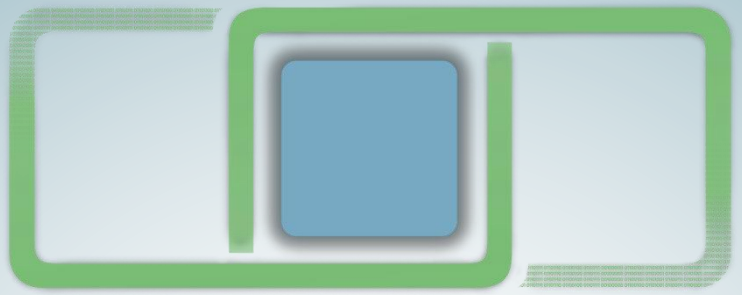


TAPPS

Trusted **Apps** for open CPSs

Secure Communication for Complex & Distributed Real-Time CPS

Marcello Coppola (ST) & George Kornaros (TEI)

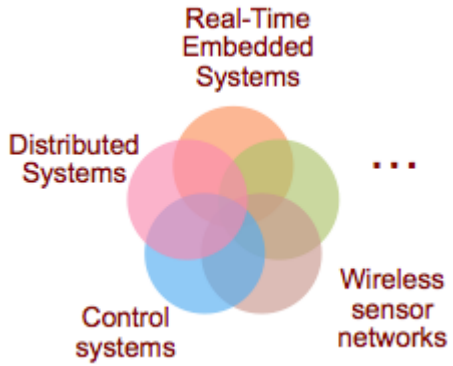
Co-funded by the Horizon 2020 Framework Programme of the European Union under grant agreement no 645119

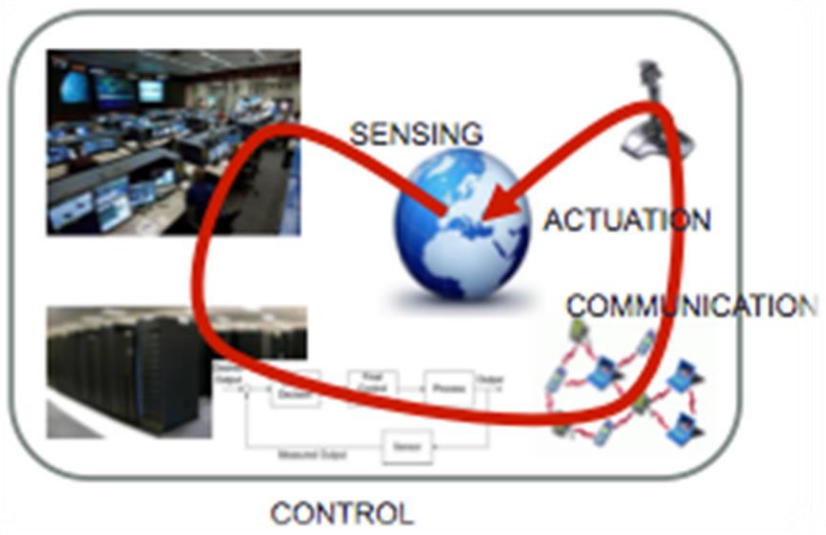
Outline

- Introduction
- Security in Open Cyber–Physical System
  - Secure Boot
  - Secure CAN
  - Secure FOTA
- Conclusions

Cyber-Physical System (CPS)

A cyber-physical system (CPS) consists of a collection of CPS units communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.

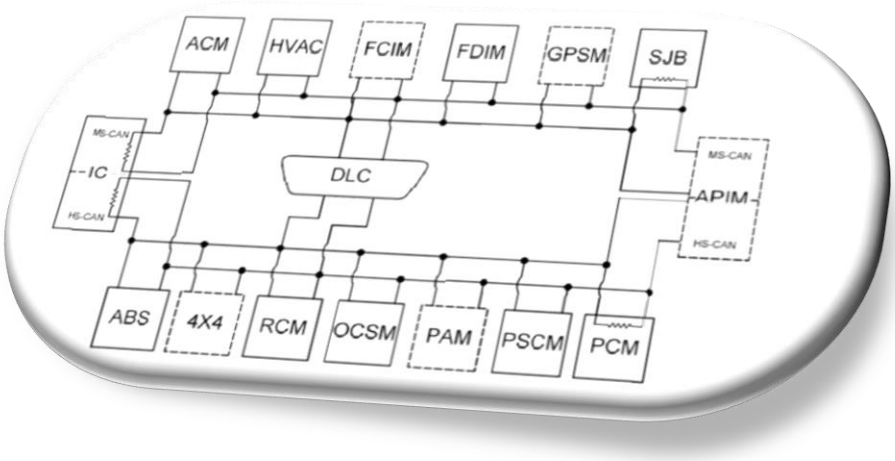


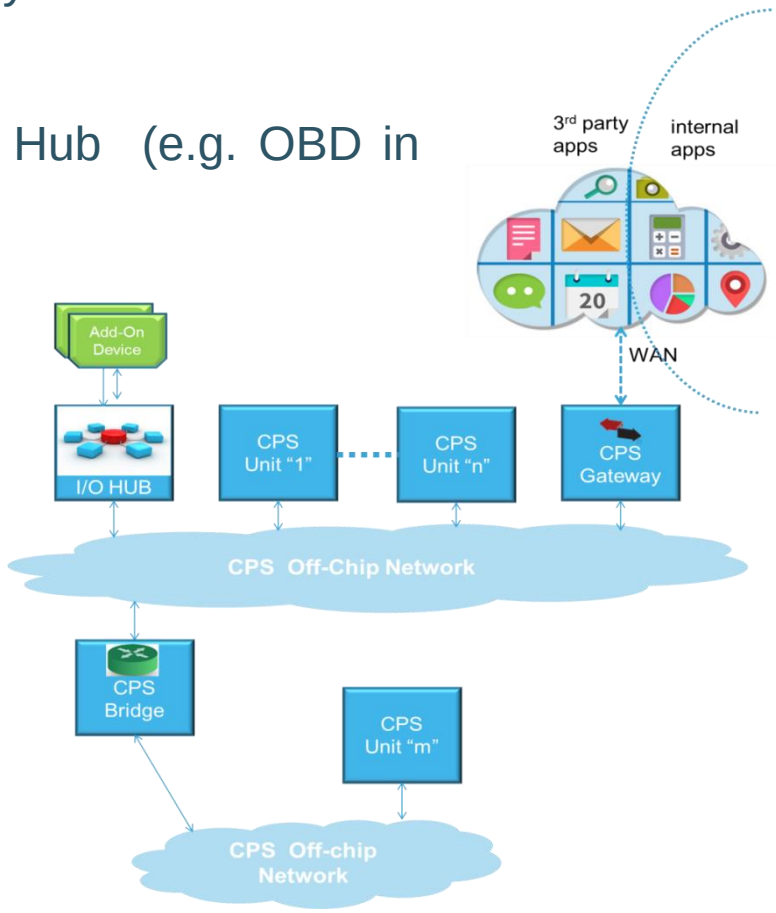


Open CPS

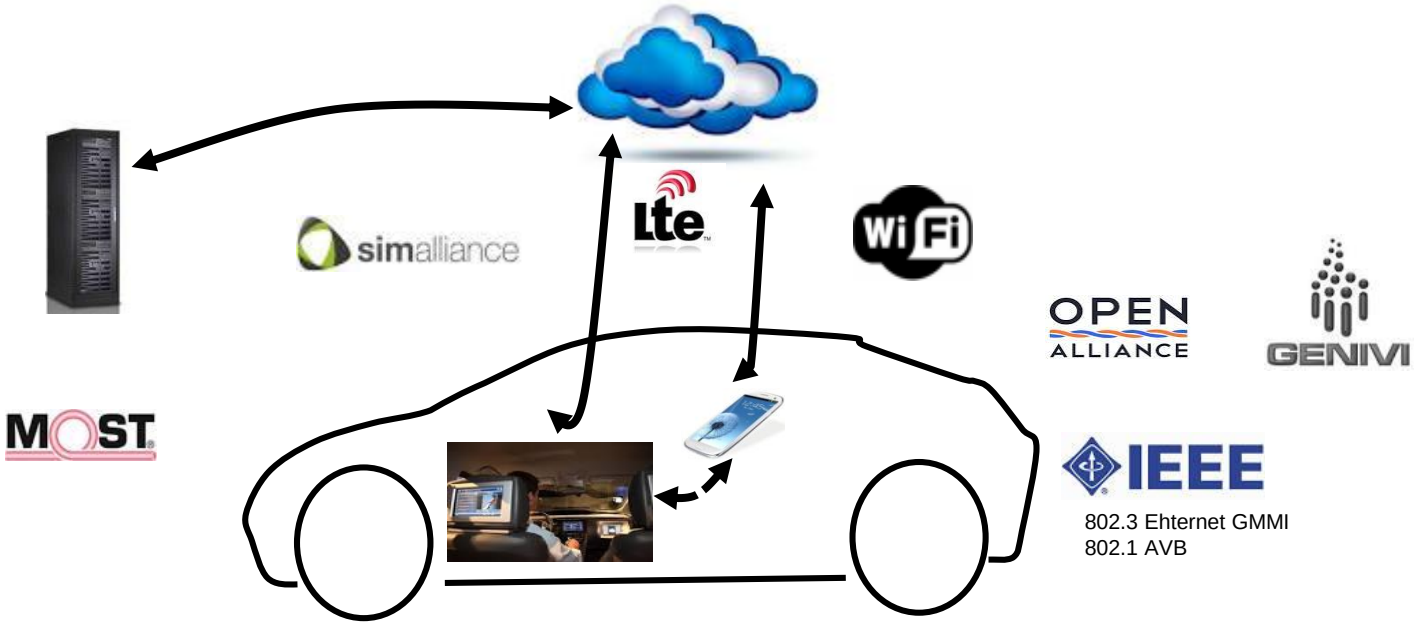
CPS system shall provide an open connectivity with the external world via the CPS gateway

CPS system may provide sockets via an I/O Hub (e.g. OBD in automotive)





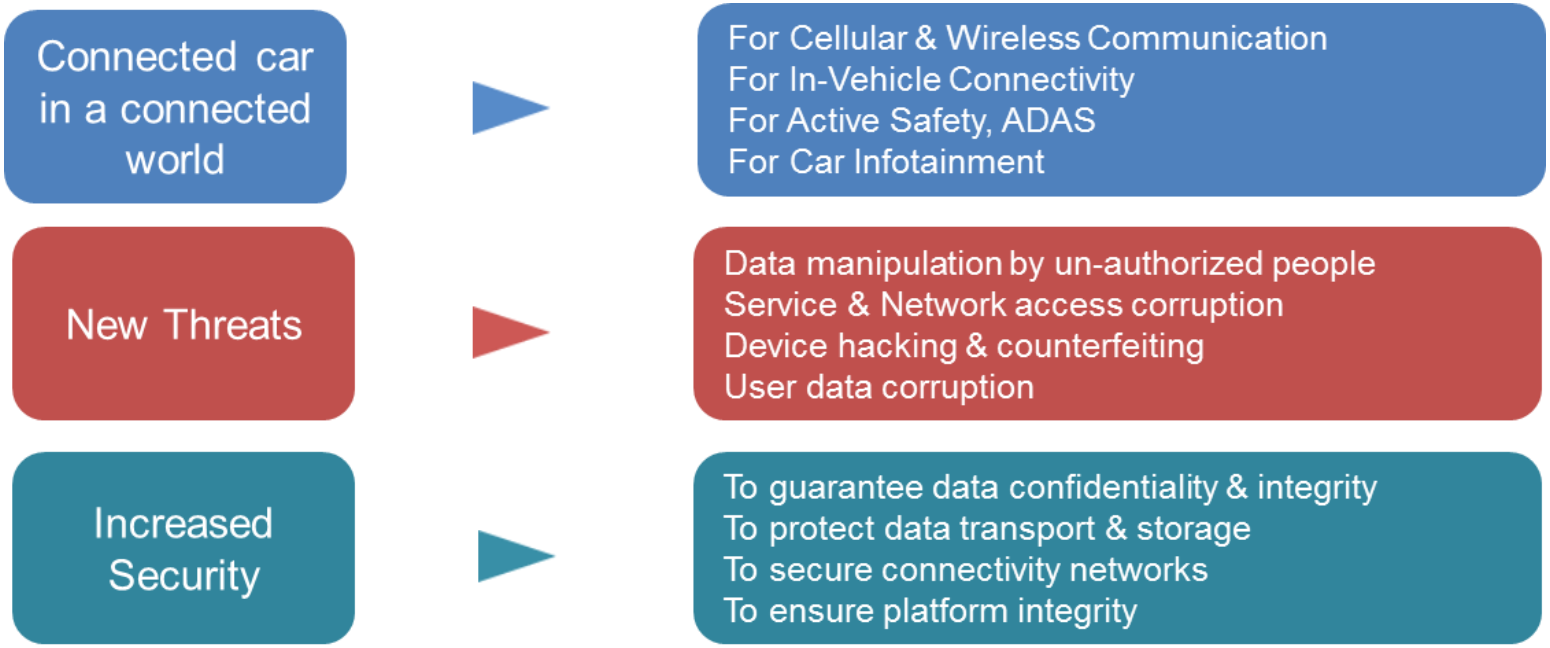
CONNECTED TO THE CLOUD



- Becomes an access point to the Cloud
- Platform data center & data distribution through efficient In-Vehicle Network

Security Is Not An Option

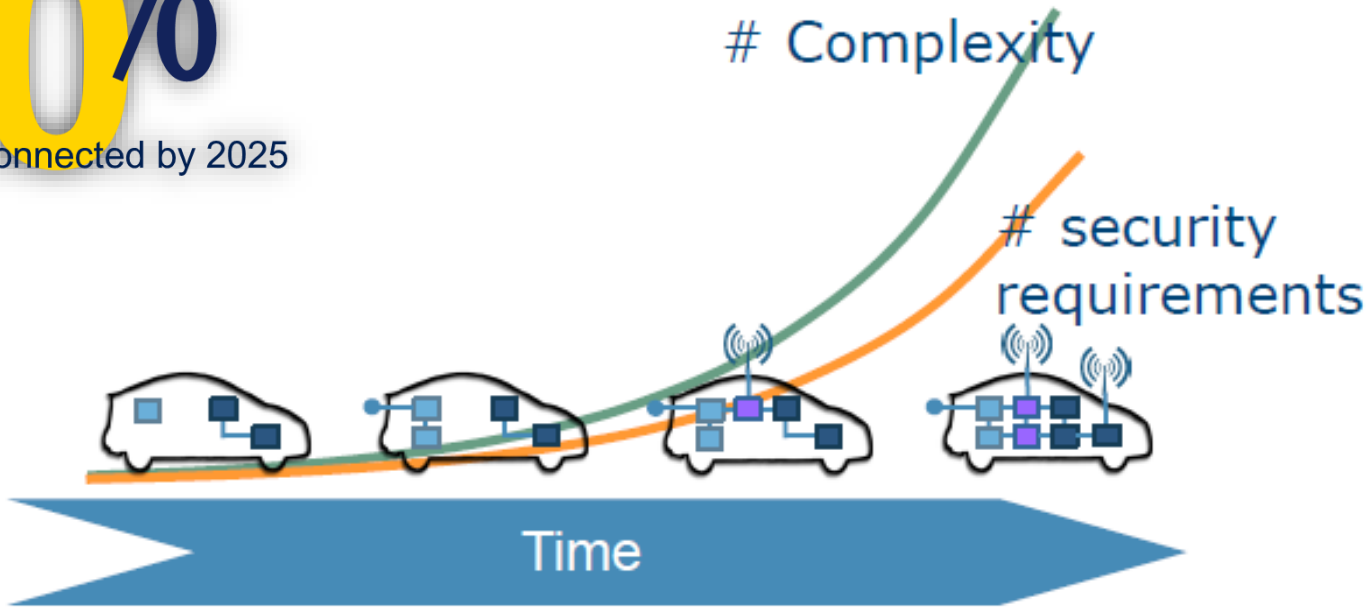
Connected cars need security



Security vs Complexity

100%

of Cars will be connected by 2025



Issuer: Henrik Broberg; Collaborative security version 2016-03-16; Security Class: Public External/internal distribution

Automotive Cybersecurity

- The number of attack surfaces, from wireless connections such as cellular, Bluetooth, Wi-Fi, and wired connections has dramatically expanded within the last few years.
  - The FCA Hack
  - GM and Tesla Hacks
  - Hacking BMW's App
  - Anti-theft Immobilizer Flaw Affects Numerous OEMs
  - Nissan LEAF Hack

Attack Surface

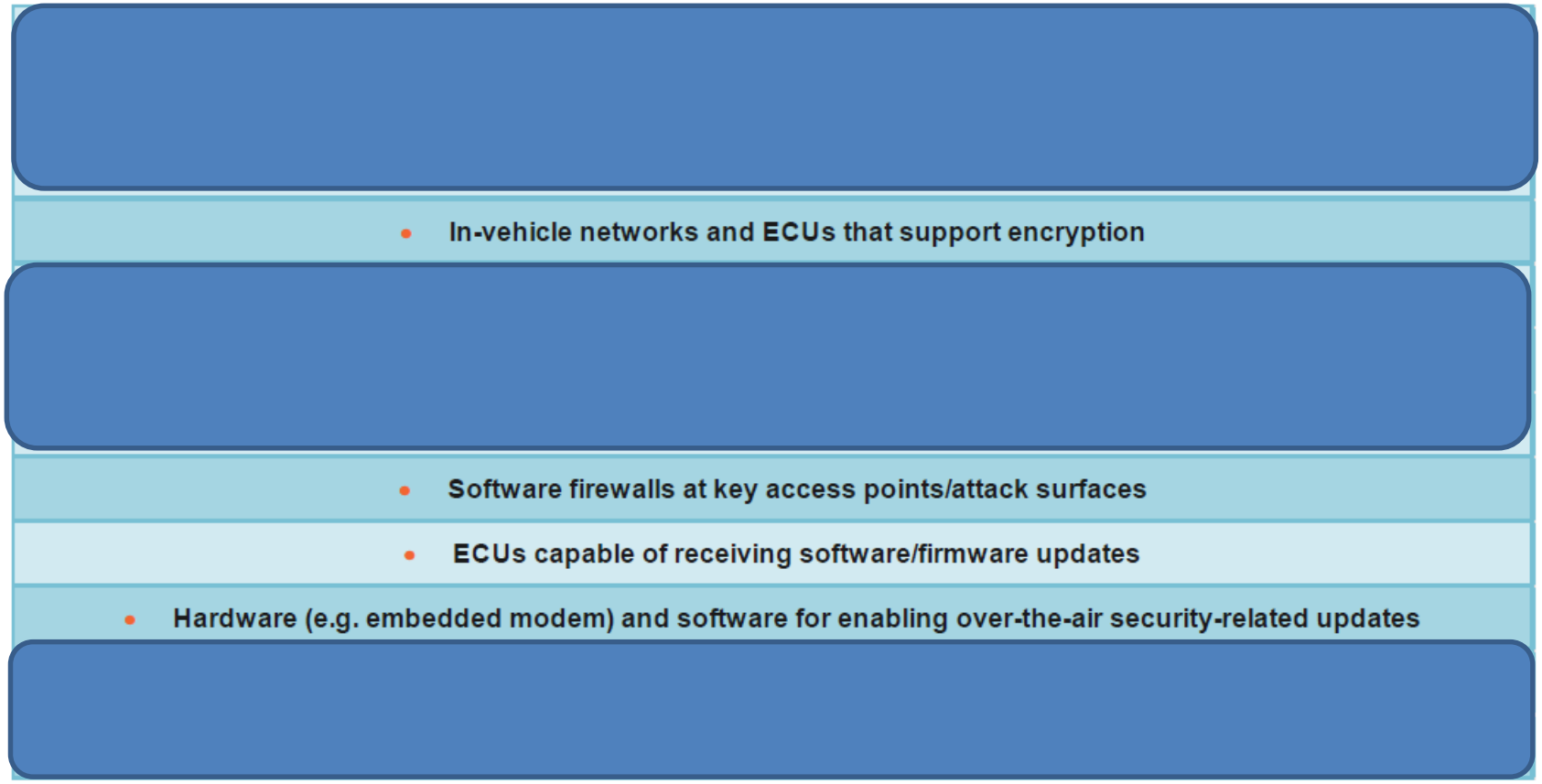
Physical Attack Surfaces		
Automotive Attack Surface	**Range**	**Threat Size**
CD/DVD Drive	Physical Access	Single Vehicle
USB	Physical Access	Single Vehicle
Flash/SD Card	Physical Access	Single Vehicle
OBDII	Physical Access*	Single Vehicle
Remote Attack Surfaces		
Automotive Attack Surface	**Range**	**Threat Size**
Bluetooth	~10	Single Vehicle
Cellular	~8 to 75 km (depends on coverage)	Vehicles On Network
Dedicated Short Range Communication	~100 to 1000m	Vehicles In Range (viral)
Electric Charging System	~5-20m	Single Vehicle
Electronic Tolling (RFID)	~5-20m	Single Vehicle
GPS	~150m to 8 km	Single Vehicle
Near Field Communication	~20 cm	Single Vehicle
Passive Anti-Theft System	~10m	Single Vehicle
Radio (RDS)	~100m	Single Vehicle
Remote Keyless Entry (RFID)	~5-20m	Single Vehicle
Satellite Radio	~100m	Single Vehicle
Tire Pressure Monitoring System	~1m	Single Vehicle
Wi-Fi	~15m/Varies	Vehicles On Network

*OBD II dongles could potentially have wireless attack surfaces (e.g. Bluetooth, Wi-Fi, or cellular) and make the OBDII port more vulnerable.

Source: Strategy Analytics

TAPPS is making Driving More Connected and More Secure

Multilayer Security

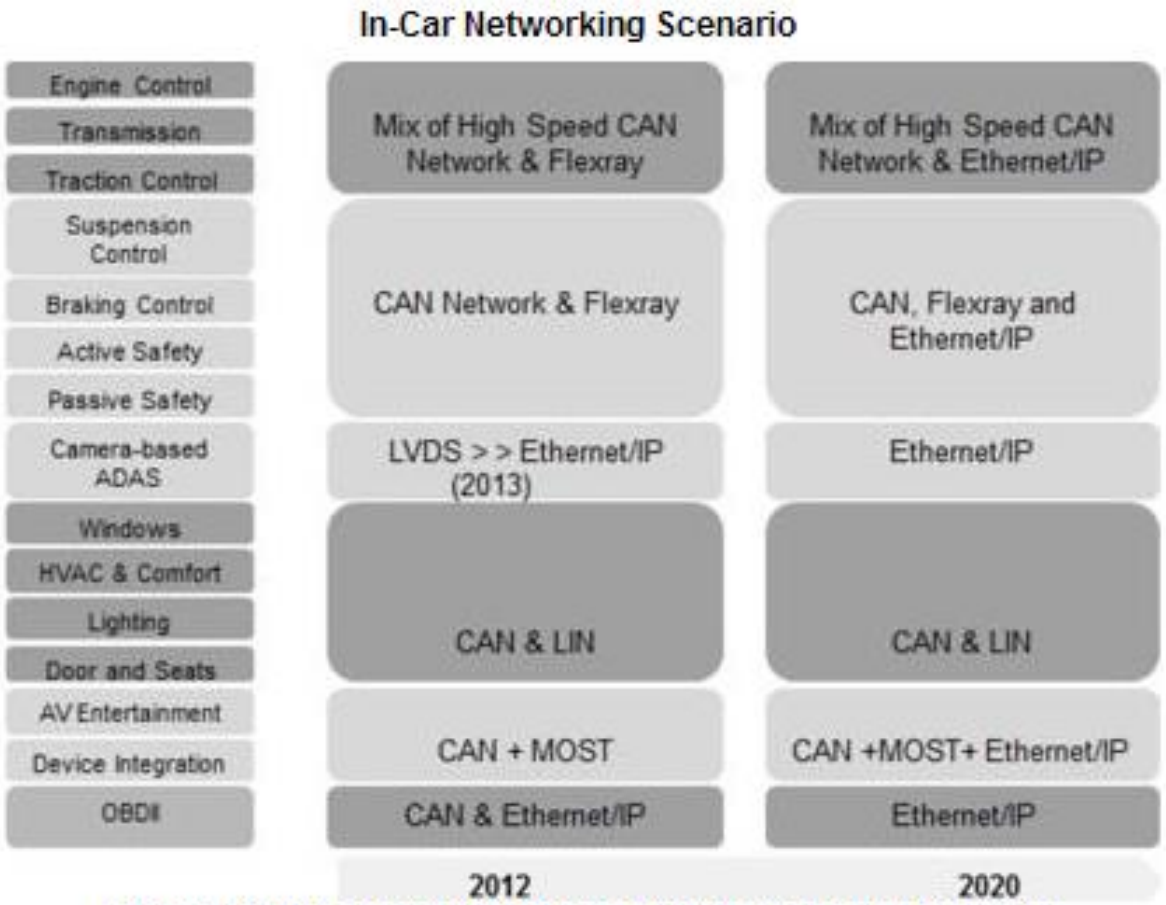


Source: Strategy Analytics

Trusted Boot

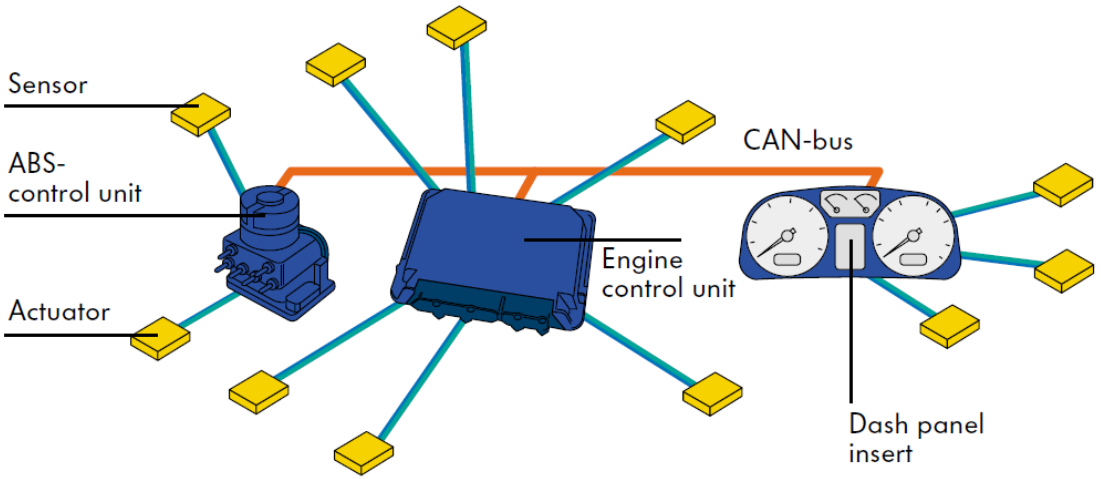
- To ensure a products integrity code should be authenticated before it is run
- Secure boot uses cryptographic functions to confirm the authenticity of a code image before allowing it to execute
- A multi-stage secure boot process, is one where each stage authenticates the next, hence a chain of trust

Why Securing CAN?



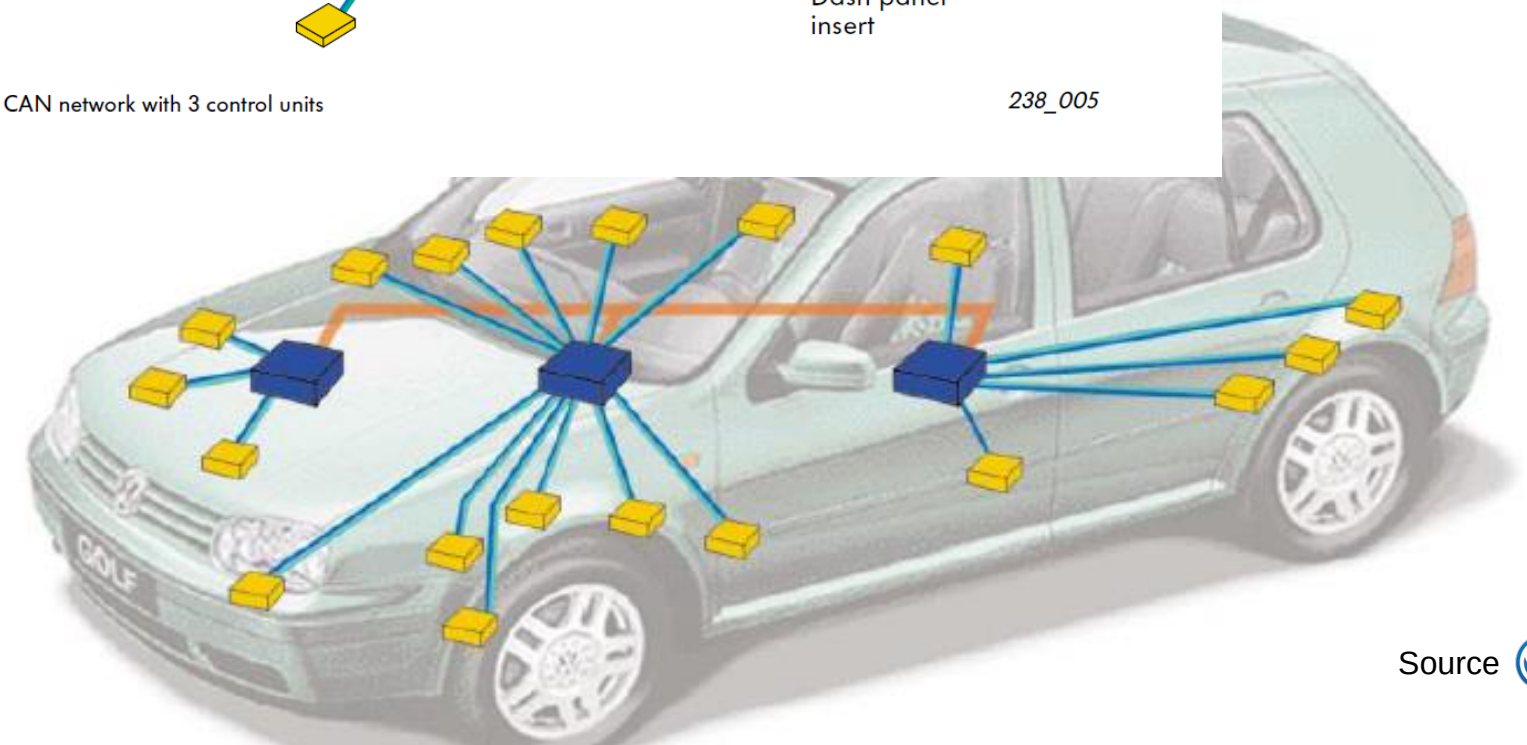
Ethernet/IP will coexist with low-bandwidth standards like CAN.
(Source: Frost & Sullivan)

Example of Drivetrain CAN



Drive train CAN network with 3 control units

238_005



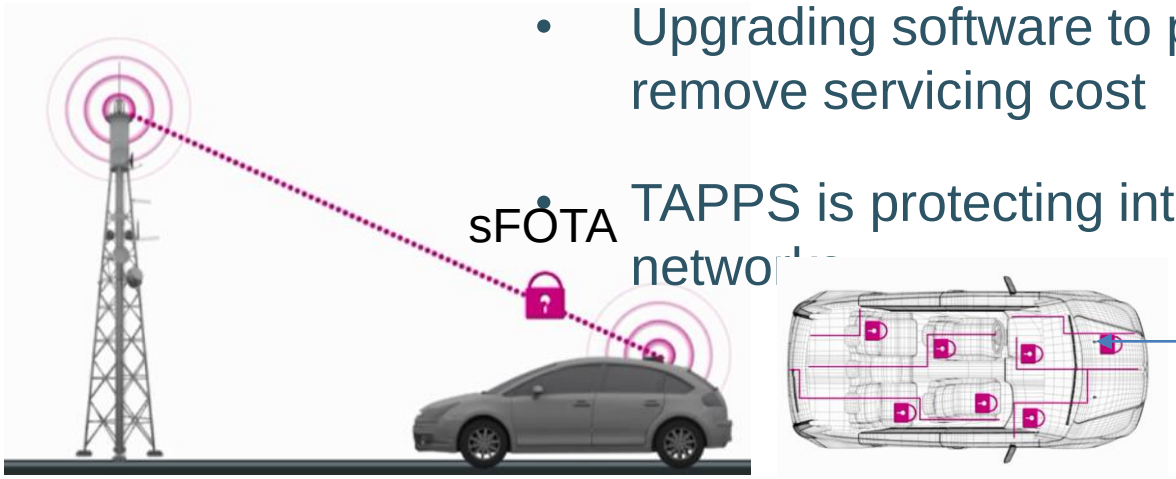
Source

Secure CAN (sCAN)

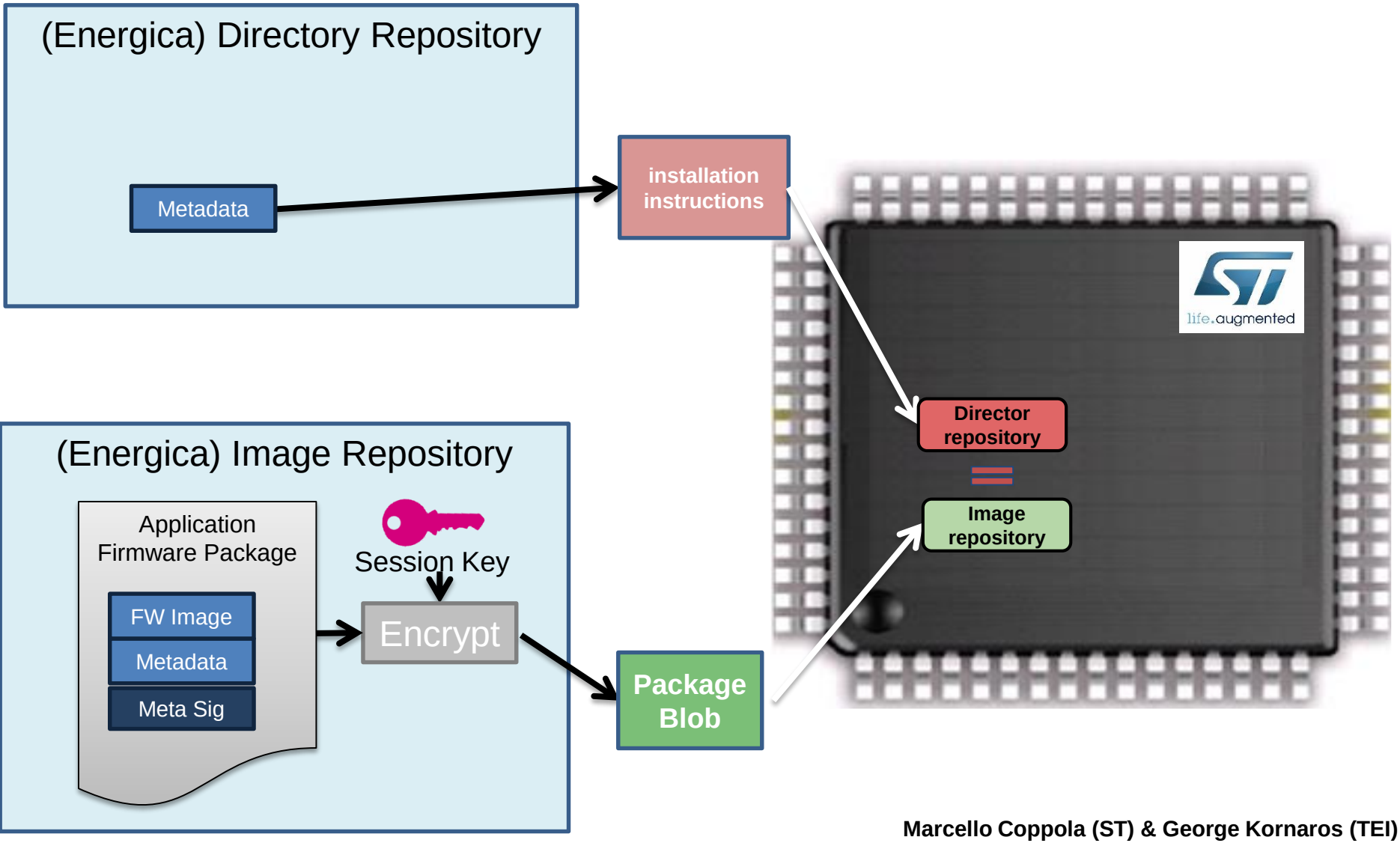
- to securing the communication between enables sCAN bus devices while supporting legacy CAN devices. More particularly to require low computation capabilities that enables real–time support
- to support in parallel secure and non secure communications
  - By the creation of a secure set of ECUs
  - by implementing secure broadcast communication within the secure set
- to support any high level protocol (eg KW2000,…)
  - No change required to standard CAN protocol and hardware
- to resource constrained ECU devices

Firmware Update Over the Air

- End-to-end vehicle security depends on securing all the electronic internal and external networks and ECUs
- Securing remote user interactions with the vehicle
- Increasing number of ECUs in vehicles combined with increased network capability creates more targets for compromising vehicle security
- Upgrading software to patch vulnerabilities and to remove servicing cost
- TAPPS is protecting internal and external networks



Secure FOTA (sFOTA)



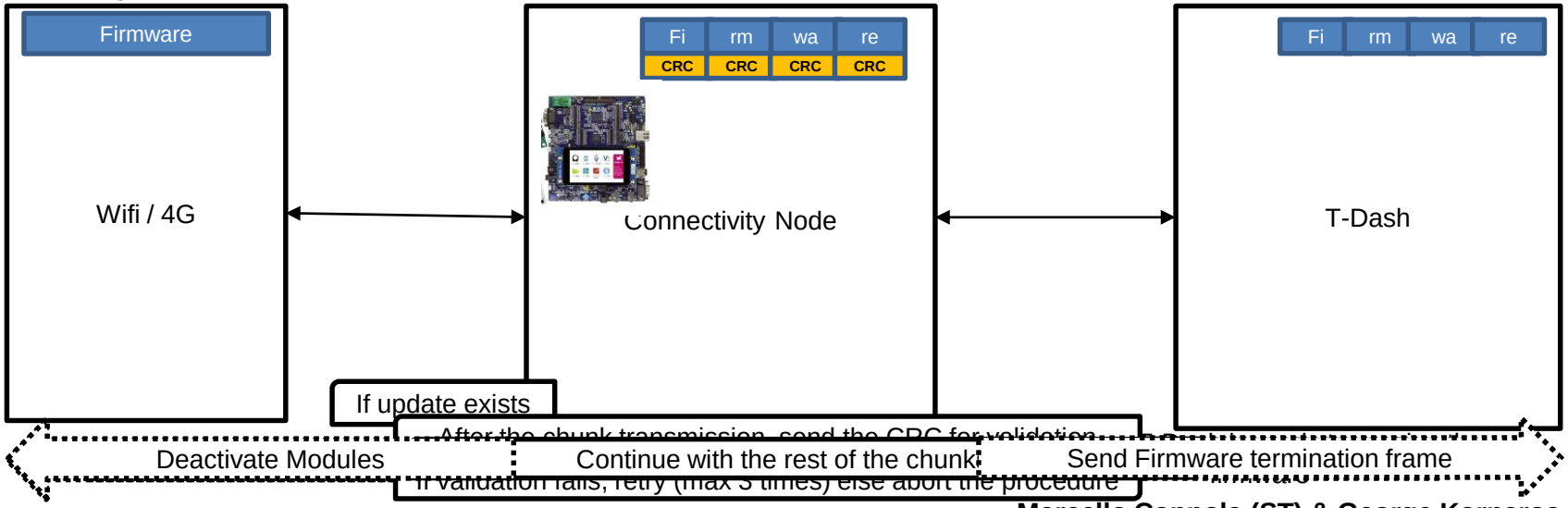
Marcello Coppola (ST) & George Kornaros (TEI)

Connectivity Node - sFOTA Procedure

Initialize
- Activate Wifi and 4G Modules

Main Execution (one-time)
- Check if Firmware update is available (internet)
- Download available Firmware update
- Start Firmware transmission procedure

Termination
- Deactivate Wifi and 4G Modules



Marcello Coppola (ST) & George Kornaros (TEI)

H2020 TAPPS: real testcase

Next generation Automotive DASHBOARD based on STM32 with external connectivity to WWW and secure CAN

Preliminary Prototype

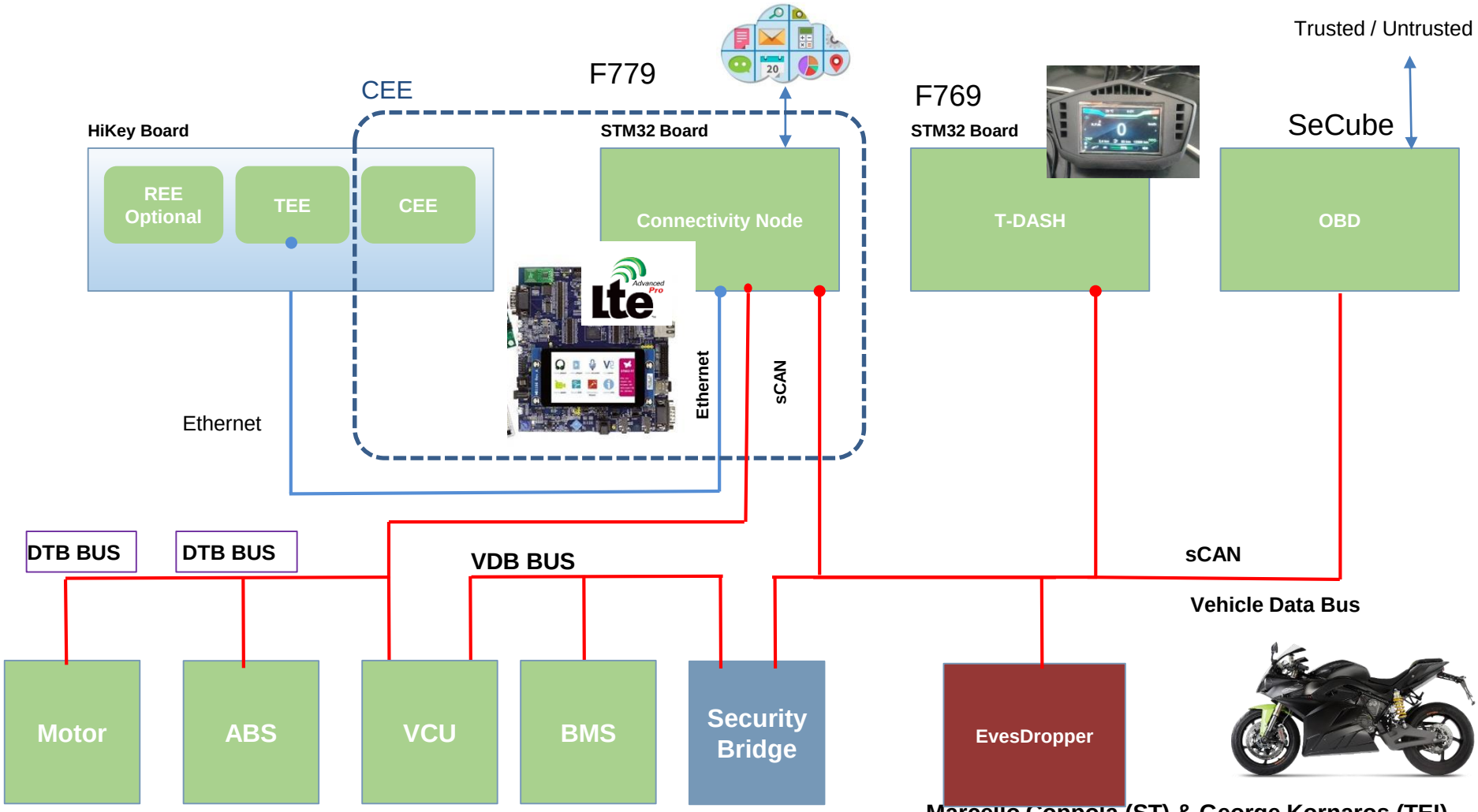
STM32 F7 + LTE Modem

eNERGICA

The Tesla of the motorcycles

Marcello Coppola (ST) & George Kornaros (TEI)

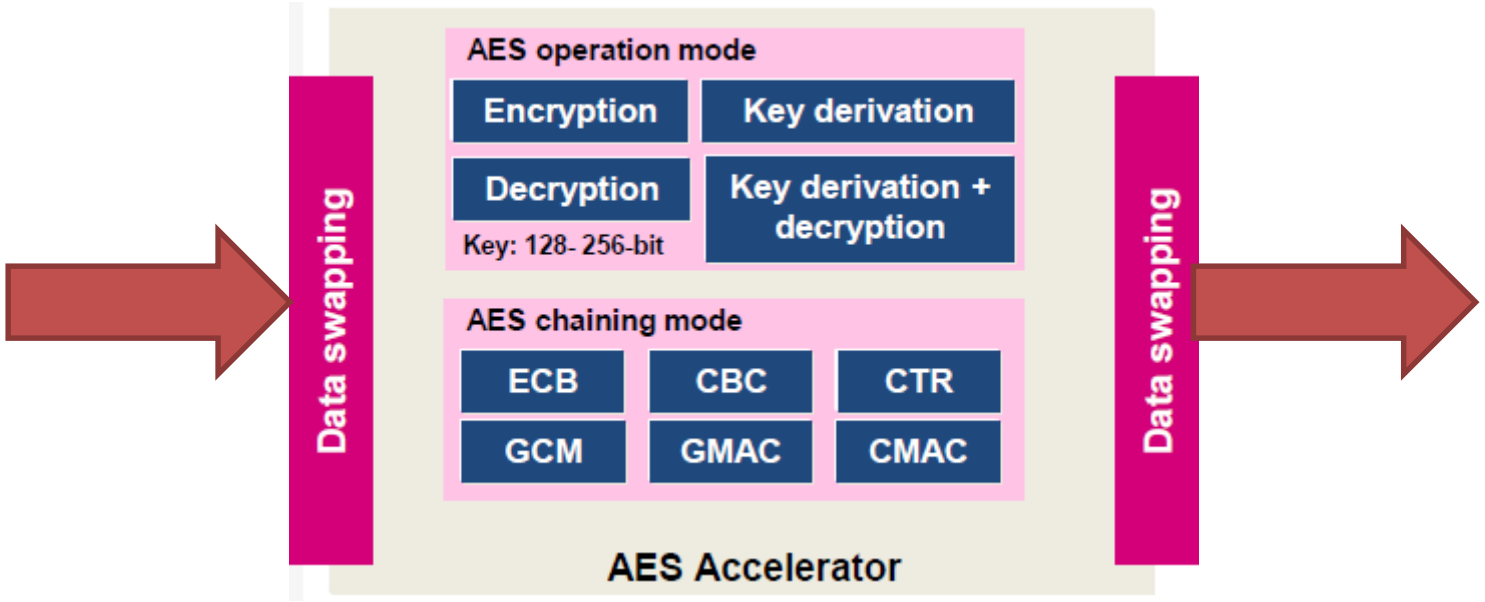
Takeaways: TAPPS in Automotive



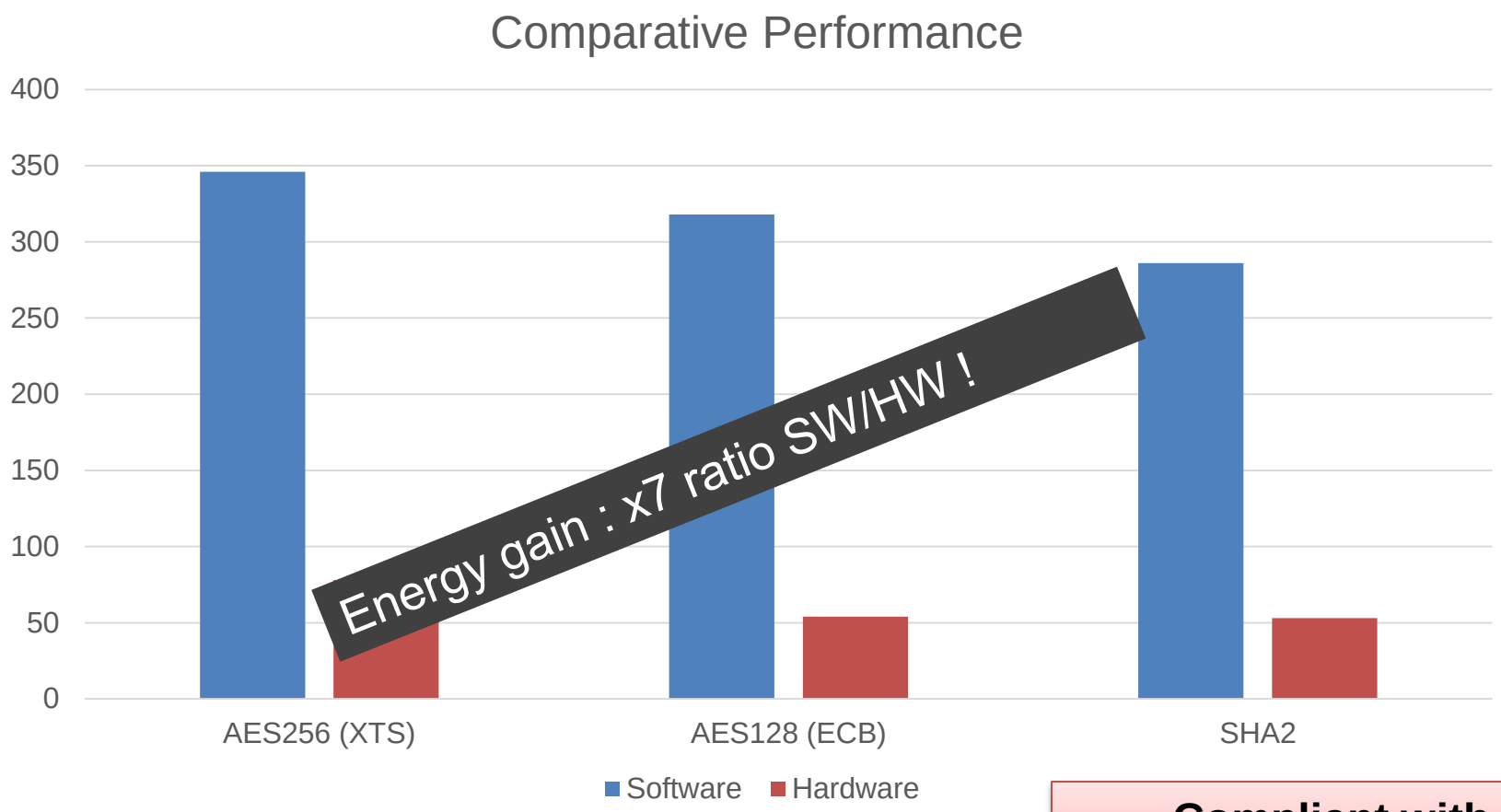
Marcello Coppola (ST) & George Kornaros (TEI)

Encryption Accelerators

- NIST FIPS 197 compliant implementation of AES



Crypto Acceleration on STM32F779NI



10K Iterations on 16B, CPU Freq: 192 MHz

Compliant with: FIPS Pub 180-2

Photo Source: slide