobility
ODD = Operational Design Domain
SAF = Safety Assurance Framework
UC = Use Case

Results

2 Flows of compromised emulated CPMs are implemented (Figure 4) and the truck controller reaction is evaluated:

- Custom camera sensor spoofing (exploiting light mechanisms inside CARLA simulator) to interfere with the quality of the raw sensor data.
- CPM falsification by introducing ghost objects inside a CPM generated by the infrastructure node and transmitted to the truck (falsifying position, speed or other object characteristics).

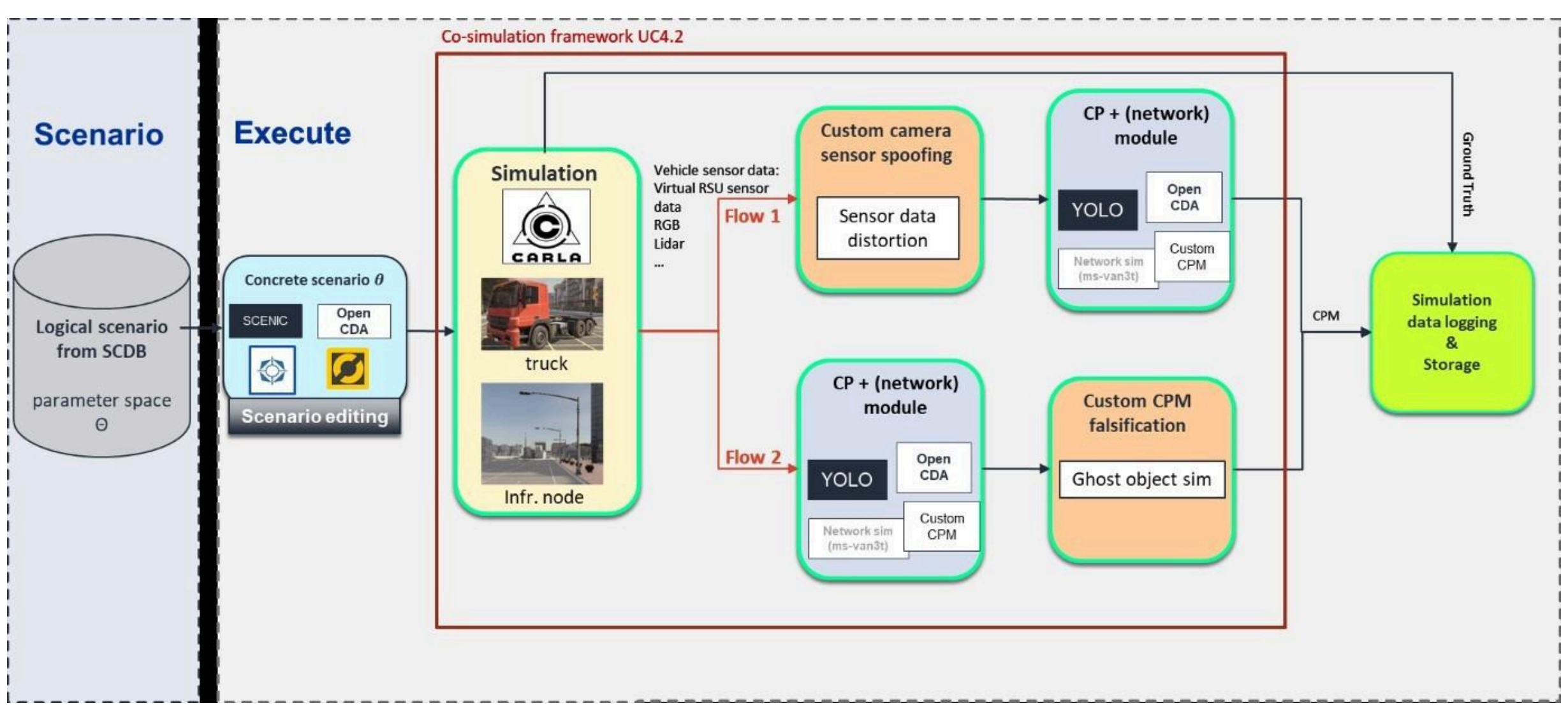
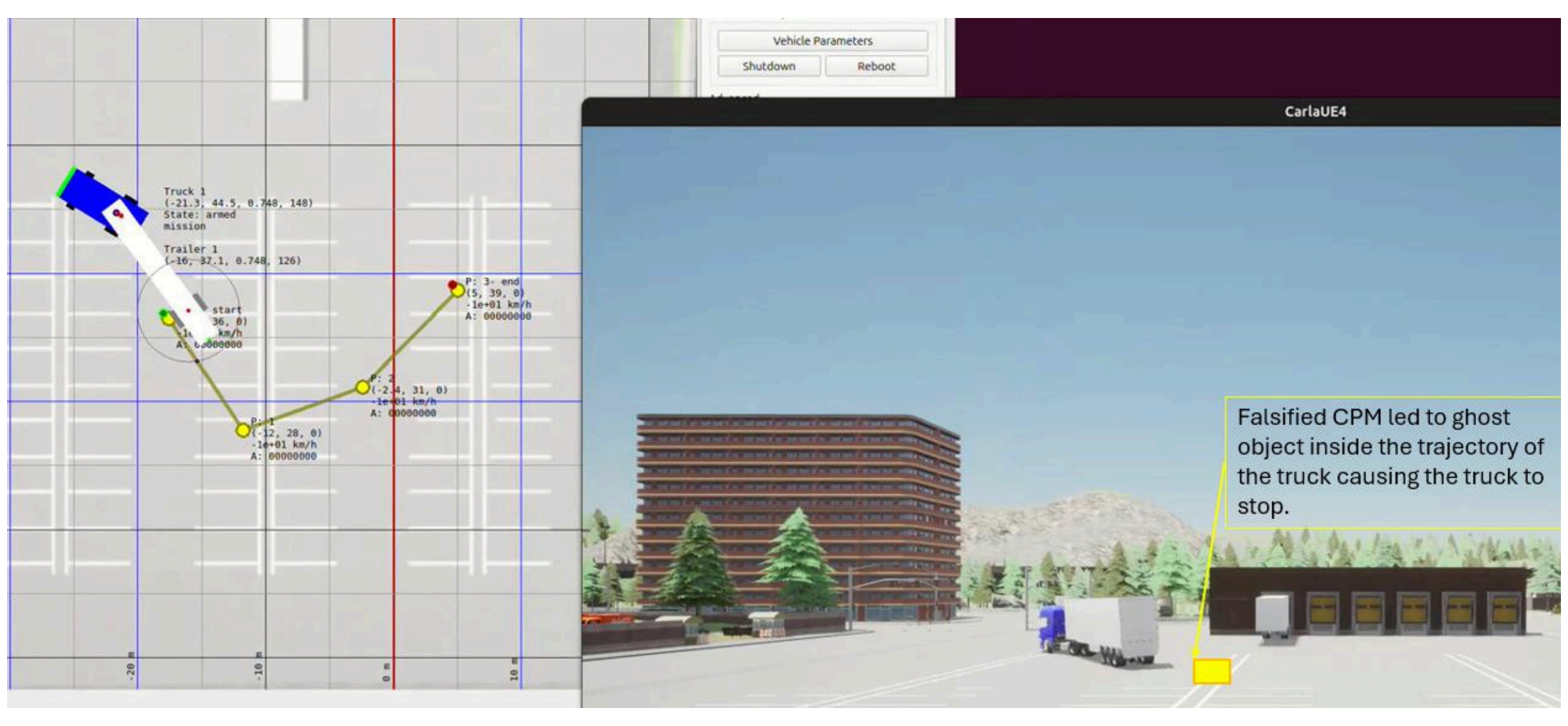


Figure 4. Co-simulation framework with 2 flows of compromised emulated CPMs



Falsified CPM led to ghost object inside the trajectory of the truck causing the truck to stop.

Figure 5. Snapshots from Carla and WayWise (ICCS, RISE collaboration)

Key take aways

SAF Execute block:

- New scenario execution mechanism to support cyber-attack triggering event.
- Co-simulation setup integrating virtual RSU and CPM spoofing in CARLA: [A] Custom camera sensor spoofing to interfere with quality of raw sensor data. [B] Ghost object spoofing on virtual scene.

SAF Test Evaluate block:

- Safety evaluation based on joint cyber-security and safety case requirements are designed based on ISO/SAE 21434 and ISO/TS 5083.

Future work

- Models for virtual camera attacks
- Methodology for modelling cyber-attacks on the NS3 environment (to integrate with CARLA via msvan3t).
- Dataset that can be used by other researchers to emulate CPM attacks.

References

- SUNRISE Deliverable D4.5

AD = Automated Driving
CPM = Cooperative Perception Message
RSU = Road Side Unit
V2X = Vehicle-to-Everything

Partners

For more information, please contact:

anastasia.bolovinou@iccs.gr

www.ccam-sunrise-project.eu

ccam-sunrise-project

The SUNRISE project is funded by
the European Union's Horizon Europe
Research & Innovation Actions
under grant agreement No. 101069573

Funded by
the European Union