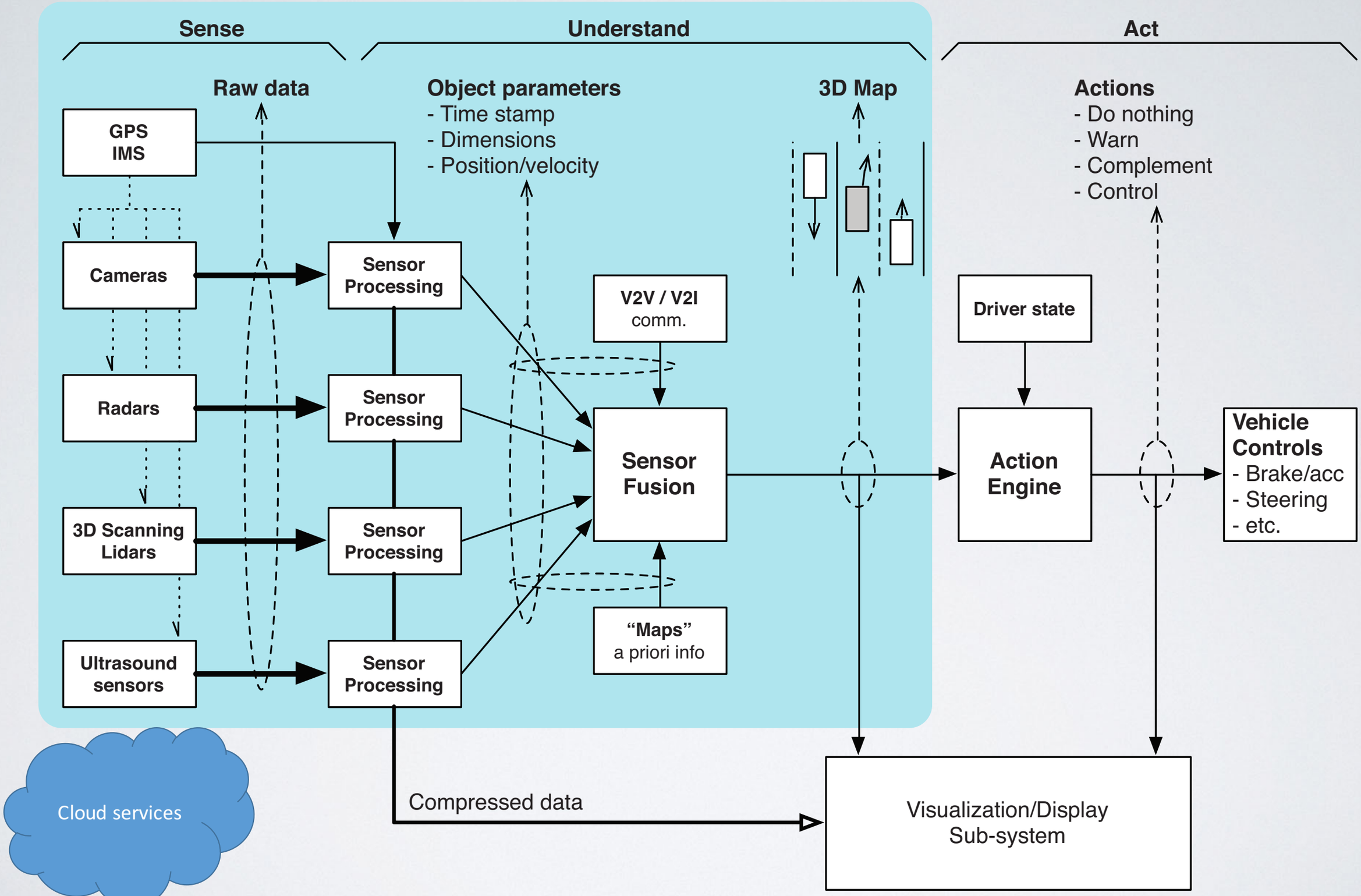
WORK-IN-PROGRESS IN SECURING CAV

Jonathan Petit

jpetit@onboardsecurity.com

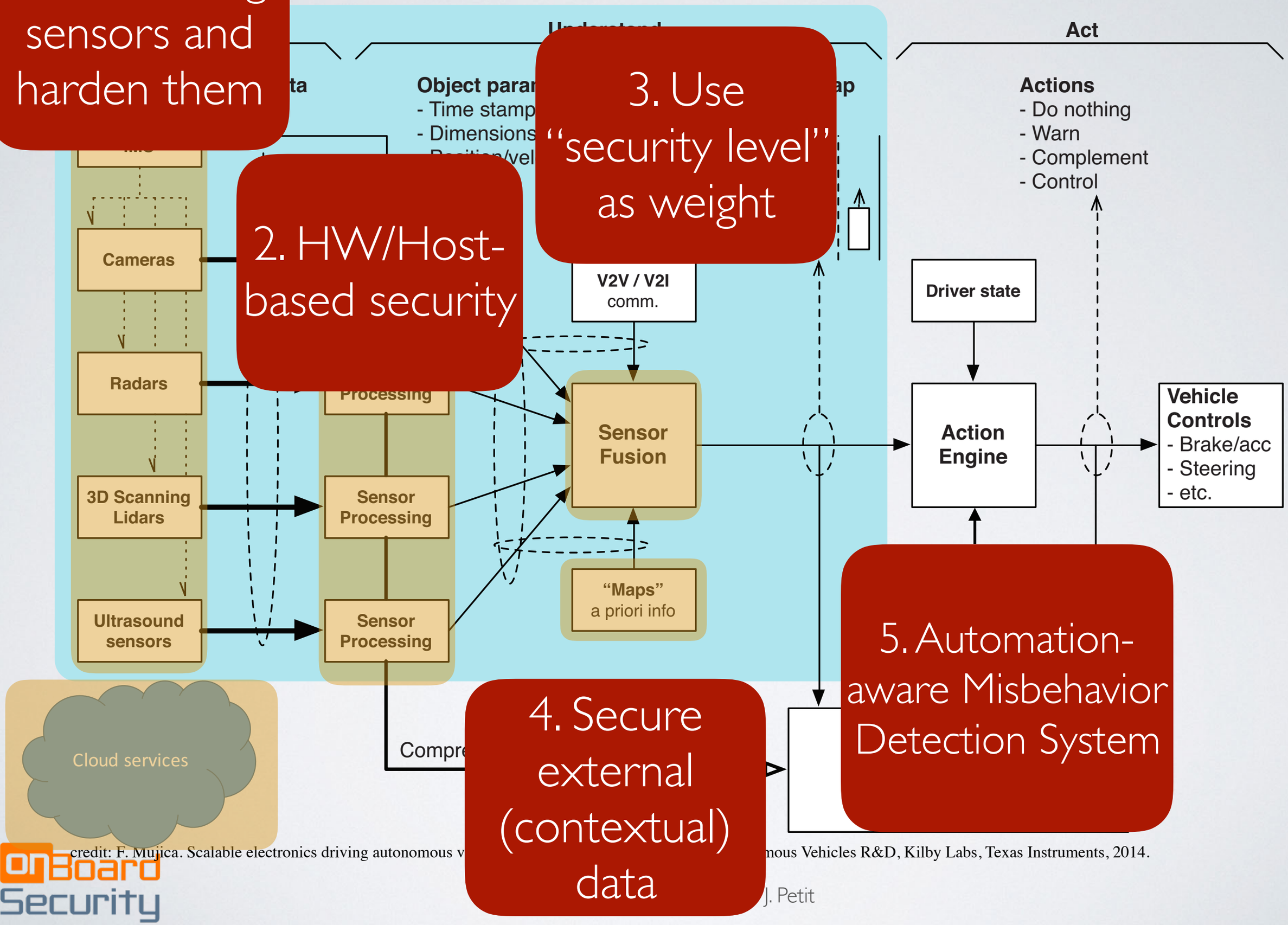


credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

3. Use "security level" as weight

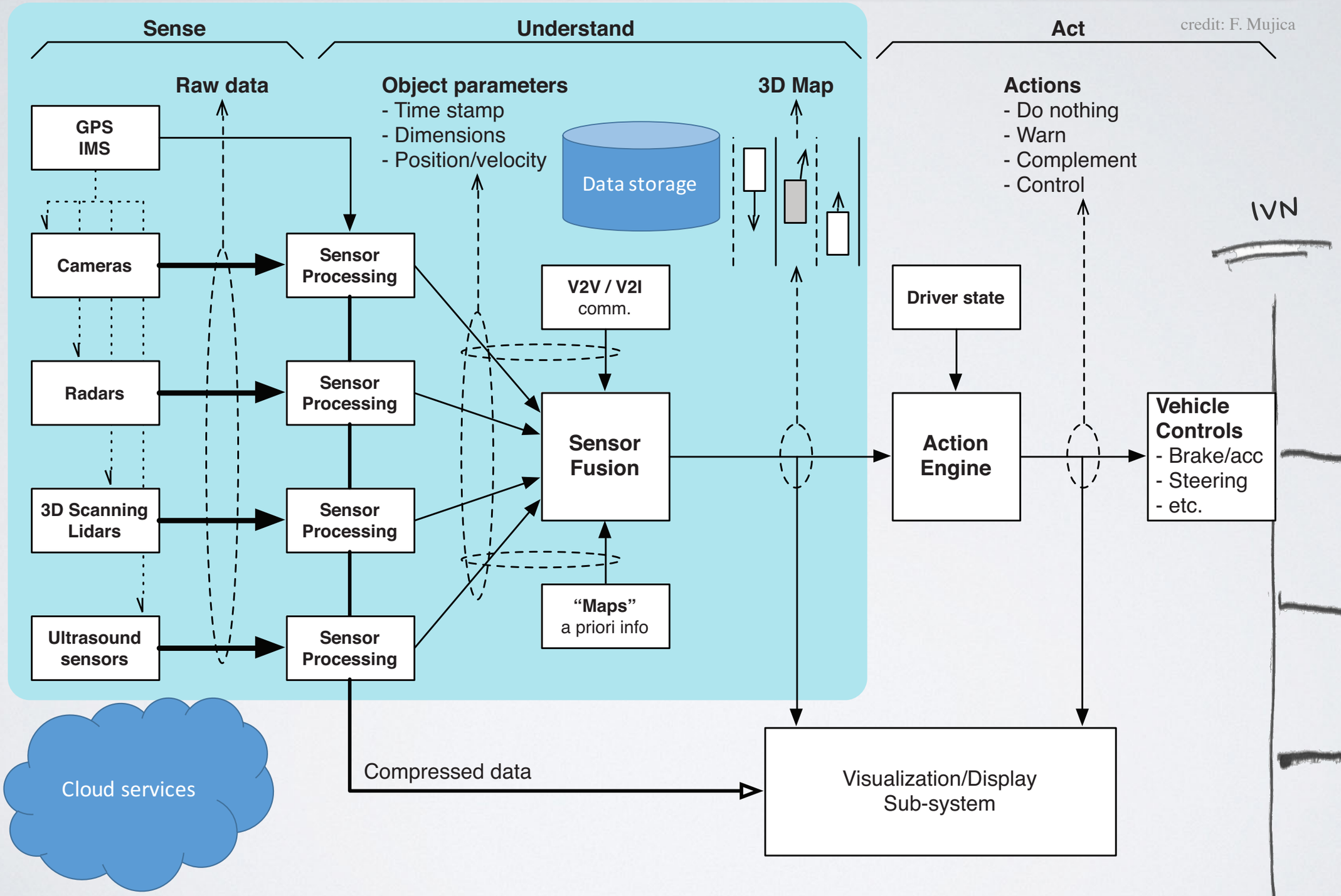


4. Secure external (contextual) data

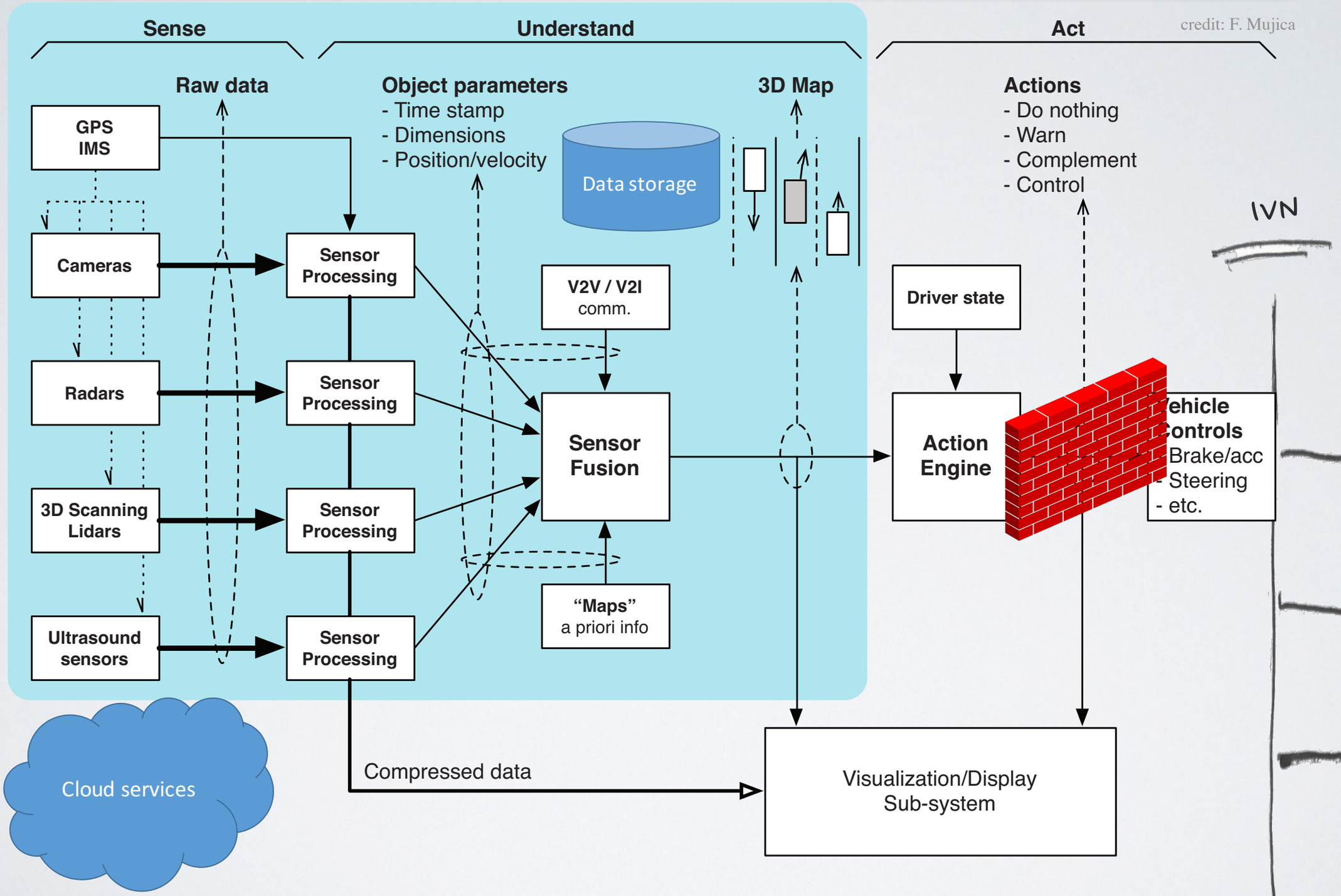
5. Automation-aware Misbehavior Detection System

credit: F. Mujica. Scalable electronics driving autonomous v… …mous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

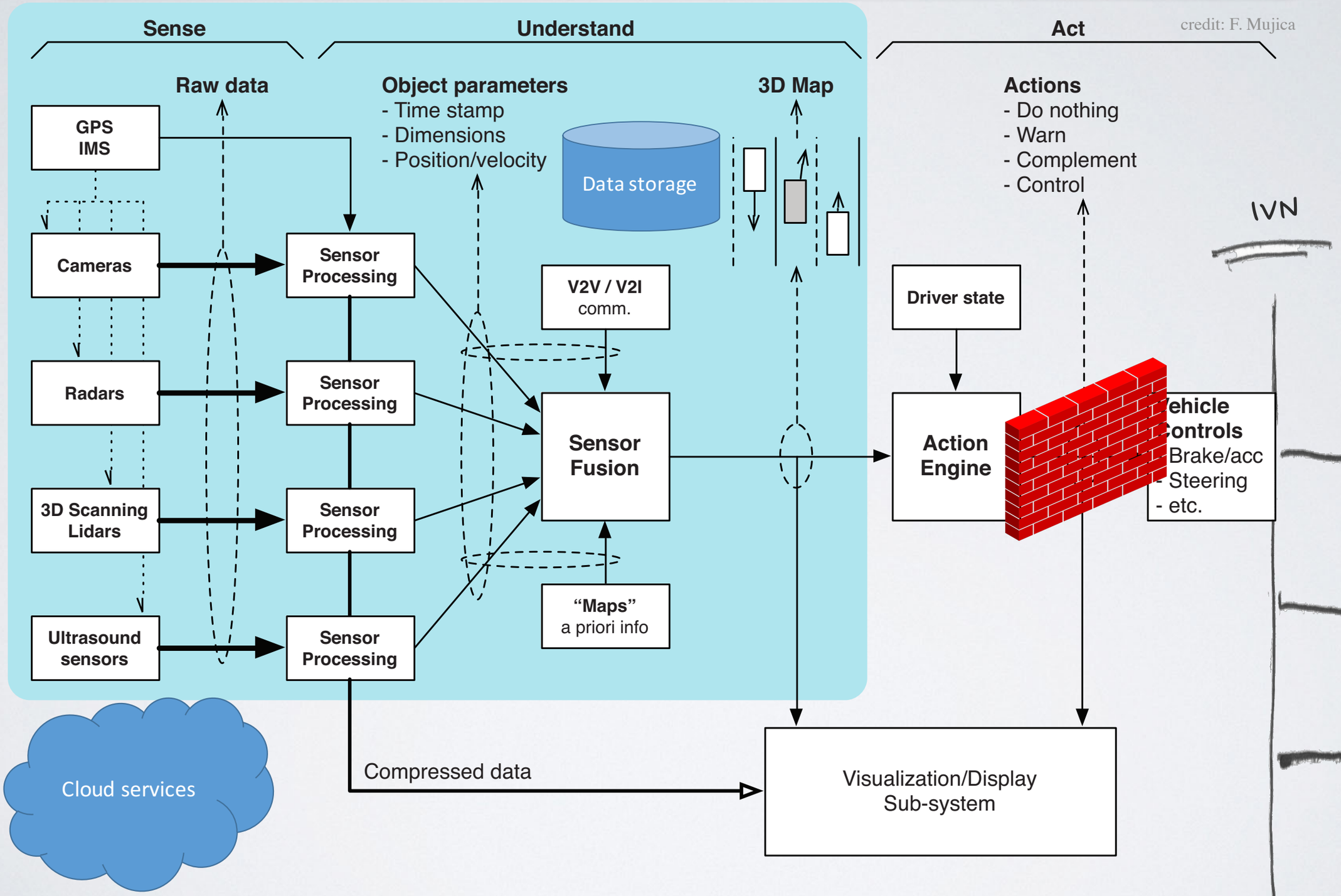
Current security efforts of automotive industry



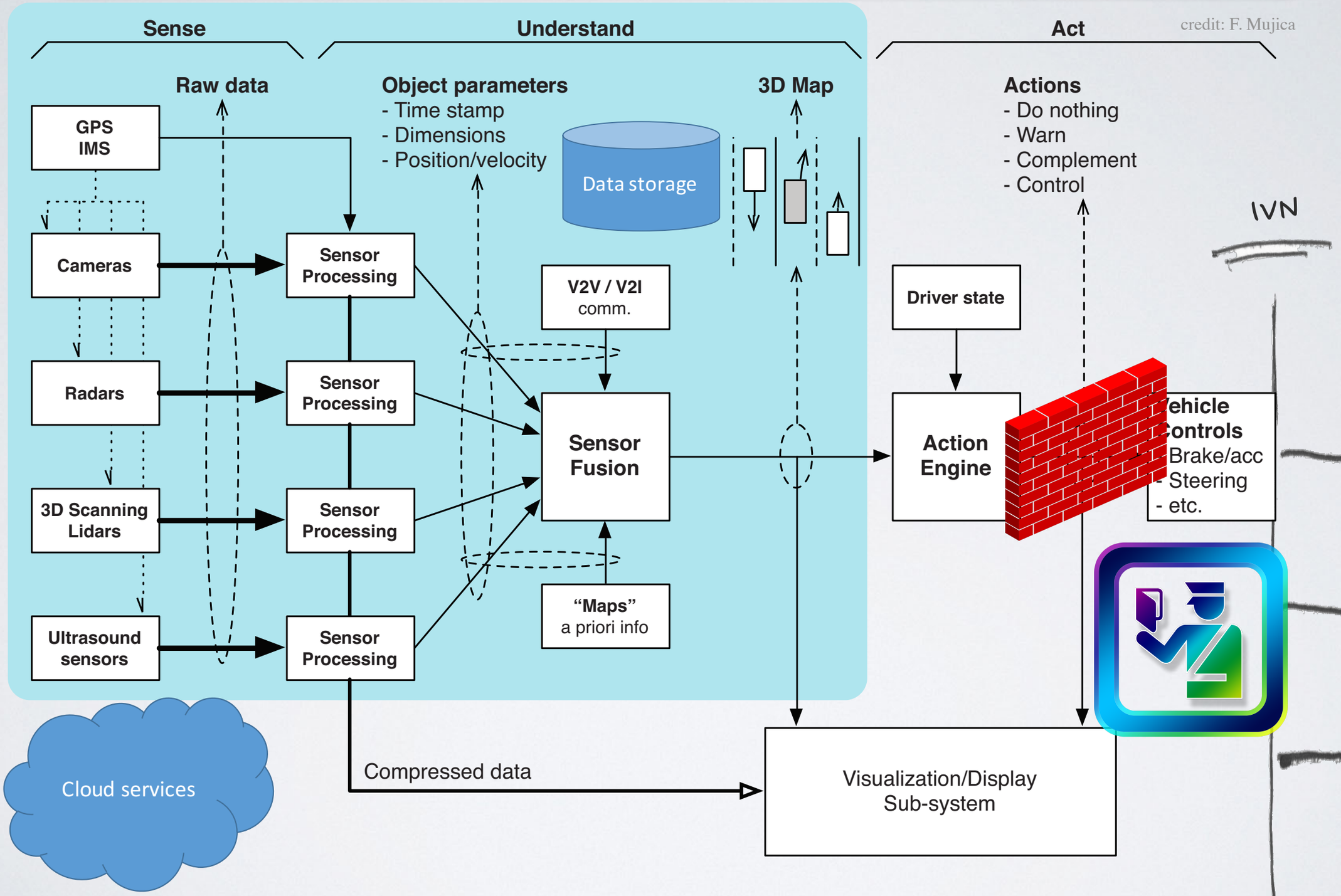
Current security efforts of automotive industry



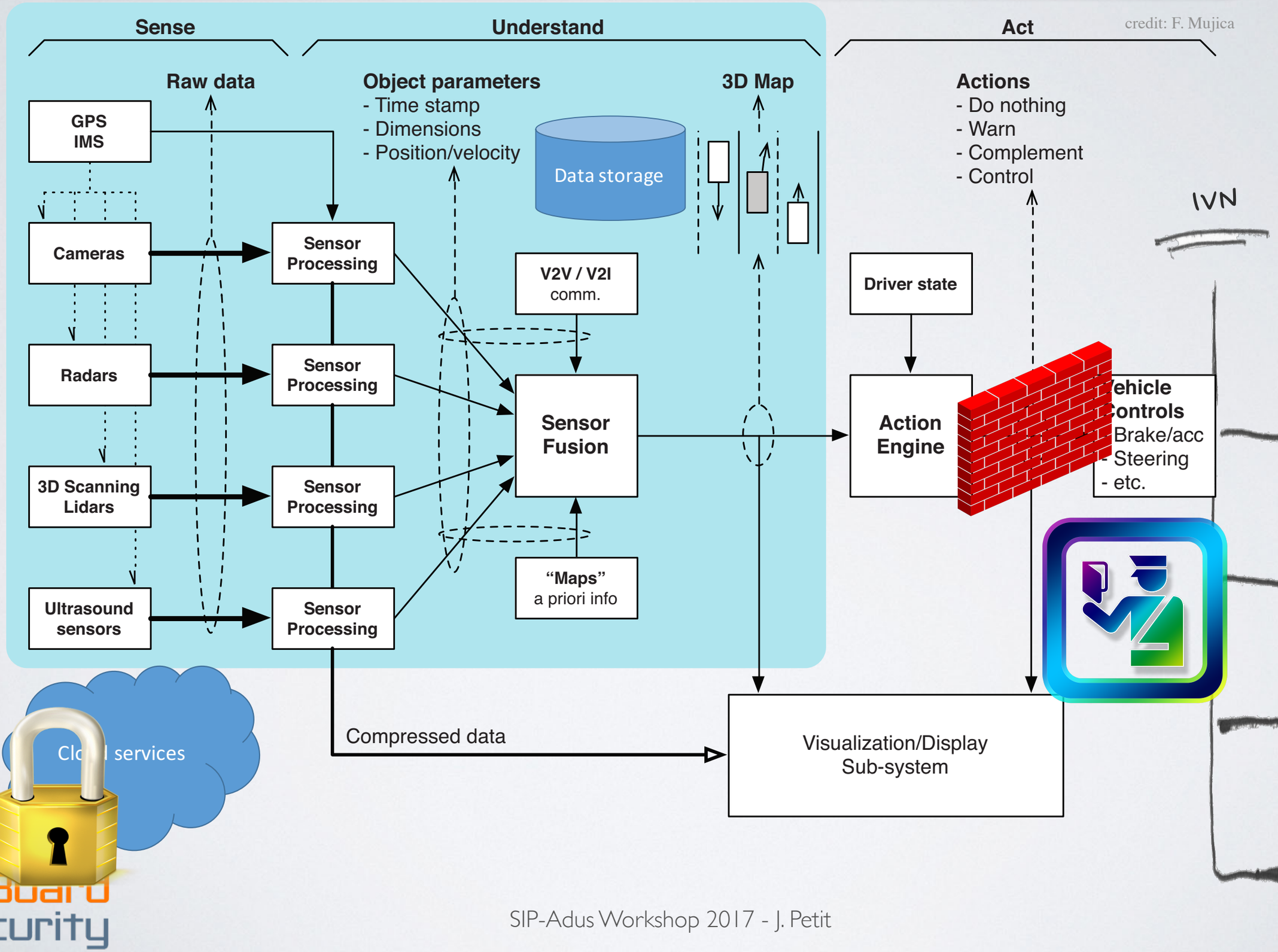
Current security efforts of automotive industry



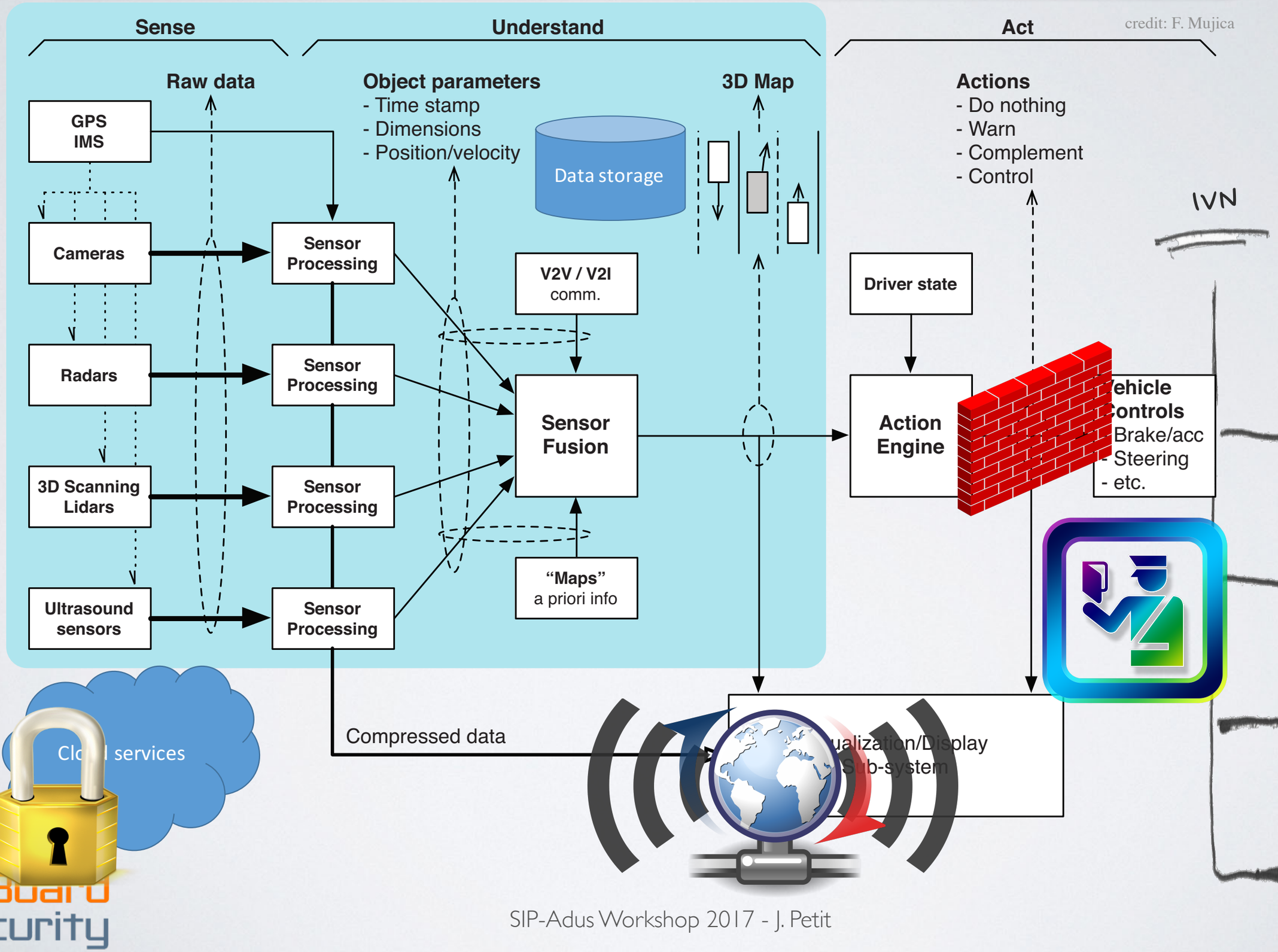
Current security efforts of automotive industry



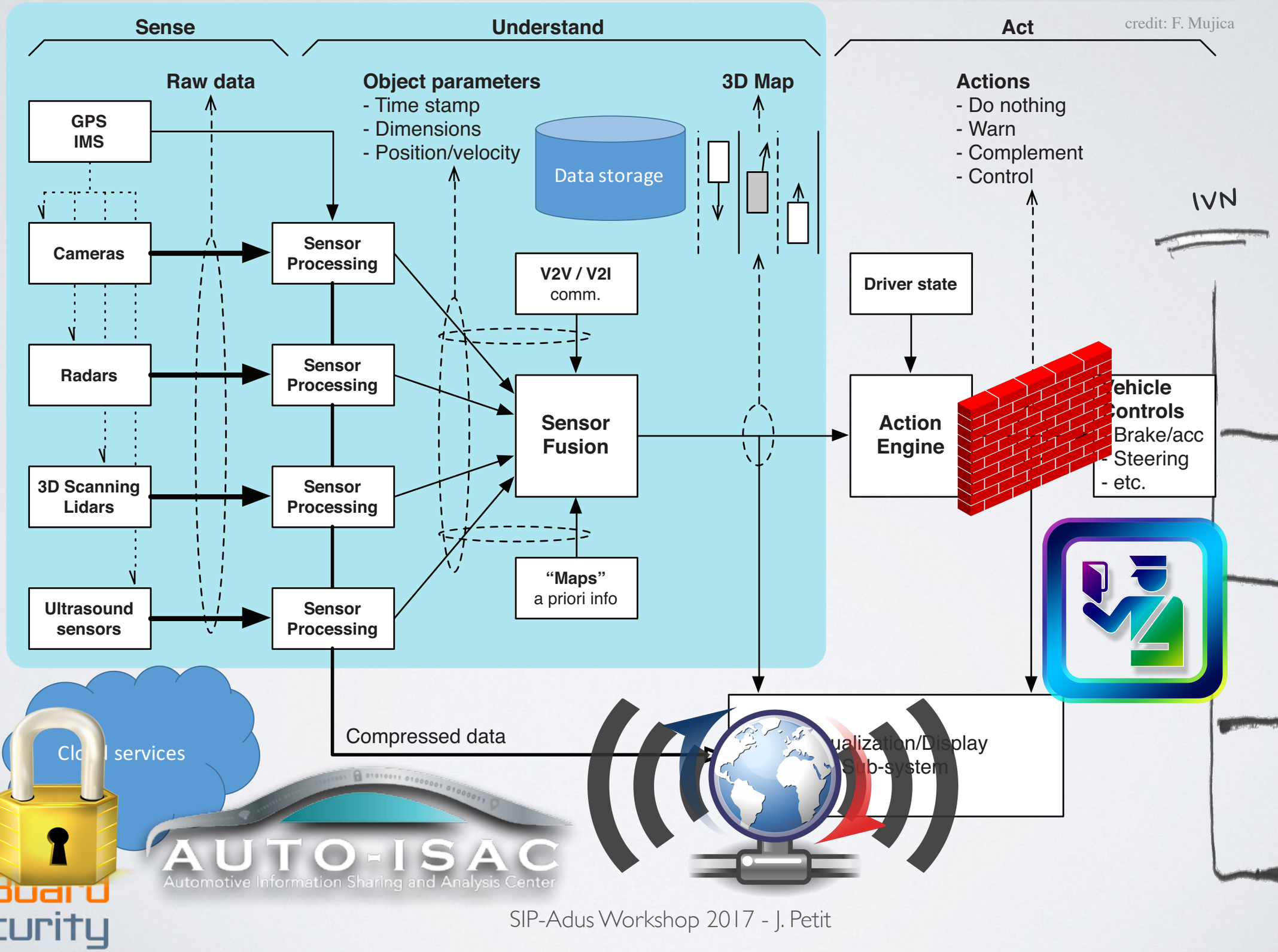
Current security efforts of automotive industry



Current security efforts of automotive industry

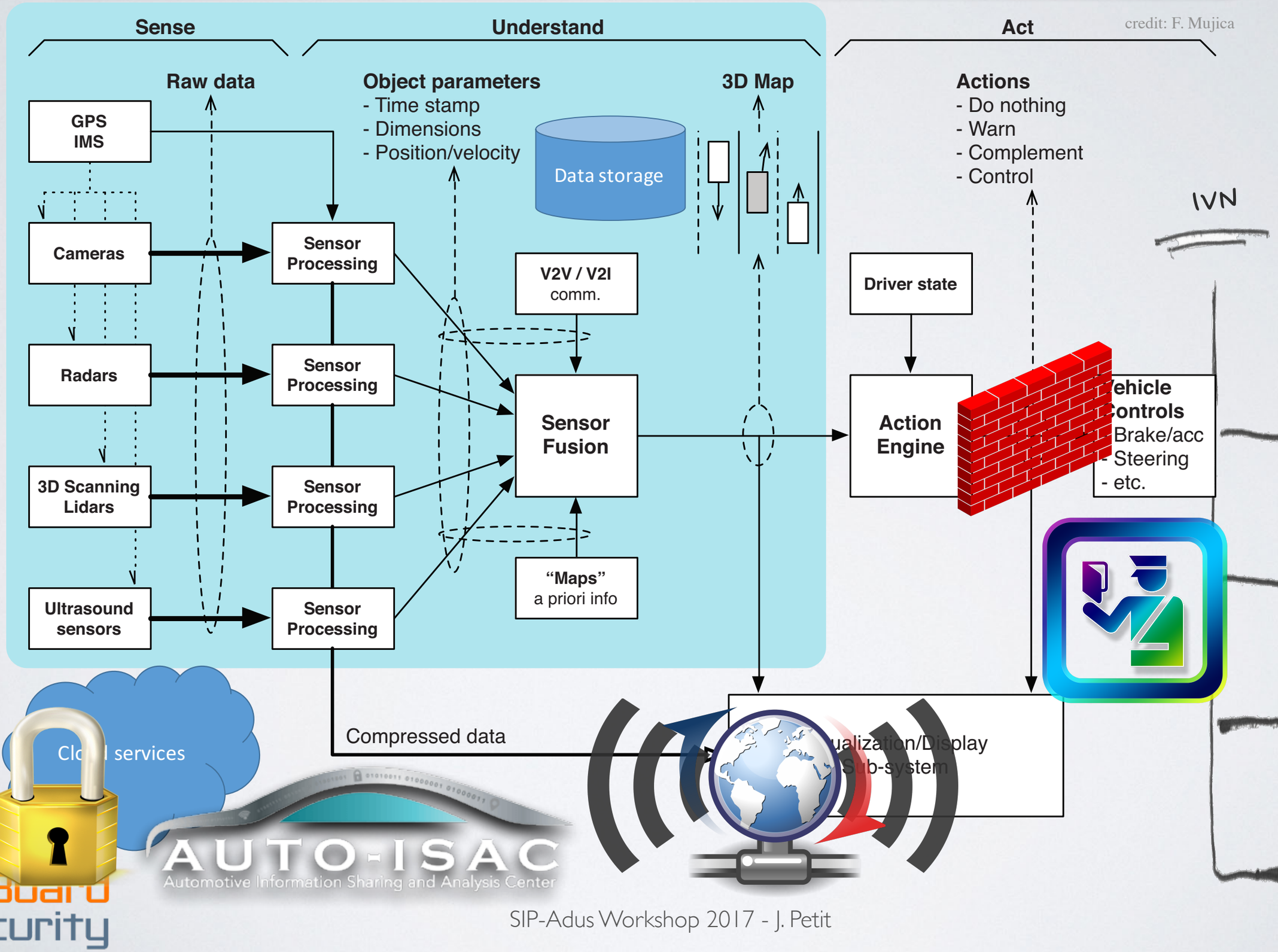


Current security efforts of automotive industry



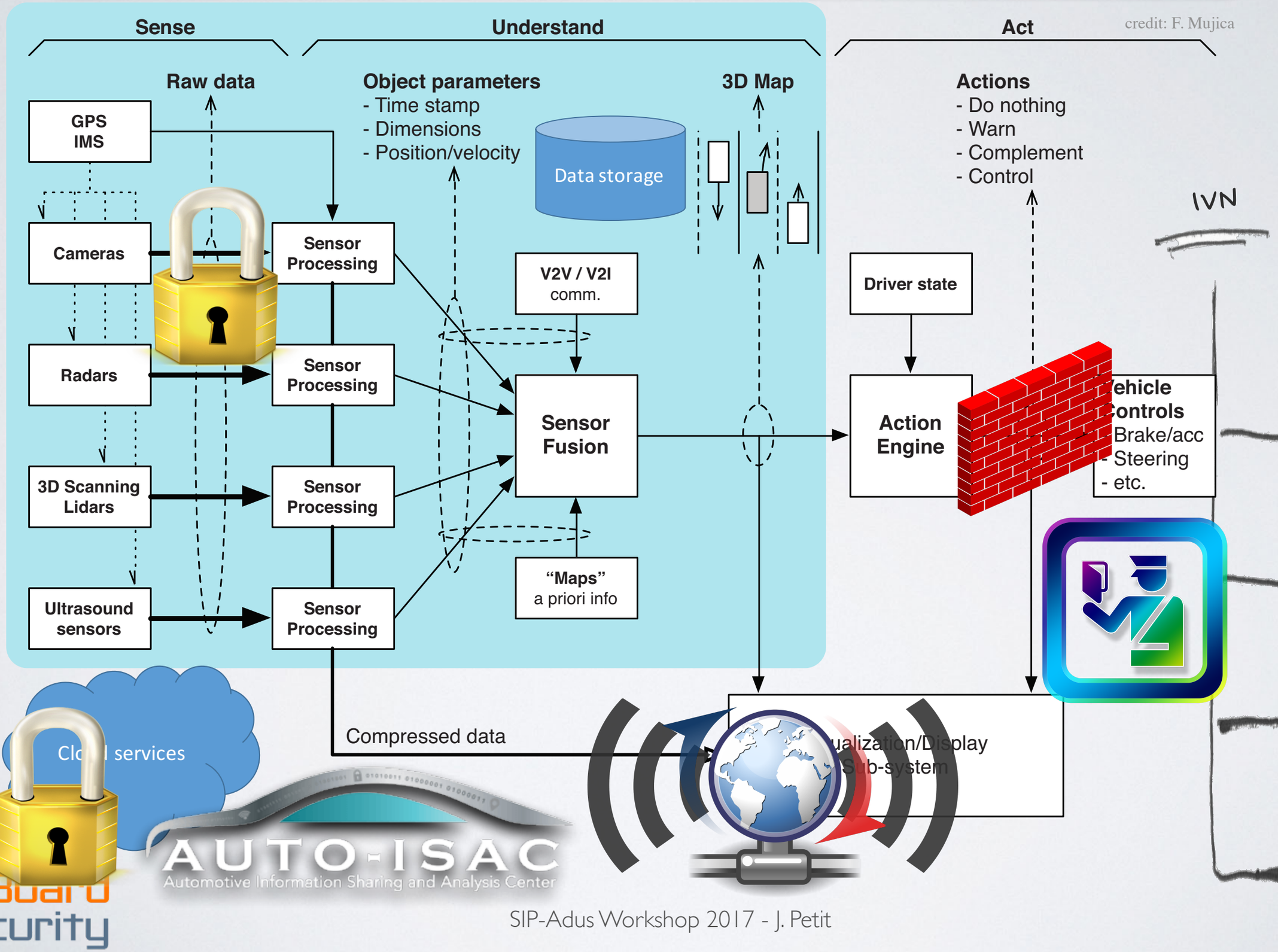
Current security efforts for **Automated Vehicle**

credit: F. Mujica



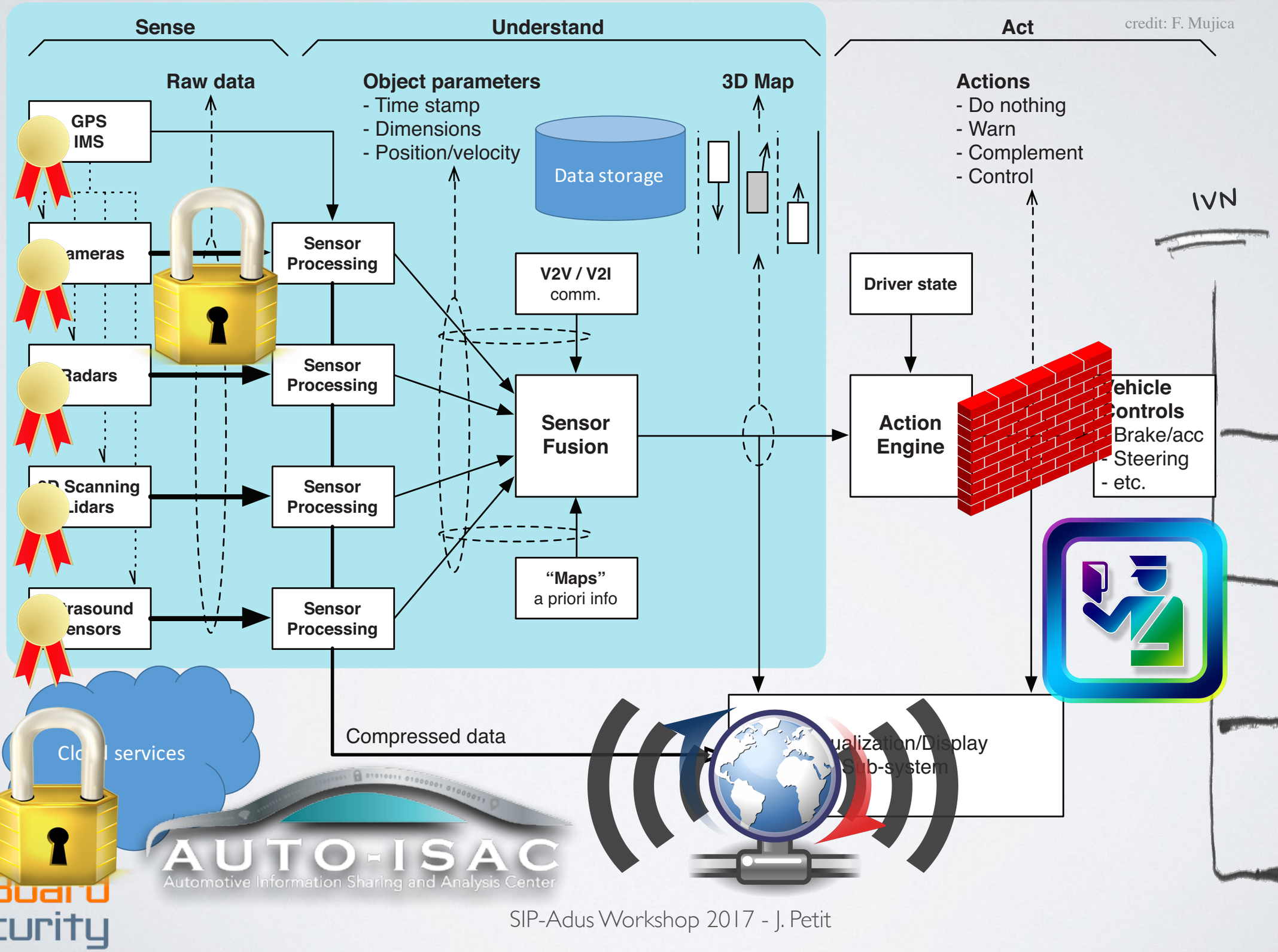
Current security efforts for **Automated Vehicle**

credit: F. Mujica



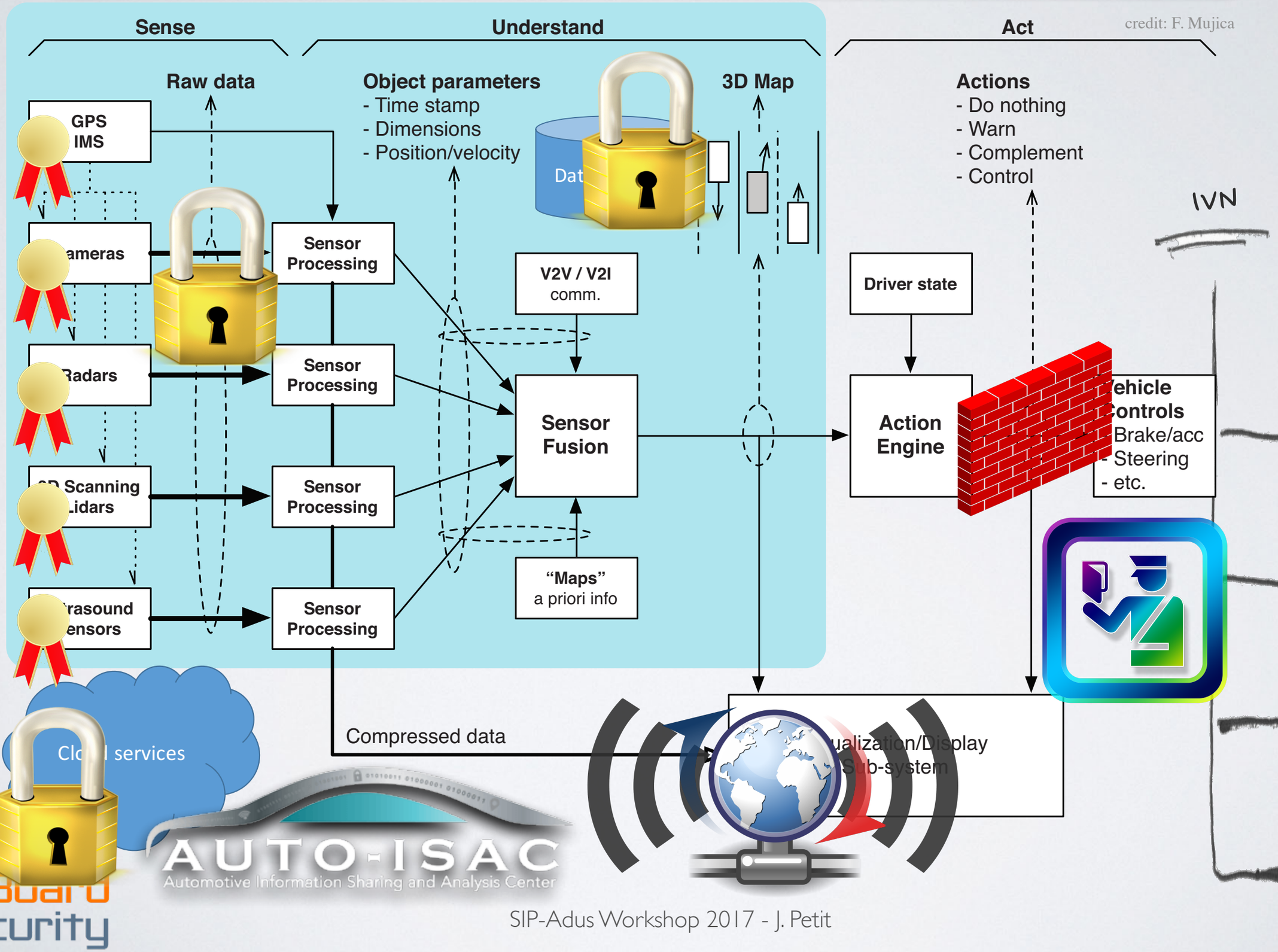
Current security efforts for **Automated Vehicle**

credit: F. Mujica



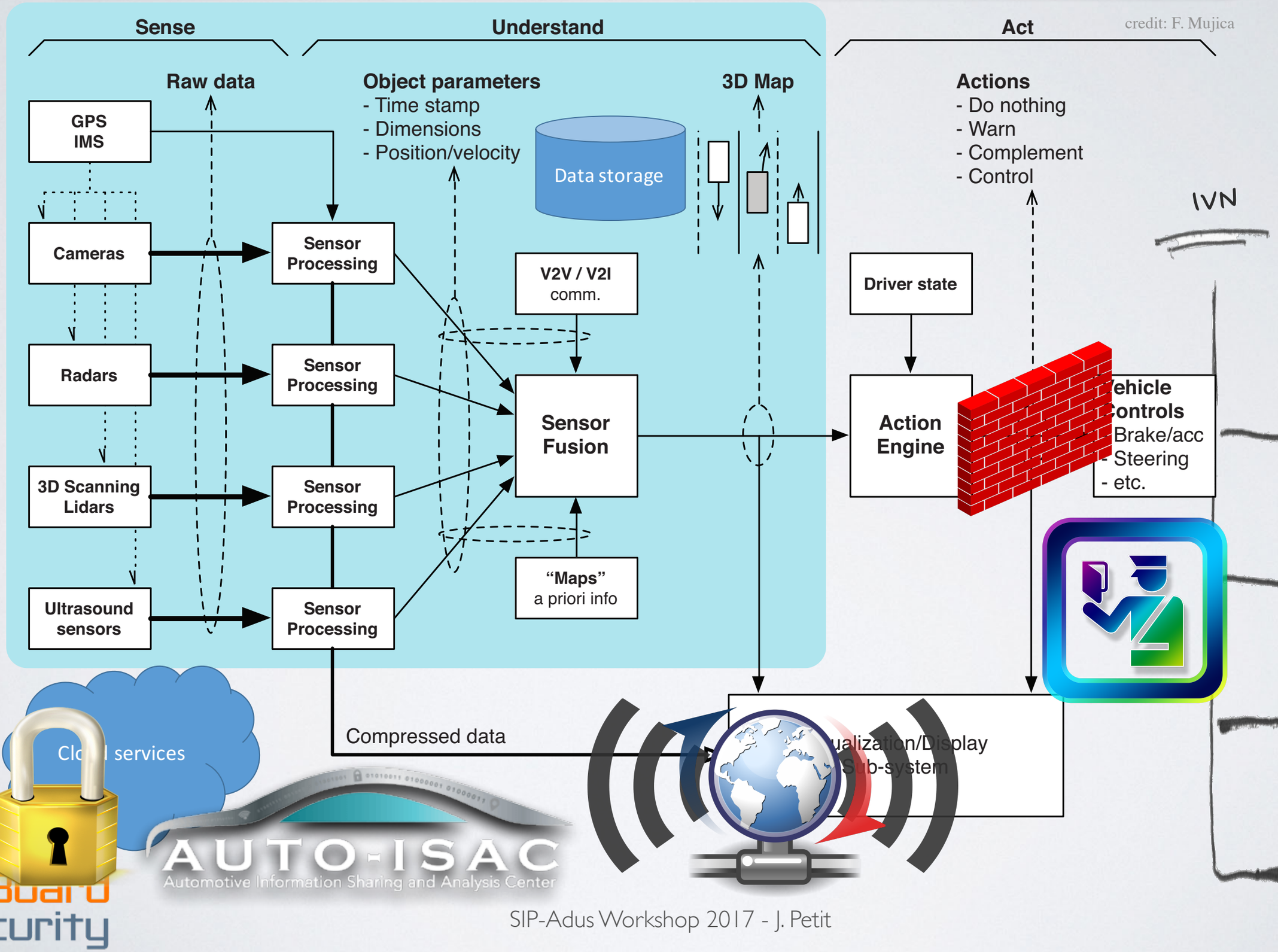
Current security efforts for **Automated Vehicle**

credit: F. Mujica

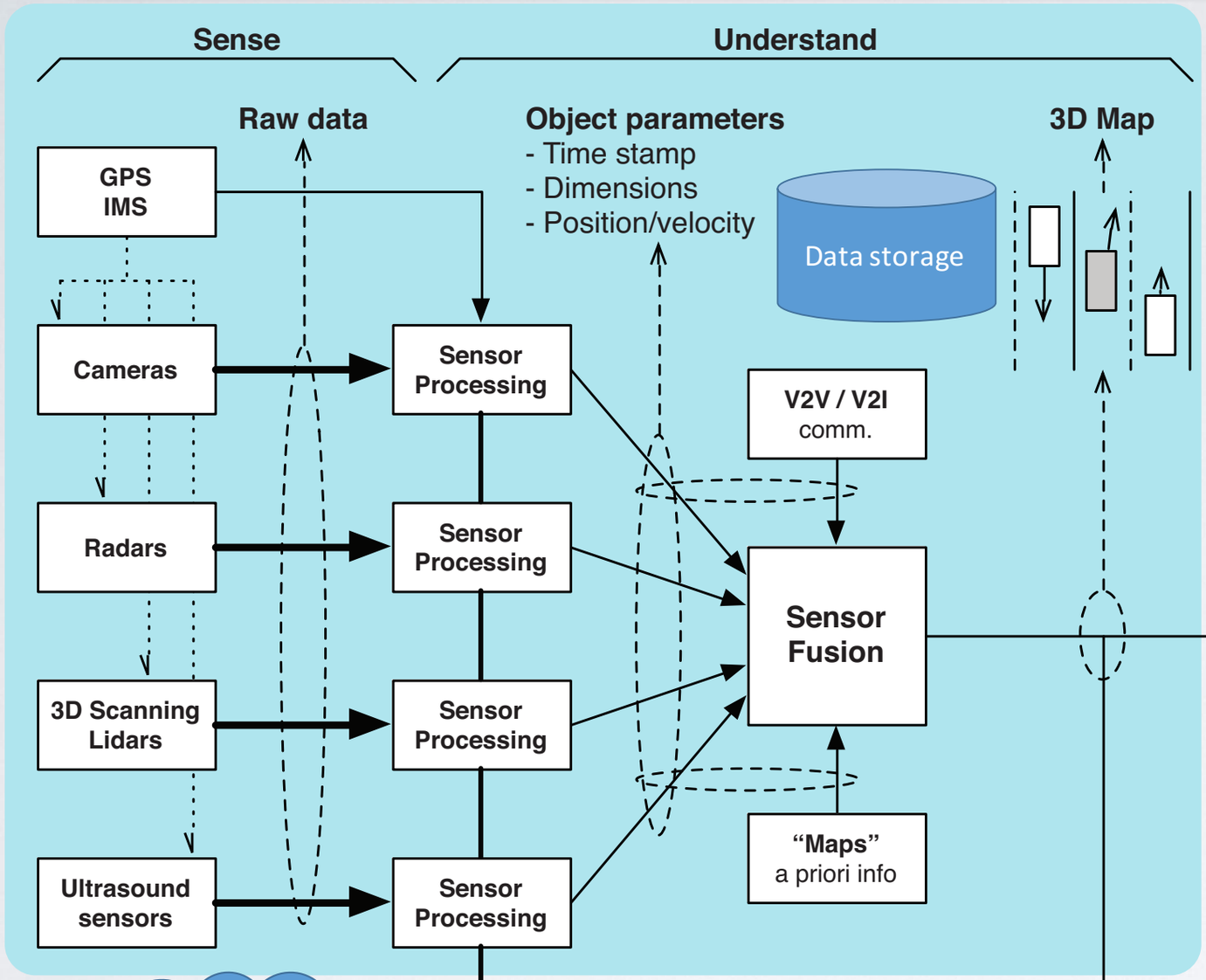


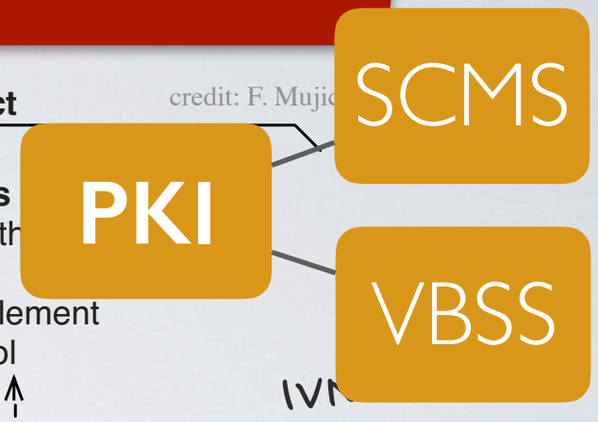
Current security efforts for **Connected Vehicles**

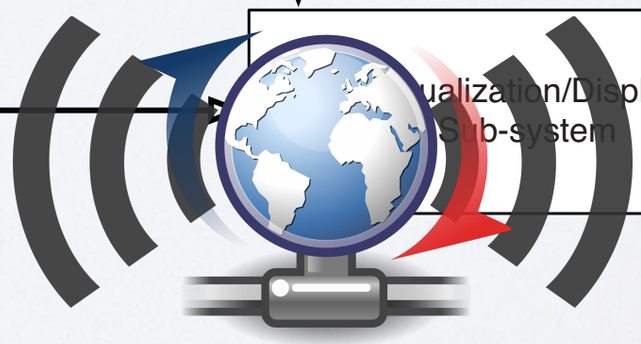
credit: F. Mujica

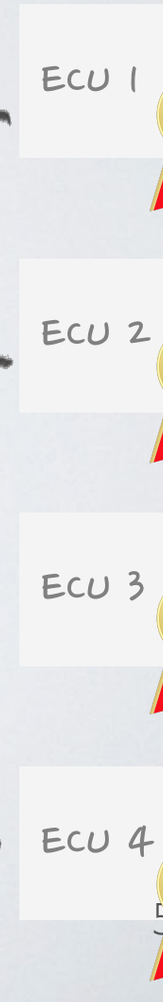


Current security efforts for **Connected Vehicles**

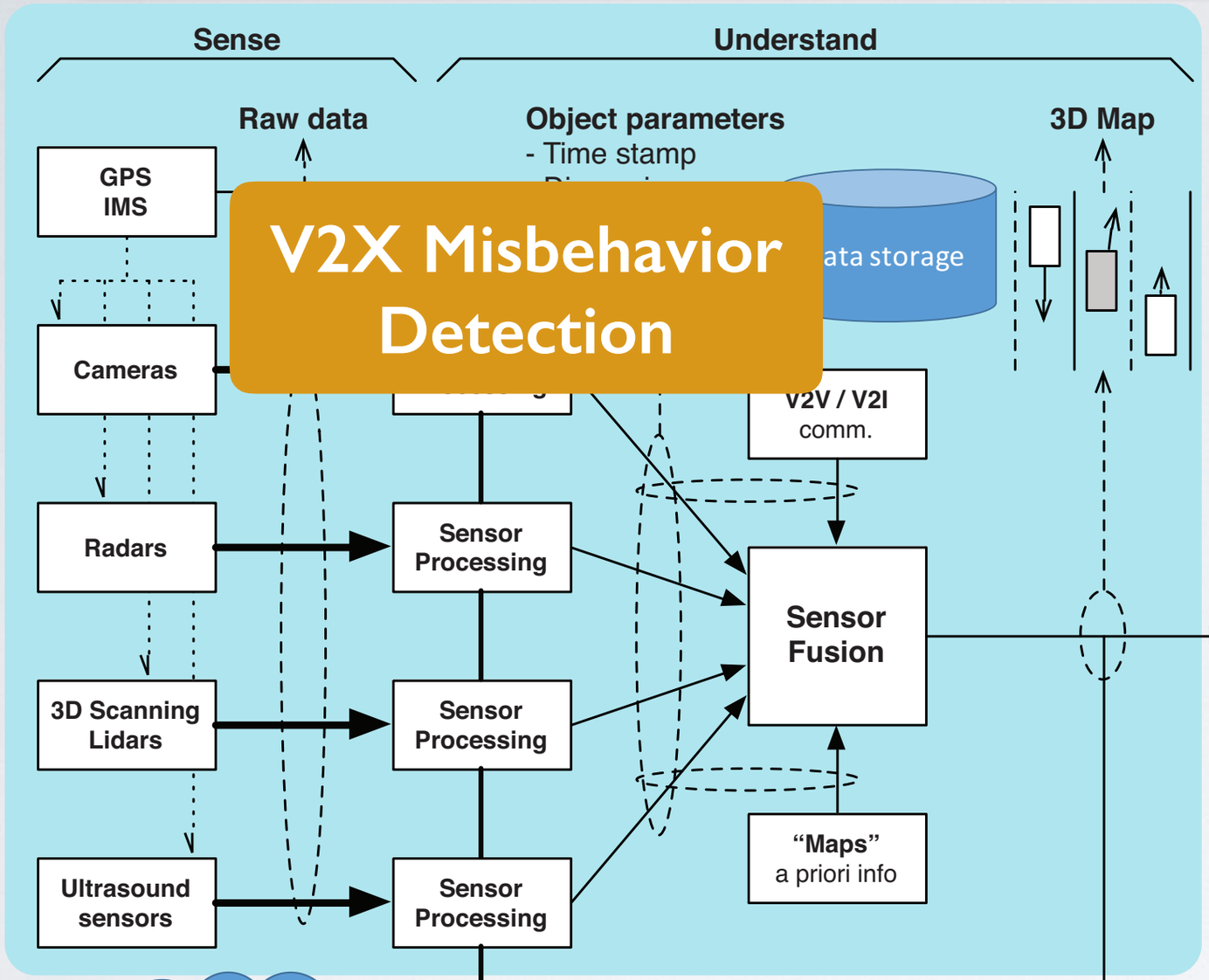








Current security efforts for **Connected Vehicles**



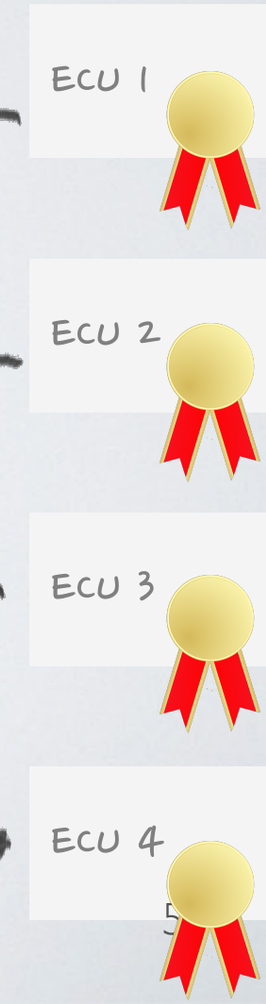
V2X Misbehavior Detection

SCMS

PKI

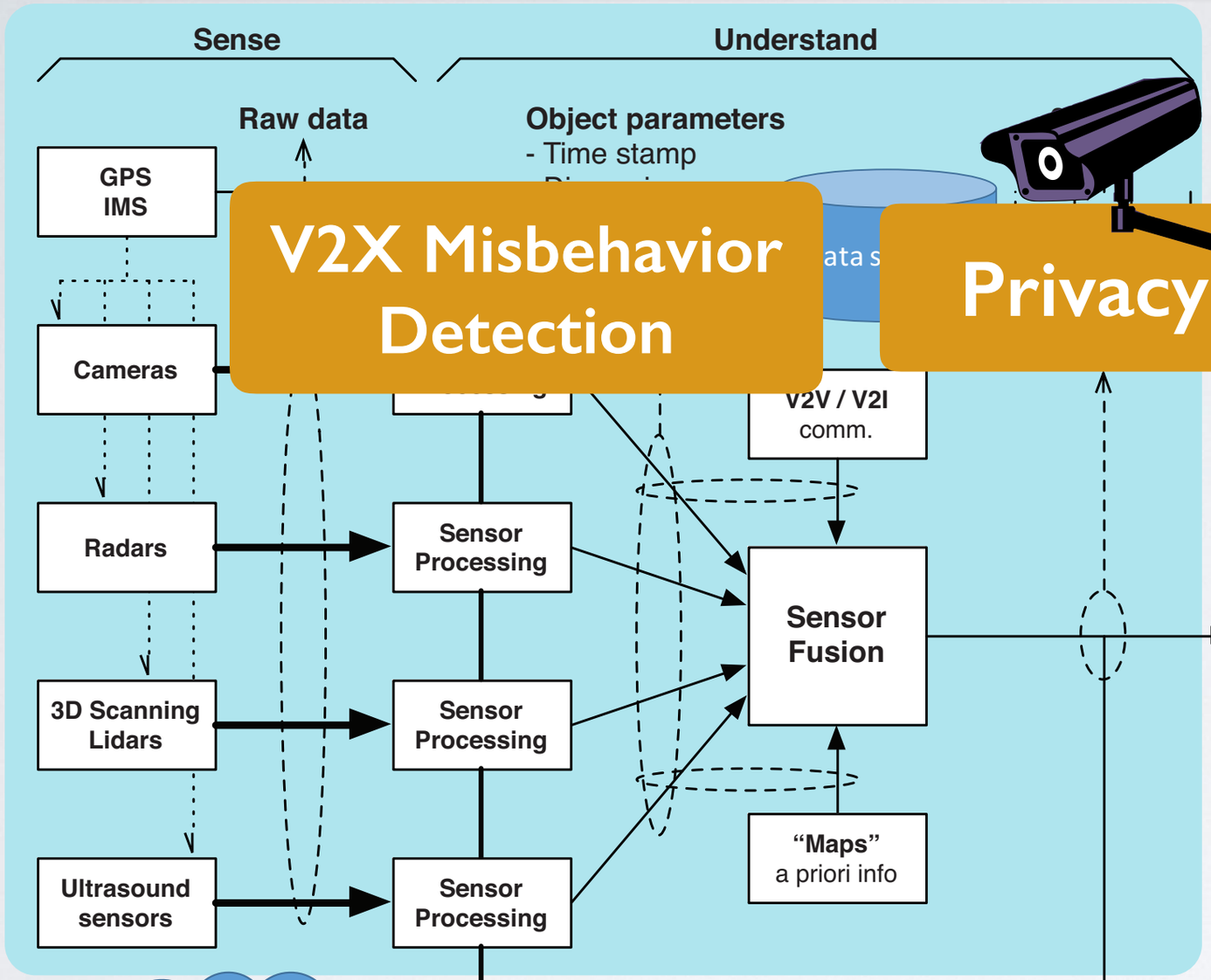
VBSS

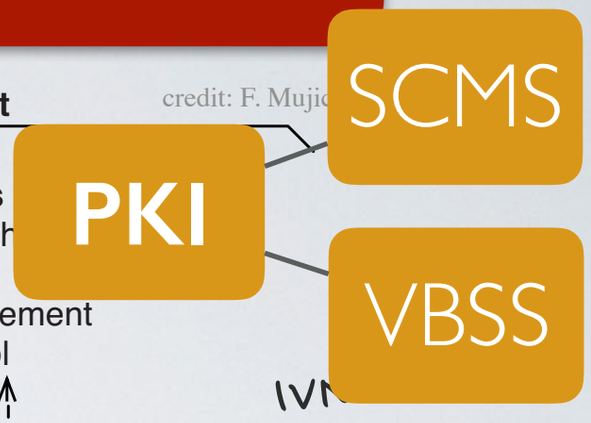
credit: F. Muji



onBoard Security

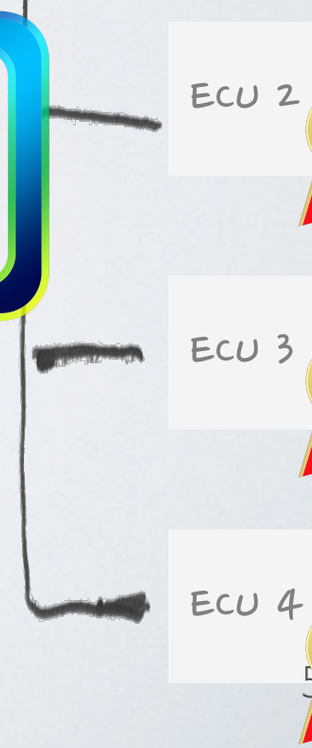
Current security efforts for **Connected Vehicles**

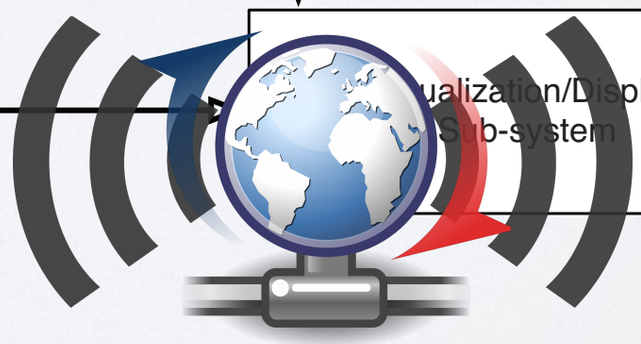


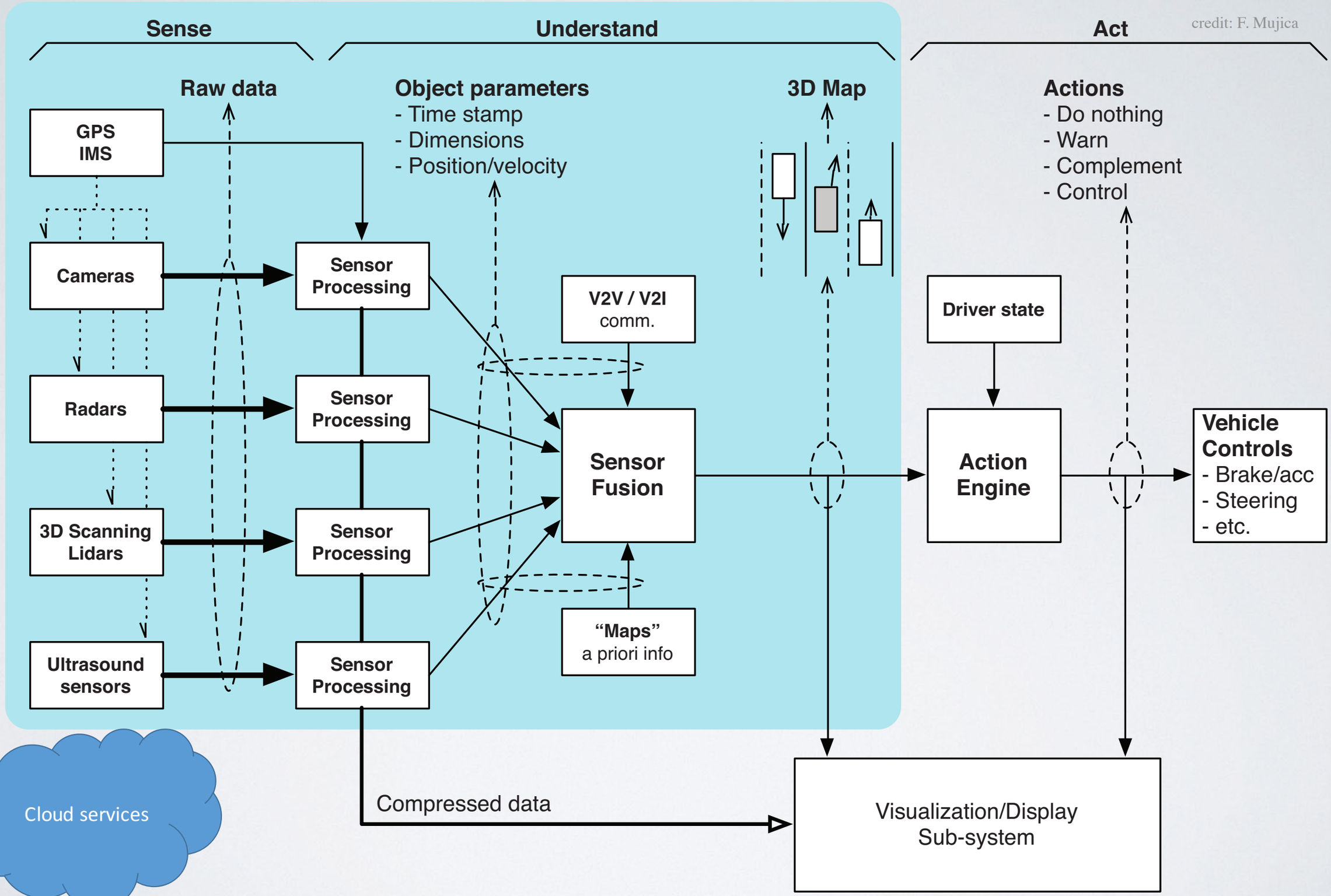


V2X Misbehavior Detection

Privacy






Sense
Understand
Act
credit: F. Mujica
Raw data
Object parameters
- Time stamp
- Dimensions
- Position/velocity
3D Map
Actions
- Do nothing
- Warn
- Complement
- Control
GPS
IMS
Cameras
Radars
3D Scanning
Lidars
Ultrasound
sensors
Sensor
Processing
Sensor
Processing
Sensor
Processing
Sensor
Processing
V2V / V2I
comm.
Sensor
Fusion
"Maps"
a priori info
Driver state
Action
Engine
Vehicle
Controls
- Brake/acc
- Steering
- etc.
Cloud services
Compressed data
Visualization/Display
Sub-system

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering
- etc.

Cloud services

Compressed data

Visualization/Display
Sub-system

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

Incident
detection

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering
- etc.

Cloud services

Compressed data

Visualization/Display
Sub-system

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

Incident
detection

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering

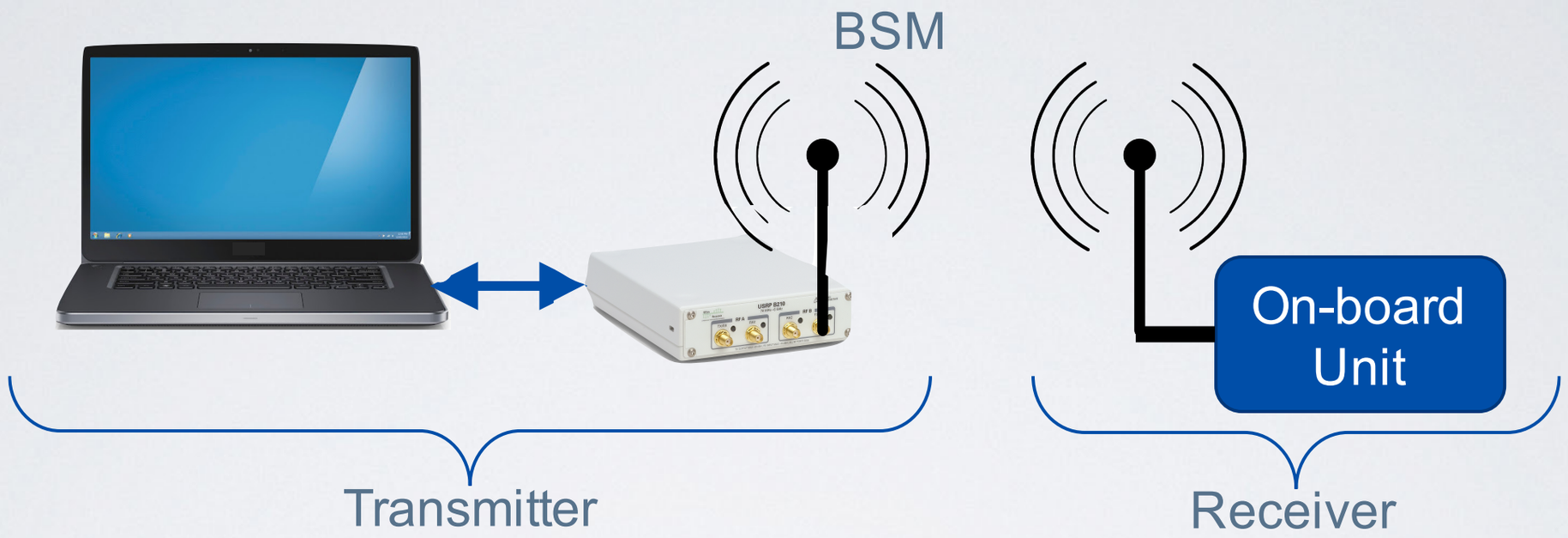
AutoPen

Cloud services

Compressed data

Visualization/Display
Sub-system

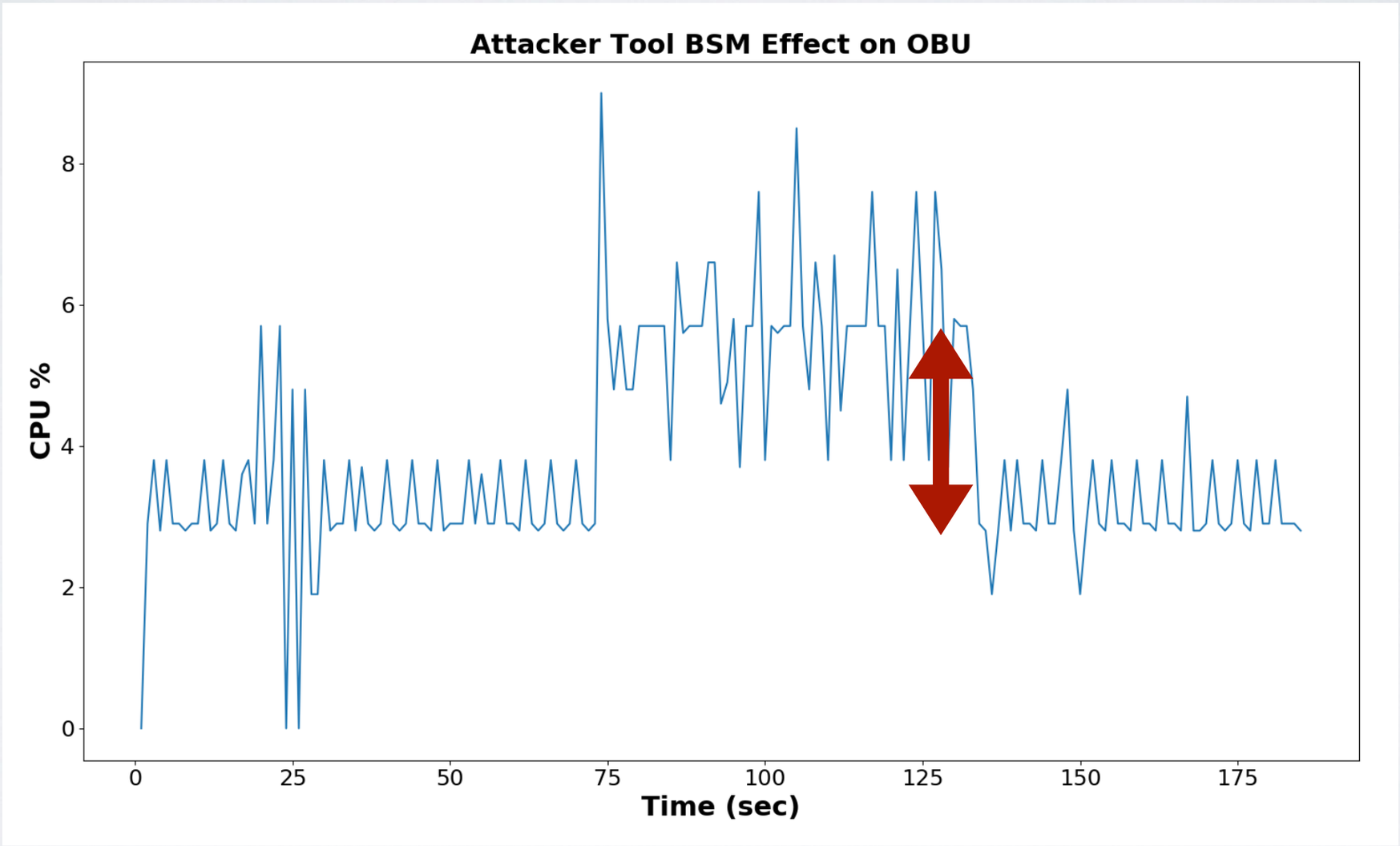
DSRC ATTACKER TOOL (1/4)



- **Goal**: Stress-test OBU implementation and detect vulnerabilities
- **Features**:
  - Works on a Raspberry Pi 3
  - Send BSMs: valid, invalid, signed, unsigned, etc.
  - Fuzzer
  - Monitor impact on receiver

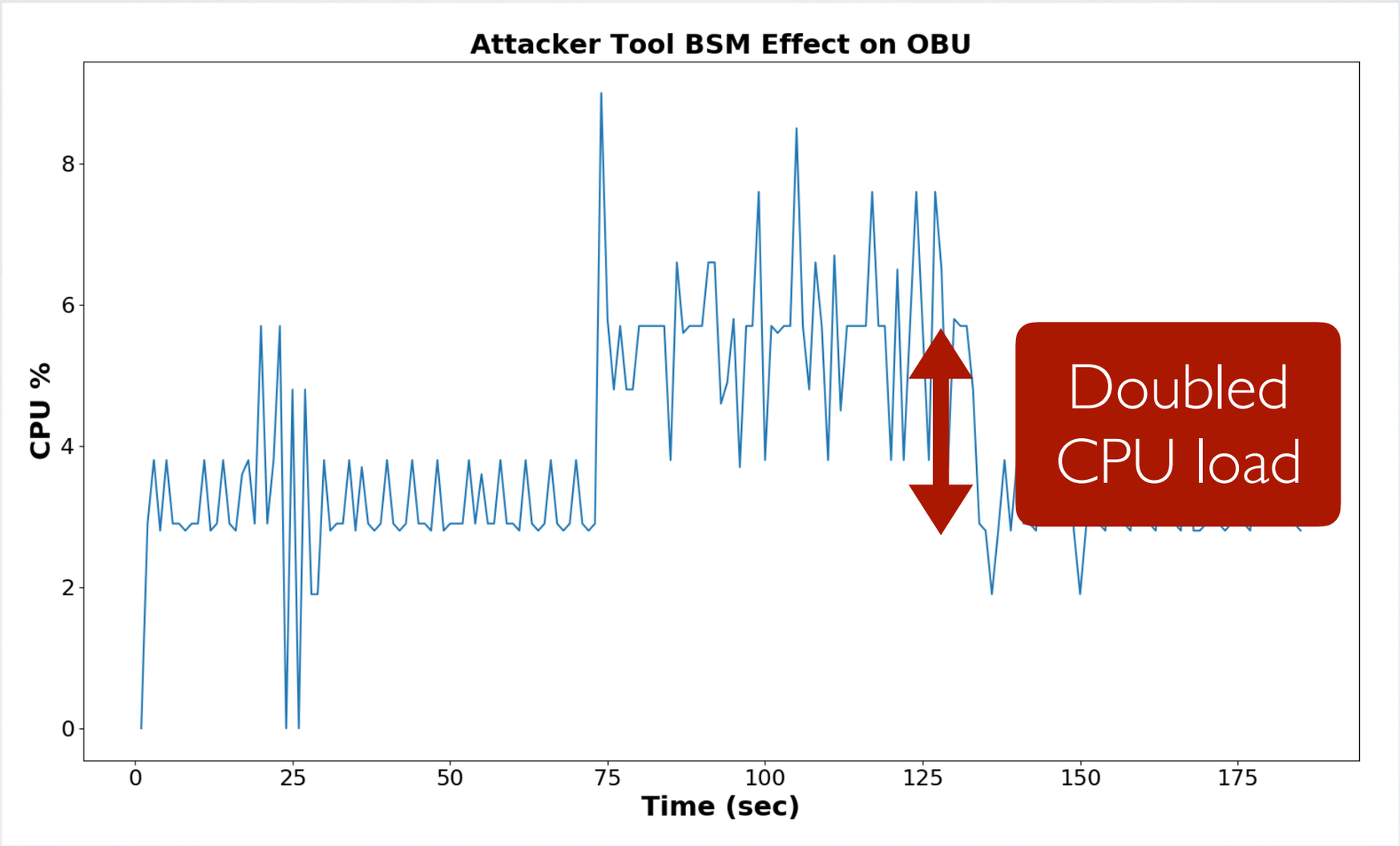
DSRC ATTACKER TOOL (2/4)

- Sending improperly signed BSMs



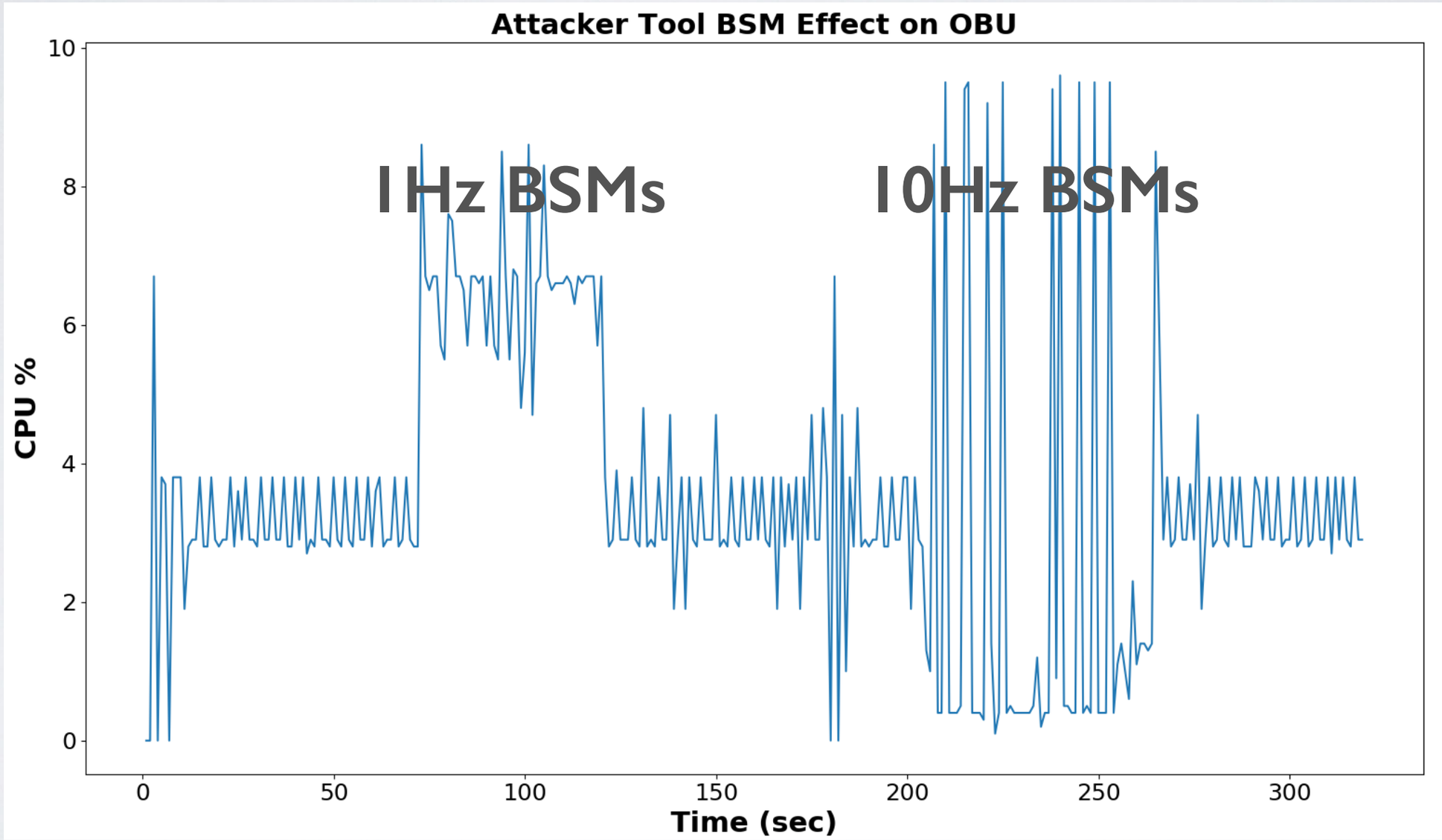
DSRC ATTACKER TOOL (2/4)

- Sending improperly signed BSMs



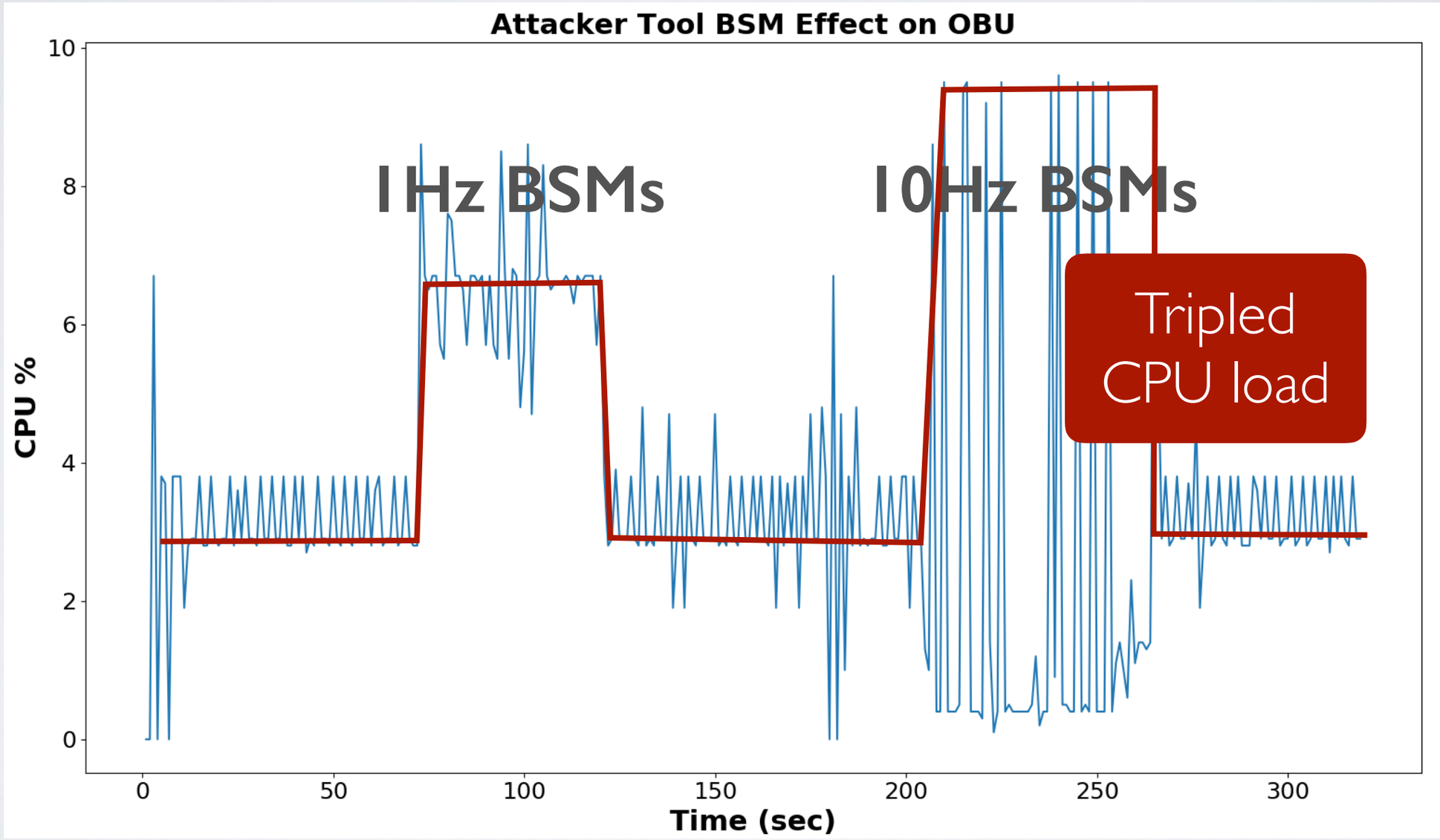
DSRC ATTACKER TOOL (3/4)

- Sending properly signed BSMs



DSRC ATTACKER TOOL (3/4)

- Sending properly signed BSMs

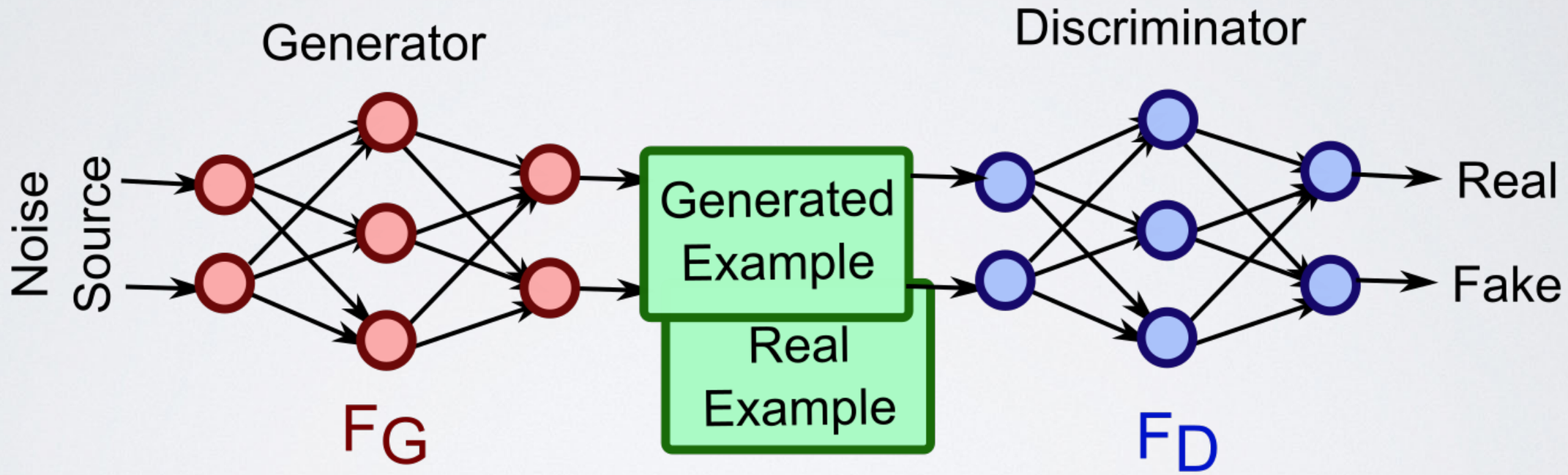


DSRC ATTACKER TOOL (4/4)

- **Next steps:**
  - Extend fuzzer, optimize code
  - Need access to CV applications
  - Field tests
  - Post on GitHub :-)
  - Port on sUAV

DEEP LEARNING FOR MISBEHAVIOR DETECTION

- Generative Adversarial Network (GAN)



- Can a GAN generate fake BSMs? (think attacker tool)
- Can a GAN discriminate fake BSMs? (detection)

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

Incident
detection

AutoPen

Cloud services

Compressed data

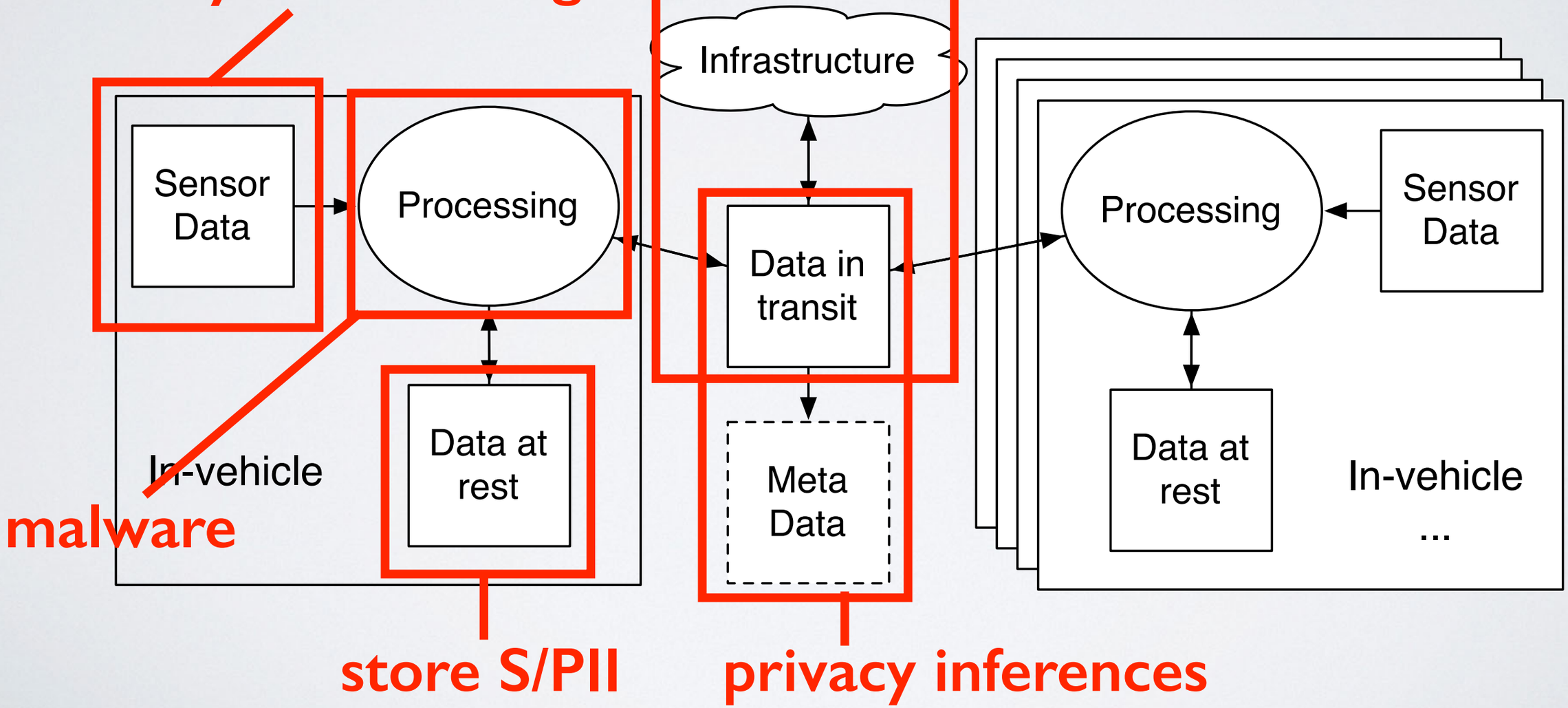
Visualization/Display
Sub-system

onBoard
Security

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

location tracking, break forward secrecy

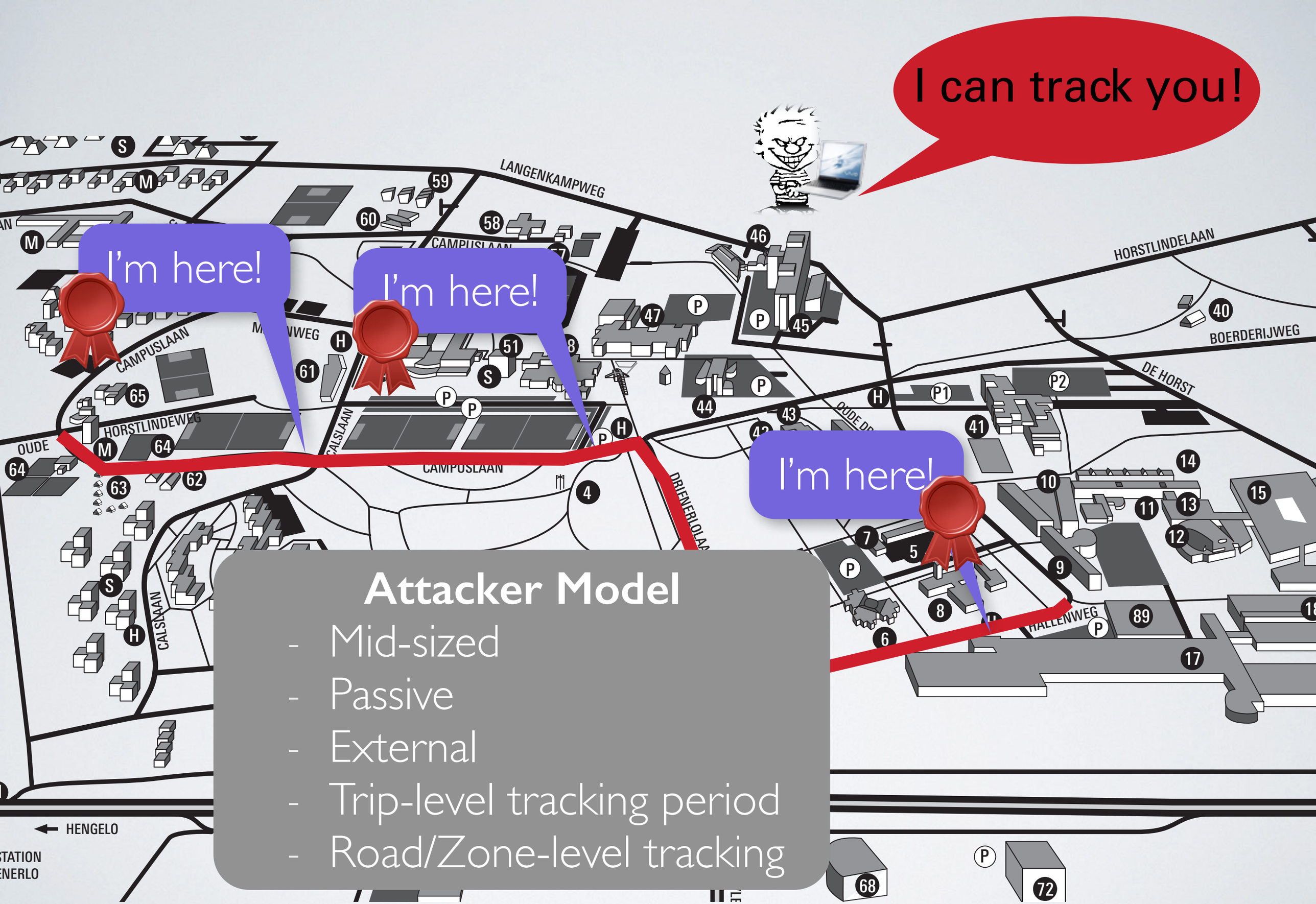


malware

store S/PII

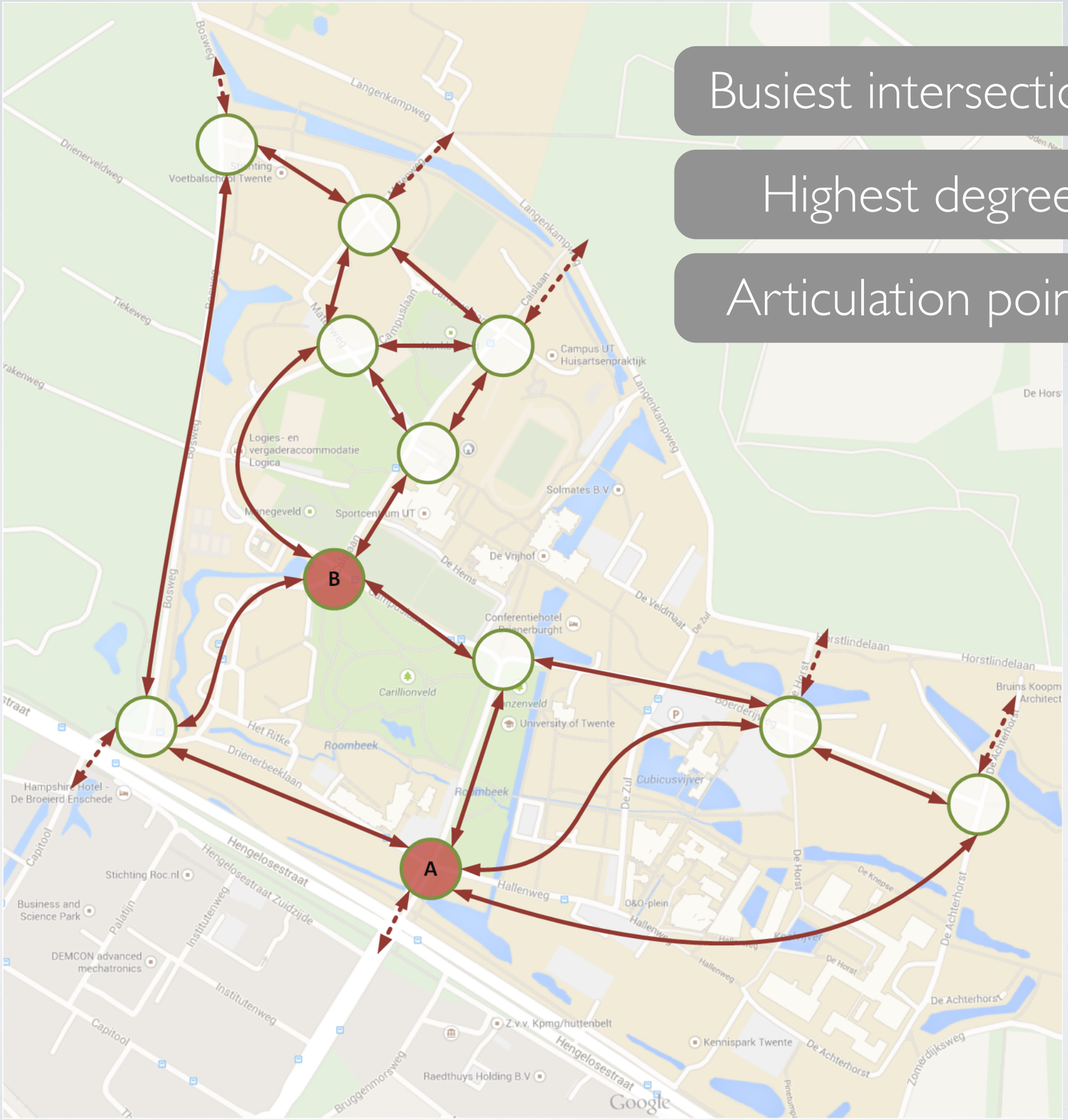
privacy inferences

J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.



Attacker Model

- Mid-sized
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking

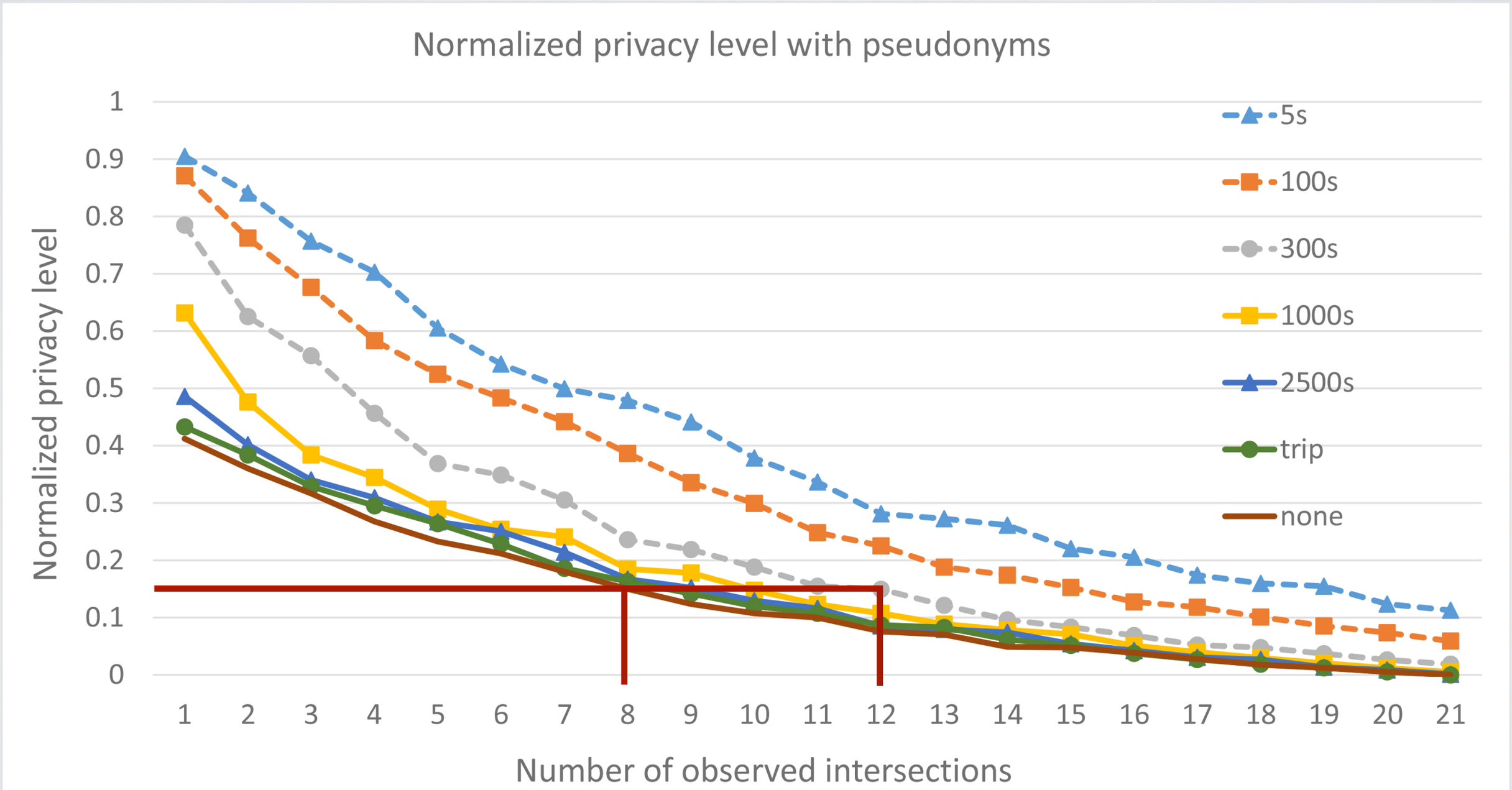


Busiest intersections

Highest degree

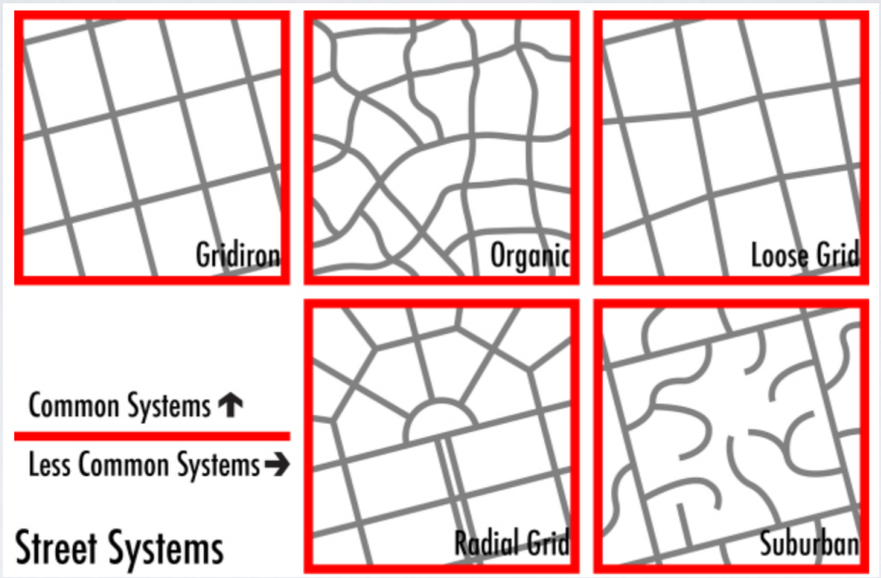
Articulation points

PSEUDONYM CHANGE STRATEGIES



PRIVACY-PRESERVING ROAD NETWORK?

1. Identify types of road network



2. Classify cities (150 to date)

3. Simulate V2X and assess privacy

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

Incident
detection

AutoPen

Cloud services

Compressed data

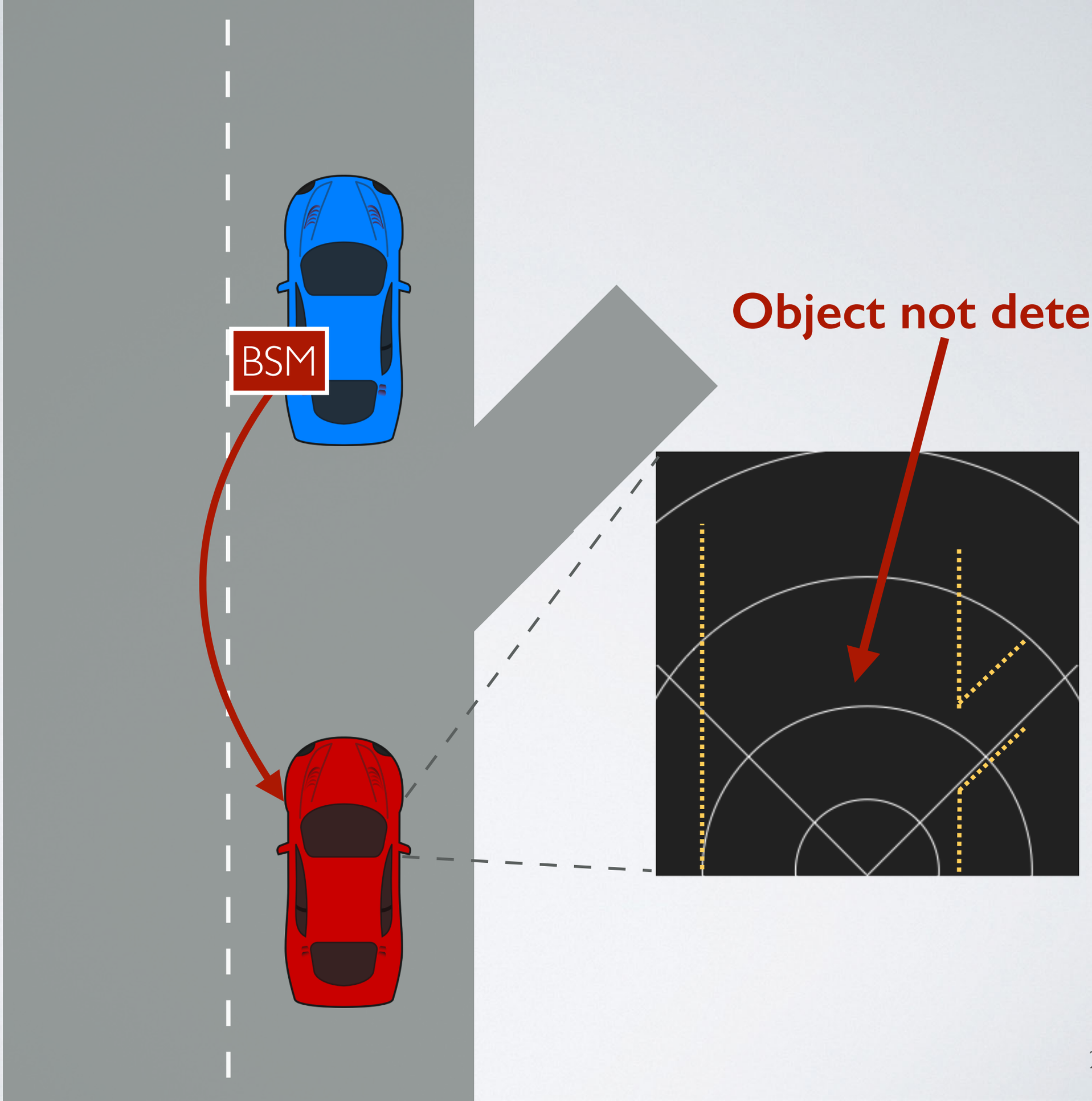
Visualization/Display
Sub-system

INCIDENT DETECTION

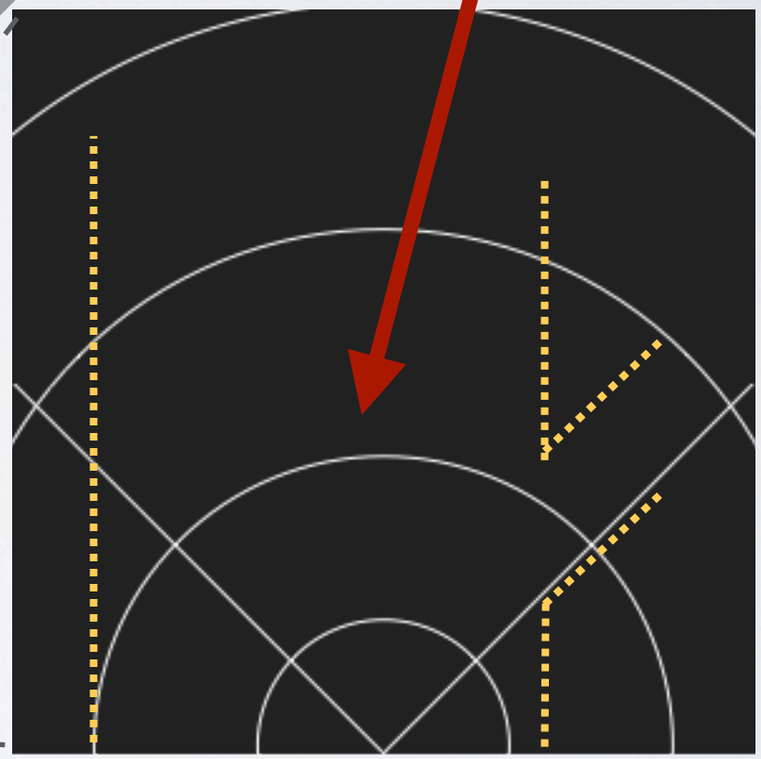
- Incident = malicious attack OR faulty sensor (local or remote)

- Idea 1: Using V2X to detect faulty local sensors

- Idea 2: Sensor fusion to detect attacks


BSM
Object not detected

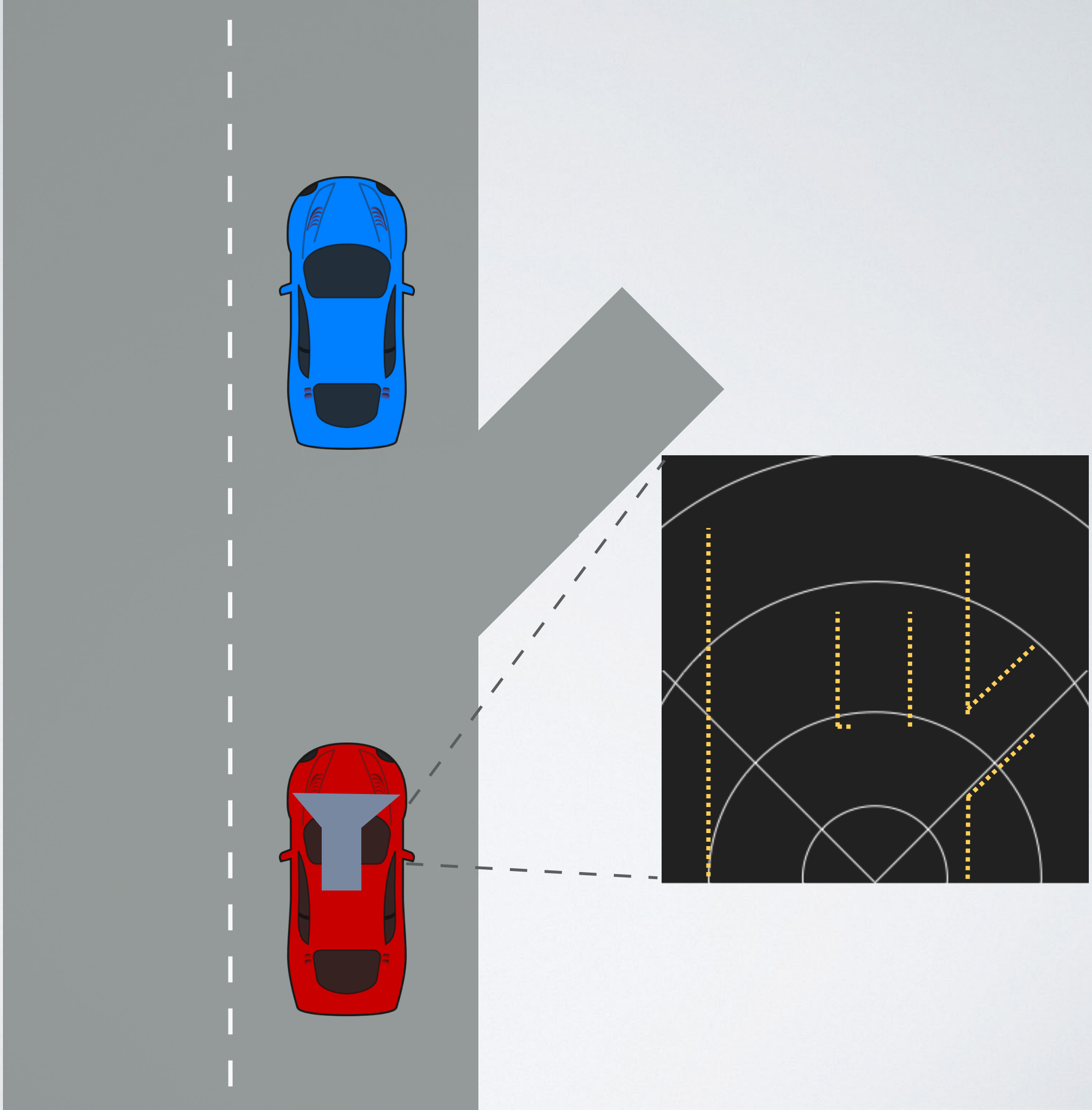
Object not detected



BSMs received!

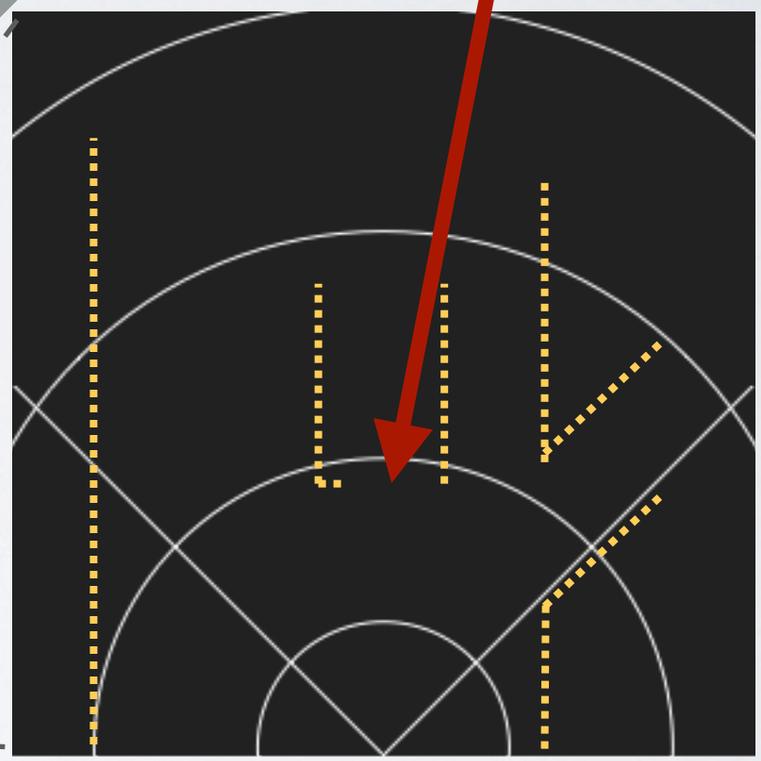
BSM

Inconsistency between sensor and V2X!



Partial jamming

Missing chirp responses



Object detected!

Inconsistency between RADAR and Camera!

credit: F. Mujica

Sense

Understand

Act

Raw data

Object parameters
- Time stamp
- Dimensions
- Positi

3D Map

Actions

GPS
IMS

Cameras

Radars

3D Scanning
Lidars

Ultrasound
sensors

Sensor
Processing

Sensor
Processing

Sensor
Processing

Sensor
Processing

V2V / V2I
comm.

Sensor
Fusion

"Maps"
a priori info

Action
Engine

Vehicle
Controls
- Brake/acc
- Steering

Privacy

DSRC Attacker Tool

Deep Learning for
Misbehavior Detection

Incident
detection

AutoPen

Cloud services

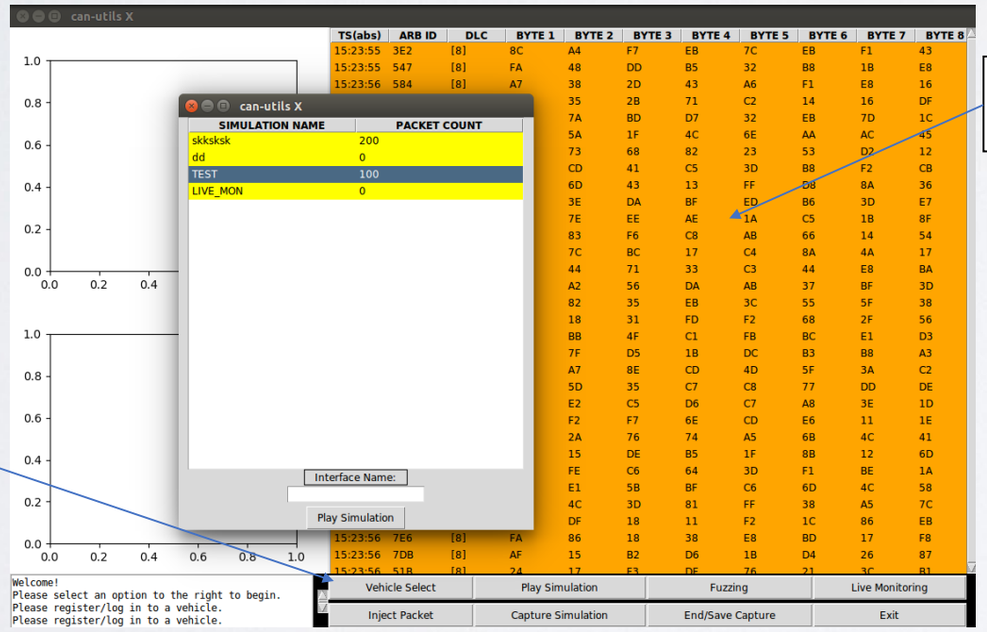
Compressed data

Visualization/Display
Sub-system

onBoard Security

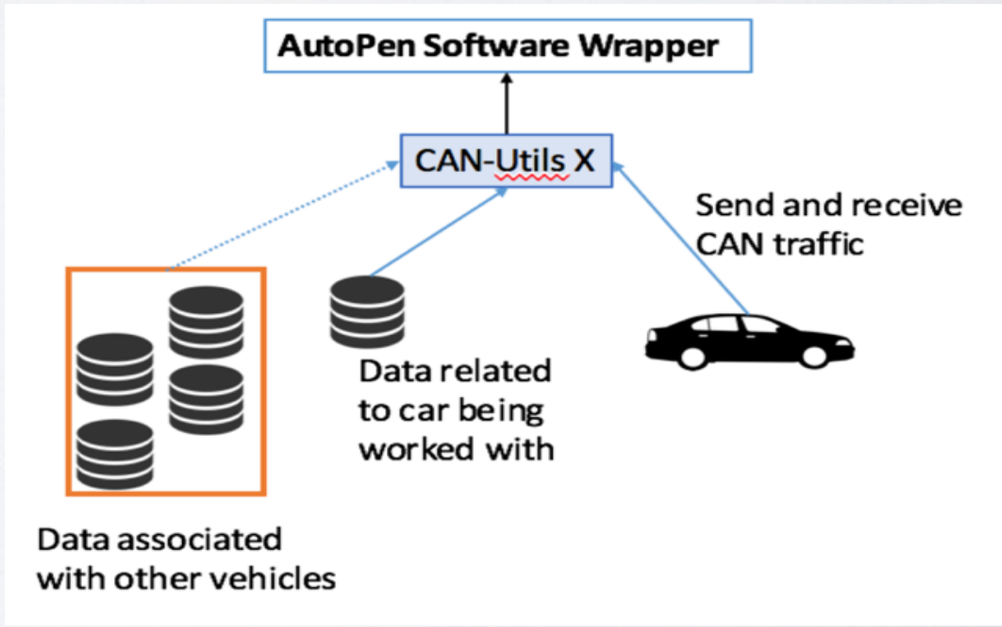
AUTOMOTIVE PENETRATION TESTING TOOL (AUTOPEN)

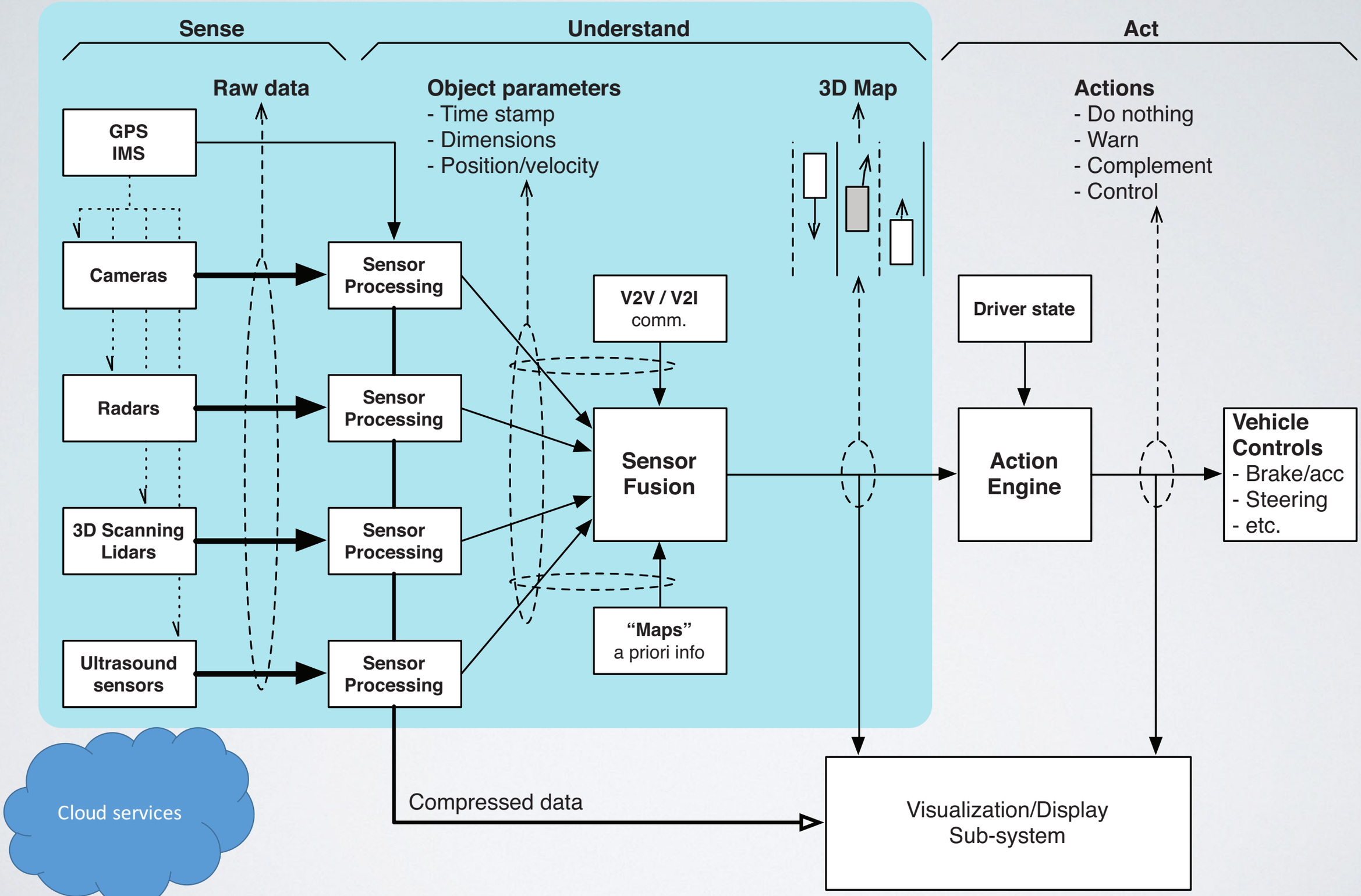
- In collaboration with Boston University
- Facilitate pentesting (CAN, RF)
- **Correlate CAN and RF signals**
- Open source



Live Network Traffic Monitoring

Penetration Testing Capabilities



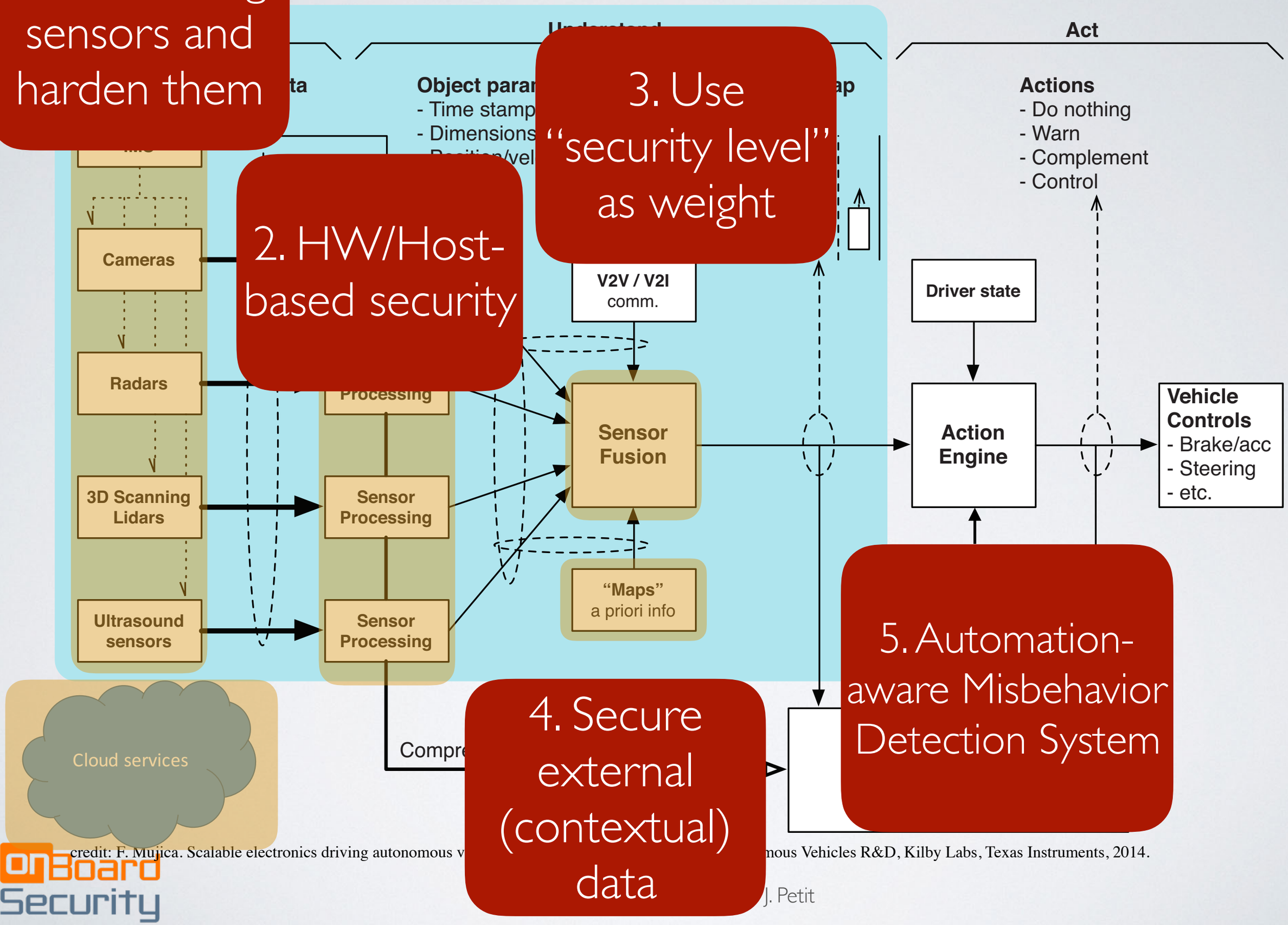


credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

3. Use "security level" as weight



4. Secure external (contextual) data

5. Automation-aware Misbehavior Detection System

credit: F. Mujica. Scalable electronics driving autonomous v … mous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

DSRC Attacker Tool

AutoPen

Host-Based Security

3. Use "security level" as weight

Act

Actions
- Do nothing
- Warn
- Complement
- Control

Object para
- Time stamp
- Dimensions

V2V / V2I comm.

Driver state

Action Engine

Vehicle Controls
- Brake/acc
- Steering
- etc.

Radars

3D Scanning Lidars

Ultrasound sensors

Processing

Sensor Processing

Sensor Fu

"Maps" a priori info

Incident detection

Deep Learning

Pseudonym management

cure external (contextual) data

5. Automation-aware Misbehavior Detection System

Cloud services

credit: F. Mujica. Scalable electronics driving autonomous v ... mous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

Questions & Answers

Jonathan Petit
jpetit@onboardsecurity.com

OnBoard Security