CCFA
20 Septembre 2017

SIA SOCIÉTÉ DES INGÉNIEURS DE L'AUTOMOBILE

L'extraordinaire défi de la définition électronique des véhicules du futur

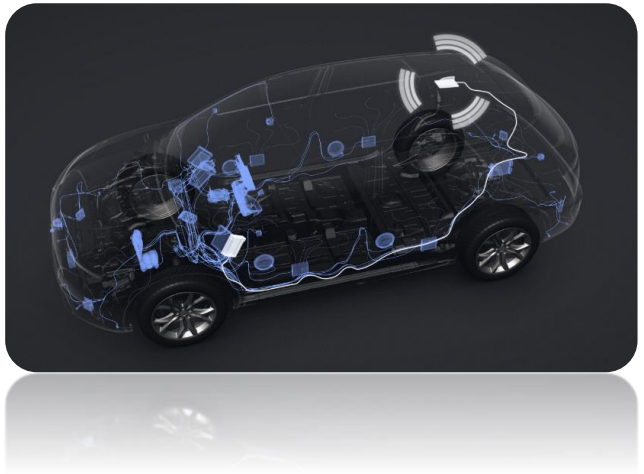
Eric Dequi
PSA : Senior Expert in EE Architecture & Cybersecurity

Alain Couvreux
Renault : EE Architecture Expert Leader

PSA GROUPE

RENAULT NISSAN MITSUBISHI

SOMMAIRE



1. Change inductors

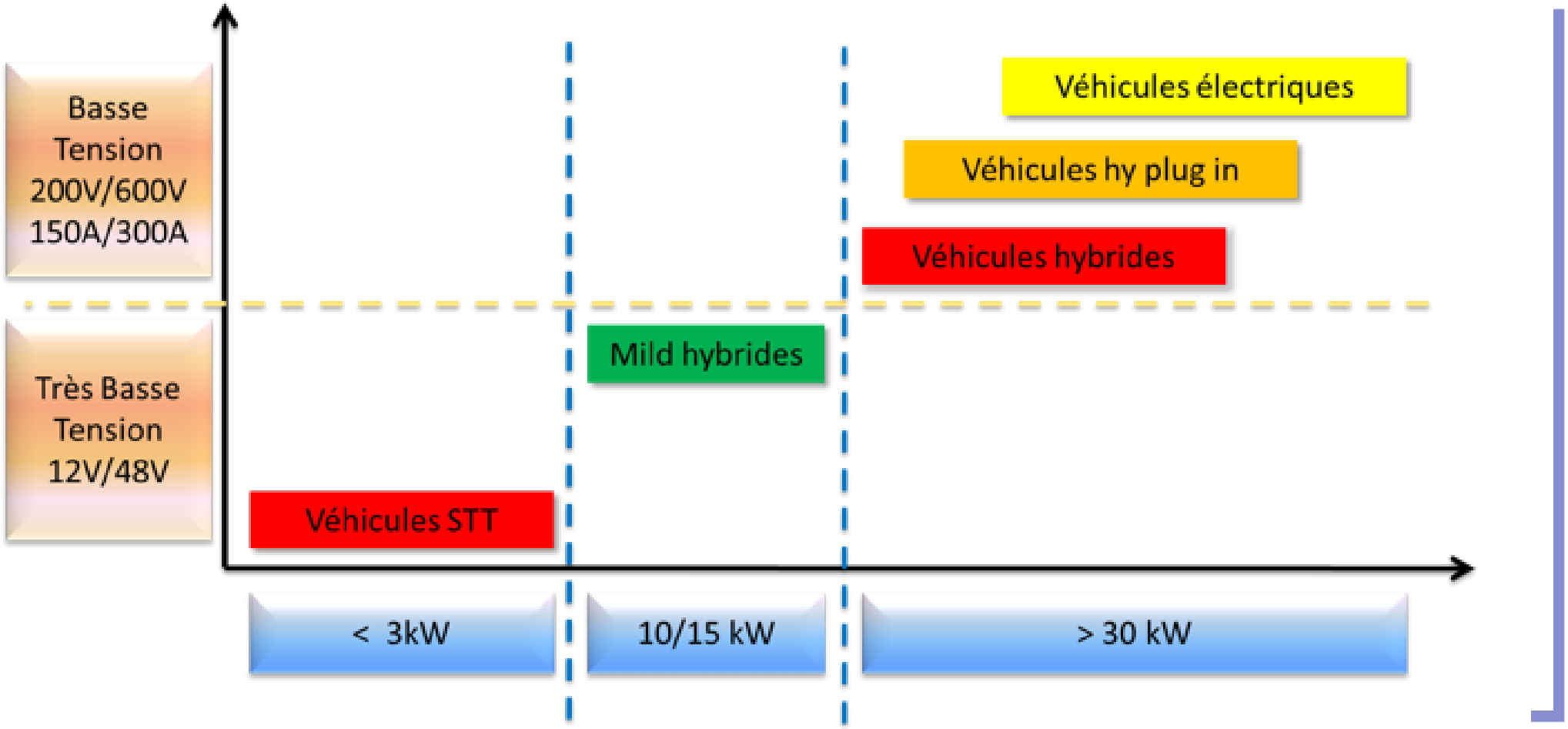
- Electrification
- Automated Driving
- Connectivity

2. Technical & Methodology responses

- Safety (ISO 26262)
- Security (ISO21434) & Privacy (GDPR)
- Quality : Hardware Software
- Firmware Over-The-Air (FOTA)
- Architecture based on GW, Ethernet, Domain masters
- Software Standards (Autosar, Adaptive Autosar, Genivi)
- Methodology & Tools

ELECTRIFICATION

Scalability : From Stop& Start, up to full Electrical Car.



E

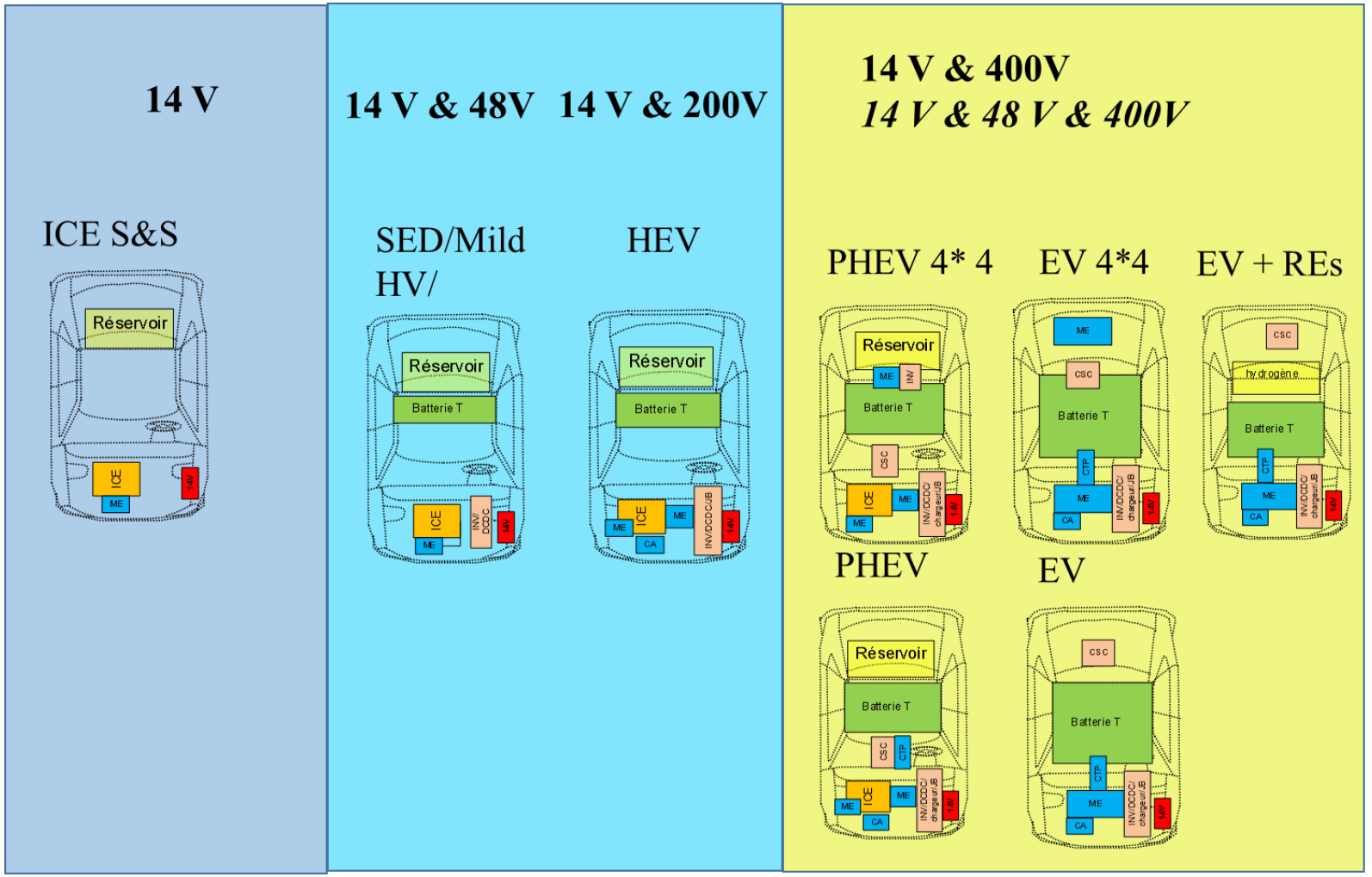
ELECTRIFICATION

- Variety of technologies to be addressed
- In particular the progressive input of 48V, with changeover to be managed for the components
- Stakes on Quality of the Boardnet

Single Voltage
- To continue using 12V components

Dual Tension
- To manage component changeover 12V->48V and safety with redundancy

Triple Tension
- For EV/PHEV vehicle



AUTOMATED DRIVING

Level 2 : Partial Automation

Level 3 : Conditional Automation

With SUPERVISION
Driver has to be attentive
in all circumstances

Without SUPERVISION
Possibility to do something
Other than driving

Fail Silent

- Safe state accessible without help from Control Unit
- Loss of function is safe state of the system

Fail Operational

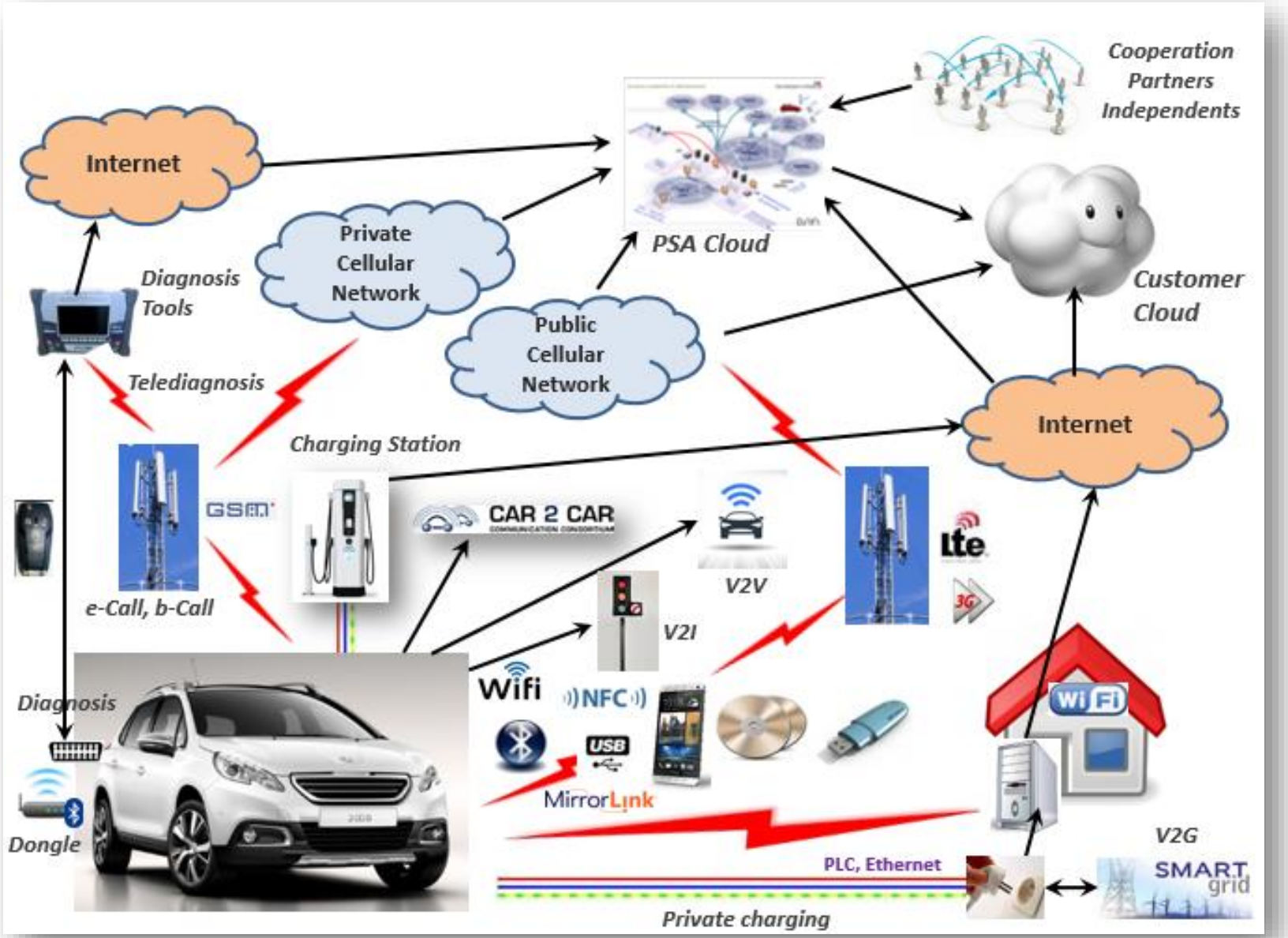
- Safe state not accessible without Control Unit
- Loss of function is generally « non safe »

E

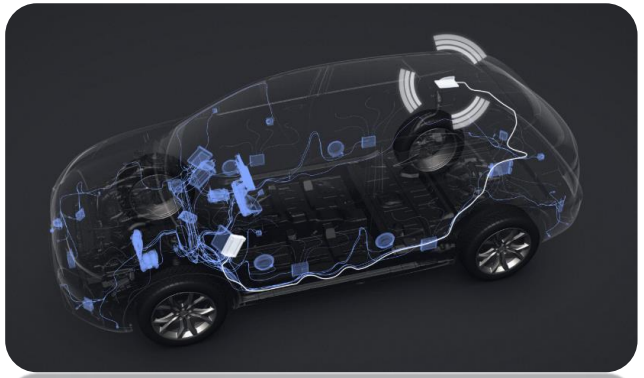
CONNECTIVITY

Uses Cases :

- ***Remote Services*** : Pre-conditioning, Start Engine, Setting information, …
- ***Big Data*** : to collect information for Quality, predictive maintenance, Usage Profil
- ***Software update*** Over-The-Air (OTA) : New Services, Quality campaign, Cybersecurity,
- ***Tele-Diagnosys :*** Read DCT Fault Code + SW update OTA
- ***V2X (Vehicle To X):*** Vehicle to Vehicle (V2V) / Vehicle to Infrastructure (V2I) / Vehicle to Grid (V2G) / Vehicle to House (V2H) / Vehicle to Cloud (V2C)



SOMMAIRE



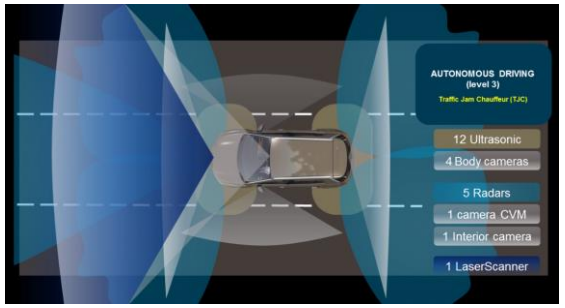
1. Change inductors

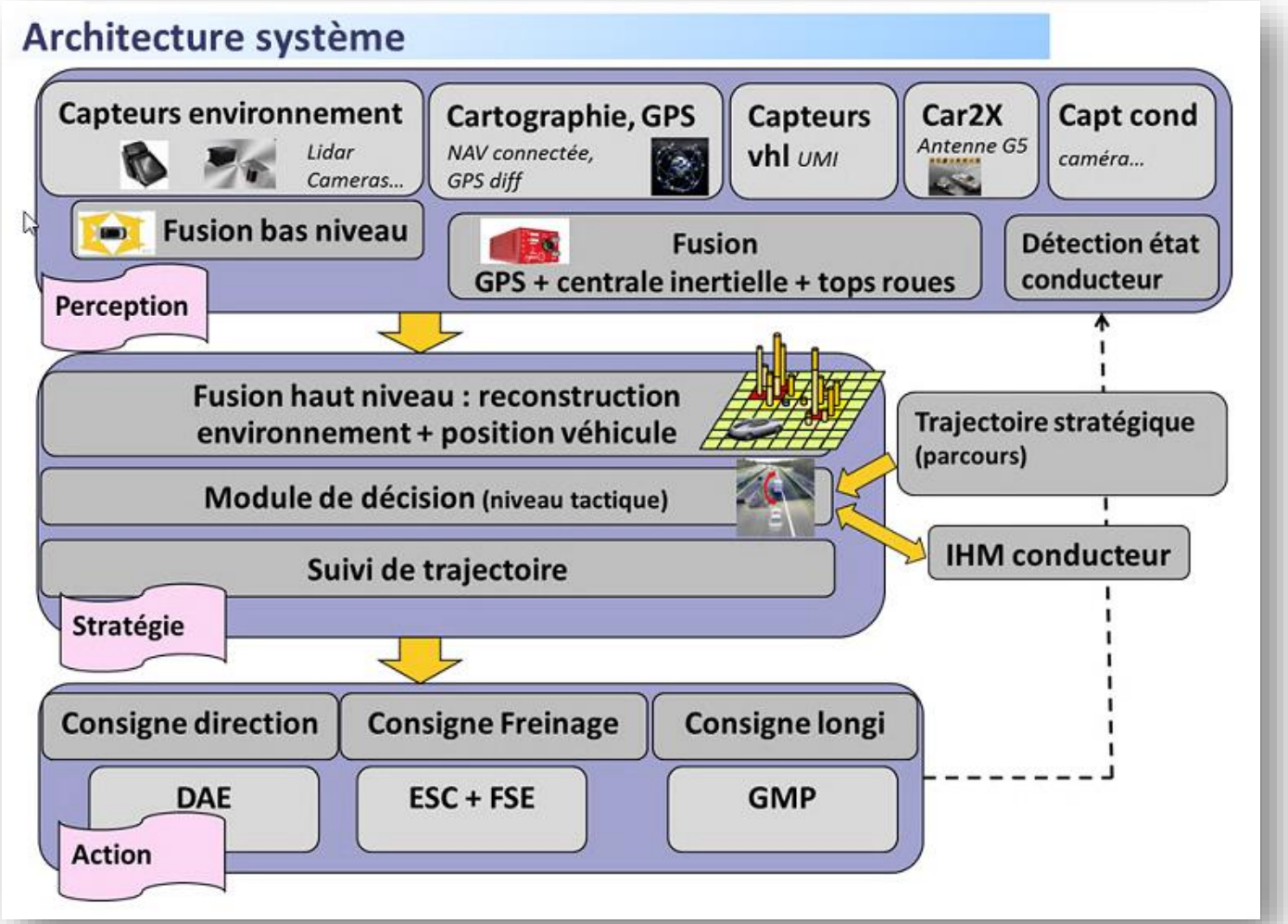
- Electrification
- Automated Driving
- Connectivity

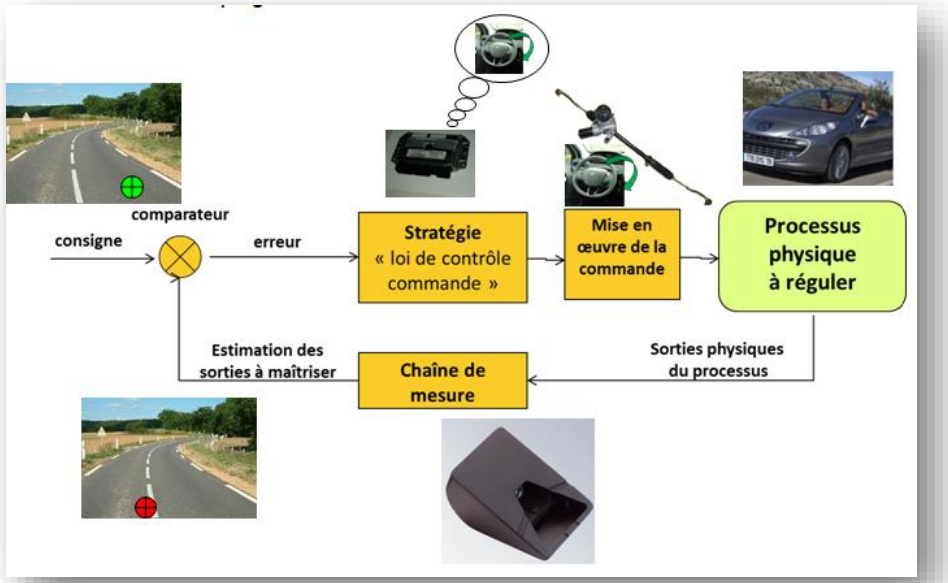
2. Technical & Methodology responses

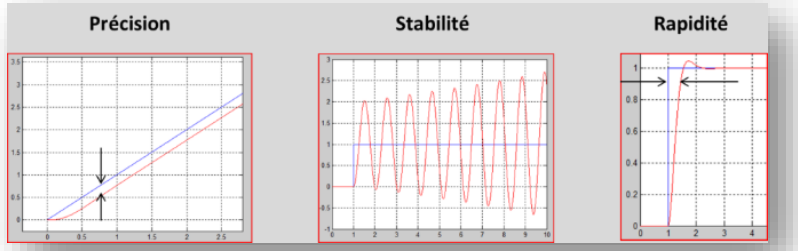
- Safety (ISO 26262)
- Security (ISO21434) & Privacy (GDPR)
- Quality : Hardware Software
- Firmware Over-The-Air (FOTA)
- Architecture based on GW, Ethernet, Domain masters
- Software Standards (Autosar, Adaptive Autosar, Genivi)
- Methodology & Tools

ADAS & FUNCTIONAL LAYERS





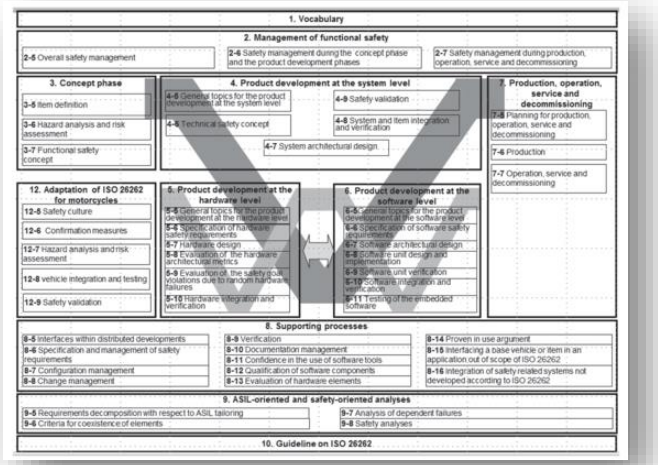




E

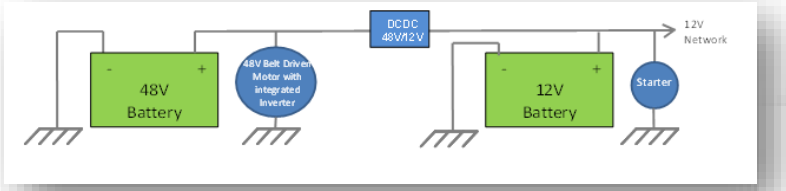
SAFETY

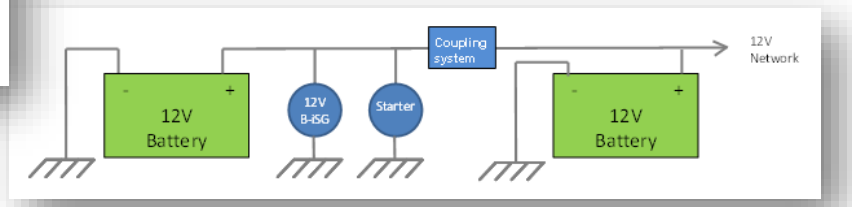
- **ISO 26262 defines how to assess a risk and the necessary activities to perform for each step:**
  - System
  - Software
  - Hardware
  - Production...



- **Redundancy for Autonomous Driving:**
  - Redundant Sensors & Actuators
  - Redundant Communication Networks
  - Redundant Power supply Networks

- **Additional Safety Stakes:**
  - For Autonomous Driving, Automotive EE Architecture has to switch from Fail Safe design to Fail Operational.
  - Safety has also to consider SOTIF (Safety of the Intended Functionality)





A

SAFETY & SOTIF

Does a camera can identify a target in a very large roundabout without line ?

Does a radar will be accurate on a metallic bridge ?

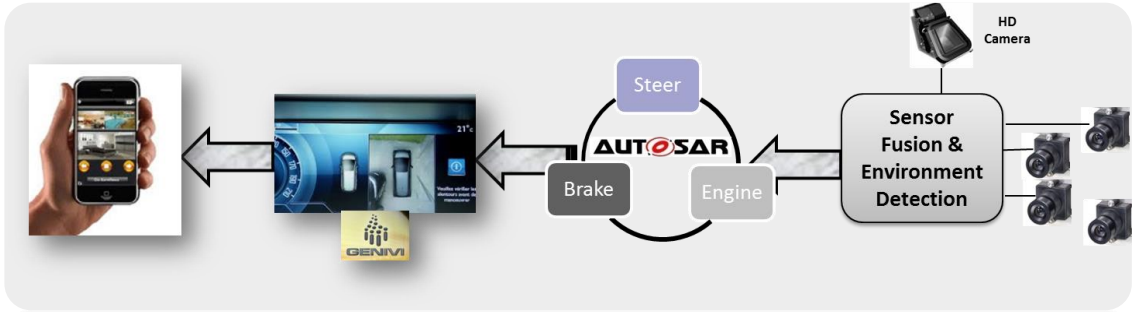
Does an ultrasound sensor can detect a children with a cotton sweater?

ISO 26262 Standard is necessary but not sufficient !

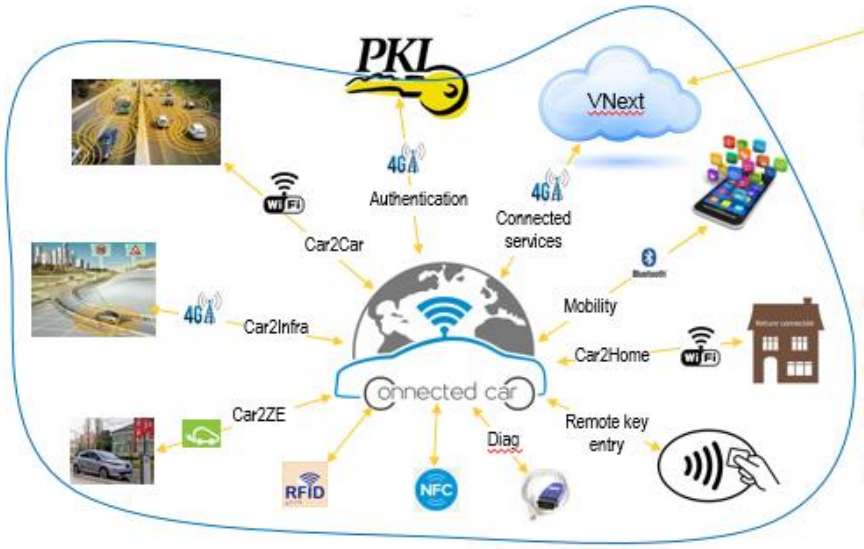
E

SECURITY and PRIVACY

- Connectivity brings new attack surfaces to hackers
- Security policy covers all dimensions of security and privacy.
- Security policy offers « in depth protection » i.e each attack surface is protected by several layers of protection
- SAE/ISO (21434) Standard on going
- GDPR (General Data Protection Regulation) for data Privacy



THE ENVIRONMENT OF THE CONNECTED CAR AND ITS SURFACES OF ATTACK



Multiple evolutive surfaces of attack

- The communication points of the vehicle and outside
- The connectivity between networks (CAN / outside, CAN-M / CAN-V, …)
- The On-board and off board software
- The communication protocols
- The authentication system (spoofing identity)
- …

1.4 CYBERSECURITY – STRATEGY OF PROTECTION

STRATEGY OF PROTECTION : 3 COMPLEMENTARY DIMENSIONS

BASTION

SYSTEM PROTECTION (On-board / Off-board / communications)
DATA PROTECTION (Privacy, context, technical, …)

SUPERVISION

SUPERVISION OF THE SYSTEM

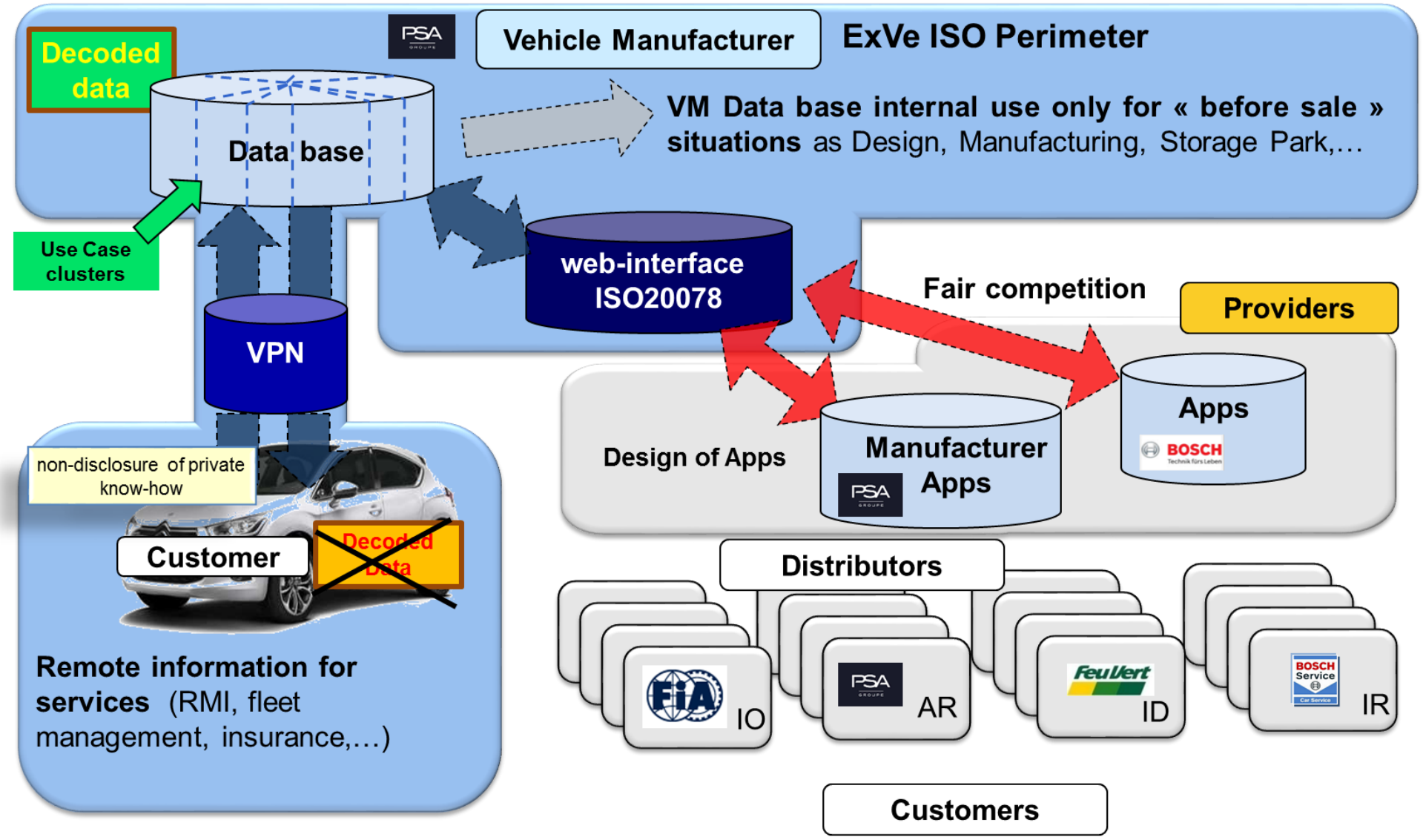
LOOKOUT

THREAT WATCH OUT (anticipation)

AVAILABILITY
INTEGRITY
CONFIDENTIALITY

E

SECURITY and EXTENDED VEHICLE (ExVe)



E

HARDWARE QUALITY : ELECTRONIC COMPONENTS

- AUTOMOTIVE ELECTRONIC COUNCIL created in 1993 to define qualification standards for the supply of components in the automotive electronic industry
- Q100 defines Stress Test Qualification for Integrated Circuits
- Most Tier 2 & Tier 1 are members of AEC
- AECQ 100 is applied world wide, for all type of Integrated Circuits

❑ AECQ Requirements or automotive policy:

- ➢ **Worldwide Quality Assurance** with mandatory requirements
  - Deviation : Cp, CpK > 1.67 (+/- 5σ → defect < 0.6ppm)
  - TS 16949 : 3D and 8D commitment , example for 8D
    - ✓ D1 :Team members
    - ✓ D2 : Problem definition
    - ✓ D3 : Containment action
    - ✓ D4 : Root cause
    - D5 : Corrective action definition
    - D6 : Corrective action Implementation
    - D7 : Prevent reoccurence
    - D8 : Team congratulation
- ➢ **Obsolescence / commercial lifetime**
  - AECQ > 8 years
  - Consumer : usually 3 years, but occasionaly very short.
- ➢ **End of production** => Information last buy order:
  - AECQ (12 months) versus Consumer (non specified)
  - Product Change Notification (PCN) & Product Termination Notification (PTN)
- ➢ Data base for Safety calculation about failure rate (FIT) → **Safety** ISO 26262

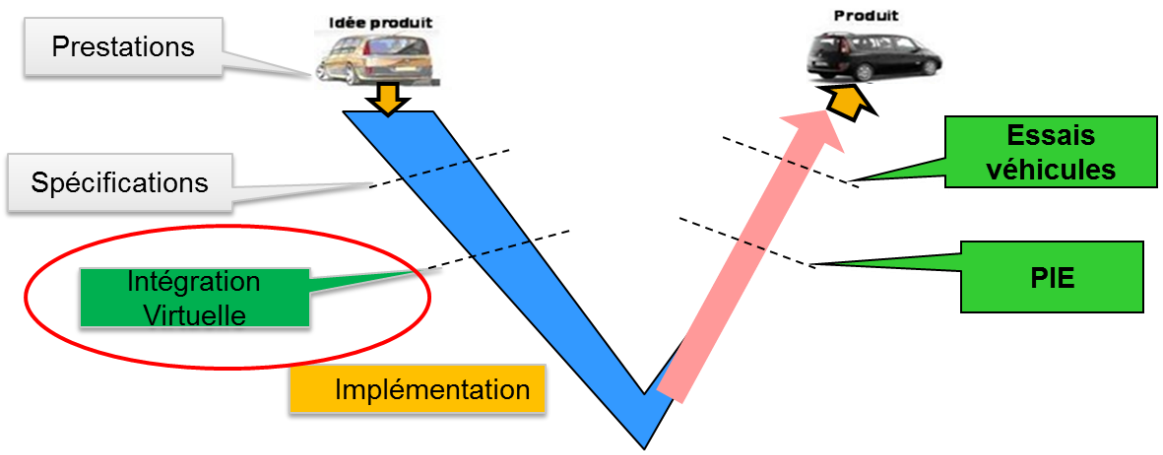
➔ AECQ = Suppliers commit Quality management
➔ AECQ = Very low component failure in serial life

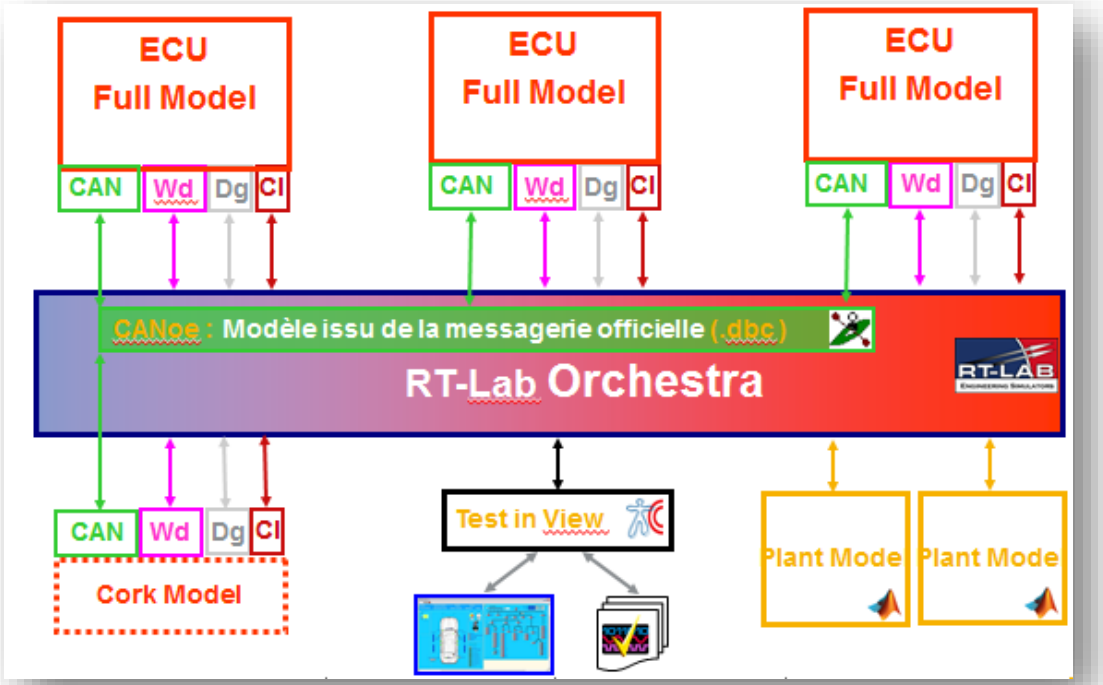
A

SOFTWARE QUALITY

- **Validation process is enhanced to deal with the complexity**
  - Hardware in the loop comes too late in the development
  - Model Based Design is key to start validation during specification phase, some months before the feature is implemented in an ECU.
  - Faster convergence, thanks to more mature specifications
  - Tools are available for high level of integration

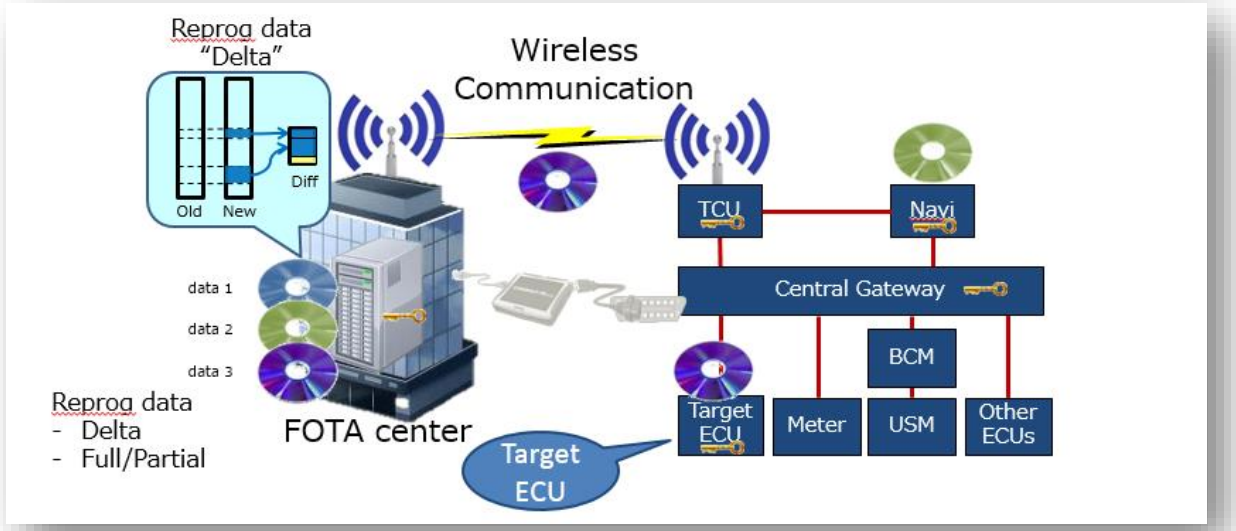
VIRTUAL INTEGRATION





A

SOFTWARE UPDATE OVER-THE-AIR



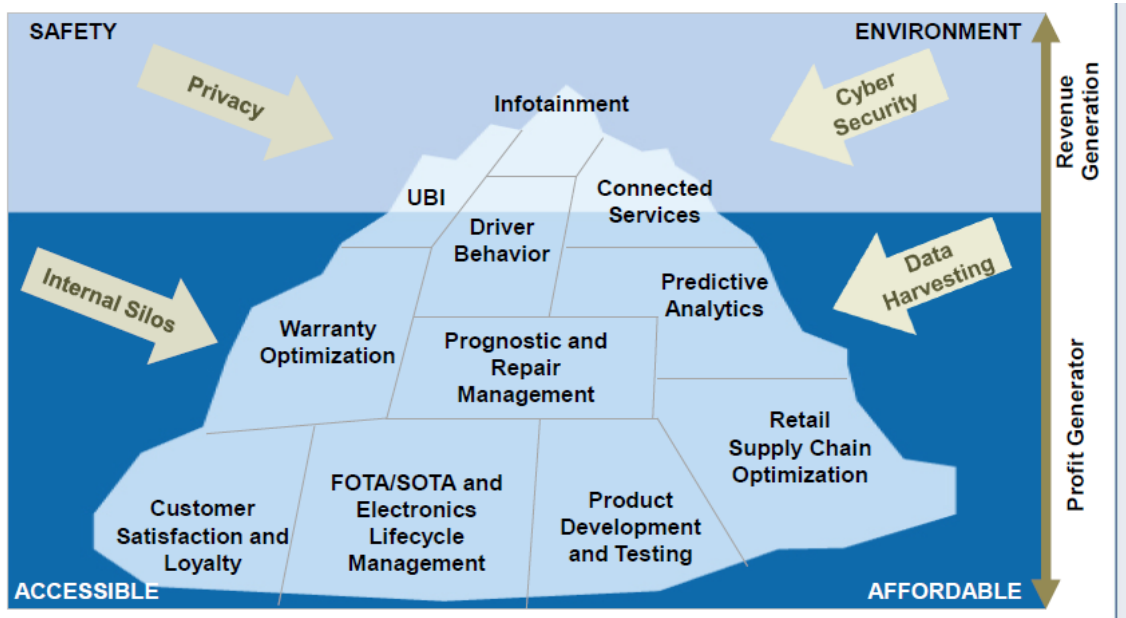
Based on proven solutions in telephony

For OEM/Dealer

- ❖ Continuous feature update by software update
- ❖ Reduce warranty cost by collecting software
- ❖ Reduce resource at Port, at Dealer

For Customer

- ❖ Continuous feature update during life cycle
- ❖ Quality/Security improvement
- ❖ Reduce effort to visit car dealer



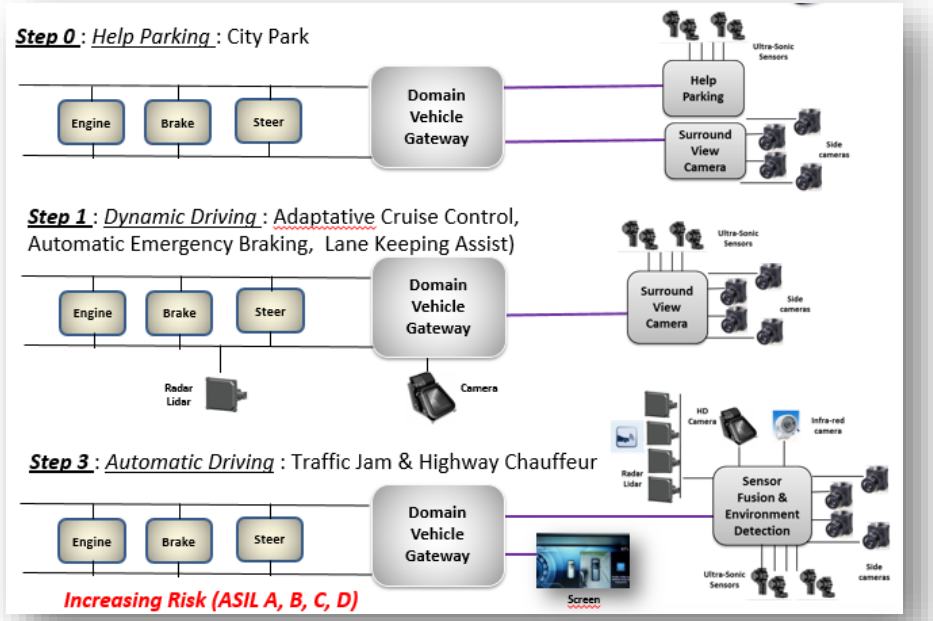
E

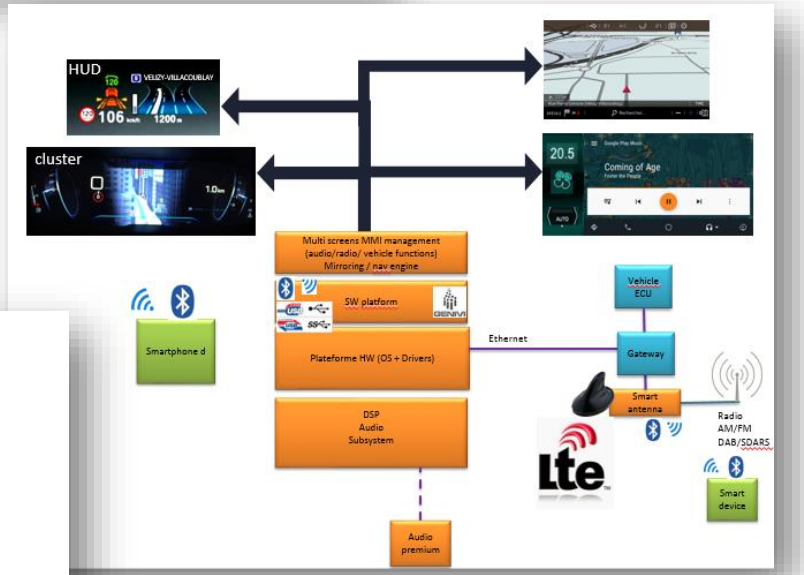
ARCHITECTURE DRIVERS

- **Domain Masters**
  - ❖ Bandwidth management
  - ❖ Segregation
  - ❖ Improvement of validation
  - ❖ Scalability, Modularity

- **Multiprotocol Central Gateways**
  - ❖ Bandwidth management
  - ❖ Interface/Isolation between different domains
  - ❖ Security Firewall
  - ❖ …

- **Strong Usage of standards**
  - ❖ Ethernet, CAN, CAN FD, Flexray, LIN
  - ❖ Graphic Processor (GPU)





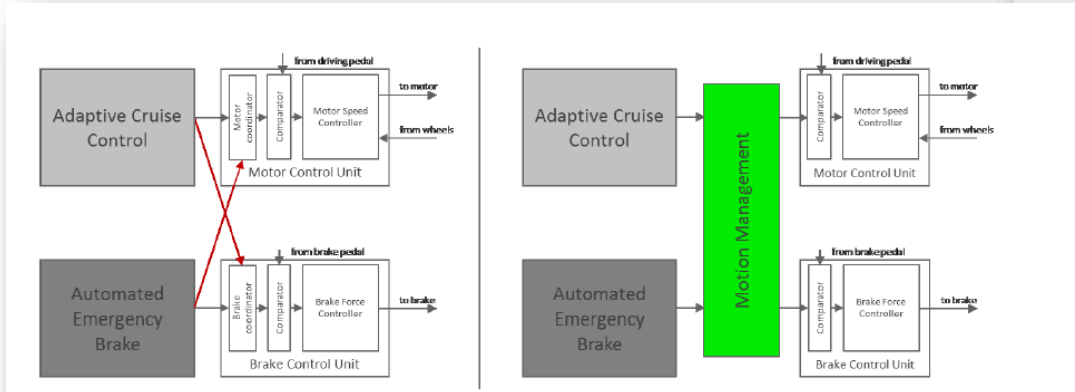


Figure 1: coordination between braking and engine management module (source: Elektrobit)

E

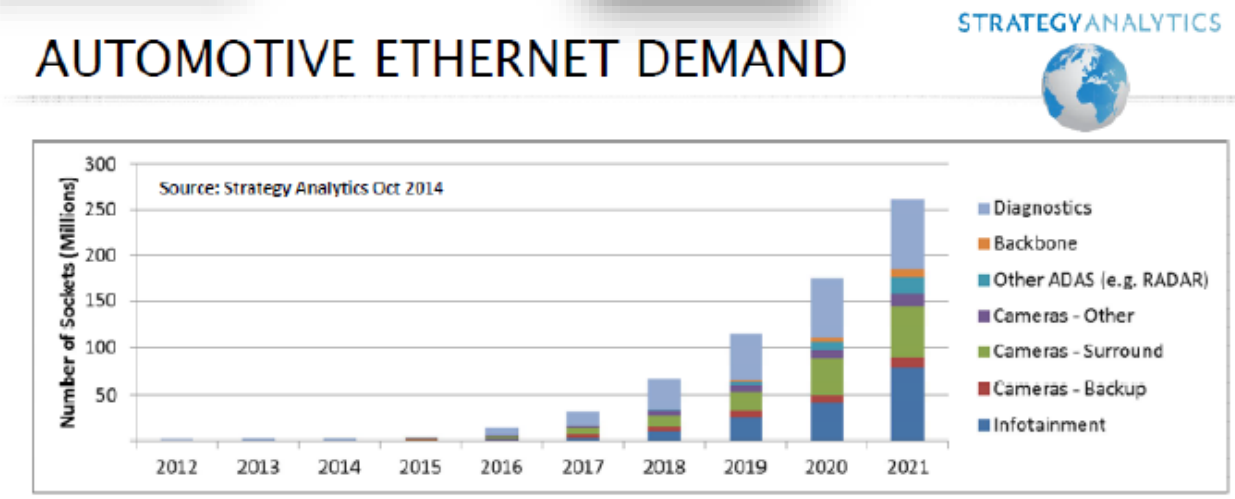
TECHNOLOGIES DRIVERS : KEY ROLE OF ETHERNET

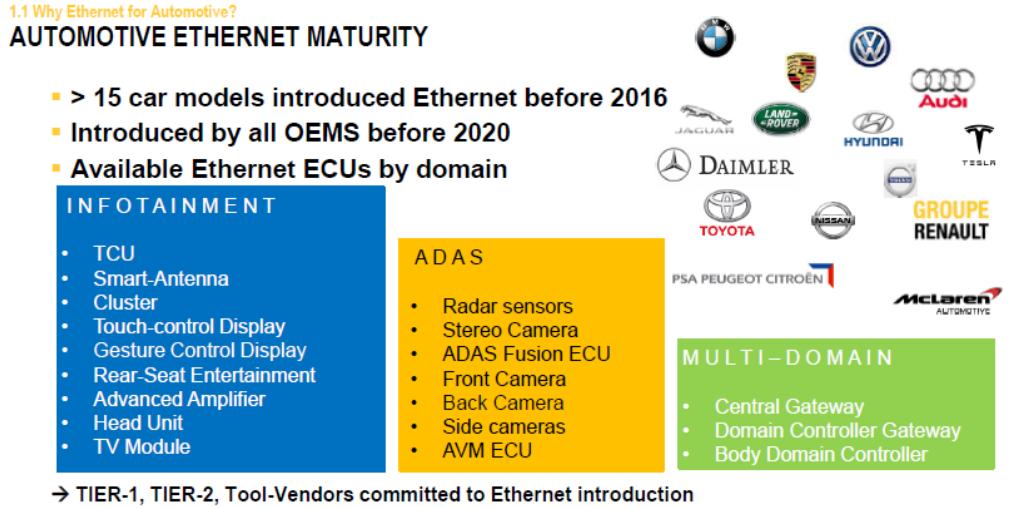
- Key Role of Ethernet
  - ❖ Offers huge Bandwith for features and OTA
  - ❖ Supports IP protocols (AVB, TSN…)
  - ❖ Is scalable

❖ Single Paire (Open Alliance standard)

MULTI USAGES

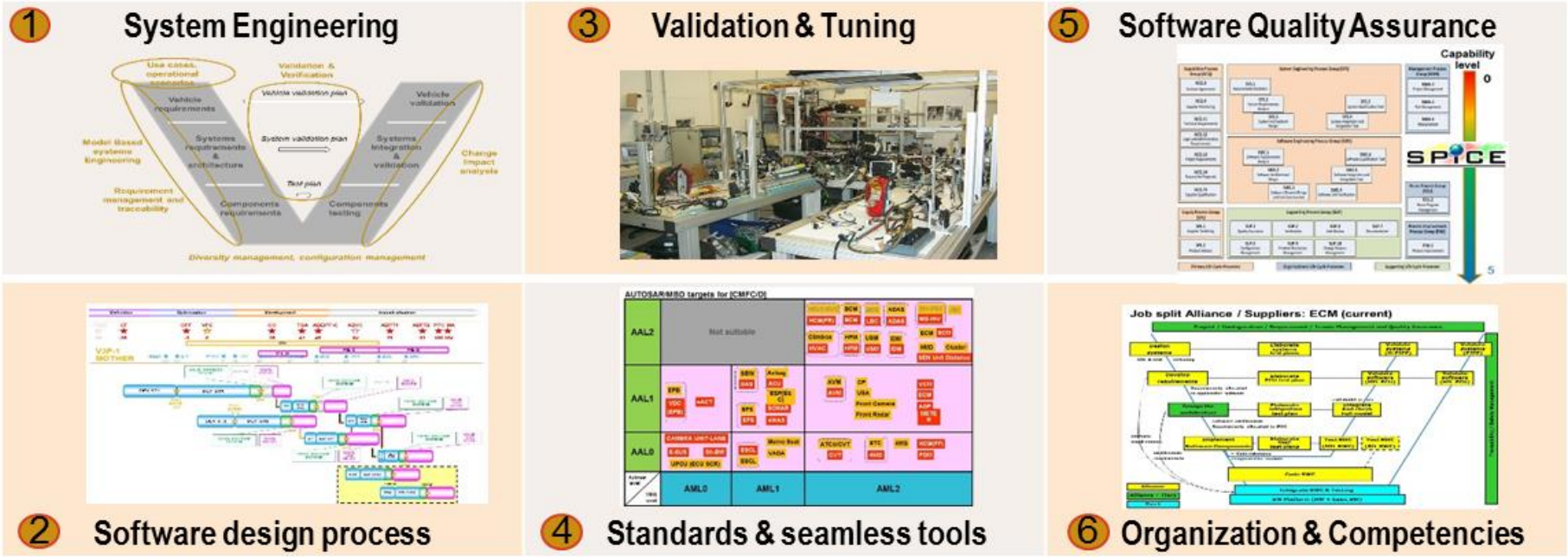
MARKET TREND





A

THE 6 LEVERS OF SOFTWARE ROBUSTNESS PLAN



Breakthrough plan including all Engineering, Quality and Purchasing divisions developing Systems and Software

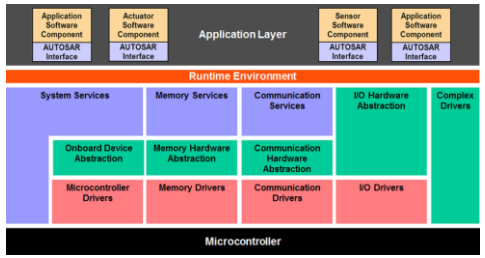
=> Improve Quality of Software at launch of new vehicles

SOFTWARE

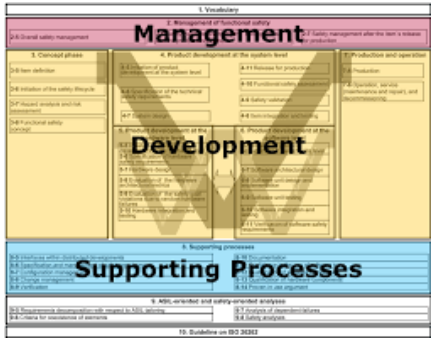
Deployment of international and widely used standards and practices such as Autosar, Genivi, Model Based Design, and of standard and seamless tools

AUTOSAR

AUTomotive Open System ARchitecture

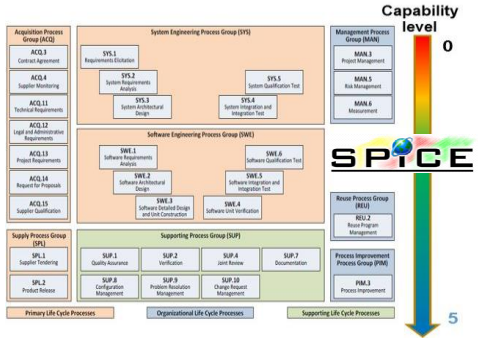


ISO 26262



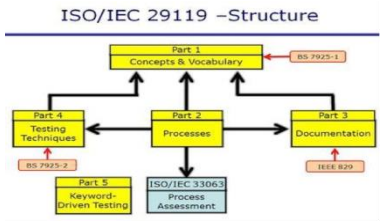
IEEE 730

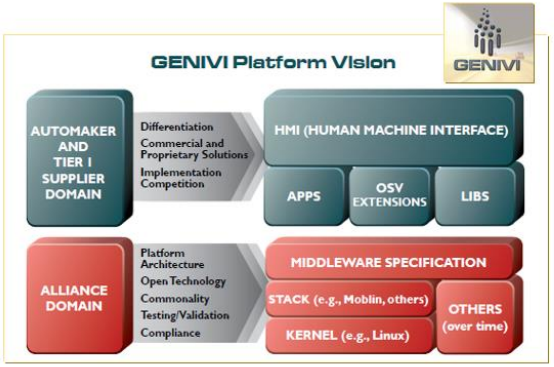
AUTOMOTIVE SPICE®



CMMI

ISO 29119

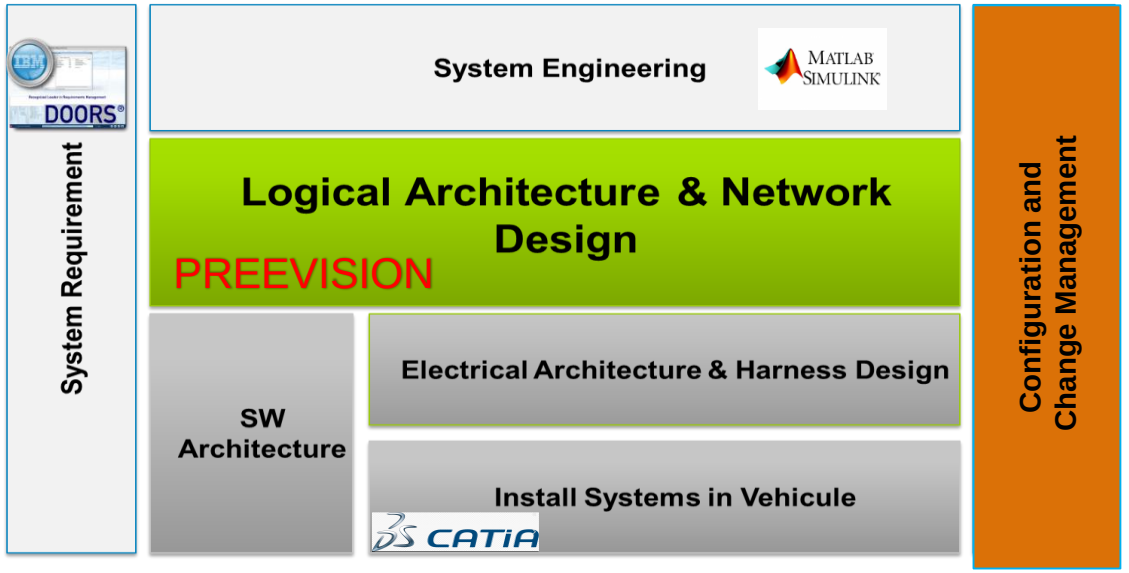


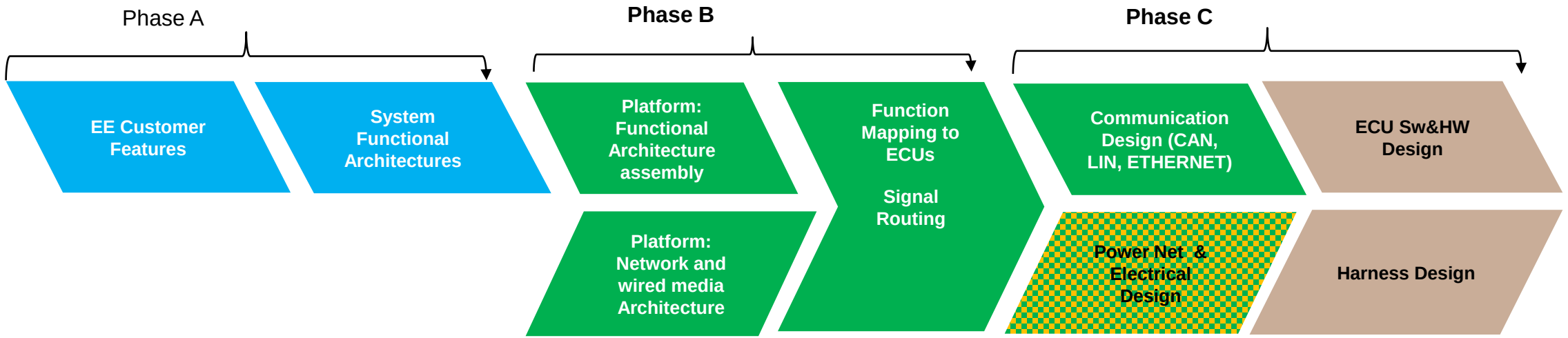


A

METHODOLOGY & TOOLS

- **Tools are now mandatory for EE Architecture needs**
  - A Continuous process from requirements to software
  - Continuity from OEM to Tiers1.
  - Continuity on V cycle with tools
  - Only Standards can offer those continuity





A

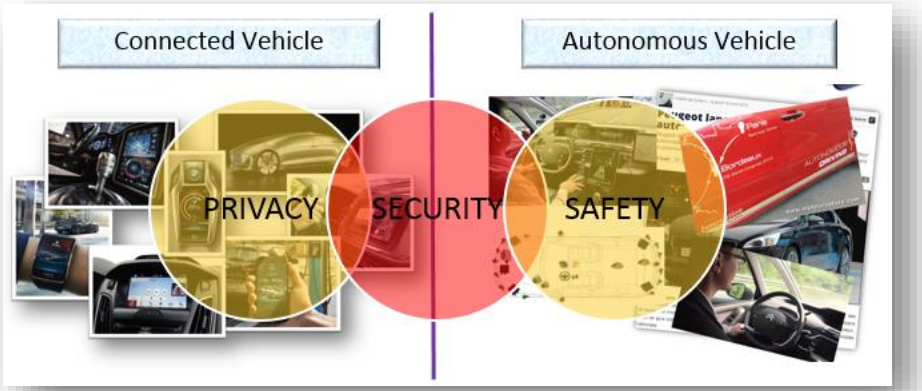
CONCLUSION



The Report

- **Electrification** on track all around the world
- **Vehicle** is and will be **connected** : Opportunity for all Automotive eco-system
- **Driving Assistance** to increase safety, from Level 2 up to Level 5

Responses



- Manage domains cohabitation : ***Safety + Privacy + Security.***
- All Architecture domain concerned : **Functional**, **Electronic**, **Electrical**
- Massive use of **standards** (Ethernet, CAN FD, Autosar, …)
- **Safety** & **Security** for all components: Hardware, Software
- **Quality** : Coverage, Completeness, and Consistancy on Product and Process

Opportunities

- New technologies challenge
- New strong skills for each domain
- Adapted System Engineering : Methodology & Tools
- Partnership and Cooperation