VOLVO

EU Hi Drive 2nd Summer School

Cybersecurity Design for Collective Perception

Agenda

- Background and Intro – Collective Perception
- V2X – A new attack surface? New challenges and vulnerabilities to look out for!
- Intro to Risk assessment - ISO21434
- SP2 WP2.5 Enablers Work in EU Hi Drive
- How can Misbehavior Detection aid
- Bookmark of ongoing related work - Car2Car, ETSI activities, EU Hi Drive CoP
- Wrap up and Outlook

VOLVO

Collective Perception

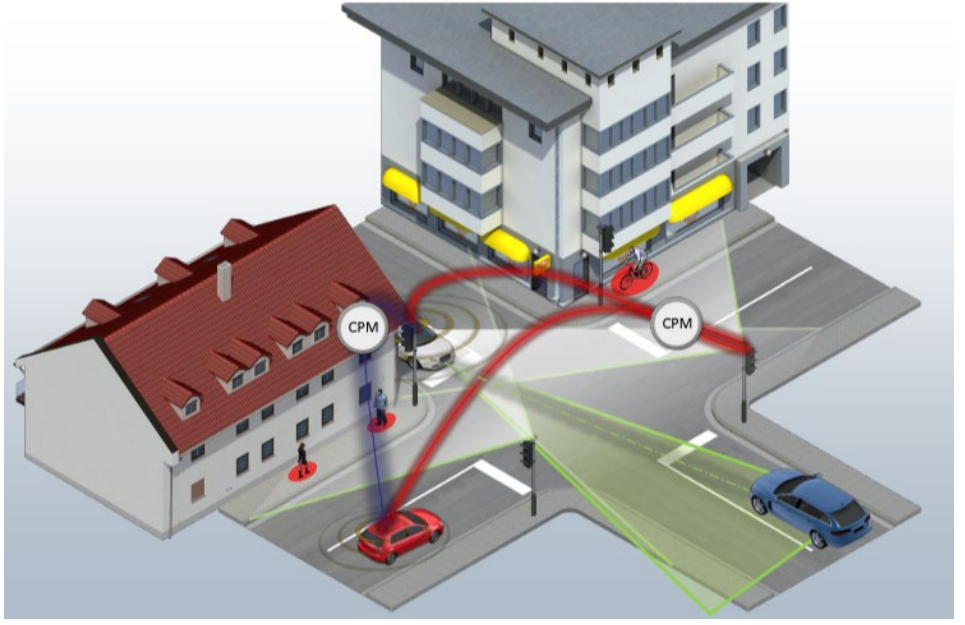
What is Collective Perception?

"Sharing the perceived environment of a station based on perception sensors."

Conceptually, it is actively exchanging locally perceived objects between different ITS-Stations via V2X, decreasing the uncertainty of its current surroundings.

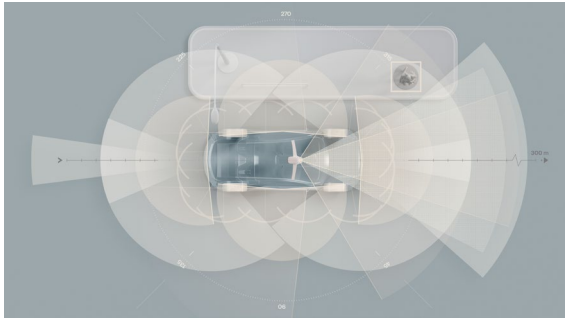
In-vehicular sensors and sensors mounted to infrastructure components can share information thereby enhancing the current ambient awareness.

ETSI Standardization on Collective Perception Service (CPS) ongoing TS 103 324



Source: Car2Car, 6th FG-AI4AD workshop AI for Good Global Summit; 2th June 2021

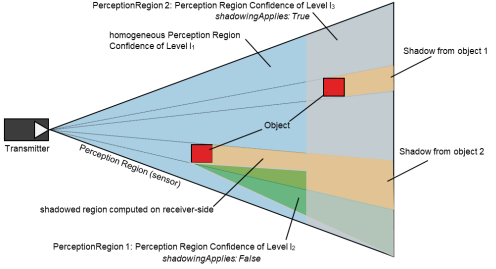
Leveraging the power of collective Perception



Enabling perception of the surroundings through seamless exchange of data and sensory information between multiple vehicles.

Tackle NLoS and Extend awareness range beyond LoS.

Share not only ego status, but also the other detected objects, confidence levels.
Capabilities to share the intentions and coordinate the maneuver.



Source: ETSI TS 103 324 V0.0.56 (2023-03)

Higher level of situational awareness – moving from reacting to responding

Collective Perception Message (CPM)

Purpose:

- Transmitted by ITS-S to share information about
  - Perceived objects (vehicles, pedestrians, animals)
  - Perception regions (unoccupied road areas)

Content of a CPM:

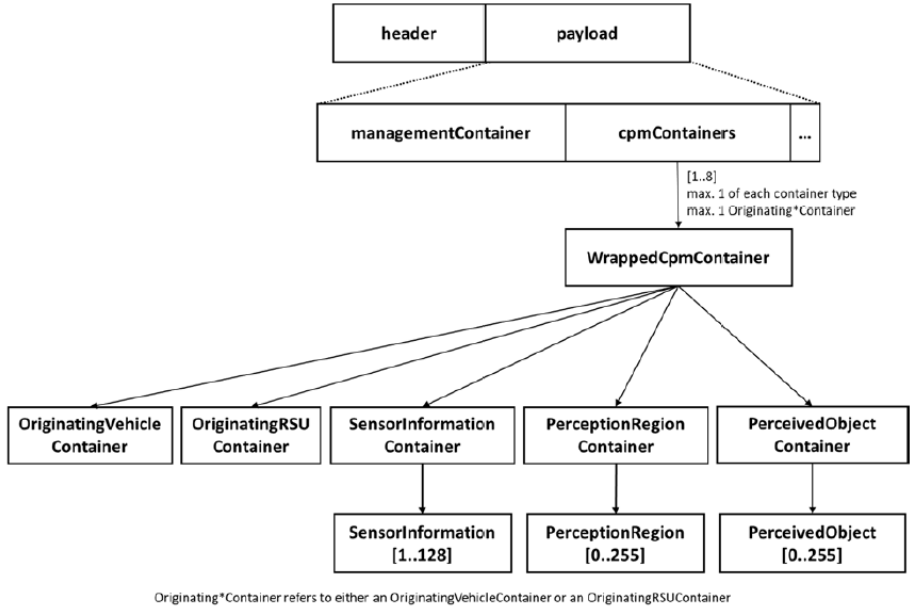
- Includes perceived objects and regions with their status and attributes.
- Status information typically includes detection time, position, and optional kinematic details.
- Senders can provide sensor information (types, fields of view) for better interpretation.

Impact on receiving ITS-Ss:

- Awareness of detected road users, objects, or regions.
- Supports applications that enhance safety and traffic efficiency, reducing travel time.
- Enhancement of Environmental Perception
  - Provides data on non-V2X-equipped road users and collision-relevant objects.
  - Increases information sources for V2X-equipped users.

Importance of CPS:

- Essential for various ITS safety and efficiency applications.
- Critical for deployments involving autonomous activities.



Source: ETSI TS 103 324 V0.0.56 (2023-03)

Challenges, Threats and Vulnerabilities; V2X, Another attack surface?

Potential cyber threats increases with increased connectivity, challenging manufacturers to ensure vehicle/fleet safety through robust cyber resilience.

Potential Threats and Attacks

Cyber Security Properties:

Data Integrity and Authenticity

Availability (of V2X unit)

Privacy and Confidentiality

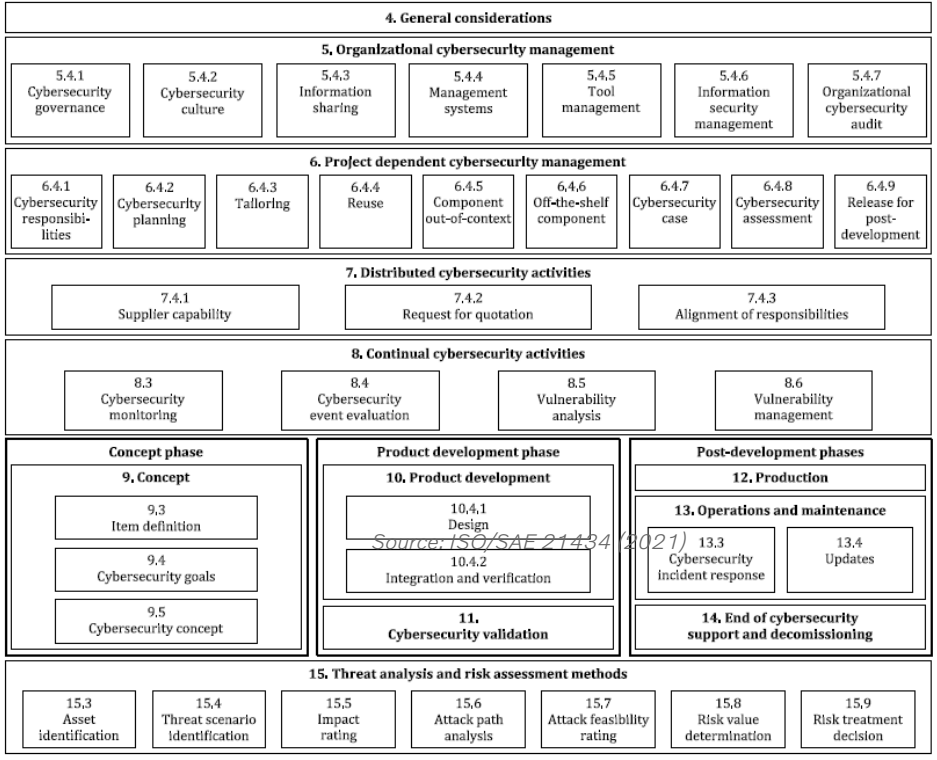
VOLVO

Cybersecurity Risk Assessment

ISO/SAE 21434 , UNECE R155

ISO/SAE 21434 and UNECE R155 – Cybersecurity assessments

- ISO/SAE 21434 specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.
- Is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.
- UNECE Regulation No. 155 focuses on cybersecurity and the management of cybersecurity risks in vehicles. It establishes requirements for manufacturers to ensure that their vehicles are secure against cyber threats throughout their lifecycle.
- Annex 5 – List of threats and corresponding mitigations

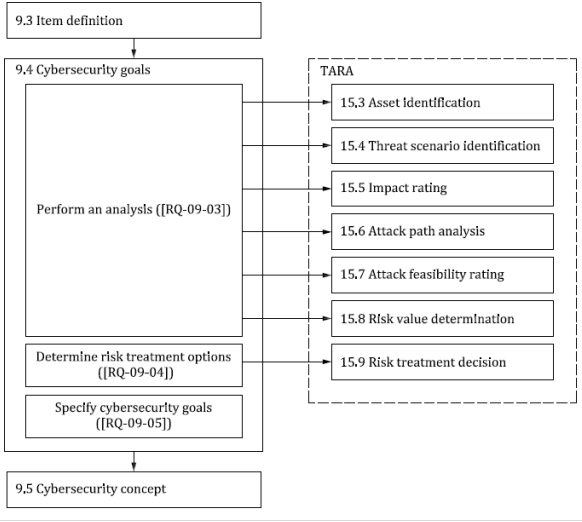


Source: ISO/SAE 21434 (2021)

Threat Analysis and Risk Assessment (TARA) Method

TARA is a modular approach/method for cybersecurity analysis of an automotive E/E system to determine the extent to which a road user can be impacted by a threat scenario.

Modules are generic and can be invoked systematically and from any point in the life cycle of the item/component.



Source: ISO/SAE 21434 (2021)

Asset Identification

- Identify assets, their cybersecurity properties and their damage scenarios;

Threat scenarios identification

- Identify threat scenarios

Impact Rating

- Determine the impact rating of damage scenarios

Attack Path Analysis

- Identify the attack paths that realize threat scenarios

Attack Feasibility Rating

- Determine the ease with which attack paths can be exploited

Risk Value Determination

- Determine the risk values of threat scenarios;

Risk treatment

- Select appropriate risk treatment options for threat scenarios.

VOLVO

EU Hi Drive – Cybersecurity Work

WP 2.5 Cybersecurity Enablers
Our approach and assessment so far

SP2 ENABLERS – WP2.5 Cybersecurity Work (ICCS, VCC, VTECH, Commsignia)

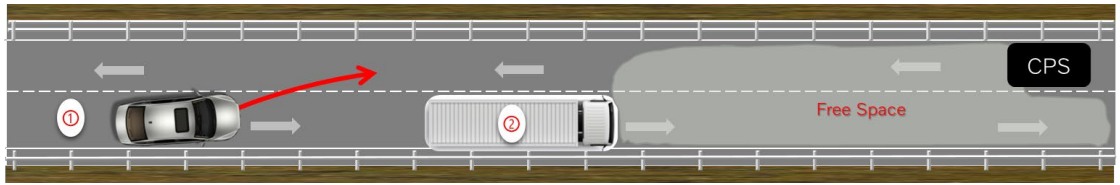
Enabler Scope: Perform the Risk assessment on V2X as an enabler for cooperative automation.

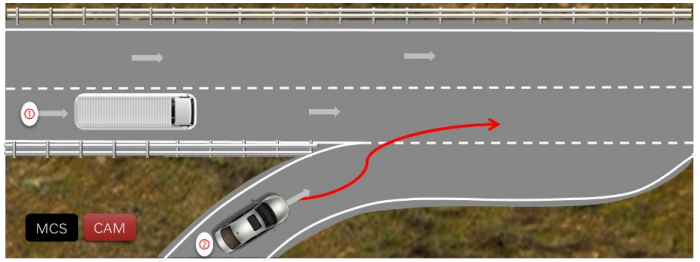
ToE – ITS G5 Unit in Vehicle

Approach: standardized risk analysis of ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering.

Use Cases: Cooperative Overtaking, Cooperative Road merging via V2X

V2X Messages considered: CAMs, CPMs, MCMs



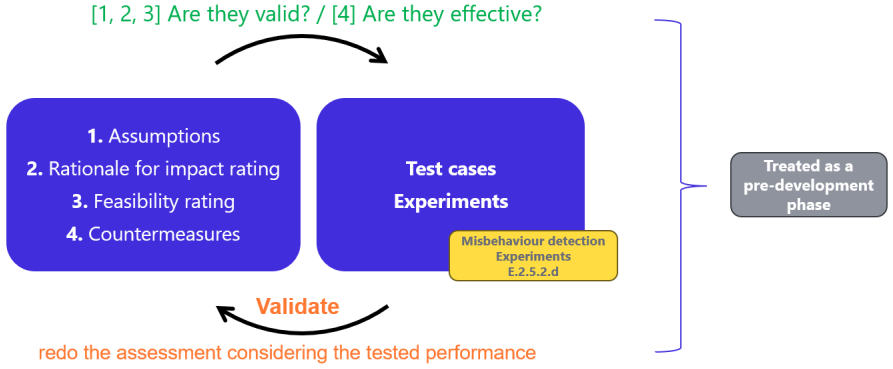


Our Approach

A unified in-vehicle architecture is introduced for carrying out the threat analysis. The architecture provides an abstracted way to model all required in-vehicle modules for C-ITS unit.

Systematically identify the expected damage and involved threats (e.g., spoofing, tampering, data leakage/manipulation etc.) potentially emerging from the usage of the CAMs, CPMs and MCMs

Provide cyber-security insights by exploring the threats and risks emerging in the Cooperative vehicle functionalities in Cooperative Automated vehicles (CAVs).



Assessment Outcomes & Observations – Examples

Asset: RVT Fusion

Message: CPM

			Impact Rating						
THREAT	**DAMAGE SCENARIO**	***Damage description***	**Safety**	**Financial**	**Operational**	**Privacy**	**Impact rating**	**Attack feasibility**	**Risk value**
Tampered information Combination of conflicting/non-consistent messages [on tracked objects data] without exact matching (CAM-CPM, MCM-CPM)	Vehicle deceived about the existence of a tracked object/open space [refers to the case of CPM being falsified]	The receiving vehicle is having a falsified view of the existence/non-existence of vehicles/objects	Major	Negligible	Negligible	Negligible	Major	Medium	3

Recommendation: “Share the risk along with in vehicle sw stack for decision making”, “Misbehavior reporting - Inconsistencies of the incoming message with the knowledge of the local environment of the ego vehicle/ Inconsistencies with on-board perception”

VOLVO

Detection, Prevention and Resilience

A “SECURITY CULTURE” IN THE ORGANIZATION!

BASIC SYSTEM PROFILE

STANDARDIZED PROTOCOLS FOR MESSAGE GENERATION

INTRUSION DETECTION SYSTEMS

SECURITY HARDENING

ENCRYPTIONS AND CERTIFICATES AND SERVICE SPECIFIC PERMISSIONS

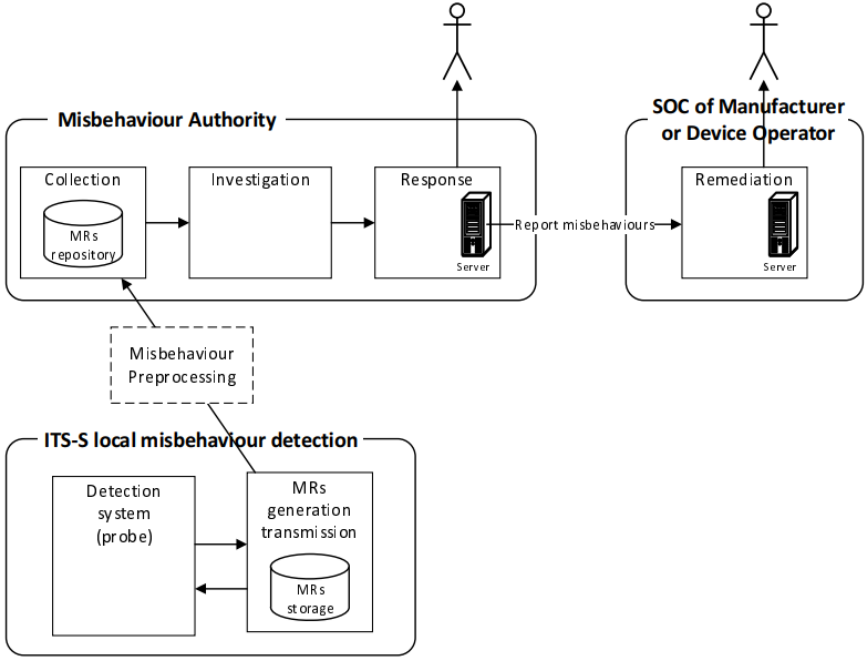
BEHAVIORAL ANALYSES AND COLLABORATIVE THREAT INTELLIGENCE

PLAUSIBILITY AND CONSISTENCY CHECKS

VOLVO

Misbehavior Detection Service

Misbehavior Detection Service - ETSI TS 103 759



Source: ETSI TS 103 759 V2.1.1 (2023-01)

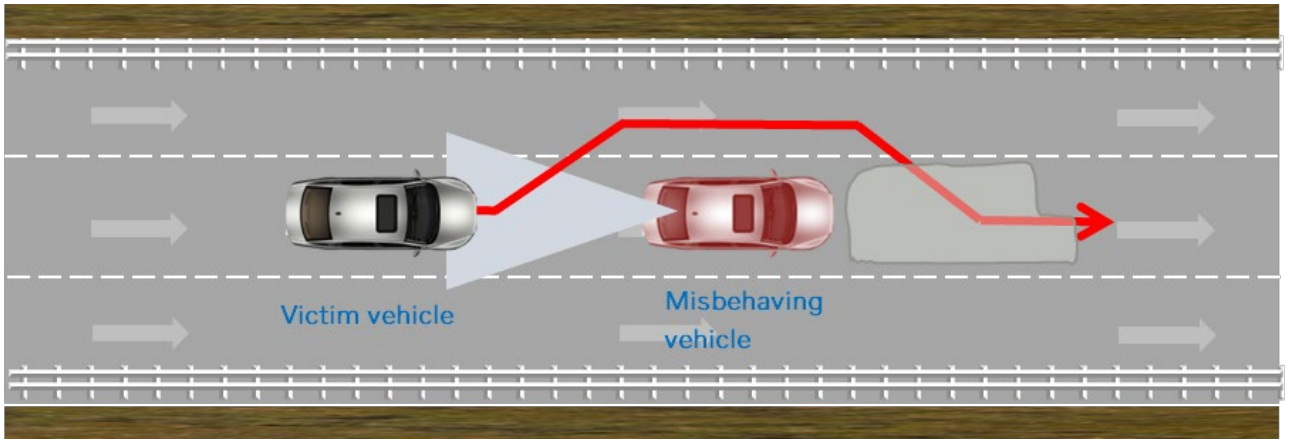
Misbehavior reporting is carried out in the context of the Misbehavior Detection Management (MDM) system.

Composed of local (part of the ITS-S) and backend subsystems.

ITS-S create Misbehavior Reports (MRs) and send them to the backend subsystem.

Backend subsystem evaluates what has happened and determines the appropriate response and remediation actions, if needed based on the information.

Misbehavior Detection Enabler in WP 2.5 – VCC, CMS Joint Testing



Use Case : Cooperative Overtaking

Misbehavior : Ego object not found in CPM

Actors: 2, CAV and Misbehaving Vehicle (MB)

Flow of Events:

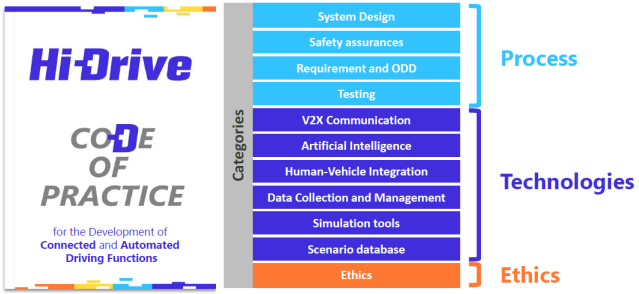
- Victim (CAV) vehicle tries to overtake MB vehicle
- Victim vehicle uses CPM from MB vehicle to gain awareness about surrounding objects
- Victim vehicle approaches the field of view of MB vehicle's sensors
- Victim vehicle cannot detect itself in MB vehicle's CPMs
- Victim vehicle stops the overtaking maneuver

VOLVO

Notable work to bookmark

Car2Car, ETSI - CPS Profiling, Security
EU Hi Drive CoP

A quick bookmark



Source: EU Hi Drive COP Webinar 17Feb2023

EU Hi Drive Code of Practice

A Web based implementation of the continued work from L3 pilot with added categories aiming to cover important elements identified by key contributors to the automotive industry intended for stimulating thought and providing recommendations for technologies that have not yet deployed int eh market or in early stages.

Car2Car

Going strong since its inception in 2002 with the objective of developing European standards for C-ITS. Few work times to keep an eye on:

- Use Cases,
- Basic System Profile, Protection Profile

ETSI

CPS – TS 103 324

Misbehavior Detection Service –TS 103 759

Functional Safety Analysis - TR 103 917

Final words and Outlook

Collective Perception expands the potential for a safe and reliable vehicular co operation on the roads and paves way for enabling connected and highly automated driving.

With this possibility also comes numerous challenges especially on having a reliable security by design as a prerequisite for effective adoption.

Several standardization efforts are ongoing to address and tackle some of these challenges.

Collective perception also brings out the question of trust worthiness of the information that is being shared which will drive another set of challenges to tackle from data fusion, safety and reliability.

Perhaps we are looking at Co engineering of Safety and security?

VOLVO

Thank you!