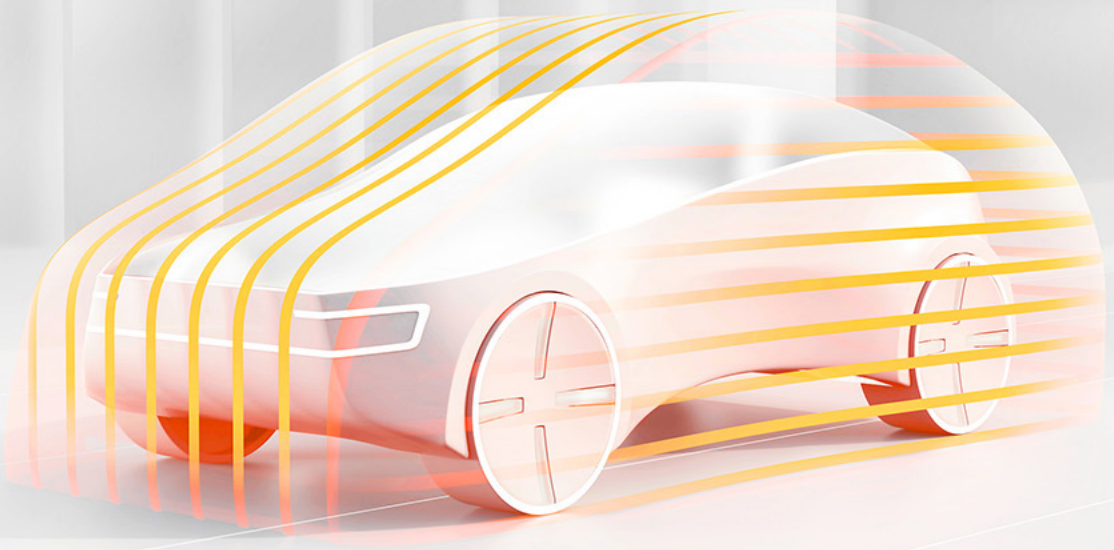
CONNECTED AND AUTOMATED VEHICLES

Cybersecurity Concerns for Cooperative Intelligent Transport Systems

October 2021



Gilad Bandel

VP Product and Marketing

Arilou Automotive Cybersecurity

Gilad.Bandel@nng.com

GENIVI®

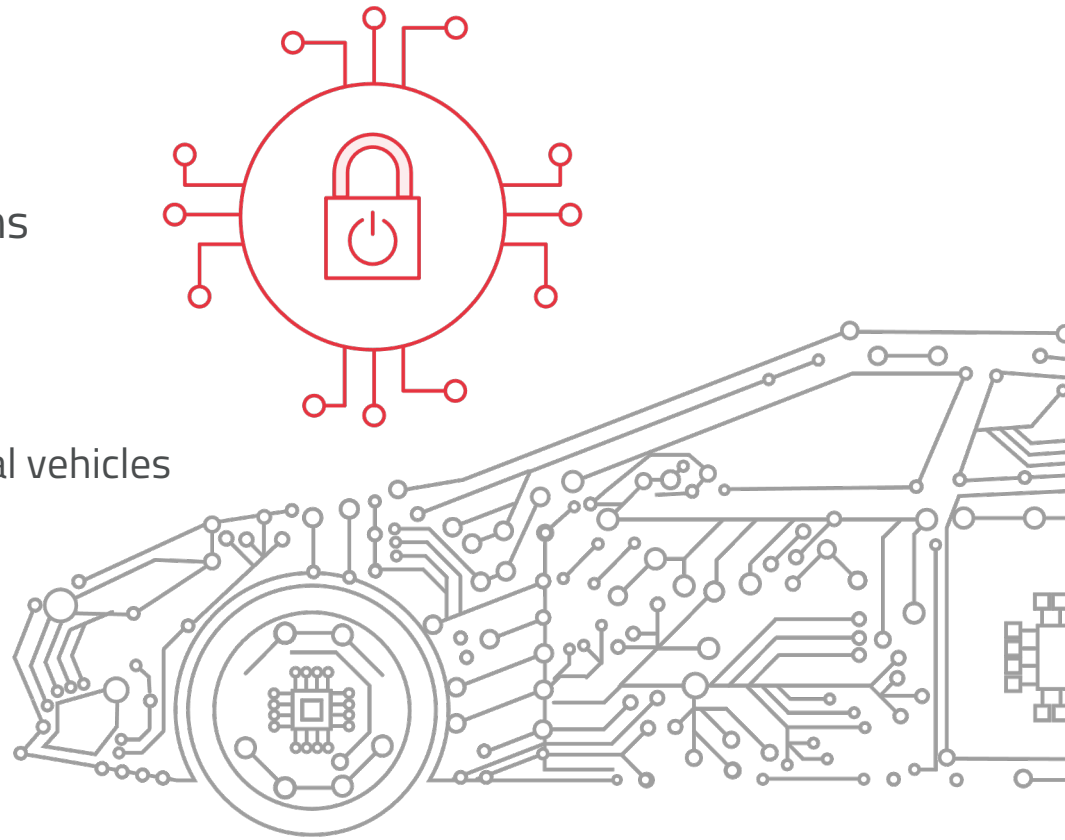
ARILOU
Automotive Cybersecurity
Part of NNG Group

ARILOU AUTOMOTIVE CYBERSECURITY

YOUR TRUSTED INDEPENDENT SECURITY PARTNER

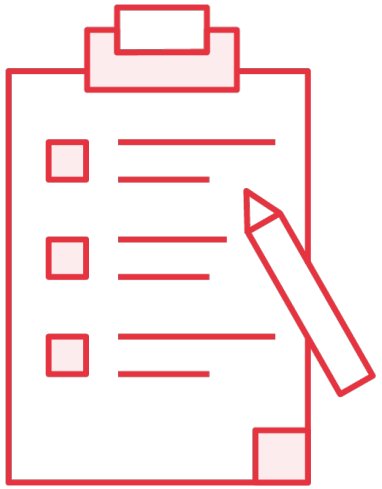
- Automotive cybersecurity pioneer since 2012
- Independent member of global automotive software supplier, NNG Group, since 2016

- **SENTINEL** – Firewall & Intrusion Detection/Prevention Systems (IDS/IPS):
  - **SENTINEL-ETH** – IDS/IPS for Automotive Ethernet
  - **SENTINEL-CAN** – IDS/IPS for CAN bus and SAE J1939 commercial vehicles
- **Secure-Boot for ECUs**
- **Professional services:**
  - **ISO/SAE 21434** – Consulting for compliance
  - **TARA** – Automotive Threat Analysis & Risk Assessment



AGENDA

- New technologies
- Attack scenarios
- Protection methods



01

NEW TECHNOLOGIES

CURRENT STATE OF AUTOMOTIVE CYBERSECURITY

- Migration from CAN bus to Automotive Ethernet –
  - Ethernet, IP and other well-known protocols by hackers
  - Multiple known public exposures
  - Many readily available attack tools

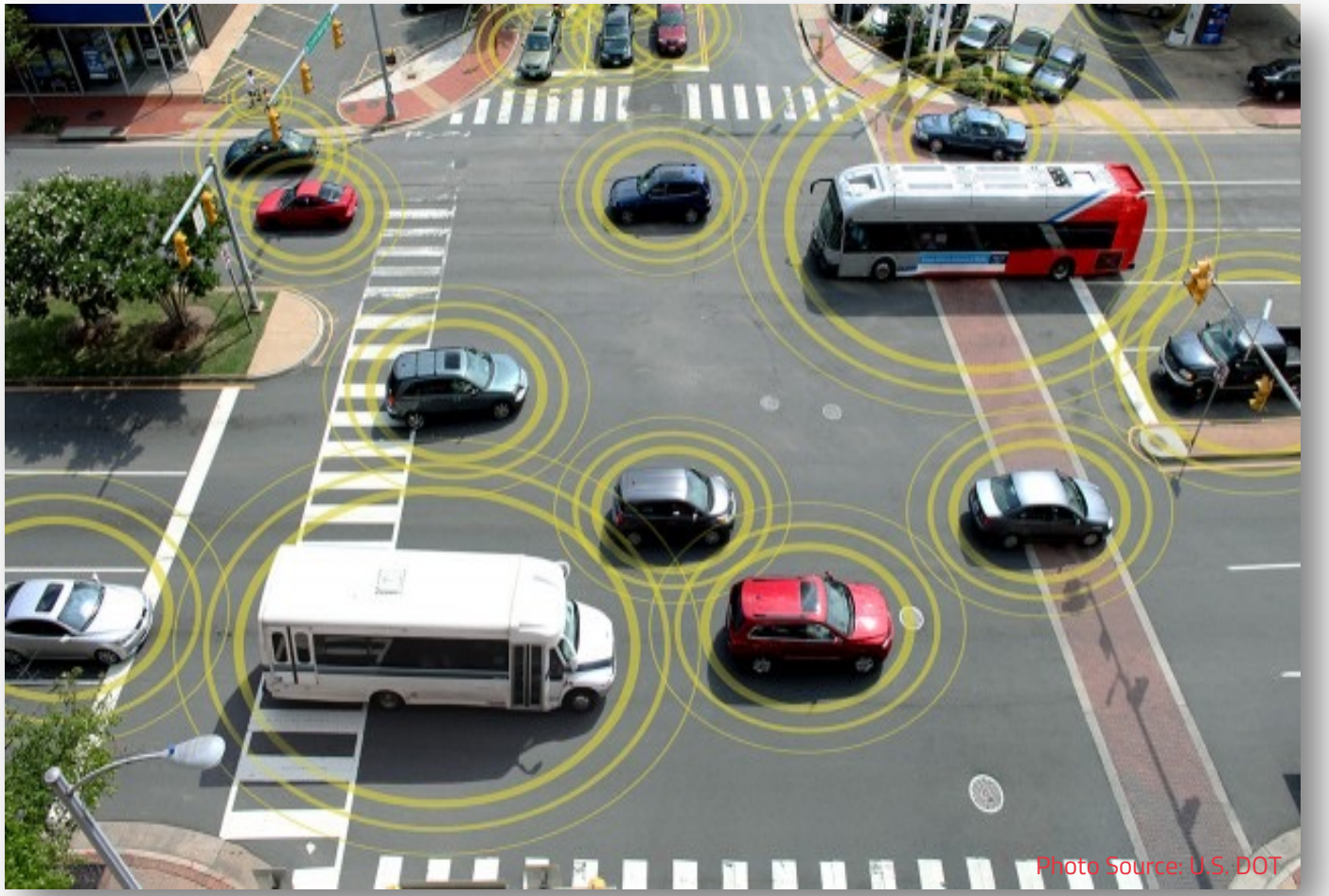
- Complexity
  - Newly developed software – new vulnerabilities
  - High computerization – higher risks
  - Increased connectivity – more potential attack vectors

- Major concerns to **safety**, **reliability** and **privacy**

- Growing cyber-threats and industry awareness but no major incidents yet with casualties or physical damage
- UNECE WP.29 UNR 155 as of 2022 as a driving force for increased cybersecurity protection

WHAT IS V2X?

Vehicles and infrastructure exchanging unmanaged messages



DO NOT PASS WARNING

LEFT TURN ASSIST

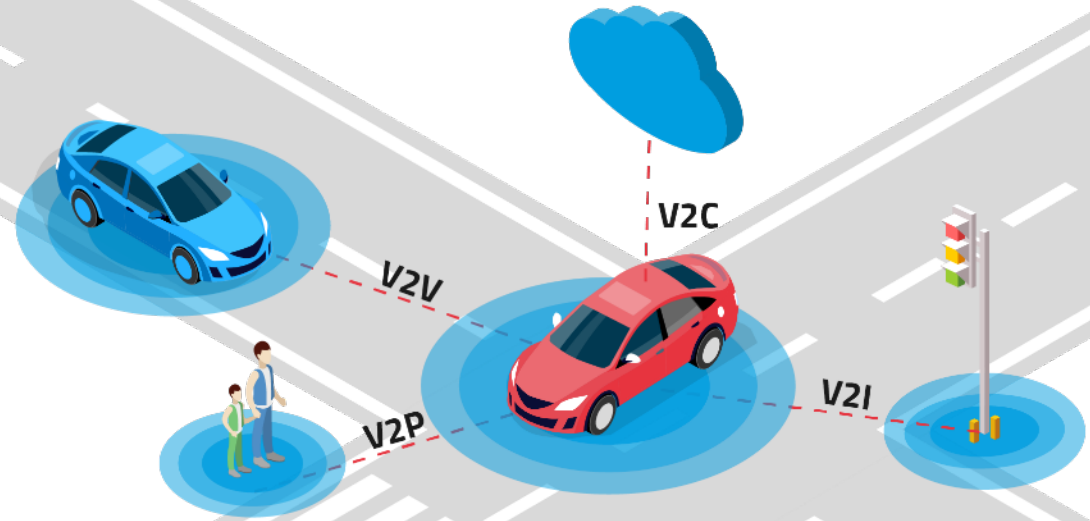
TRAFFIC LIGHT ASSISTANT

Photo Source: Audi/jalopnik.com

CONNECTED VEHICLES AND V2X

- Most vehicles are connected to the internet via cellular interface (infotainment, telematics, electronic data recorders, insurance company dongles, etc.) – there are many attack options

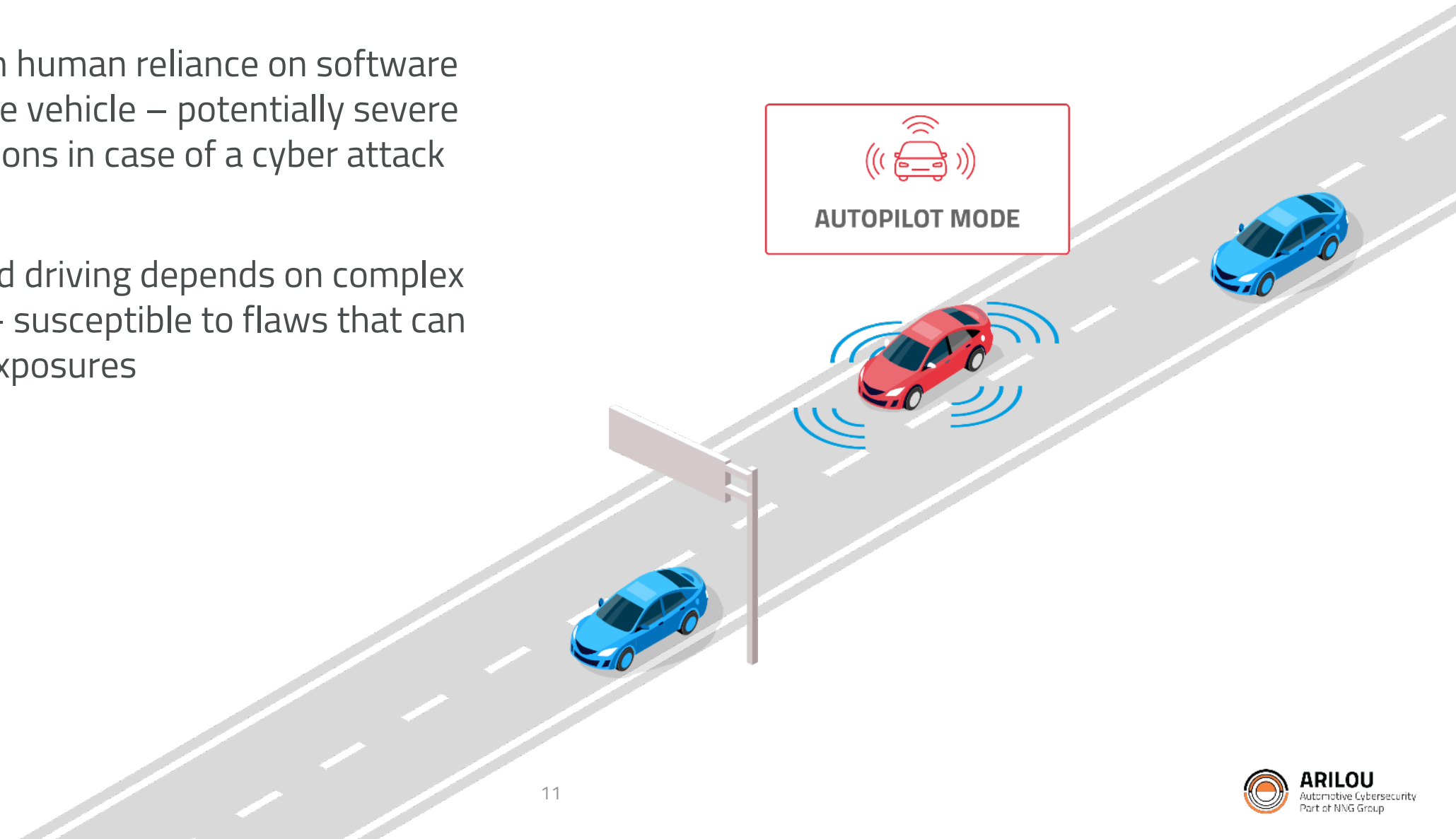
- V2X will be a major platform for inter-vehicle comms, in addition to comms between the vehicle and multiple entities – a basis for many exciting applications, but also cyber risk.



AUTOMATED DRIVING

- Increase in human reliance on software to drive the vehicle – potentially severe repercussions in case of a cyber attack

- Automated driving depends on complex software - susceptible to flaws that can result in exposures



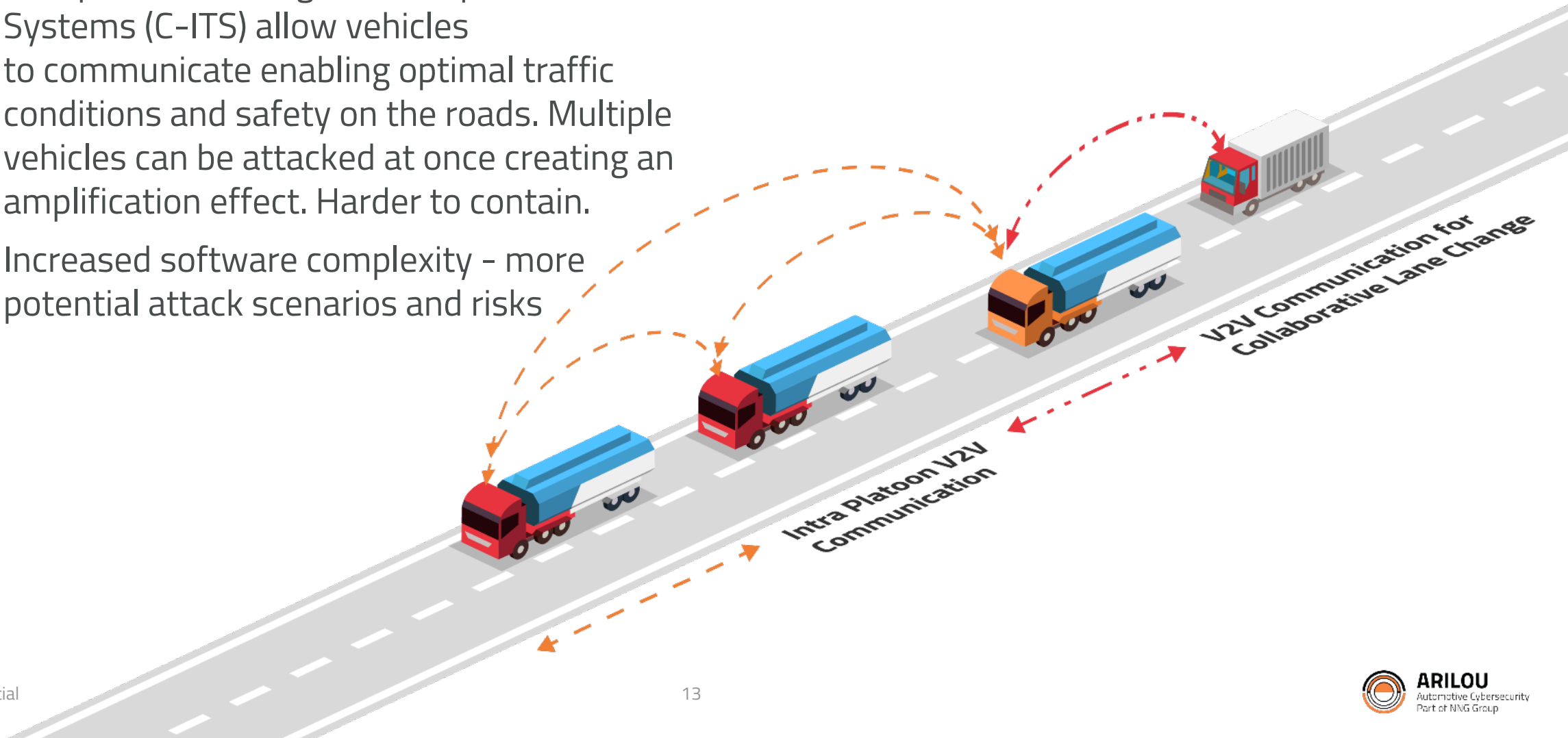
CONNECTED AND AUTONOMOUS VEHICLES (CAV)

- The combination of automated driving and vehicle connectivity multiplies the cyber risk

a.k.a CAD (Connected and Automated Driving)

CO-OPERATIVE DRIVING

- Co-operative Intelligent Transportation Systems (C-ITS) allow vehicles to communicate enabling optimal traffic conditions and safety on the roads. Multiple vehicles can be attacked at once creating an amplification effect. Harder to contain.
- Increased software complexity - more potential attack scenarios and risks



02

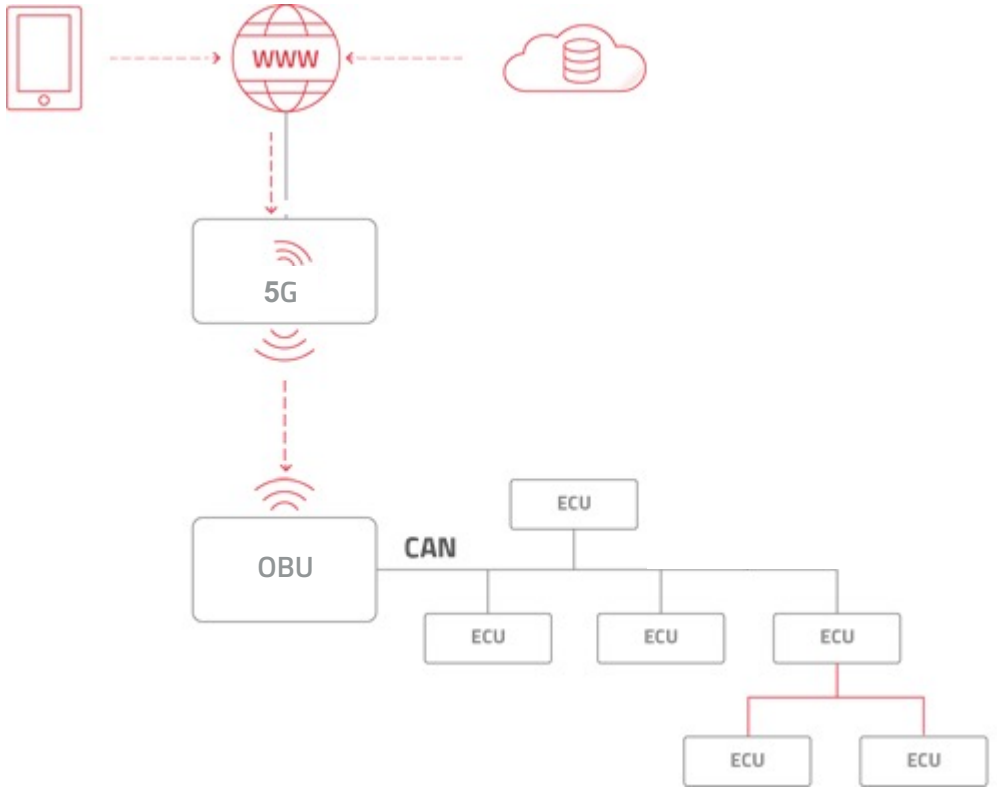
ATTACK SCENARIOS

V2X OBU (ON BOARD UNIT) CYBERSECURITY

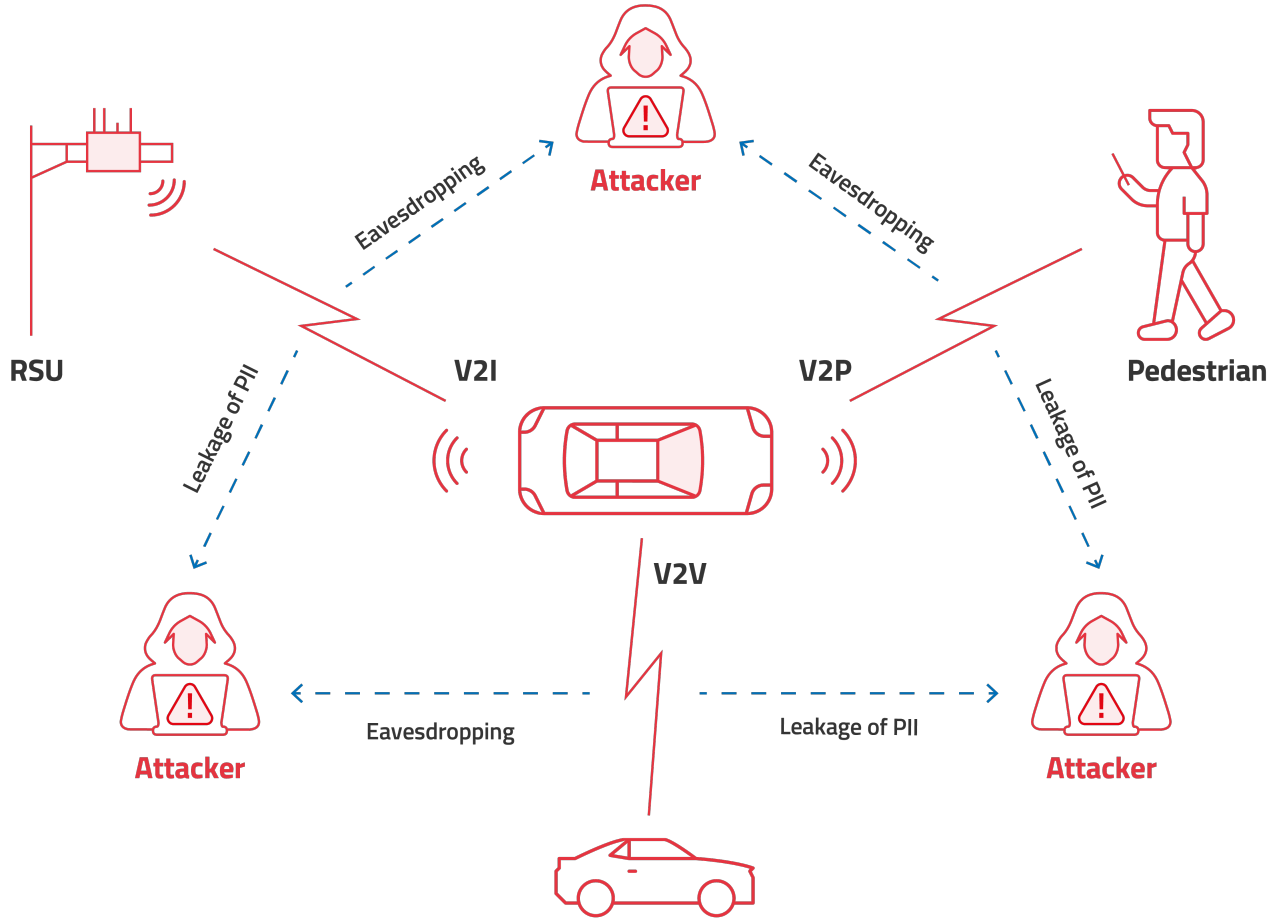
C-V2X case attack vector example

REMOTE ATTACKS ARE THE MOST SEVERE THREAT TO THE VEHICLE

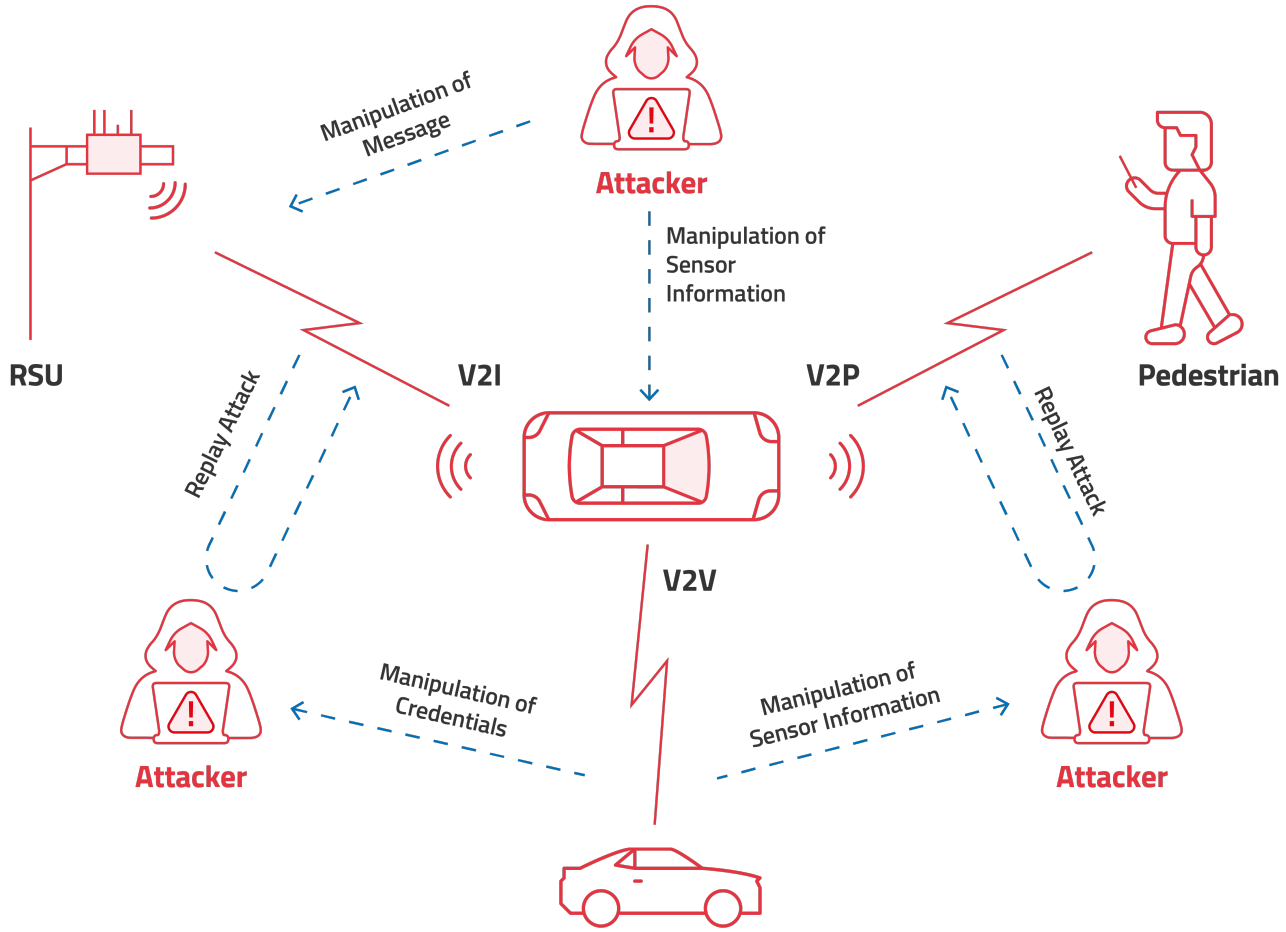
- Incoming traffic from the cellular network



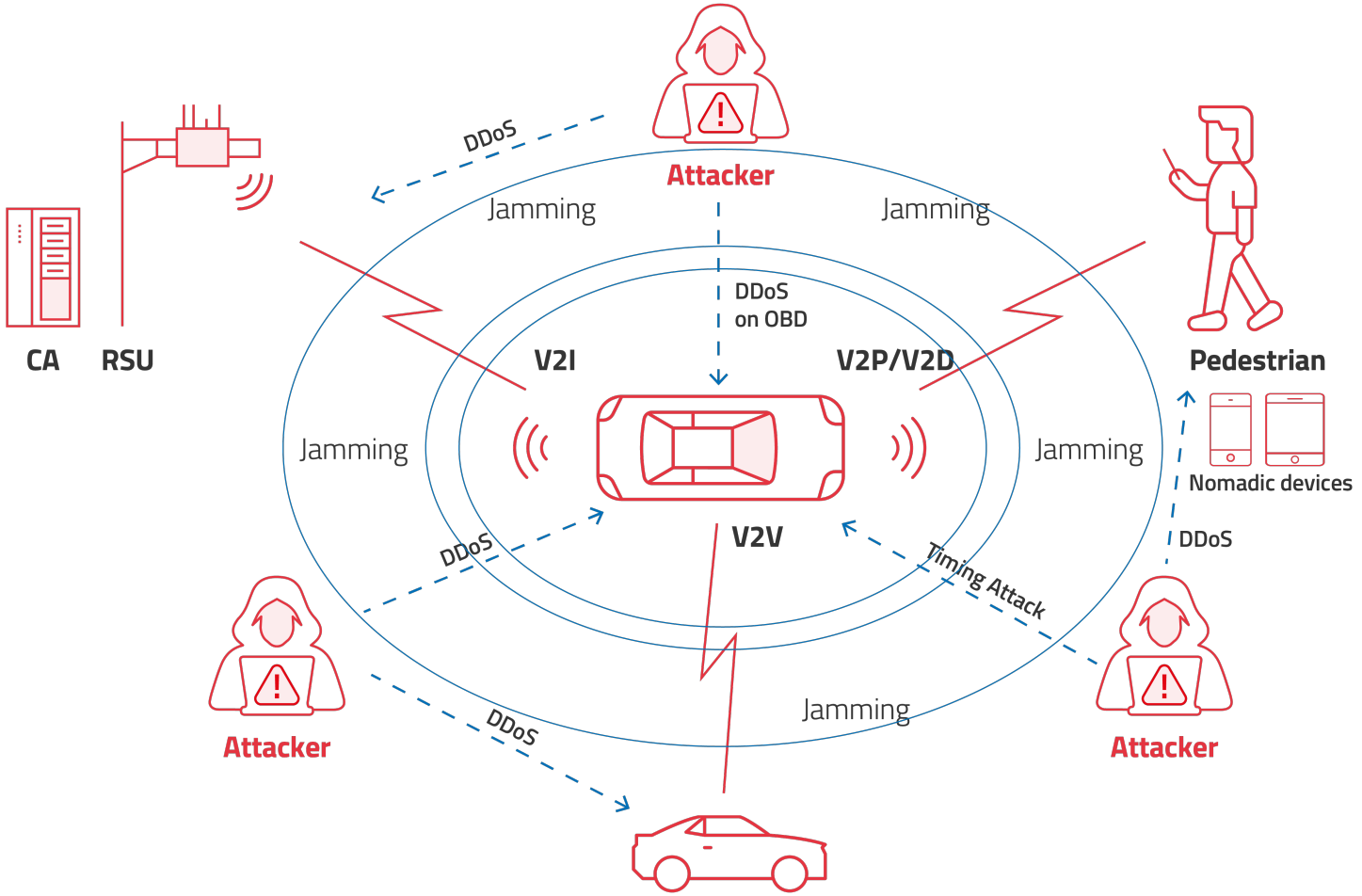
THREATS TO CONFIDENTIALITY



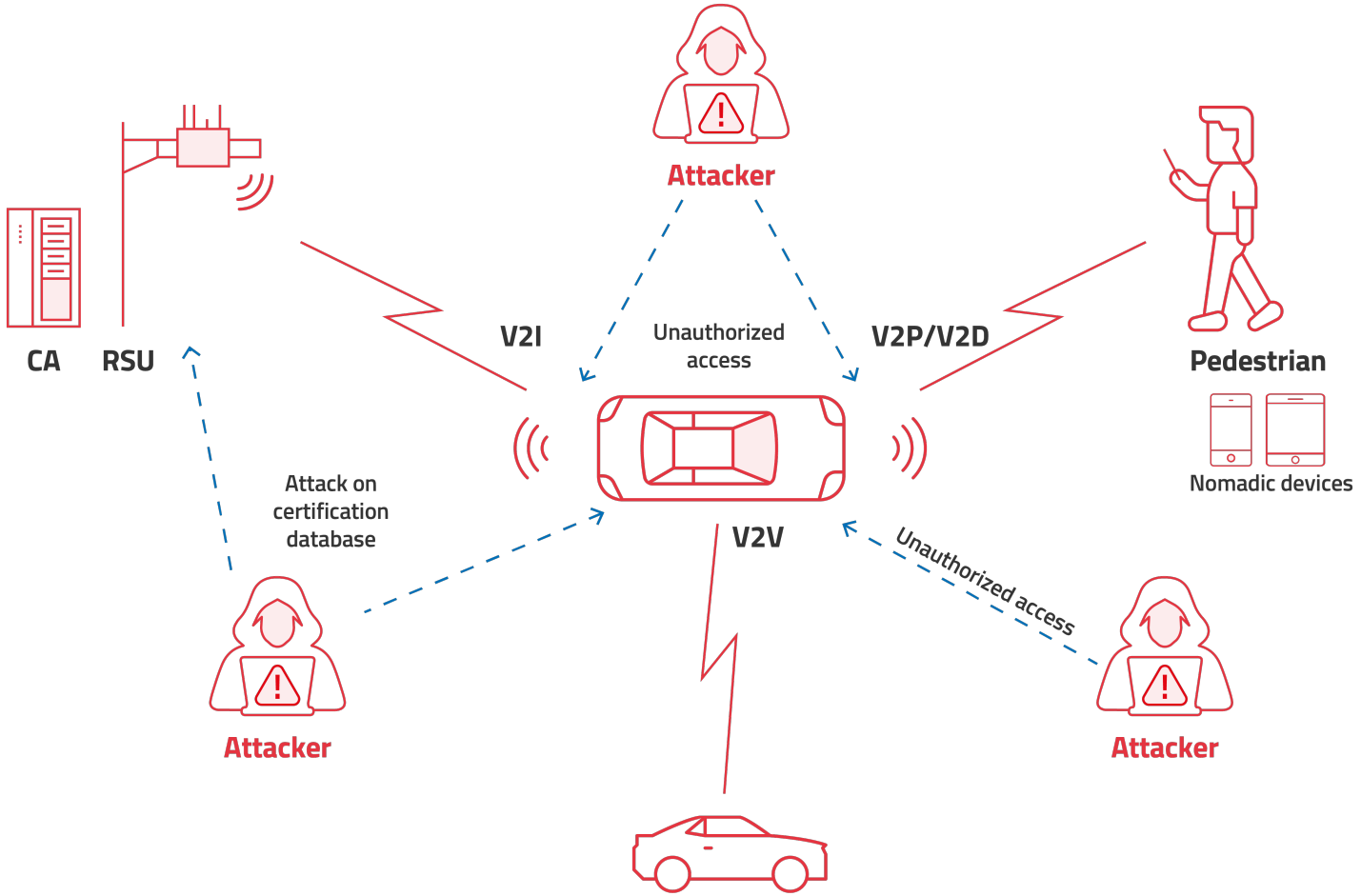
THREATS TO INTEGRITY



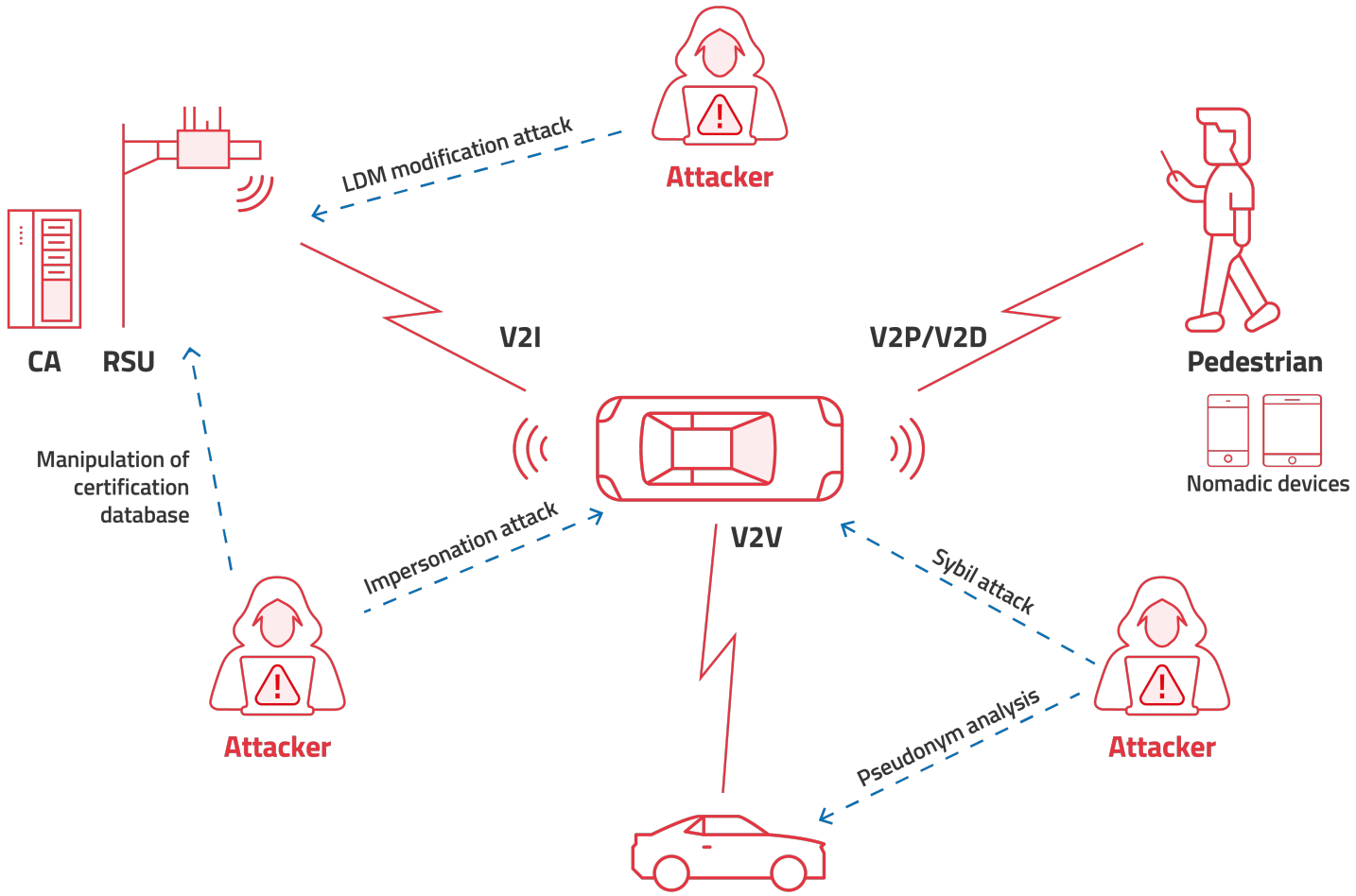
THREATS TO AVAILABILITY



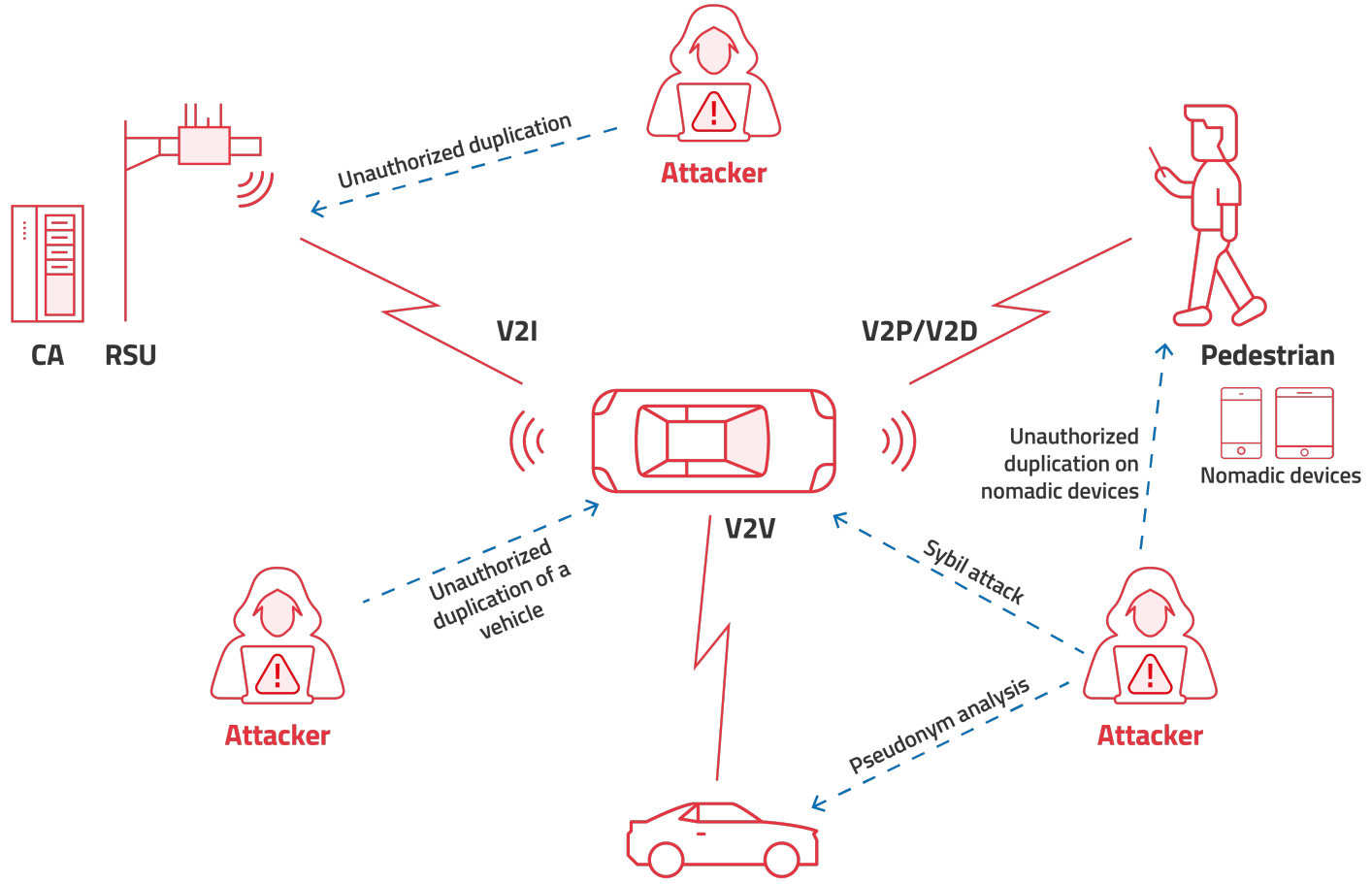
THREATS TO NON-REPUDIATION



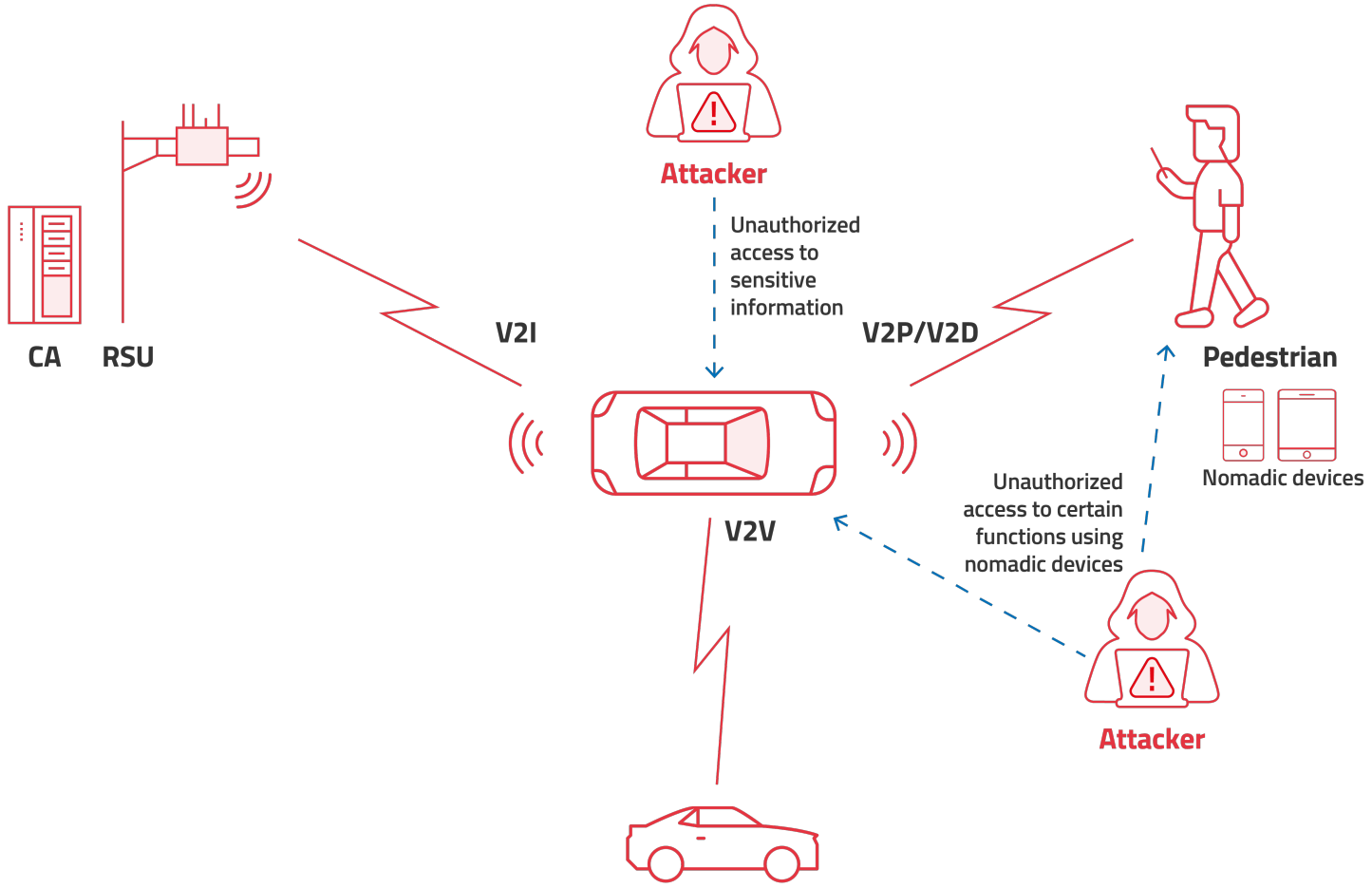
THREATS TO AUTHENTICITY



THREATS TO ACCOUNTABILITY



THREATS TO AUTHORIZATION

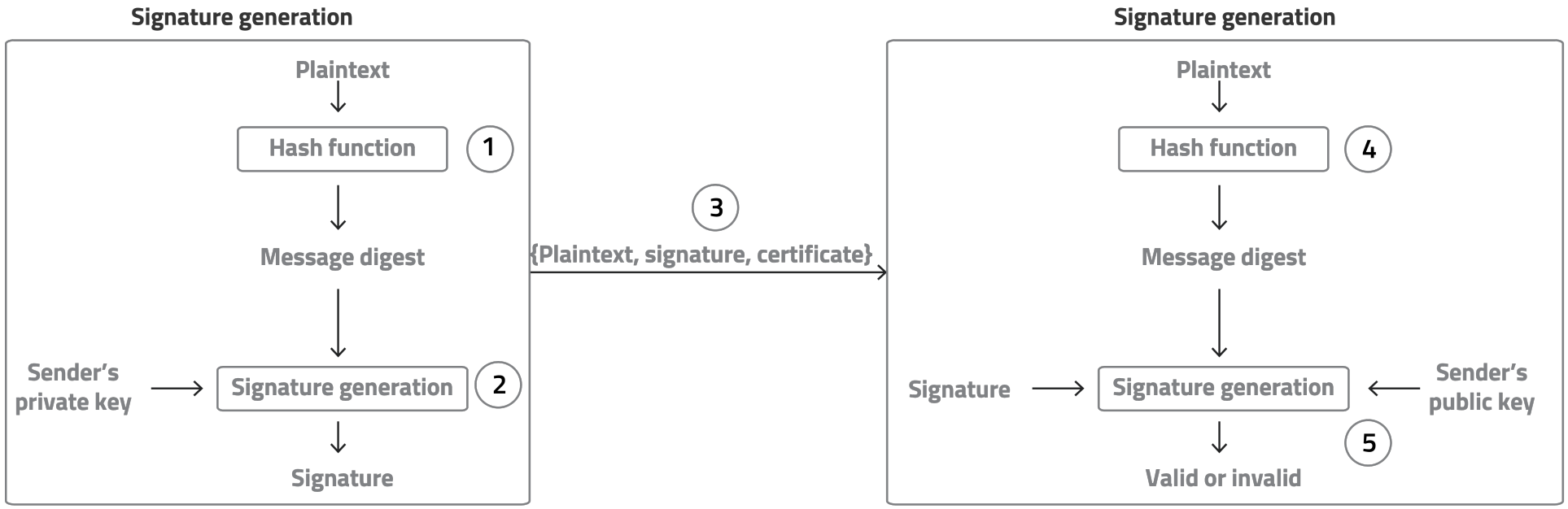


03

PROTECTION OPTIONS

CRYPTOGRAPHIC MECHANISM

- Important tool but not sufficient. No protection against compromised devices.
- Cannot validate the contents of the message



OBU CYBERSECURITY

Protection on two fronts

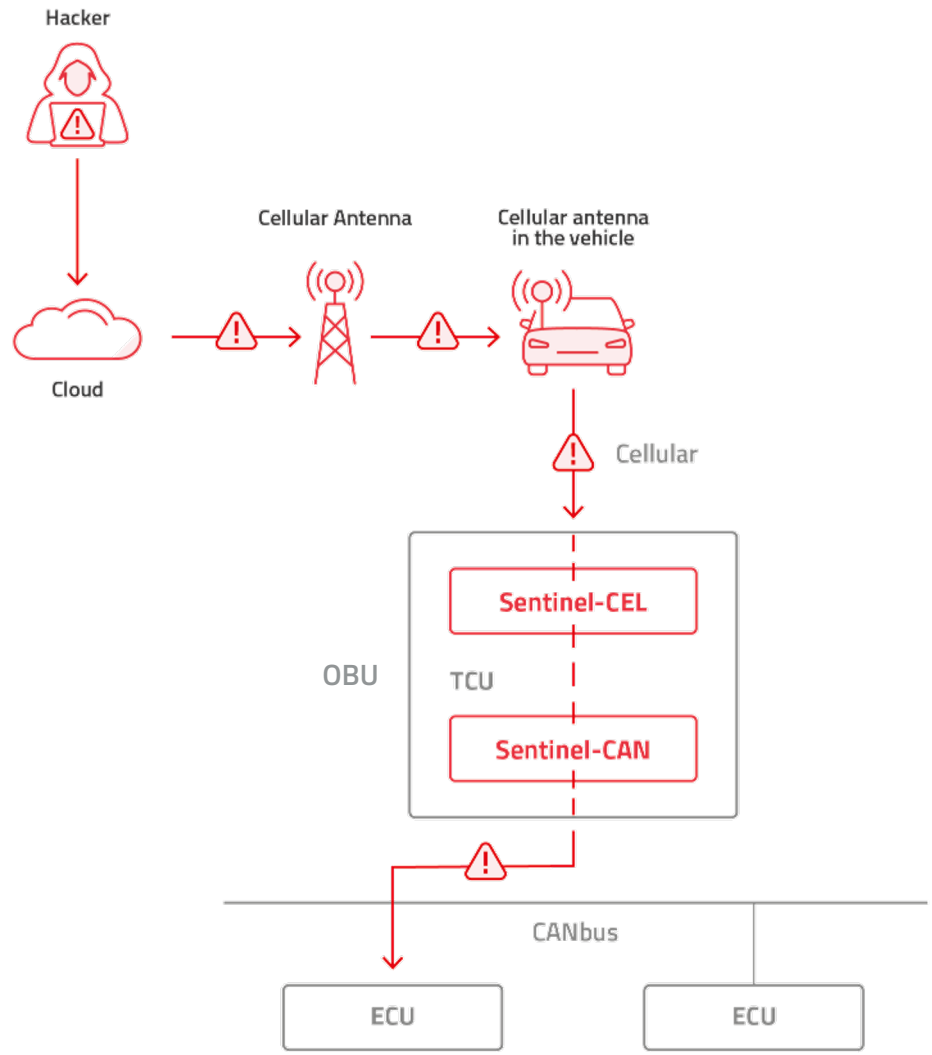
INSPECTING THE CELLULAR – INCOMING TRAFFIC

Incoming cellular traffic to the OBU should be inspected in case the OBU is the target – or used as a bridge to the in-vehicle network.

INSPECTING THE IN-VEHICLE TRAFFIC

Incoming and outgoing CANbus traffic should be inspected to prevent attack on the OBU or on other ECUs

New emerging Automotive Ethernet has grater risks



PLAUSIBILITY VERIFICATION

- **Range plausibility:** Check if the position of the sender is inside the maximum range
- **Position plausibility:** Check if the position of the sender is at a plausible place (e.g., on a road, no overlaps with physical obstacles, etc.).
- **Speed plausibility:** Check if the speed advertised by the sender is less than a predefined threshold.

PLAUSIBILITY VERIFICATION

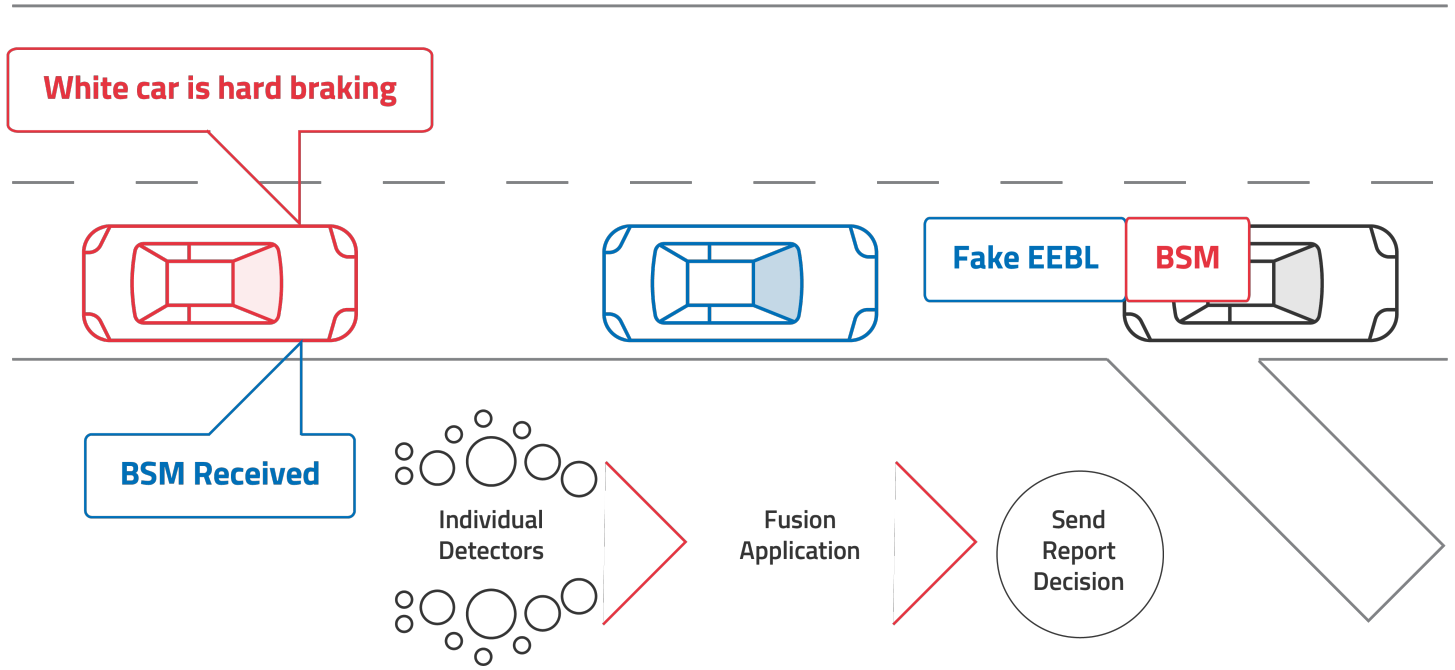
- **Position consistency:** Check if two consecutive beacons coming from the same sender have plausible separating distance.
- **Speed consistency:** Check if two consecutive beacons coming from the same sender have plausible acceleration or deceleration.
- **Position speed consistency:** Check if two consecutive beacons coming from the same sender have consistent speed and separating distance.

PLAUSIBILITY VERIFICATION

- **Beacon frequency:** Check if the beacon frequency of a sender is compliant with the standards.
- **Position heading consistency:** Check if the positions in two consecutive beacons coming from a same sender correspond to the heading advertised by that sender.
- **Intersection check:** Check if no two beacons coming from two different senders have overlapping locations (i.e., both senders overlap each other).
- **Sudden appearance:** Check if no sender suddenly appeared within a certain range/distance.

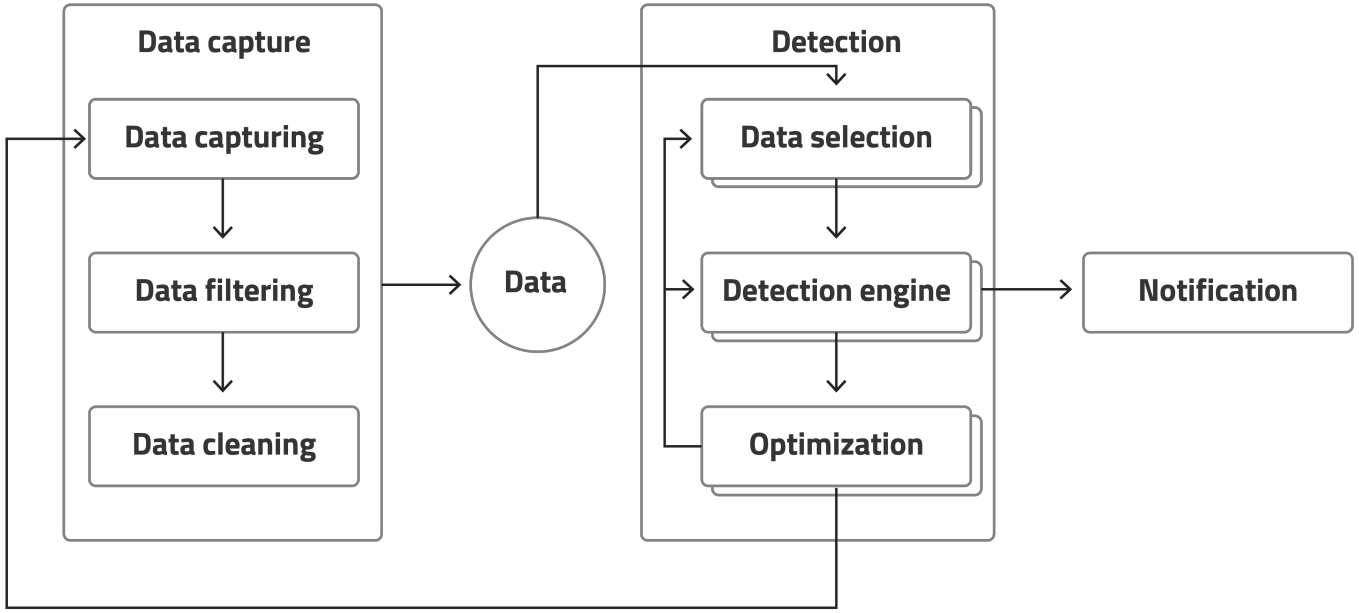
EXAMPLE OF MISBEHAVIOR
FAKE EEBL (EARLY EMERGENCY BRAKE LIGHT)

- Message plausibility can be checked using sensor fusion by comparing the signal strength (RSSI) from the physical layer and compare it with the vehicle locations (GNNS and V2X message)



MISBEHAVIOR DETECTION PROCESS

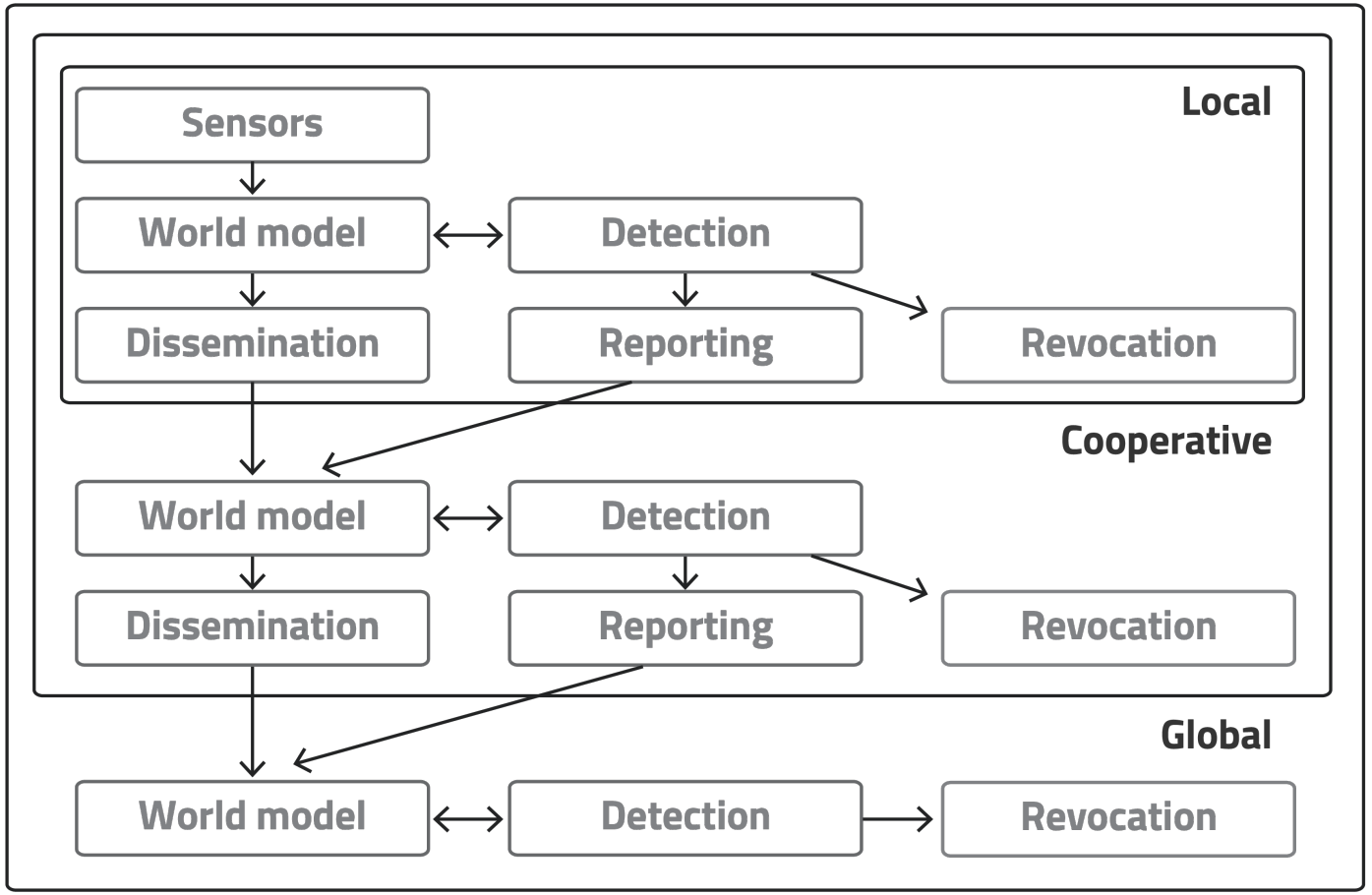
- **Data capture** - definition of the types of data and information that can be captured from different sources, including automotive, infrastructure, original equipment manufacturers (OEMs) and suppliers, for misbehavior detection.
- **Detection** - analysis of the data captured to detect misbehavior.



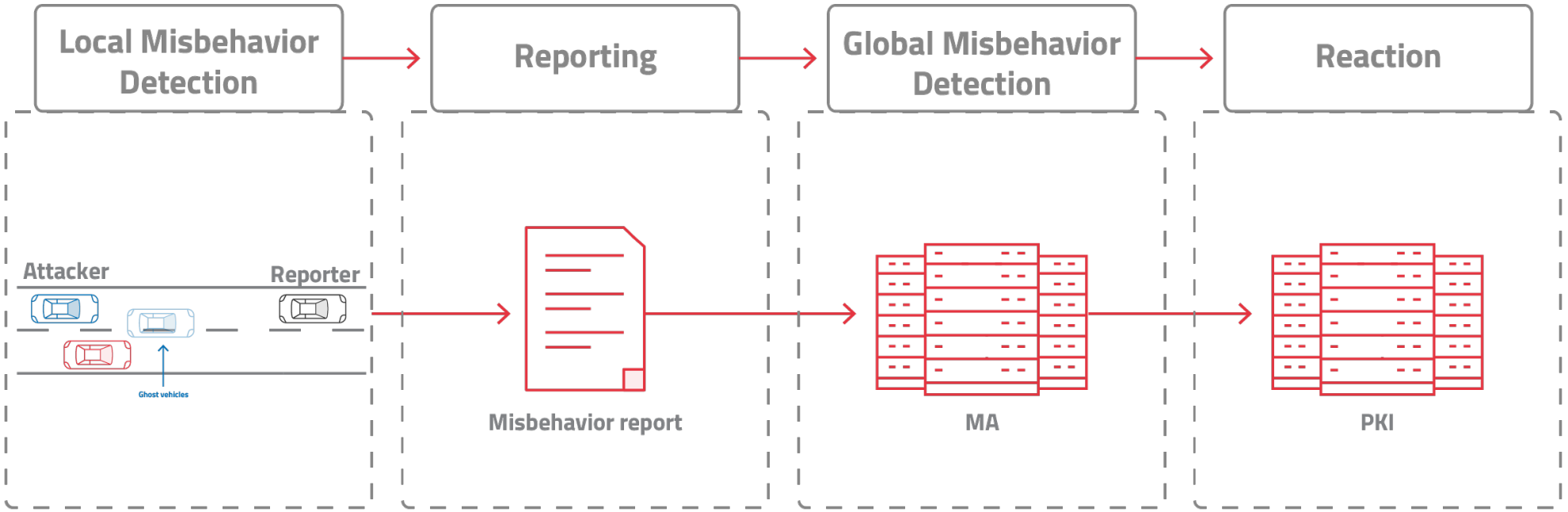
MISBEHAVIOR REACTION SCALE

- No reaction
- Warning message is sent to the vehicle
- Warning point is deducted from the vehicle's score
- Passive revocation where the vehicle cannot request more certificates
- Active revocation where the current certificates of the vehicle are revoked (CRL)

DETECTION AND REVOCATION SCOPE



MISBEHAVIOR DETECTION END-TO-END PROCESS



TAKE HOME MESSAGES

- V2X cybersecurity needs to be addressed from day zero with a secure by design approach
- Regulation will be a major driving force, but corporate and organizational responsibility is equally important
- A multi-layer, defense-in-depth approach is required to protect the V2X traffic in the OBU
- Secure software and hardware development & testing in addition to functional safety
- Dedicated, devoted, and independent protection components such as firewalls, IDS and IPS to oversee the whole V2X traffic
- Use professional companies to guide and support you along the way
- For more information, please see our web site https://ariloutech.com/
- Please follow us on LinkedIn https://www.linkedin.com/company/arilou/

ARILOU
Automotive Cybersecurity
Part of NNG Group

THANK YOU FOR YOUR ATTENTION!

Gilad Bandel

VP Product and Marketing

Email: Gilad.Bandel@nng.com

Tel: +972 (54) 246–0006

Website: ariloutech.com