STELLANTIS

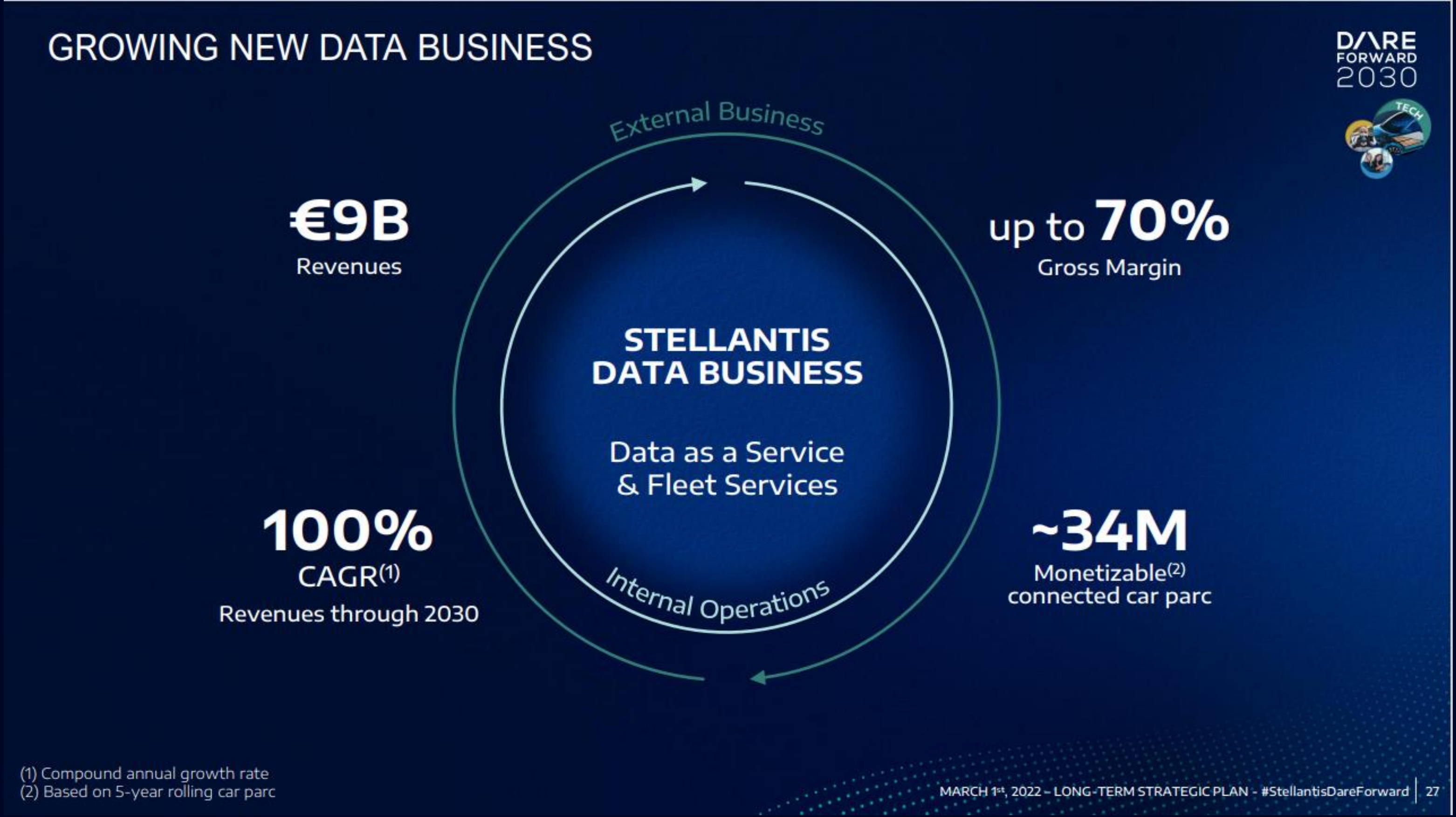
Cybersecurity per il veicolo connesso

Francesco Lilli
Global Head of Advanced Connectivity - Stellantis

April 11th, 2024 - Automotive e cybersecurity: vulnerabilità, sistemi di protezione e quadro normativo

WE LIVE
IN A INCREASINGLY
CONNECTED
WORLD

Stellantis Strategy → Dare Forward 2030



GROWING NEW DATA BUSINESS

DARE FORWARD 2030

€9B
Revenues

up to 70%
Gross Margin

External Business

STELLANTIS DATA BUSINESS

Data as a Service & Fleet Services

Internal Operations

100%
CAGR[1]
Revenues through 2030

~34M
Monetizable[2]
connected car parc

[1] Compound annual growth rate
[2] Based on 5-year rolling car parc

MARCH 1st, 2022 – LONG-TERM STRATEGIC PLAN - #StellantisDareForward | 27

Evolution of Vehicles - Then

Evolution of Vehicles - Now

STELLANTIS

Services (V2X)
to improve road user safety

Autonomous driving

Comfort and convenience connected services
to enhance user experience

Electrification

Anti Theft Services

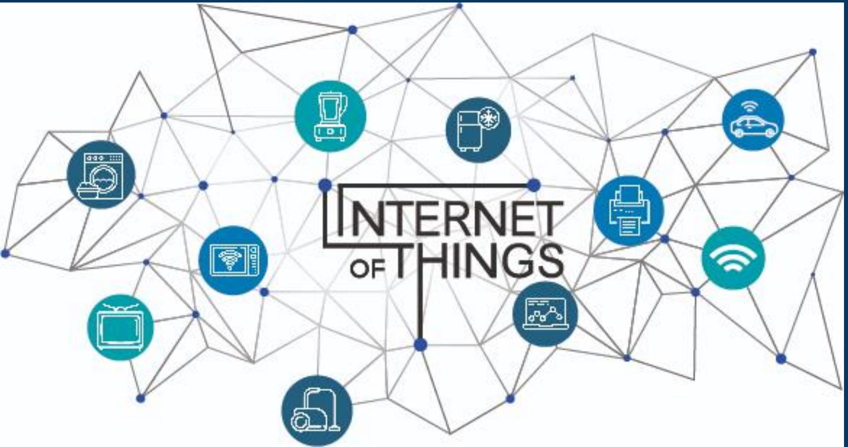
Software Defined Vehicles

STLA Brain
HPC Central
STLA Brain
Edge ECU
Ethernet Bus
ZONE FRONT
ZONE CENTER
ZONE REAR
Zone ECU

All these new features requires connectivity!

Vehicles are nodes in the Internet of Thing

(or its evolution… Internet of everything)



CYBERSECURITY

SW DEFINED CONNECTED VEHICLE

What Is A Cyber Attack?

Money

Intellectual property

Brand tarnishing

Politics, misinformation

Sabotage
nation state

Private Data

Ultimate aim – Money, Power, Ideology

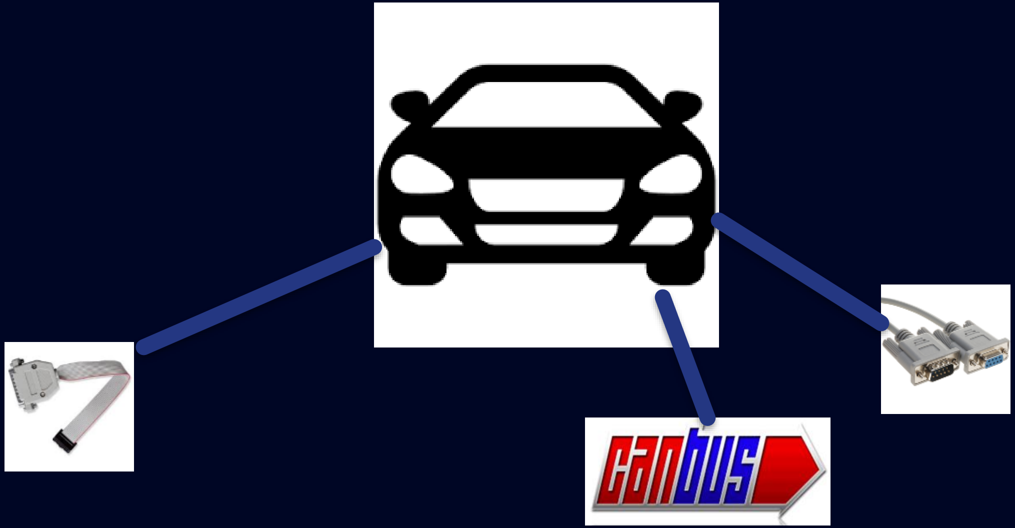
SOFTWARE INTENSIVE CONNECTED CAR

HACKABLE EXPOSED CAR

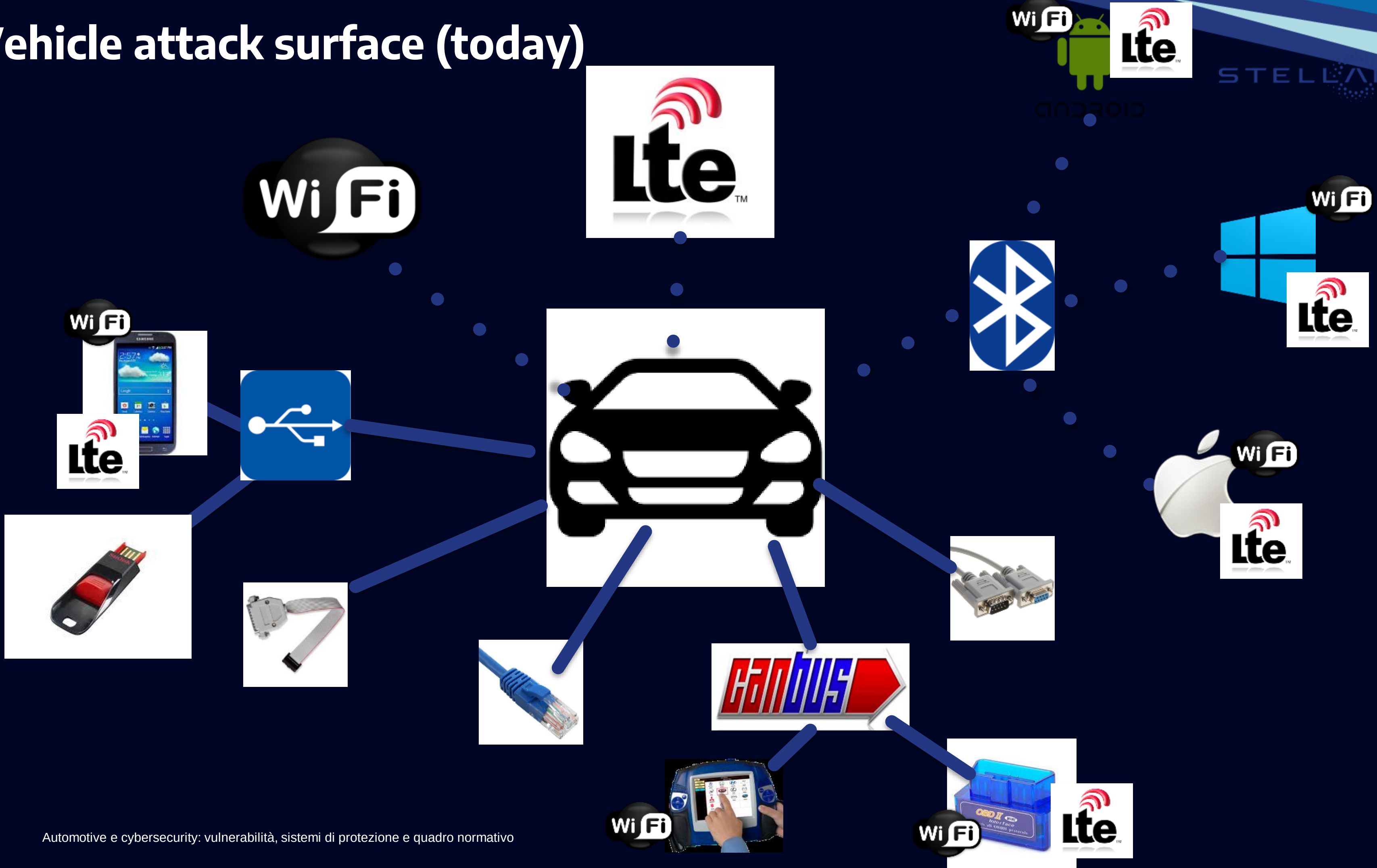
- → **Provide connected services and enhance driver experience with new features**

- → **Increase the attack surface and exposing the vehicle to cyberattacks!**

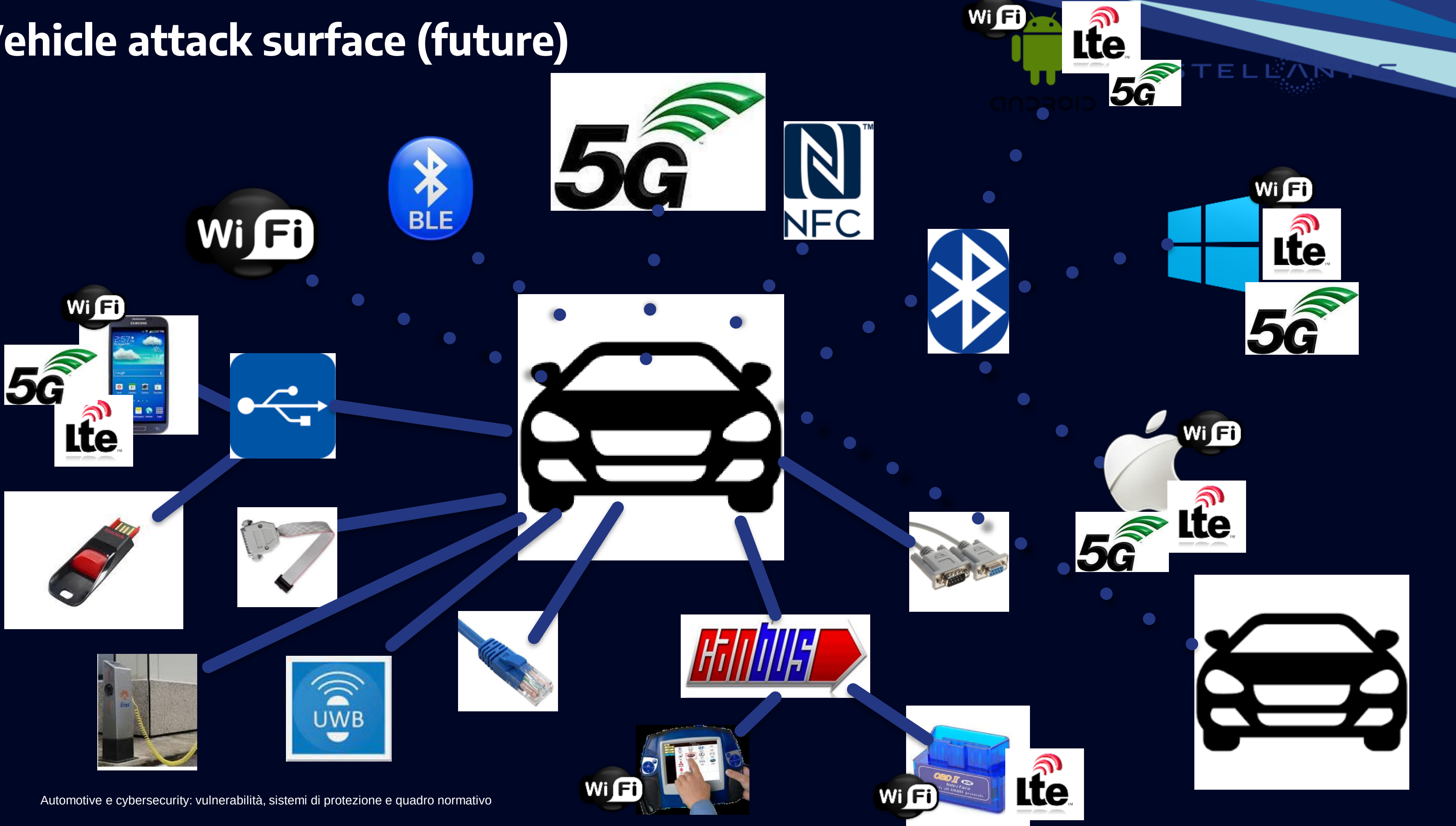
Vehicle attack surface (past)



Vehicle attack surface (today)



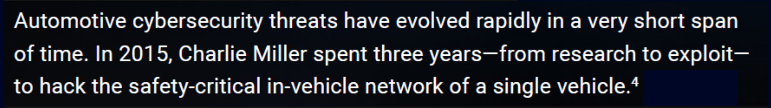
Vehicle attack surface (future)



Cyber attack impacts

July 2015

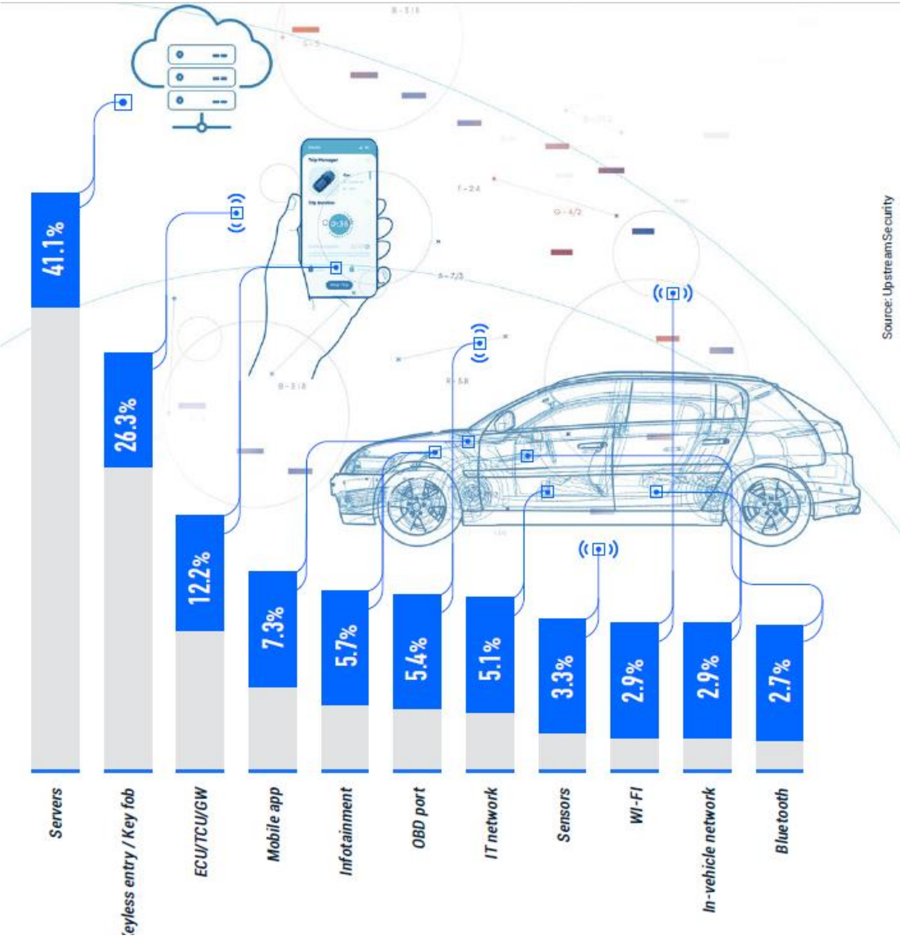
2015 old but… still relevant!


Automotive cybersecurity threats have evolved rapidly in a very short span of time. In 2015, Charlie Miller spent three years—from research to exploit—to hack the safety-critical in-vehicle network of a single vehicle.[4]

2024 Upstream Global Automotive cybersecurity report

April 2022

Most common attack vector

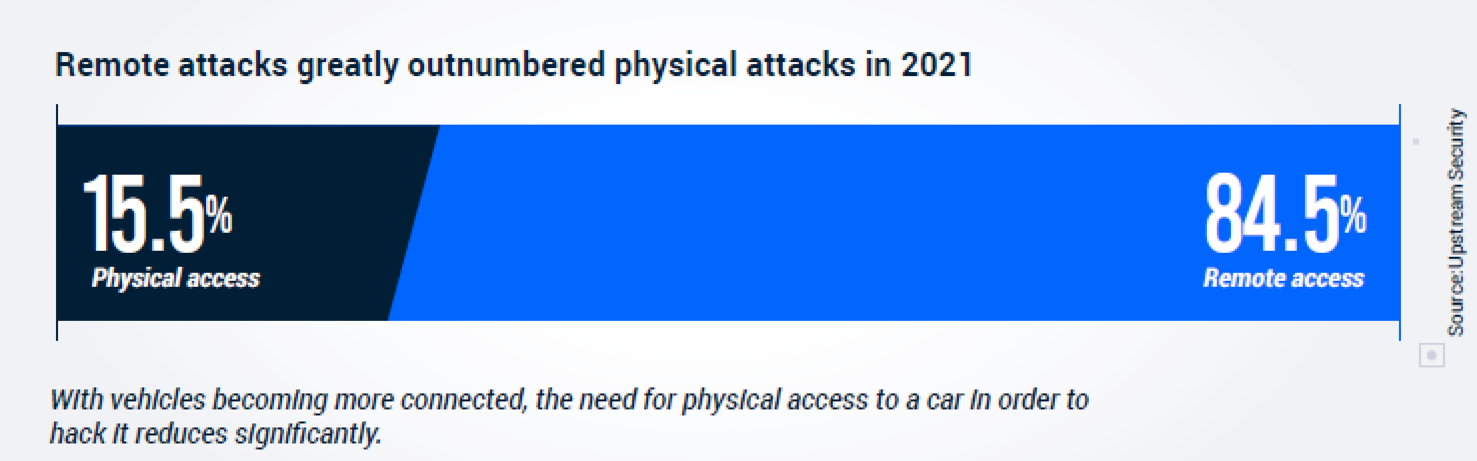


26.3% of the attacks on a connected vehicle are attacks aiming to steal the car

41.1% of the attacks on a connected vehicle are server attacks

Source: *UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2022*

Remote vs Physical 2022



Remote attacks greatly outnumbered physical attacks in 2021

With vehicles becoming more connected, the need for physical access to a car in order to hack it reduces significantly.

Source: Upstream Security

SDV and attack surface

With SDV the attack surface changes over time because Software (decoupled from Hardware) evolves over time… new features are added or updated…

What do we do at Stellantis on Vehicle Cybersecurity?

Secure by design

- Cybersecurity Policy
- Regulations & Privacy
- Threat Analysis and Risk Assessment
- Cyber security requirements

Secure Implementation

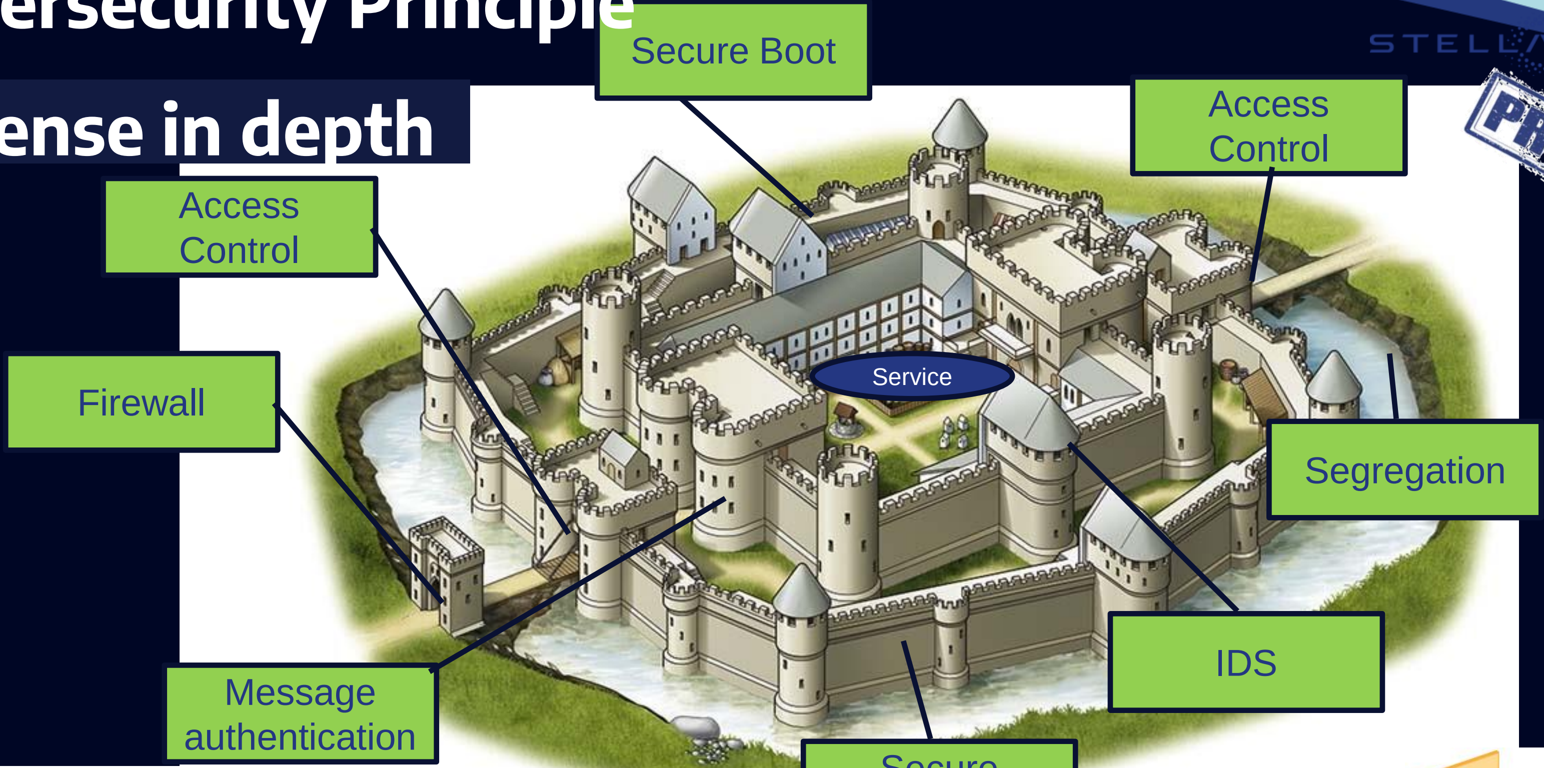
- Design and implementation reviews with suppliers
- End to end security - vehicle and connected services

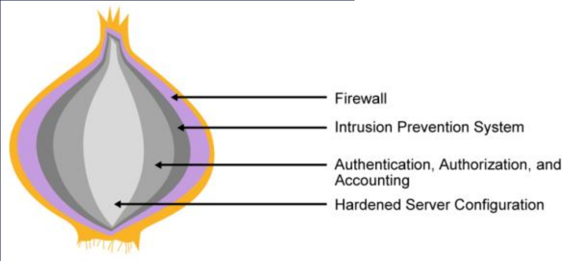
Security Testing

- Cybersecurity validation plan review
- Cybersecurity validation review

Cybersecurity Principle

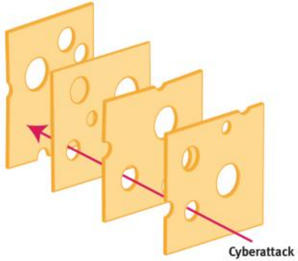
Defense in depth




Firewall
Intrusion Prevention System
Authentication, Authorization, and Accounting
Hardened Server Configuration

dro normativo

AKA onion model or Swiss cheese model



PROTECT

Cybersecurity principle
Zero Trust Model

PROTECT

Paradigm that eliminates the implicit trust and requires authentication and authorization at each stage of a digital interaction

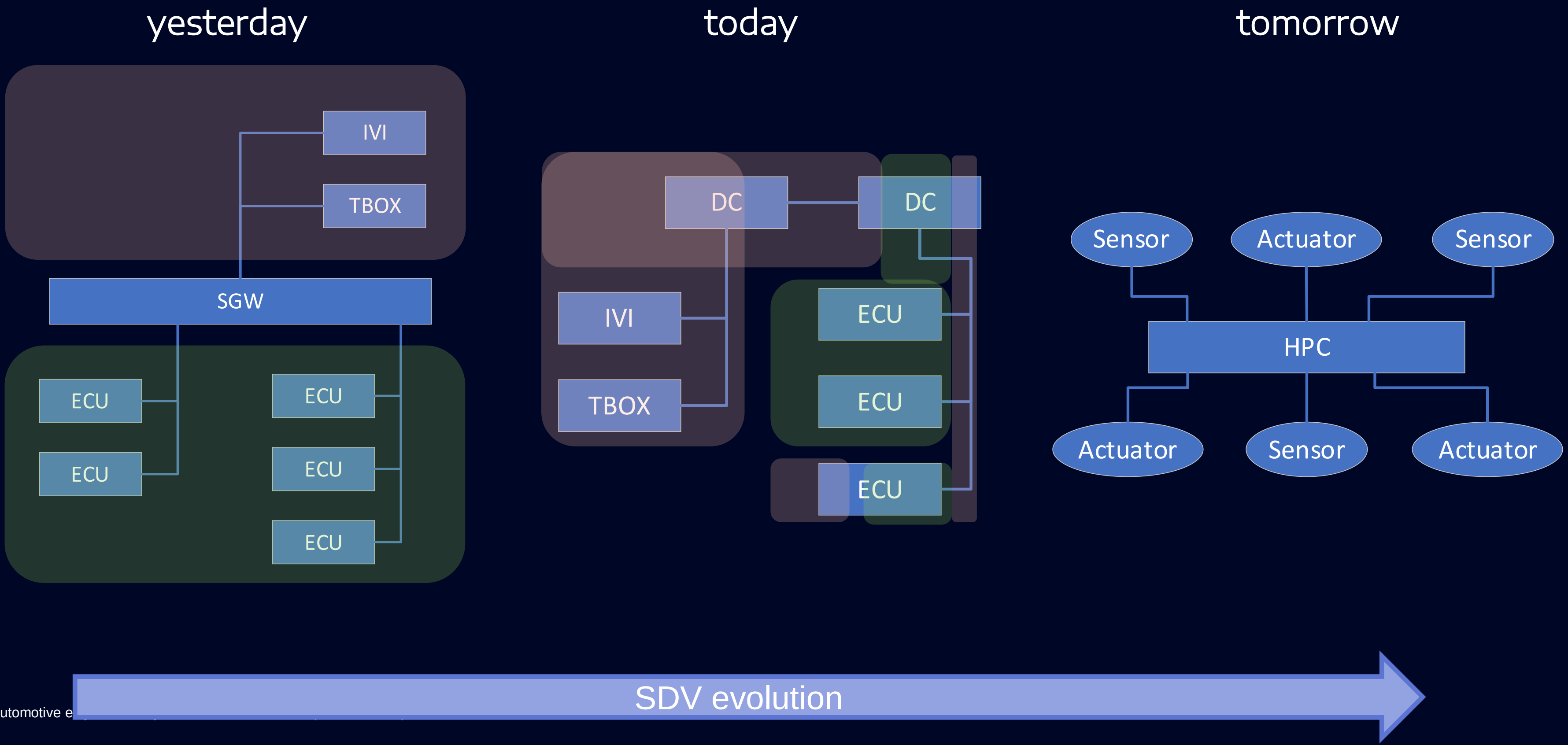
Network (vehicle architecture) location does not imply trust!

With SDV the network will shrink with function concentrating in HPCs.

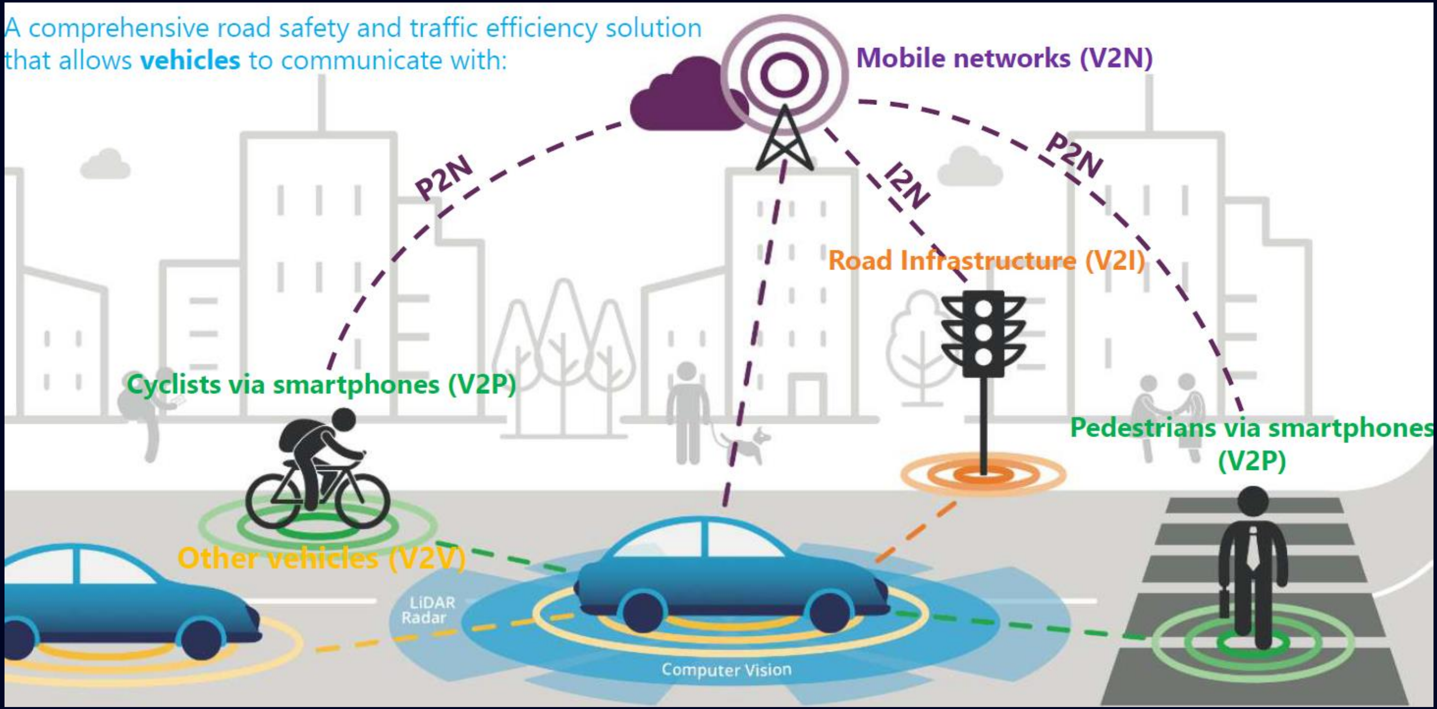
The old paradigm of untrusted network vs 'secure network' with firewalls in between is not working anymore

Cybersecurity principle
Zero Trust Model

Network location does not imply trust!



Connected Vehicles (CV) and V2X (Vehicle to Everything)



A comprehensive road safety and traffic efficiency solution that allows **vehicles** to communicate with:

Mobile networks (V2N)
P2N
I2N
P2N
Road Infrastructure (V2I)
Cyclists via smartphones (V2P)
Pedestrians via smartphones (V2P)
Other vehicles (V2V)
LiDAR
Radar
Computer Vision

Source: 5GAA Cellular V2X

Safety System:
“Connected vehicles ***enable*** *safe, interoperable networked wireless communications among* ***vehicles****, the* ***infrastructure****, and passengers’ personal communications* ***devices****.”*–USDOT

Safety and Traffic efficiency solutions. CV is a Safety System.
First step towards Autonomous Driving (AD)

Main security concerns in CV & V2X

Trust

- **Vehicle from different OEM must be able to trust each other, messages have to be authentic against sybil attacks;**
- **Vehicle must accept ITS messages only from legitimate ITS stations**
- **.... But authentication in connected services is not enough.... Trustworthiness is needed!**
- **Chain of trust to detect misbehaviour**

Misbehaviour detection

- **Vehicle that misbehave (injecting in the system false information) shall be detected and removed from trusted groups;**

Privacy (Anonymity)

- Drivers shall not be related to messages and vehicle behaviors;
- Multiple pseudonym Certificates are issued to vehicles to protect the privacy of the customer. These certificates are periodically refreshed.

Availability

- Safety messages have to be there when needed with very low latency

Integrity

- To be sure that data has not been tampered with while flowing in the system

our challenge is to make this possible at affordable costs on millions of cars on the roads

STELLANTIS

Grazie

CONTACT

Francesco Lilli
Global Head of Advanced Connectivity
francesco.lilli@stellantis.com

Corrado Derenale
Cybersecurity Architect
corrado.derenale@stellantis.com