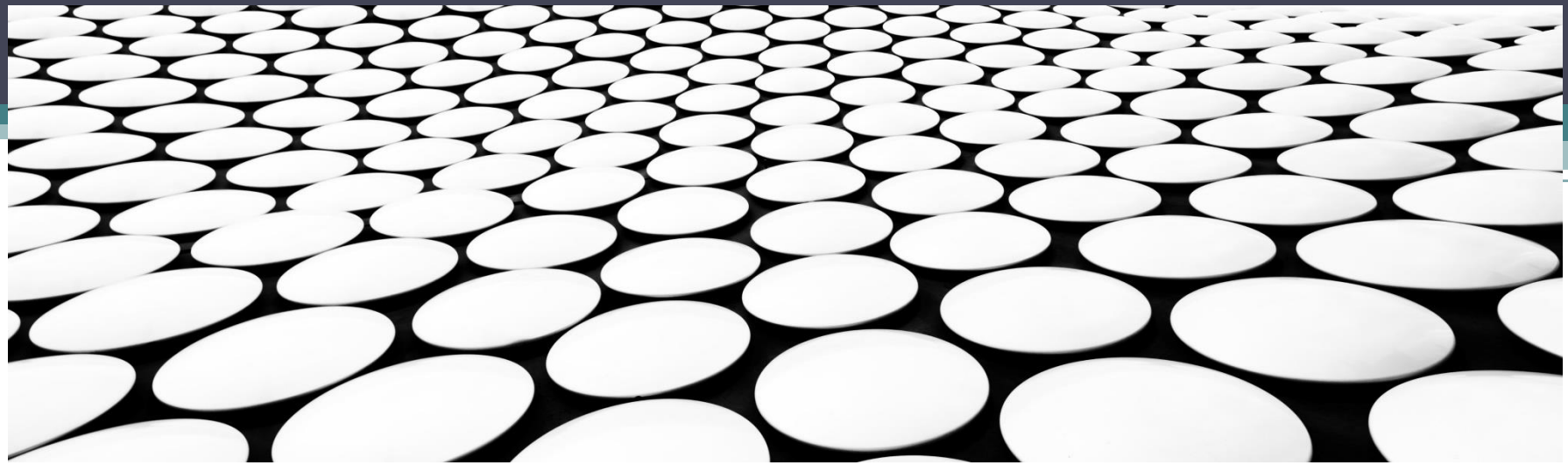
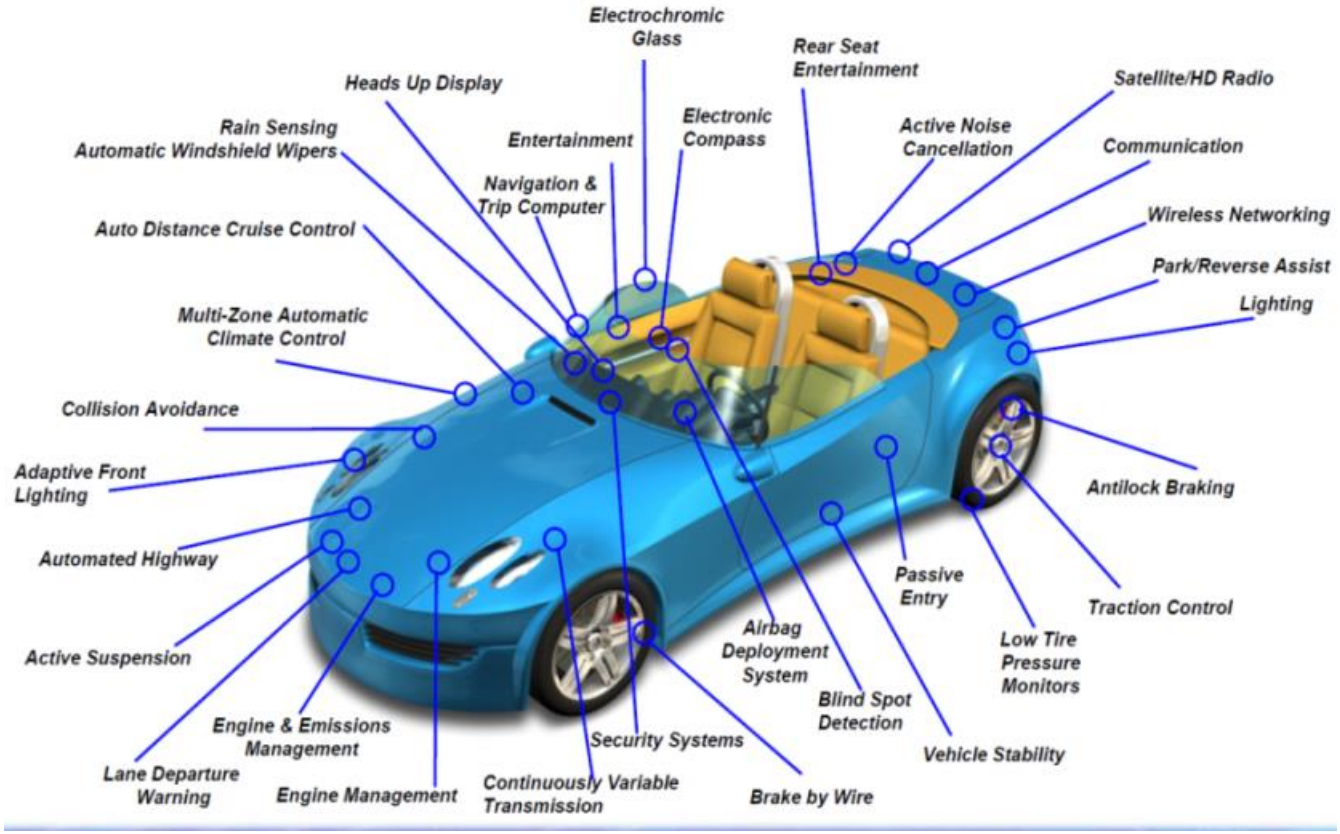
Rethinking the E/E System Architectures for Future Cars

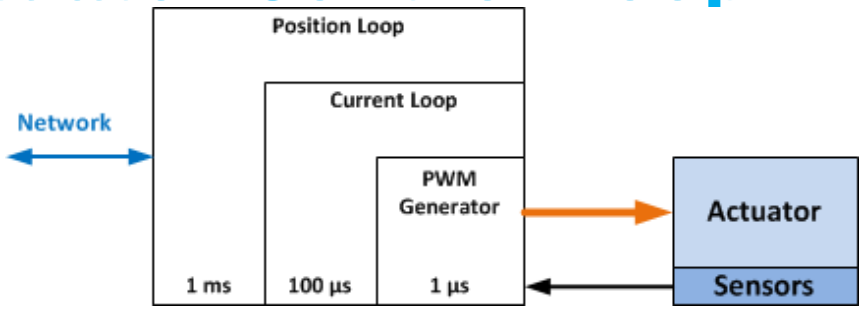


Embedded Systems are everywhere



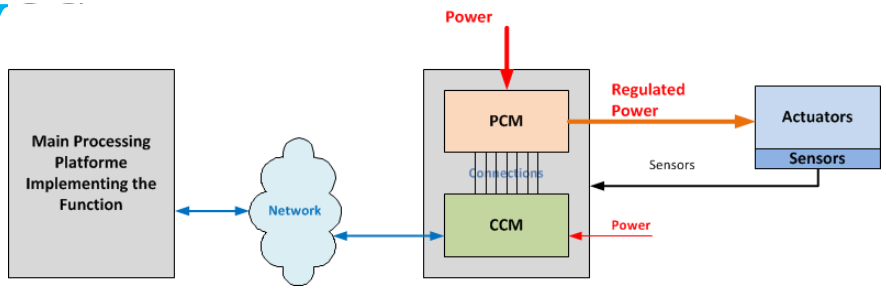
Embedded Systems control every Actuators

- **Actuator Control Loop**

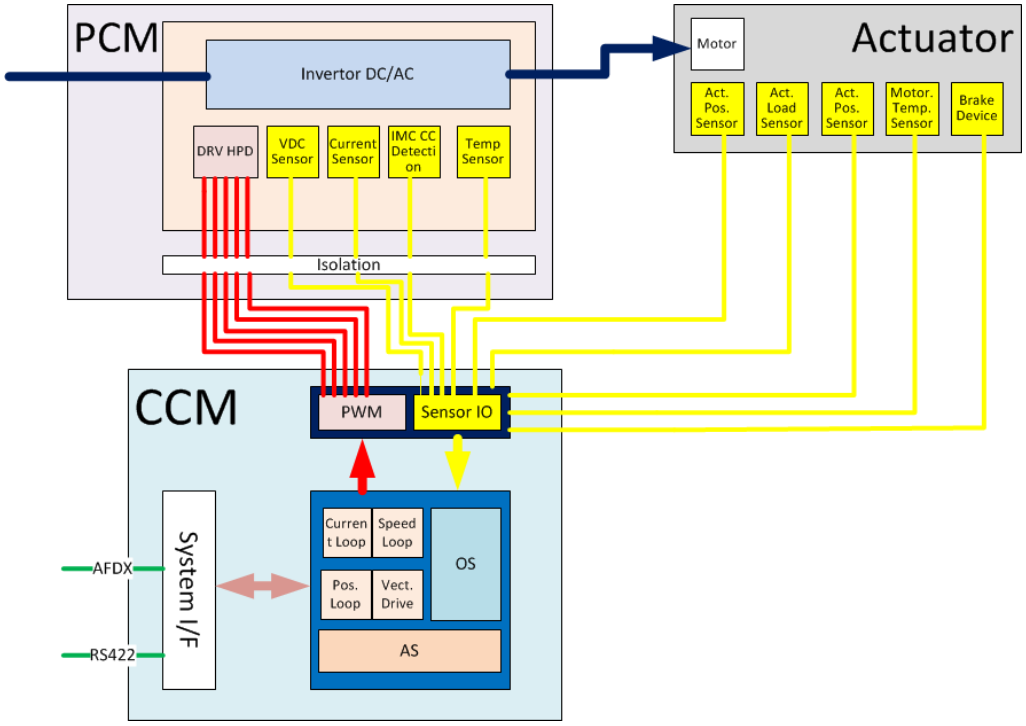


PWM : Pulse With Modulation
PCM : Power Control Module
CCM : Command Control Module

- **Typical Implementation of Actuator Driv**



Typical Actuator Drive



Typical controllers

- Vehicle Motion
  - ABS, ESP
  - Active Dumping
  - Active Steering (4WD)
  - Intelligent tires
  - Torque Vectoring
  - …
- Traction/Power train Control
  - Engine Control
  - Regenerative Breaking
  - Hybrid-Power Management
  - Torque Vectoring
  - …
- Vehicle Body Control
  - Window regulator
  - Thermal regulation
  - Rain sensing automatic whisper
  - Active node cancellation
  - Seat regulation
  - Occupant protection systems (Air Bag/Pre-tension)
  - …
- Driving assistance systems
  - Electronic all-around visibility
  - Driver information systems
  - Communication Systems
  - Navigation
- Automated Driving
  - Lane Assist
  - Adaptive Cruise Systems
  - Partial autonomous Drive
  - Full autonomous Drive

Safety Critical Systems

- **Safety Critical Systems** are ***Systems*** whose ***failures*** have ***potential catastrophic consequences***
  - *Loss of the vehicle*
  - *Destruction of other vehicles & equipments*
  - *Death or injury of vehicles occupants*
  - *Death or injury of people staying around the vehicle*
- **Estimating the reliability of a Safety Critical System:**
  - *Determining the Feared Events*
  - *Determining the Severity of the Feared Events*
  - *Estimating the occurence of the Feared Events*

The attributes of a DEPENDABLE SYSTEM

- **Availability (“readiness for correct service”),**
- **Reliability (“continuity of correct service”),**
- **Integrity (“maintaining the consistency of data”),**
- **Maintainability (“ability for a process to undergo modifications and repairs”),**
- **Safety (“absence of catastrophic consequences on the users and the environment”)**
- **Security (“prevention of unauthorized disclosure of information”)**
- **Certificability (“capacity of to obtain safety certification from standard authority“).**

The Risk Assessment MatriX

PROBABILITY	SEVERITY				
	A Catastrophic	B Critical	C Major	D Minor	E Negligible
5 Frequent	5A	5B	5	5D	5E
4 Occasional	4A	4B	4C	4D	4E
3 Remote	3	3B	3C	3D	3E
2 Improbable	2A	2B	2C	2D	2E
1 Extremely Improbable	1A	1B	1C	1D	1E

Estimating the criticity of an Equipment

- **Light System**
- **Emergency Braking System**
- **Air conditioning System**

Safety Versus Reliability versus Availability

- **Reliability**:
  - Capacity to maintain the operation without interruption.
  - Reliable service may be costly to ensure safety
- **Availability**:
  - Capacity to deliver the service at the given time
  - Available System may be neither reliable nor safe

- **Safety:** Absence of catastrophic errors
  - Detects a dangerous condition and bring the system in safety modus
  - Safe system may offer very little „availability“

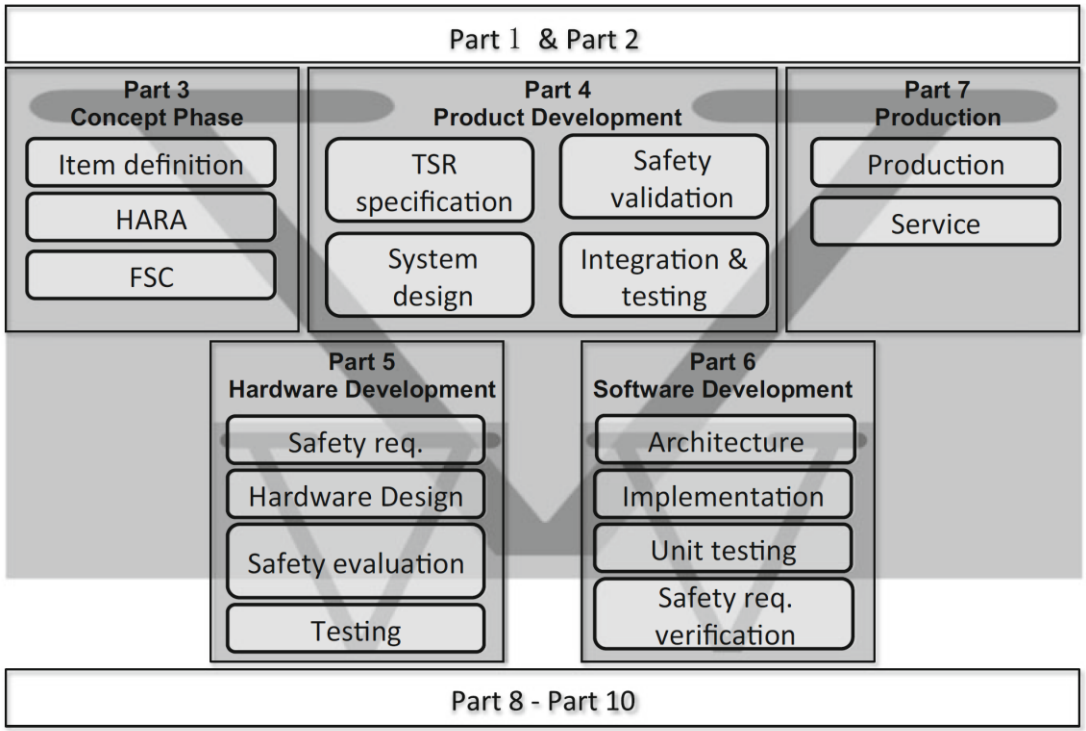
Why Safety matters ? The criticity associated to the controlers

- Vehicle Motion
  - **ABS, ESP**
  - **Active Dumping**
  - **Active Steering (4WD)**
  - **Intelligent tyres**
  - **Torque Vectoring**
  - …
- Traction/Power train Control
  - **Engine Control**
  - **Regenerative Braking**
  - Hybrid-Power Management
  - **Torque Vectoring**
  - …
- Vehicle Body Control
  - Window regulator
  - **Thermal regulation**
  - Rain sensing automatic whisper
  - **Active node cancellation**
  - Seat regulation
  - Occupant protection systems (Air Bag/Pre-tension)
  - …
- Driving assistance systems
  - Electronic all-around visibility
  - Driver information systems
  - Communication Systems
  - Navigation
- Automated Driving
  - Lane Assist
  - Adaptive Cruise Systems
  - Partial autonomous Drive
  - Full autonomous Drive
  - Automated Emergency Braking

Function Reliability Versus Component Reliability

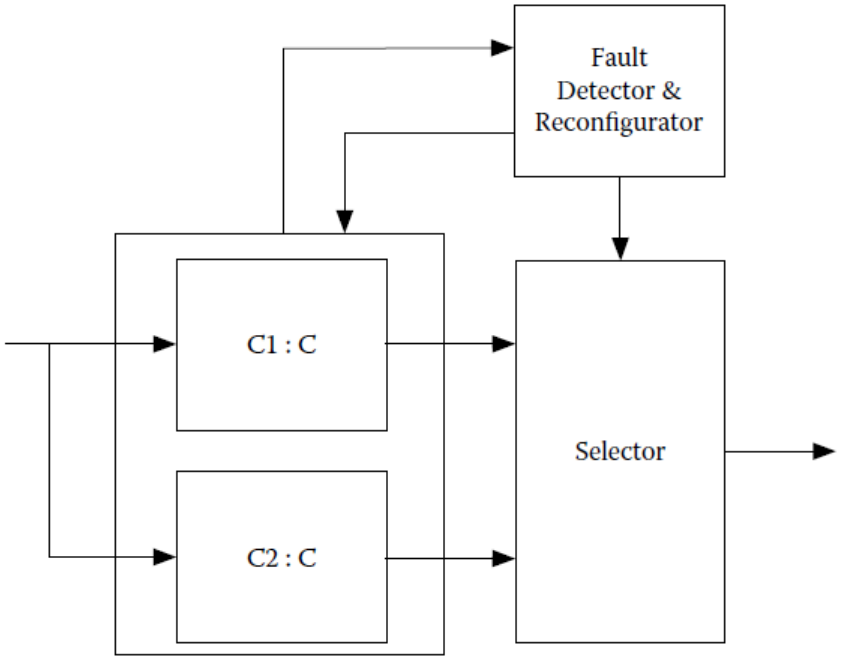
- **Function reliability**
  - The requirements regarding the function itself, with no indication about how the function is implemented.
- **Compoment reliability**
  - The estimated reliability of the components that host one or many functions.
- **Function mapping**
  - A function is mapped to a set of components that host this function
  - A component may host many functions

ISO26262 – Safety Standard Focusing on Automotive Electrical/Electronics Application



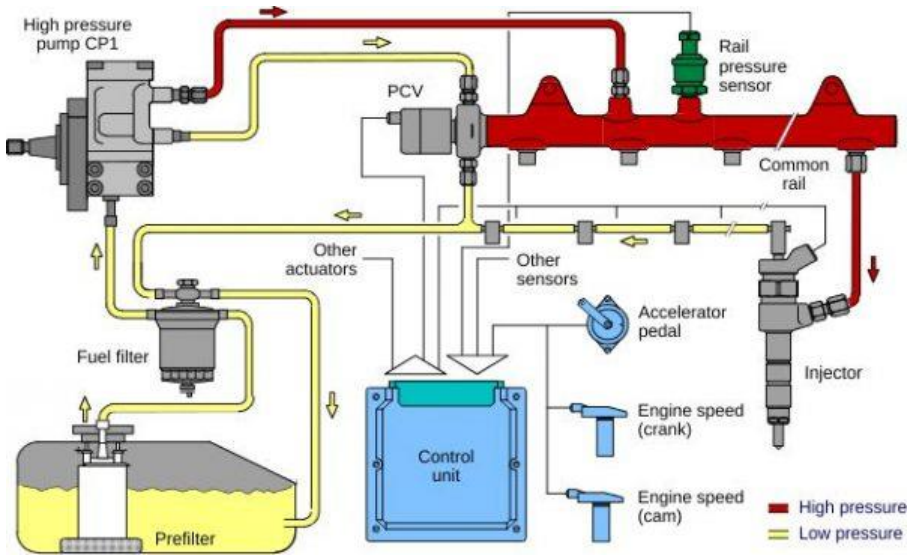
The Safety Dilemna

- No electronics component offers **the required level of reliability**
  - **Maximum level of reliability: $10^{-5}h^{-1}$**
- No way to ensure the level of reliability without monitoring and/or duplication.
- This dramatically increases the cost of the vehicle



Safety Analysis of the pressure control of a common rail injection system

- Identification of the feared events
- Determining the criticity of this function
- Propose a mechanism to ensure a safe operation
- Propose an implementation to support the mechanism



Current Car architecture

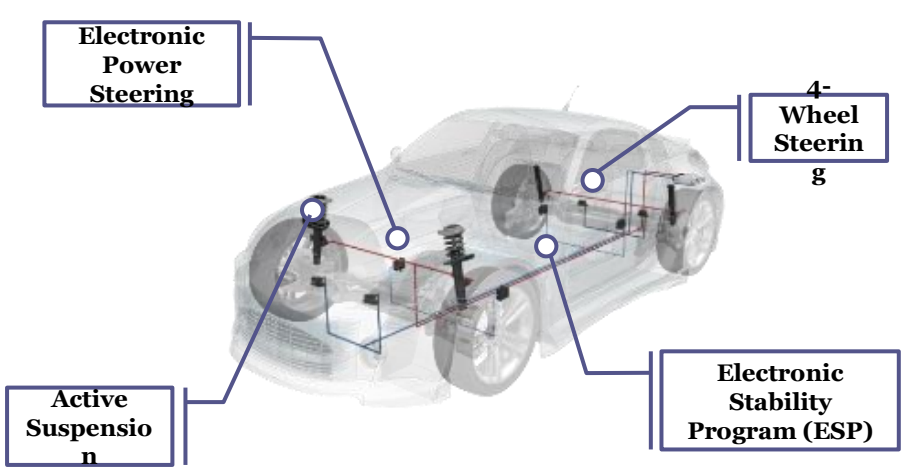
- What is the main knowledge of a car maker ?
  - Designing the global car architecture
  - Designing the body
  - Designing the chassis
  - Specifiying the multiple functions to be integrated
  - Integrating and orchestrating a set of functions that are either internally or externally developped
- Car Maker are thinking in terms of functions
  - Power train function
  - Breaking function
  - Entertainement function
  - …

A function or group of functions ⇔ A set of components to implement it

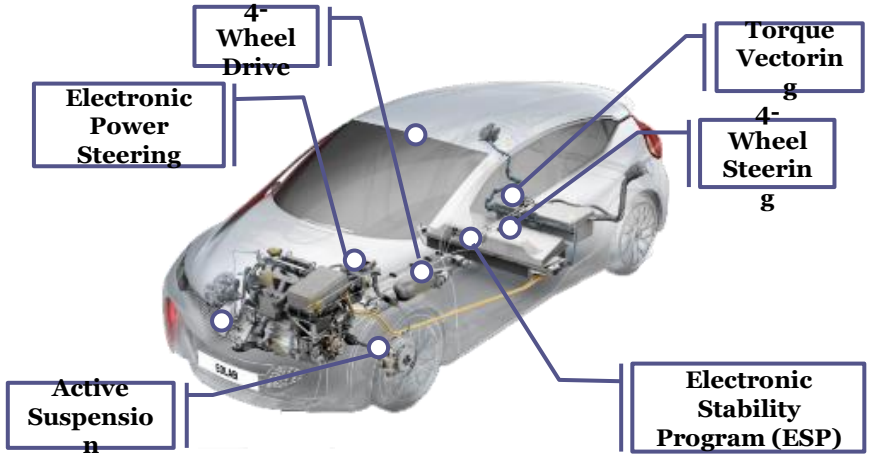
Strengths and Limits of this approach

- **Strengths**
  - Function segregations
  - Easily substituable
  - Model and Data independent
- **Limits**
  - Uses its own hardware
  - Limited global coordination with other functions
  - May not use the full potential of the car equiments (overactuated vehicle)

CONTROLING AN OVERACTUATED CHASSIS

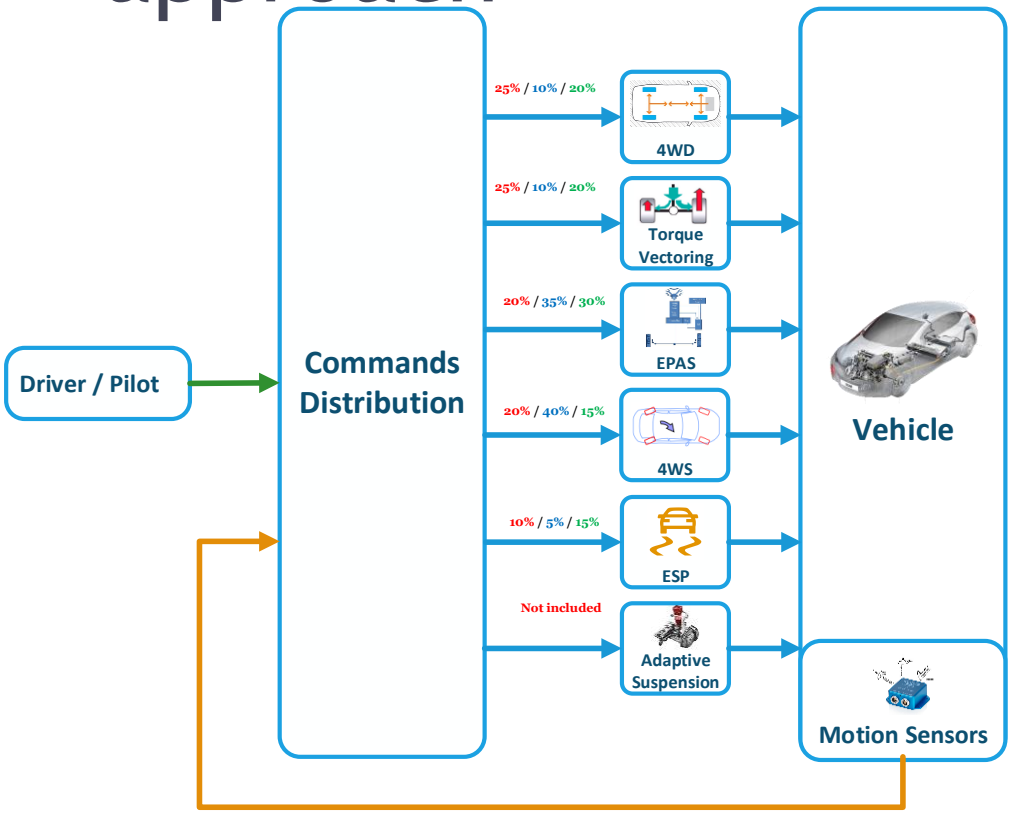


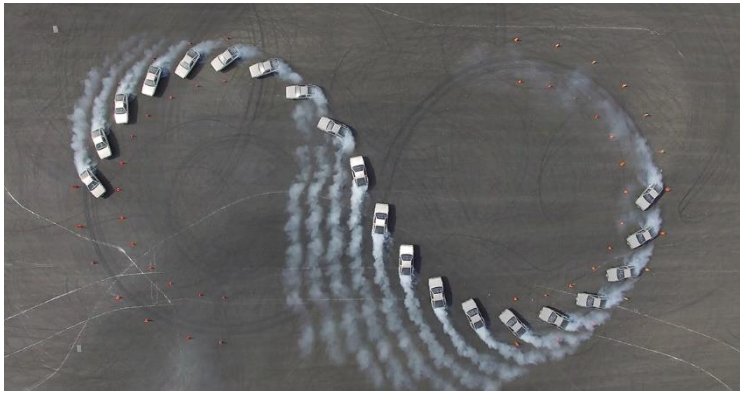
Current Situation



Future Situation

Towards a Global Orchestration approach





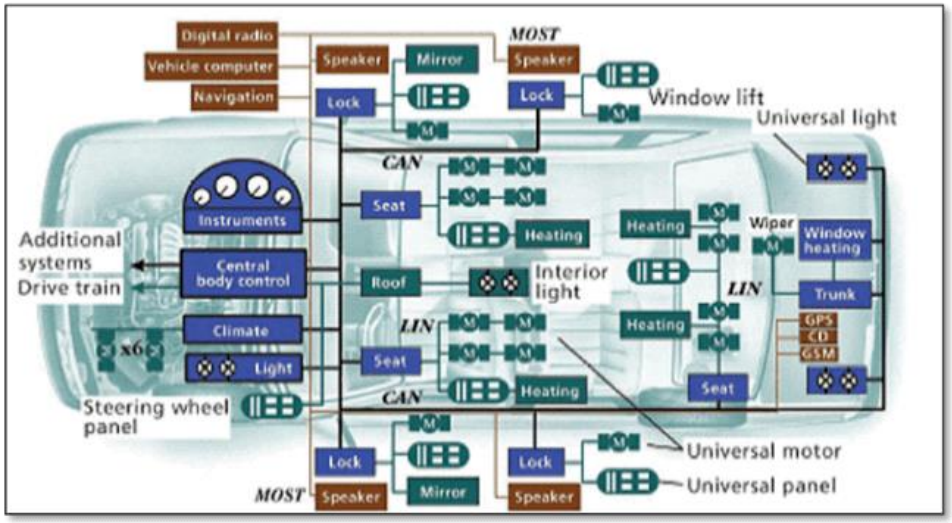
Sport / **Comfort** / **Eco**

What makes overactuated cars interesting

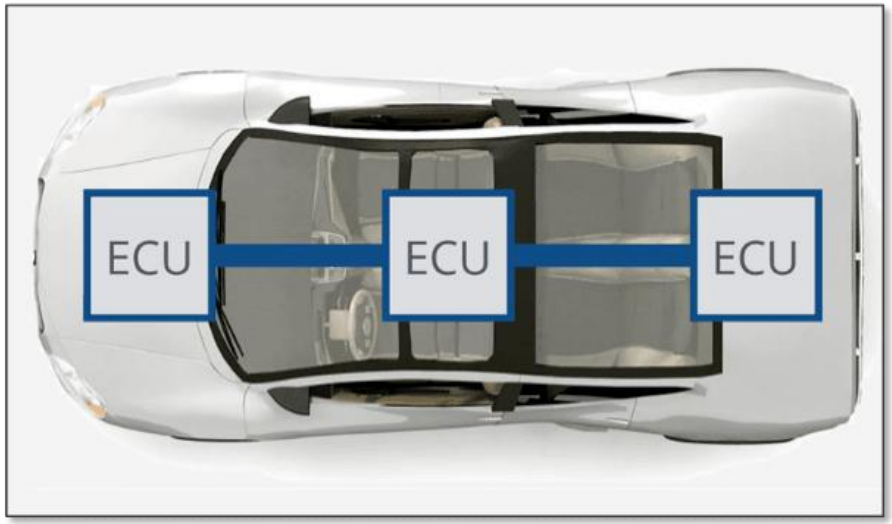
- Performance-wise
- Safety-wise
- Confort-wise

Moving From An Function segegrated architecture to a Centralized architecture

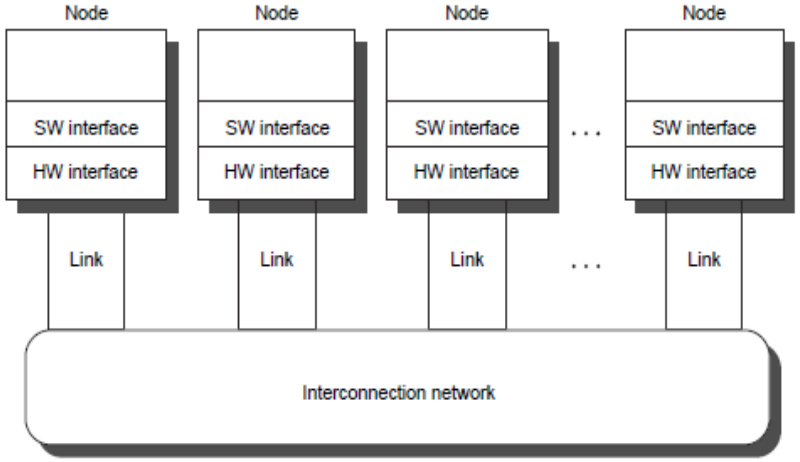
Conventional Architecture



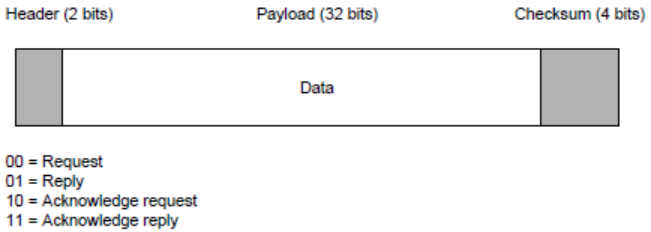
Software Centric Approach



Networking: A short introduction

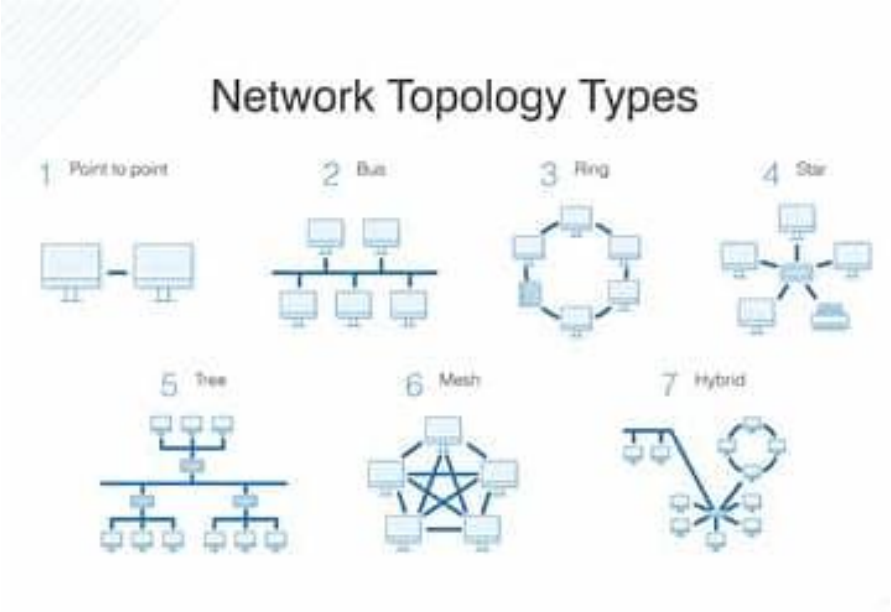


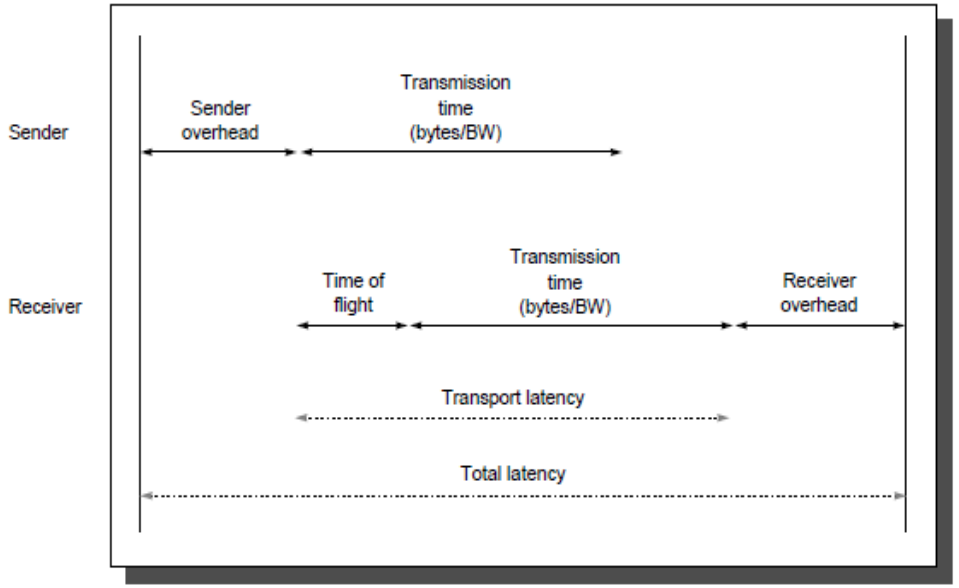
- A small message structure



- Bandwidth : the maximum rate at which the interconnection network propagates information.
- Time of flight : The time the first bit of the message reached at the receiver.
- Transmission time : The time for the message to pass through the complete network.

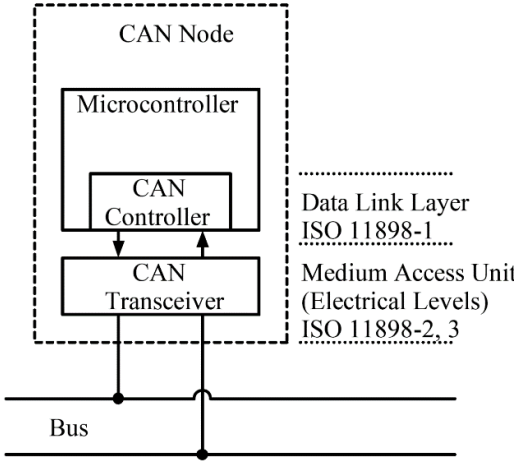
Typical Timing Issues And Network Topologies



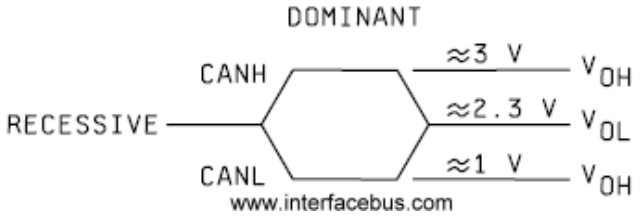


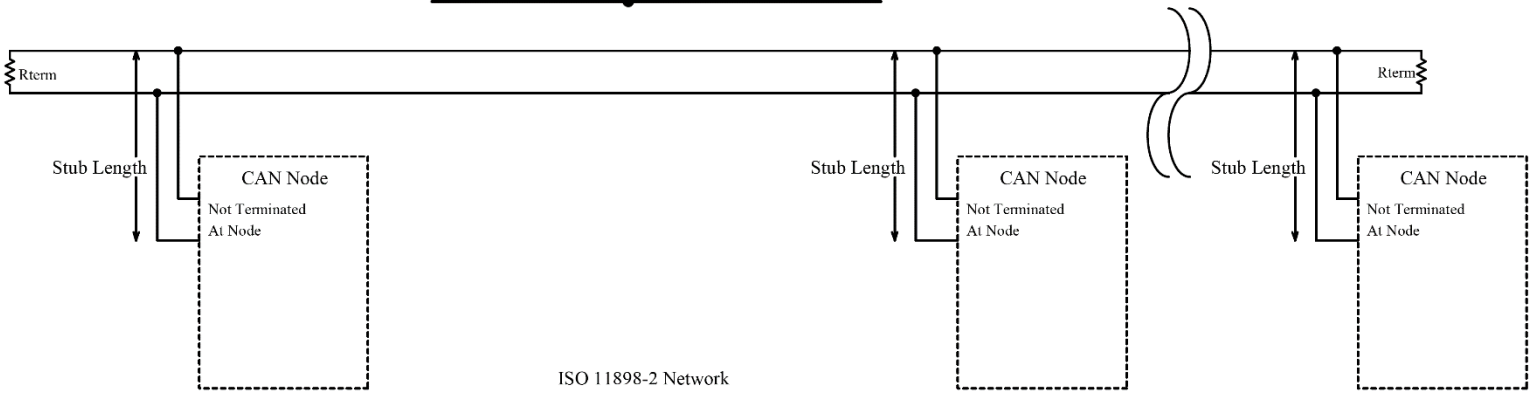
CAN: A Short Introduction

- **CAN functionality is divided into two layers**
  - Data-Link
  - Physical



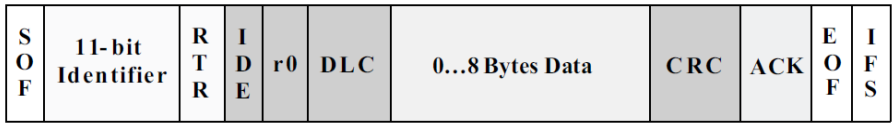
- **Physical layer**
  - bit encoding and de coding, bit timing, synchronization processes.
  - Differential signal encoding





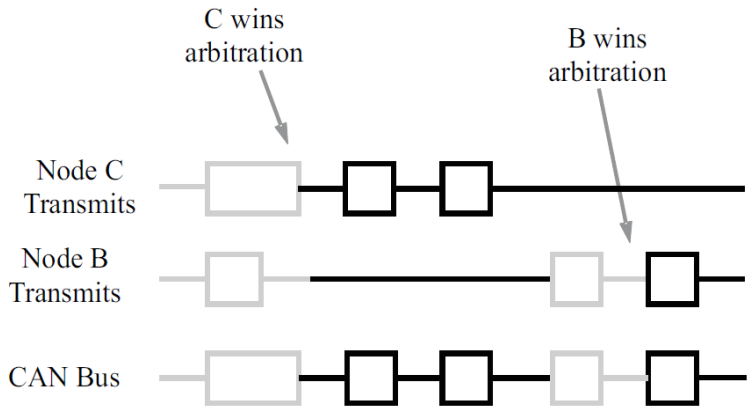
CAN: Messages and arbitration

Standard CAN Message

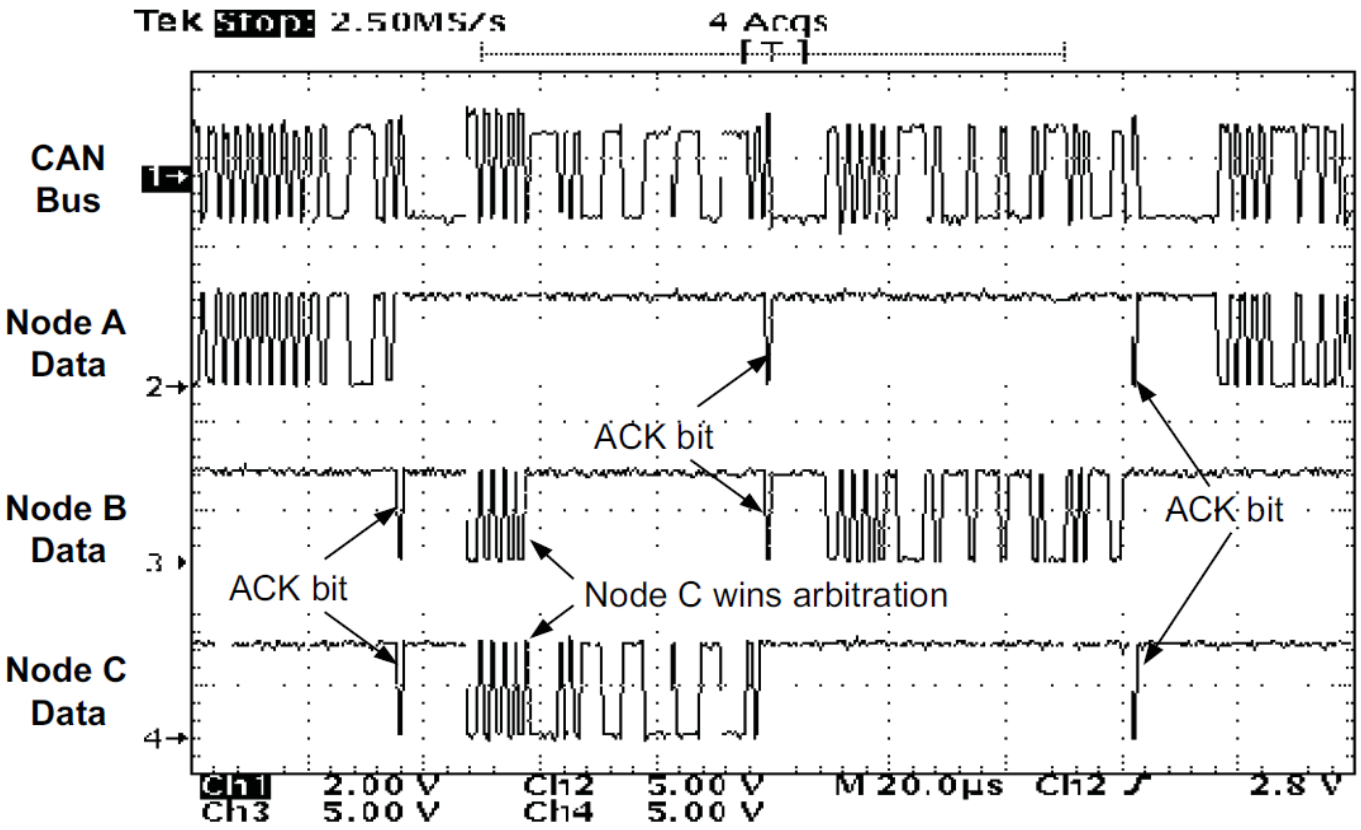


- **Data Frame**: Send data
- **Remote Frame**: Request data
- **Error Frame**: misformed frame to signal an erroneous state
- **Overload Frame**: misformed frame to signal a busy state.

Arbitration



CAN : Typical Bus-Traffic



NETWORK: Safety Issues

What may go wrong ?

- Wires get damaged
- Message get lost
- Message get corrupted
- Node can never access to the network
- Node never releases access to the network.
- Node is polluting network

Real-Time related constraints and issues

- Cyclic Message
  - Each message occurs every x ms.
- Event-Based Message
  - An event generates the message

- **Problem**
  - How to garantee that all the messages can be successfully delivered ?

The Mixed-Criticality Challenge

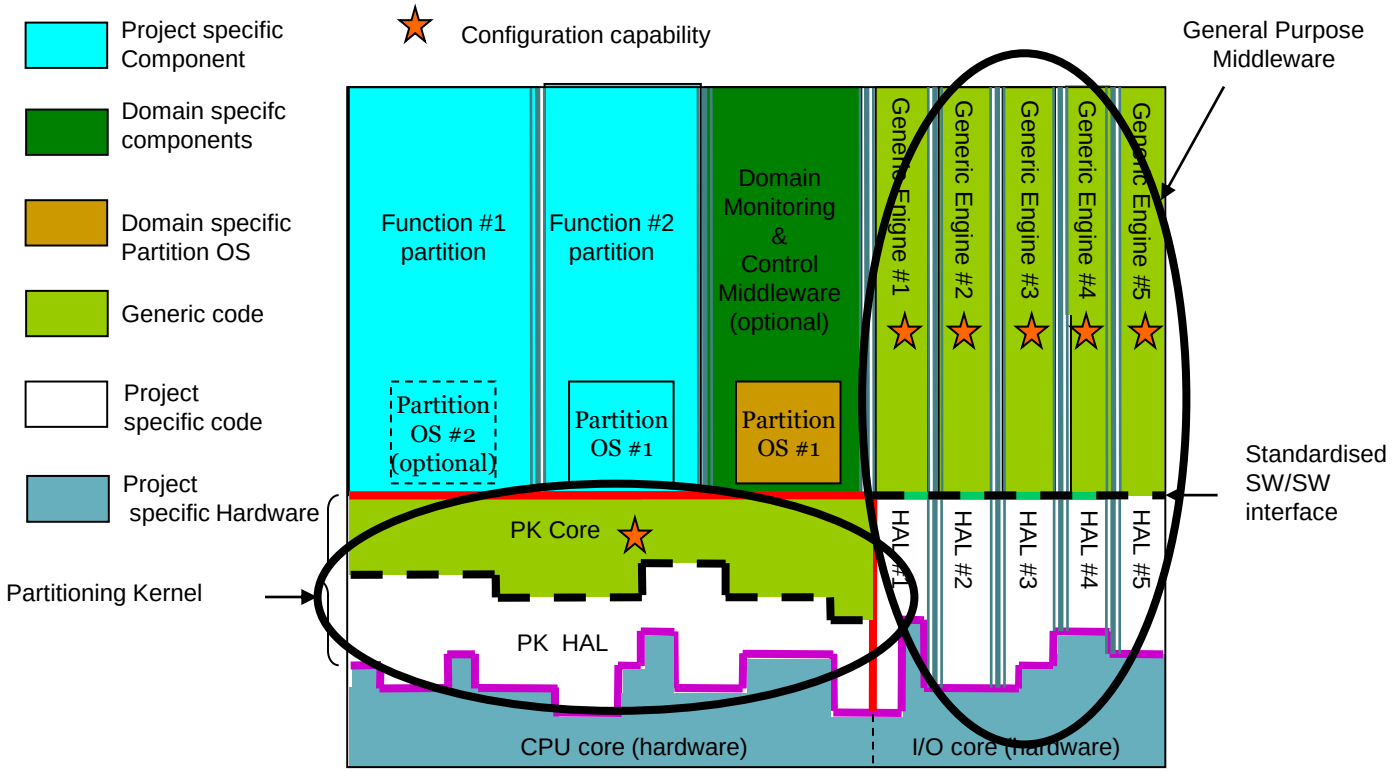
- **Mixed criticality System:**

System Platform that executes several applications of different criticality, such as safety-critical and non-safety critical or of different ASILs.

- **Central ECU, Shared hardware (sensors, actuators, networks):** may become a Single Point Of Failure to many when not all applications

- **Computational Node:** segregation must be warranted.

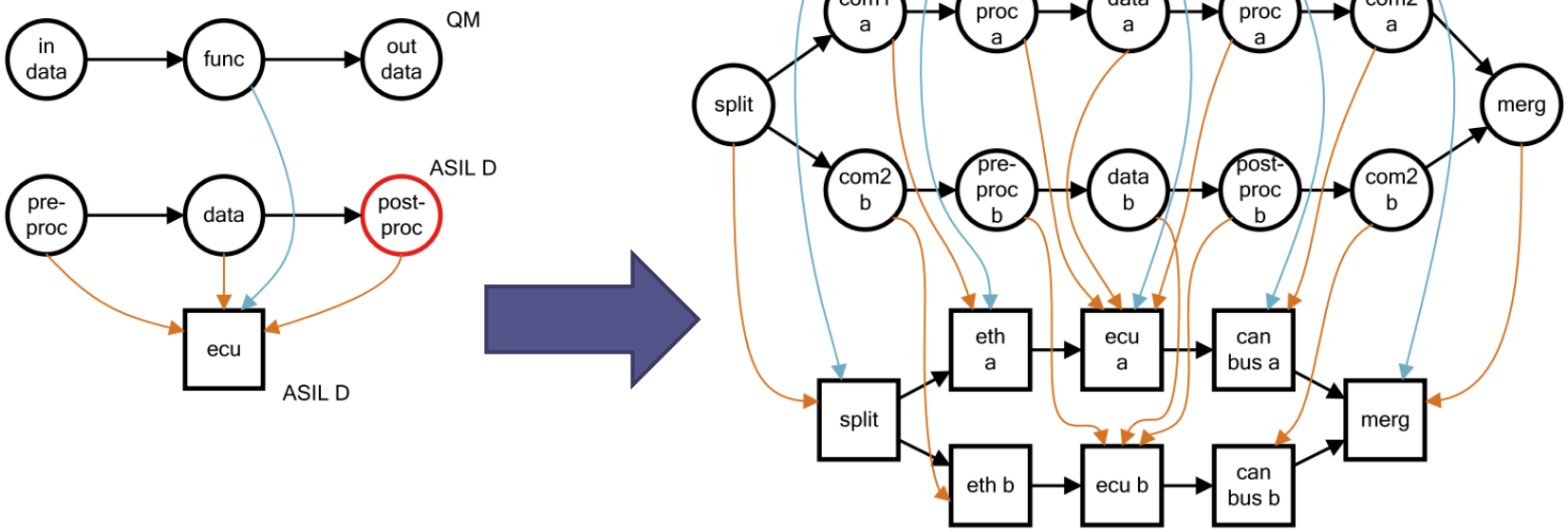
Hypervisors as a Solution to handle Mixed-Criticality



Examples of typical ECU processing types per functional domains

Domain	Control loop time	Real time	ASIL	Processing type	Software type	Examples
Infotainment	ms	AVB, soft real time	Mostly QM, Up to B	µC with GPU	Possible	No
Body and comfort	ms	Soft real time	Mostly QM, Up to B	µP	Possible	Possible
Powertrain	µs	Hard real time	Up to D	µP Multi-core	Possible	No
Chassis	ms /µs	Hard real time	Up to D	µP Multi-core	Possible	User permission
ADAS domain	ms	Hard real time	Up to D	µC with GPU	No*	User permission
ADAS sensors	ms	Hard/soft real time	Up to D (B and C common)	µC with GPU	No**	No

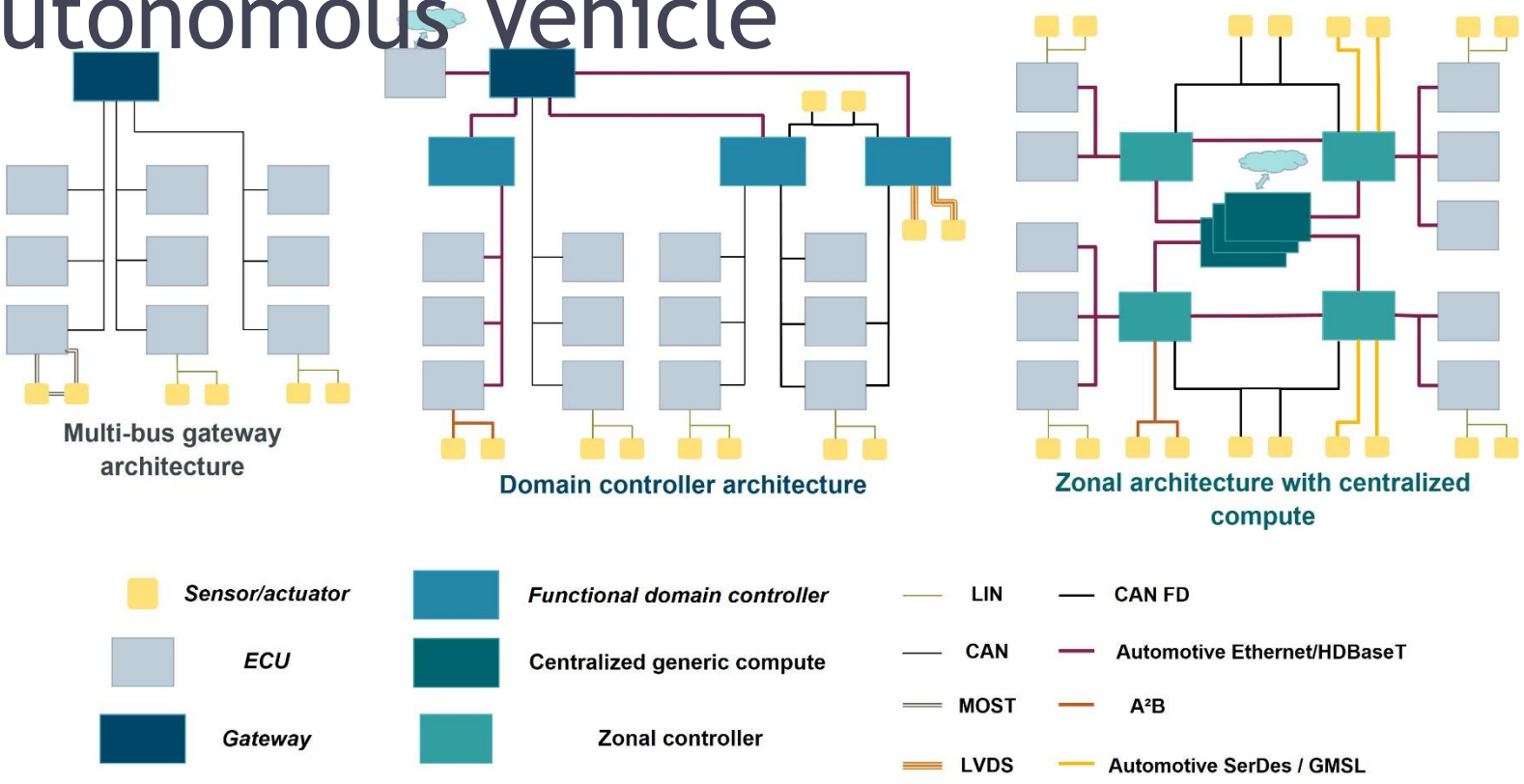
Mapping NodeS according to Criticality



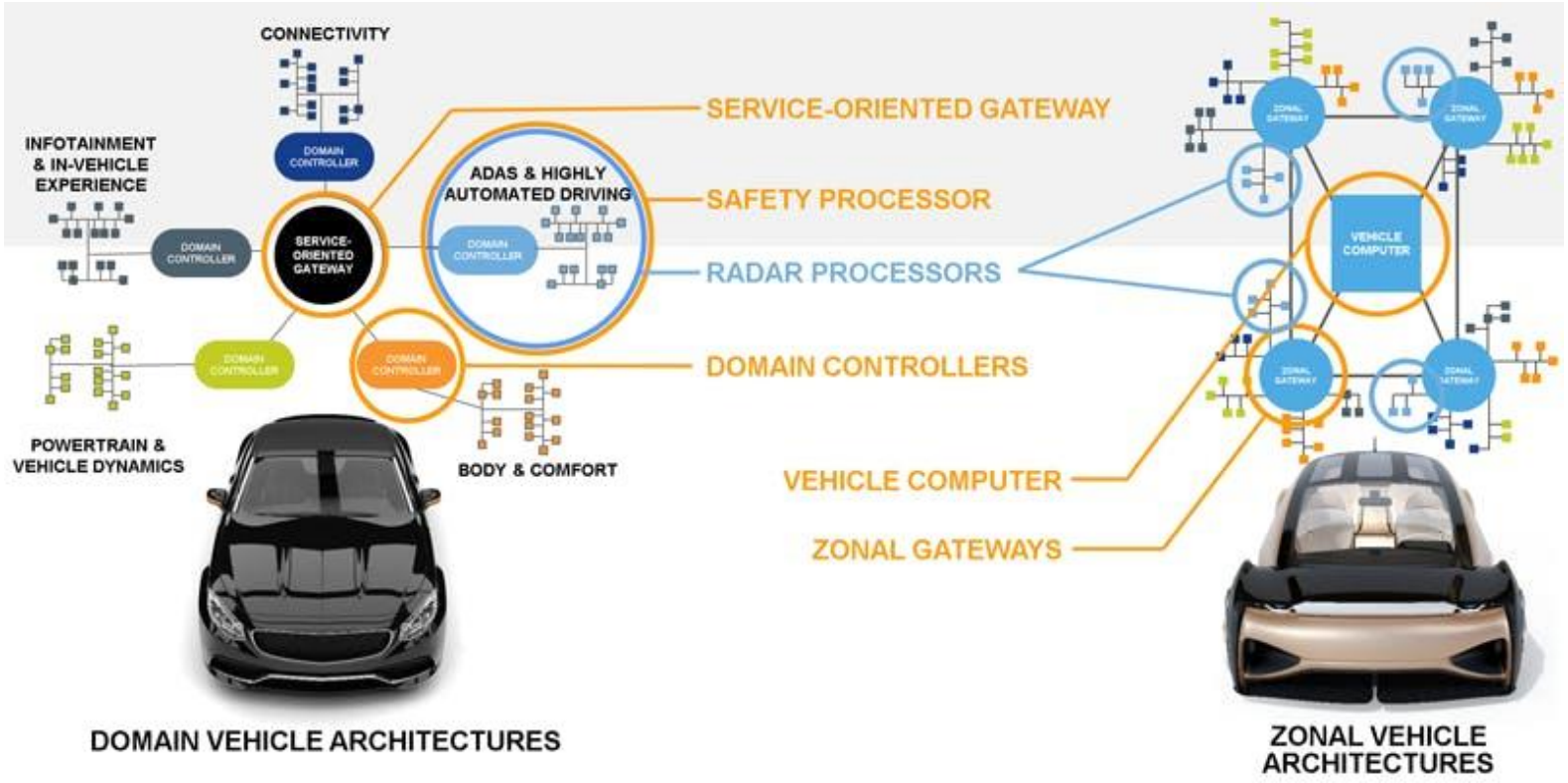
Automotive Architecture Topologies

- **Domain-Based (D):** System components are grouped according to their functionality. A domain is supervised by a controller and all the sensors and actuators are connected to this controller.
- **Zone-Based (Z)**: System components get grouped according to their location. groups system components according to their physical position in the vehicle. All the components are connected to the nearest controller with a direct connection or a local zone network. Zone are connected to the central unit or to other zones via a backbone.
- **Vehicle-Centralized (VC):** All the computational nodes are mapped to the central unit. Domain and local controllers are gateway.
- **Controller-Based (CB):** Computational nodes may be mapped to domain or controllers that are local to zones, a central computation unit may handle the data that belongs to many zones or domains.

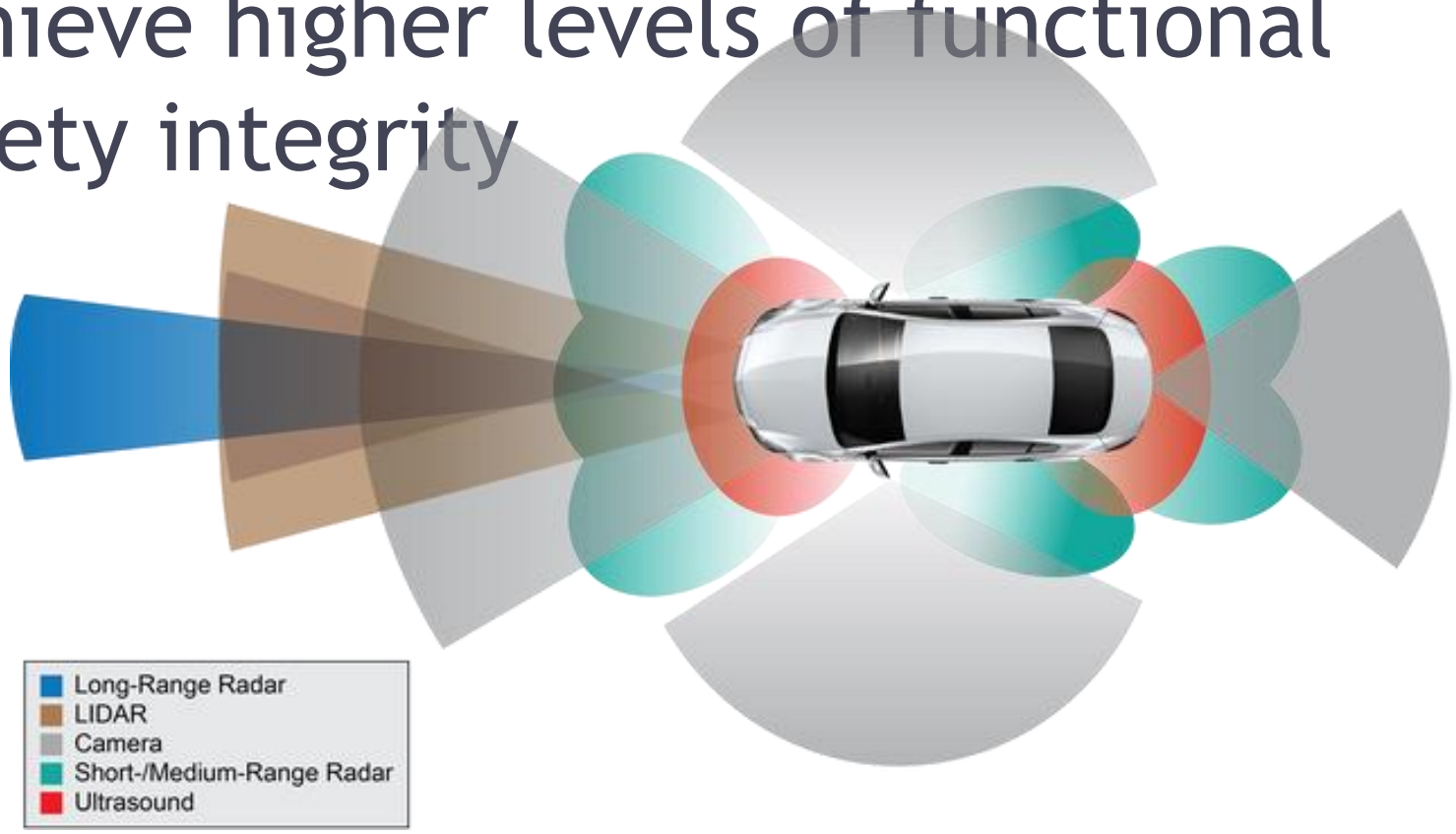
Electrical/Electronics Architecture For Autonomous Vehicle



Difference between Domain Vehicle Architectures and zonal Vehicle Architectures



Overlaying redundant sensors enables ADAS and self-driving systems to achieve higher levels of functional safety integrity



Network-Centric Vehicle

Security Challenges for the Connected Car

Valuable Data

- Collection of data/info
- Storage of data
- Diagnostic functions

Protect Privacy

High Vulnerability

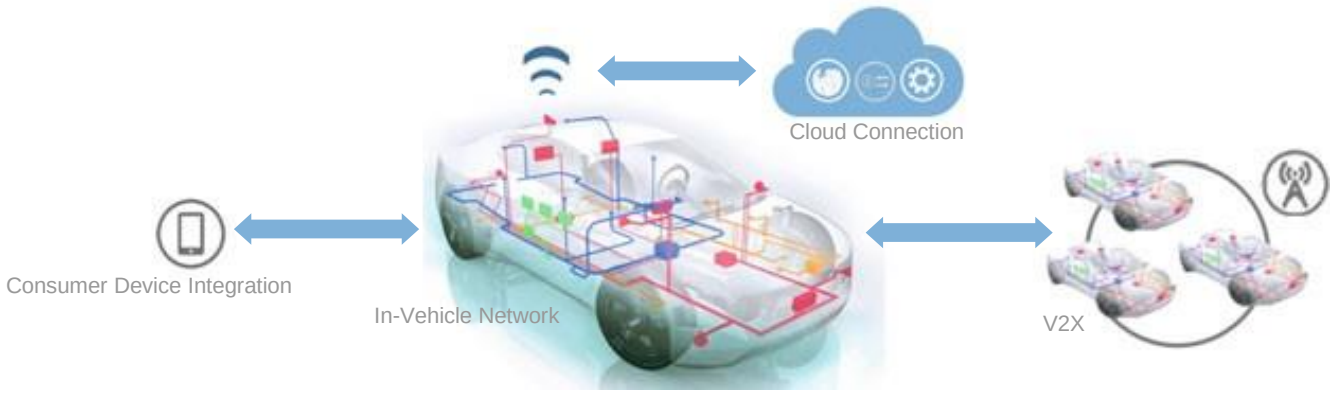
- Increasing number of nodes
- More advanced features
- More and more software

Increase Safety

Easy (Remote) Access

- Fully Connected Car
- External & internal interfaces
- Wired & wireless interfaces

Prevent Unauthorized Access



USE CASE : Integrating an AUTOMATED EMERGENCY STEERING into a VEHICLE