Prevent hacking for Connected Vehicle

GENIVI
27 April 2016

Eric DEQUI

Senior Expert in EE Architecture & Networks
Responsible for Cybersecurity activities on Connected Car

Summary

- Drivers of change : Connectivity & Uses Cases
- PSA and Connected Services Offers & Historic
- Technologies for Connected vehicle
- Connected & Autonomous Vehicle consideration
- Risk & Solution classification
- Security by Design
- Way for standardization
- Autosar & Genivi solutions
- Conclusion

Key Trends for evolutions

3 keys factors for evolutions with new Functionalities & Technologies

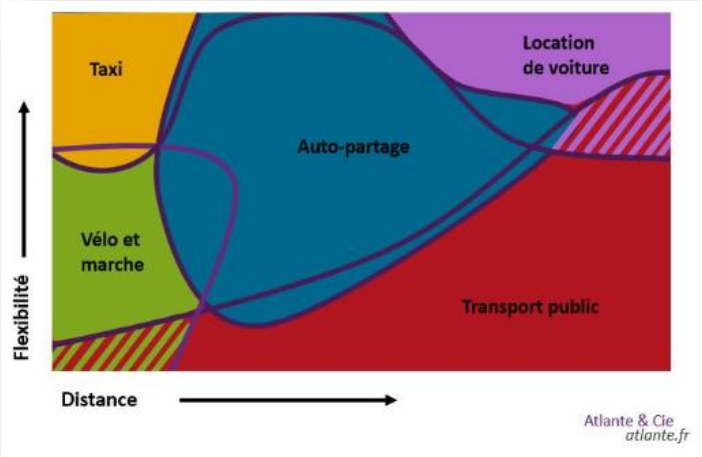
- ***Be Green* : Hybridization :**
  - ***Micro Hybrid*** : Stop & Start System with regenerative Braking (Diesel & Gasoline)
  - ***Mild Hybrid*** : Introducing 48V Technology with Battery Li-ion
  - ***Full Hybrid*** : Introducing Plug-in & Autonomous optimization (Batt Li-ion)
  - ***Full Electric*** : First generation with Ion Peugeot and C0 Citroën

- ***Be Safe* : Advanced Driving Assistance (ADAS) :**
  - **Parking Assistance** : Interaction between several functions
  - **Driving Assistance** : Introducing Radar, Lidar, Camera Technologies
  - **Driving Automated** : Highway Chauffeur, Traffic Jam Chauffeur

- ***Feel @ Home* : Connected Car**
  - Connectivity for services (Telediagnostic, Teleservices, Teleassistance)
  - Car To X communication for Safety, Depolution, Infotainment
  - Vehicle to Grid (V2G) for Smart Grid connection (Plugged Vehicle)

☞ ***Multiplication of features increase the complexity of EE Architecture…***

Connectivity : Uses Cases



Change of user styles

- Car sharing public or private
- Multimodal Transport
- Internet of things (Big Data)

Assistance for Customer & Compagnies

- Emergency Call (*e_Call*), Assistance Call (*b_Call*)
- Fleet management public or Private
- Remote Diagnosys, Remote Maintenance (software update *Over-the-Air*)

Security : Help for autonomus car (Autonomous Driving Assistance)

- Connected vehicle to increase the security (hazard warning, automatic brake)
- Solution Car_to_X (802.11 / G5.A/B) : see as additionnal detection sensor for ADAS
- Recommended Speed, warning zone, weather alert, accident area, …

CO2 reduction

- Connected vehicule to reduce the CO2 emission
- Coupling speed control with navigation (road profile + speed + traffic)
- Green wave : adjusting the vehicle speed and synchronization with traffic lights

Electrical & Hybrid Car with the Smart Grid

- Communication with the vehicle plugged during recharge (Hybrid or Electric Vehicles)
- Using Wireline (powerline) or wireless (3/4G, wifi, bluetooth, NFC)

PSA Connected Vehicle History

1st Generation (before 2012) : GSM, Bluetooth

- 2003 : *Emergency Call* (eCall) and *Customer Assistance* (bCall)
- 2007 : Stand alone Telematic Communication Unit (TCU)
- No customer data acquisition & No Data mining in IT Servers

2nd Generation (after 2012) : GSM, USB, Bluetooth, Wifi

- 2012 : Peugeot Connect Apps on 208 (with USB/GSM Key)
- 2014 : Connected Navigation / B2B, B2C Services
- Fleet Management for company with driving data
- Customer Eco-Coaching : Fuel consumption, Kms, travel time, alert,…
- Mirror Link : screen smartphone deported
- Telediagnostic : Read & Erase default code (DTC)
- Remote Control : lighting activation, doors unlock

3rd Generation (2020) : 4G/5G, Wifi, Wifi.p, NFC, BTLE, …

- Remote Control : Function remote activation : Thermal preconditioning, Park assistance, Home Zone Trajectory Replay, ...
- Software update : Over-the-Air and Download Services
- Big Data : Data processing (ECU Data collection, Data storage, calculation in IT Servers)
    1. Mission profiles for vehicle design
    2. Preventive Maintenance, Quality amelioration, Crisis prevention, …
    3. Customer services sales

PSA Connected Services offers

Remember : PSA pioneer since 2003 on Emergency Call (e_Call) and Automated Assistance (b_CALL) with 1.7 million connected cars

Car sharing B2C

- ***Multicity Berlin*** with 250 Electrical Car (C0 Citroën)
- ***Partnerships*** with *Bolloré* and *Koolicar* for B2C car sharing
- ***Peugeot Rent***

PEUGEOTRENT
LOCATION DE VOITURES PEUGEOT

Fleet Management B2B

- ***Connect Fleet Management*** with 10000 connected car
- ***Share Your Fleet*** for B2B car sharing

Smart Devices

- Services to offer intelligent car for Smart Cities
  - Automatic parking payment with any customer action
  - Pre-heating remote control

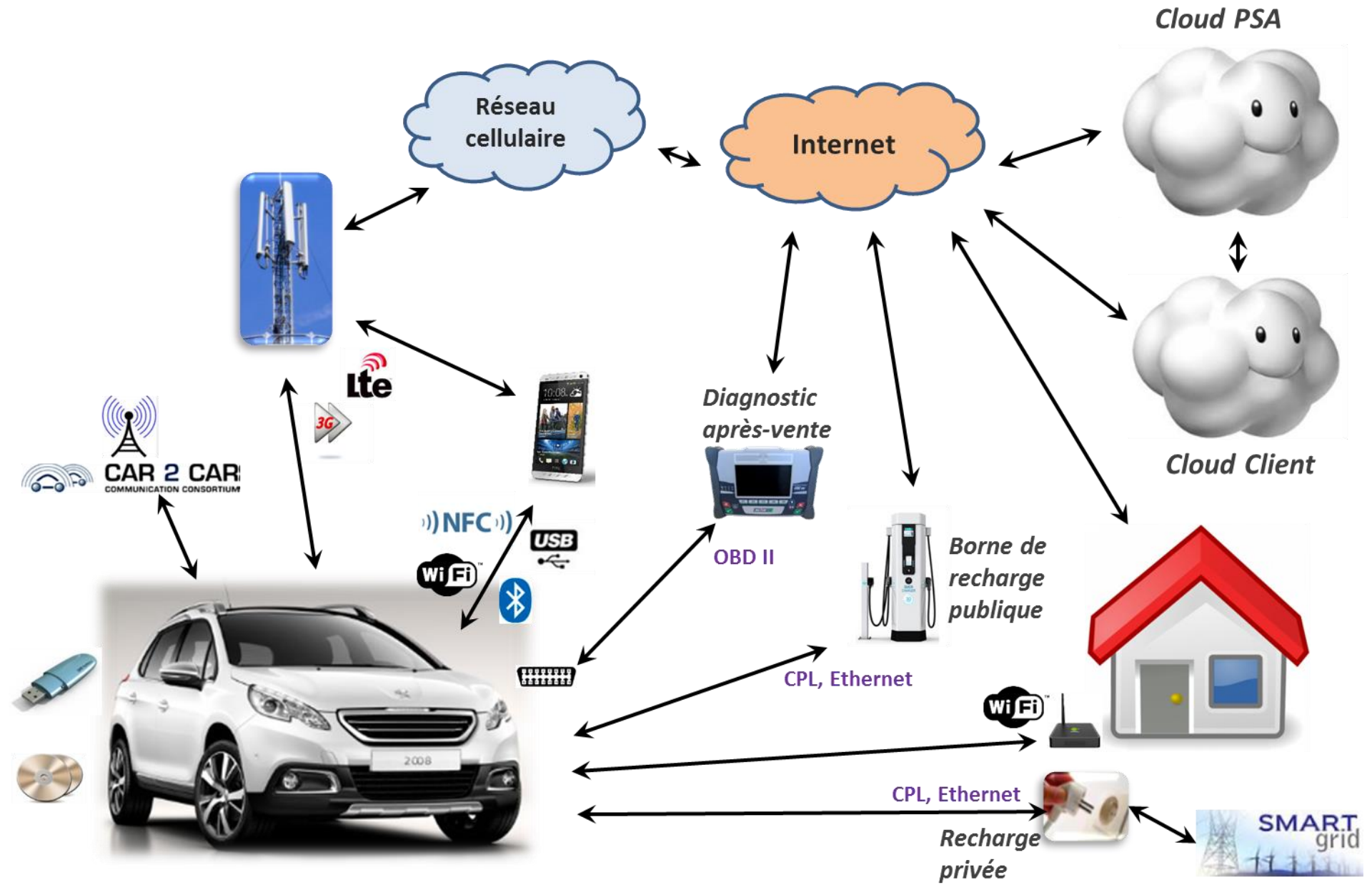
DS CONNECT FLEET management

Data Services

- Data collection to exploit information : ABS/ESP, Weather,
- Experience in Nice et Wallonie (Belgium region)
- ***Partnerships*** with IBM

PSA PEUGEOT CITROËN
IBM

Technologies for Connected vehicle



Connected & Autonomous Vehicle consideration

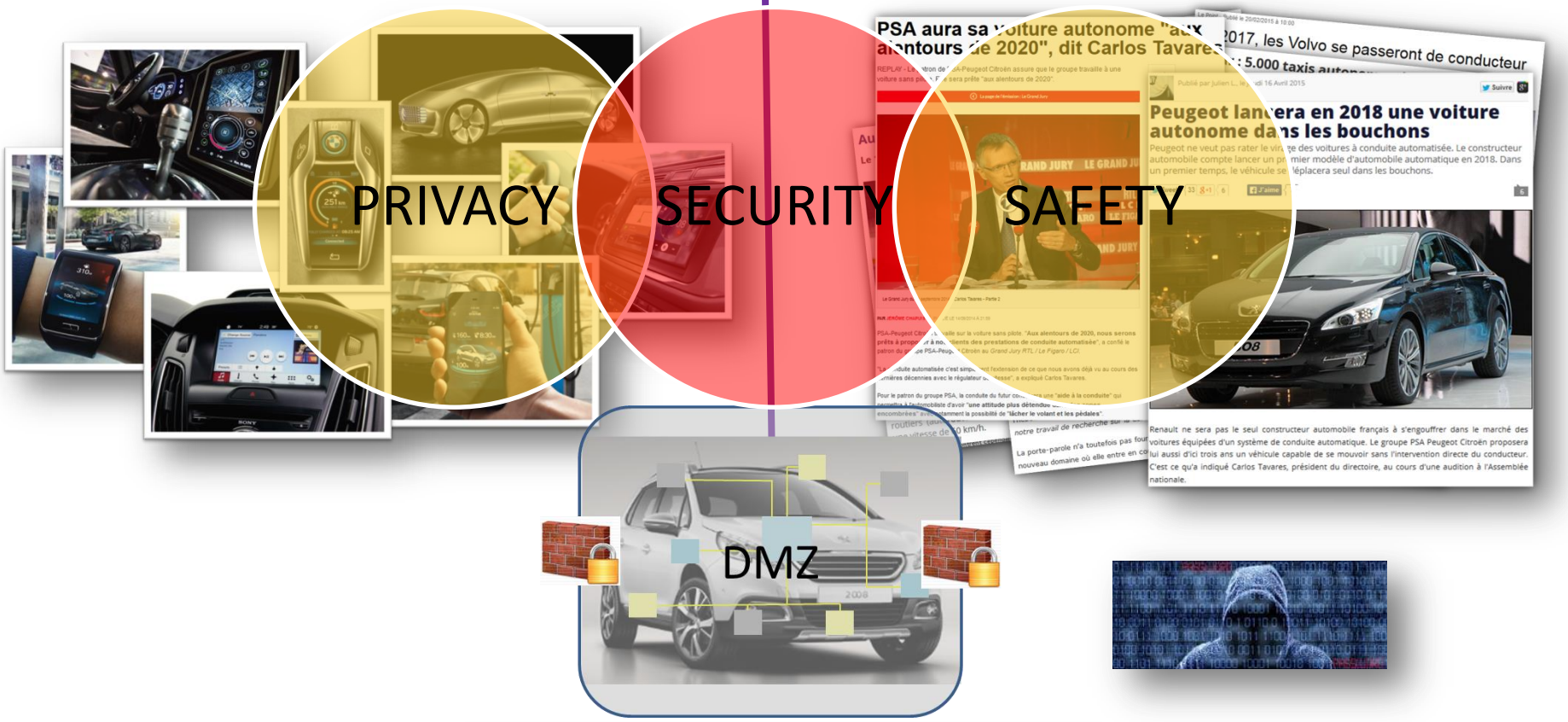
PSA PEUGEOT CITROËN

Connected Vehicle

CES Las Vegas 2016

Autonomous Vehicle

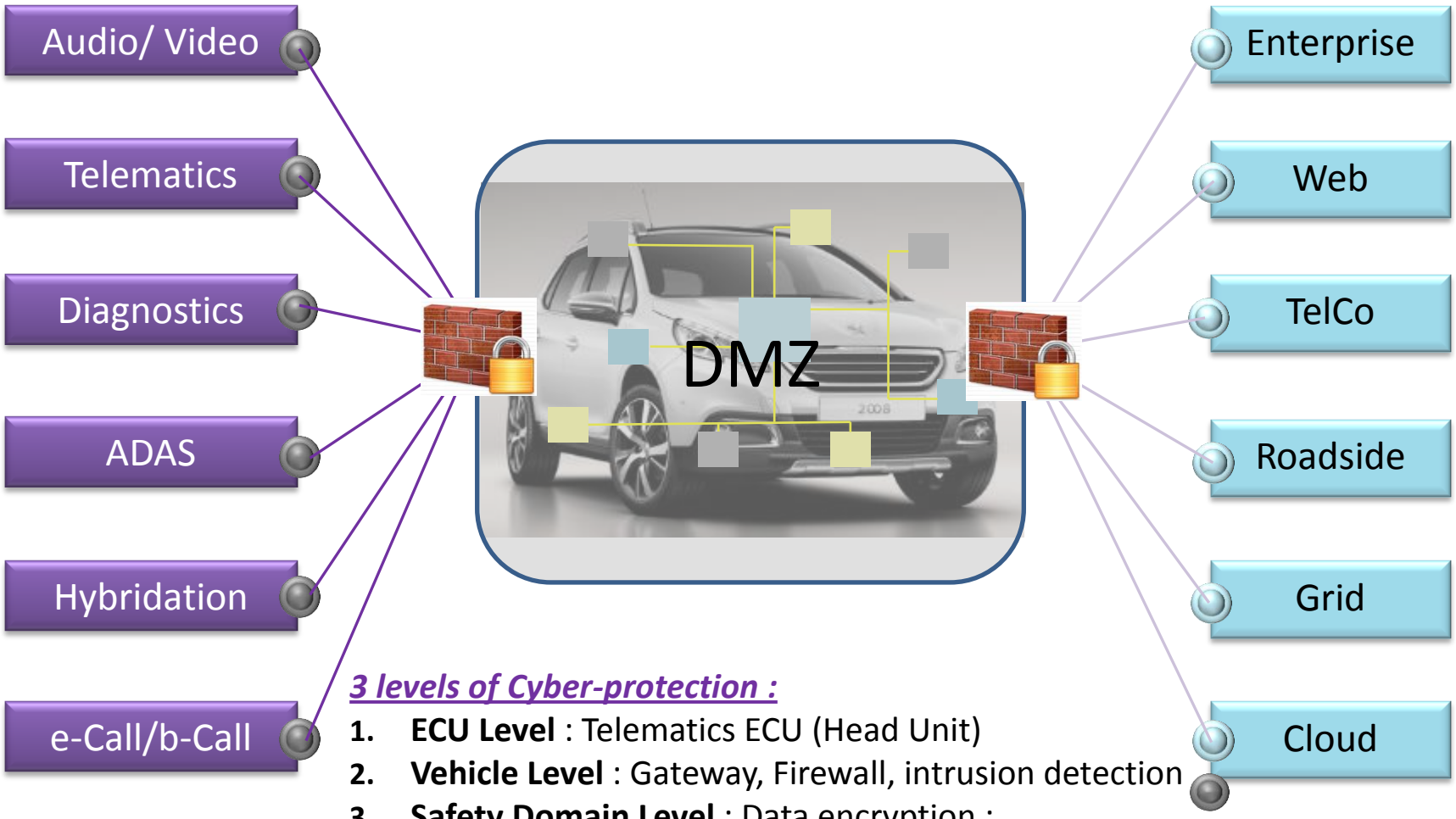
Help driving : strong tendancy



Opening data is dangerous
Data protection are essential
Firewall is fundamental

Connectivity & Cybersecurity.

Changing from a segmented world to a connected world



3 levels of Cyber-protection :

1. **ECU Level** : Telematics ECU (Head Unit)
2. **Vehicle Level** : Gateway, Firewall, intrusion detection
3. **Safety Domain Level** : Data encryption :
   HW : Hardware Secure Element (HSM) / Secure Hardware Extension (SHE),
   SW : SW Crypto Security Module

Automotive Cybersecurity actualities

PSA PEUGEOT CITROËN

Attack Historic

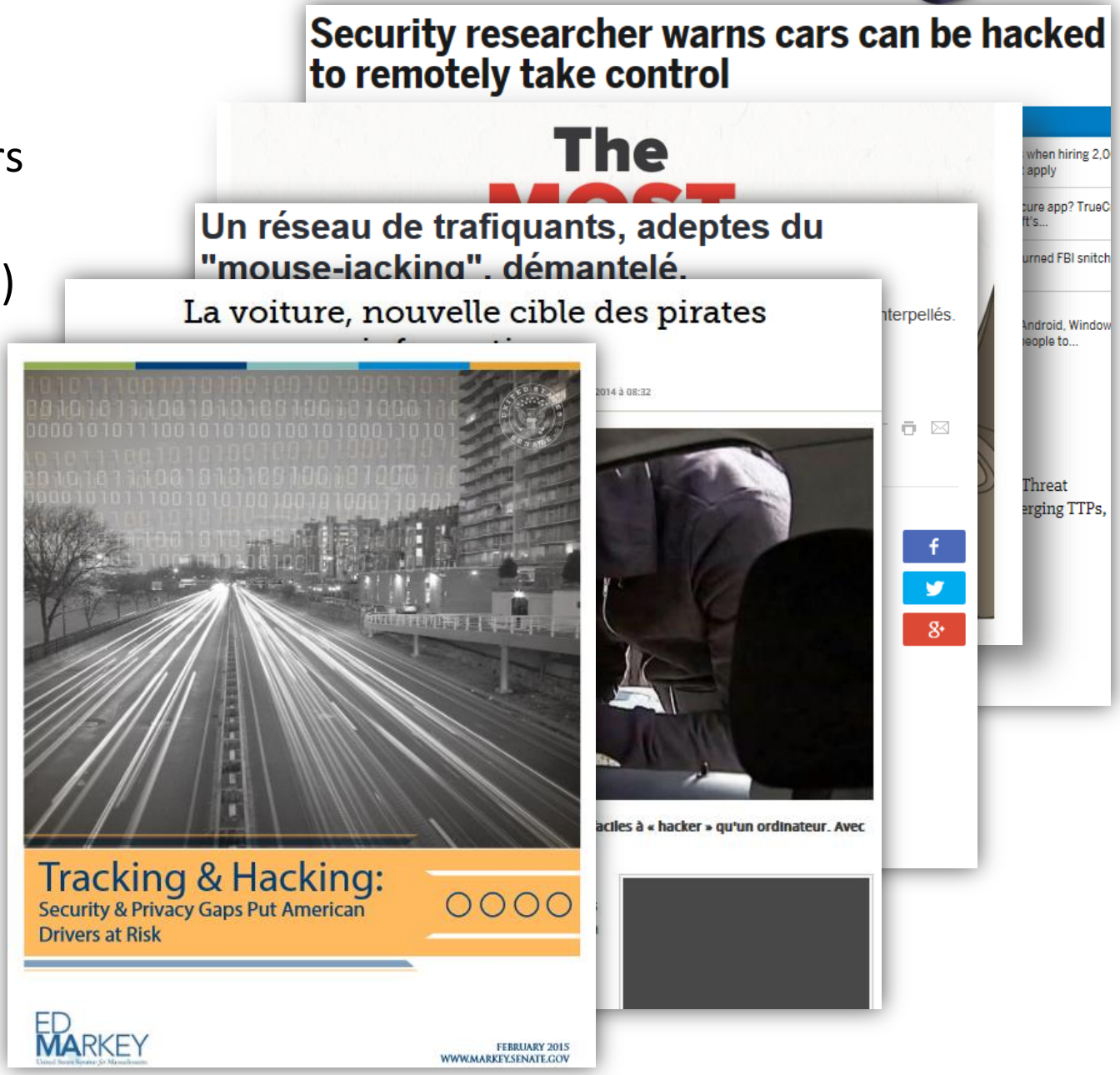
- 2010 : First research on Audio System and Tires Pressure Detection
- 2013 : Command injection on powertrain and chassis domain (but inside the car)
- 2014 : National competition in China to hack one Sport Electrical Car
- 2015 : Wireless intrusion in multimedia system connected to powertrain and chassis domain
- 2015 : Wireless intrusion in Dongle connected to OBD Port
- 2016 : Intrusion in non secure App in Smartphone, with Bluetooth connection => activation climate control end recover *Historic Driving Data*

Attack Categories

- **Disturbance** :
  - ✓ Change radio station, Display picture on screen, Switch off the climate control, …
- **Safety :**
  - ✓ ASIL_A/B : Switch_off Lights, Wipers, … / Switch_on Klaxon, Windscreen Washer
  - ✓ ASIL_C/D : vehicle dynamic control : stop engine, brakes, Steer, …
- **Privacy** :
  - ✓ Recovery personal information (navigation historic, speed vehicle, position, …)

Automotive cybersecurity interest

- Security Researchers
- Hackers (White Hat)
- Thieves
- Journalists
- Authorities
- …



Risk & Protection classification

Types of attacks

1. Malicious services (without subscription)
2. Theft with opening doors & start engine / Chip tuning
3. Theft of customer data (embedded or in PSA Servers) => Privacy
4. Remote control on vehicle mobility (longitudinal/lateral) => *Security* + *Safety*
5. Cyber-attacks: individual or organized groups => Security & Financial Risk / Media image

Distances Attack vs Risks

- ✓ Short distance: Bluetooth, NFC => necessity to be near the vehicle
- ✓ Middle distance: Wifi, 802.11 (Car-to-X) => remote risk
- ✓ Long distance : Internet, LTE (4G/5G in 2020) => more difficult to counter attack

The Protections

1. Customer : Safety by Design
2. Data : Confidentiality, Integrity
3. Services: Availability, Accountability
4. Exchanges: Authenticity
5. Image of PSA

Security Objective

1. Confidentiality (data)
2. Integrity (data)
3. Availability (services)
4. Accountability (services)
5. Authenticity (sources)
6. Security (safety)

The Solutions

- ✓ Symmetric / Asymmetric Algorithm (AES, RSA), Hash Function (SHA-1/2)
- ✓ Public Key Infrastructure (PKI) for the achievement of safety

Secure-by-Design

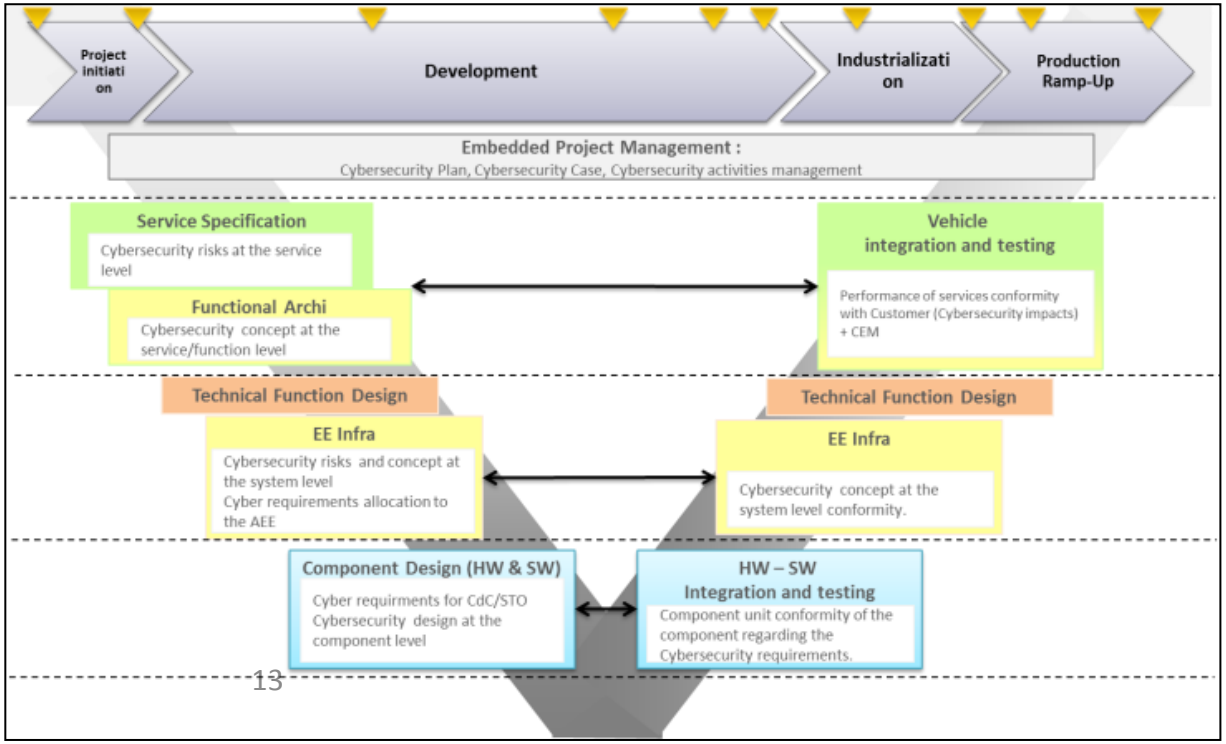
Process & Methodology

- Need to have dedicated process and methodology
  - ✓ To design complete HW & SW solutions
- Official *Security_Opinion* for each project millstone
  - ✓ End to end qualification opinion : From embedded architecture to IT Servers

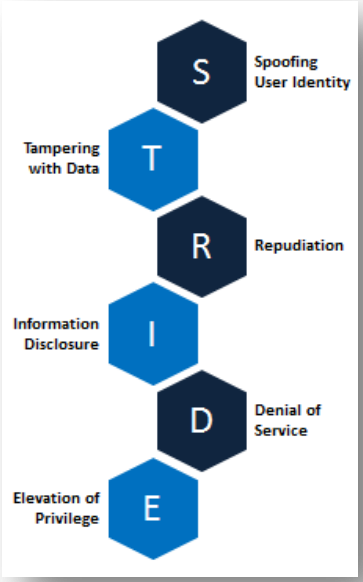
Based on 3 main responses

1. **Technical Cybersecurity Policy** : HW & SW solution
2. **Risk Assessment** to evaluate the risk
3. **Security validation**

Implemented in all phases of vehicle life cycle by PSA & Suppliers.
Including Tools, Policies, concepts and security mechanisms, Risk management, actions, training, best practices and technologies to ensure Cybersecurity.

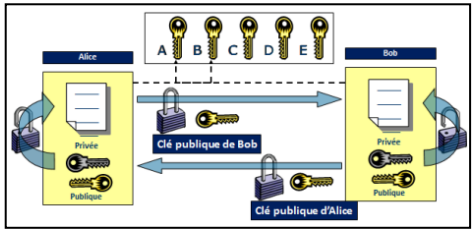


Secure-by-Design (1/3) : Technical Policy



Cybersecurity requirements specification :

- Confidentiality : Data Encryption (Key management, ..)
- Authentication : Signatures, Hash function, MAC, certificates, PKI,
- Integrity : Hash function, signature
- Non repudiation : signature, certificates
- Authorization : Password, certificates, configurations, firewall,..
- Availability : IT Servers redundancies

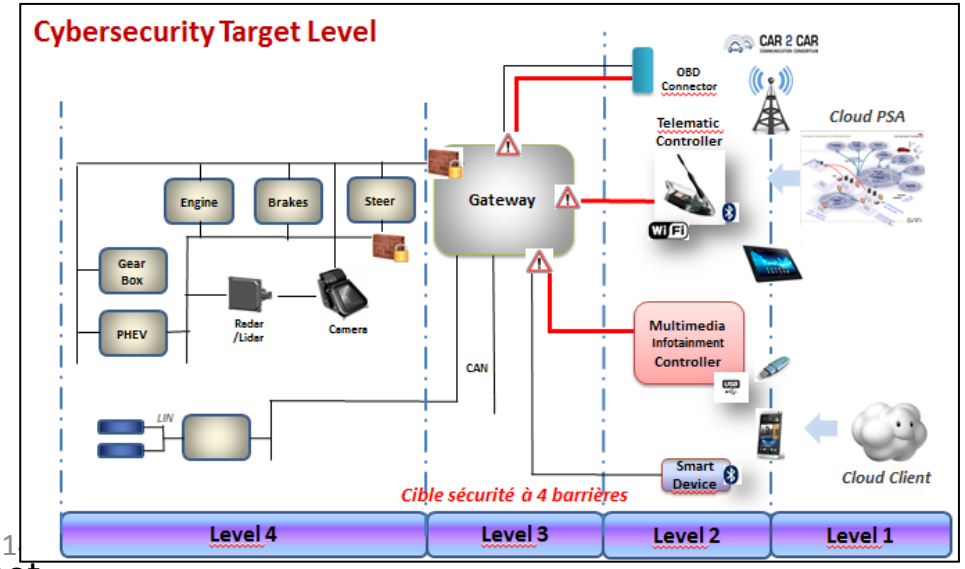


Technical Solution :

- Symmetric/Asymmetric Algorithm (AES, RSA)
- Hash Function (SHA-1/2)
- Challenge/Response mechanism (Seed & Key)
- MAC Authentication

Technical Levels :

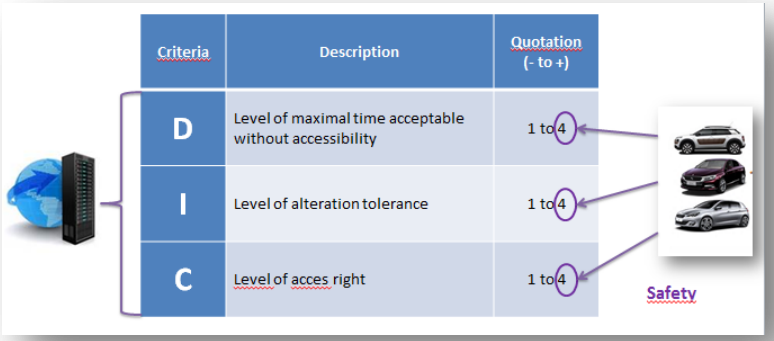
1. Vehicle-PSA Servers level
   - ✓ Security Operational Center
2. System Infotainment Level (TCU, IVI)
3. Architecture Level (Gateway)
   - ✓ Firewall, Monitoring, Login,
   - ✓ IDS, IPS, OTA
4. ECU Level
   - ✓ Authentication, Virtualization, Secure Boot



Secure-by-Design (2/3) : Risk Assessment Methodology

Risk Assessment Methodology :

- Methodology customized for Automotive
  - ✓ eBIOS from ANSSI
  - ✓ TVRA from ETSI
- 3 criteria used :
  - ✓ Availability, Integrity, Confidentiality



Threat Group

- Evaluation of Attack
- Evaluation of Impact
- Evaluation of Risk

Attack					Impact	Risk
Factor	Range	Value	Potential	Likelihood		
Time	<= 1 day	0	No Rating	Likely	Low	Major
Expertise	Layman	0				
Knowledge	Public	0				
Opportunity	Unnecessary	0				
Equipment	Standard	0				
Asset Impact	Low	1				
Intensity	Single instance	0				

Countermeasure

- Evaluation of Cost
- Evaluation of Benefit

Cost		Benefit			Result
Category	Value	Risk Level	Original Count	Revised Count	
Standards design	No Impact	Minor	2	3	17
Implementation	No Impact	Major	1	1	
Operation	No Impact	Critical	3	1	
Regulatory Impact			No Impact		
Market Accpetance			No Impact		

Secure-by-Design (3/3) : Test Validation

Identified vulnerability	Impact	Priority	Criticity	Difficulty
Login prompt available on serial port	DICP	High	High	Technician
Alternative root account without credentials	DICP	Critical	Very High	Technician
Firewall rules misconfiguration	DICP	Medium	Medium	Technician
Log interface on serial port	C	Weak	Weak	Technician
Debug interface available	C	Weak	Weak	N / A
Insufficient WiFi keys complexity	C P	Weak	Weak	Technician
WiFi keys stored in plain text	C P	Medium	Medium	Technician
Bypass of the update image signature	DICP	Critical	Very High	High

Security validation method :

- Security test, Penetration Test, Attack simulation
- Shall be planned at the beginning of the project
- Need HW & SW maturity system (HW + SW) :
  - ✓ Late in the development
  - ✓ Considered as a « Final » verification, assessment

Goals:

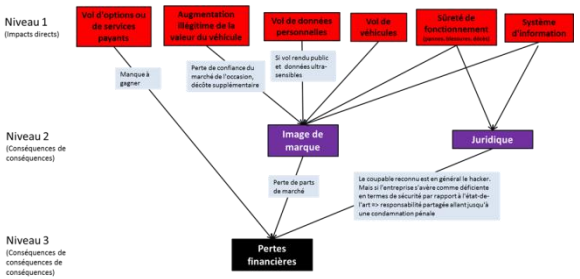
- Take control of the execution flow of ECU for arbitrary code execution
- Inject arbitrary CAN/LIN frames to attack ECU and other connected systems
- Demonstrate the ability to use link (USB, Bluetooth, Wifi,…) to attack ECU
- Demonstrate the ability to reach the PSA infrastructure through TCU access.

Focus points:

DEFINING THE LEVEL OF EXPLOITABILITY	LEVEL
Exploitation of this vulnerability requires few resources and skills. The operation is technically affordable without special knowledge.	User
Exploitation of this vulnerability requires the resources and skills of a person with technical knowledge. This operation may require the use of tools or various documentations.	Technicien
Exploitation of this vulnerability requires the skills of a hacker. This requires a thorough knowledge in SSI.	Hacker

- Reprogramming methods
- Customer Media : USB, CAN
- Physical attacks on internal/external ports
- JTAG, UART, SPI, USB, WiFi, CAN, Bluetooth…
- Malicious usage of map functions, map updates and navigation functions
- Customer Media pairing protocols

Cybersecurity and Safety



Key points for Safety and Cybersecurity synchronisation

Cybersecurity Risk Analysis

Ensure the right level of Safety impact

Safety Impact quotation

Functionnal / Technical Cybersecurity Concept

Ensure Consistency with Technical Review

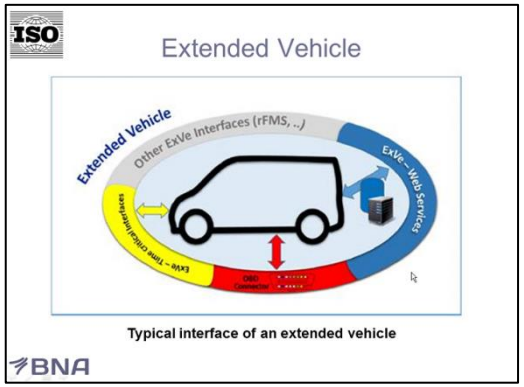
Functionnal / Technical Safety Concept

Cybersecurity Status

Assess Safety status about Cybersecurity issues **Safety Assessment**

Safety Status

Way for Standardization…



Interest of Standardization

- *Security is no competitive differentiating feature*
- *Higher quality of the security with more experts (cf. ISO26262)*
- *Cost down for standardized solution of the shelf*
- *Improved interoperability between different ECU manufactures*

No Automotive Standard existing :

- Norms: ISO 2700X, Common Criteria (ISO 15048)
- Next Step ISO and SAE, with same ISO26262 approach (ex IEC61508)
- SAE (J3061) : Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

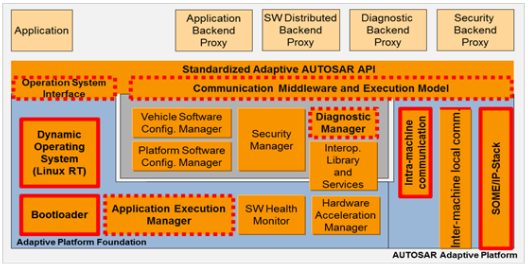
No Regulation

- American law Project (2015) : *SPY_CAR_ACT* (Security and Privacy in Your Car Act), by NHTSA and FTC (Federal Trade Commission)

Hardware Standard Solution

- SHE : Can be used in CSM by a special CRY module, and for some CSM service ports while others use software-CRY
- EVITA : offers different levels following the security objectives:
  - EVITA Light is similar to SHE features,
  - EVITA Medium offers more storage capacity and specific CPU with medium performance
  - EVITA Full offers RSA and ECC Cryptographic acceleration, more storage capacity and more high CPU performance capacity

AUTOSAR solution



Autosar Authentication (Secure Onboard Communication)

- Available since 4.2.1 Release

Abstract interfaces for cryptographic routines:

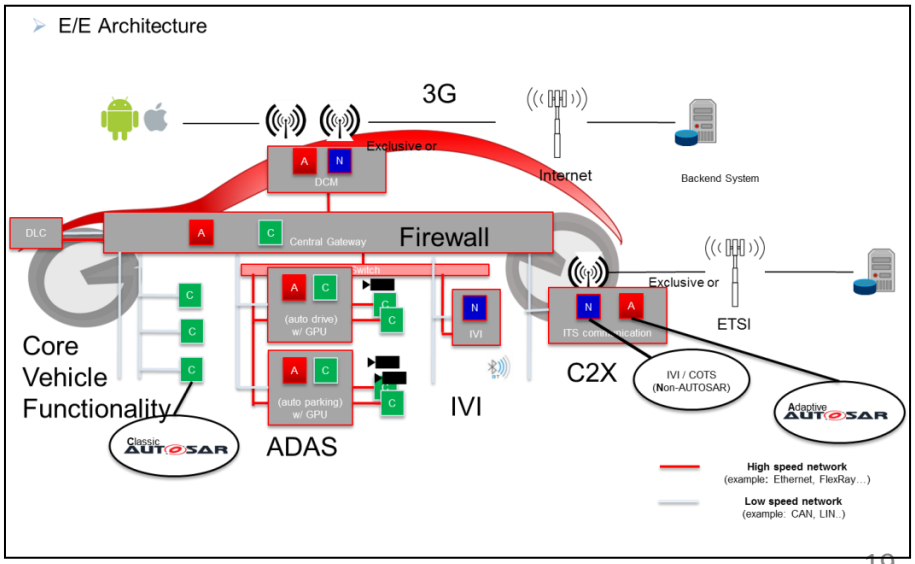
- **CSM** - Crypto Service Manager (Service, provides service ports through RTE)
- **CAL** - Crypto Abstraction Layer (Library, can be called directly from BSW and Applications)

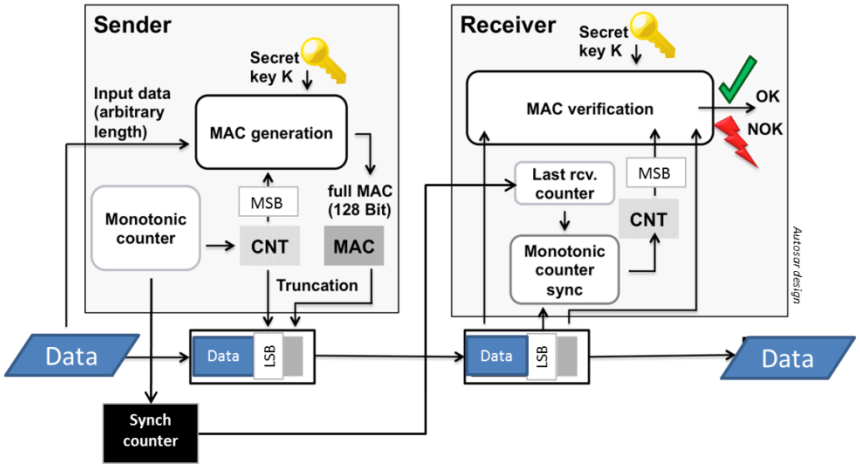
Implement Cryptographic Routines

- **CRY** – CRYptographic library for CSM - hardware

Architecture including different Types of ECU

- Type N: **N**on Autosar ECU: In-Vehicle Infotainment (IVI) or Component Off-The-Shelf (COTS) = « Black box » ECU
- Type C: Autosar **C**lassic ECU
- Type A: Autosar **A**daptive ECU

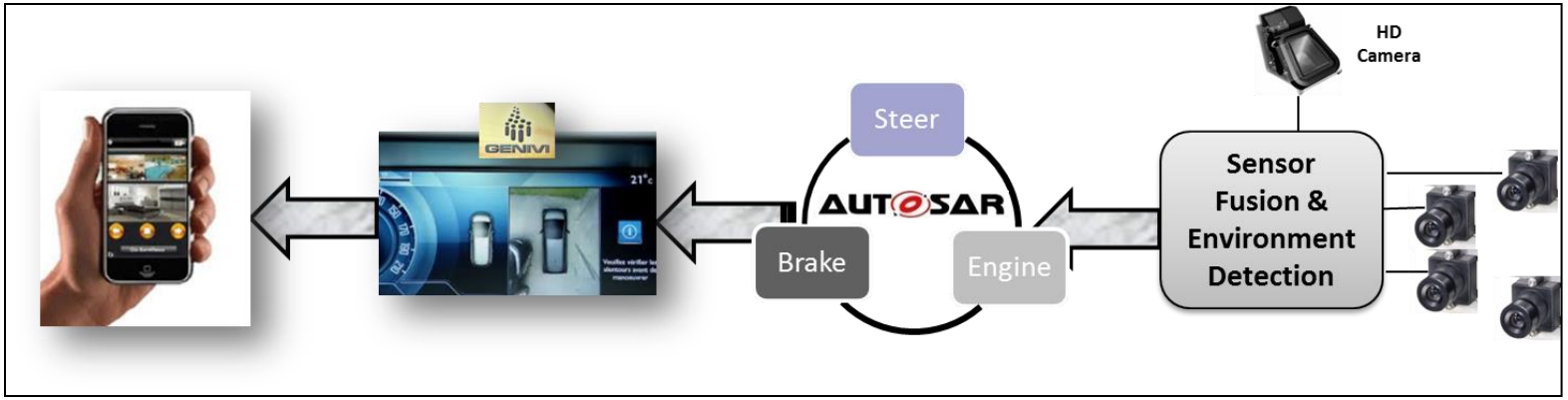




GENIVI solution

Authentication (Secure Onboard Communication)

- What is the equivalent of Autosar (requirements, specification) ?
- Cryptographic services ?
- Equivalent of ECU classification (Genivi compliant or adaptive) ?
- Interoperability with Autosar?



GENIVI : Risk or Opportunity ?

- Based on Open Source software development : Number of vulnerability

  Webinar: Automotive Security Threat Landscape *(Sep 24, 2015) => Last year, over 4,000 vulnerabilities were reported in open source software (and thousands more in proprietary code).*

  "Increasing integration of open source in In-Vehicle Infotainment (IVI) head units and other automotive systems makes vehicles potentially subject to the same types of exploits. For automakers, this year was crowned by white hat attacks on IVI, vehicle control and security systems using standard 3G connections and readily available aftermarket components."

Conclusion

Facts

- Vehicle is and will be connected : Automotive eco-system opportunity.
- ***Safety***, ***Security*** and ***Privacy*** management is mandatory***.***
- OEM responsibility : Regulation respected but managing vehicle access control to limit impact => extended Vehicle way for security

Risks & Threats

- *Consumerist* : Actualities, Communication, Bug Bounty
- *Regulation* : Initiated in USA : *SPY_CAR_ACT*
- *Legal* : *Class-action* engaged in USA.
- *Economic* : Massive car recall.
- *PSA Image* : Media effect (24h) : Press, Social network

Response

- Methodology, Process,
- Cybersecurity Technical Policy
- Standardization & Regulation with ITS
- Experts network, Cooperation
- Innovation : Continually Processing, Testing & Verification … because no stable !

Thank for your attention