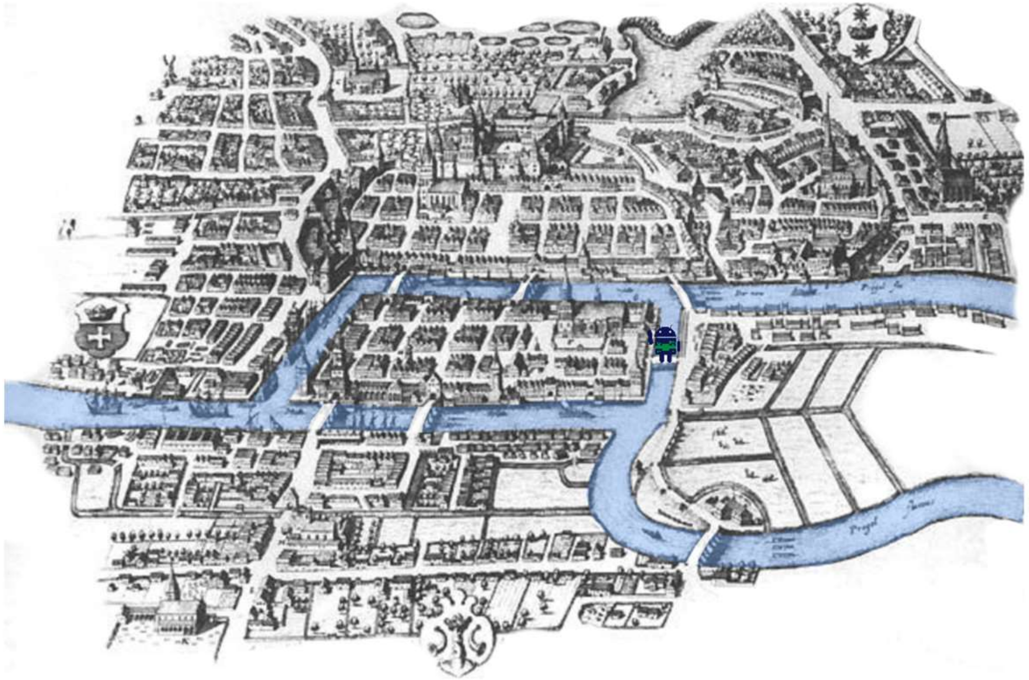
ISTITUTO DI INFORMATICA E TELEMATICA



IoV SECURITY

Internet of Vehicles: security challenges and open issues

Marco De Vincenzi

Mauriana Pesaresi Seminar, March 2023

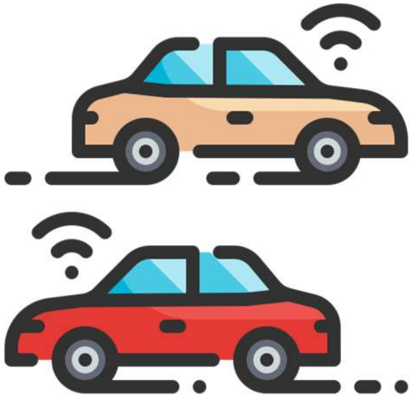
AGENDA

- INTERNET OF VEHICLES (IoV) INTRODUCTION
- SECURITY ATTACKS
- OPEN ISSUES

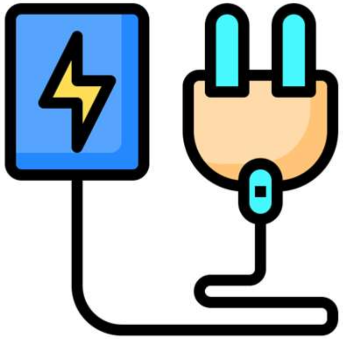
AUTOMOTIVE REVOLUTION

4 MAIN REINFORCING TRENDS (ACES)

Autonomous Driving



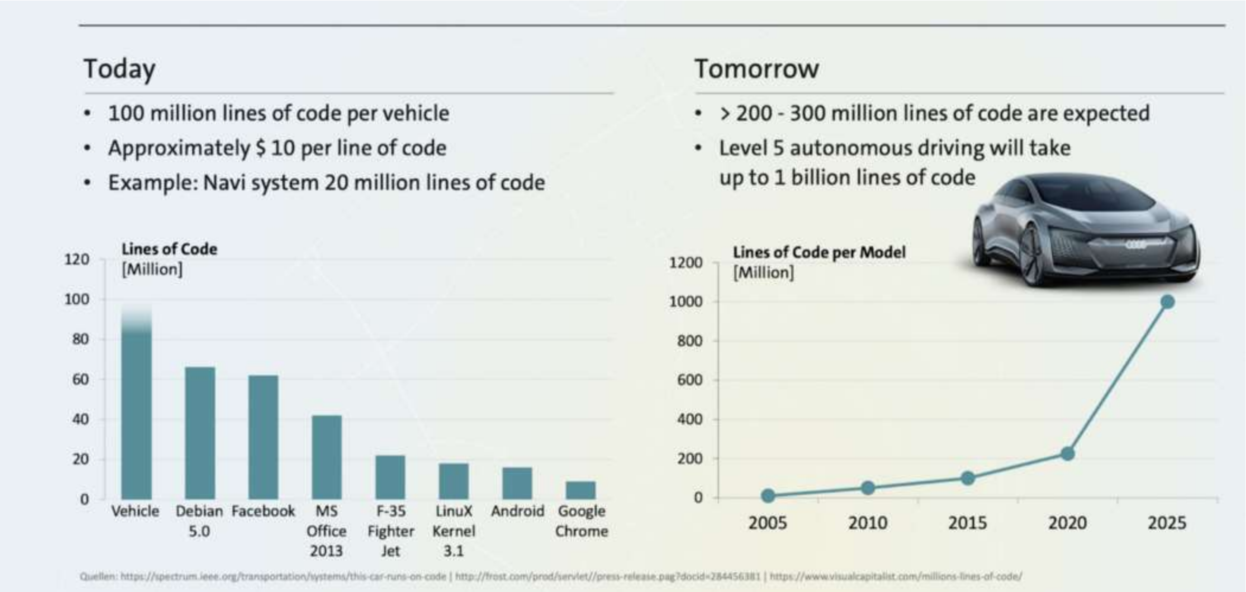
Connected Vehicles



Electrification

Sharing Mobility

VEHICLES TODAY



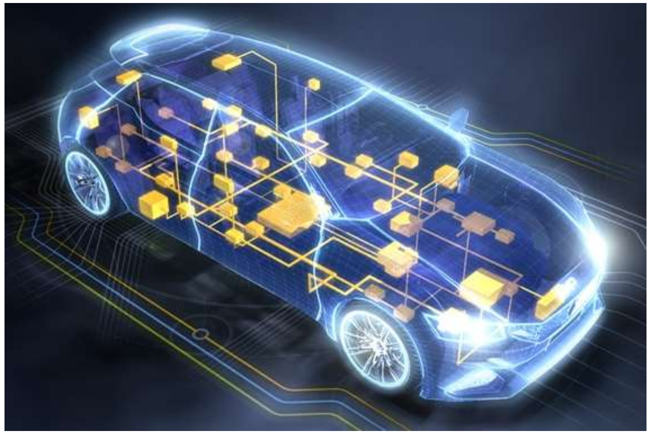
Today

- 100 million lines of code per vehicle
- Approximately $ 10 per line of code
- Example: Navi system 20 million lines of code

Tomorrow

- > 200 - 300 million lines of code are expected
- Level 5 autonomous driving will take up to 1 billion lines of code

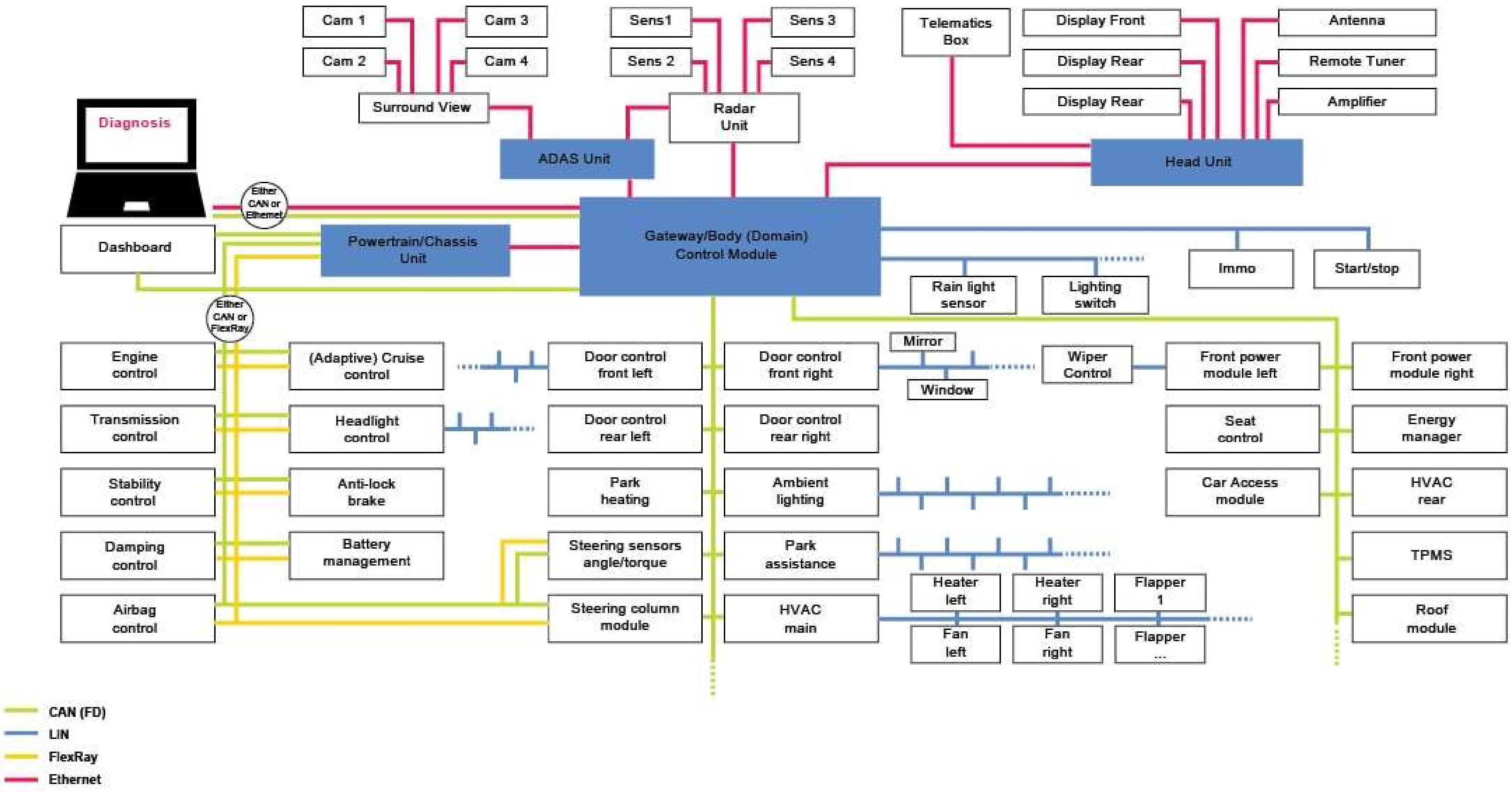
Quellen: https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code | http://frost.com/prod/servlet//press-release.pag?docid=284456381 | https://www.visualcapitalist.com/millions-lines-of-code/



Reference: https://mondaynote.com/code-on-wheels-a4715926b2a2

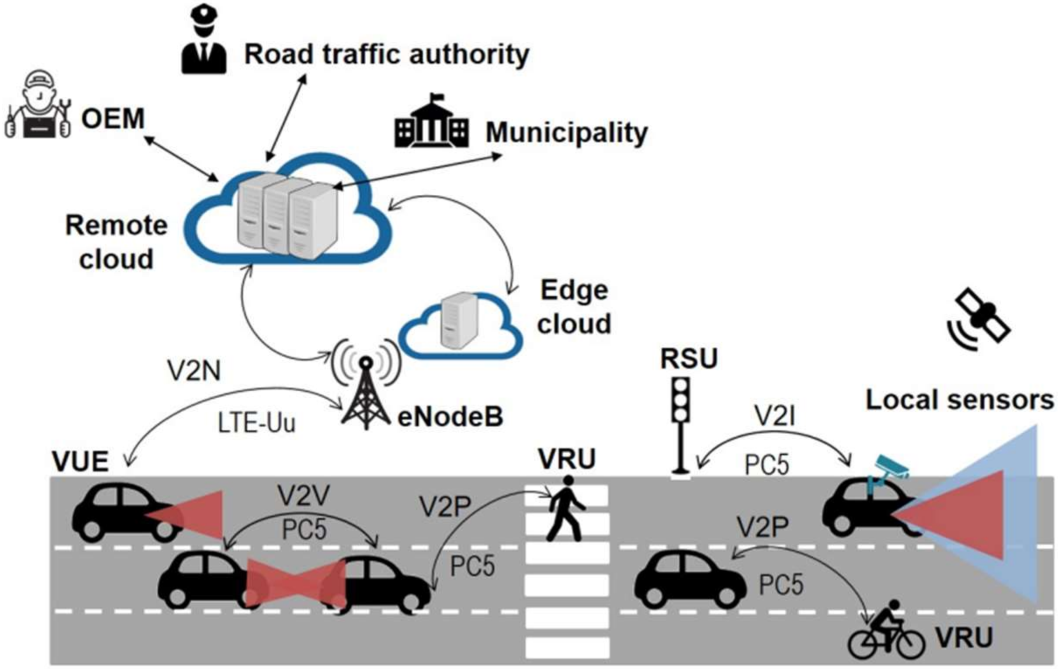
Reference: https://www.nxp.com/products/interfaces/in-vehicle-network:WIRED-CONNECTIVITY-AUTO

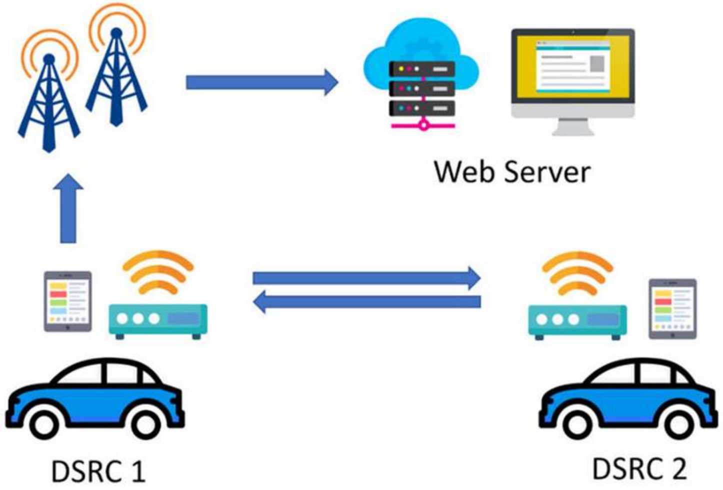
In-Vehicle Network - Example



Reference: https://www.nxp.com/products/interfaces/in-vehicle-network:WIRED-CONNECTIVITY-AUTO

INTERNET OF VEHICLES (IoV)





Reference: https://www.5gitaly.eu/2018/wp-content/uploads/2019/01/5G-Italy-White-eBook-5G-for-V2X-Communications.pdf.

Why is vehicle connectivity complex?

- Different nodes (vehicles, antennas, satellites, data centres, …) in a mixed static/dynamic environment;
- Impact on safety;
- Proprietary solutions;
- Standard solutions to be defined;
- Cost pressure;
- …

V2…

V2X: Vehicle-to-Everything

V2V: Vehicle-to-Vehicle

V2H: Vehicle-to-Home

V2P: Vehicle-to-Pedestrian

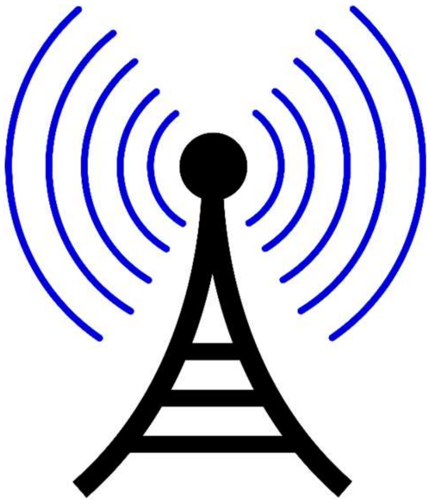
V2D: Vehicle-to-Device

V2I: Vehicle-to-Infrastructure

V2N: Vehicle-to-Network

V2R: Vehicle-to-Road-Side-Unit

V2G: Vehicle-to-Grid



ACRONYMS

ITS: Intelligent Transportation System

RSU: Road Side Unit

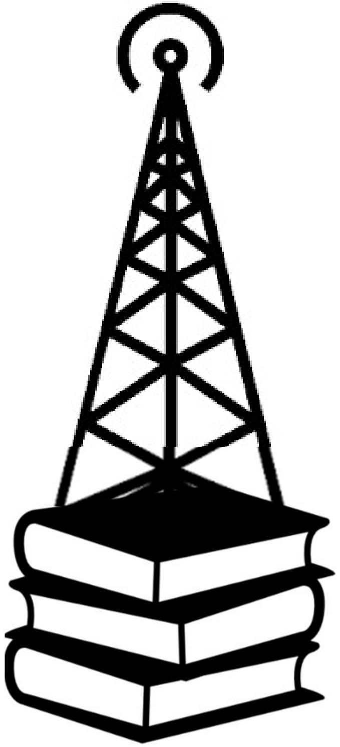
OBU: On-Board Unit

GPS: Global Positioning System (USA) [Glonass (Russia), Beidou (China), and Galileo (Europe)]

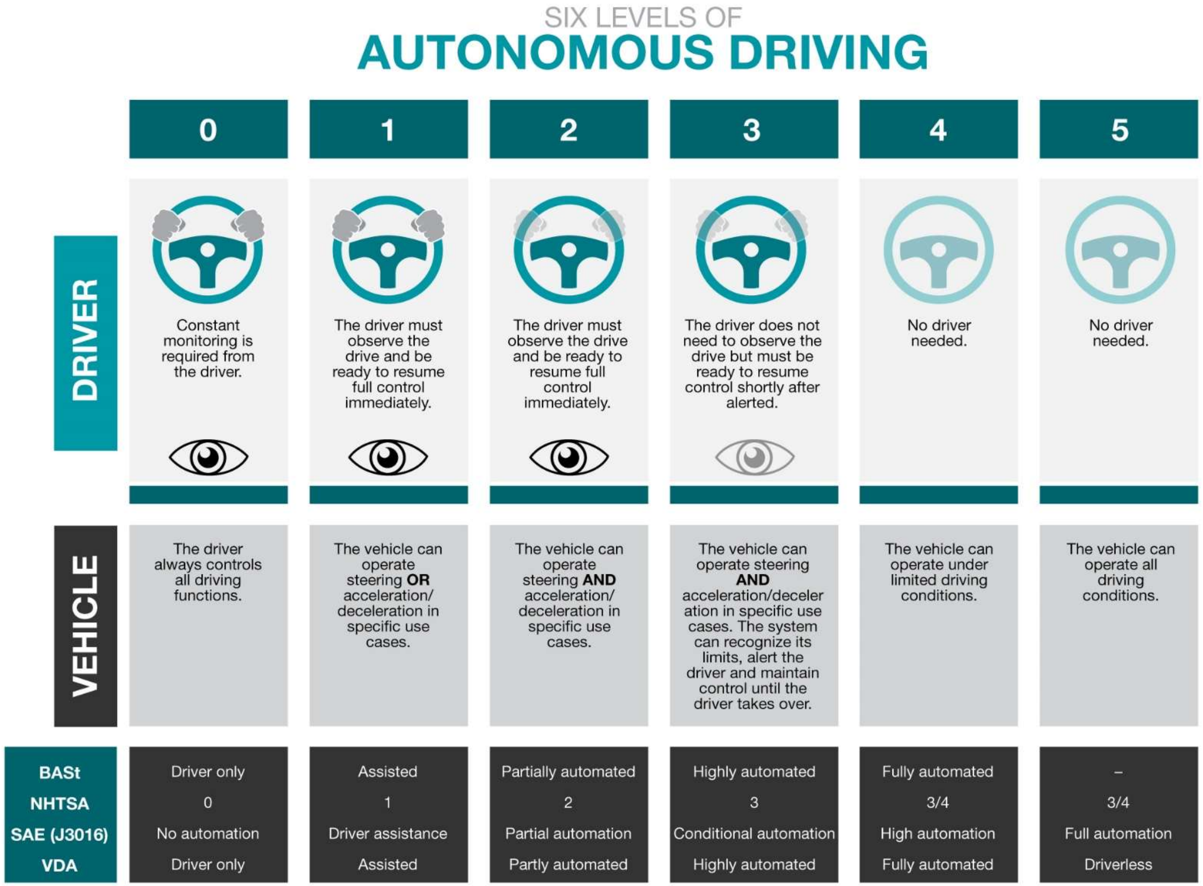
ADAS: Advanced Driver Assistance Systems

ECU: Eletronic Control Unit

CAN: Controller Area Network



ADAS LEVELS



SIX LEVELS OF

AUTONOMOUS DRIVING

	0	1	2	3	4	5
DRIVER	Constant monitoring is required from the driver.	The driver must observe the drive and be ready to resume full control immediately.	The driver must observe the drive and be ready to resume full control immediately.	The driver does not need to observe the drive but must be ready to resume control shortly after alerted.	No driver needed.	No driver needed.
VEHICLE	The driver always controls all driving functions.	The vehicle can operate steering **OR** acceleration/ deceleration in specific use cases.	The vehicle can operate steering **AND** acceleration/ deceleration in specific use cases.	The vehicle can operate steering **AND** acceleration/deceleration in specific use cases. The system can recognize its limits, alert the driver and maintain control until the driver takes over.	The vehicle can operate under limited driving conditions.	The vehicle can operate all driving conditions.
BASt	Driver only	Assisted	Partially automated	Highly automated	Fully automated	–
NHTSA	0	1	2	3	3/4	3/4
SAE (J3016)	No automation	Driver assistance	Partial automation	Conditional automation	High automation	Full automation
VDA	Driver only	Assisted	Partly automated	Highly automated	Fully automated	Driverless

Defined by the Society of Automotive Engineers **(SAE) J3061**

(first version January 2016)

SAE INTERNATIONAL®

Reference: https://www.5gtechnologyworld.com/how-adas-is-paving-the-way-for-autonomous-driving/.

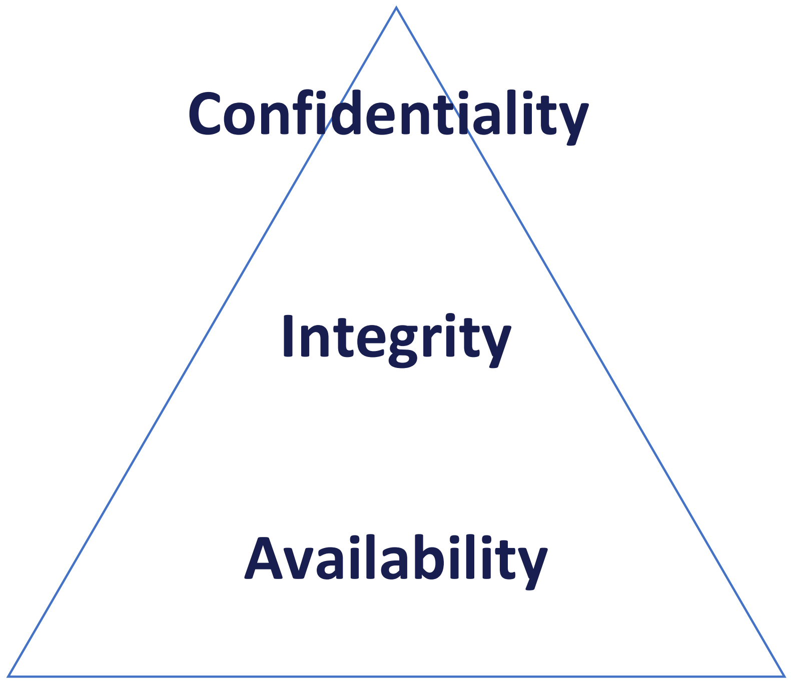
INFORMATION SECURITY

Def. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [NIST SP 1800-10B].

Security Property [NIST definitions]

- Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;
- Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner;
- Availability: Ensuring timely and reliable access to and use of information.

INFORMATION SECURITY



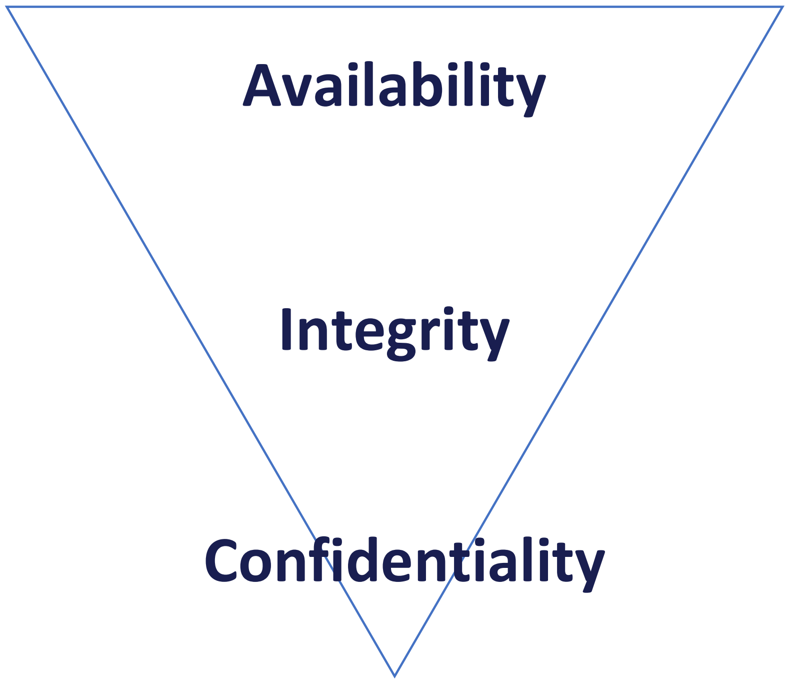
Confidentiality

Integrity

Availability

IT

What is a vehicle IT or OT?



Availability

Integrity

Confidentiality

OT

PRIVACY REGULATIONS

GDPR

Article 4.

personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

CCPA

Title 1798.140. 15.

Personal Information: biometric information, …

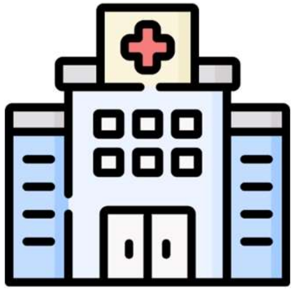
PRIVACY REGULATIONS

USE CASE SCENARIO

The company XYZ collects the location timestamps with date, time, and coordinates of the vehicle [of the driver]. They discover that in the last two months, every Monday, the vehicle goes to a cancer hospital. Which kind of information can they infer?

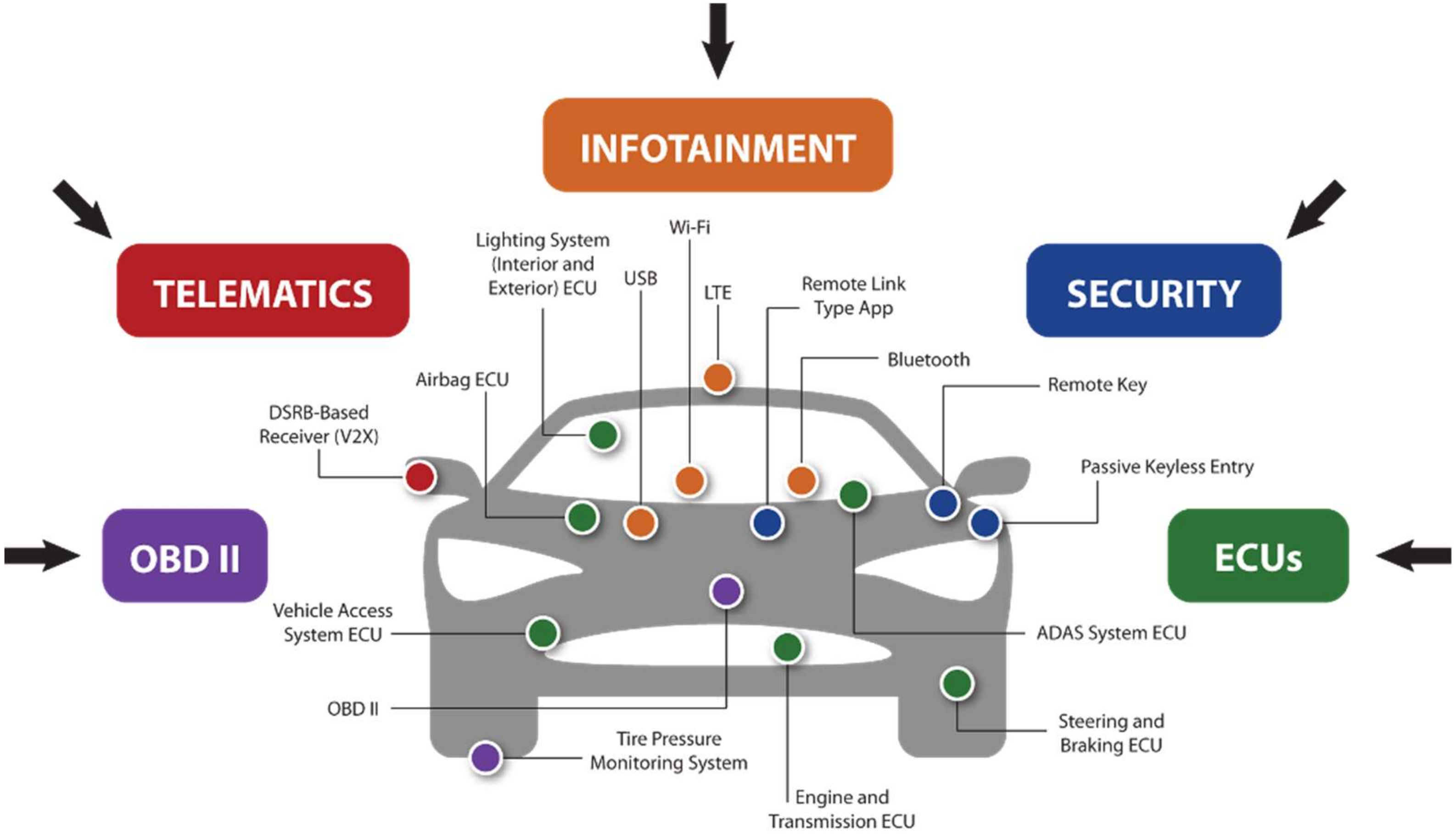
Every Sunday the vehicle is parked near a church for about one hour. Which kind of information can they infer?

Are these personal information? Can our smartphone already collect these information?



VEHICLE THREATS AND ATTACKS

ATTACK SURFACES



SHORT HISTORY

Remote Exploitation of an Unaltered Passenger Vehicle.
C.Miller and C. Valasek, BlackHat 2015

2014

2018

0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars
BlackHat 2019

2020

TBONE – A zero-click exploit for Tesla MCUs
R. Weinmann and B. Schmotzle

2021

ATTACK EXAMPLE

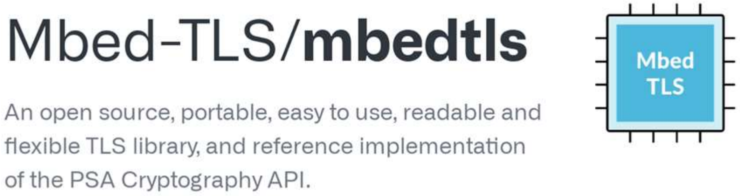
How a print can ruin your day…

ATTACK RECIPE

Connected Vehicle

Infotainment System and its firmware

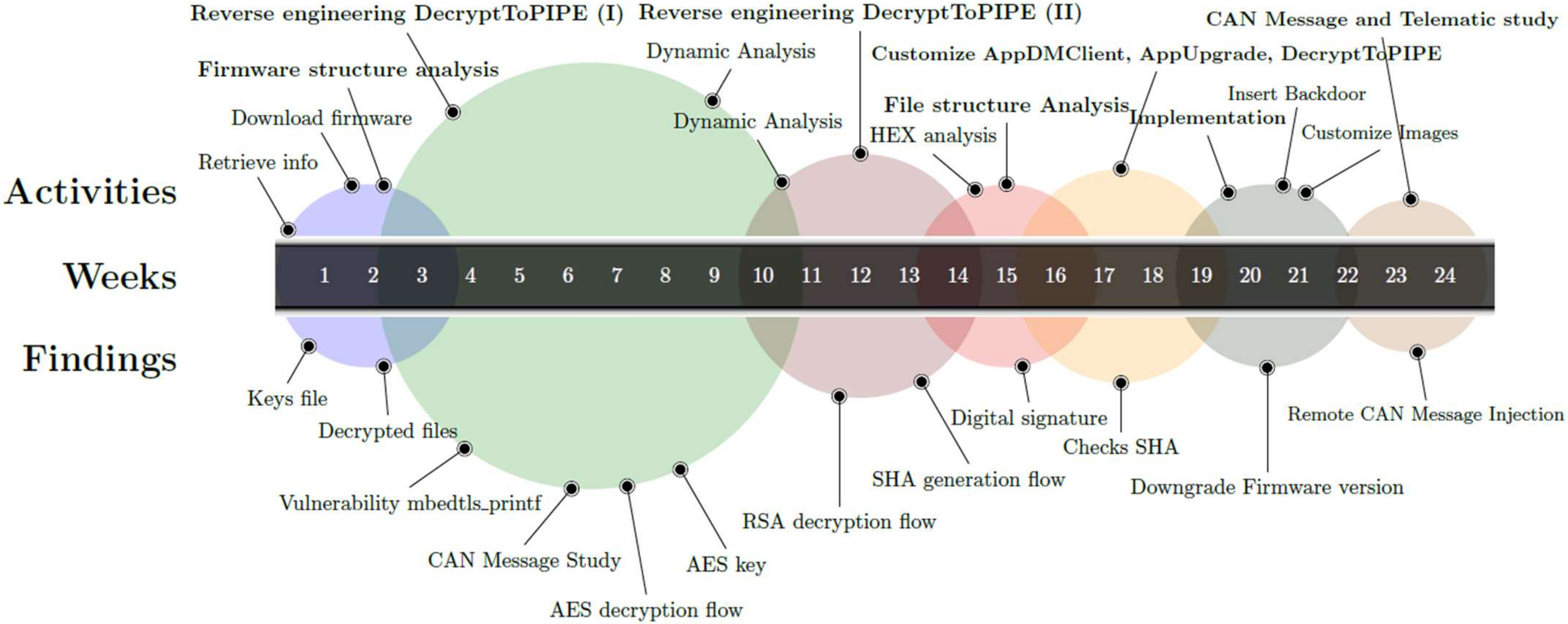
And a library…



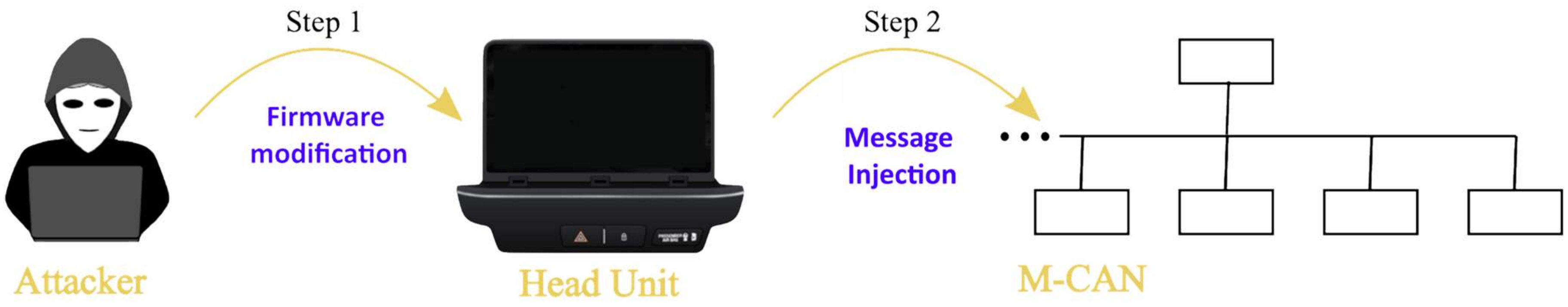
Mbed-TLS/**mbedtls**

An open source, portable, easy to use, readable and flexible TLS library, and reference implementation of the PSA Cryptography API.

TIME AND EFFORT LINE (2022)



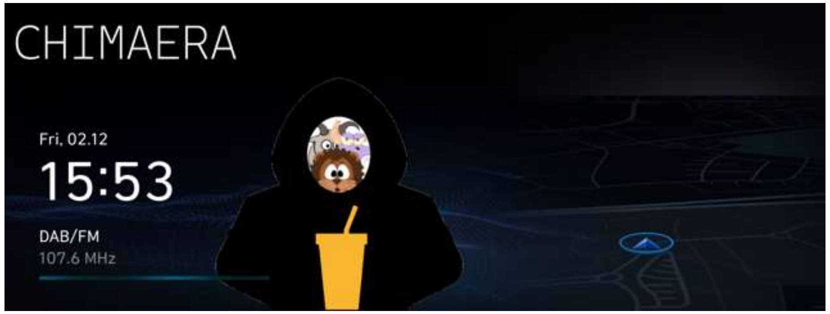
RESULTS

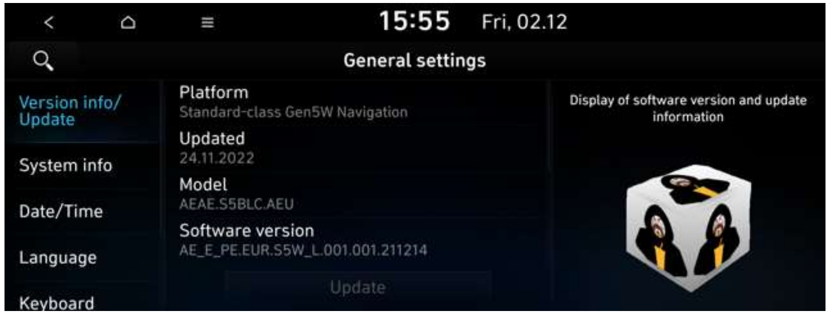


Goal

- Remotely Injecting micom message to activate HU functionalities and sending CAN bus frames into M-bus

RESULTS





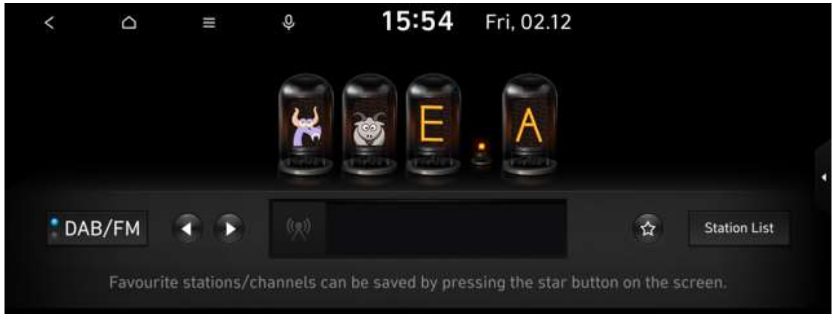
Platform
Standard-class Gen5W Navigation

Updated
24.11.2022

Model
AEAE.S5BLC.AEU

Software version
AE_E_PE.EUR.S5W_L.001.001.211214

Display of software version and update information



Favourite stations/channels can be saved by pressing the star button on the screen.

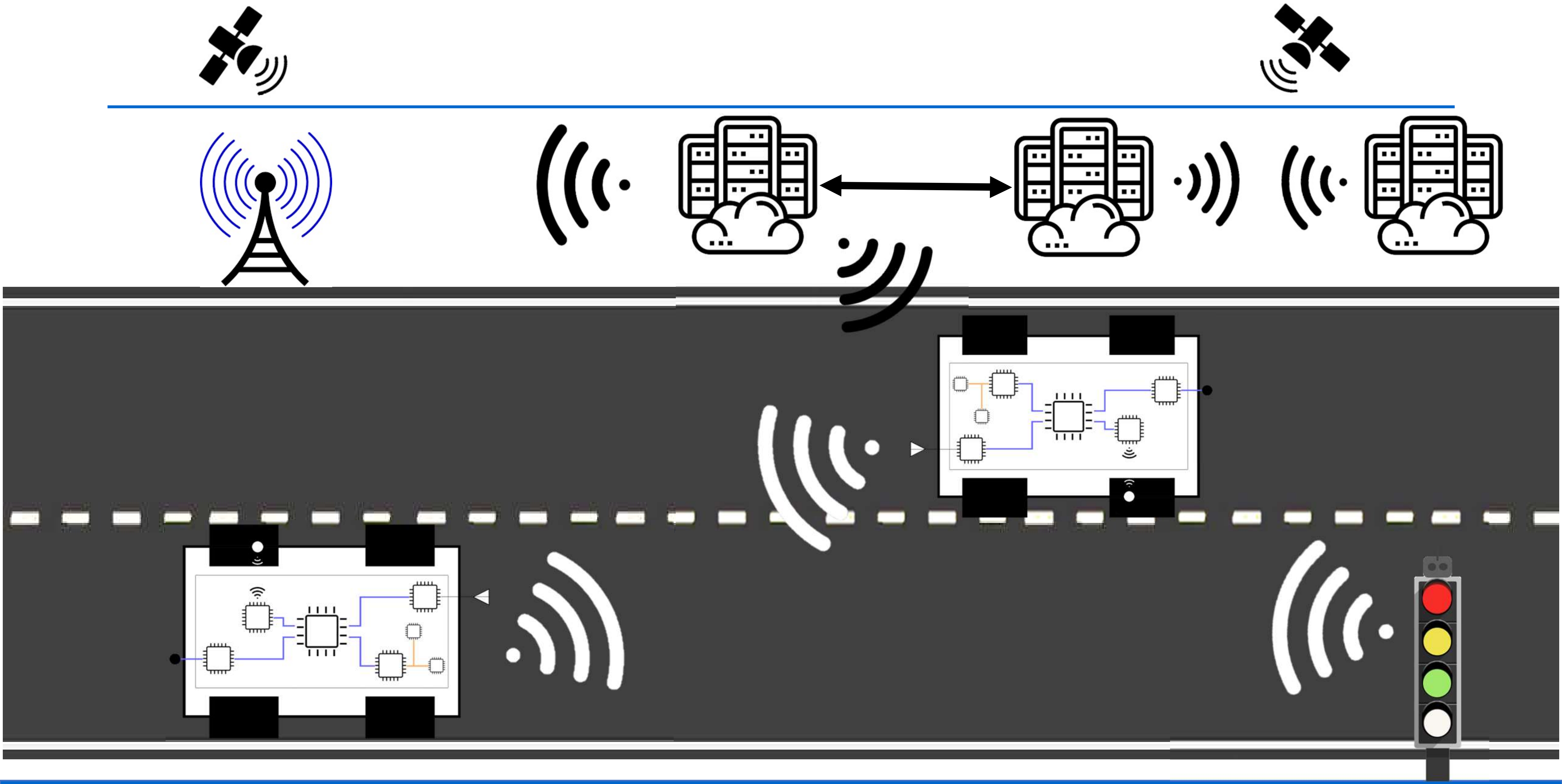
- Compute and read the encrypted AES-CBC 128 key; **[a623….bdafc47]**
- Extract the RSA public key;
- Decode the AES-CBC 128 key using the previous RSA public key;
- Compute the SHA256 of the content of each file;
- Discover the algorithm that generates the Initialization Vector (IV) for the AES-CBC cryptosystem;
- Generate the Initialization Vector (IV);
- Encode and decode each file with the AES-CBC 128 Key and the IV;
- Bypass the check of the digital signature during the firmware installation by upgrading AppDMClient binary patch in Head-Unit;
- Remotely control the Gen5W IVI system **by injecting remote commands that impact also the CAN bus intoM-bus, B-bus and C-bus**. In particular, we forge CAN bus frames like we trigger services from the telematic app, e.g., Bluelink. This is possible only leveraging 1-Day exploit or using our custom firmware.

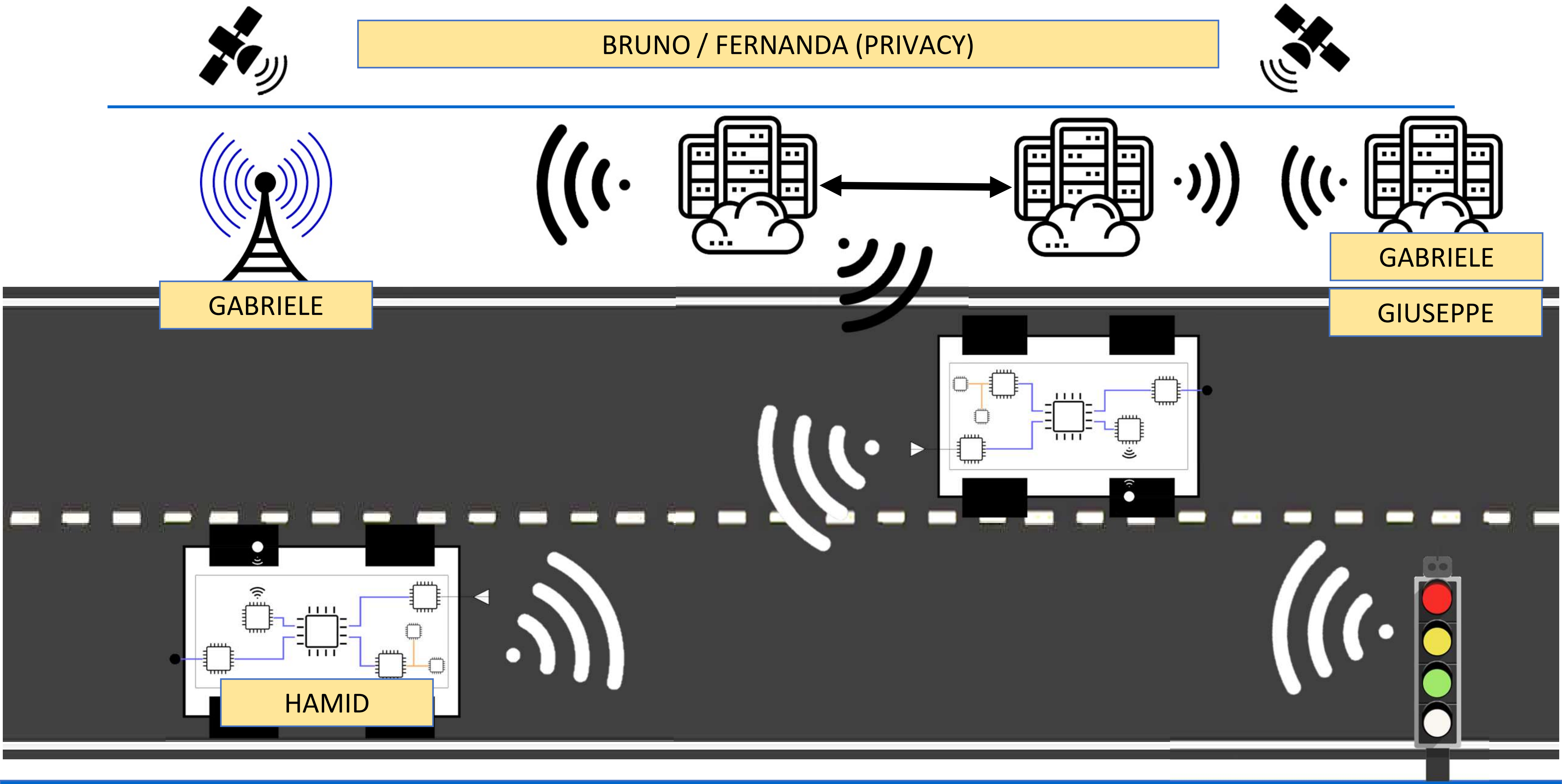
OPEN ISSUES

- **Automotive**: is IT or OT?
- **Privacy**: how receive services and preserve privacy?
- **Security**: how can we balance safety/security/costs?
- **Ethics**: in case of accident that involves an autonomous vehicle who is responsible?

Panda solution!

FINAL SOLUTION?




BRUNO / FERNANDA (PRIVACY)
GABRIELE
GABRIELE
GIUSEPPE
HAMID

Thanks

Questions?

For any further information please contact me at marco.devincenzi@iit.cnr.it