


Making Driving More Connected and More Secure



Marcello Coppola



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

Outline 2

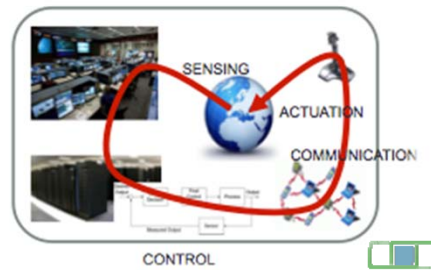
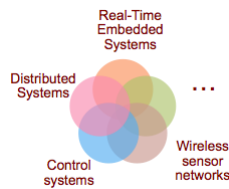
- Introduction
- Security in Open Cyber-Physical System
 - Secure SOTA
 - Secure CAN
- Conclusions



Cyber-Physical System (CPS)

3

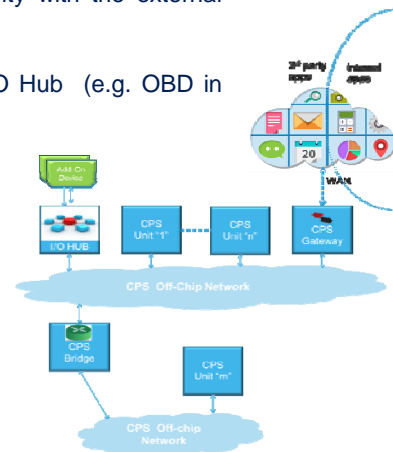
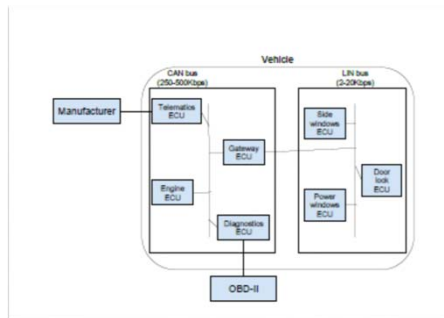
A cyber-physical system (CPS) consists of a collection of CPS units communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.



Open CPS

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

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





CONNECTED TO THE CLOUD

5

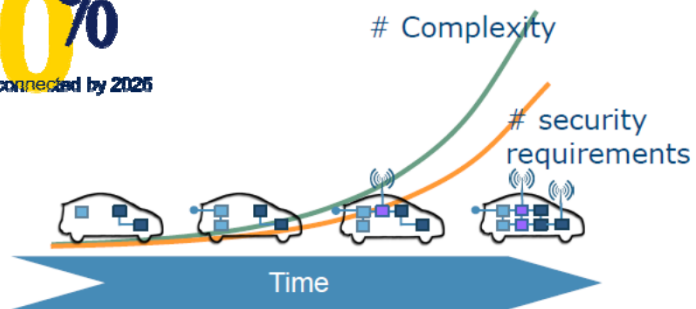
- 75% of shipped cars will be connected by 2020
- 100 sensors per car => 200 sensors per car
- 1.3M sensor readings per second
- Platform data center & data distribution through efficient In-Vehicle Network is key



Security vs Complexity

6

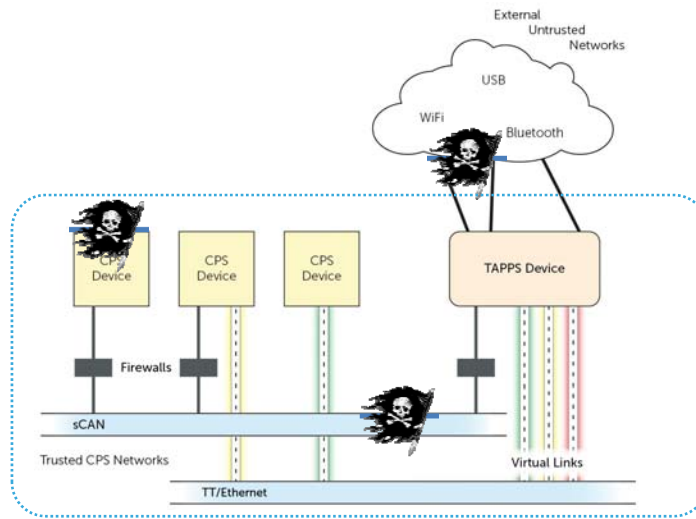
100%
of Cars will be connected by 2025



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



Setting the stage



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



Automotive Cybersecurity 9

- 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**



The FCA Hack 10



Software updates over-the-air (SOTA)

11

- Many good reasons to update software on vehicles over-the-air
 - Can improve existing features (e.g., better maps)
 - Can add new features (e.g., self-driving software)
 - Can update software bugs w/o expensive manual recall
- However, must do SOTA carefully, because...



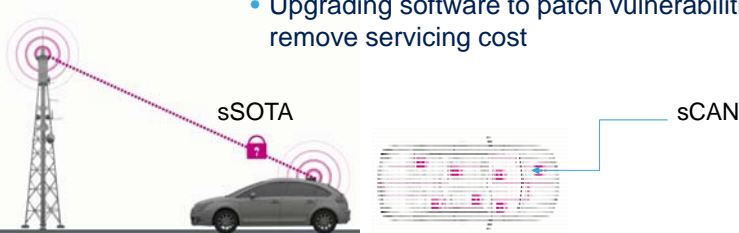
- Microsoft Windows Update (2012): Flame malware spread via MitM attack.
- South Korea cyberattack (2013): \$756,000,000 USD in economic damage due to malware spread partly via automatic software updates.

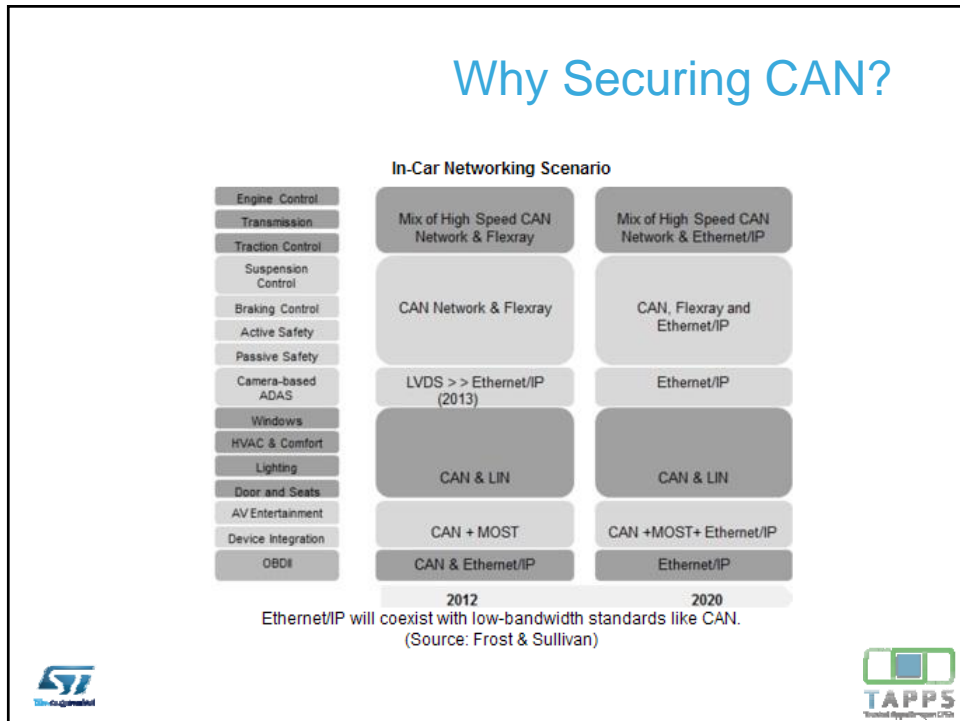
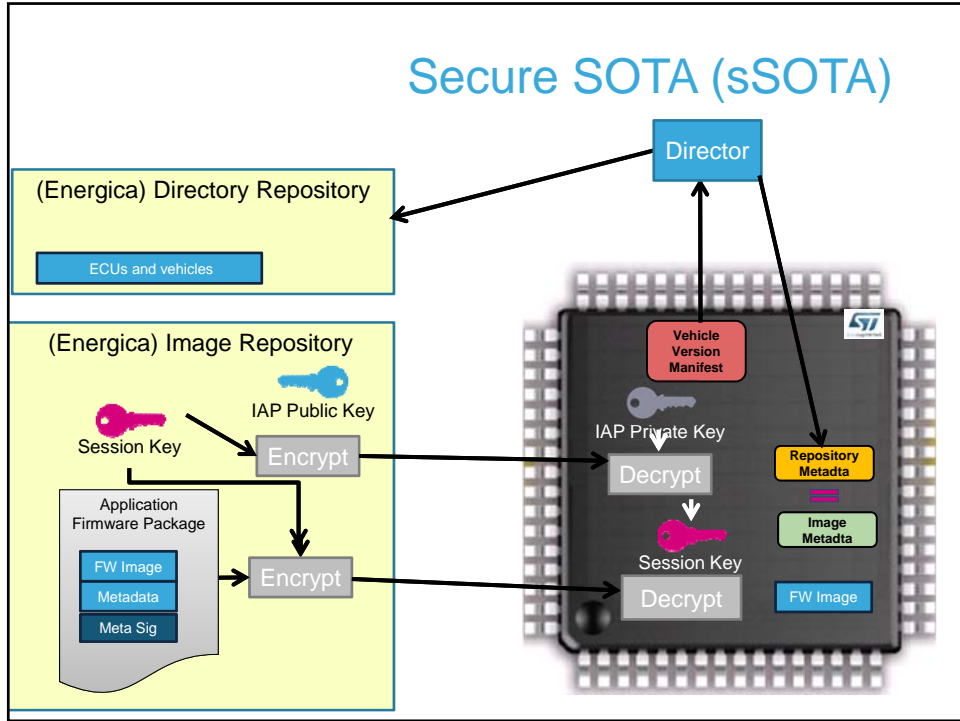


What More Secure Driving Means

Software Update Over the Air

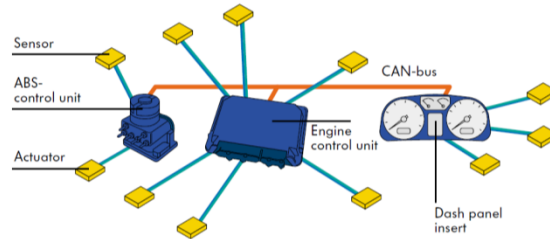
- End-to-end vehicle security depends on securing all the electronic internal and external networks and ECUs
- Securing remote user interactions with the vehicle
- Increasing number of ECUs in vehicles combined with increased network capability creates more targets for compromising vehicle security
-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





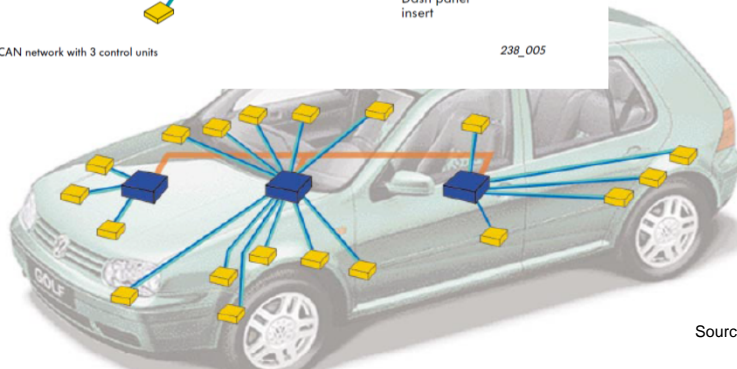
Example of Drivetrain CAN network

15



Drive train CAN network with 3 control units

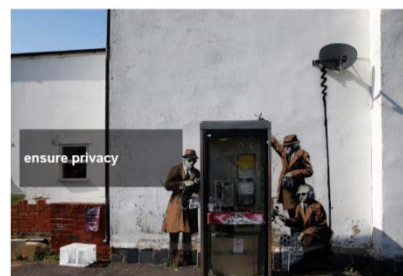
238_005

Source  

Secure CAN (sCAN)

16

- 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



H2020 TAPPS: real testcase

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

Takeaways: TAPPS in Automotive

