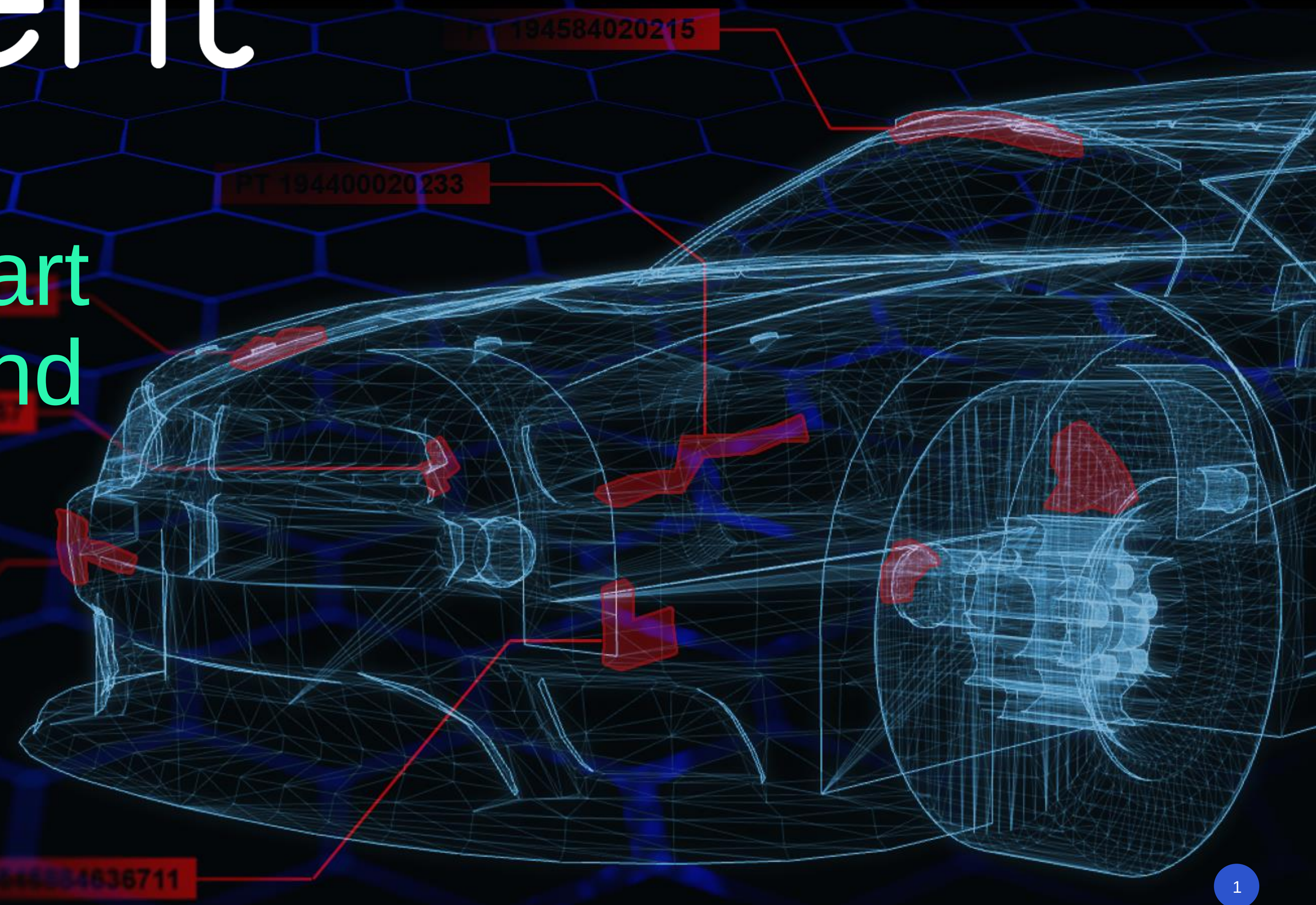
Security of Smart Cars in 2023 and Beyond



Aleksander Gorkowienko

Senior Consultant in Cybersecurity

About myself

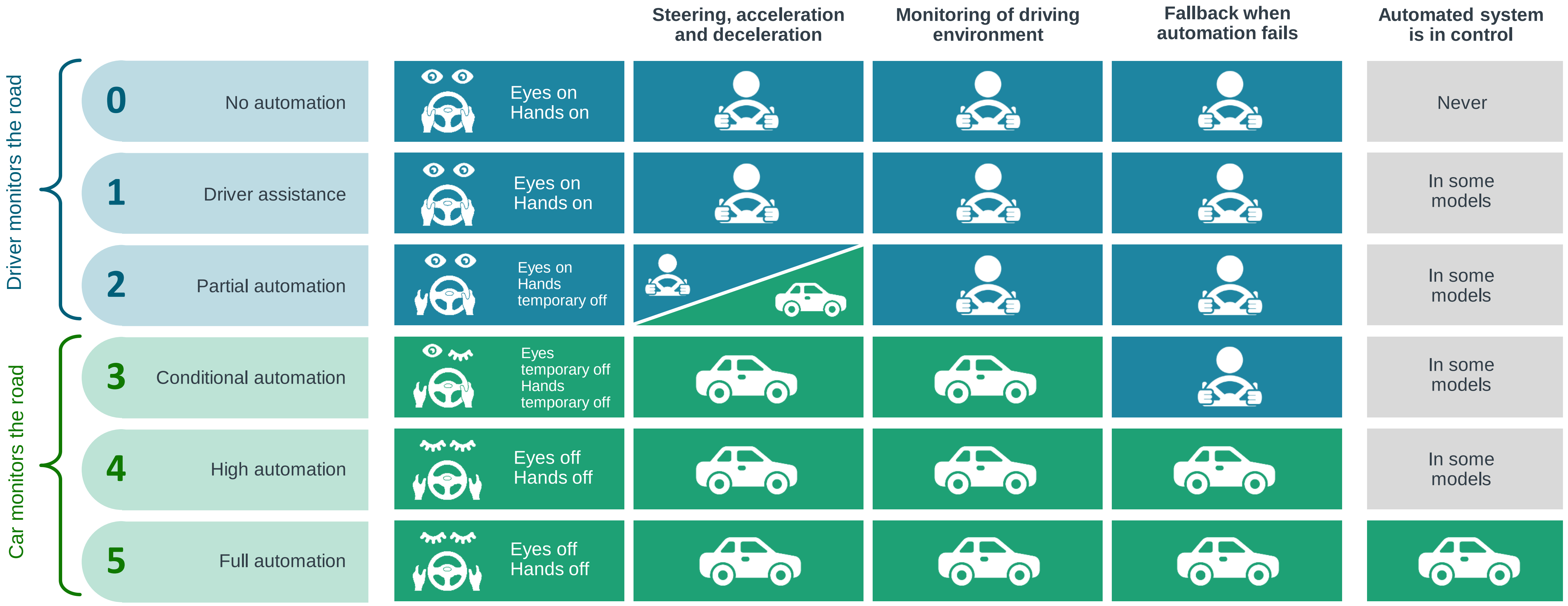
Aleksander Gorkowienko

- Cybersecurity advocate, practitioner and researcher with more than 20 years of experience
- A part of the Spirent SecurityLabs team (UK branch)
- Specialised in security of automotive and industrial systems, IoT and telecommunication
- Speaker at various international cybersecurity conferences
- Running complex security projects around the globe
- Experimenting with AI applied to cybersecurity
- Every day learning something new

What do we mean by “smart car"

Definition by SAE J3016

The SAE J301639 standard defines six levels of driving automation for on-road vehicles, ranging from **level 0** with no driving automation at all to **level 5** with full driving automation and no need for a driver.



Definition by SAE J3016

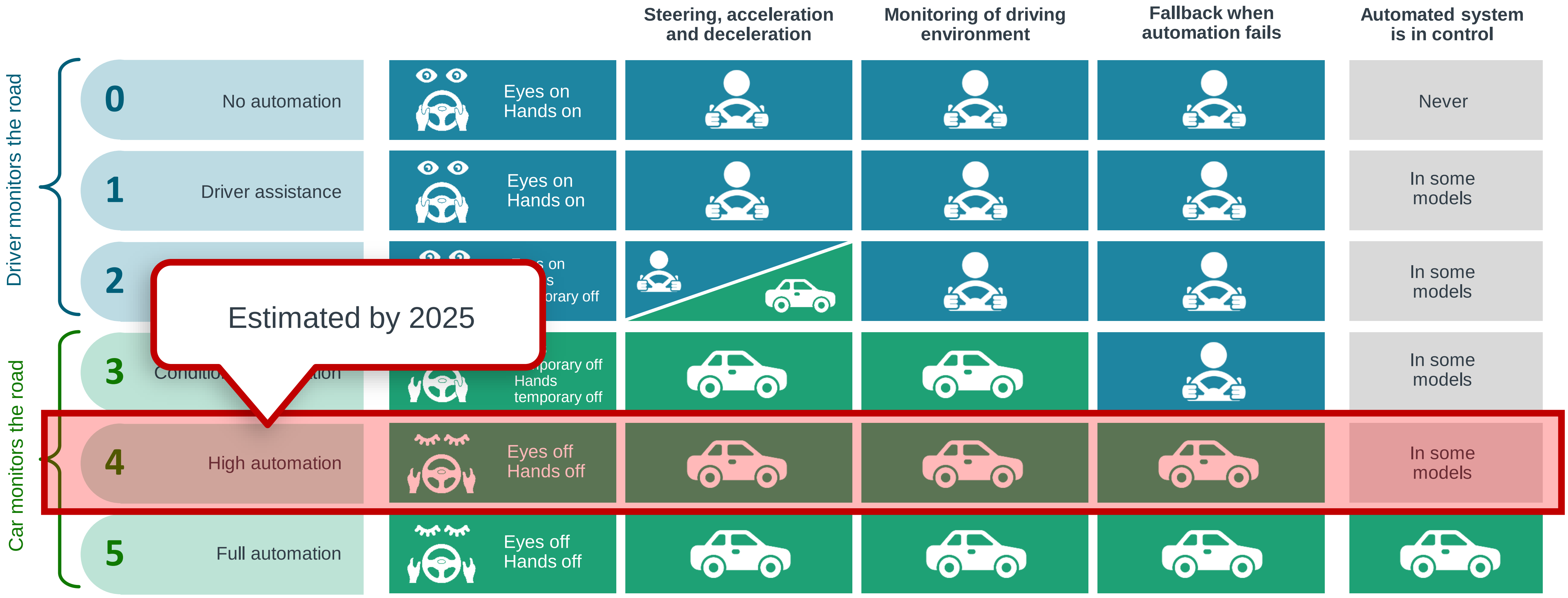
The SAE J301639 standard defines six levels of driving automation for on-road vehicles, ranging from **level 0** with no driving automation at all to **level 5** with full driving automation and no need for a driver.

	Level			Steering, acceleration and deceleration	Monitoring of driving environment	Fallback when automation fails	Automated system is in control
Driver monitors the road	0	No automation	Eyes on Hands on				Never
	1	Driver assistance	Eyes on Hands on				In some models
	2	Partial automation	Eyes on Hands temporary off				In some models
Car monitors the road	3	Conditional automation	Eyes temporary off Hands temporary off				In some models
	4		Eyes off ds off				In some models
	5		off ds off				

We are here

Definition by SAE J3016

The SAE J301639 standard defines six levels of driving automation for on-road vehicles, ranging from **level 0** with no driving automation at all to **level 5** with full driving automation and no need for a driver.



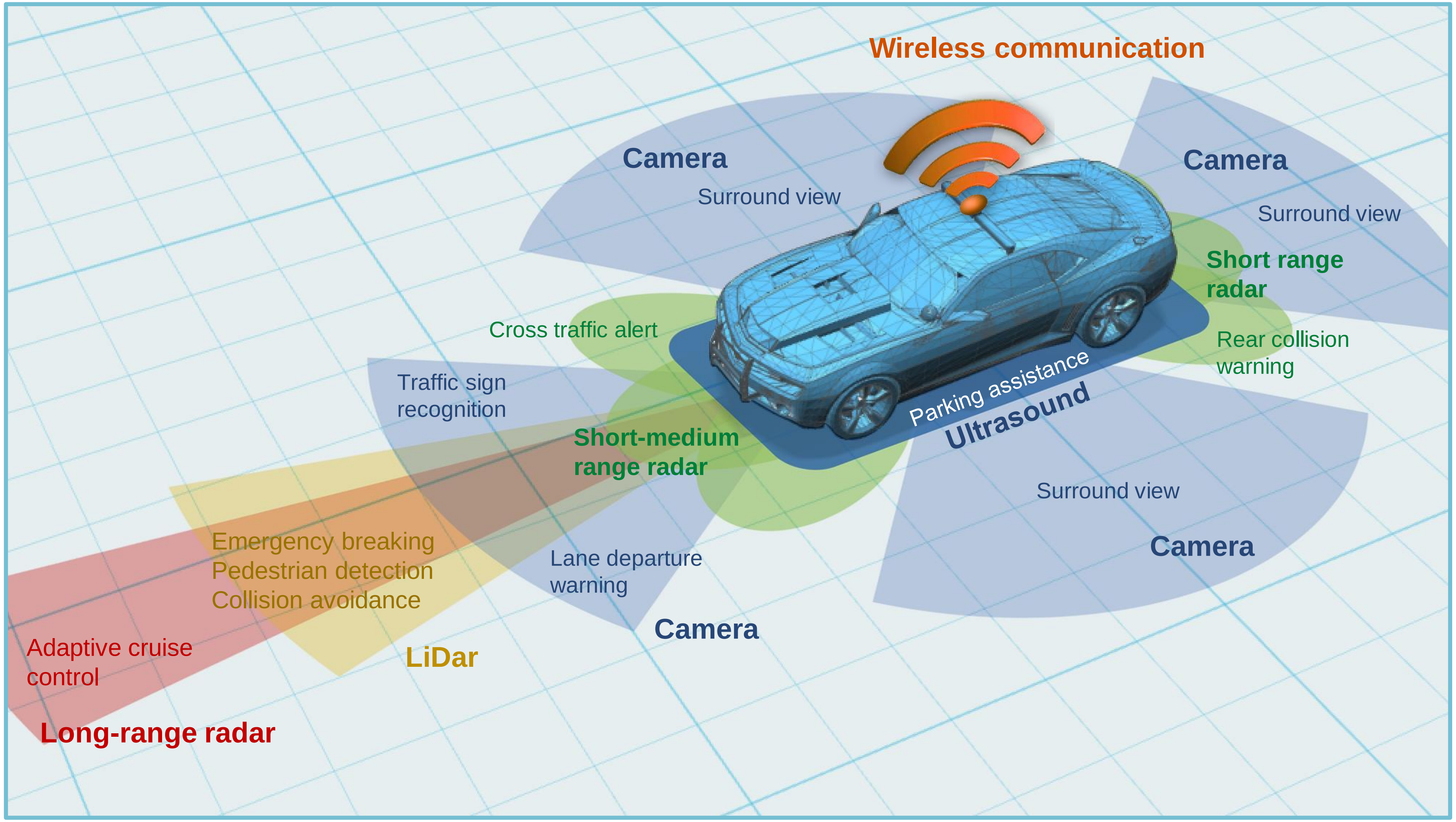
Definition by SAE J3016

The SAE J301639 standard defines six levels of driving automation for on-road vehicles, ranging from **level 0** with no driving automation at all to **level 5** with full driving automation and no need for a driver.

				Steering, acceleration and deceleration	Monitoring of driving environment	Fallback when automation fails	Automated system is in control
Driver monitors the road	0	No automation	Eyes on Hands on				Never
	1	Driver assistance	Eyes on Hands on				In some models
	2	Partial automation	Eyes on Hands temporary off				In some models
Car monitors the road	3		Eyes … orary off … ds … orary off				In some models
	4	H… … tion	… s off Hands off				In some models
	5	Full automation	Eyes off Hands off				

Estimated by 2050

Modern cars are full of automation and sensors



Typical ADAS sensors used in modern smart and self-driving cars

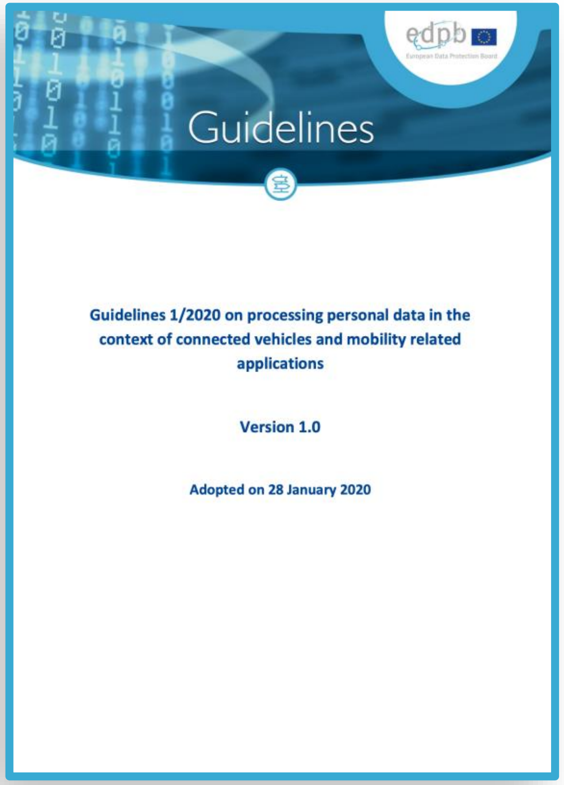
Sensors generate an incredible amount of data

1.5 hrs of driving generates

4TB of data

- Can we process, store but also sufficiently protect this sensitive information?
- Additional problem is that this information must be shared with the other cars on the road (V2V) to optimize traffic and with external infrastructure (V2X)

Processing personal data in the context of connected vehicles: guidelines by European Data Protection Board


edpb
European Data Protection Board

Guidelines

Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

Version 1.0

Adopted on 28 January 2020

Vehicle management - functions that are supposed to aid drivers in reducing operating costs and improving ease of use, e.g. notification of vehicle condition and service reminders

Road safety - functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection

Entertainment - functions providing information to and involving the entertainment of the driver and passengers, such as various smart phone interfaces, WLAN hot spots, music, video, Internet, social media, mobile office or "smart home" services

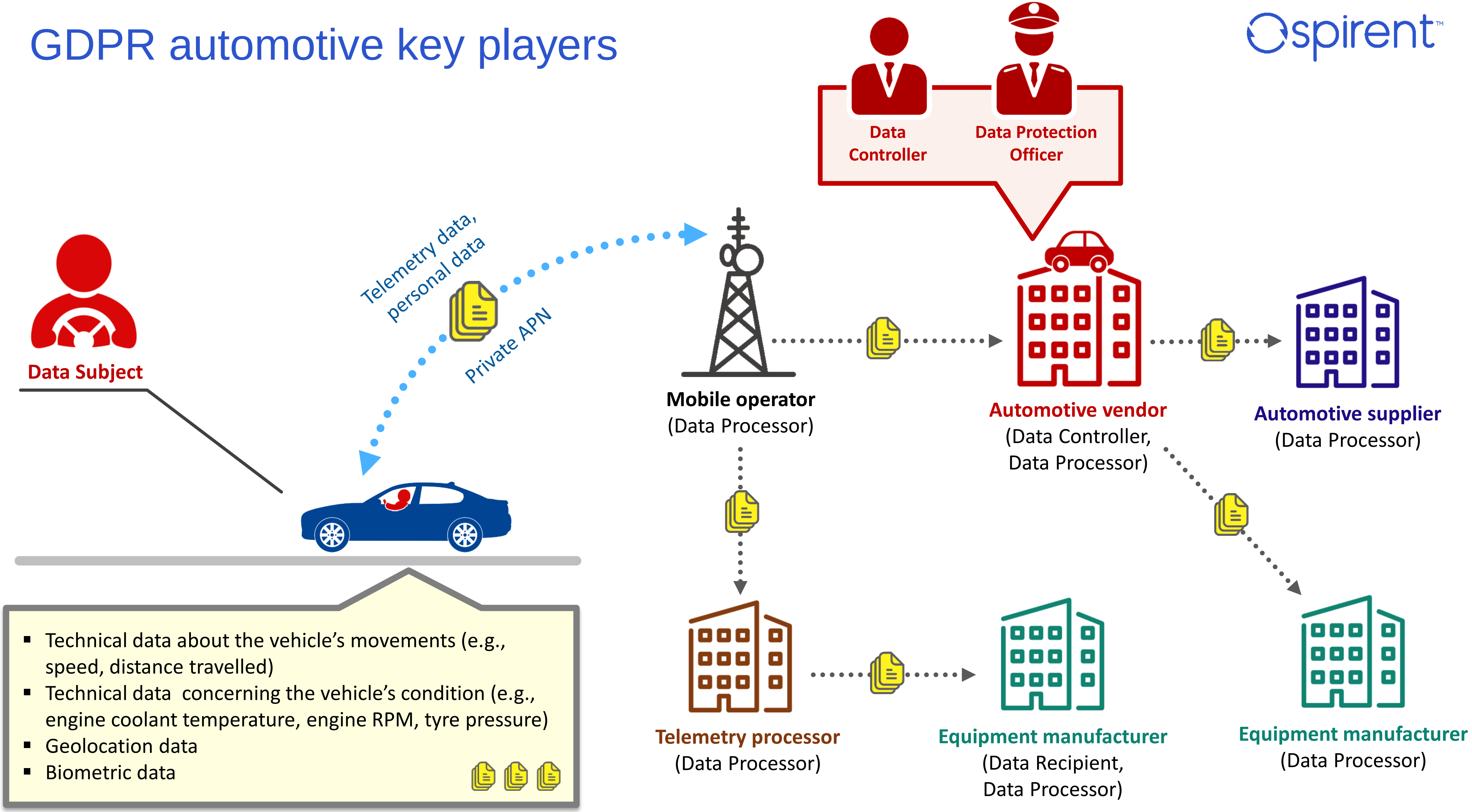
Mobility management - functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, such as GPS navigation, integration with active traffic management systems

Driver assistance - functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways

Well-being - functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance

The **connected vehicle** can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle.

GDPR automotive key players



Hacking cars

What hackers can do with your car?

A quick answer:

Turn your shiny new car…

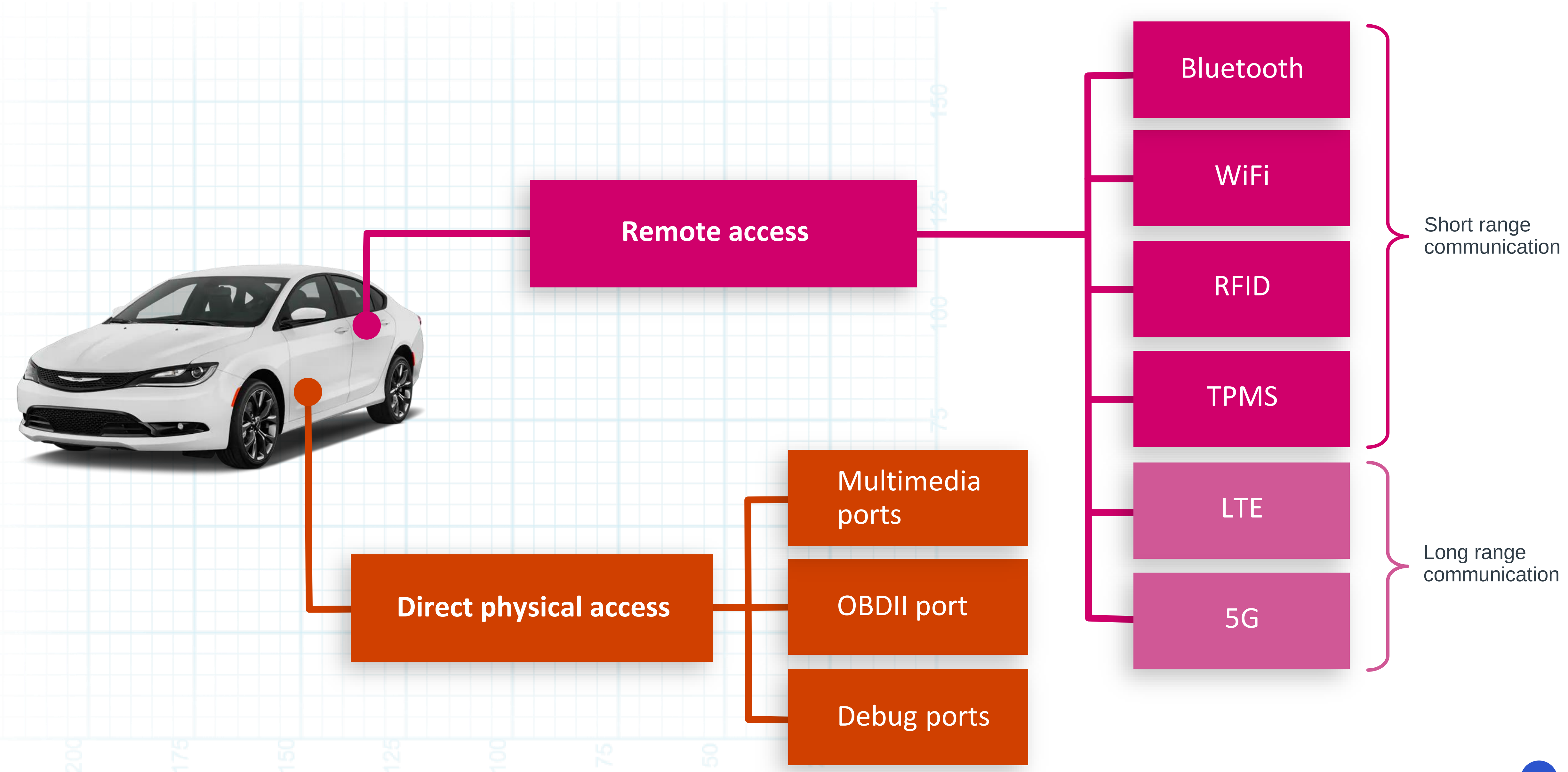
A quick answer:

Turn your shiny new car…   into…

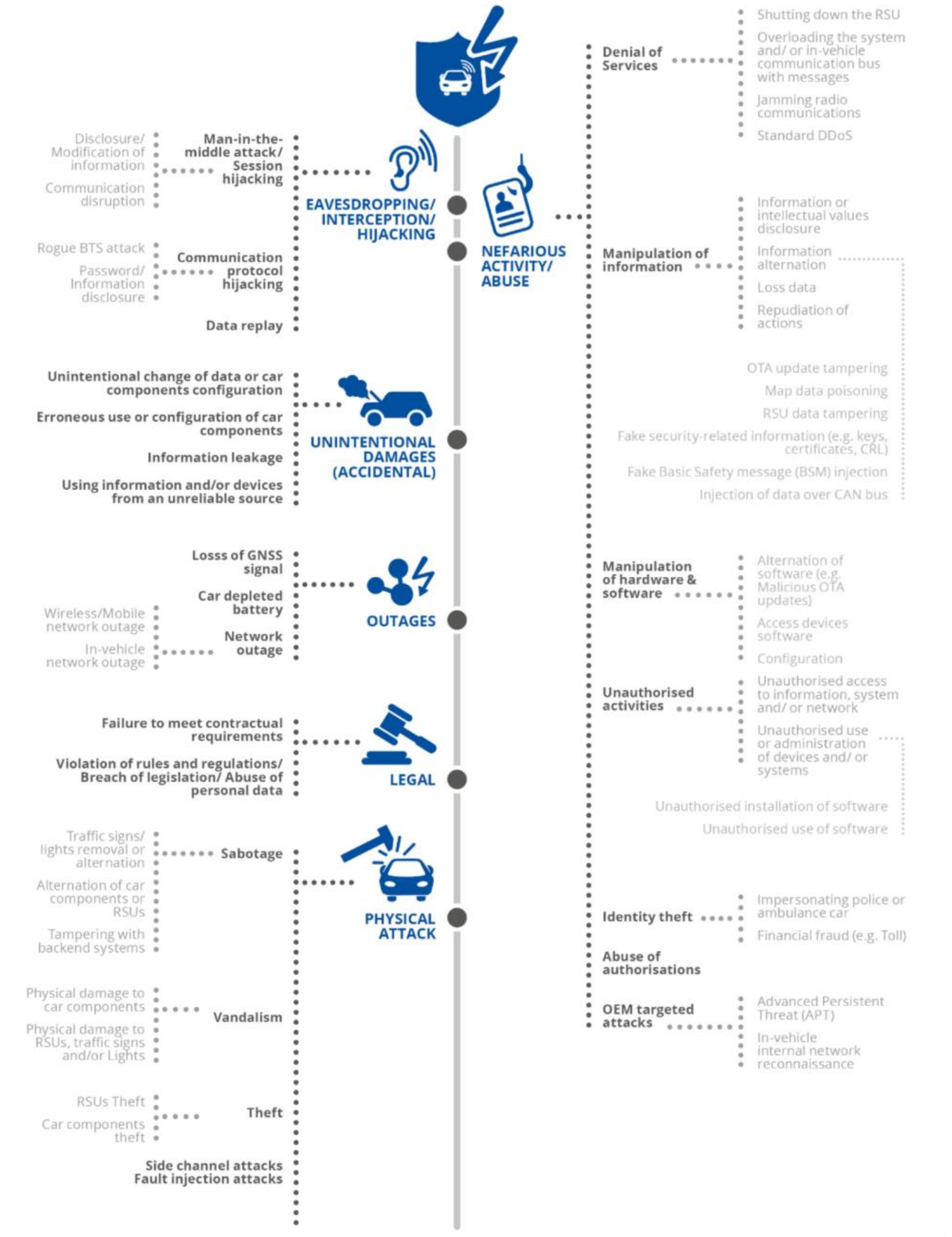
A quick answer:

Turn your shiny new car… into… **this.**

“Doors and windows” to the smart car



Threat taxonomy according to ENISA



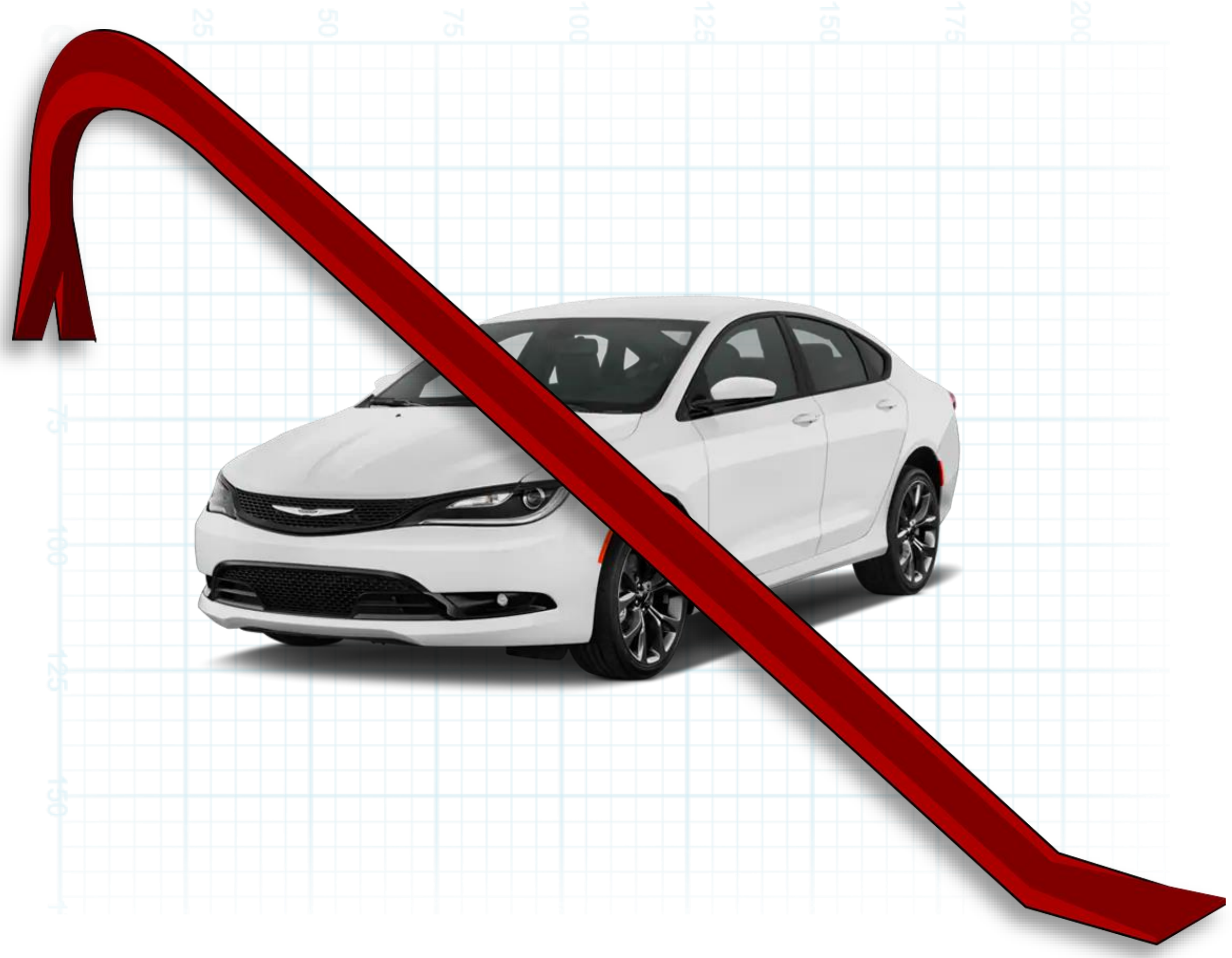
Threats to modern smart cars

Standard ”menu” of threats:

- Unlock and steal a vehicle
- Remotely take over a vehicle
- Remotely stop and shut down a vehicle (denial of service)
- Spy on vehicle occupants, steal their sensitive data
  - Access GPS data and track a vehicle
  - Circumvent safety systems and cause crash/pre-crash conditions etc.
  - Install malware on the vehicle

Threats specific to self-driving cars:

- Circumvent autonomous navigation system and e.g. stop or change the route of the vehicle
- Smart sensor spoofing
- Circumvent car’s AI
- Change the computer’s logic and priorities in crash conditions

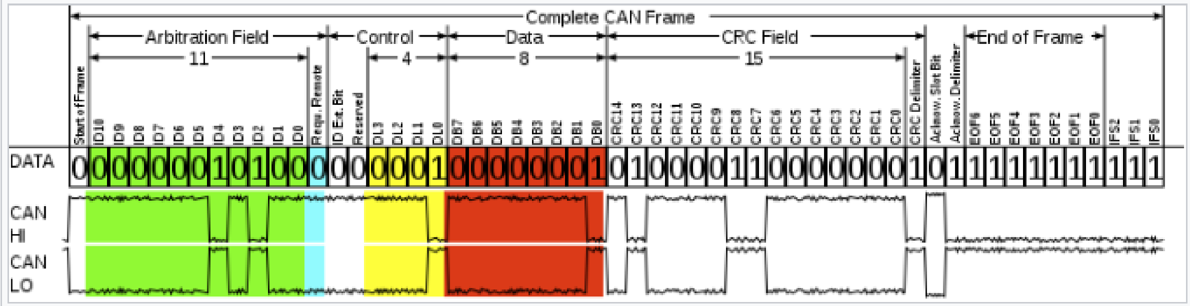


CAN Bus and car hacking

The **Controller Area Network (CAN)** bus is a standard developed by Bosch and Intel in 1983.

We use the CAN Bus version which was released in the 1990’s.

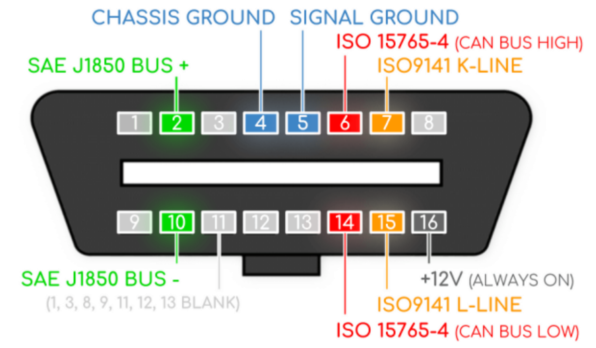
CAN is a serial communications protocol that allows distributed real-time communication and control between various vehicle components like: brakes, power steering, windows, A/C, airbags, cruise control, infotainment systems, doors, battery and recharging systems etc.



CAN-Frame in base format with electrical levels without stuffbits

OBD II (on-board diagnostics) and CAN bus are the entry point in monitoring and also (partially) are controlling a car (pretty much any car since 1996!).

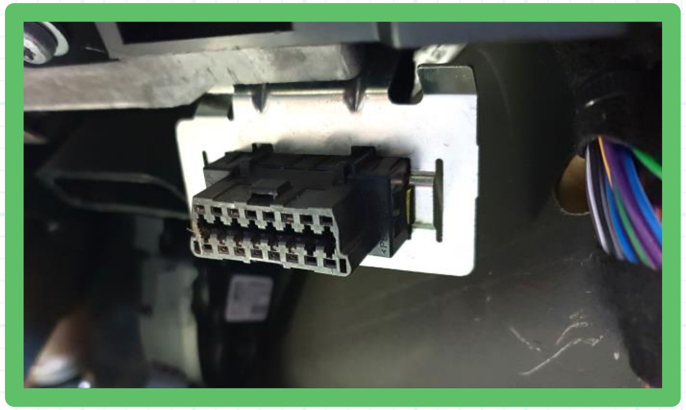
Smart cars and self-driving cars use this protocol!



CAN Bus and car hacking

CAN is a **broadcast serial bus standard** for connecting (electronic control units) ECUs. All of them are connected to the same "internal network" meaning **there is no central computer**.

When an ECU sends a message, **every other ECU on the bus receives it** and can choose to respond to it or ignore it.



ODB II socket

WiFi to ODB II interface
(connected to my own car, btw.)

Hacker's way of thinking:

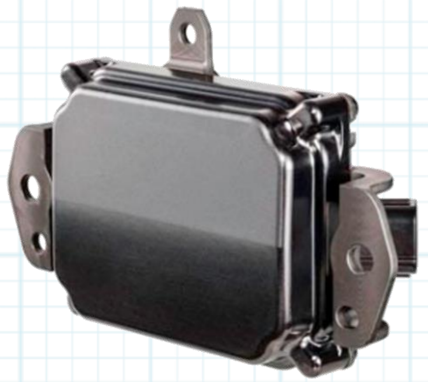
- If we can reach CAN Bus **– we can potentially "talk" to all electronics in the car**.
- Consider the simplest approach first: secretly connect your ODB II wireless device to the ODB port in the victim's car and access it over WiFi or Bluetooth. **The car is immediately under your control!**

Hacking sensors: Jamming

Each type of sensor rely on distinctive physical principles. Once you know them – you can find a way to circumvent or “blind” a sensor.

Jamming attack (or Denial of Service): sending a very strong signal of the same type to the sensor, overload it with data and make it “blind”.

- **Parking assistance ultrasonic sensors:** if jammed, cannot detect obstacles
- **MMW radar:** attackers can send back a fake signals which makes object detection impossible. A simple jamming technique uses a scanner to determine the frequency of a radar signal and later generate a jamming signal at the same frequency, disrupting the car radar’s receiver.
- **Cameras** – can be temporarily or permanently blinded by a very strong source of light or laser (visible or infrared). Btw, laser beam from the distance of 0.5m to 1m directly at the camera irreversibly destroys CMOS/CCD.



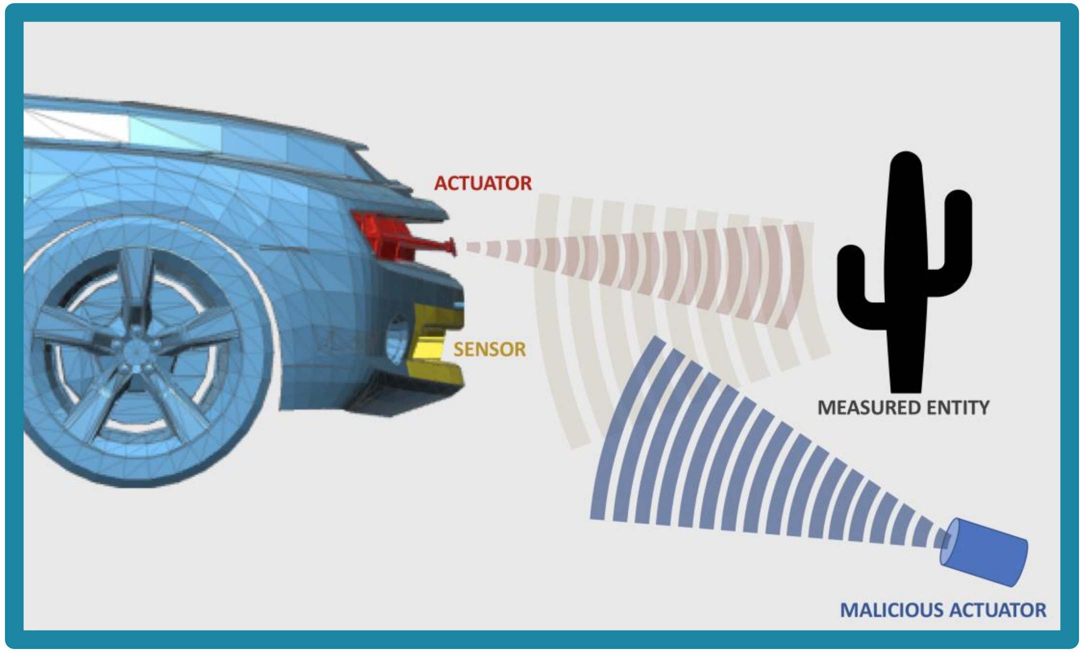
Car MMW radar

Car video camera

Hacking sensors: Spoofing

Spoofing attack: sending to the sensor a carefully crafted signal which is undistinguishable from real which provides false data to the on-board computer.

- **Attacking ultrasonic sensors**: absorbing sound or using active echo cancellation. The object “disappears” from the radar’s view.
- **Attacking MMW radar**: sending back a signal with artificial “radar shadows” producing fake doppler shift.
- **Attacking cameras**: playing with light and shadows and e.g. simulate non-existing obstacles on the road.

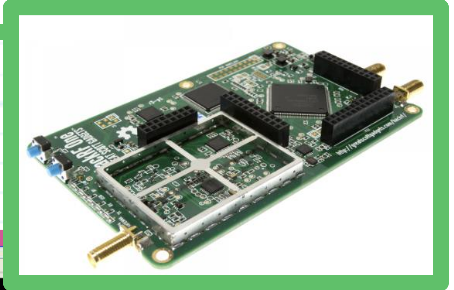


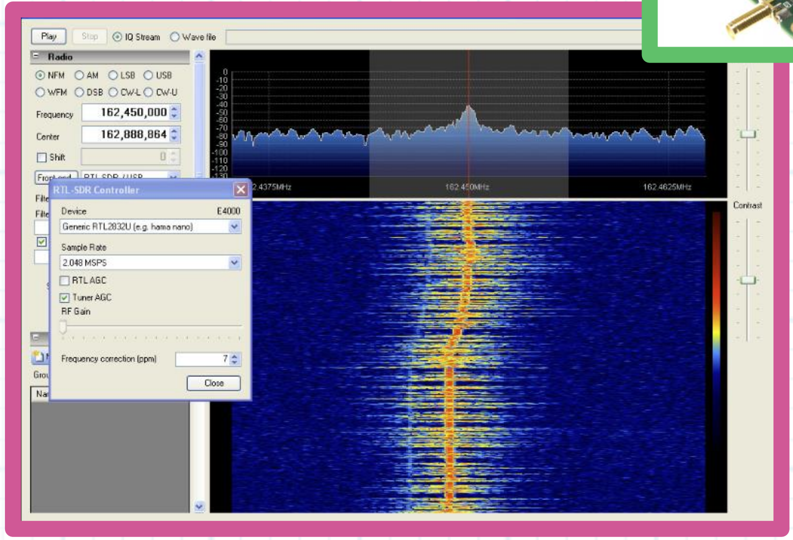
Hacking V2V And V2X: Sniffing

Sniffing: passive radio reconnaissance, "listening" to the information in the air broadcasted by the car

- Software defined radio (SDR) covering frequencies from 100 KHz to 6 GHz is widely used and incredibly affordable these days. Cost from £5 to £200. (Note: professional devices cost from £2000 and up.)
- Collected information can be used for protocol analysis and potentially for "re-play attacks".
- More advanced devices are **"transceivers" can not only listen but also send radio signals**. The technology which was reserved for government agencies and the army now is in the hands of hackers.

RTL SDR USB dongle


HackRF One



RF analysis using free software

Hacking V2V And V2X: Jamming

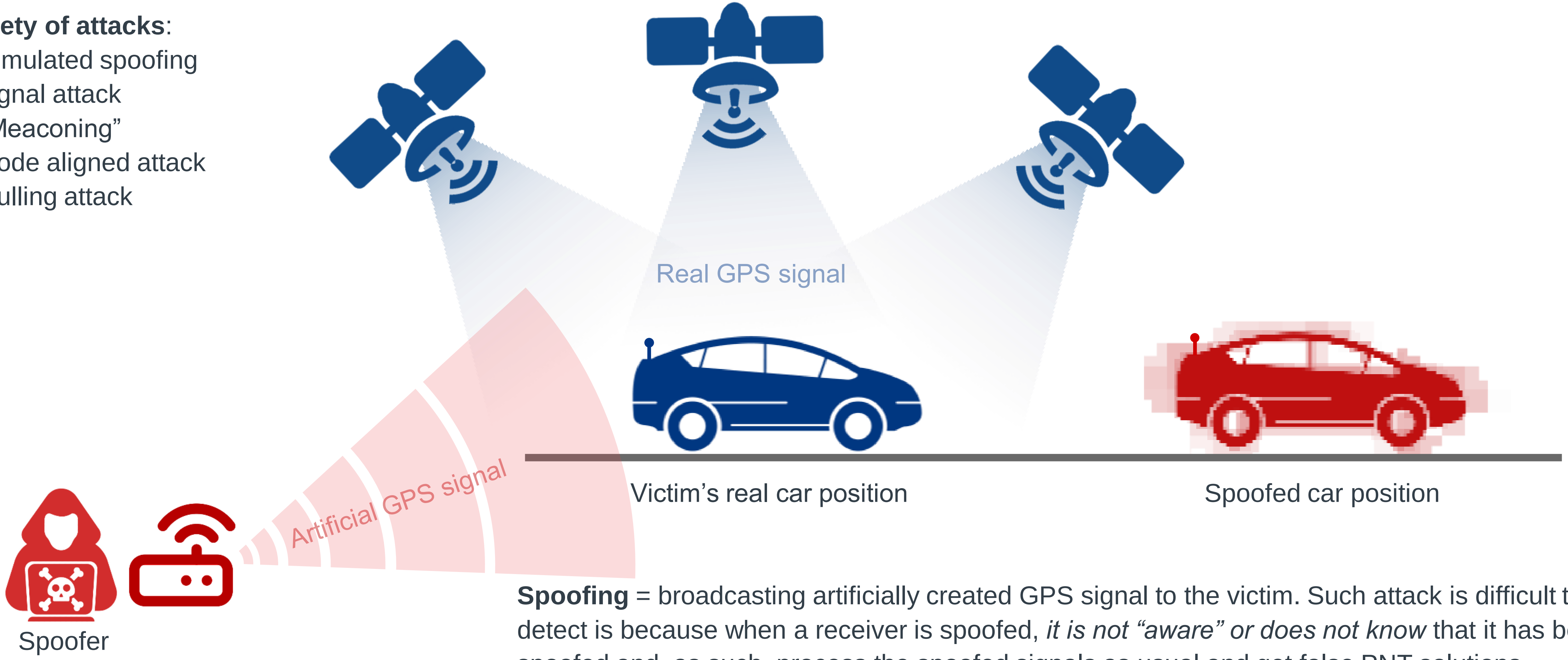
Jamming: simply making communication impossible by jamming RF (generating noise).

- Self-driving car without the up-to-date information about the situation on the road can potentially switch to a “safe mode” (e.g. imagine it running 50 mph on highway). The similar safety approach is used now by railways, btw.
- Having no connectivity the car might ask the driver to take control, or stop. (which depreciates the whole concept of smart or self-driving car)
- Note: jamming RF and GPS data is illegal in many countries.

RF and GPS jammer that you can buy on the Internet or build your own

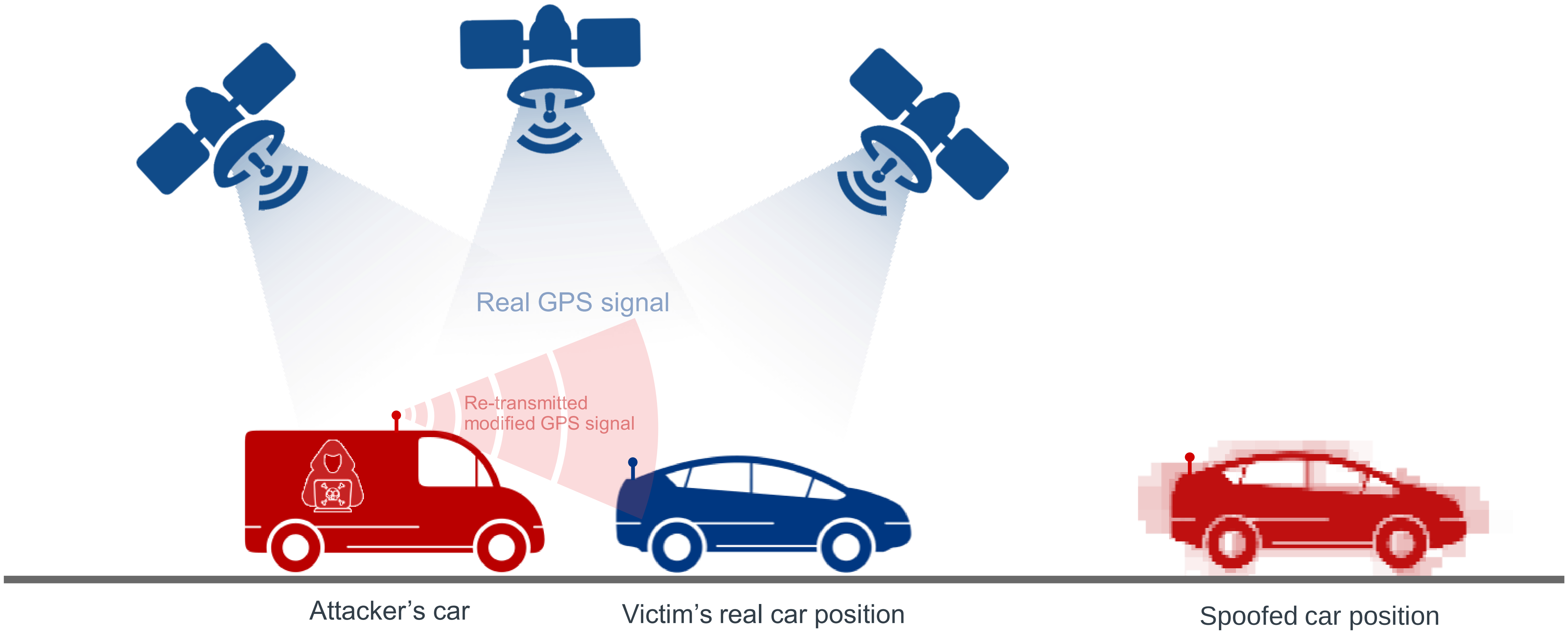
Hacking V2V And V2X: GPS Spoofing

Variety of attacks:
- Simulated spoofing signal attack
- "Meaconing"
- Code aligned attack
- Nulling attack



Spoofing = broadcasting artificially created GPS signal to the victim. Such attack is difficult to detect is because when a receiver is spoofed, *it is not "aware" or does not know* that it has been spoofed and, as such, process the spoofed signals as usual and get false PNT solutions.

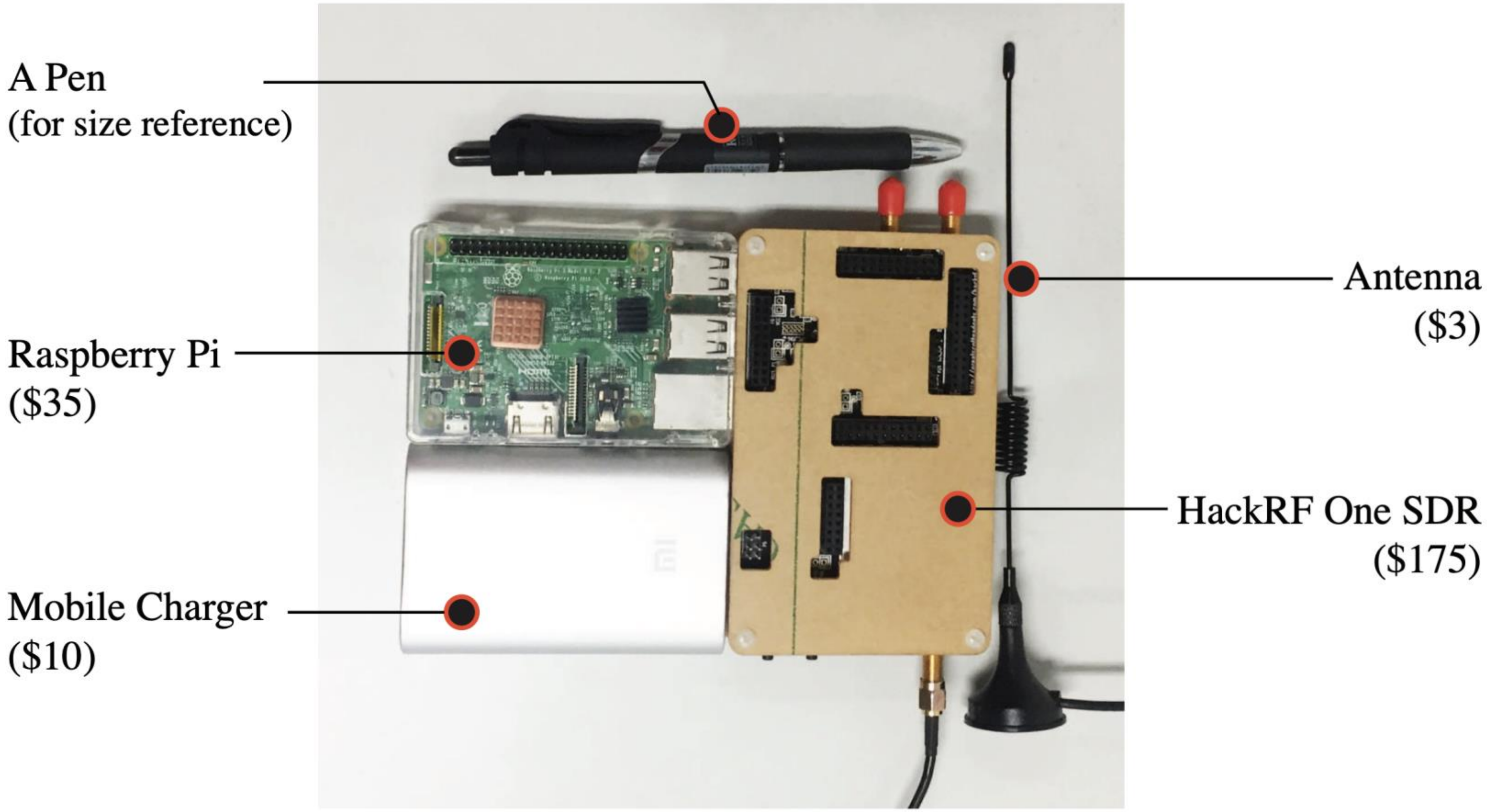
Hacking V2V And V2X: GPS Spoofing – “Meaconing attack”



In meaconing, an attacker captures a real GNSS signal from its receiver and then re-transmits it to the victim. With this meaconing method, the signal resembles a real-world GNSS signal with various channel impairments (ionospheric delay, phase noise) due to multipath.

Hacking V2V And V2X: GPS Spoofing

Cost of equipment for GPS spoofing:
From about $250 to hundreds of thousands of $$$



A low-cost portable GPS spoofer

Preventing the disaster

Follow the industry best practices

Picture from: ENISA Good Practices for Security of Smart cars

Secure SDLC

Identify and/or define relevant security policies and pick those applicable to the software.

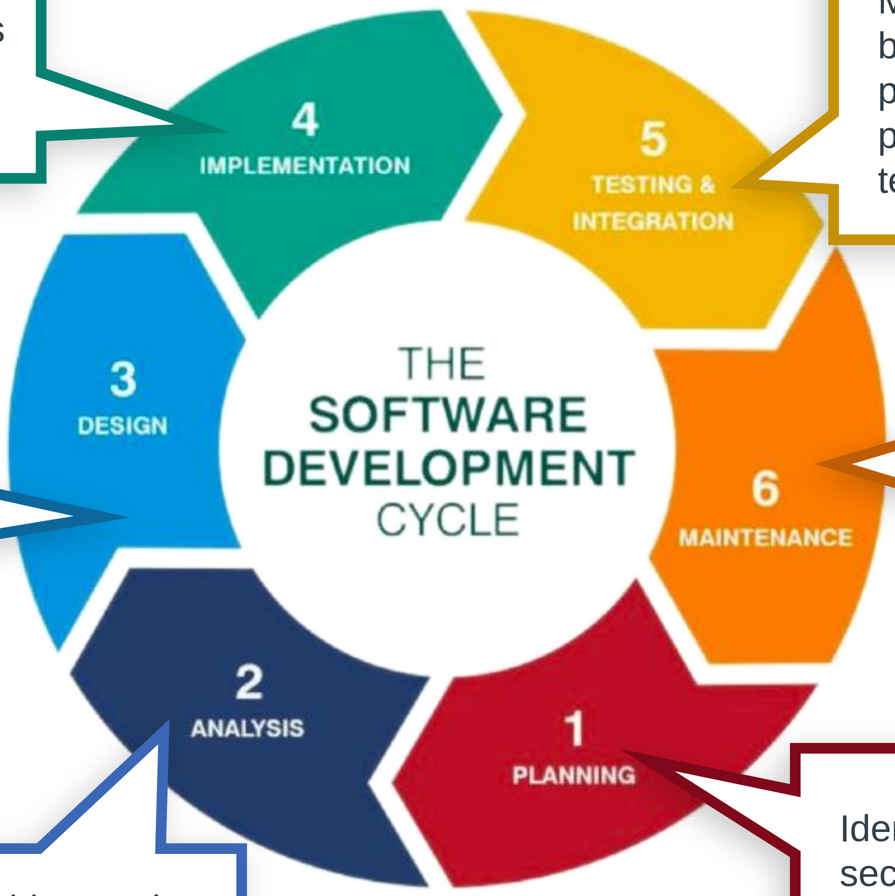
Conduct architectural risk analysis that identifies security flaws in the very early stage.

Develop guidelines to address risks evaluated during previous phases. A comprehensive Product Security Risk Assessment ("Static Assessment").

Developers follow the robust secure coding practices. Security guidelines are set and awareness campaigns are conducted regularly.

Monitoring of the product is carried out both in its production and post-production environment. Under production, the developed software is tested/re-tested again.

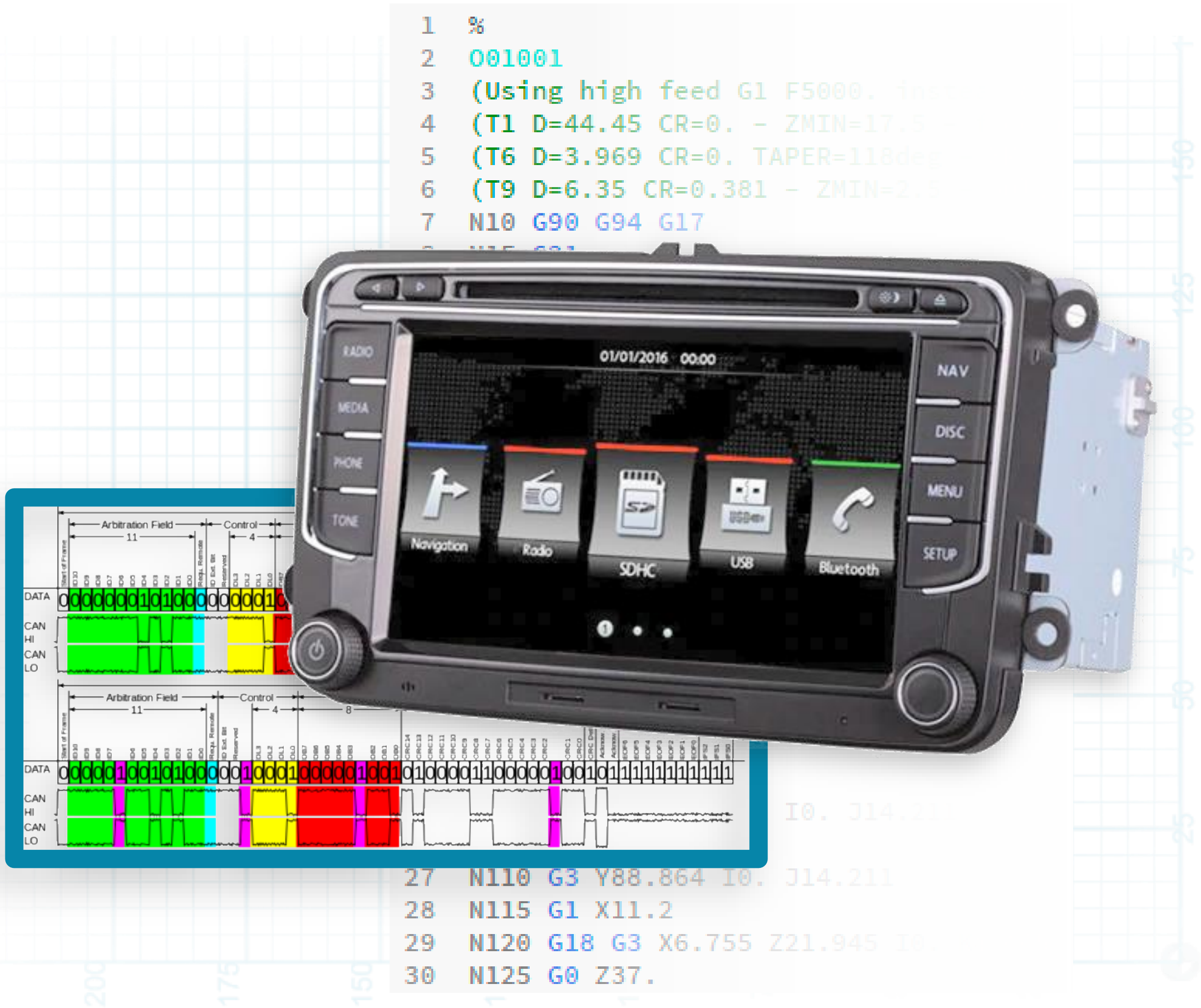
Continuous attempts to identify new, recently discovered and published, vulnerabilities.



Each phase in the SDLC requires its own set of security tools that need to be mapped with the teams' IDEs, code repositories, build servers, and bug identifying tools to gauge any scope of risk and to address them.

Follow ISO/SAE 21434

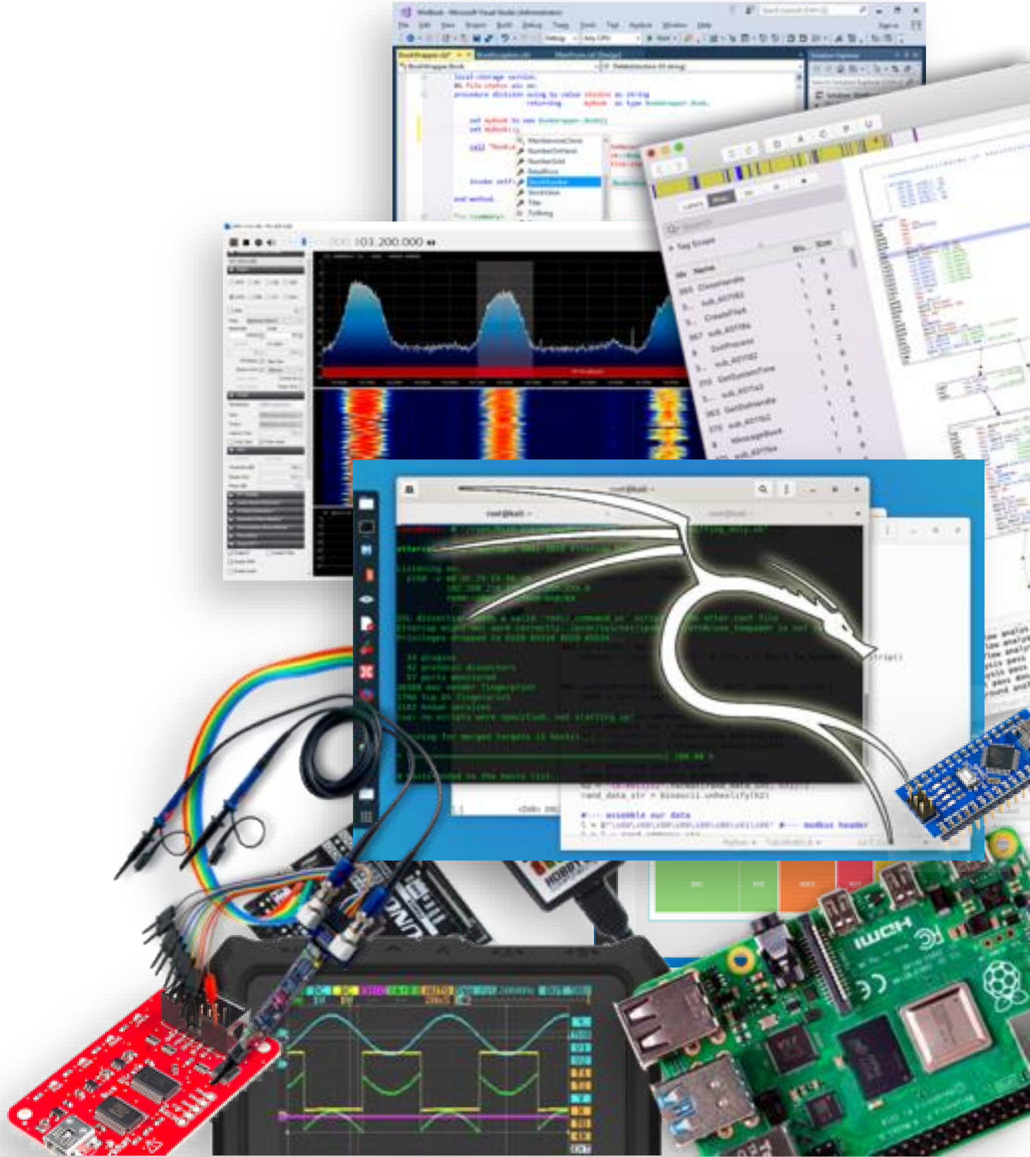
- ISO/SAE 21434 ” Road Vehicles – Cybersecurity Engineering” is an automotive standard that focuses on **managing cybersecurity risks in every stage of the lifecycle of a vehicle** and **across the entire supply chain**.
- With the volume of embedded software and increased connectivity in vehicles, compliance with ISO 21434 is essential for ensuring the security of EV software.
- The ISO standard covers all software devices within the vehicle, as well as connectivity to external systems.
- A few notes for software developers:
  - Adopt security culture: make security a priority
  - Choose the right programming language
  - Follow the secure programming design patterns
  - Add security and fuzzing to your CI/CD



Thorough independent security assessment is mandatory

Assessment steps are driven by the area of testing, methodology and our experience

- **Fingerprinting** automotive systems in scope (port scanning, non-invasive services probing, passive and active reconnaissance)
- **Identifying security weaknesses** in processes, systems, configurations or protocols in use
- **ECU security:** hardware, software, fuzzing
- Issues with **authentication and authorization**
- **Automotive protocols:** CAN, LIN, I2C, Automotive Ethernet
- **Security of all interfaces** (wired, wireless, diagnostic, GUI, CLI)
- **Firmware update** mechanisms (e.g. OTA)
- Security of **wireless communication** (WiFi, Bluetooth, BLE, proprietary protocols, etc.)
- **Internet of Vehicle (IVI) communication:** CAN bus, ECUs, Sensors, Actuators, T-box
- **Source code review**
- **Stress-testing (spoofing and jamming)** your RF and PNT equipment in scope
- Researching security features of the hardware in scope and **writing own exploits**



Professional testing the car's RF communication

University of Warwick together the Spirent lead the way to 5G automotive test innovation

UK-based University of Warwick together, with Spirent help carmakers understand how future vehicles will perform in the wireless network fast lane.

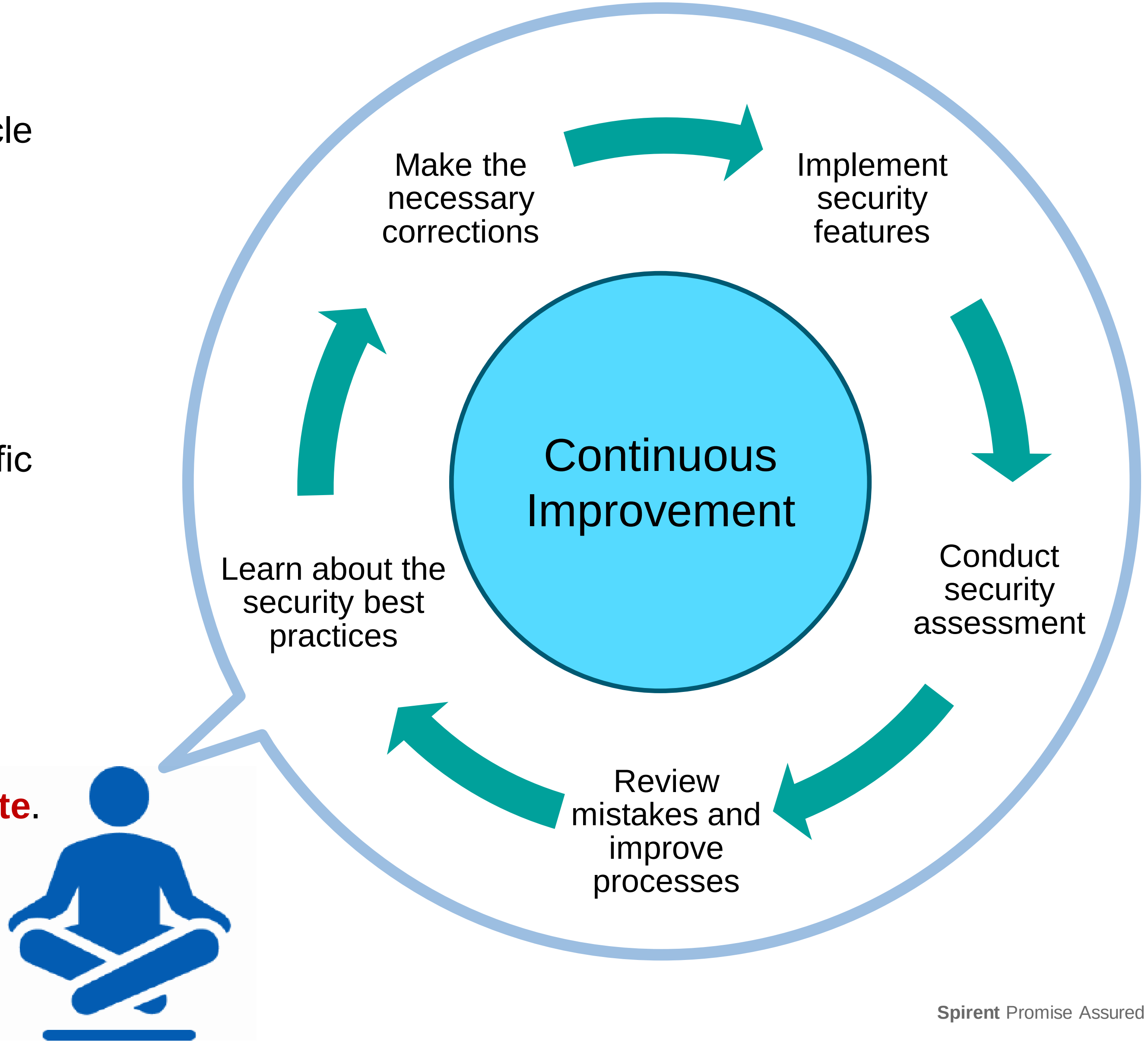
In conjunction with the University's Midlands Future Mobility (MFM) initiative, Spirent deployed 5G Digital Twin technology that emulates 5G networks for testing connected vehicles in a controlled environment, within a 3xD drive-in simulator operated by WMG.

Images: courtesy of University of Warwick and Spirent Communications

Takeaways: what to do to prevent the disaster?

Change your mindset first

- **Security testing is** a **mandatory** part of lifecycle of any modern car or its components
- Security is a **continuous process**, where an organization is learning and improving their processes and the security posture all the time *(very much related to "The Toyota Way")*
- A system can be called "secure" only in a specific moment in time. It cannot be "always secure", therefore **regular testing is imperative**
- **Adopt zero-trust mindset**: ensure sufficient authentication is everywhere
- **Eliminate unnecessary public IP** addresses
- Have always **software and firmware up-to-date**.



spirent™

securitylabs

Aleksander Gorkowienko
e: aleksander.gorkowienko@spirent.com
m: +44 (0) 7974431025