SIEMENS

TUM, Jan 2014

RACE – ECAR

Dr. Ludger Fiege, Siemens AG

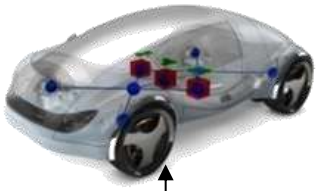
Three independent development paths leading to the Smart eCar

Function development

ADAS* vertically integrated → ADAS horizontally integrated with strategy level

*Advanced Driver Assistant Systems

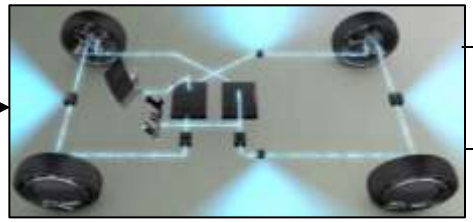
Zero Accidents with intervening decision



Smart eCar autonomous driving

© Photo: Nissan

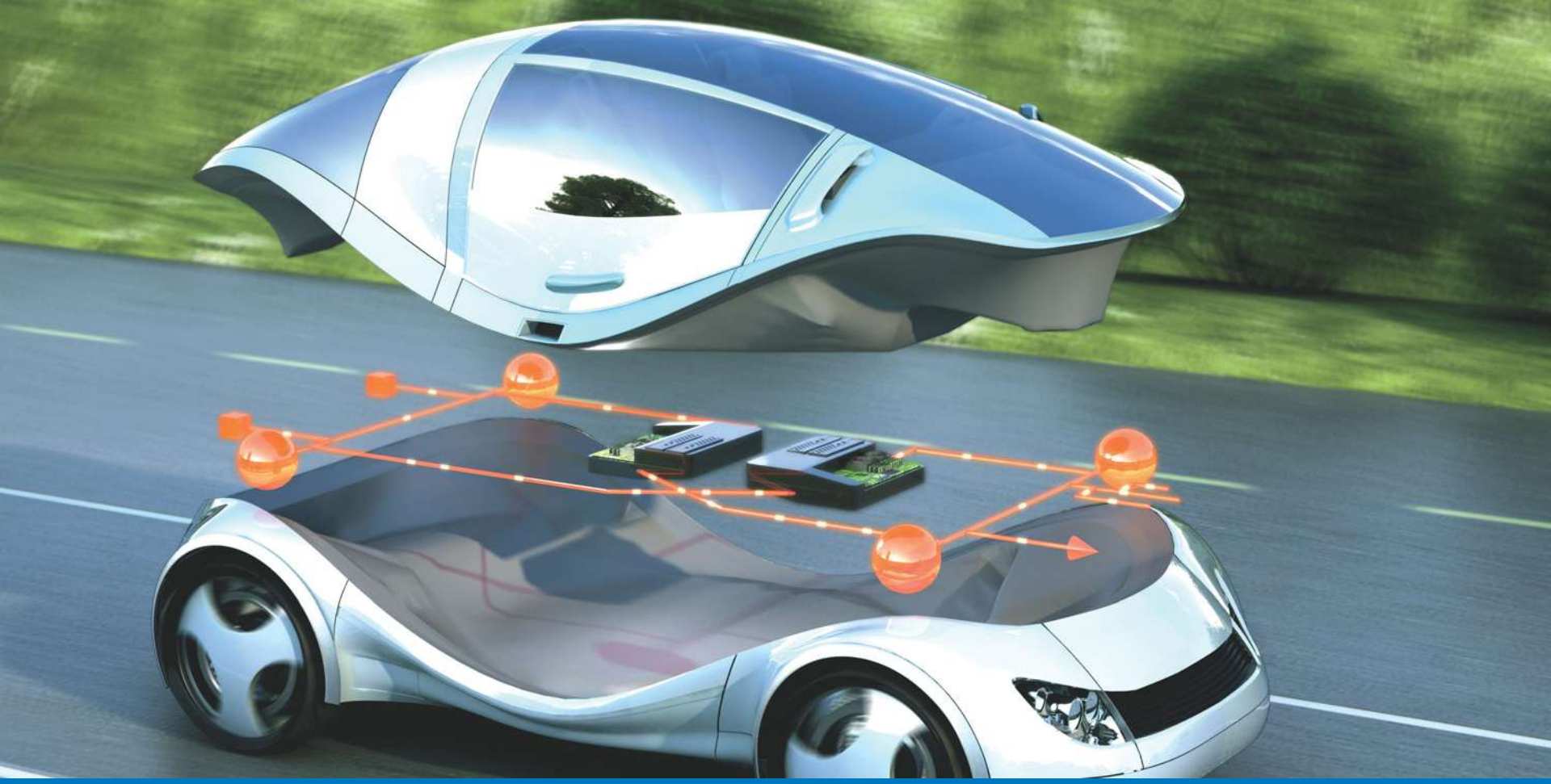
RACE platform development



Electro mechanical integration

- E-Motor
- Brake
- Damping
- Steering

New ergonomic concepts through mechatronic integr.



*R*obust and reliable *A*utomotive *C*omputing Environment for future *e*Cars

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

race

Agenda

- Motivation
- RACE setup
- System Overview
- RACE Runtime Environment

Project RACE

Robust and reliant Automotive Computing Environment for future eCars

Bundesministerium für Wirtschaft und Technologie

WIRTSCHAFT. WACHSTUM. WOHLSTAND.

- Funded by BMWi
- Project time: January 2012 – December 2014
  http://www.projekt-race.de

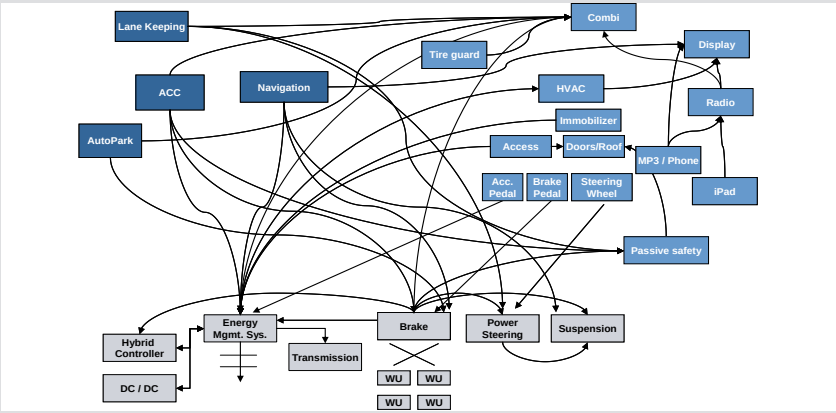
- Project based on study „Mehr Software (im) Wagen“
  http://www.fortiss.org/ikt2030

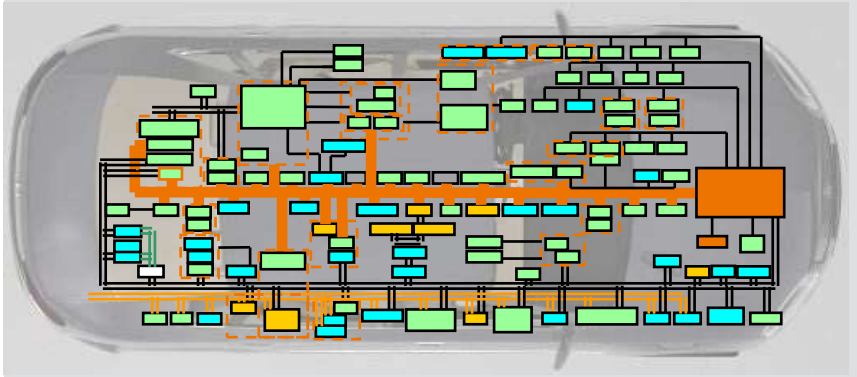
SIEMENS | fortiss | AVL | TRW

TUM | Universität Stuttgart | Fraunhofer AISEC | RWTH Aachen

To discover the full potential of electric vehicles a new E/E architecture is mandatory

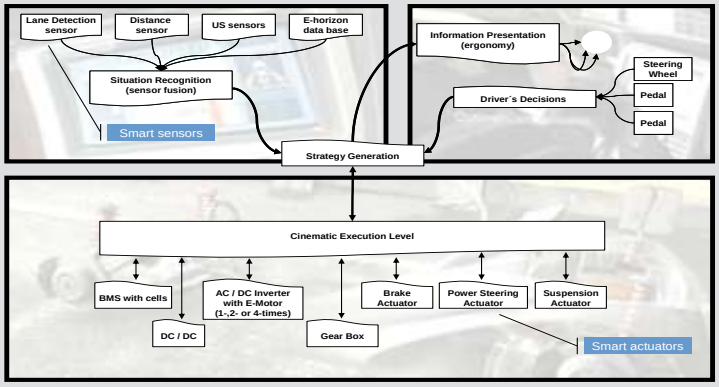
Symbolic pictures

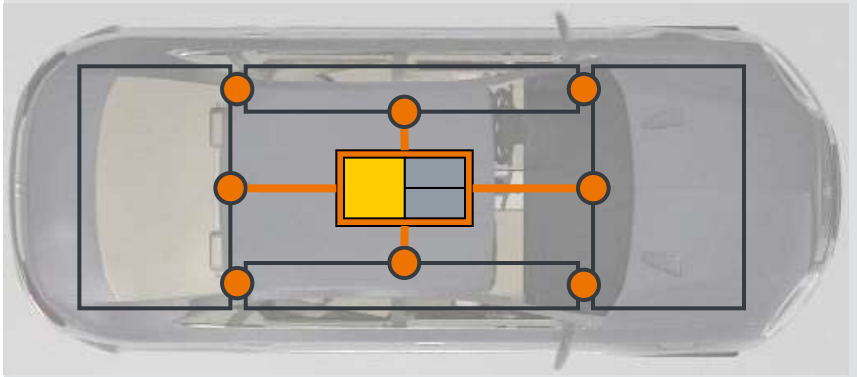




- Get rid of position oriented partitioning
- Well defined information flow
- Hierarchical decision making

- Less controller
- Likely less copper
- Less different connector

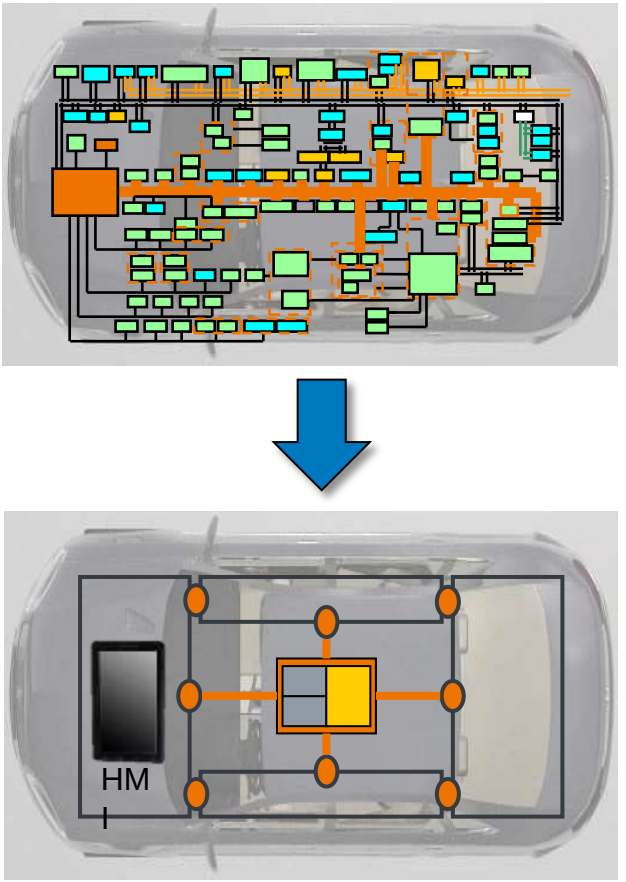




RACE Platform Idea

Main Project objectives:

- **Aim 1:** Reduction of complexity of ICT-Architecture by homogeneous and open basis platform
- **Aim 2:** Support if new complex functional vehicle features
- **Aim 3:** Plug & Play capability of ICT-Architecture
- **Aim 4:** Ability to certify the ICT-Architecture
- **Aim 5:** Show an migration path to the new architecture



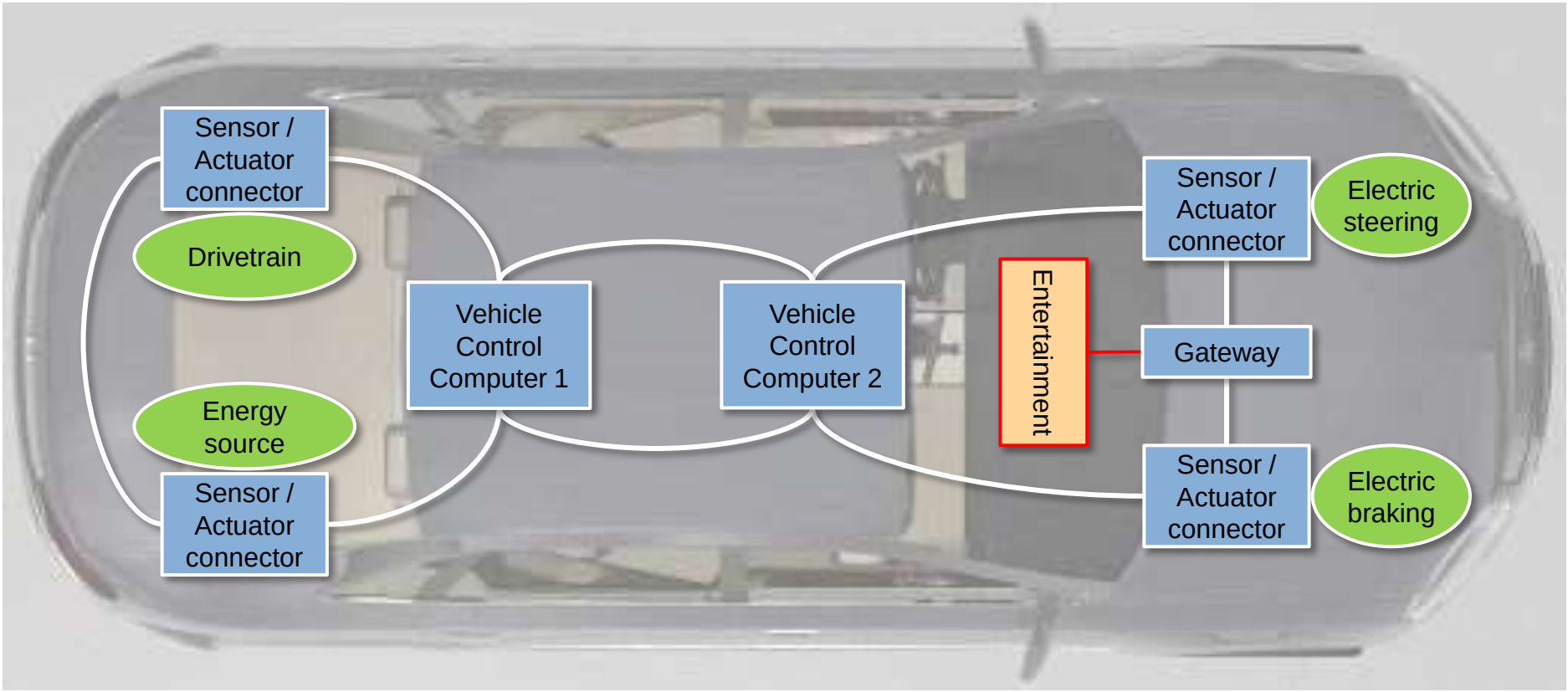
Main Principles:

- Centralized ICT-Architecture
  - Central-Platform-Computer, mixed critical features
  - Data-centric approach: All data about Sensors and Actuators is accessible everywhere
- Communication
  - Switched Ethernet
  - Publish/Subscribe communication pattern
- Fail-Operational vehicle features

Agenda

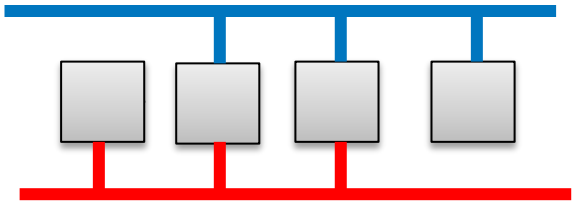
- Motivation
- RACE setup
- System Overview
- RACE Runtime Environment
- Safety Aspects
- Outlook

Ethernet-based redundant communication as data backbone

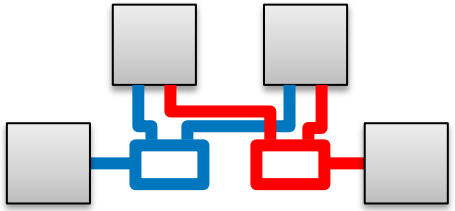


Realization of the Multipath Network

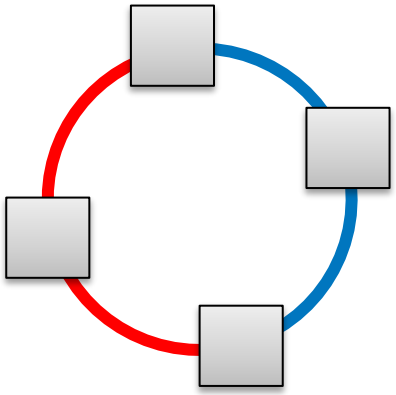
Parallel redundant bus:
Shared medium on each bus
Two physically independent busses
- High cabling effort
- „Slightly of specification“ failures possible



Switched Ethernet alternative 1:
redundant star architecture (AFDX)
- High cabling effort
+ Physically independent disjoint paths



Switched Ethernet alternative 2:
ring topology (industry automation)
+ Disjoint paths
+ Low cabling effort
- Physical independence of paths is lost → additional effort



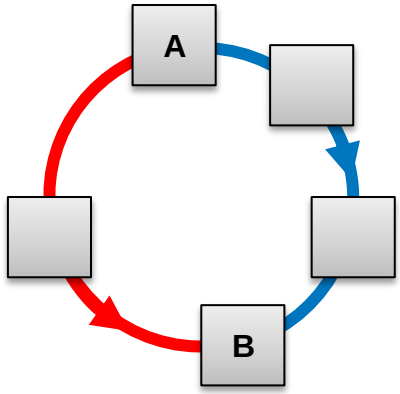
Ringtopologie

Vorteile:

- unabhängige Pfade
  (Ringrichtungen **links** und **rechts**)
  - keine gemeinsamen Geräte
  - unabhängige Punkt zu Punkt Verbindungen (Switched Ethernet)
- *Trennung auf logischer Ebene*
  - Mixed Criticality möglich
- vermeidet doppelte Verkabelung
- ermöglicht Vermaschung

Nachteile

- Ringschluss
- Energieversorgung muss explizit berücksichtigt werden
- „Babbling Idiot“ Szenario komplizierter
- Exotische Ethernetvariante
- Jeweils ein kurzer und ein langer Weg



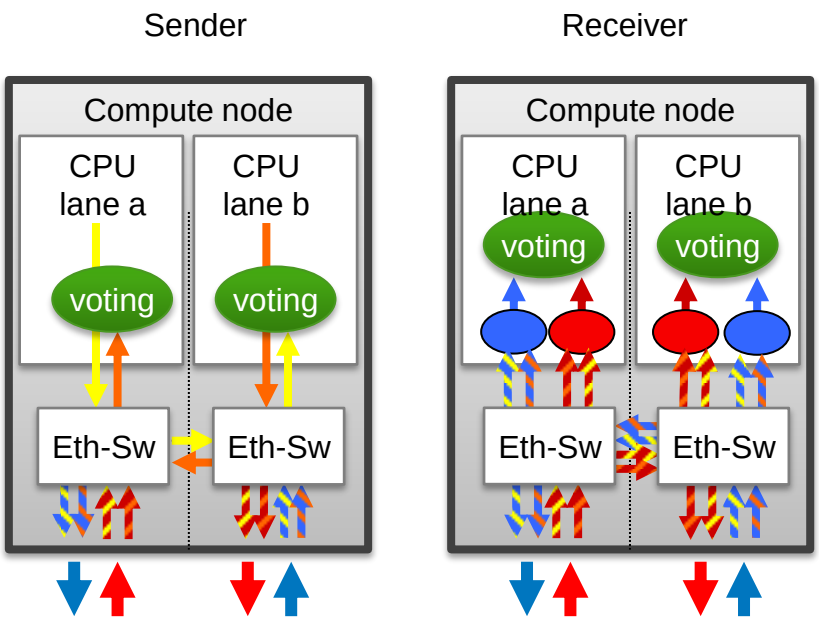
Fail-tolerant architecture: N-Duplex

core idea:

- pair of compute nodes monitor each other
- sensors and actuators don‘t need system know-how & are independent of scalability of platform core

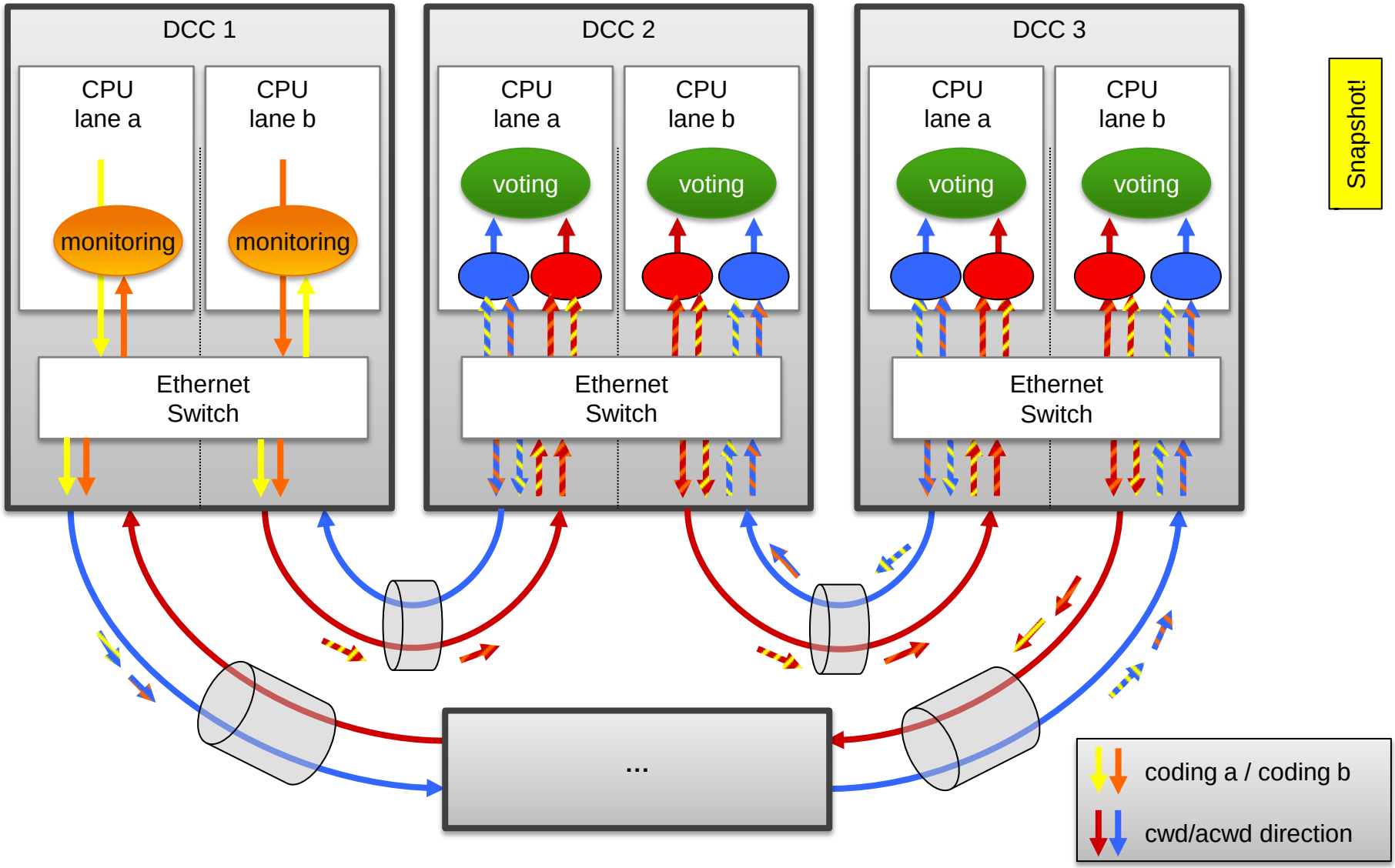
N-Duplex Platform:

- duplex unit
  guarantee integrity
- duo duplex
  fail-operational availability
- N-duplex
  scalability w.r.t. availability, mission time, performance



Compute node:
CPU, RAM plus communication-HW

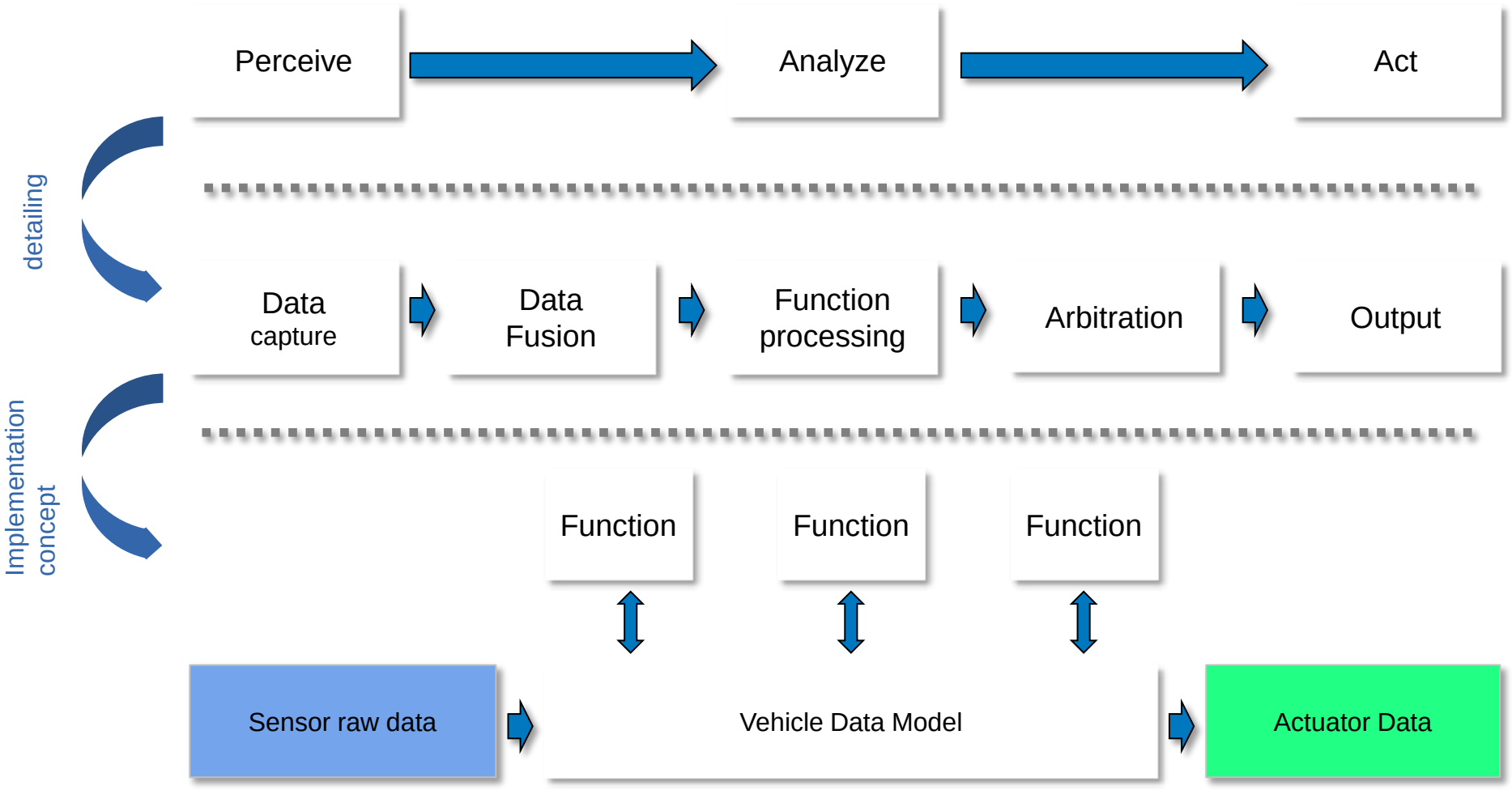
Consistent Communication in the Platform



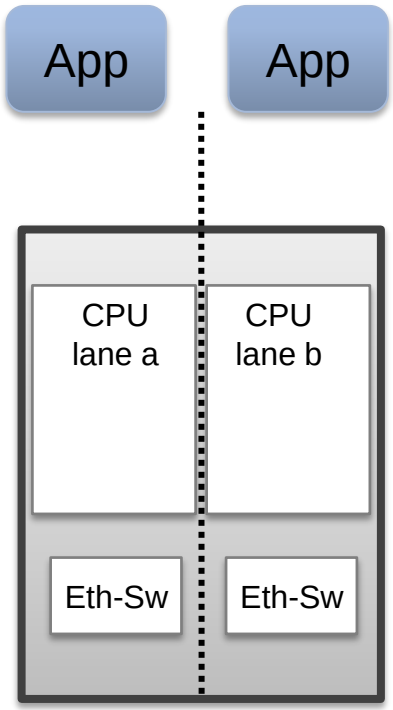
Agenda

- Motivation
- RACE setup
- System Overview
- RACE Runtime Environment
- Safety Aspects
- Outlook

Basic information flow



Simplex application development



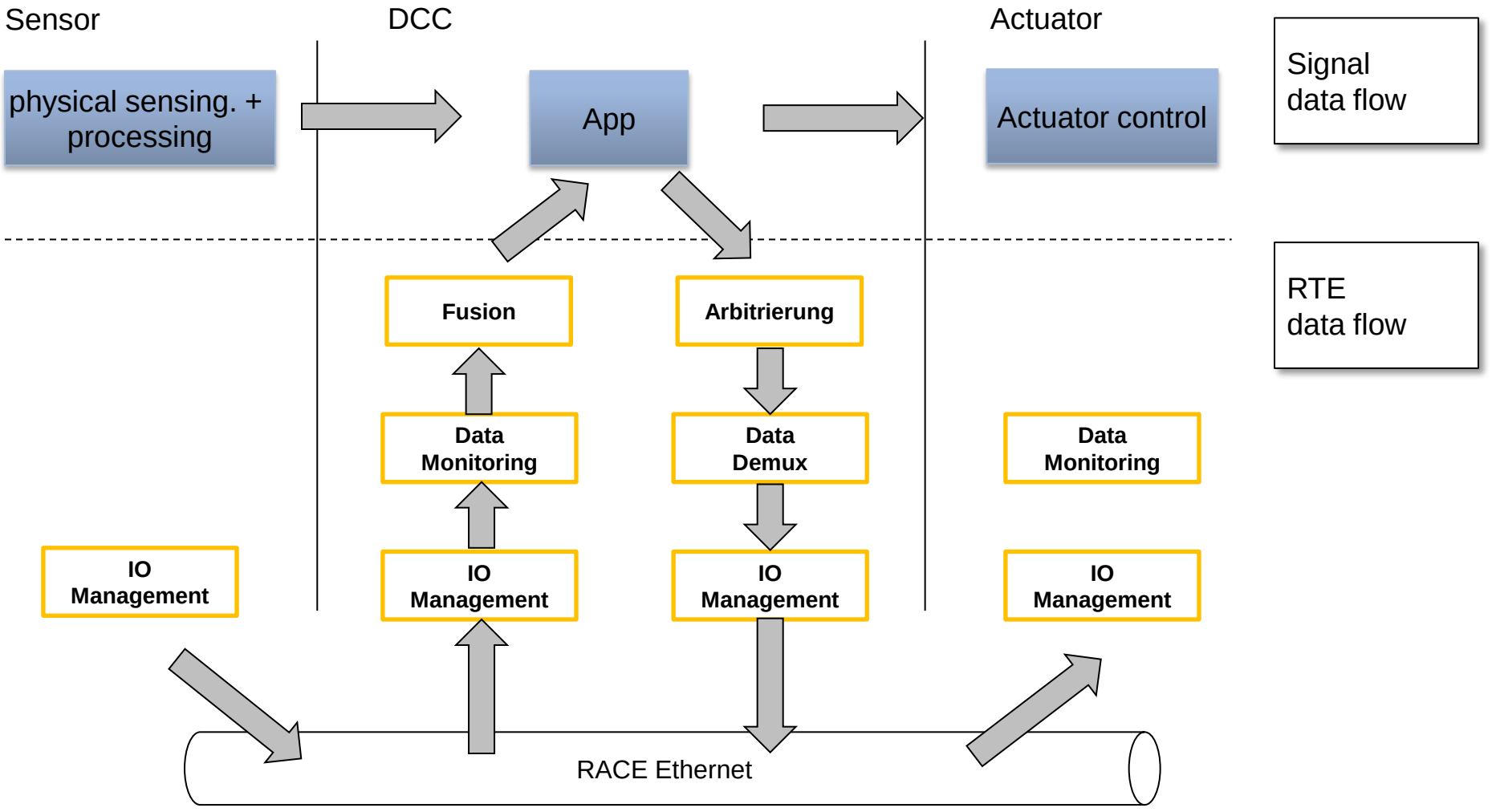
duplex control computer

applications
- developed for single channel deployment
- without dealing with redundancy

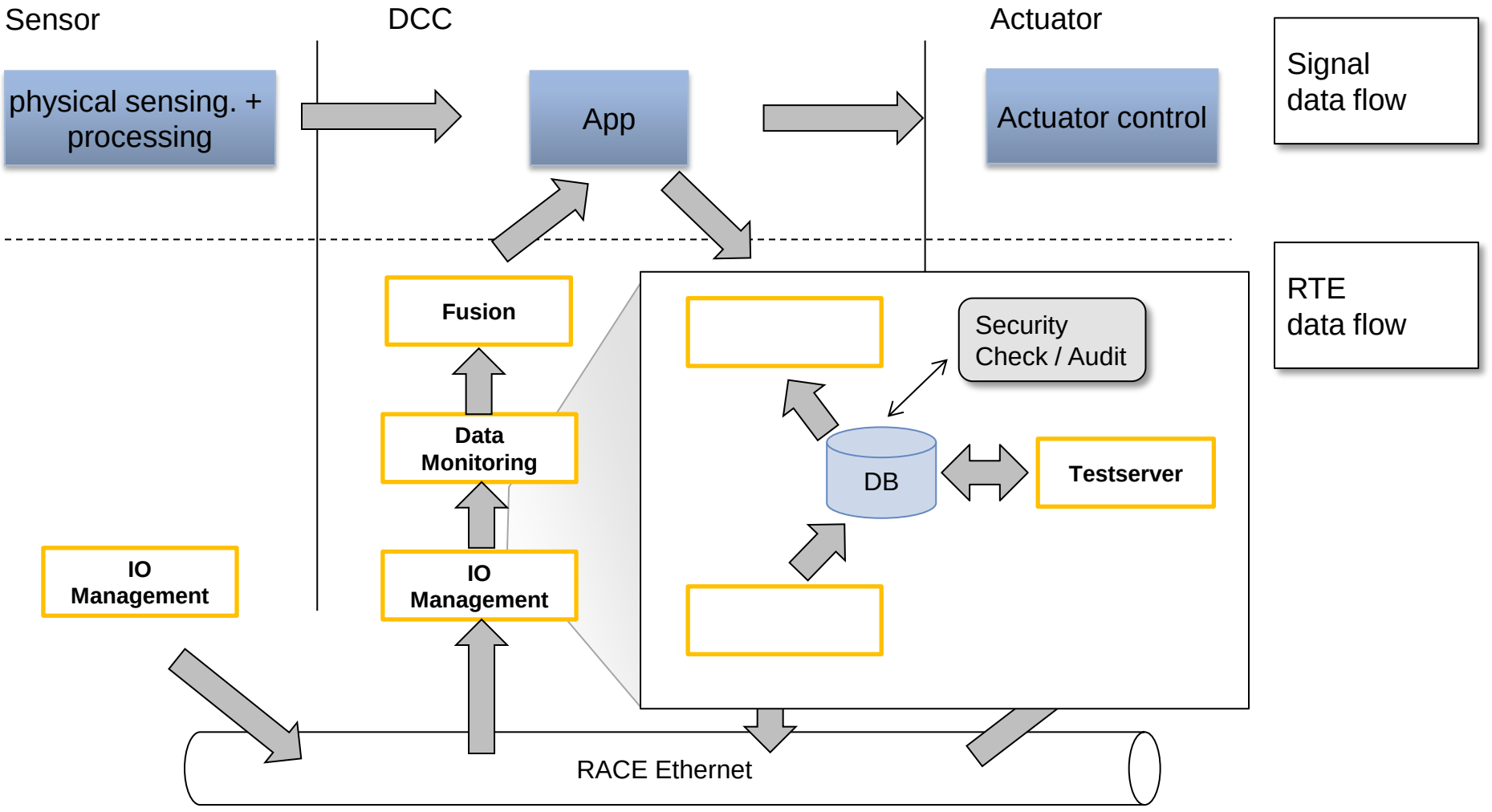
OS / MW function
- compare IO
- detect failures,
- identify fault containment region unanimously in distributed system

platform failures
- detected (masked) in platform
- offers “correct” RTE

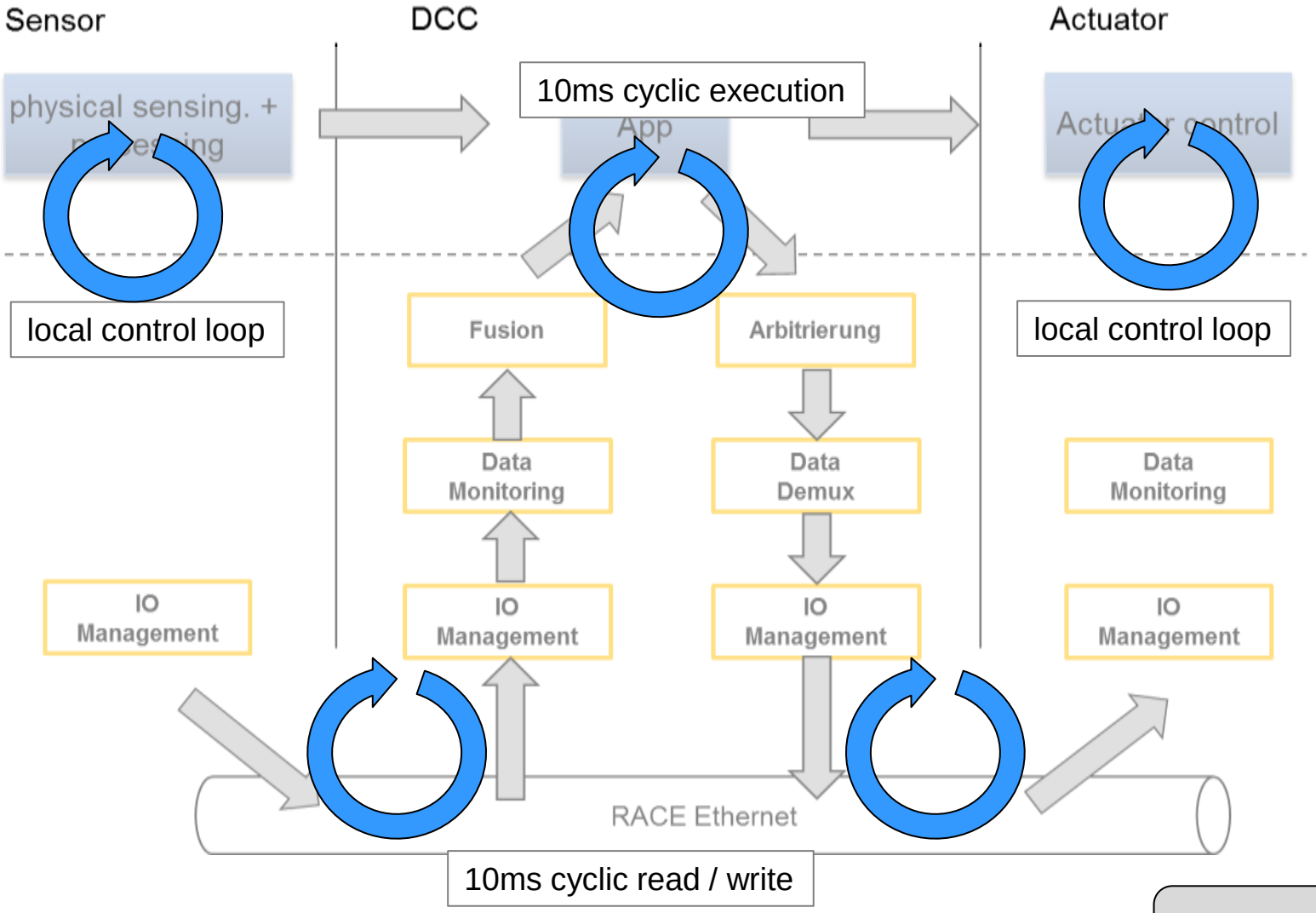
RTE: Data flow



Data-oriented communication



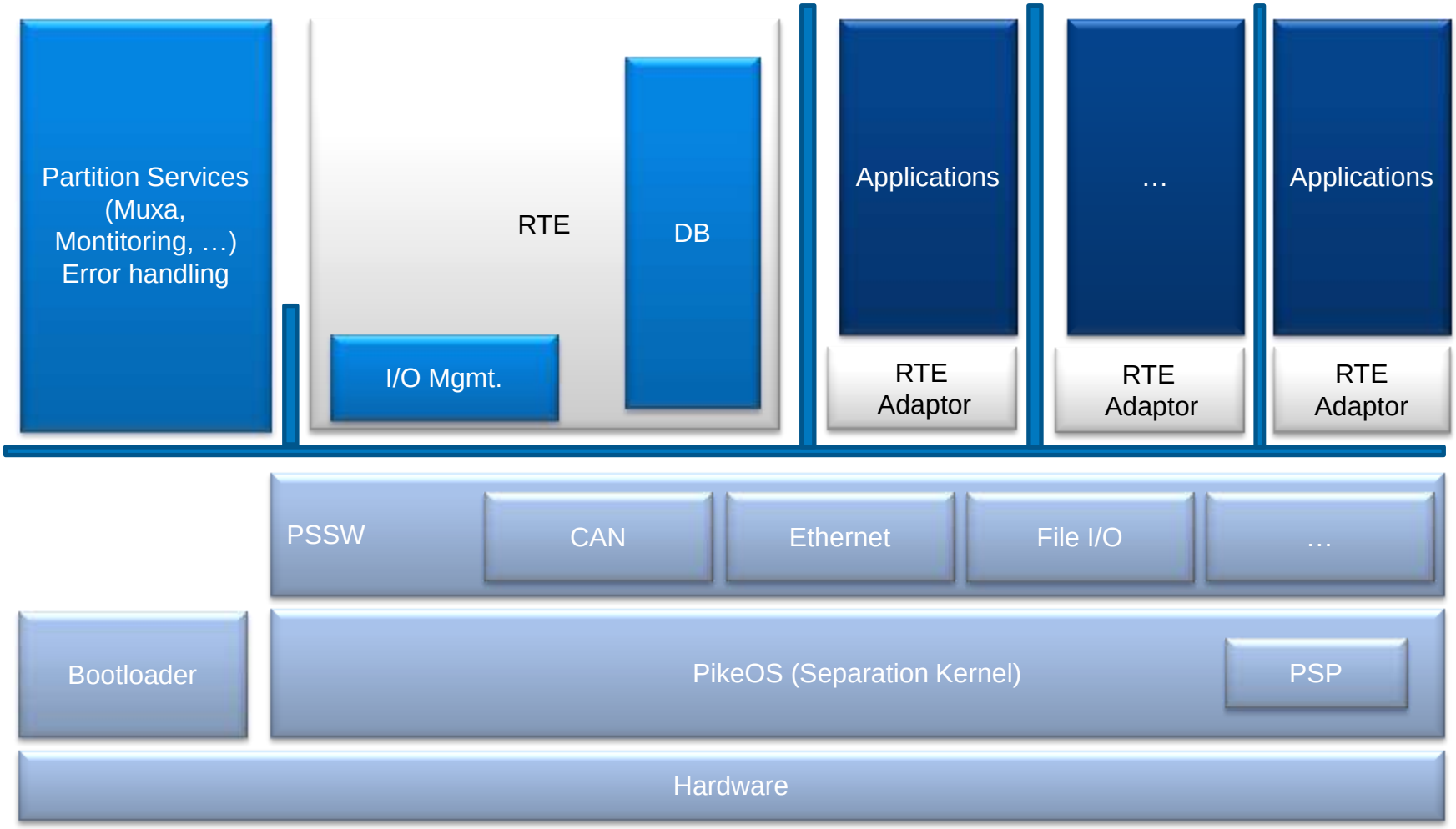
cyclic execution



long-running, event-triggered
not considered here

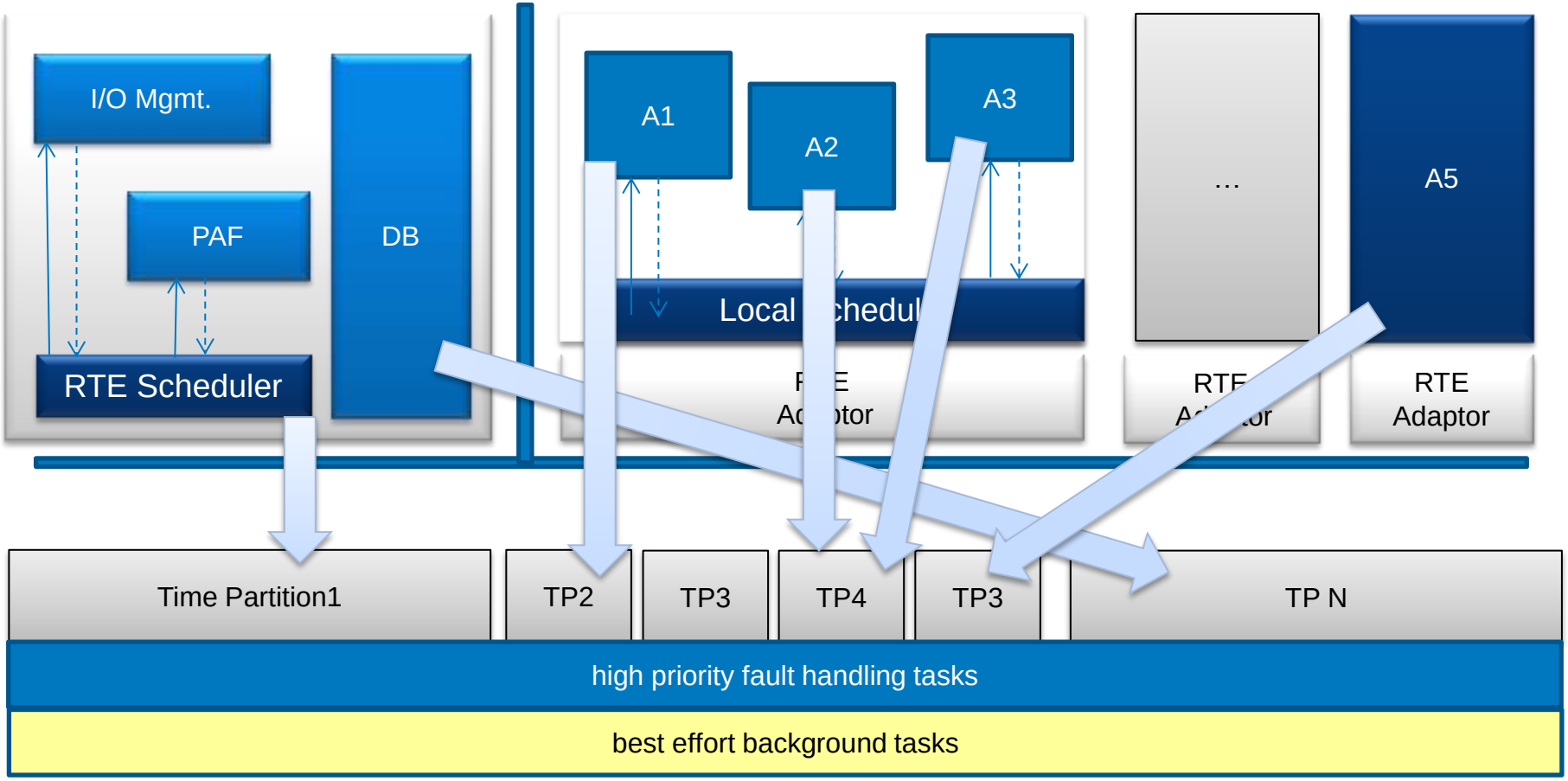
Partitioning in RACE

separate applications from each other and RTE



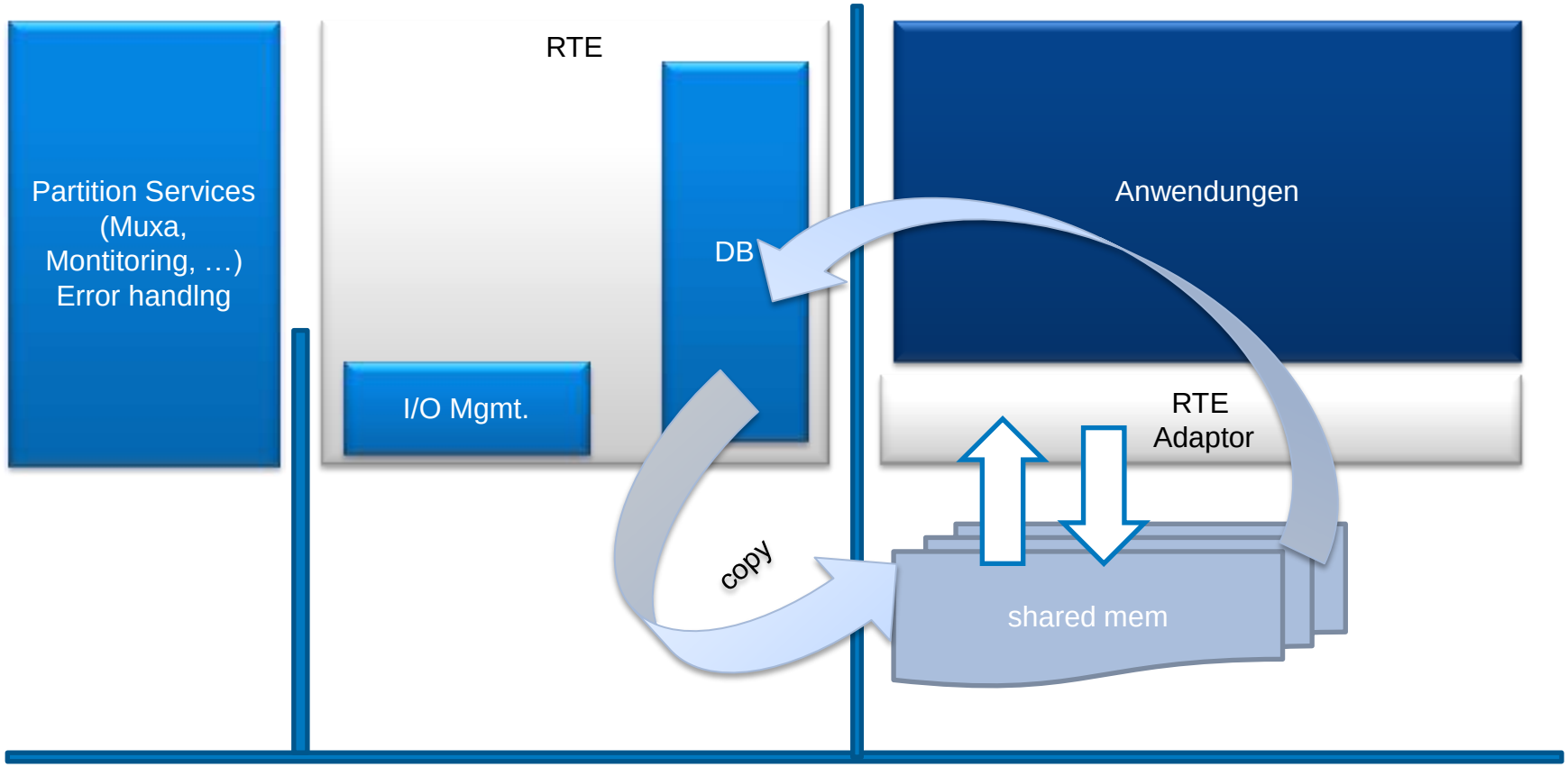
Time Partitioning

using PikeOS scheduling (ARINC 653 + priority based)



long running background tasks are always active

inter partition communication (RTE – App)



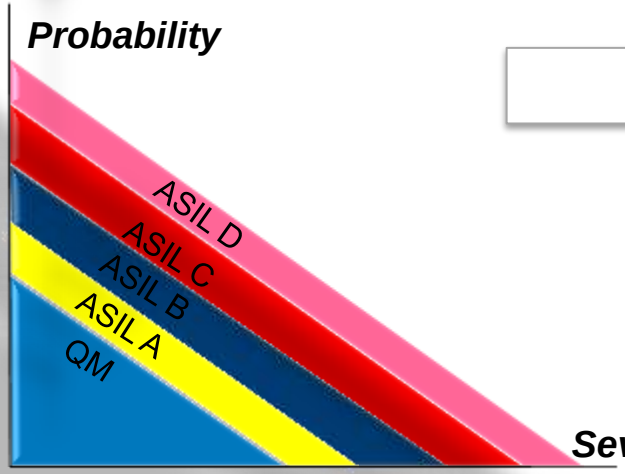
separated shared mem segment for each partition facilitates:
access control, auditability

Agenda

- Motivation
- RACE setup
- System Overview
- RACE Runtime Environment
- Safety Aspects
- Outlook

Application of the ISO within RACE

Acc. To TÜV SGS - documents



hazard & risk (H&R) assessment

ASIL ≥ A

no

development acc. to standard-process

yes

additional risk-reduction measures have to be applied

measures to avoid systematic faults

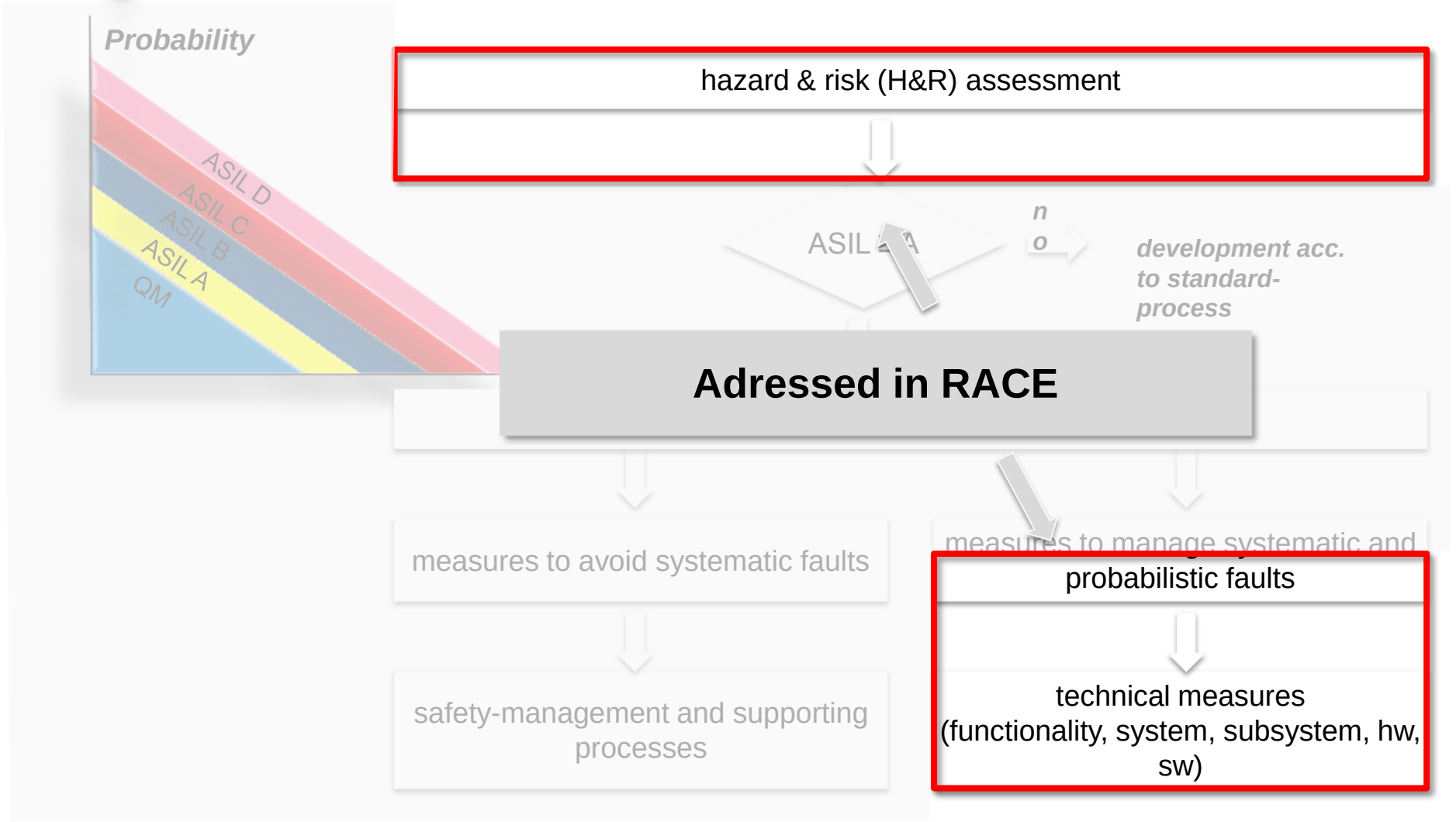
measures to manage systematic and probabilitsic faults

safety-management and supporting processes

technical measures (functionality, system, subsystem, hw, sw)

Application of the ISO within RACE

Acc. To TÜV SGS - documents

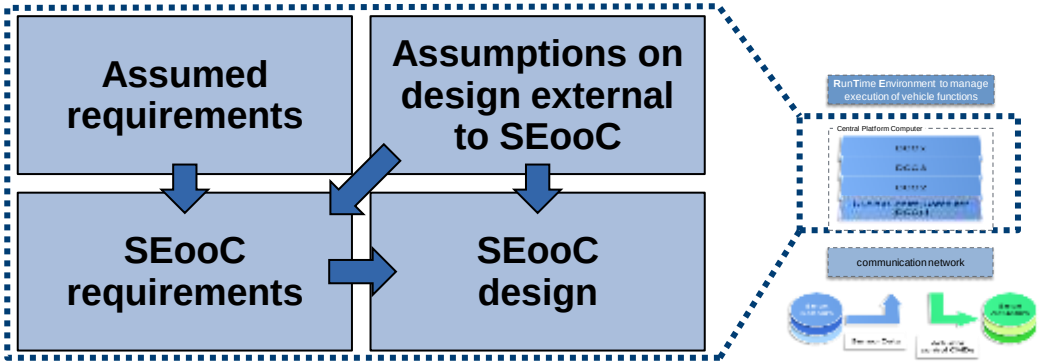


New ICT as safety-element out of context (SEooC)

Assumed requirements on central platform:

Req.: Execute any driver assistance functionality up to automated driving

Relation to SEooC (ISO 26262-10, Figure 17)



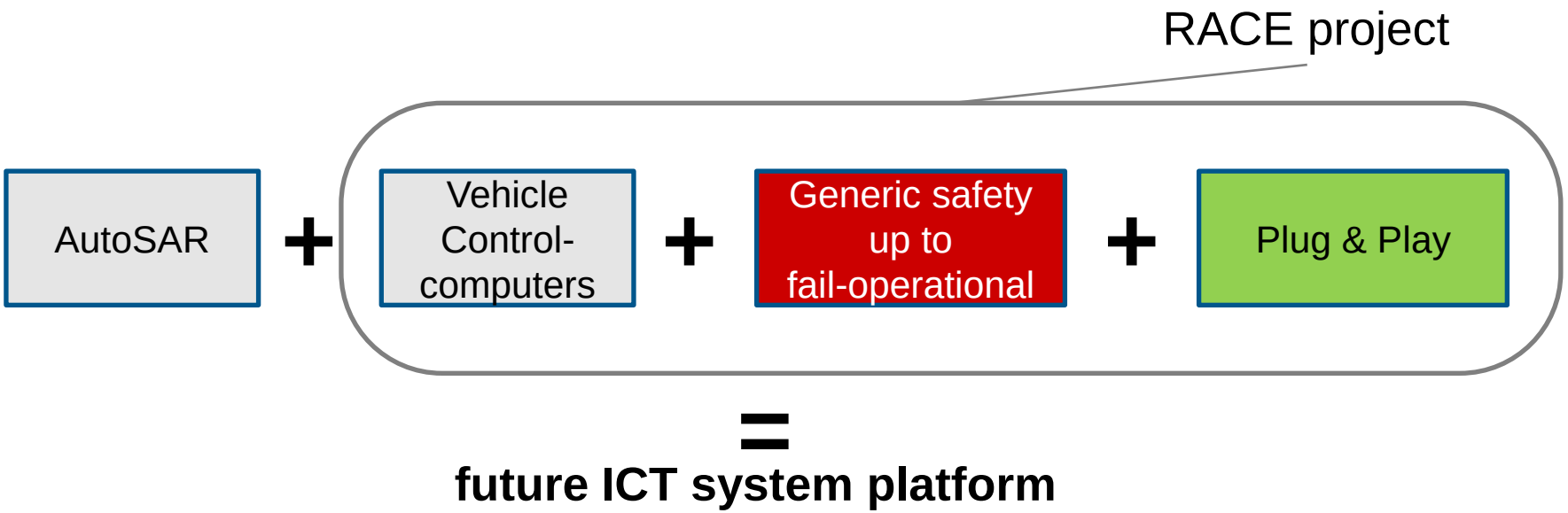
Failure ooC	Scenario	E	C	S	ASIL	Safe state	Fault-tolerance time (loss / invalid)
Uncontrolled command-output (incl. no output)	**Highway**	E4	C3	S3	D	None	50ms / 10ms
	Secondary road				D	None	50ms / 10ms
	Country road				D	None	50ms / 10ms

Agenda

- Motivation
- RACE setup
- System Overview
- RACE Runtime Environment
- Safety Aspects
- Outlook

The vision of the future ICT system platform

- The future ICT system platform facilitates fully automated driving and dynamic extensibility in field.
- The concept is based on an enlarged modularisation *) concept that leads to less end-to-end interface complexity.



*) to further reduce the dependancy from automotive functions to HW, topology, communication links but also to SW-functionality ensuring non-functional qualities.

the road ahead

not mentioned, but part of the project

- network protocols and Ethernet AVB Gen2 prototype
- ECU board design and low-level drivers
- test framework
- automotive functions …

R&D topics not addressed currently

- sensor fusion (how to boil data down)
- scale IO and processing bandwith
- car2X
- BYOD
- …

Join and make it happen!

Questions?

Ludger Fiege

ludger.fiege@siemens.com