RTSS 2011

AUTOSAR at the cutting edge of automotive technology

01 December 2011

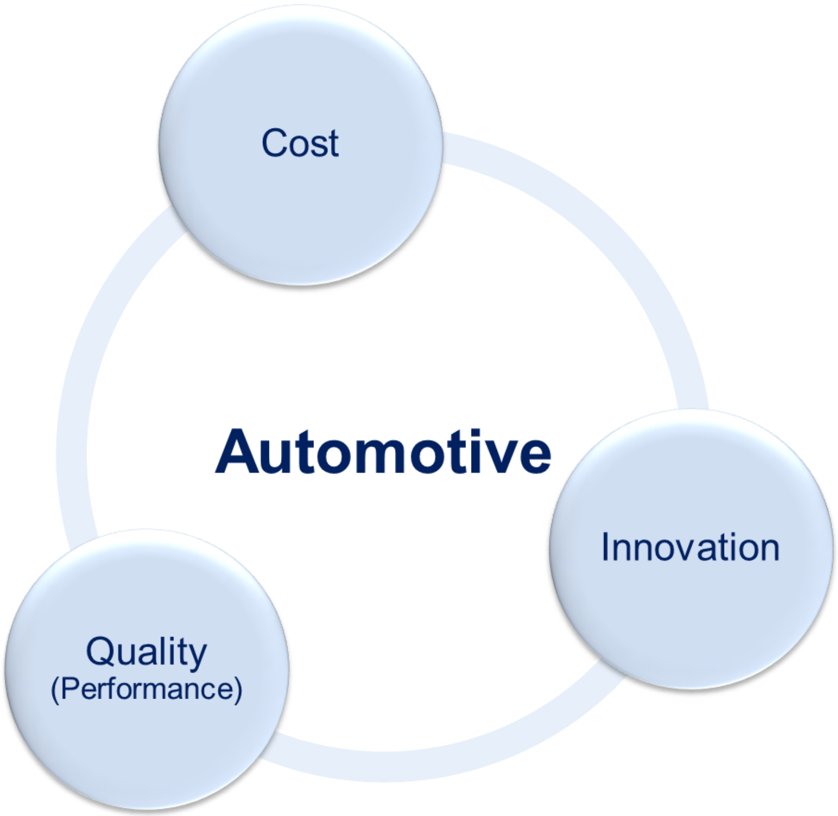
The 32nd IEEE Real-Time Systems Symposium (RTSS)

Dr. Bert Böddeker – DENSO AUTOMOTIVE Deutschland GmbH

Dr. Rafael Zalman - Infineon Technologies AG, Automotive Electronics

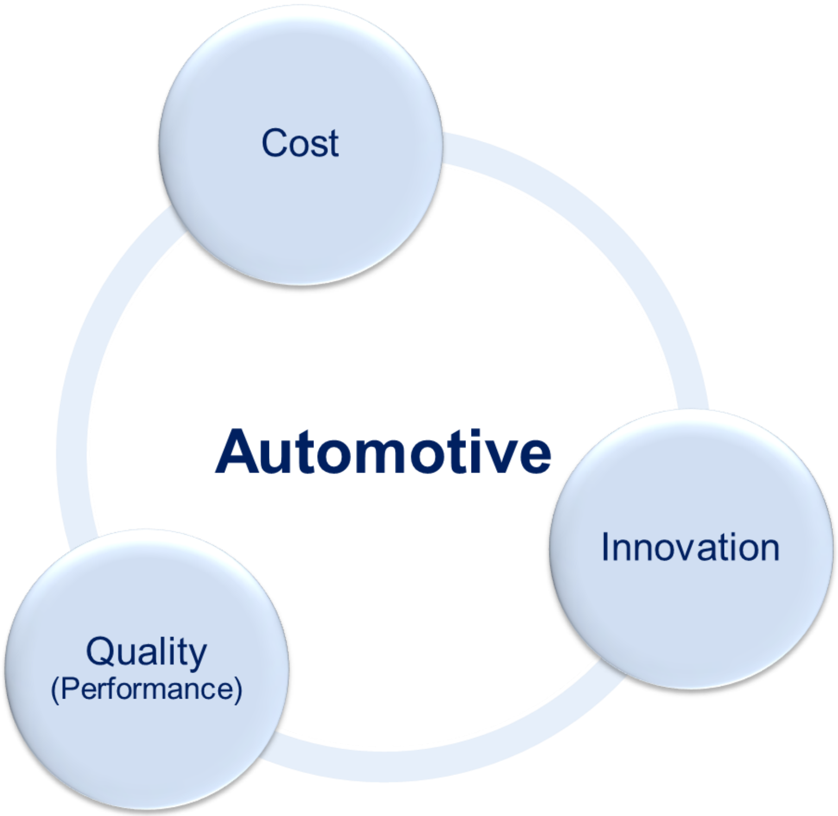
Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Content

- **Automotive Context**
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words

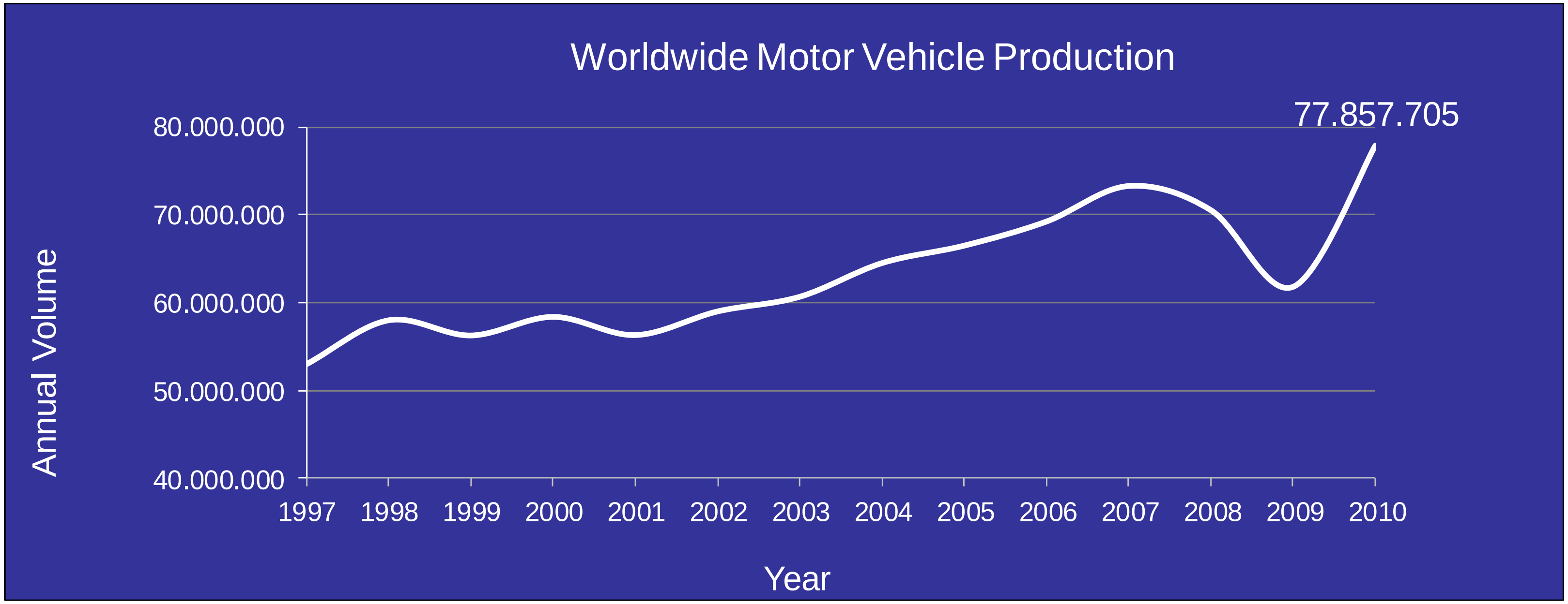


Automotive Context

Automotive Numbers

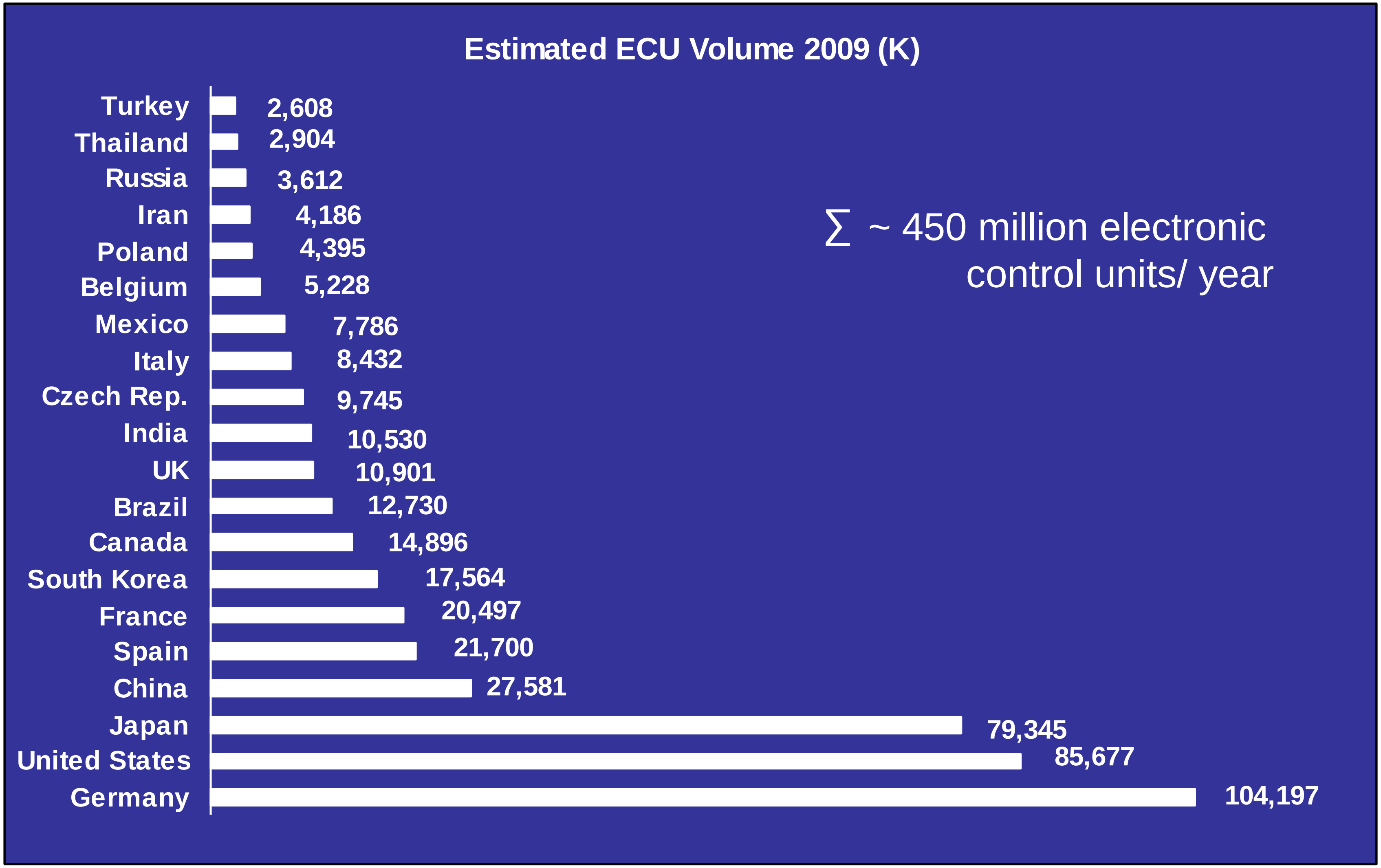
- Total estimated number of cars on the street worldwide ≈ 600 millions
- G7 countries have 749 vehicles / 1000 people
- Around 87% of total motor vehicles are passenger cars

- Car production worldwide:



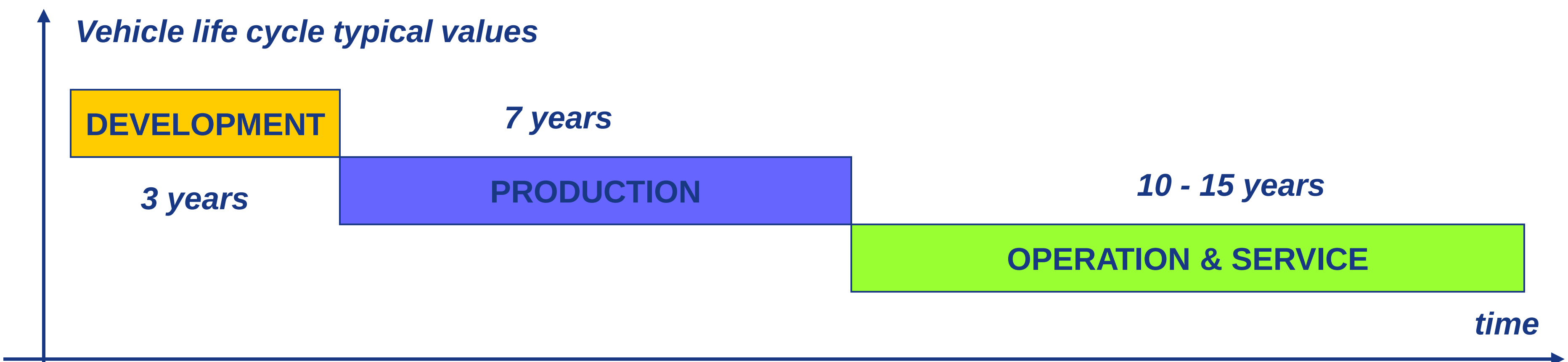
Source: OICA

Automotive Context



Lifecycles

- Vehicles have a long life cycle – state of the art = 25 years
- Electronic components have a dramatically shorter life cycle
- Impact on the SW architectures!
  - Standardization of SW architectures
  - HW independent specification of SW functions
  - Updates = SW life cycle is shorter than ECU life cycle
  - Robustness instead of fast innovation



Just orientation values – may differ for concrete examples

Automotive Context

Market

- Volume
- Places
- Players

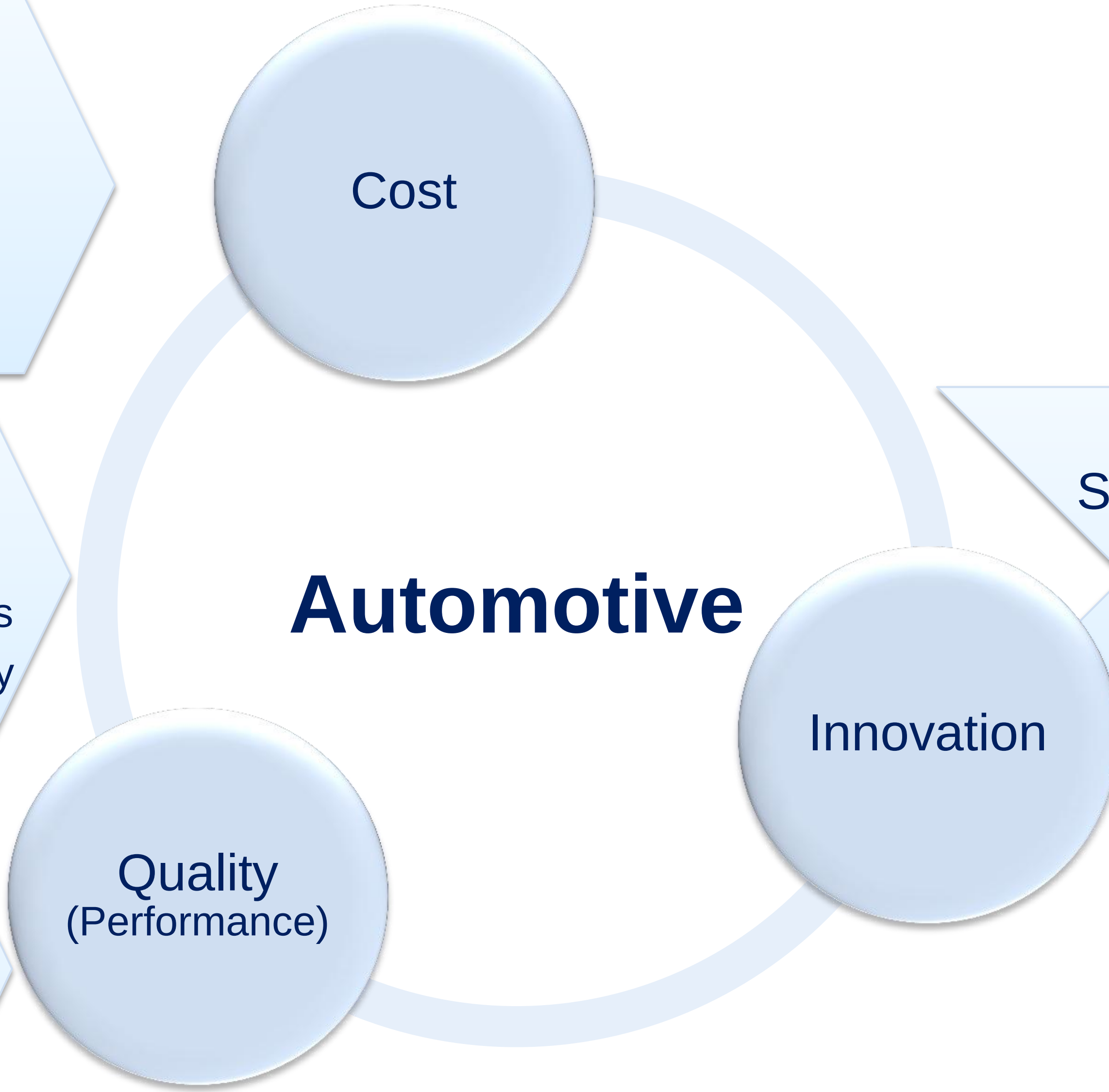
Society

Regulations

- Environment
  CO_2 regulations
- Function. safety
  ISO 26262

Technology

- Multi core
- Ethernet
- Software Product Lines
- …

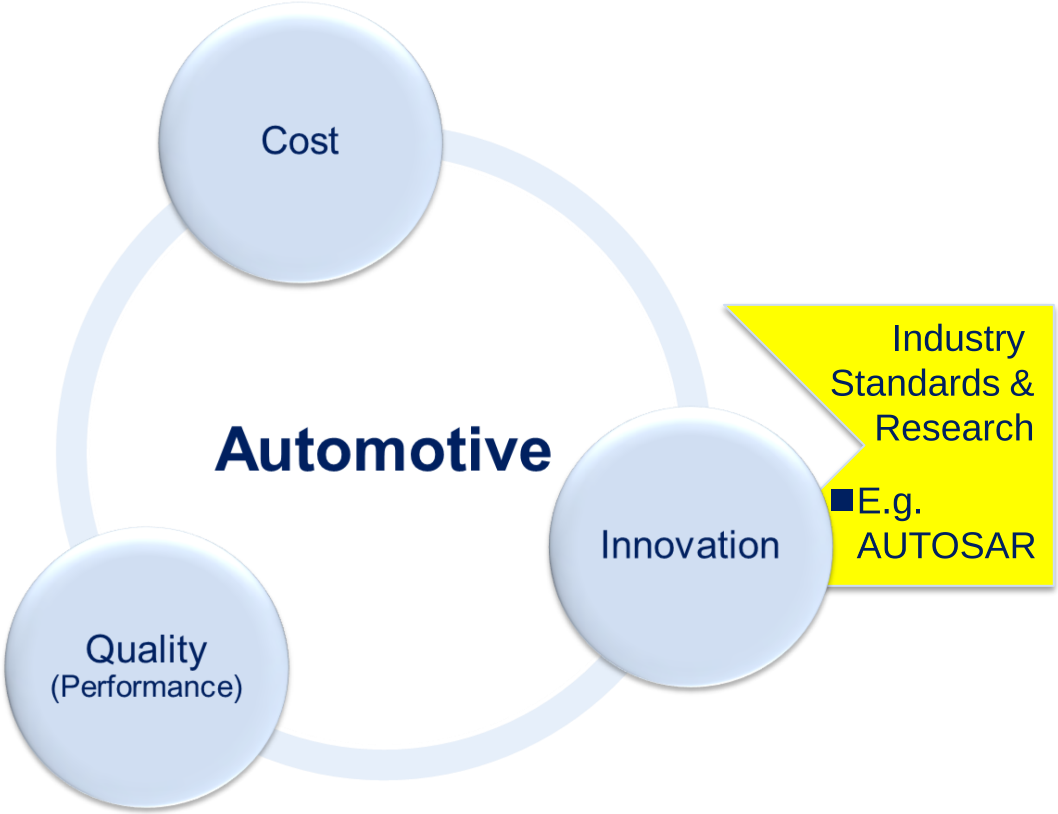


Industry Standards & Research

- E.g. AUTOSAR

Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



AUTOSAR Introduction

AUTOSAR

AUTomotive
Open
System
ARchitecture

Core Members

Bayerische Motoren Werke AG
Robert Bosch GmbH
Continental AG
Daimler AG
Ford Motor Company
General Motors Holding LLC
Peugeot Citroën Automobiles S.A.
Toyota Motor Corporation
Volkswagen AG

Premium Members

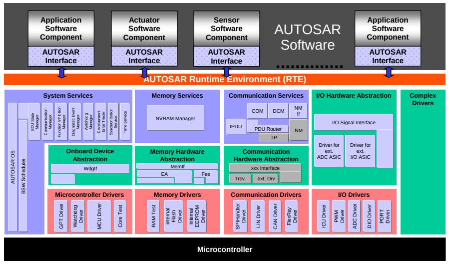
ALTRAN Group
Autoliv
B2i
CEA List
Dassault Systèmes
Delphi Corporation
Denso Corporation
dSpace GmbH
Elektrobit Group Plc
ETAS Entwicklungs- und Applikationswerkzeuge für elektronische Systeme GmbH
Electronics and Telecommunication Research Institute(ETRI)
Fiat Auto S.p.A.
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Freescale Semiconducters
Hella KGaA Hueck & Co.
Honda Motor Co., Ltd. & Honda R&D Co., Ltd.
Hyundai Motor Company
IAV
IBM Corporation
INCHRON GmbH
Infineon Technologies AG
Intecs - Informatica e Tecnologia del Software SpA
Johnson Controls GmbH
JTEKT CORPORATION
KPIT Cummins Infosystems Limited
M/S Larson & Toubro Limited
Lear Corporation
Magna International Inc.
Magneti Marelli Holding S.p.A
Mazda Motor Corporation
MB-Technology GmbH
Mentor Graphics Corporation
NXP B.V.
Patni Computer Systems Ltd.
Dr. Ing. h.c. F. Porsche AG
Renault SaS
Renesas Electronics Corporation
Saab Automobile AB
See4sys
STMicroelectronics NV
TATA Elxsi Limited
The MathWorks, Inc.
TRW Automotive Inc.
TTTech Computertechnik AG
Valeo Electronique et Systèmes de Liaison - VESL
Vector Informatik GmbH
Volvo Cars
AB Volvo
ZF Friedrichshafen AG

AUTOSAR Introduction

AUTOSAR Standardization areas

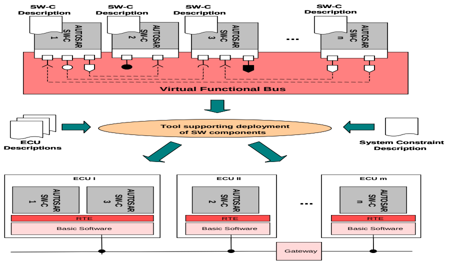
Software & Architecture

- Automotive Basic Software
- Run Time Environment (RTE)



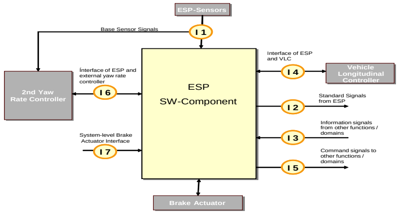
Methodology

- Virtual Function Bus (VFB)
- Configuration Language



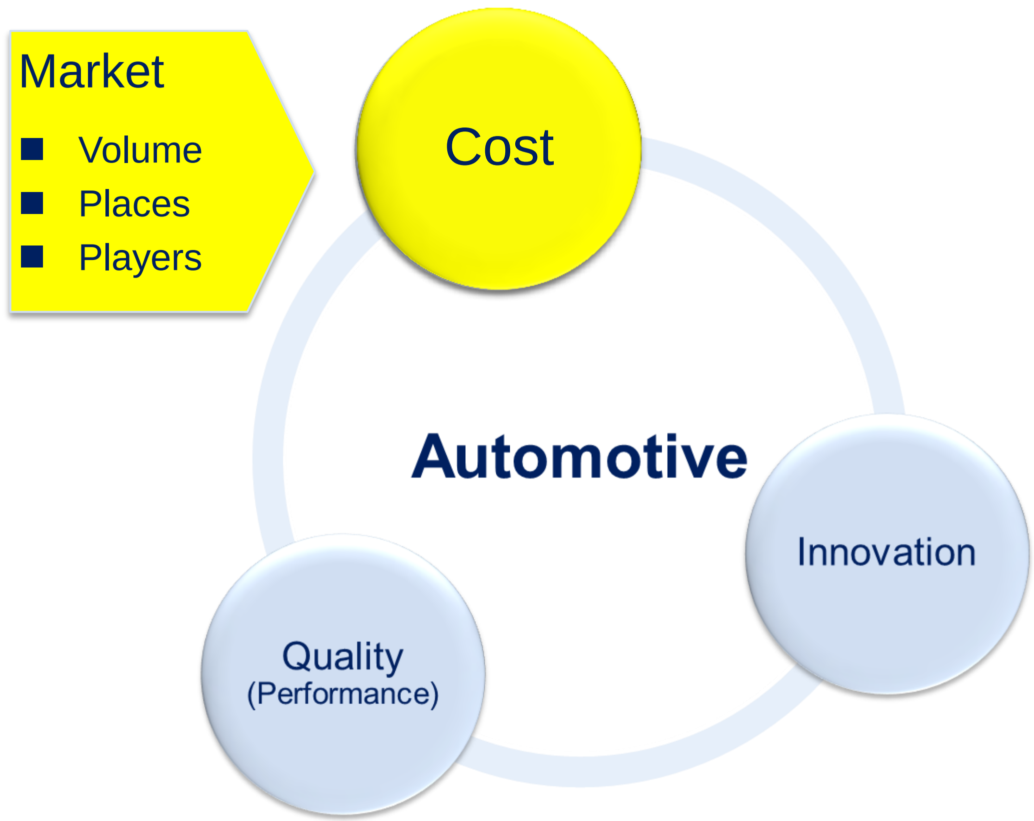
Application interfaces

- all application domains



Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Background

Software Reuse

Image removed

Vast majority of software development effort is spent on adaptation of existing solutions.

Background | **AUTOSAR Standard**

Reusability of software

Components with standard format
→ Reuse for different suppliers
→ Reuse for different car lines

Integration by configuration

Layered architecture
→ Reuse for different HW

Built in variant handling
→ Software product lines

Standard interfaces & behavior
→ Mature implementations
→ Implementations shared by many OEMs

Reusability of software still required:

Components with standard format
→ Reuse for different suppliers
→ Reuse for different car lines

Assume guarantee pattern
(→FAT AK31)
→ Reusable certification
→ Easy integration

Application interfaces (Semantic)
→ Reuse for different OEMs

Integration by configuration

Layered architecture
→ Reuse for different HW

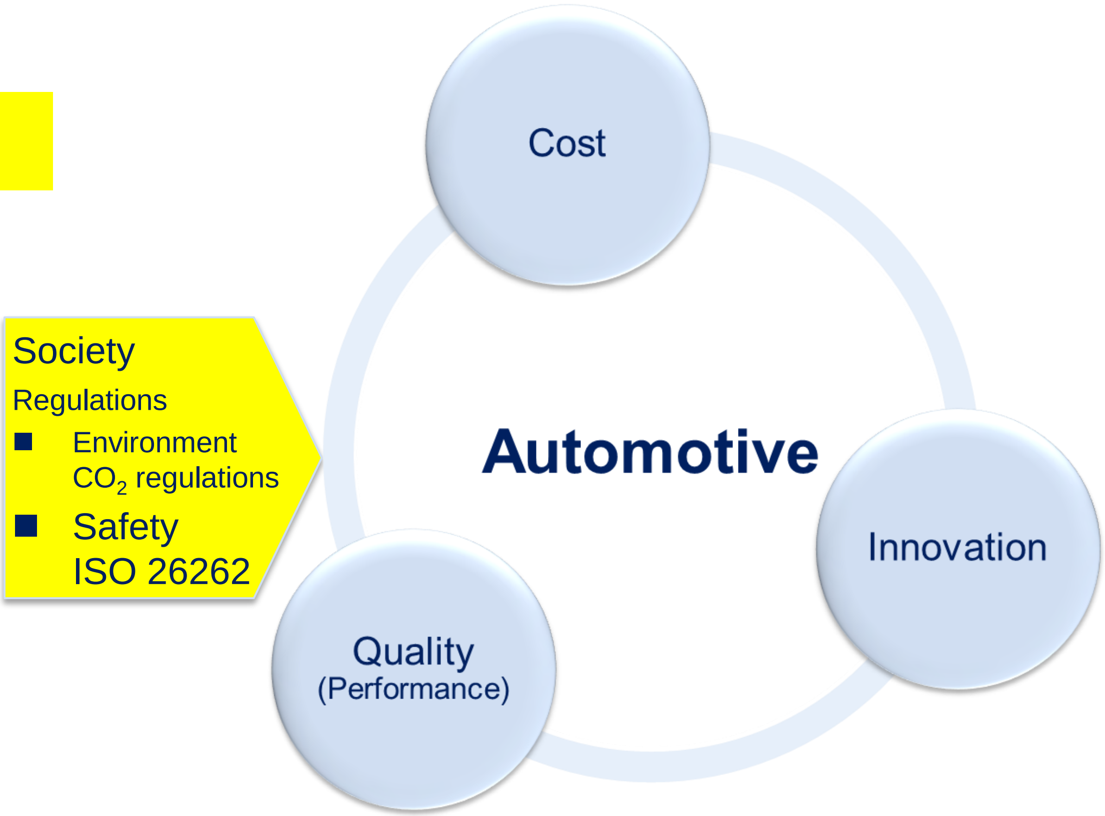
Built in variant handling
→ Software product lines

Standard interfaces & behavior
→ Mature implementations
→ Implementations shared by many OEMs

Whole PLM approach
(→AMALTHEA)

Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Background

Functional Safety

Background

Safety is absence of unreasonable risk

- Society judges the level of acceptable risk

*Functional Safety is the absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems**

- Avoid malfunctions of E/E systems
- Applicable to all E/E systems with intrinsic risks

*) ISO 26262-1

Scope of ISO26262

Target

- Passenger cars < 3.5t
- OUT: Trucks, Motorbikes, Tractors,…

Hazards under consideration

- Human damage
- OUT: material damage

Object under consideration

- E/E System device, semiconductor, hardware design, software
- OUT: mechanic structure, material

Faults under consideration

- Systematic design faults, random hardware faults, etc.
- OUT: abnormality due to high voltage, ageing, fire hazard, heat, corrosion, performance

Functional Safety

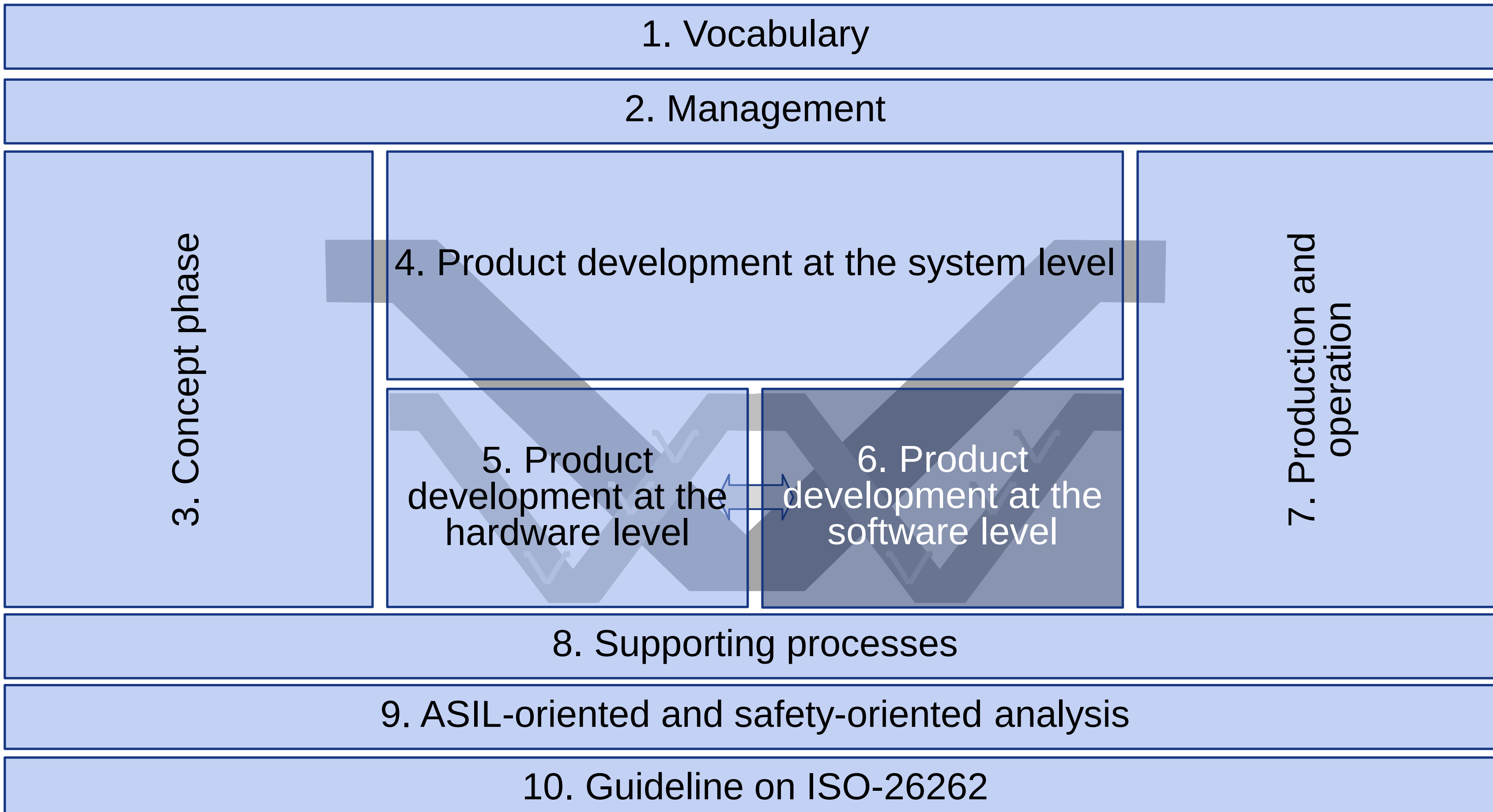
Background

Standard: ISO 26262

Release date: 2011/11/15

Road vehicles — Functional safety

Parts:



Background

Purpose of ISO 26262

What it is **not**:

- **Certification** requirement

What it is **partially**:

- **Legal** requirement
  only through product liability requirement for **‘state of the art’**

What it **is**:

- **Guidance** to find right level of functional safety effort to spend.
  - Reduce number of **callbacks** for safety reasons.
- **Defense** against liability claims.

Background | **AUTOSAR Standard**

Disclaimer

AUTOSAR (AR) does NOT guarantee any Functional Safety (FS) properties of the final system

- AR provides mechanisms to support FS (SW level)
- Helps during the design phase for SW level
- Each system has its own context of use, functionality and implementation

The full responsibility for selecting and implementing appropriate safety mechanisms as described inside the AUTOSAR framework fully resides on the implementer

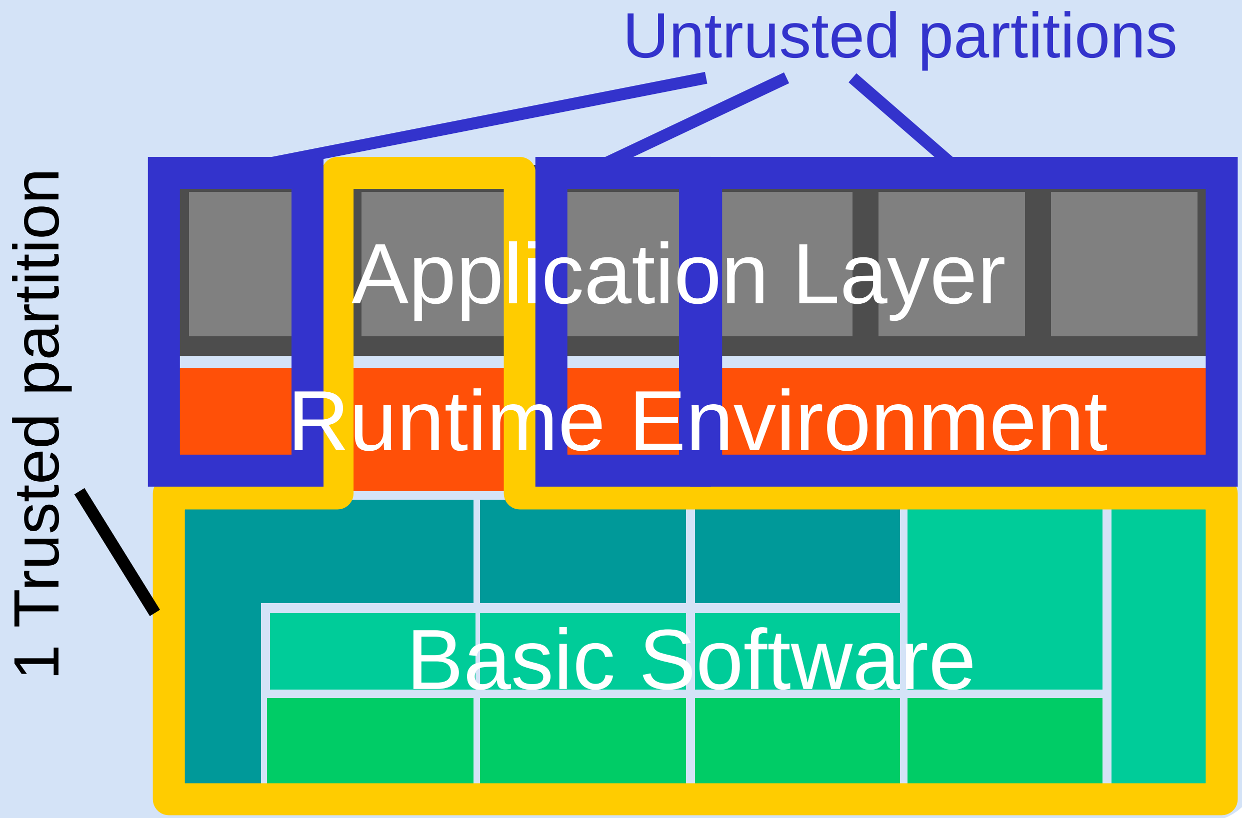
Functional Safety

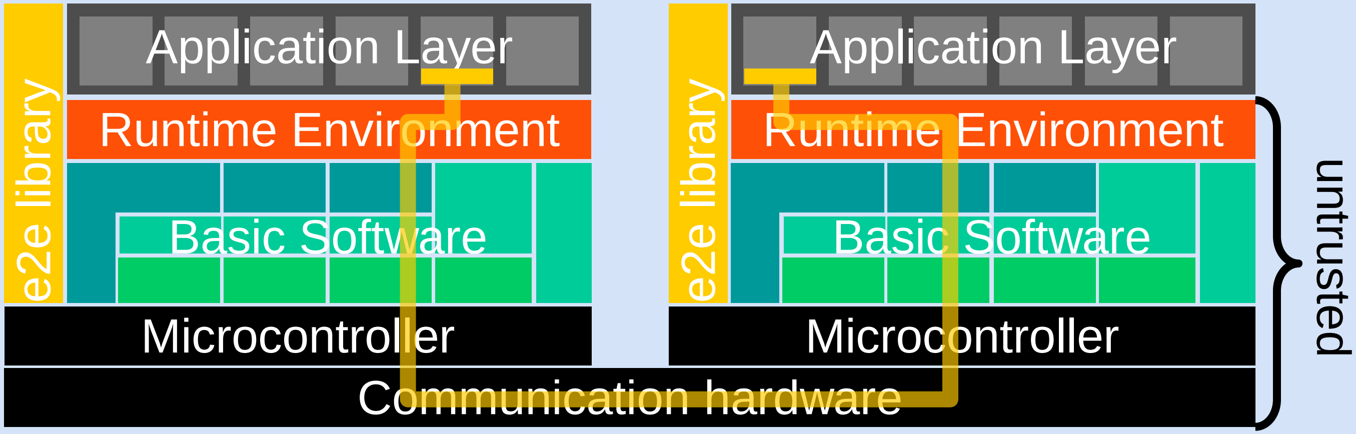
Background | **AUTOSAR Standard**

Partitioning

- ☐ Memory protection
- ☐ Timing protection (time budgets)
- ☐ Selective stop of partitions for increased critical function availability

- ■ Permits separation
  - ☐ Mixed safety integrity levels
  - ☐ Responsibility sharing across SW vendors



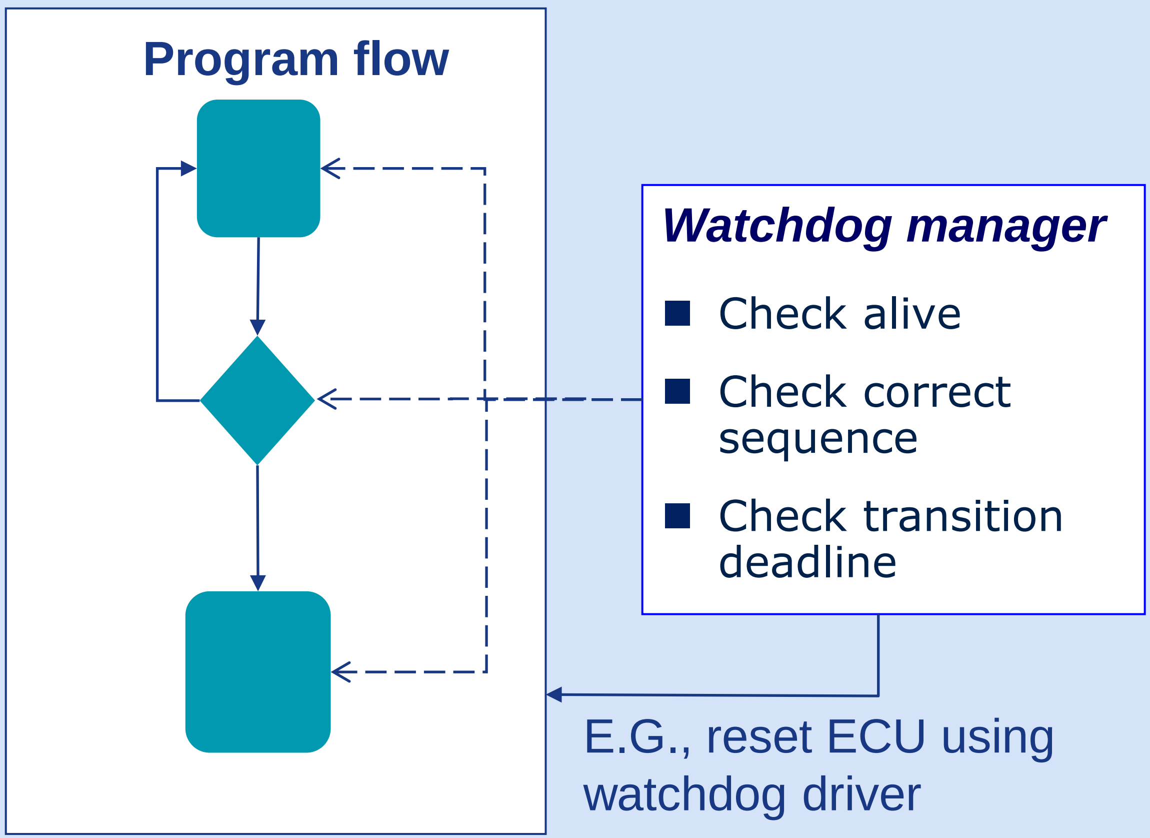


- Provides
  - Data integrity,
  - Authentication,
  - Sequence check
- Implemented by
  - Static end to end protection library
  - Wrapper code for handling protection context for communication

Functional Safety

Background | **AUTOSAR Standard**

Partitioning | End to End Communication Pr | Program Flow Monitoring



A problem has been detected and Windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.

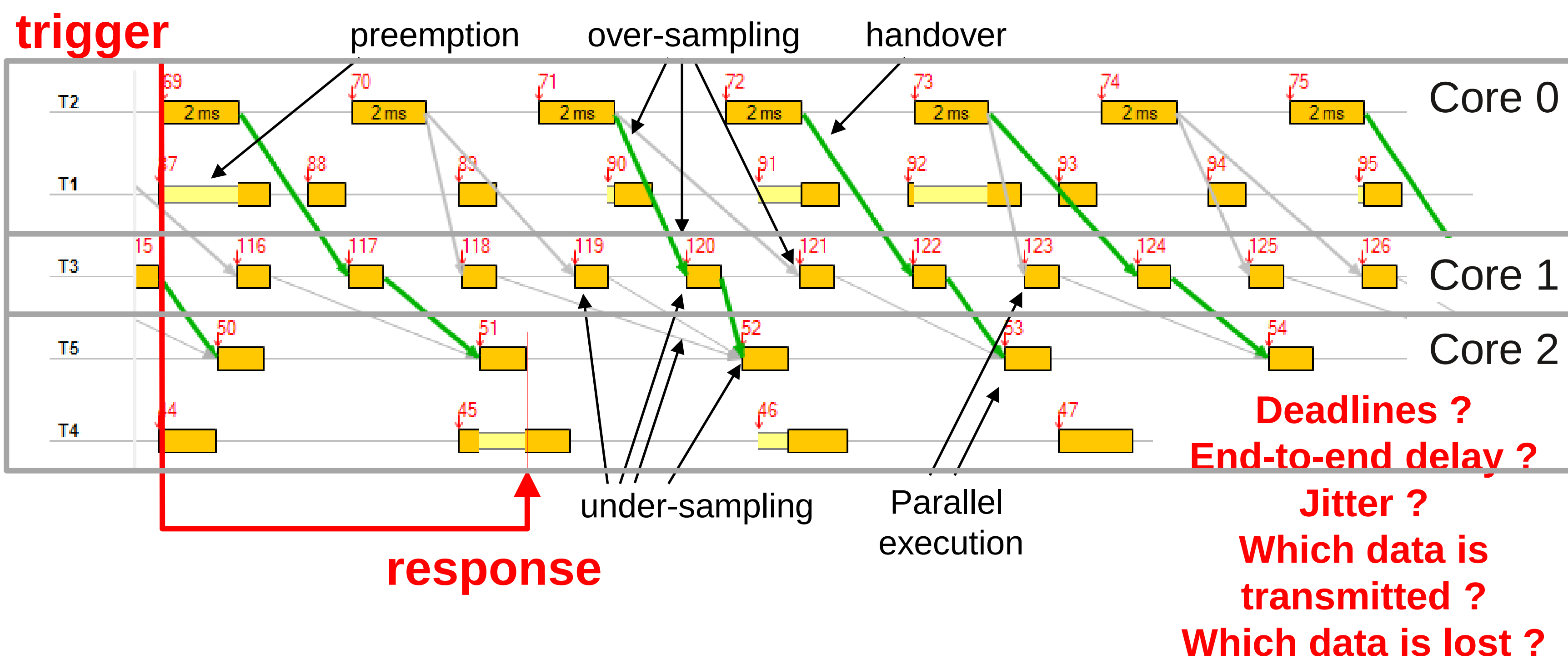
Functional Safety

Research

- Availability / fault operational concepts
- Safety related extensions for methodology (→SAFE, AR internal)
- Use of multi core for hardware partitioning
- Runtime HW tests integration
- Convergence of safety & security (→SESAMO proposal)

- Safe and reliable integration of components (→TIMMO-2-USE,recomp).
  - Safe and robust software execution (AR internal)

Timing Constraints and Scheduling



Scheduling effects are already complex in small systems

- More complex in multi cores

Fulfillment of timing constraints must be checked

- Already in single cores and even more in multi cores
- Scheduling Analysis is one way

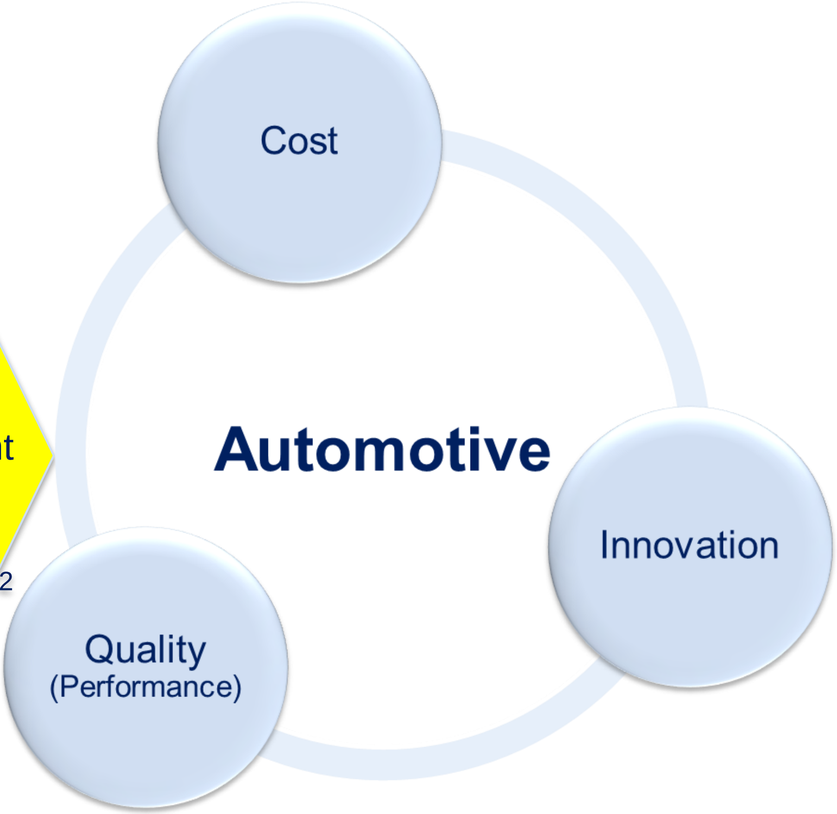
Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - ☐ Cost
  - ☐ Functional Safety
  - ☐ Energy Efficiency
  - ☐ Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words

Society

Regulations

- Environment CO_2 regulations
- Safety ISO 26262



Energy Efficiency

Background

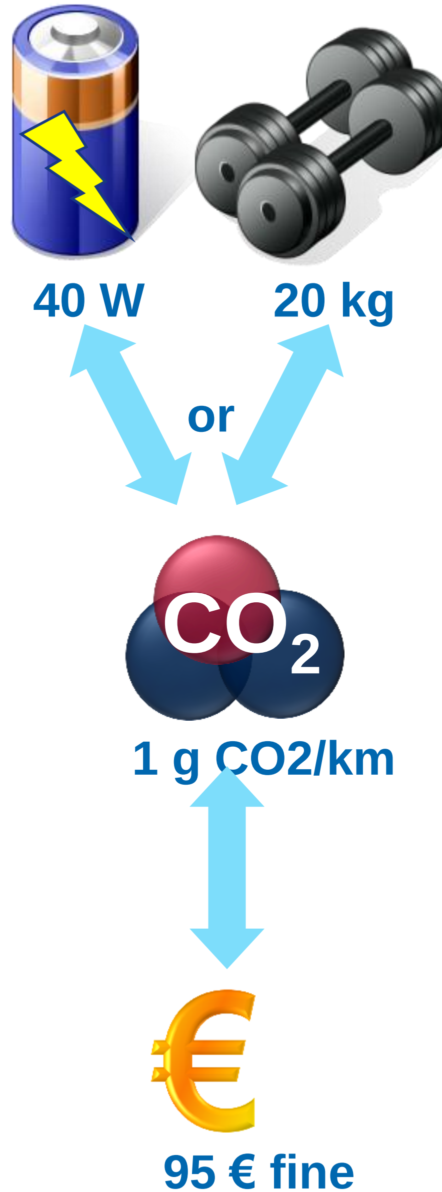
*EC CO_2 Emissions Regulation 443/2009

100 W electrical	⇔	0.1 ℓ/100km
50 kg	⇔	0.1 ℓ/100km

1 ℓ/100km Fuel	⇔	23.6 g CO2/km
1 ℓ/100km Diesel	⇔	26.5 g CO2/km

1 g CO2/km	⇔	40 W electric
1 g CO2/km	⇔	20 kg

1 g CO2/km	⇔	95 €*
current consumption per ECU		~200 mA



Similar battery cost results for electric cars

Energy Efficiency

Background | **AUTOSAR Standard**

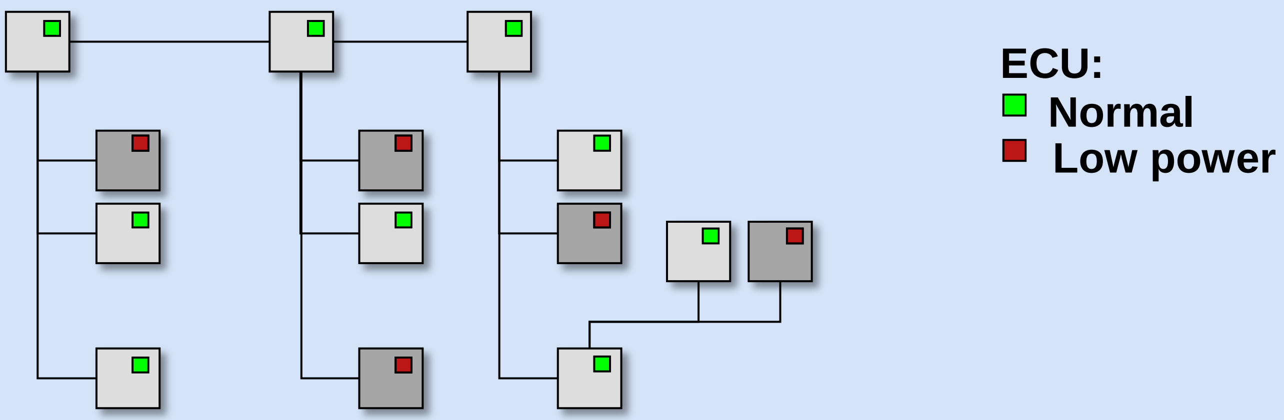
Partial Networking

Many Functions are only sporadically required:

- Seat heating
- Trailer connector
- Window lifter
- In total: ~10 ECUs

Idea:

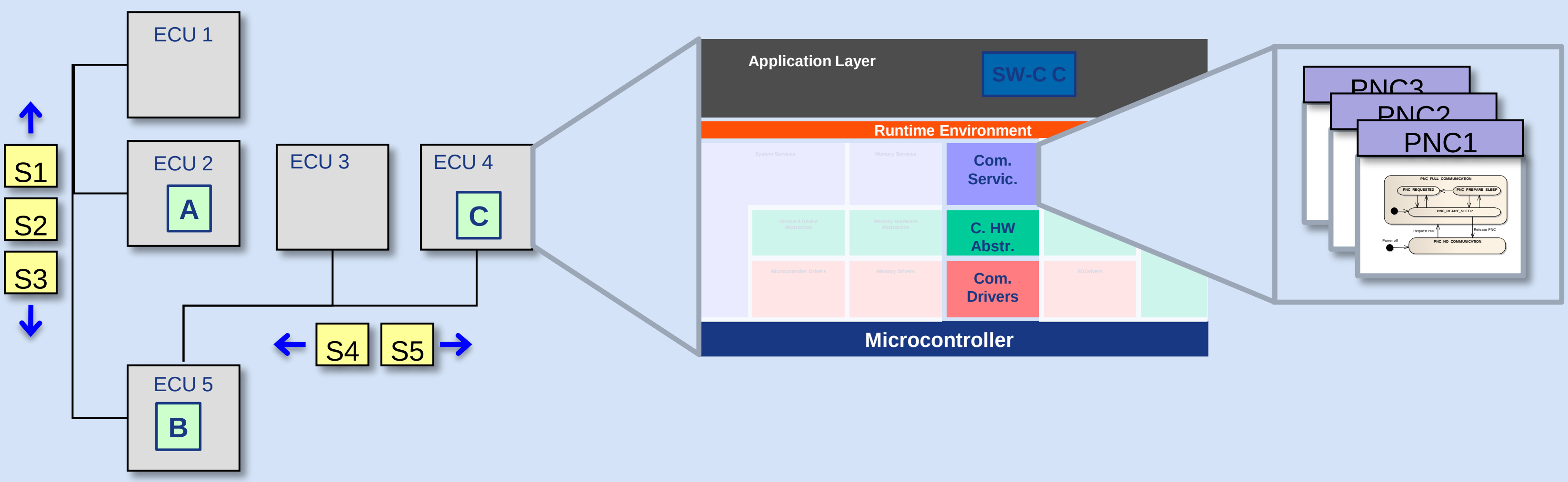
- Turn off all nodes that do not contribute to any active function



Partial Networking

Challenges:

- Methodology to map functions to software component and communication resources
- Bookkeeping of active functions / partial network clusters
- Coordinate partial communication
- Coordinate sleep and selective wakeup of some nodes



Energy Efficiency

Background | **AUTOSAR Standard**

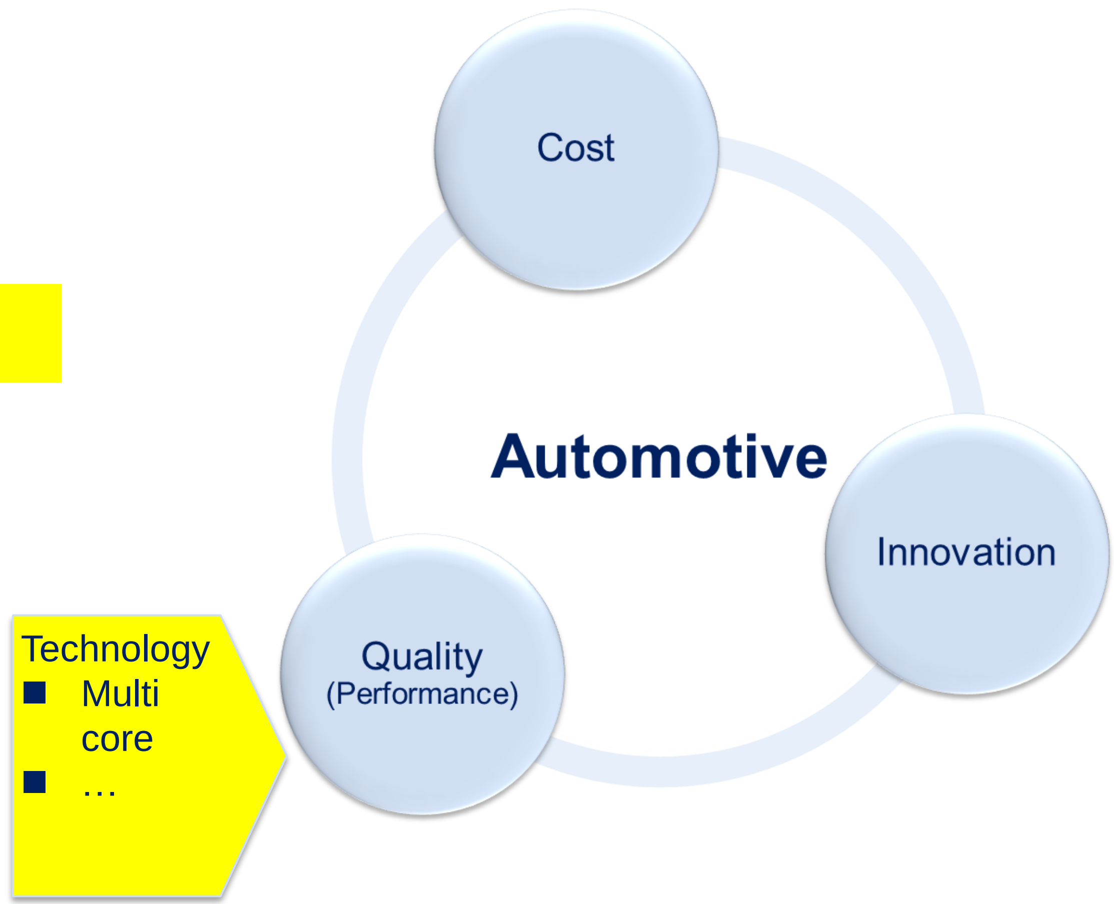
Partial Networking | ECU Degradation

ECU local measures (to be published in rev. 4.04)

- vehicle mode architecture:
  How to consistently control vehicle resources and vehicle functions with contradicting optimization criteria like energy consumption, comfort, safety, …

Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Background

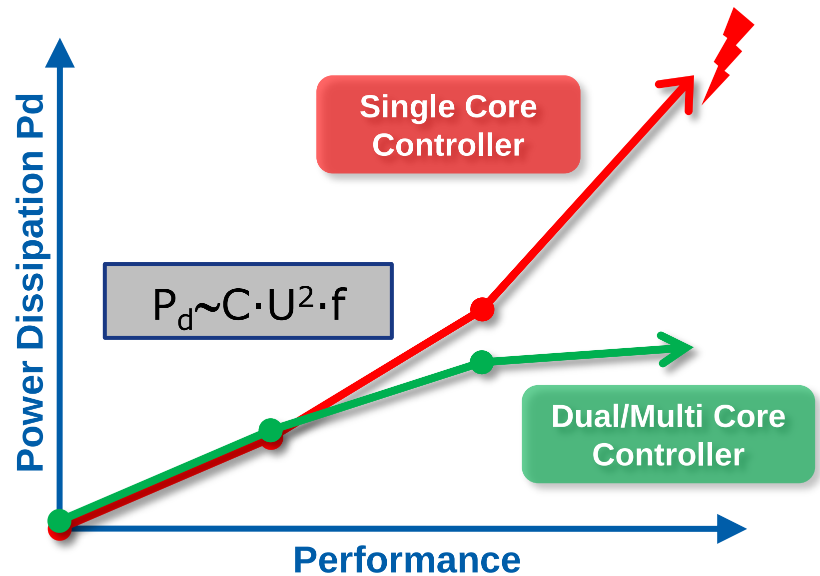
Multi Core Benefits

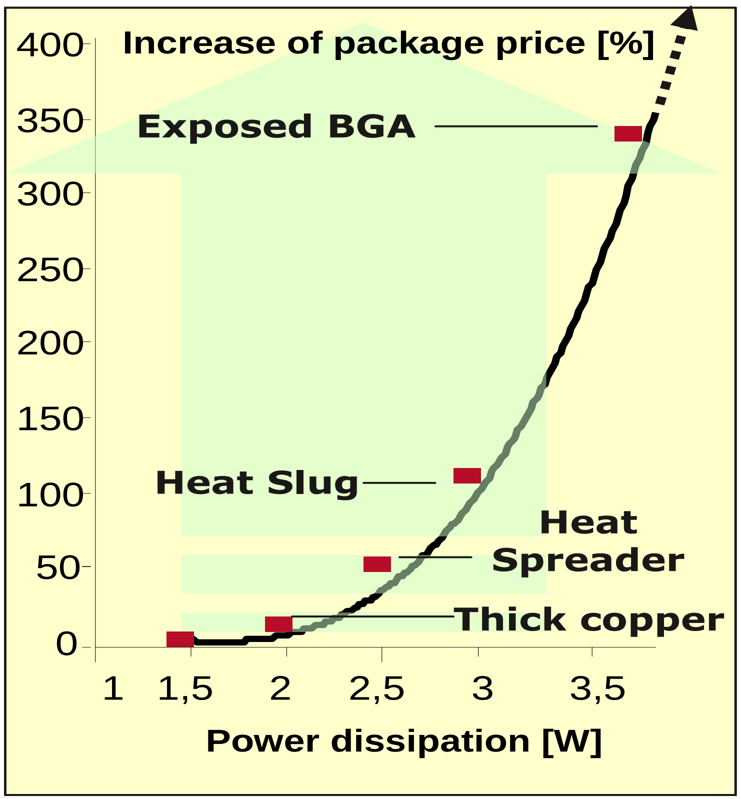
Image removed

Background

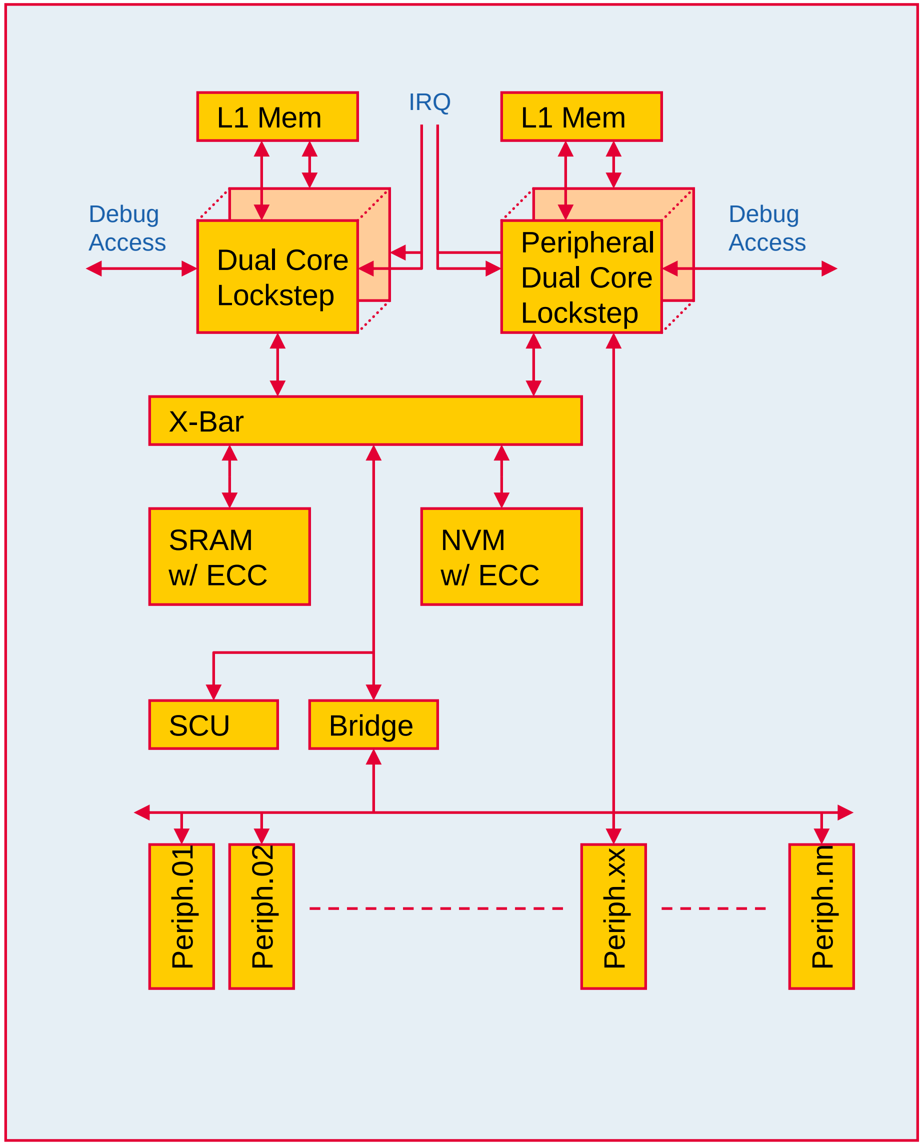
Multi Core – Energy efficiency & performance

- Dual (multi) core is the solution to the Moore law & power dissipation problem.





Background

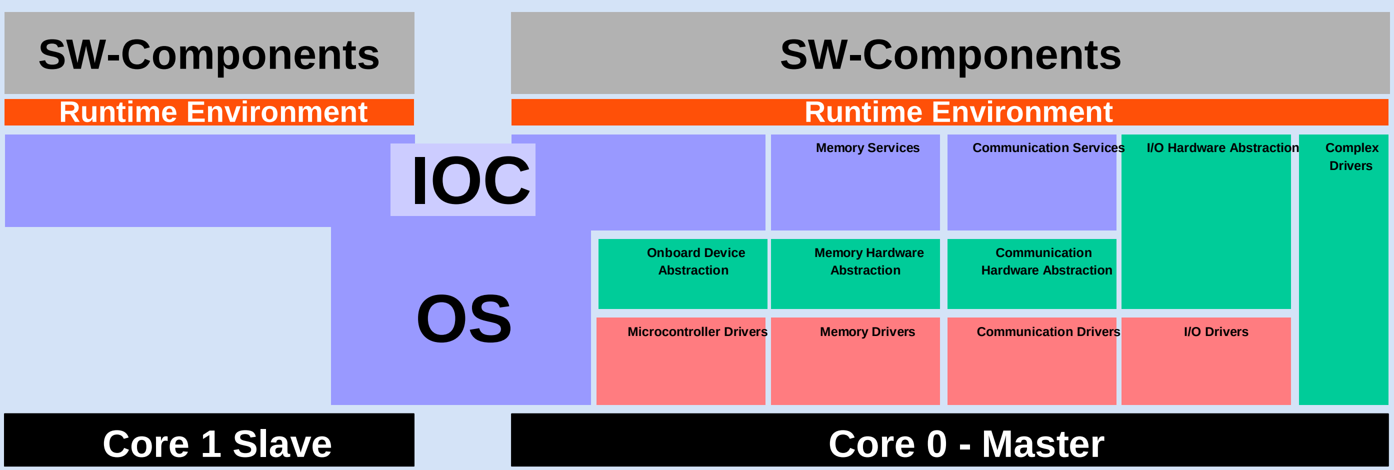


Example Concept for Hybrid Architecture

- Safe Processing Concept (Aurix, Infineon)
- Lockstep application processor
- Lockstep peripheral control processor
- able to run diversity mode
- memory management for Cores and DMA have,
- ECC protection for memory and busses
- scalable and composable in performance and memory size

Multi Core Support

- Single image OS
- Tasks and software components bound to cores
- Shared memory assumption (not exploited)
- Generic module for inter core communication (IOC)
- Spin-locks for explicit synchronization



Multi-Core

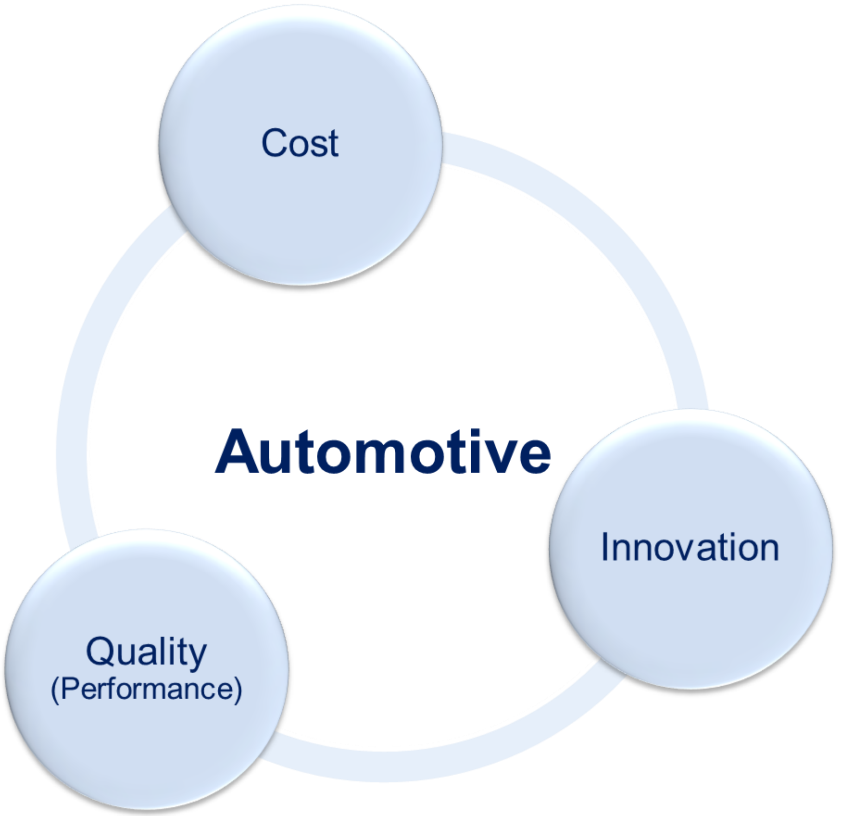
Background | AUTOSAR Standard | **Research**

Automotive related multi-core research

- How to scale with large number of cores (TERAFLUX)
- Load balancing
- (Semi-) Automatic parallelization
- Better scheduling mechanisms than local PCP and spin locks.
  - Predictable multi core scheduling (parMERASA)

Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Example

parMERASA

Multi-Core Execution of *parallelised* Hard Real-Time Applications Supporting Analysability

EC FP-7 project 2011-2014

start: Oct. 1, 2011

3.3 Mio EC contribution

Project webpage: http://www.parmerasa.eu

Example

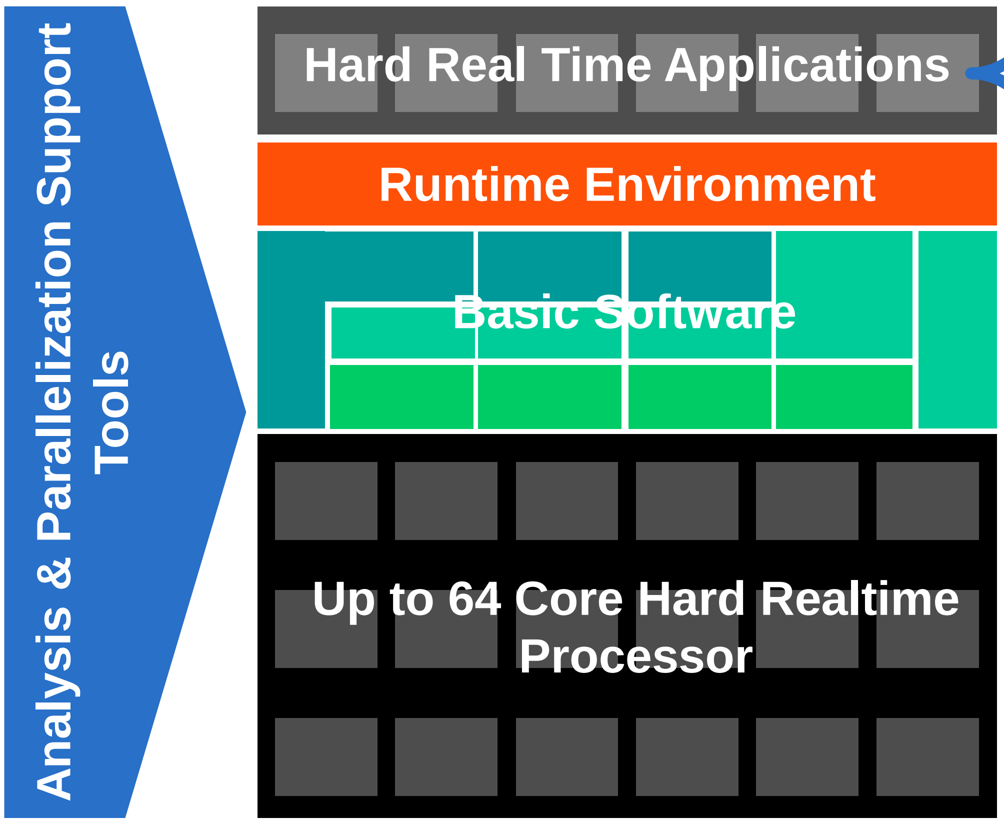
parMERASA Project partners

- **University of Augsburg** (Project Coordinator)
- **Barcelona Supercomputing Center**
- **Université Paul Sabatier**
- **Technical University of Dortmund**
- **Rapita Systems Ltd.**
- **Honeywell international s.r.o.**
- **BAUER Maschinen GmbH**
- **DENSO AUTOMOTIVE Deutschland GmbH**

parMERASA Industry Advisory Board

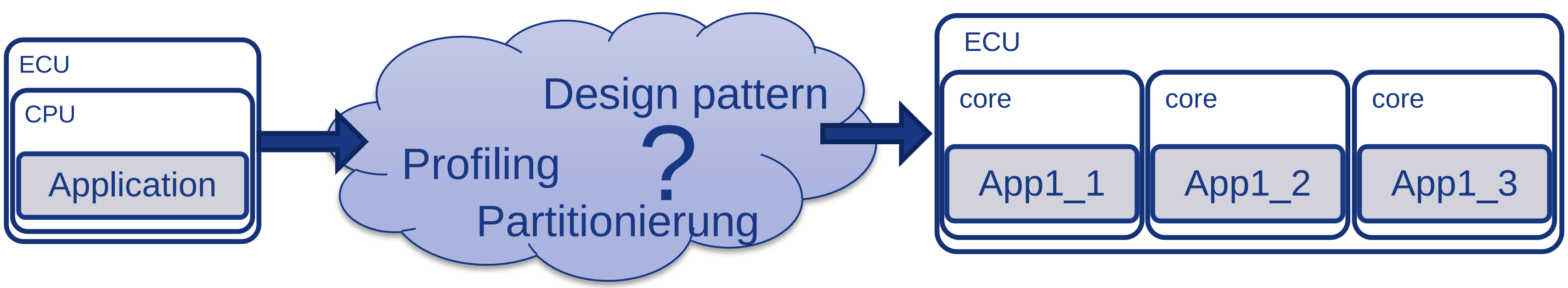
- **Benoit Triquet,** Airbus,
- **Philippe Chevalley,** European Space Agency ESA,
- **Glenn Farrall,** Infineon Technologies UK Ltd,
- **Rafael Zalman,** Infineon Technologies AG,
- **Andre Lajtkep,** BMW Group,
- **Hakan Sivencrona,** MECEL AB,
- **Claus Stellwag,** Elektrobit Automotive GmbH,

parMERASA Scope



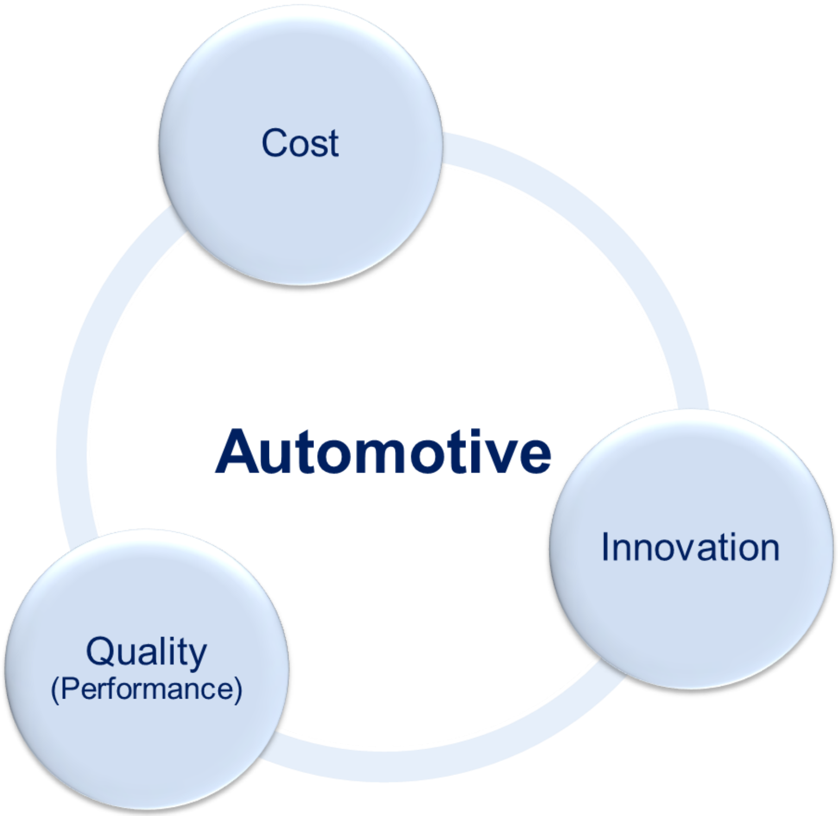
parMERASA relevance for automotive

- How to parallelize automotive applications while preserving the real time properties?
- Safe scheduling (not only in multi core ECUs)
- Where are the limits for parallelization of automotive applications?
- Use cases
  - Fuel efficient engine control
  - Vehicle internal router
  - High integration - compound ECU



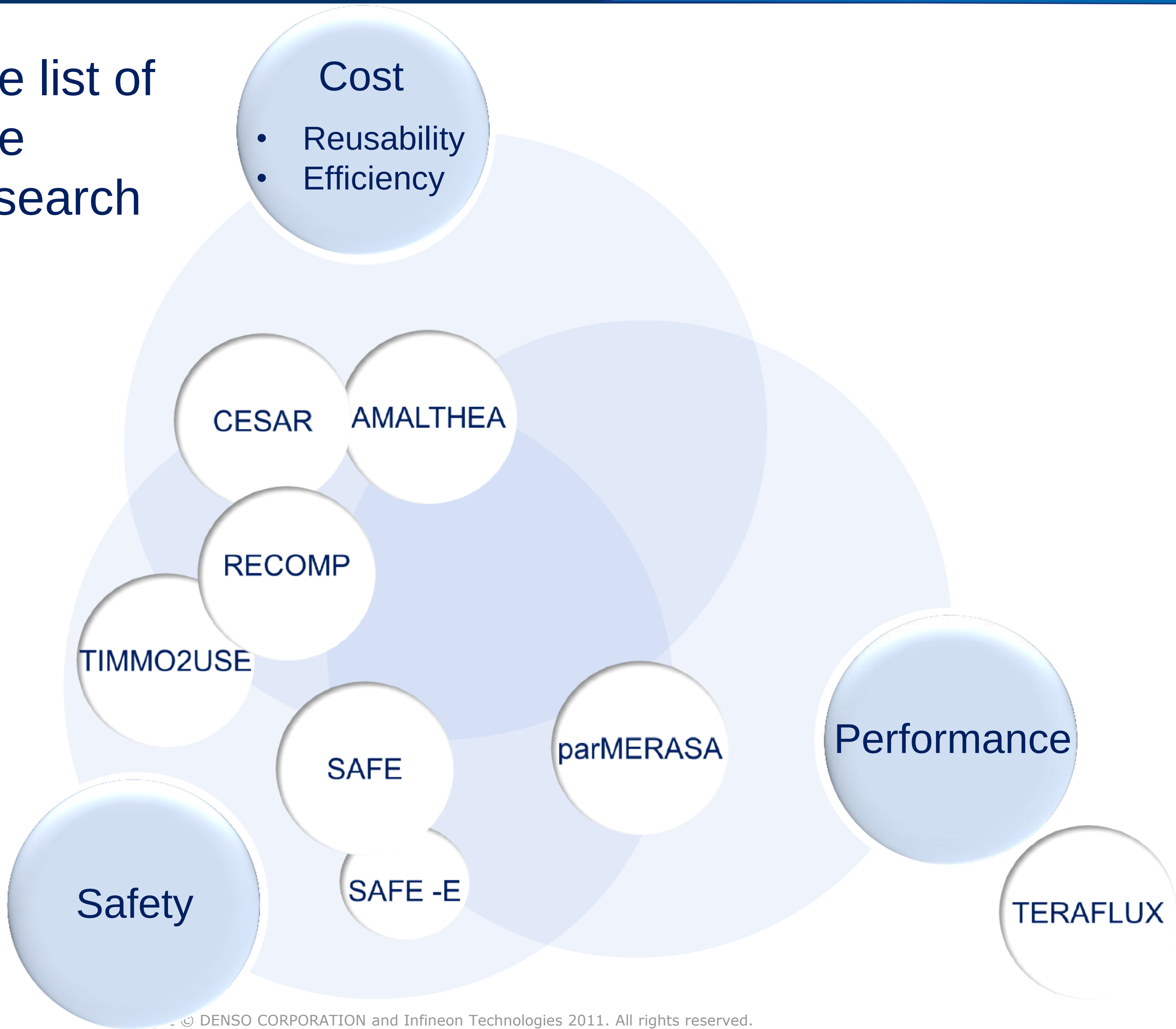
Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



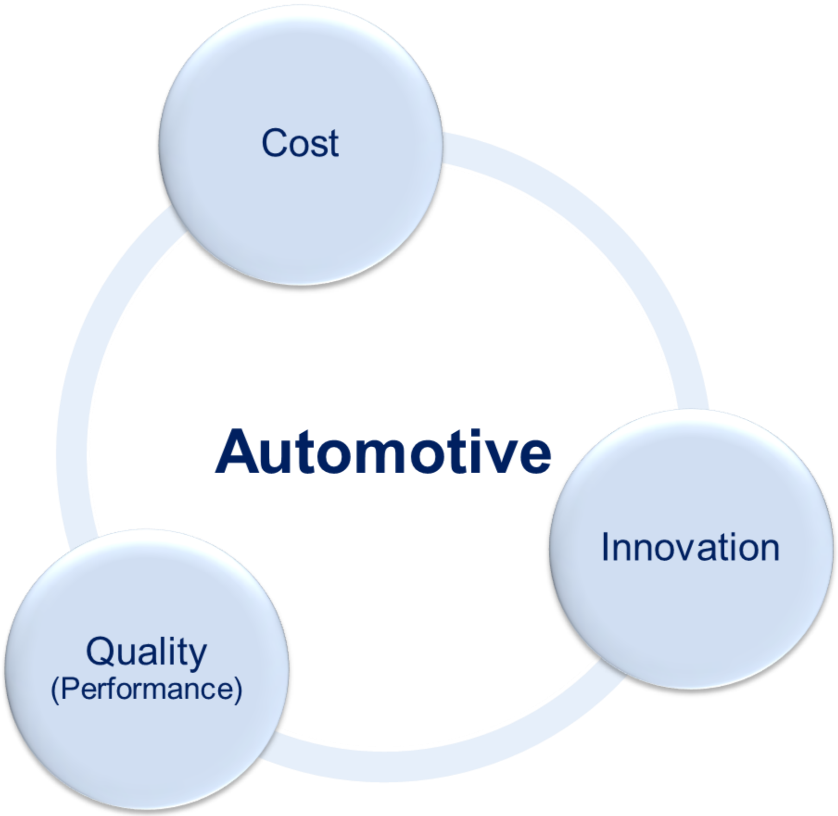
Public Research Landscape

Incomplete list of automotive related research projects



Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words



Closing Words

- The automotive industry has found in AUTOSAR a standardization body for standardization of their system and software architecture framework.

- Innovations are brought in from public research projects

- Future concerns of AUTOSAR:
  - **Fragmentation**: How to master different releases, how to prevent cherry picking and simplified subsets in BRICS?
  - **Ageing**: Easy to integrate innovations, difficult to clean up

Questions