Software Architectures for Advanced Driver Assistance Systems (ADAS)

Elektrobit

Robert Leibinger
July 7th, 2015

Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture

Agenda

- Short overview of Elektrobit automotive
- The road to Advanced Driver Assistance Systems
- Challenges for ADAS
- System Architecture
- ECU Software Architecture

About Elektrobit (EB) Automotive

EB'S TECHNICAL CORE COMPETENCES ARE:
Automotive-grade software
System and software architectures

OVER 1300 EMPLOYEES

GLOBAL PRESENCE:
development and business offices in Austria, China, Finland, France, Germany, Japan, Romania and USA

2014 NET SALES* OF MEUR 171.4, up 24%

LISTED ON NASDAQ OMX HELSINKI: EBC1V

Over **70 million** vehicles on the road and
1 billion embedded devices

** including 51% of e.solutions*

Our solutions for the automotive world

Infotainment software and services

- Connected navigation software
- HMI tools for in-dash, digital instrument clusters and head-up displays
- Global software integration and engineering services

Connected services

- Connected experiences around urbanization and electrification
- Online diagnostics
- Software and content updates

Car Infrastructure software and services

- EB tresos – integrated ECU software and tools, based on AUTOSAR standards
- Complete solutions for: basic software, functional safety, automotive security
- Test & Analyzing solutions
- Functional Safety consulting

Driver Assistance software and services

- Software development for driver assistance functions
- Electronic horizon and test drive recording solutions
- Driver Assistance modules and algorithms

Delivering unique experiences year over year

1997 – Establishing the idea of **embedded systems control via Internet technologies**

2003 – Providing **navigation for the first fully connected solution** (Daimler A-class and smart)

2004 – Pioneering the **separation of HMI software by rest of the vehicle** (Audi A6)

2008 – **e.solutions** is formed, a joint venture between **EB and Audi Electronics Venture GmbH (AEV)**

2010 – **Strategic partnership of Daimler and EB** centered around **driver assistance software development**

2012 – EB, the **first company to take AUTOSAR 4.0 to the road across the globe** (all BMW carline)

2014 – Expanded innovation focus: **Automated Driving, Car as a Sensor, Connected Everything**

EB at the forefront of automotive technology

Paving the way to automated driving

Automated Driving

- EB's electronic horizon information is playing a major role for predictive driving
- Connected Navigation in combination with Driver Assistance is the lever for highly automated driving

Car as a Sensor

- Delivering ADAS and navigation data (electronic horizon) to enable future driving experiences
- Long-standing experience with connected services in safety- and security-critical environments

Connected Everything

- Know-how in OBD with experience in mission critical client/server systems
- Secure back-end infrastructure to enable OTA data and service updates.
- Always up-to-date maps validated by EB via vehicle sensor data to provide the highest quality maps

Agenda

Short overview of Elektrobit automotive

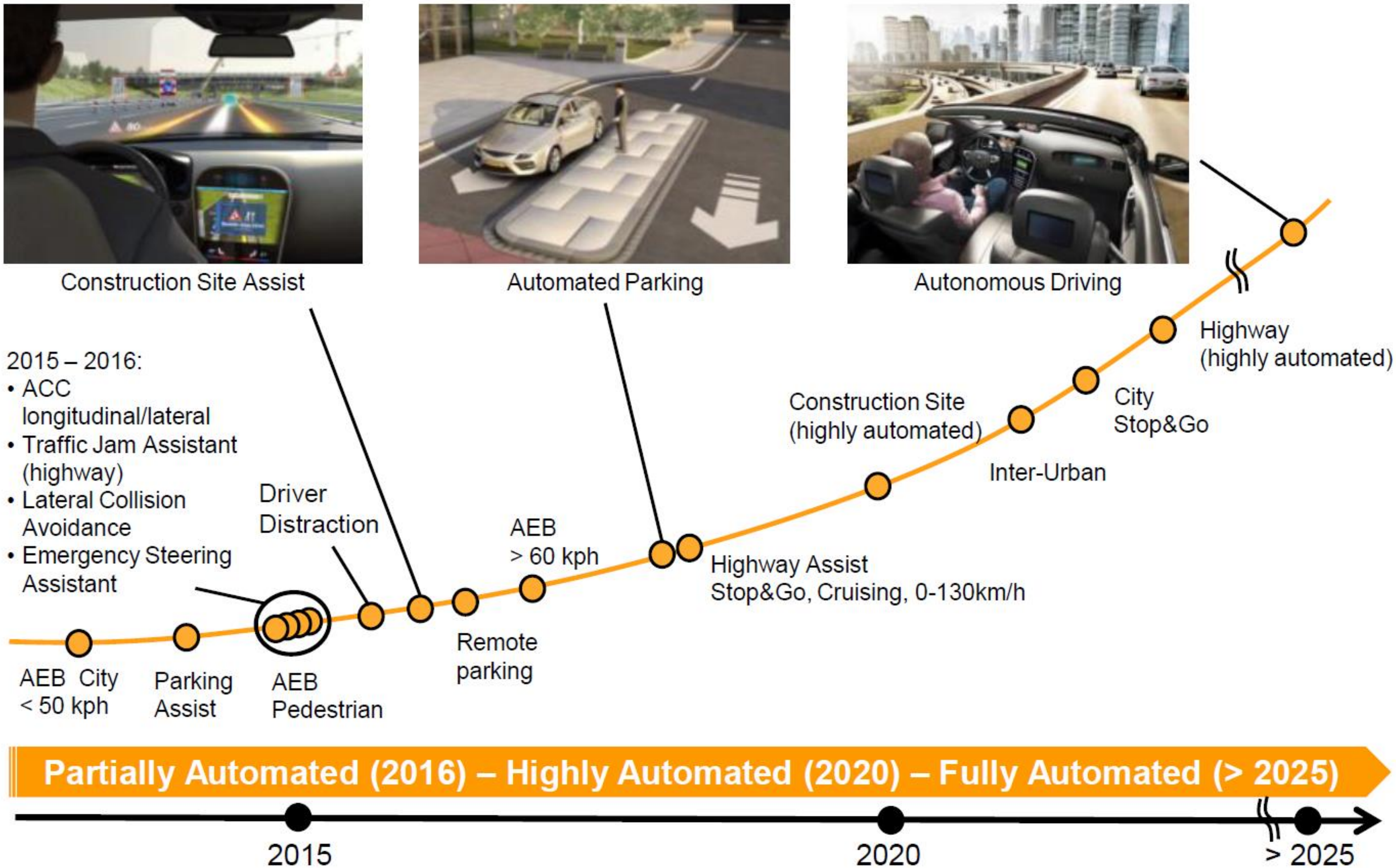
The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture

History and Roadmap for Accident-Free Driving



http://www.continental-corporation.com/www/download/portal_com_en/themes/ir/financial_reports/download_download_channel/fb_2014_en.pdf

Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture

Confidence

Taken from wikipedia.org

Who was this woman?

Bridget Driscoll

- Bridget Driscoll received instant notoriety when she stepped off the kerb and into the history books on August 17th 1896.

- Mrs Driscoll, a 44 year old housewife, who was travelling from Old Town, Croydon to a folk-dancing display in Crystal Palace, became **the first pedestrian in the UK to be killed by a car**.

- Mrs Driscoll, a resident of Croydon, was hit by a demonstration car **travelling at 4mph**. She died within minutes of receiving a head injury.

The Case

- Witnesses said that the car, driven by Arthur Edsel, was travelling at a **reckless pace**, in fact: “like a fire engine”.
- Mr Edsel claimed that he had only been doing 4 mph and that he had **rung his bell as a warning**.
- The jury took six hours to reach a verdict that Mrs. Driscoll had died of **accidental death**.
- At Mrs Driscoll’s inquest, Coroner William Percy Morrison said he hoped that ***“such a thing would never happen again”*** and was the first to apply the term **“accident”** to violence caused by speed.
  Coroners across the country have followed his example ever since.

Today…

Bild

1. MONAT FÜR 0,99 € | STIMMUNG | WETTER 29°C HANNOVER

BILDplus NEWS POLITIK GELD UNTERHALTUNG SPORT BUNDESLIGA LIFESTYLE RATGEBER REISE

01.07.2015 - 17:02 UHR HOME › NEWS AKTUELL › DEUTSCHLAND › VOLKSWAGEN › VOLKSWAGEN: ROBOTER TÖTET MITARBEITER

WERK IN BAUNATAL

Roboter tötet VW-Mitarbeiter!

Das VW-Werk in Baunatal (Archivbild)

Foto: dpa Picture-Alliance

TEILEN TWITTERN

01.07.2015 - 15:53 Uhr

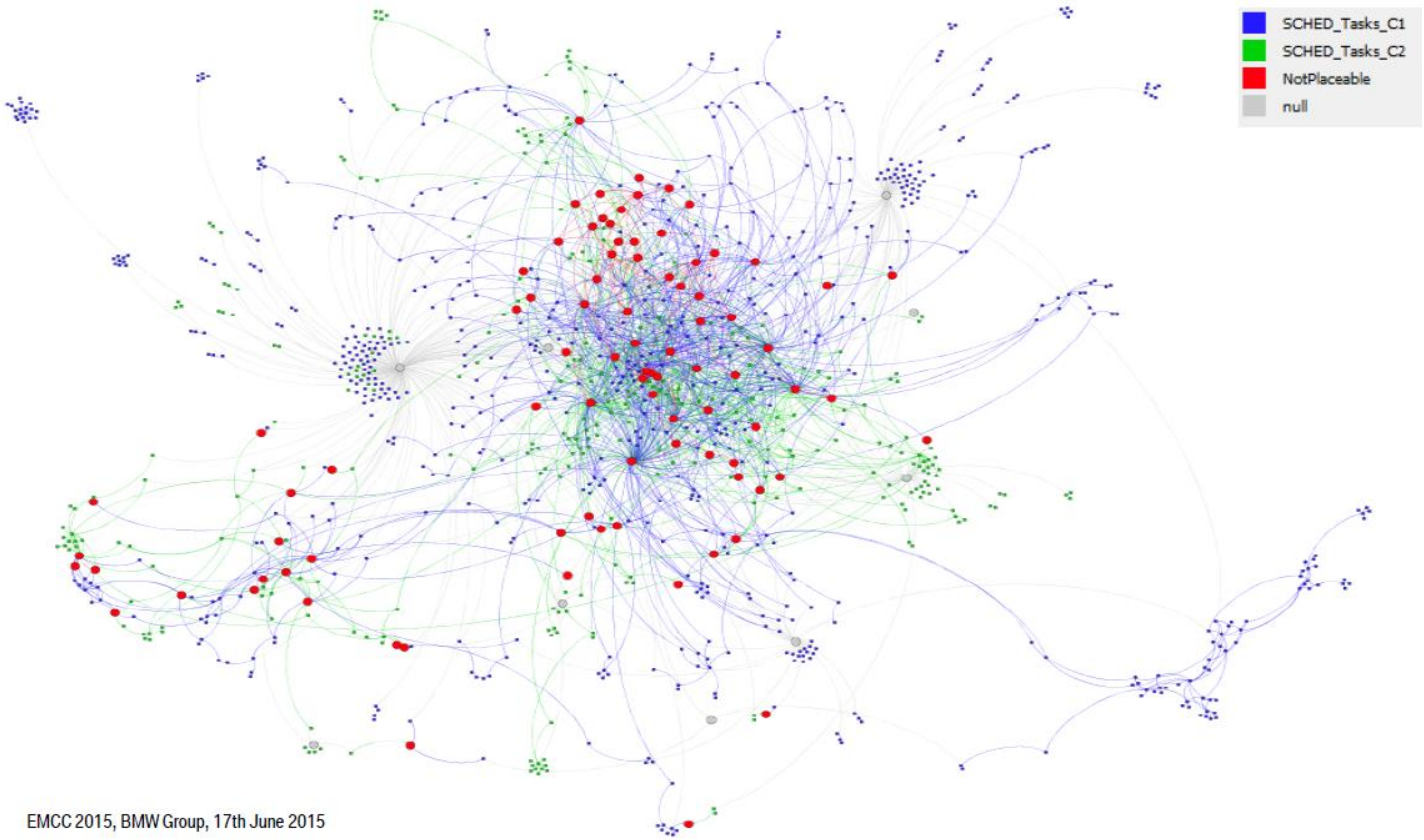
Baunatal (Hessen) – **Horror-Unfall im Volkswagenwerk Baunatal: Ein Mitarbeiter ist von einem Roboter getötet worden!**

Der 22-Jährige war am Montag bei einer neuen Produktionslinie der Elektromotorenfertigung mit dem Einrichten des Roboters beschäftigt, als dieser ihn erfasste und gegen eine Metallplatte drückte. Das teilte ein Sprecher des VW-Werks am Mittwoch mit.

Der Mitarbeiter einer Fremdfirma aus Sachsen erlitt schwere Quetschungen im

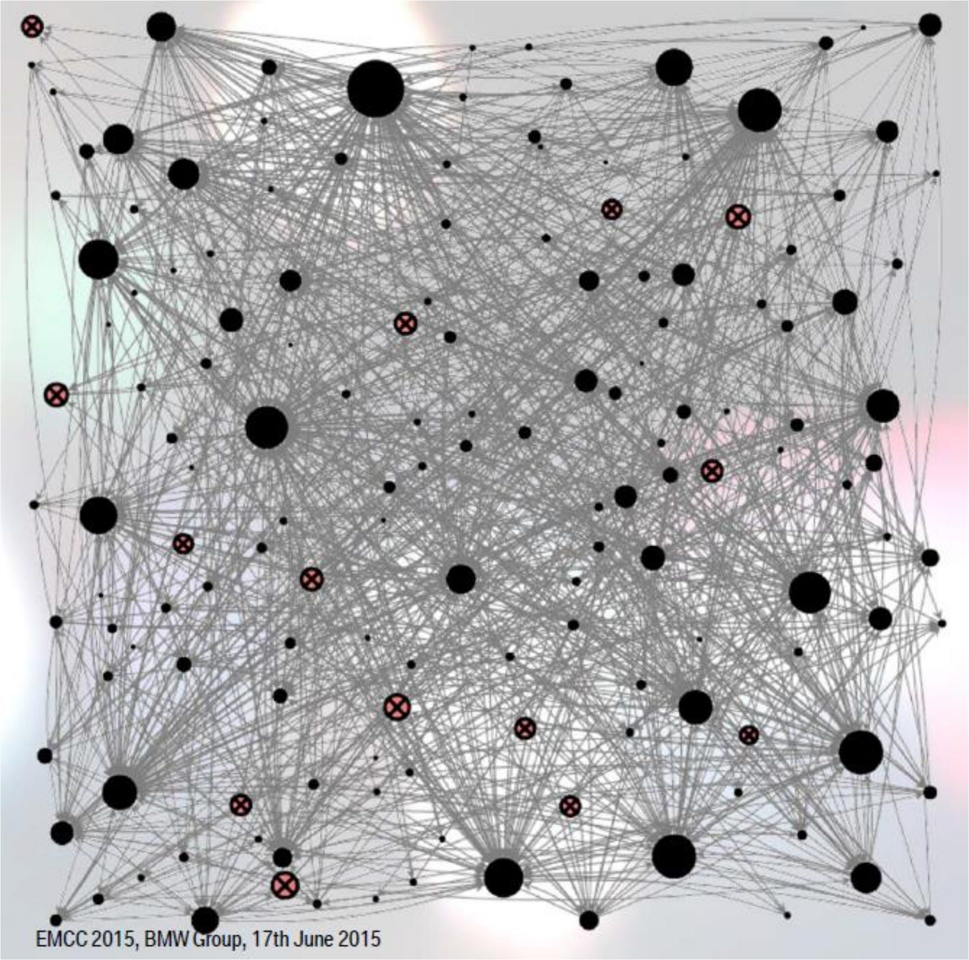
Complexity

Complexity - Callgraph of an Engine Control Unit



Simon Fürst, BMW, EMCC2015 Munich

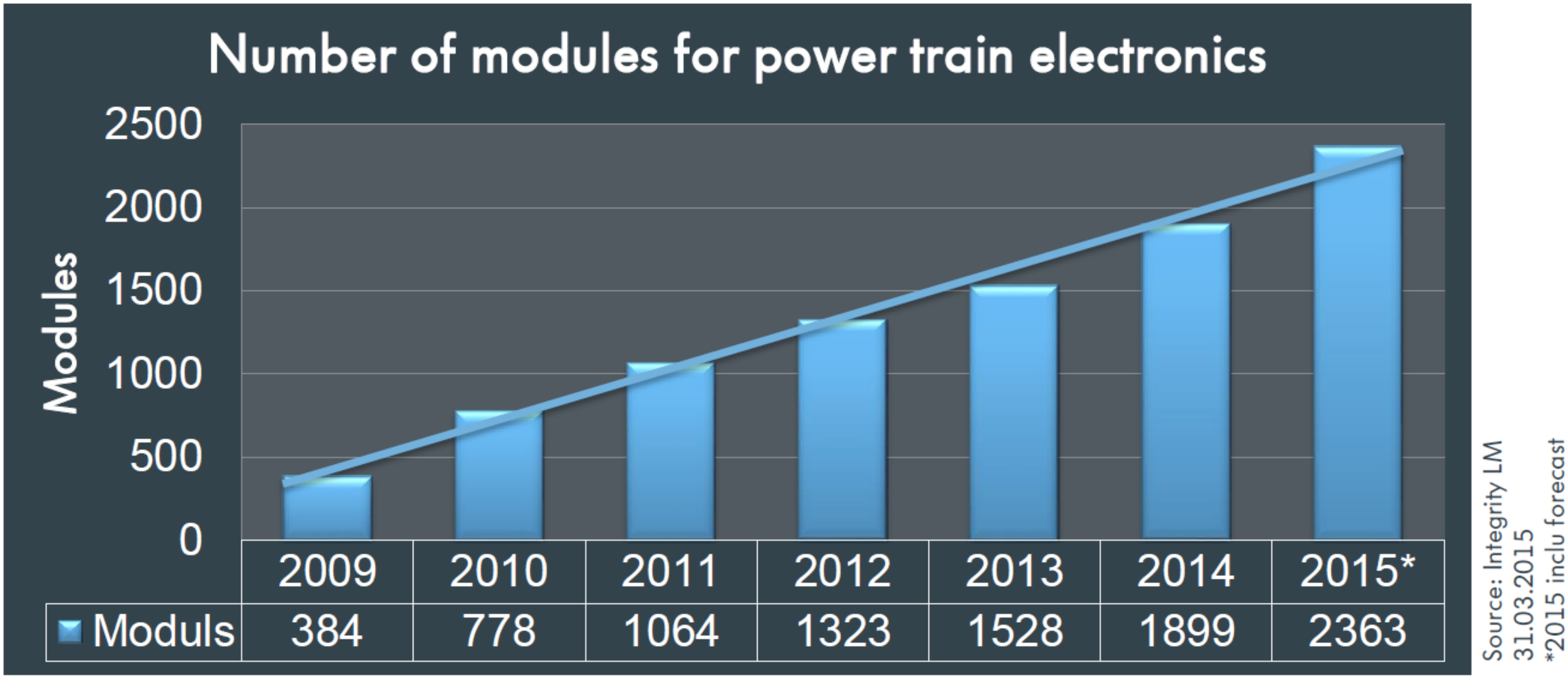
Complexity - Callgraph of an integration platform



Simon Fürst, BMW, EMCC2015 Munich

- 150 software components
- 14 of them are safety-relevant according to ASIL B
- Over 1000 assembly connectors
- Multiple n:m edges between SWCs

Rising amount of OEM application software at Volkswagen



	2009	2010	2011	2012	2013	2014	2015*
Moduls	384	778	1064	1323	1528	1899	2363

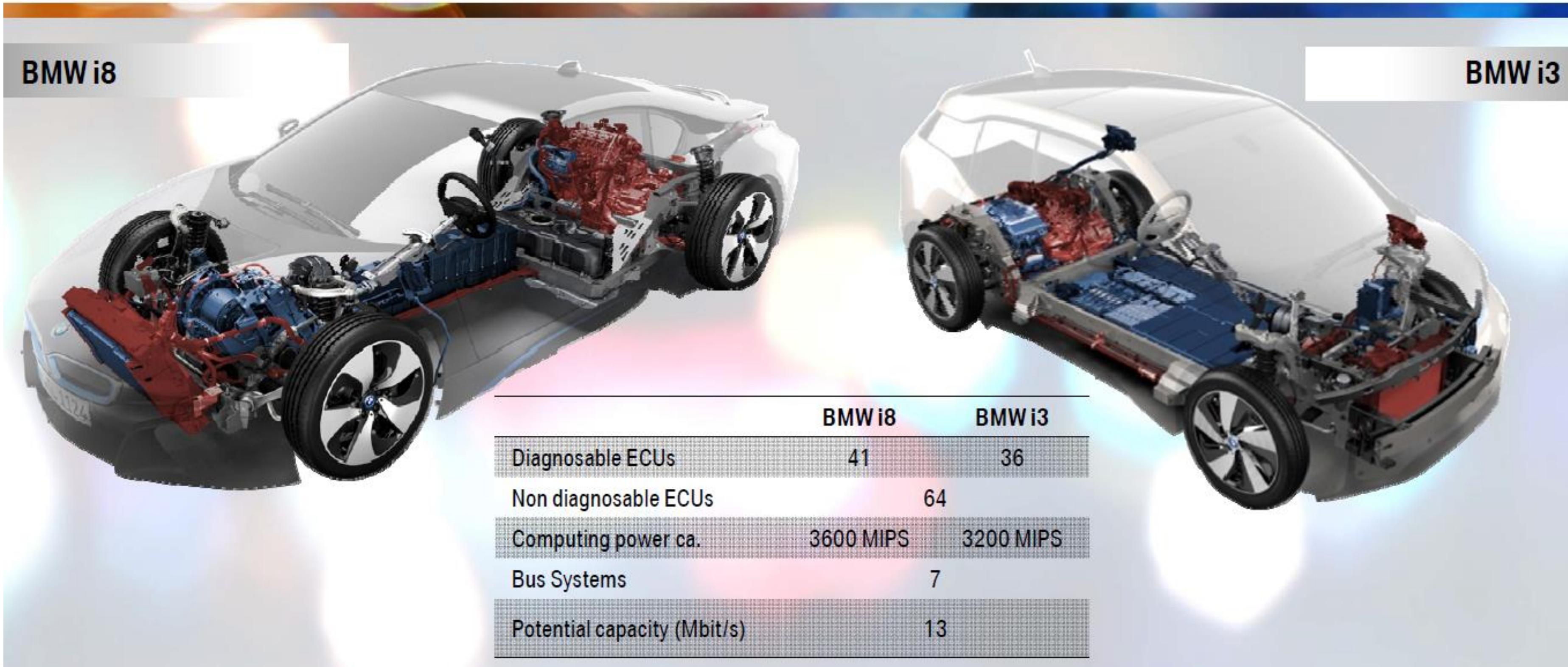
T. Flämig, Volkswagen, EMCC2015 Munich

Standardized software architectures necessary.

AUTOSAR is the first step to handle this complexity.

Computing Power

BMW i8 and i3 – Figures and Facts

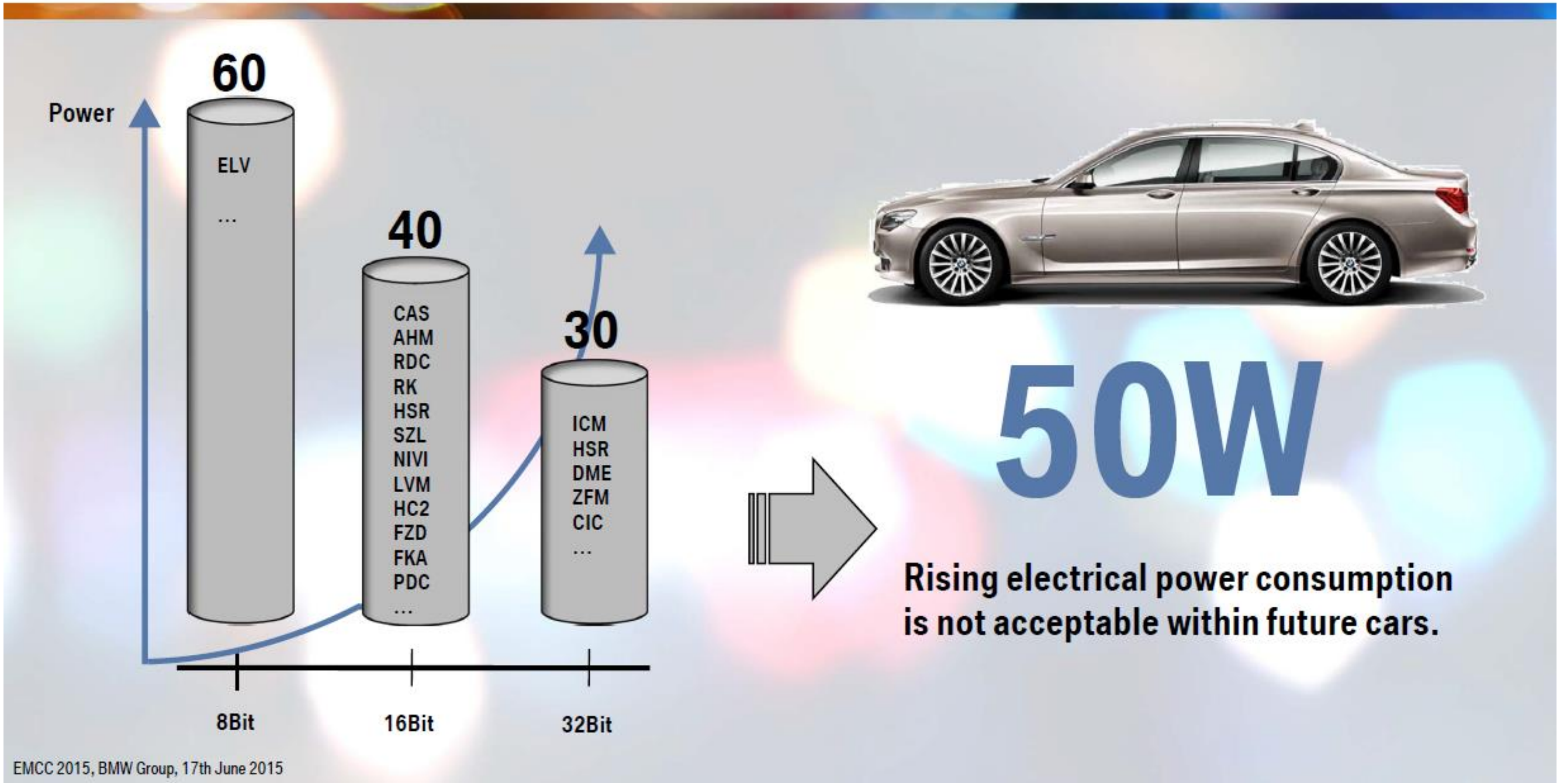


	BMW i8	BMW i3
Diagnosable ECUs	41	36
Non diagnosable ECUs	64	
Computing power ca.	3600 MIPS	3200 MIPS
Bus Systems	7	
Potential capacity (Mbit/s)	13	

Simon Fürst, BMW, EMCC2015 Munich

Already large number of ECUs
Where to get the computing power for ADAS?

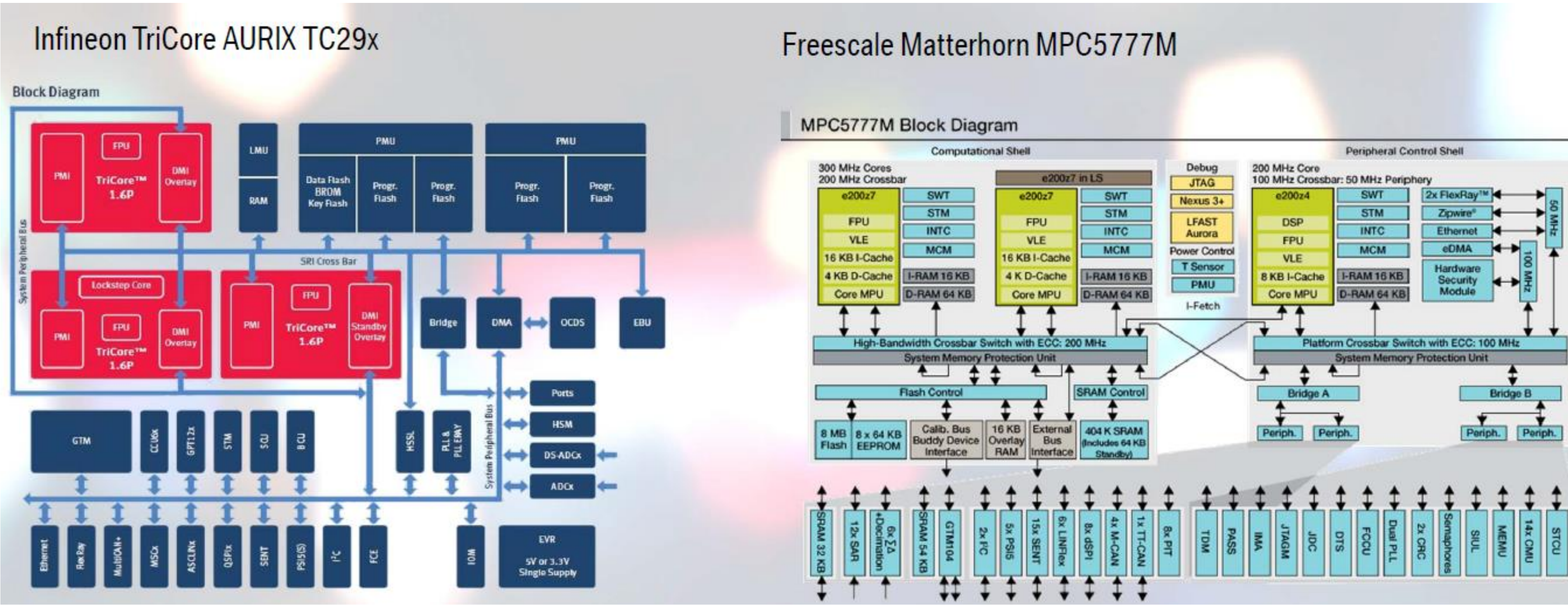
Power Consumption within BMW cars



Simon Fürst, BMW, EMCC2015 Munich

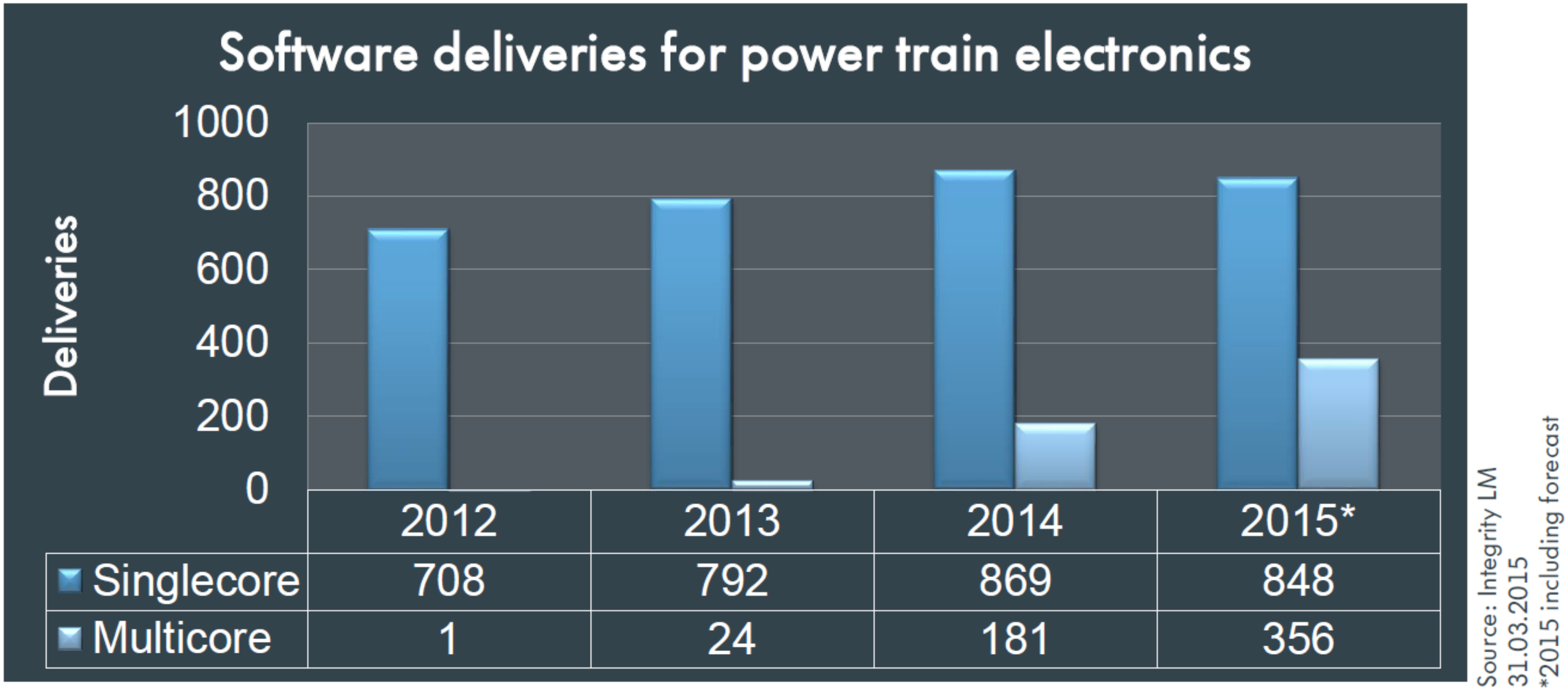
Max. power consumption limits the number of ECUs

Automotive Multicore Microcontroller



Simon Fürst, BMW, EMCC2015 Munich

Rising Quota of Multicore deliveries at Volkswagen



T. Flämig, Volkswagen, EMCC2015 Munich

Multicore usage ramps up (e.g. Powertrain).

ADAS will speed this up.

Next level of Functional Safety

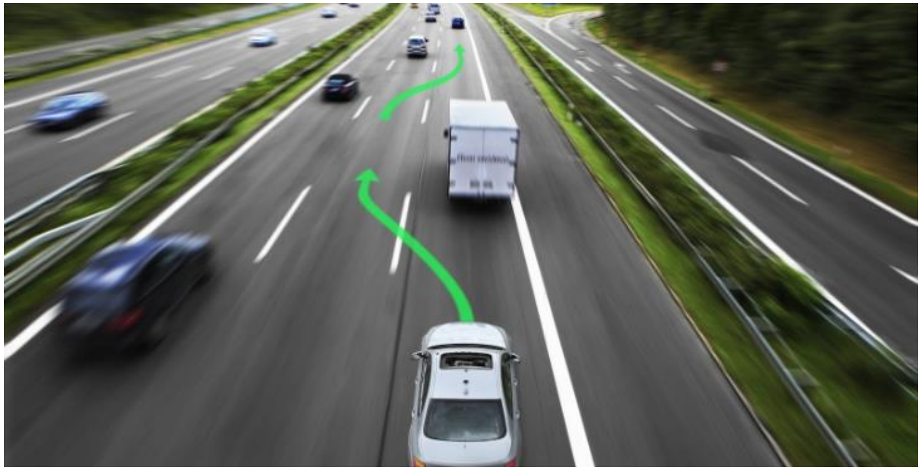
„Definition“ of a safe system

There is a very basic and helpful definition for a safe system:

“You know what the system does”

Current Systems (usually fail-safe)

Failure Detected?



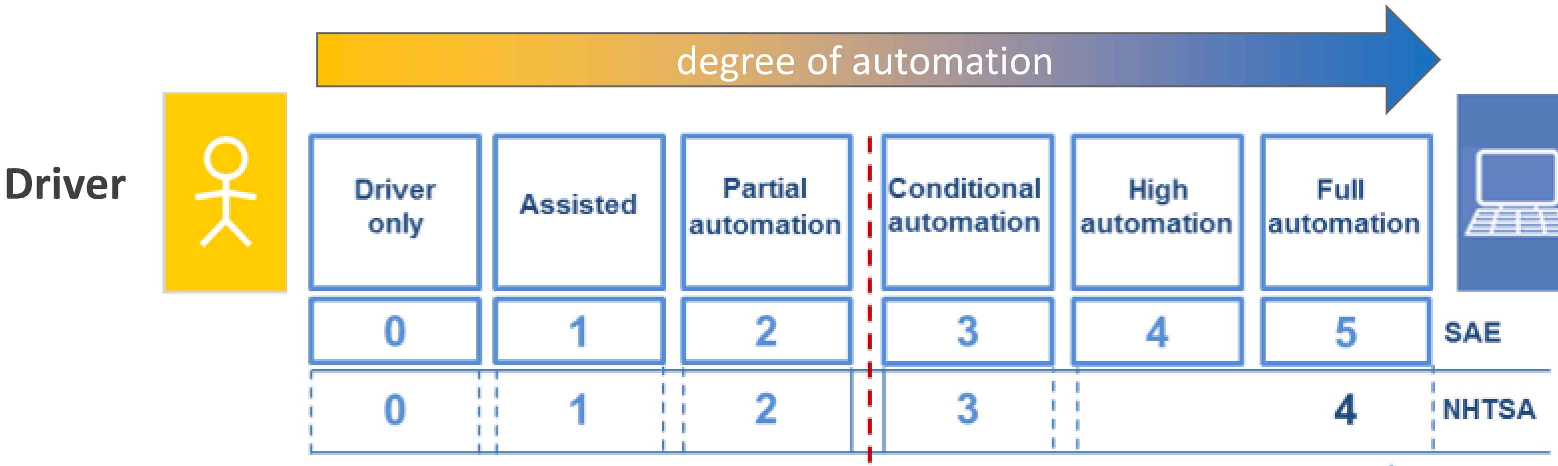
- Deactivate / degrade function
  → Safe State
- Inform the driver
- Report a diagnostic error

Standard approach in many safety relevant systems:
- Airbag, ESP, air conditioning, battery charging, …
- Driver assistant functions such as adaptive cruise control, lane assist, …

Some functions provide a degraded mode, sometimes limited in time:
- Electronic Power Steering
- Braking

Wolfgang Schäfer, Continental, May 19, 2015

Levels of Autonomous Driving (AD)



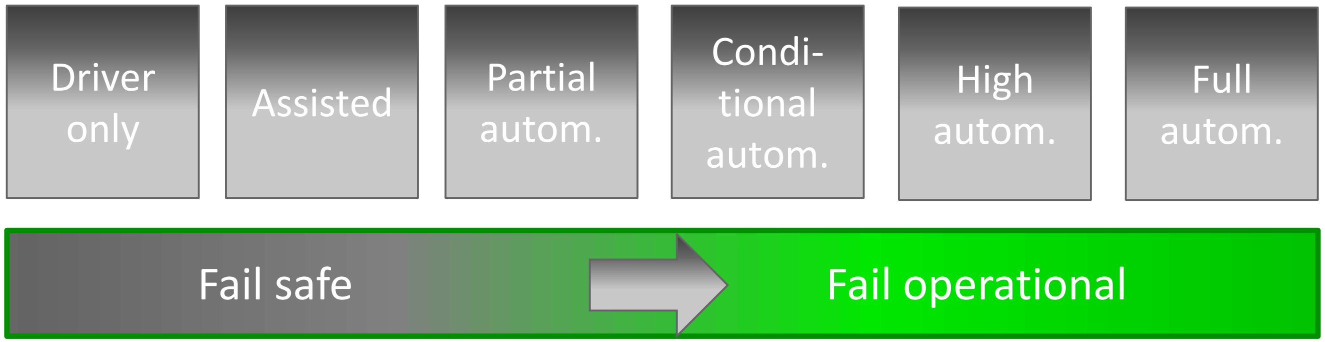
driver in the loop	yes (required)			not required		
time to take control back	-	~ 1s		several seconds	couple of minutes	
other activities while driving	not allowed			specific	all (even sleeping)	
examples	FCW, LDW	ACC, LKA	Traffic Jam Assistant	Highway Chauffeur	Valet Parking	Robot car

FCW … Forward Collosion Warning
LDW … Lane Departure Warning

ACC … Adaptive Cruise Control
LKA … Lane Keeping Assistant

Source: SAE, NHTSA, VDA

Goal: Autonomous driving



Safe State means:

- Continue driving until driver is in the loop
  - approx. 7-15s for conditional autonomous driving
  - Several minutes for high and full autonomous driving
- Perform an autonomous „safe-stop“ (stand-still at a non-hazardous place)
  - Main issue is to get the driver attention focused on the situation
  - Several minutes, depending on the situation

Agenda

Short overview of Elektrobit automotive

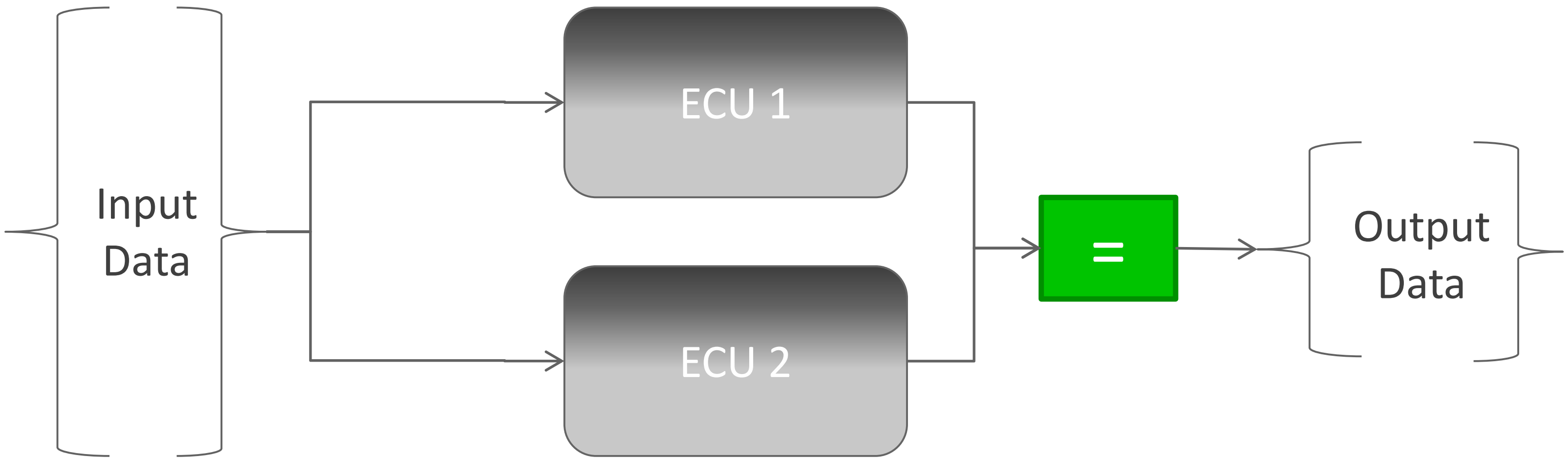
The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture

Approach: 2 channels with comparison

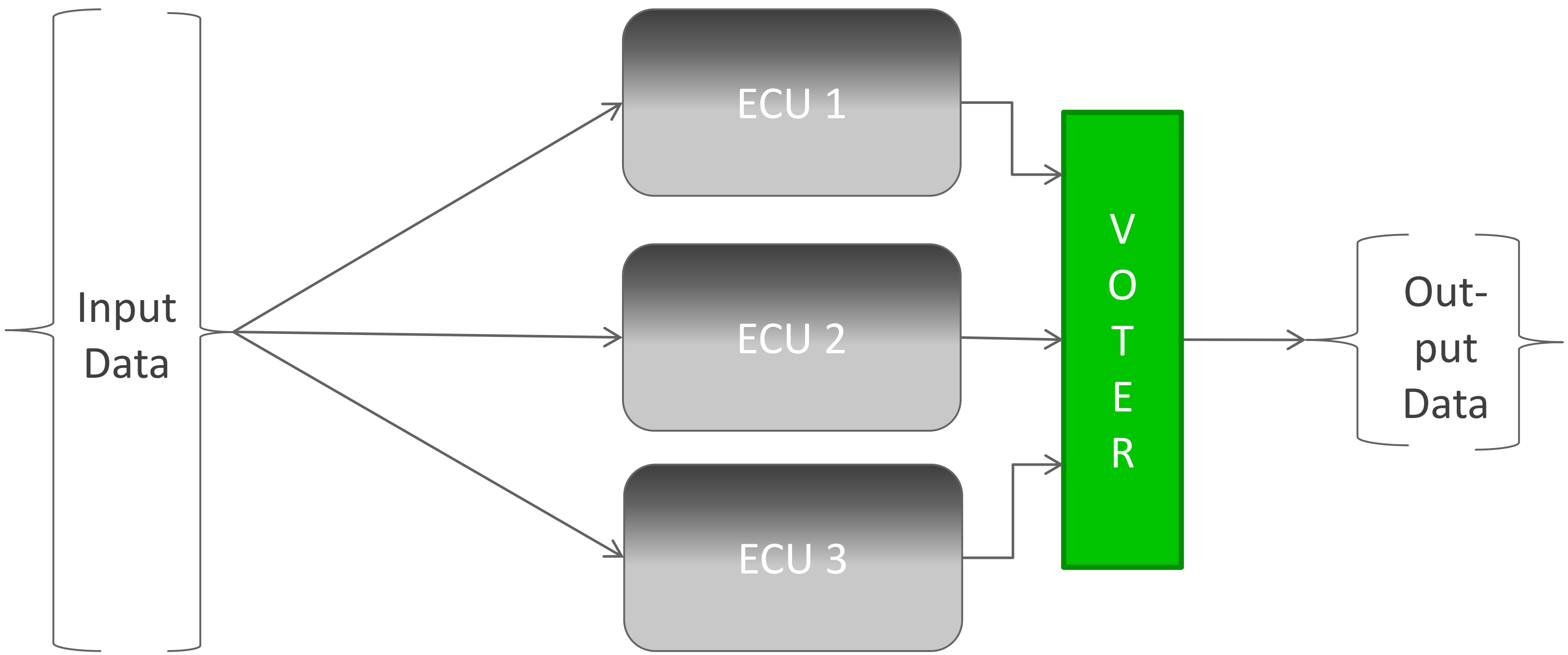


Two ECUs working on the input data, outputs are compared

A 2 channels with comparison system is simply fail-safe and since you cannot distinguish between “ECU1 not ok” and “ECU2 not ok”.

The safe state is a complete system shutdown.

Approach: 2oo3 Systems



If one of the ECUs fails the system can continue with the remaining two ECUs.

Failures in the input data can be detected by an “Input-Voter”.

This pattern is well established.

2oo3 Systems and automotive

Applicable for automotive?

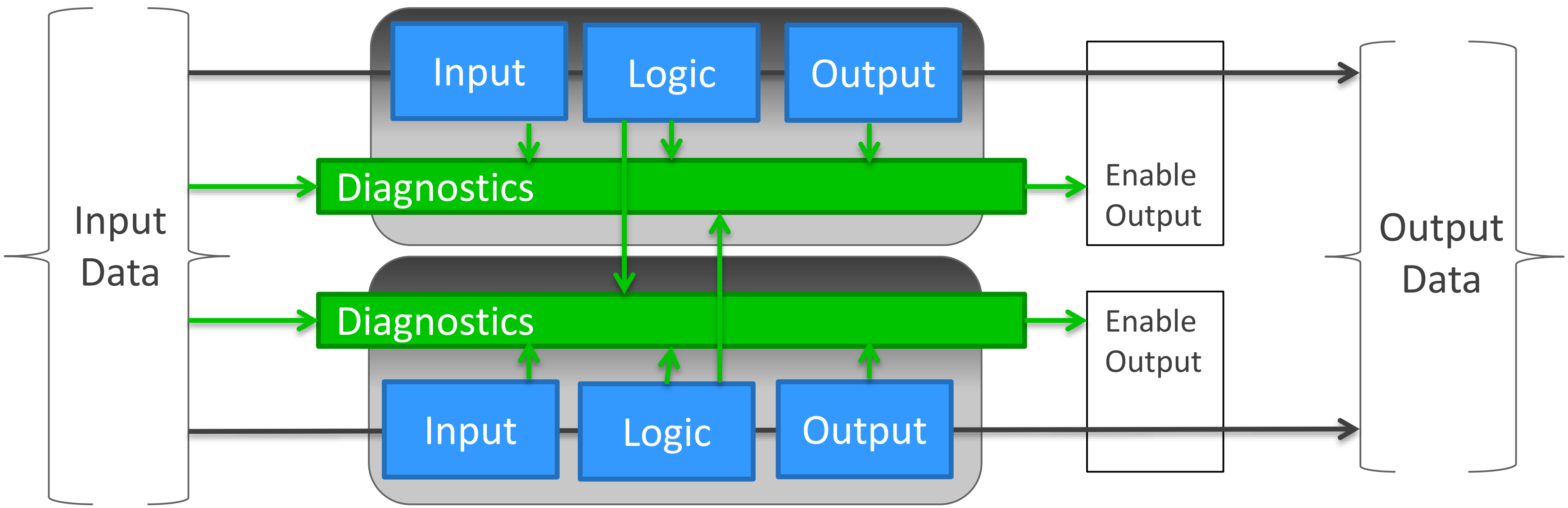
- More ECUs
- More wiring
- More weight
- More power consumption
- Higher complexity to manage

Will we as a customer accept that?

- Different opinions and market studies
- Referring to several studies, customer will pay 1500 - 3000€ more for autonomous driving car (mid-size car).

Source: KPMG(2013), autelligence (2015)

Approach: 1oo2D System



- High diagnostic coverage needed to detect failures in one channel
- IF component fails in one of the two channels, the system does not shut down but continues to operate with one channel

Common sense:

The best policy is not to operate on a single channel, or not for a long period of time.

→ See above: only some seconds may be needed.

Diagnostics in software in autonomous driving systems

Integrity mechanism

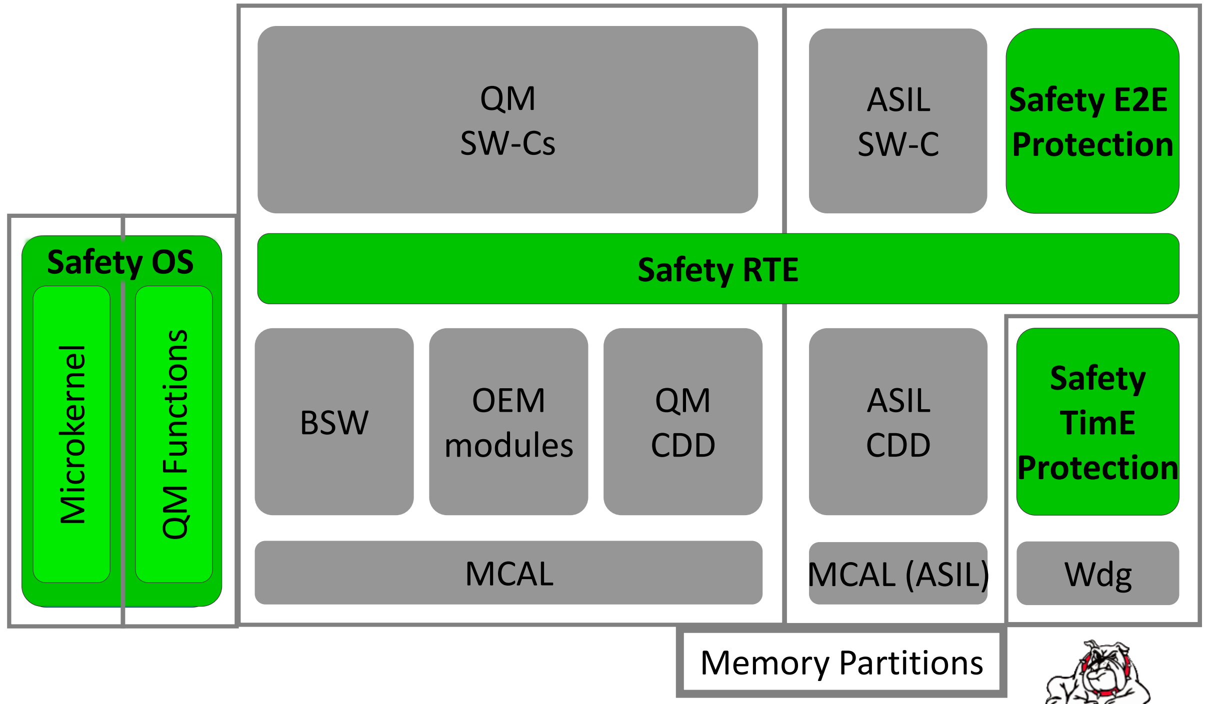
- Memory Partitioning
- Temporal Monitoring
- Data protection

Infrastructure

- Fault tolerant Ethernet
- Service Orientated communication

Software Engineering

- Plausibility checks
- Functional monitoring
- Defensive programming
- Dynamic analysis



Safety OS

- Data Protection
- Stack Protection
- Context Protection
- OS Protection
- Hardware Error management

Safety E2E Protection

- Safe communication

Safety TimE Protection

- Alive supervision
- Deadline Monitoring
- Control flow monitoring

Outlook: Reconfiguration for rebuilding 1oo2D

1oo2D

- Normal operation

1 channel

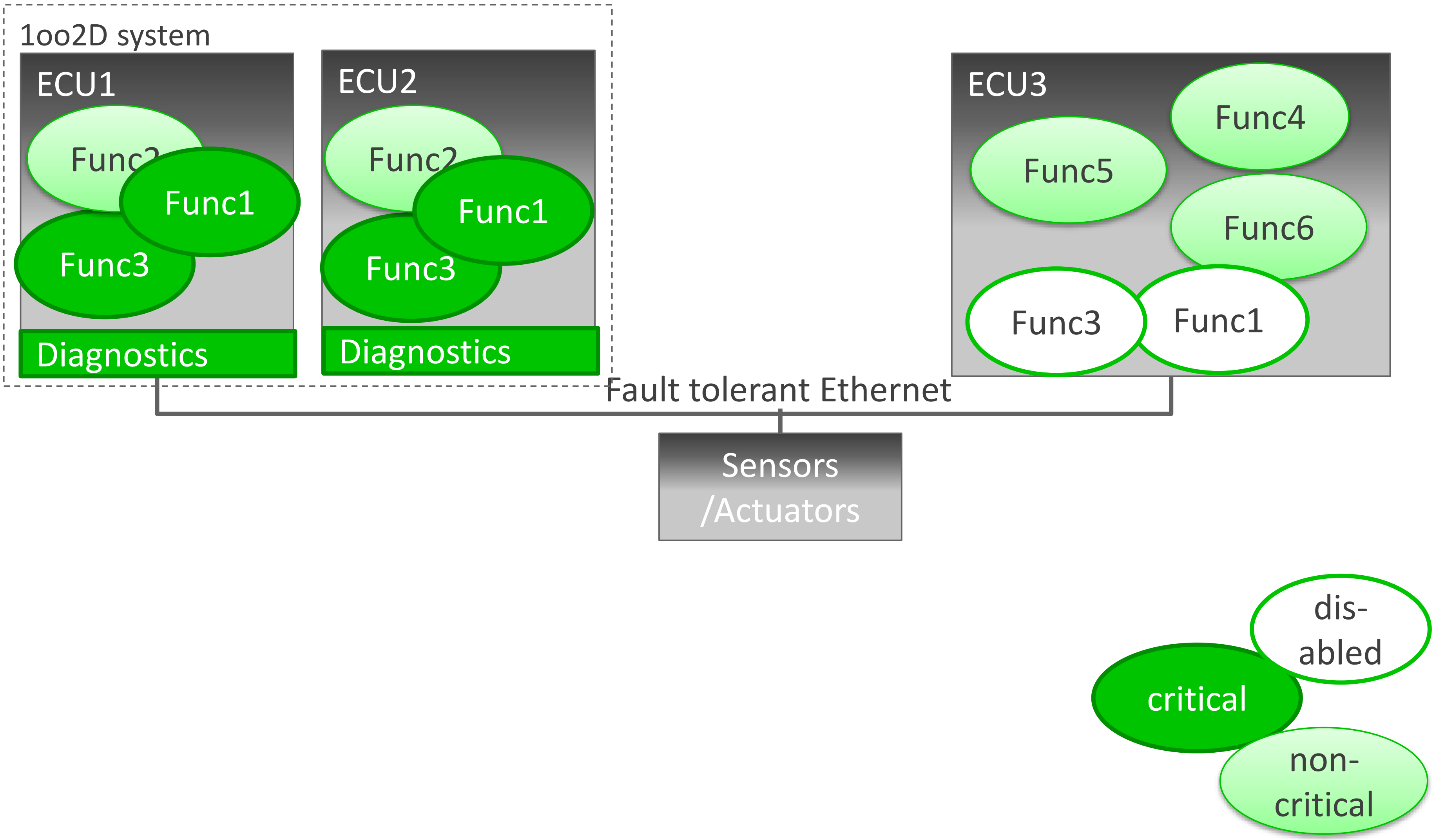
- Still Operational
- Handover to driver
- Failure recovery
- Internal recovery

1oo2D*

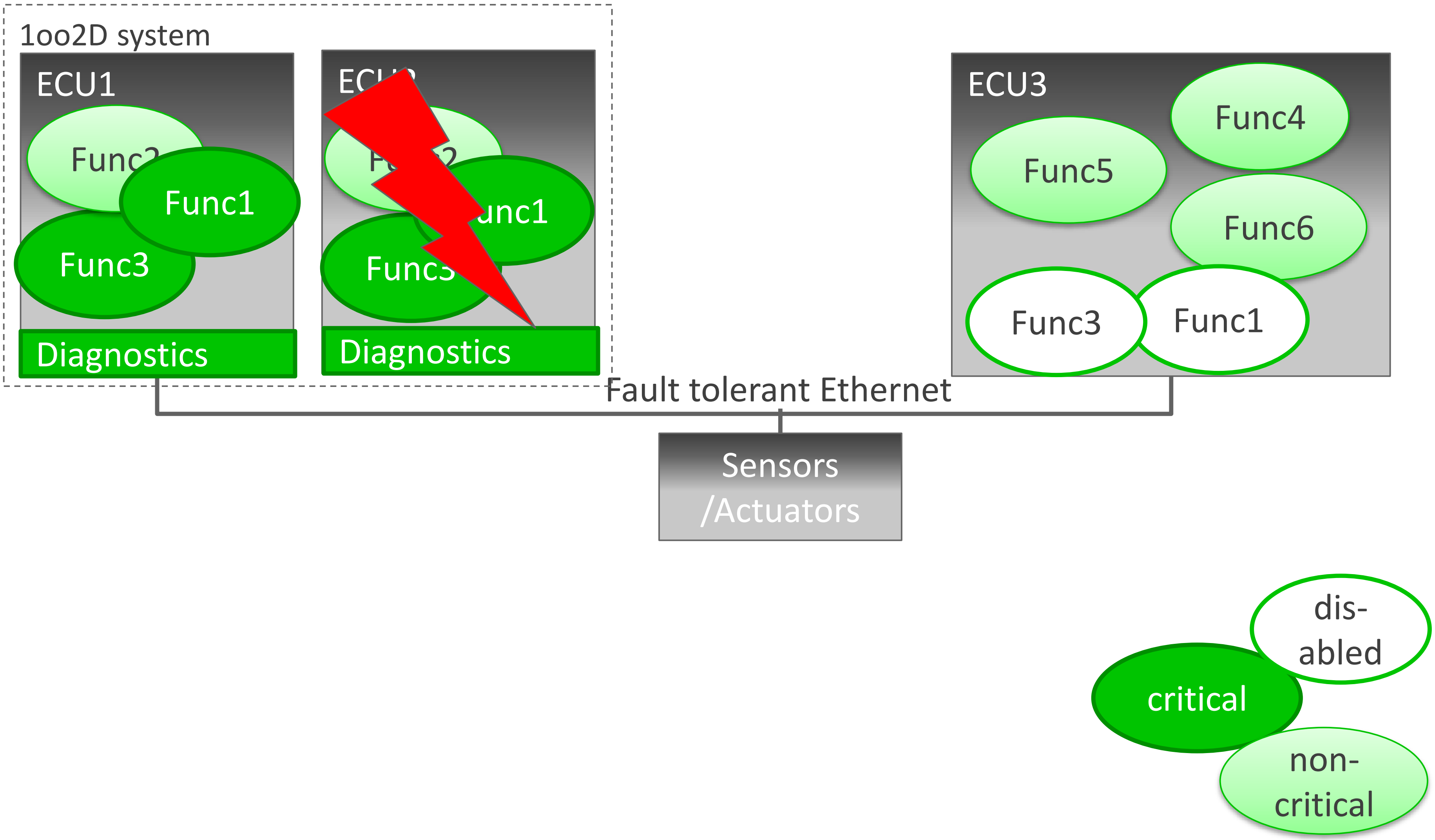
- Rebuilding 2 channel system
- Disabling of comfort functions

< 10s

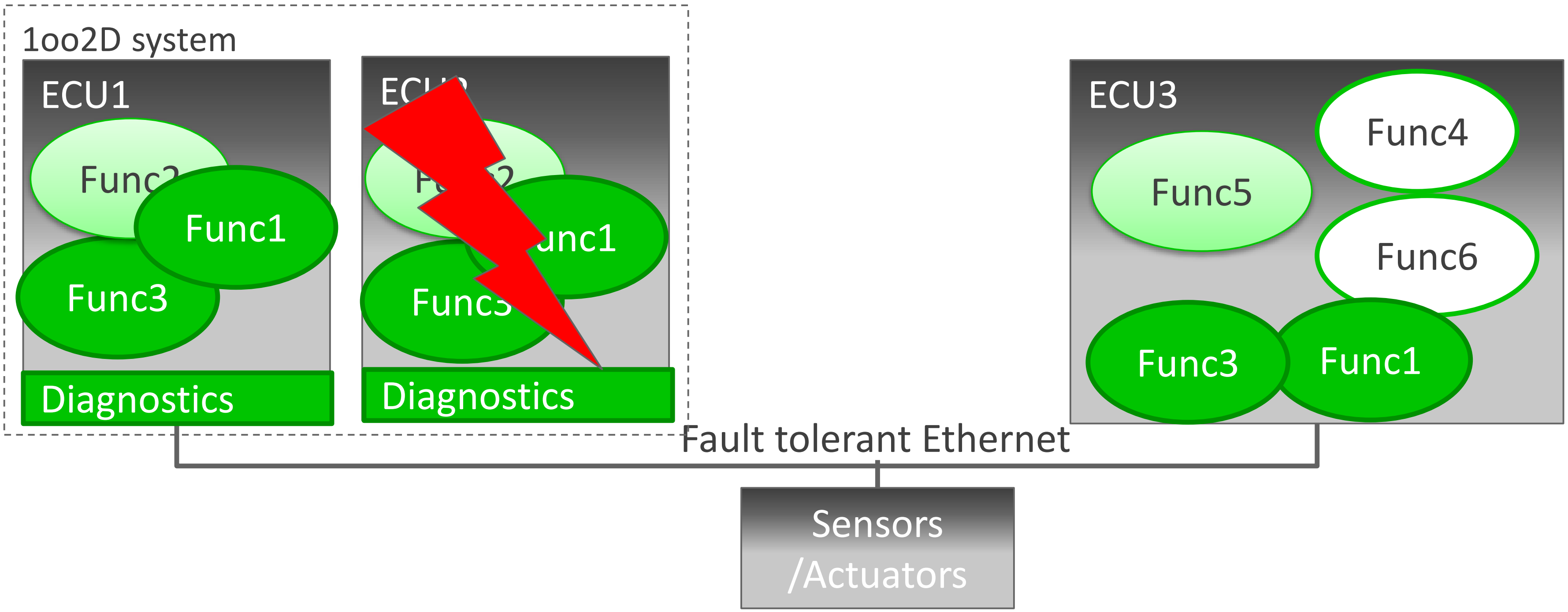
1oo2D - Normal operation



1oo2D – 1 channel

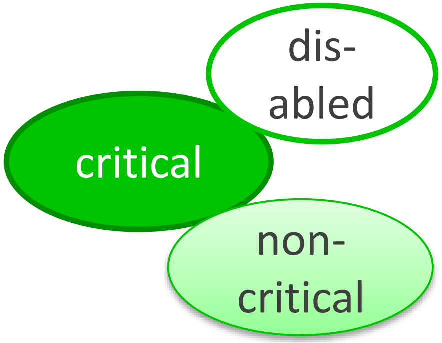


1oo2D*



Requirements for Reconfiguration

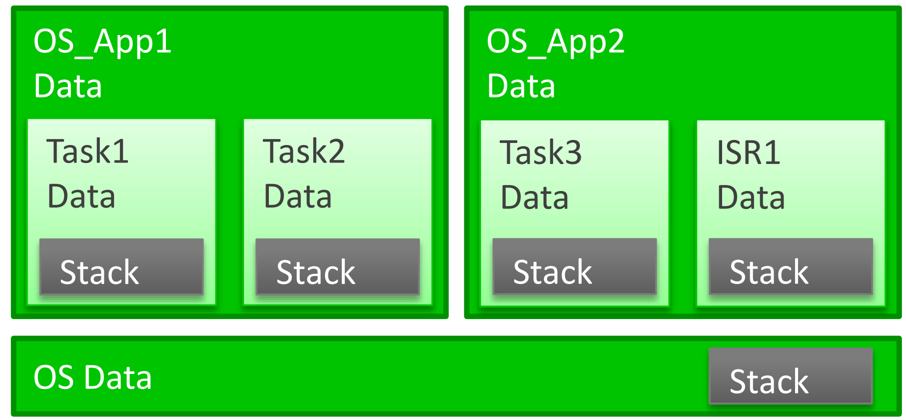
- Req. 1: Functions can be dynamically relocated
- Req. 2: Sensor/Actuators are redundant or accessible via network



Dynamic Reconfiguration

Req. 1: Functions can be dynamically relocated

- Application information based on AUTOSAR xml description available
- Runtime environment (RTE) supporting reconfigurable software components
- Threads can started/stopped in EB tresos Safety OS



Req. 2: Sensor/Actuators are redundant or accessible via network

- Service orientated communication
- Multi-cast fault-tolerant Ethernet

Agenda

Short overview of Elektrobit automotive

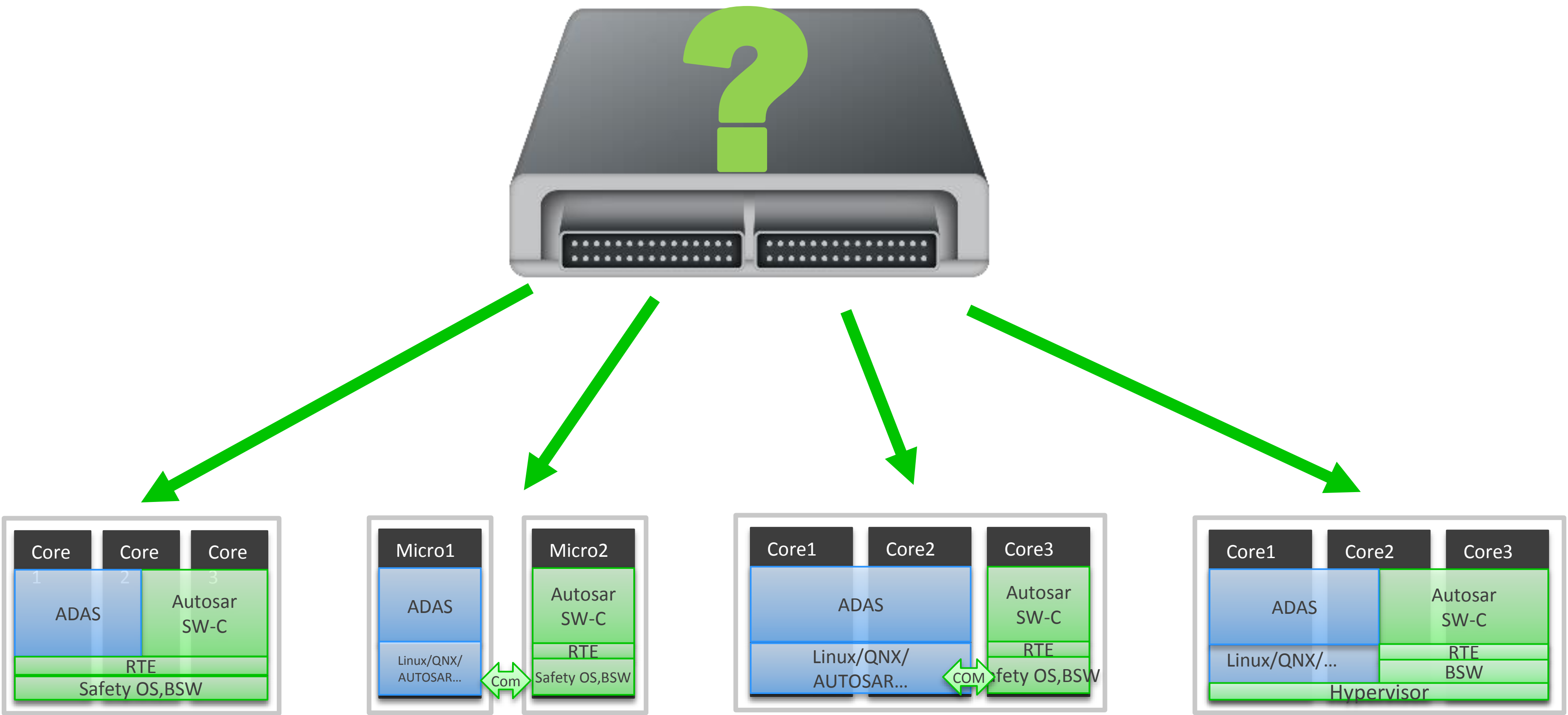
The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture

Overview of different architecture approaches



Full AUTOSAR

Microcontroller Partitioning

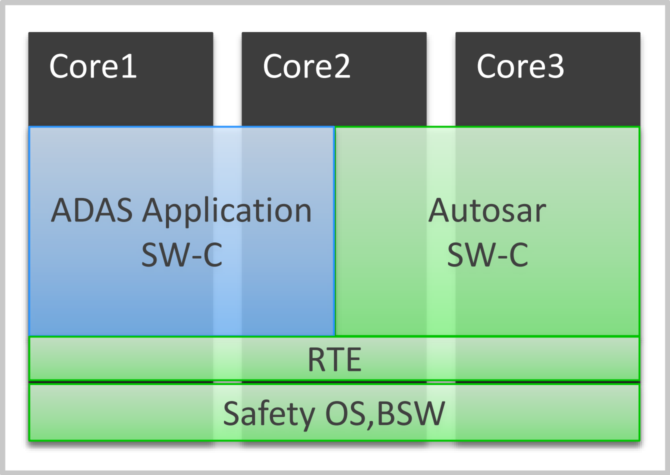
Core Partitioning

Hypervisor

Elektrobit

Full AUTOSAR architecture

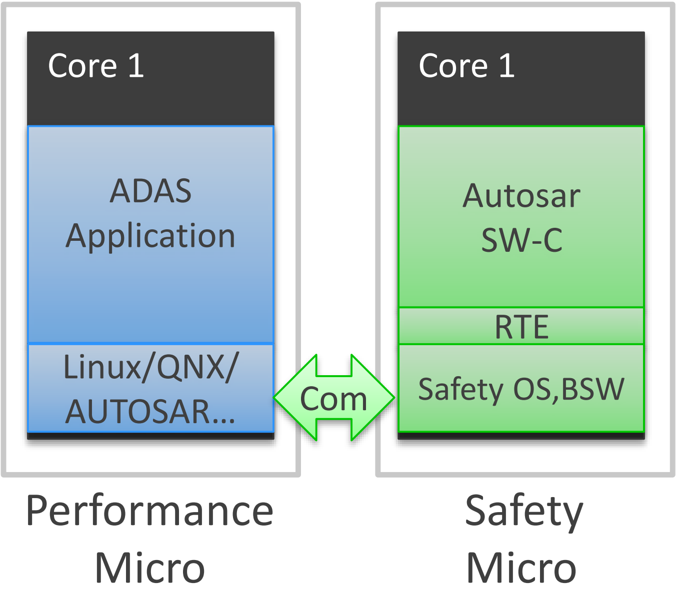
- Safety Microcontroller
- AUTOSAR Multi-Core Safety OS
- ADAS algorithms as SWC
- Advanced hardware drivers integration as Complex Device Drivers
  - e.g. OpenCL, AVB
  - Proprietary video bus systems



Pro	Con
Easy integration into OEM/T1 AUTOSAR process	Advanced hardware support needs AUTOSAR complex device drivers
One System	High Performance Safety Microcontoller necessary

Microcontroller partitioning architecture

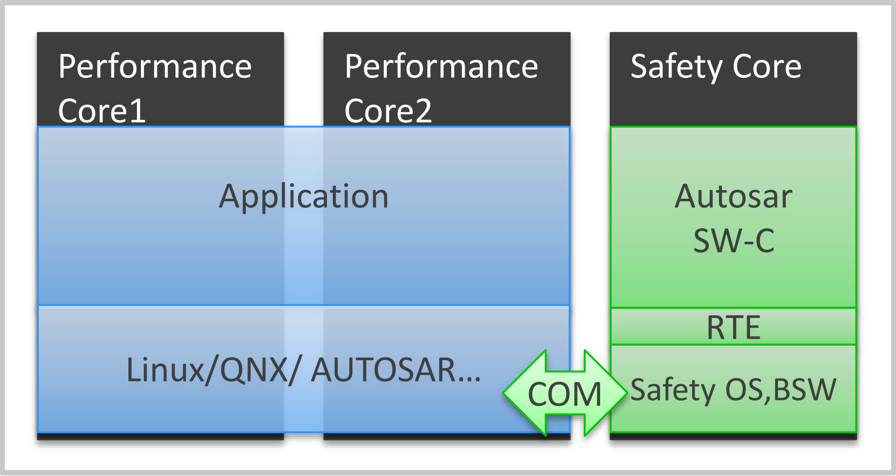
- Partitioning in Safety and Performance Microcontroller
- Separated applications treated as different ECUs during development
- Private Network for communication



Pro	Con
Scalable (combine two or more Microcontoller)	Additional hardware costs
Suitable Micocontroller already available	Need for private communication link
	Complex Flashloader and Startup

Core partitioning architecture

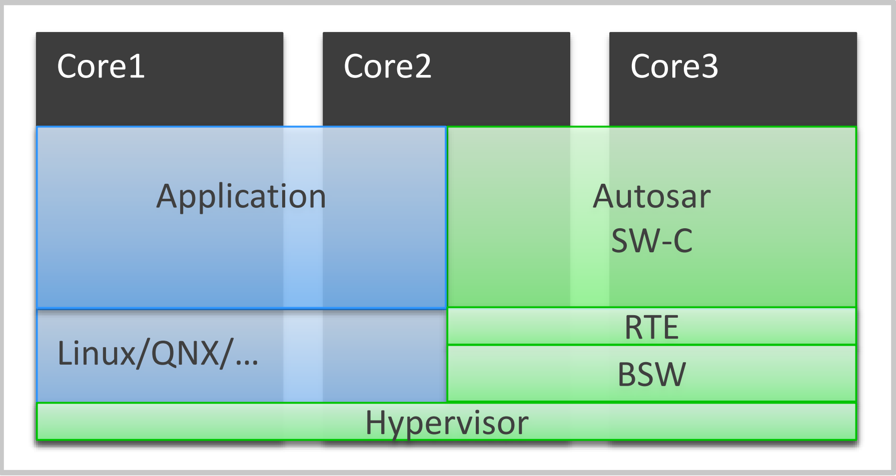
- One Microcontroller with several performance cores and one safety core (typically Lockstep)



Pro	Con
No need for private network hardware	No suitable Microcontroller available today
Performance and Safety in one Micro	

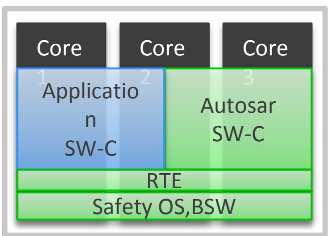
Hypervisor architecture

- Host OS with AUTOSAR guest system on one Microcontroller
- Hypervisor could be part of Guest OS



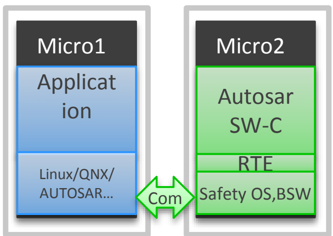
Pro	Con
Hypervisor as Gateway between different OS	Limited realtime capabilites
Hypervisor as Security Gateway between car and cloud	Limited Performance

Compare and contrast each architecture



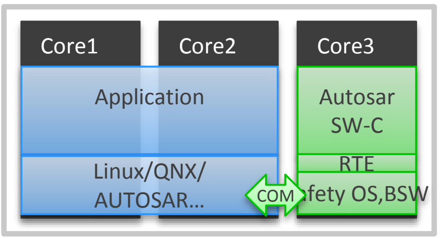
Full AUTOSAR

Safety or Performance



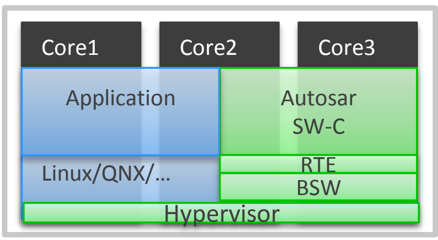
Microcontroller Partitioning

Safety & Performance



Core Partitioning

Safety & Performance optimized



Hypervisor

Security Architecture

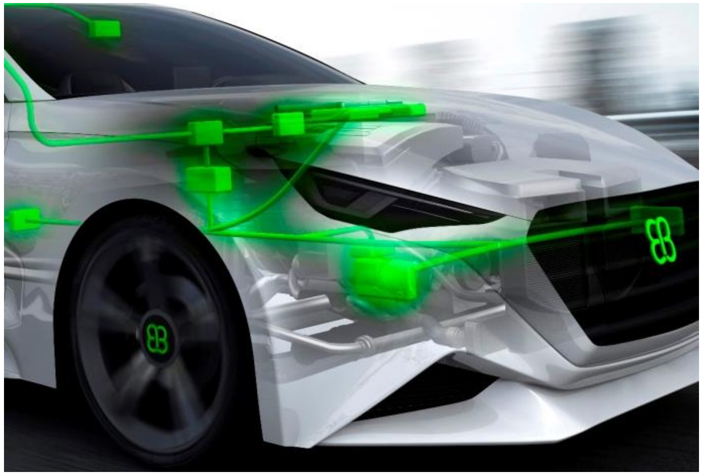
Software Architectures define next generation Microcontroller Architectures

AUTOSAR is part of each architecture as a common standard for

- **Basic Software, Safety and Security in ECUs**
- **Synchronized development process between OEM and T1**

Summary

- Re-use of available integrity mechanisms from fail-safe systems is the basis for building fail-operational systems.
- Software systems that are designed to achieve a high diagnostic coverage are available today
- Fault tolerant Automotive Ethernet is available today.
- Established concepts for fail-operational system are available and can be reused in automotive systems with cost constraints.



Let‘s build the next generation software systems for autonomous driving!

Elektrobit

automotive.elektrobit.com
Robert.Leibinger@elektrobit.com