Ethernet-based and function-independent vehicle control-platform

motivation, idea and technical concept fulfilling quantitative safety-requirements from ISO26262

Andreas Zirkler, Michael Armbruster, Ludger Fiege,
Gunter Freitag, Thomas Schmid, Gernot Spiegelberg,
Siemens AG Corporate Technology

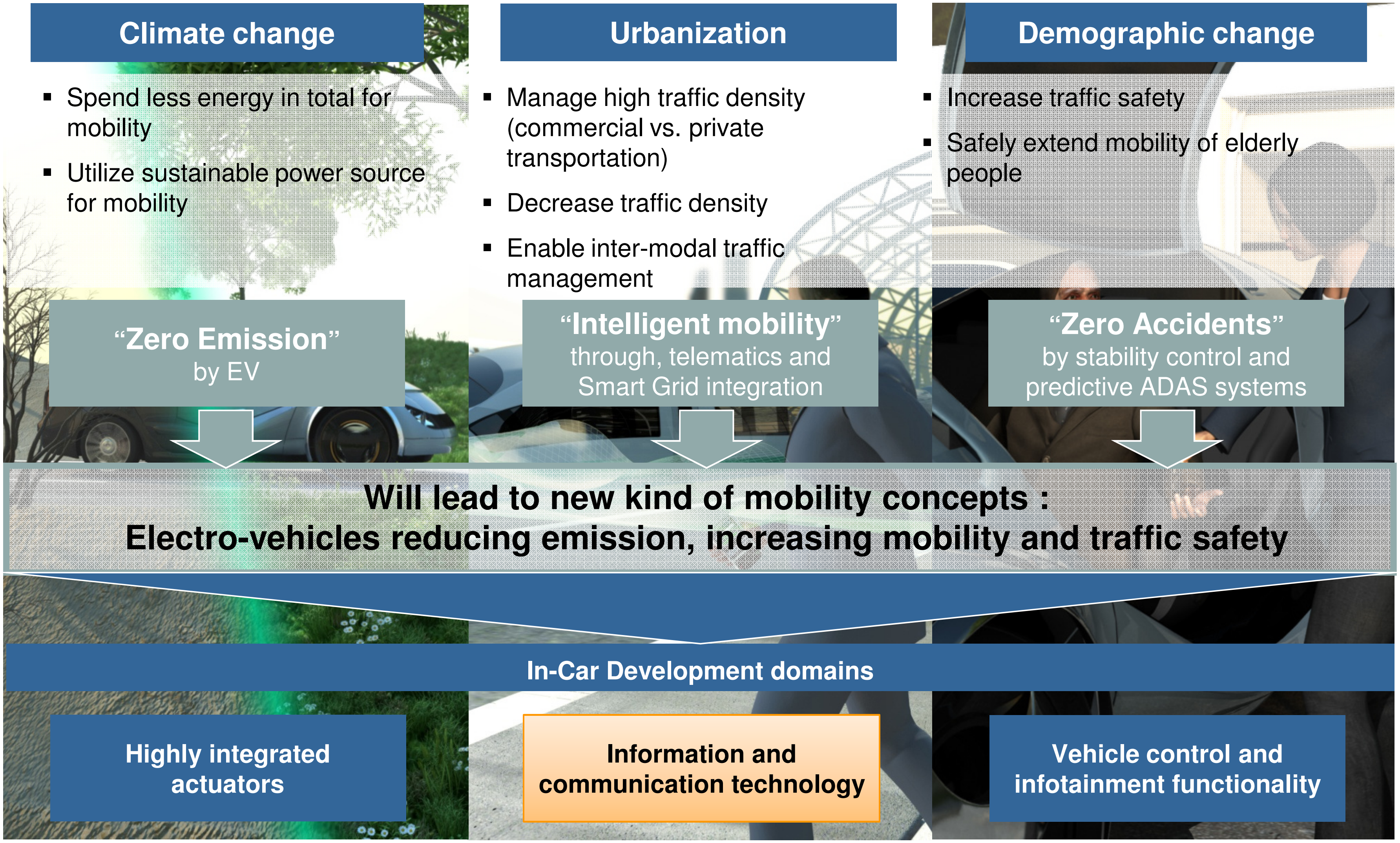
Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

race

Requirements for the vehicle ICT resulting from megatrends



Climate change

- Spend less energy in total for mobility
- Utilize sustainable power source for mobility

"Zero Emission"
by EV

Urbanization

- Manage high traffic density (commercial vs. private transportation)
- Decrease traffic density
- Enable inter-modal traffic management

"Intelligent mobility"
through, telematics and Smart Grid integration

Demographic change

- Increase traffic safety
- Safely extend mobility of elderly people

"Zero Accidents"
by stability control and predictive ADAS systems

Will lead to new kind of mobility concepts :
Electro-vehicles reducing emission, increasing mobility and traffic safety

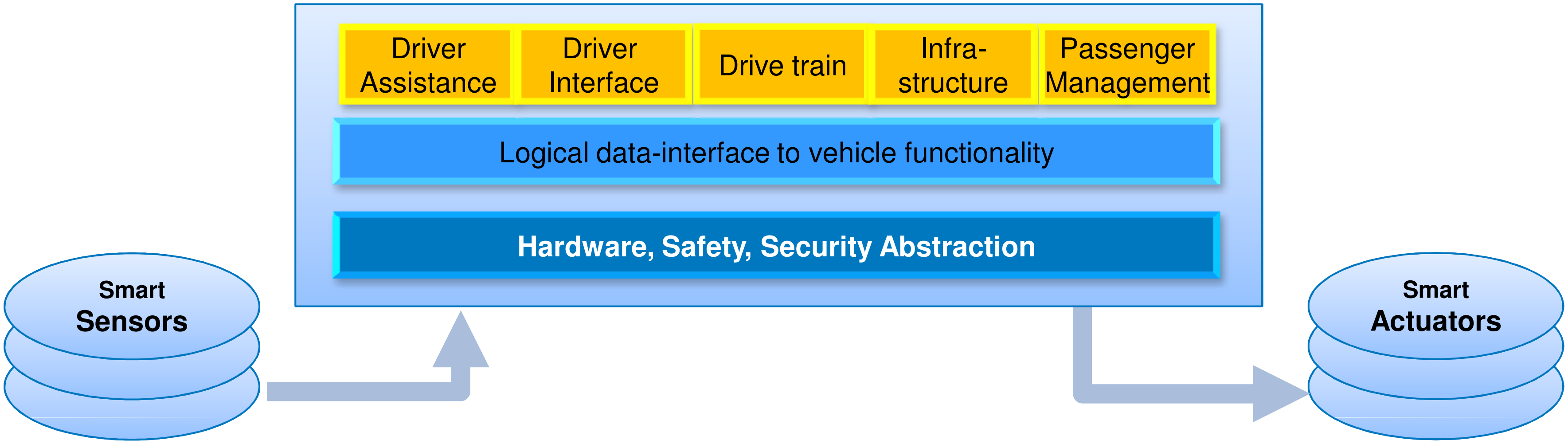
In-Car Development domains

Highly integrated actuators

Information and communication technology

Vehicle control and infotainment functionality

Idea: Logically centralized platform



New vehicle ICT:

- Scalable central processing units
- Intelligent sensors and actuators
- Middleware decouples functionality from safety, security and physical layers
- Support of mixed-criticality applications → one network for everything
- Plug & play for functions, sensors and actuators
- Support for incremental certifiability
- **Logically centralized platform** realizes vehicle control-functions up to ASIL-D

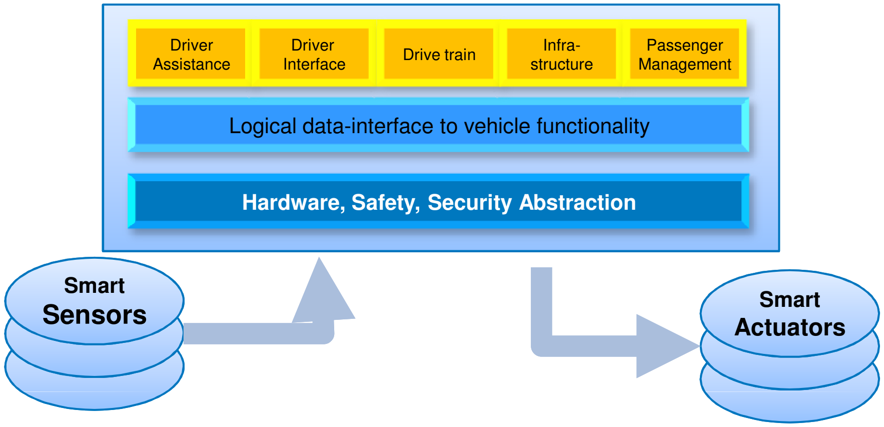
Requirements for the centralized platform

Requirements

- *Any driver assistance functions (e.g. auto-pilot)*
- *X-By-Wire (without mechanical backup)*

ooC Hazard & Risk Scenario

Hazard……………………..: uncontrolled / missing command output
ASIL……………………..….: D
Safe State………………..…..: none
Fault-tolerance time…….: 50 ms (exemplary)
Random HW failure rate..: < 10^{-8} h^{-1}



Platform must provide ASIL-D with fail-operational behavior

Fault-tolerant Architecture with aligned Communication Network

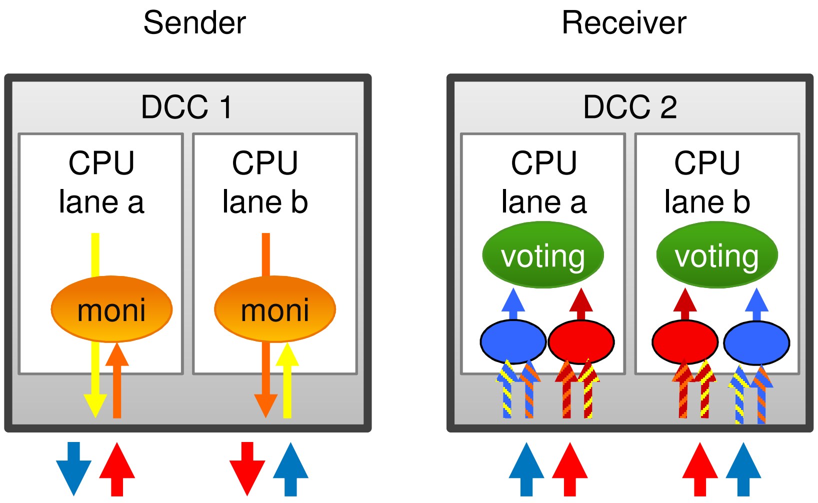
Realization of the Platform: N-Duplex

N-Duplex Platform:

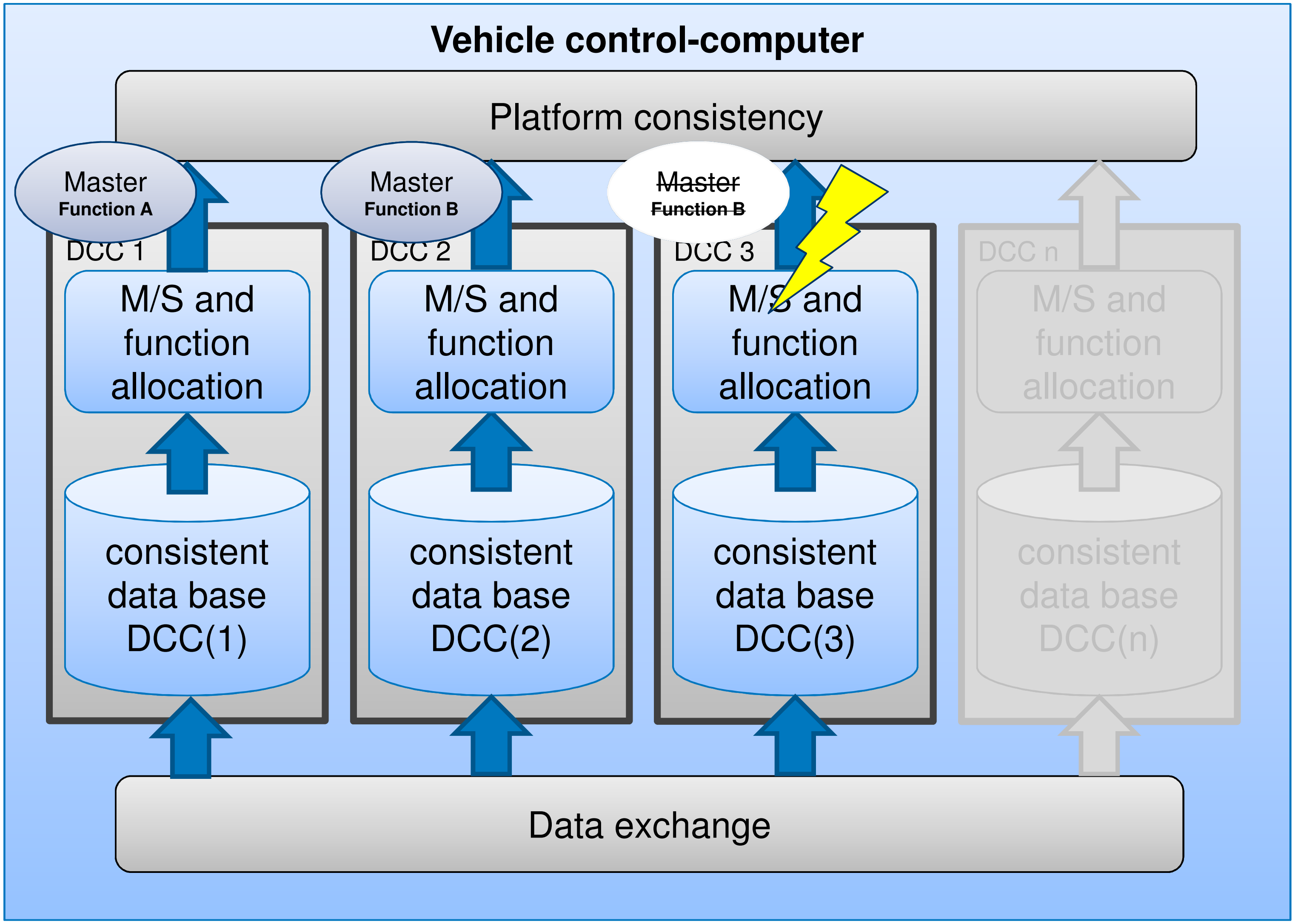
- Duplex Control Computer (DCC): ensures data integrity
- Duo-Duplex realizes fail-operational behavior
- N-Duplex realizes scalability (e.g. availability, performance)

Mode of operation:

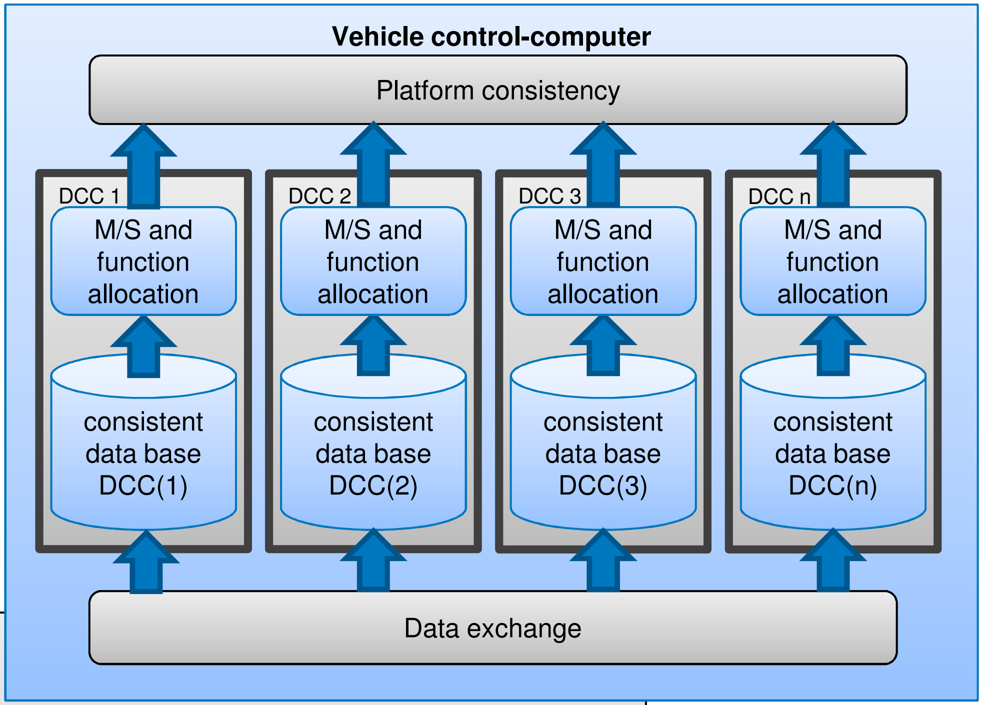
- DCCs realize uniqueness of control commands
- Aggregates (sensors and actuators) need no information about redundancy level or function allocation within the core platform.



Platform consistency:
unique Function- and M/S-allocation


Vehicle control-computer
Platform consistency
Master
Function A
Master
Function B
~~Master~~
~~Function B~~
DCC 1
DCC 2
DCC 3
DCC n
M/S and function allocation
M/S and function allocation
M/S and function allocation
M/S and function allocation
consistent data base DCC(1)
consistent data base DCC(2)
consistent data base DCC(3)
consistent data base DCC(n)
Data exchange

Platform consistency:
unique Function- and M/S-allocation

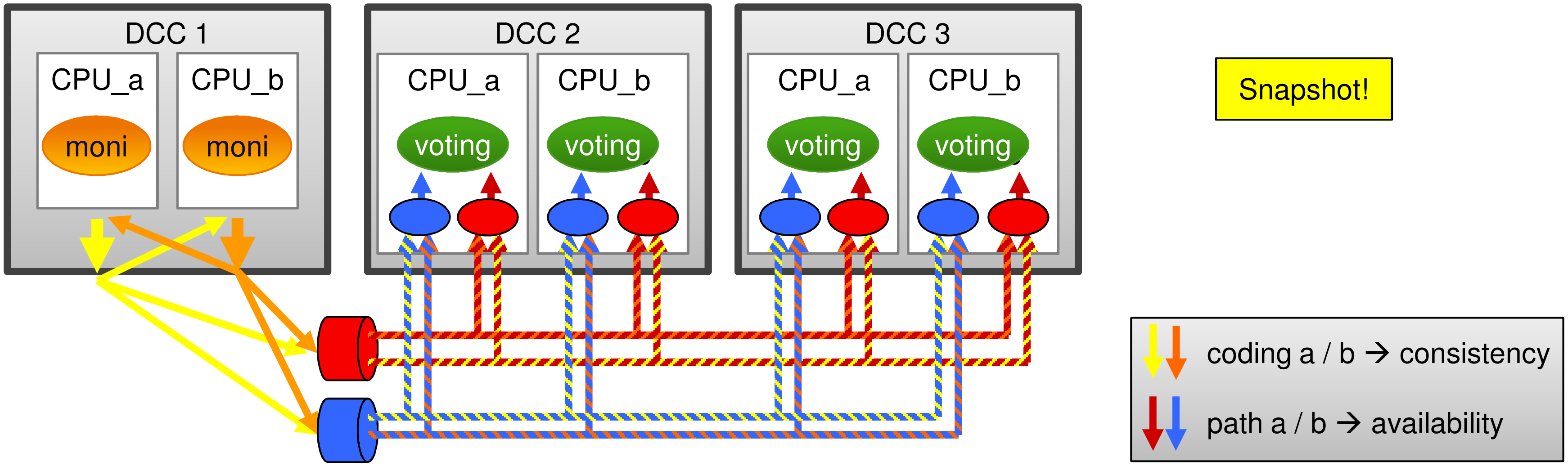

Vehicle control-computer
Platform consistency
DCC 1
M/S and function allocation
consistent data base DCC(1)
DCC 2
M/S and function allocation
consistent data base DCC(2)
DCC 3
M/S and function allocation
consistent data base DCC(3)
DCC n
M/S and function allocation
consistent data base DCC(n)
Data exchange

Safety requirements (estimated budget):
P{loss of platform consistency} < 1E-10

Design requirements:
- Multi-path data exchange to ensure availability
- X-lane data exchange (from lane a to lane b of one DCC) to ensure integrity (failure detection)

Resulting Requirements for the Communication Network

Logical view on communication relations:



Snapshot!

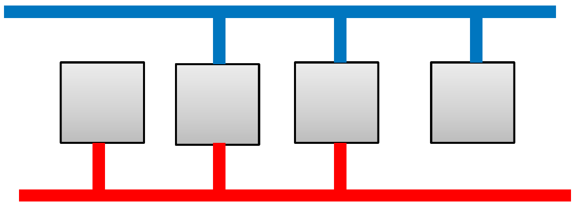
Resulting Requirements for the Communication Network:

No single failure must lead to a loss of data consistency and thus platform consistency, as ASIL-D functions with fail operational behavior shall be implemented

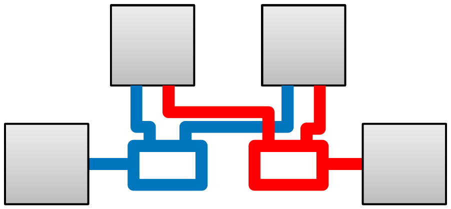
► **Multipath data exchange between DCCs is required!**
(To Aggregates, a single path is sufficient, if a redundant aggregate using a disjoint path is available.

Realization of the Multipath Network

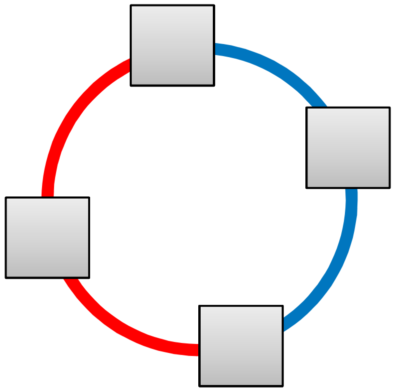
Parallel redundant bus:
Shared medium on each bus
Two physically independent busses
- High cabling effort
- „Slightly of specification“ failures possible



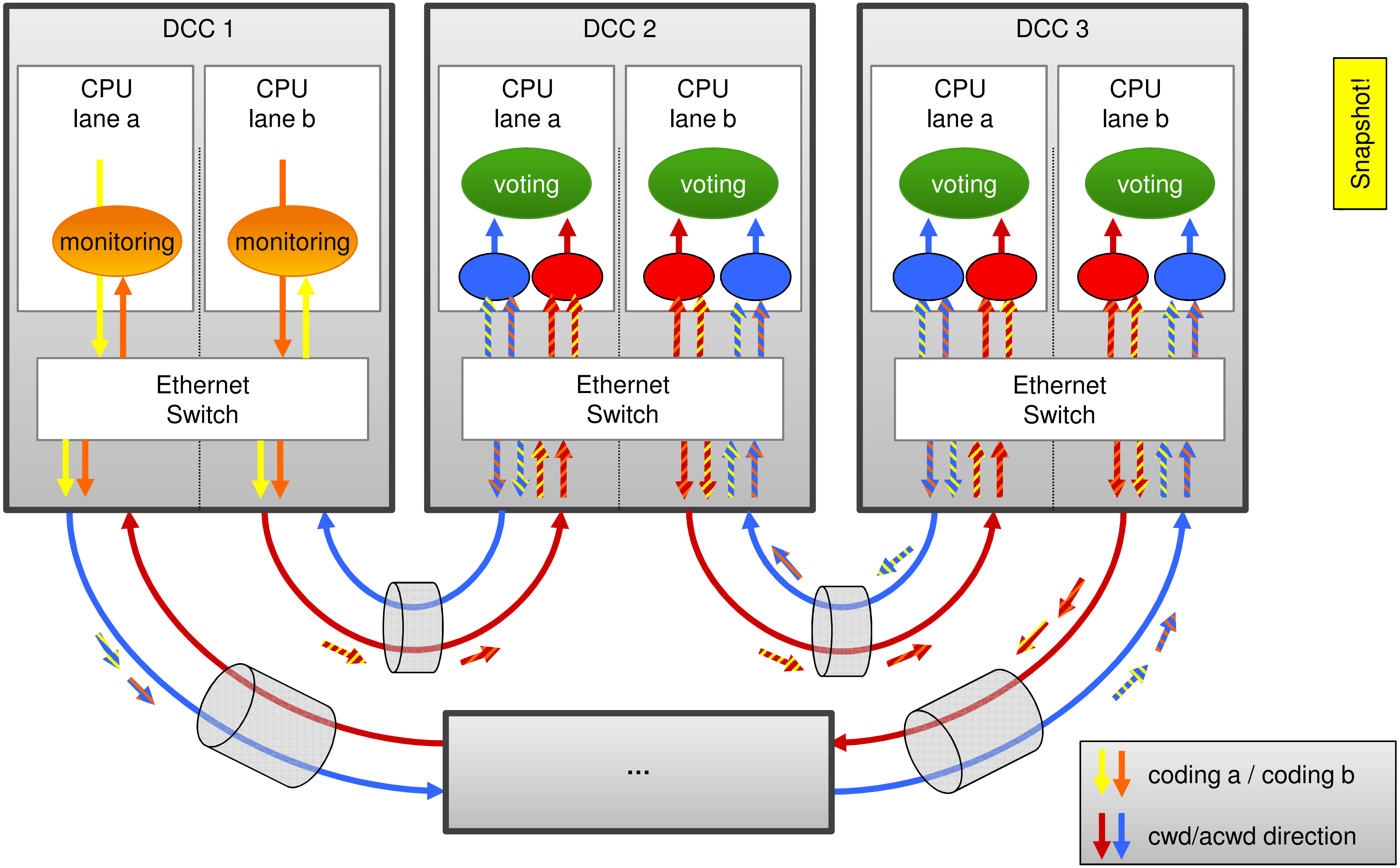
Switched Ethernet alternative 1:
redundant star architecture (AFDX)
- High cabling effort
+ Physically independent disjoint paths



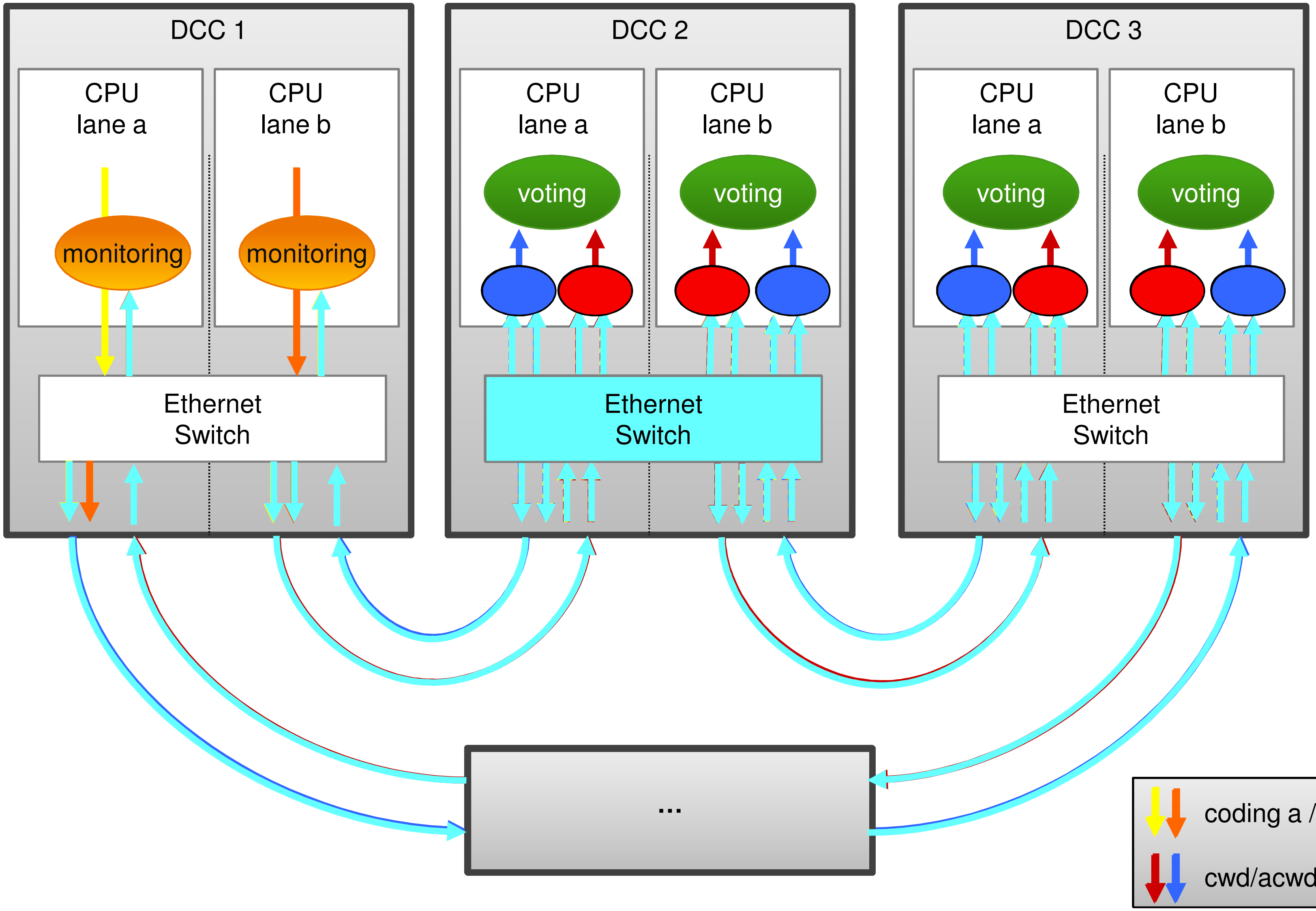
Switched Ethernet alternative 2:
ring topology (industry automation)
+ Disjoint paths
+ Low cabling effort
- Physical independence of paths is lost → additional effort



Consistent Communication in the Platform



Disadvantage: No physical independence

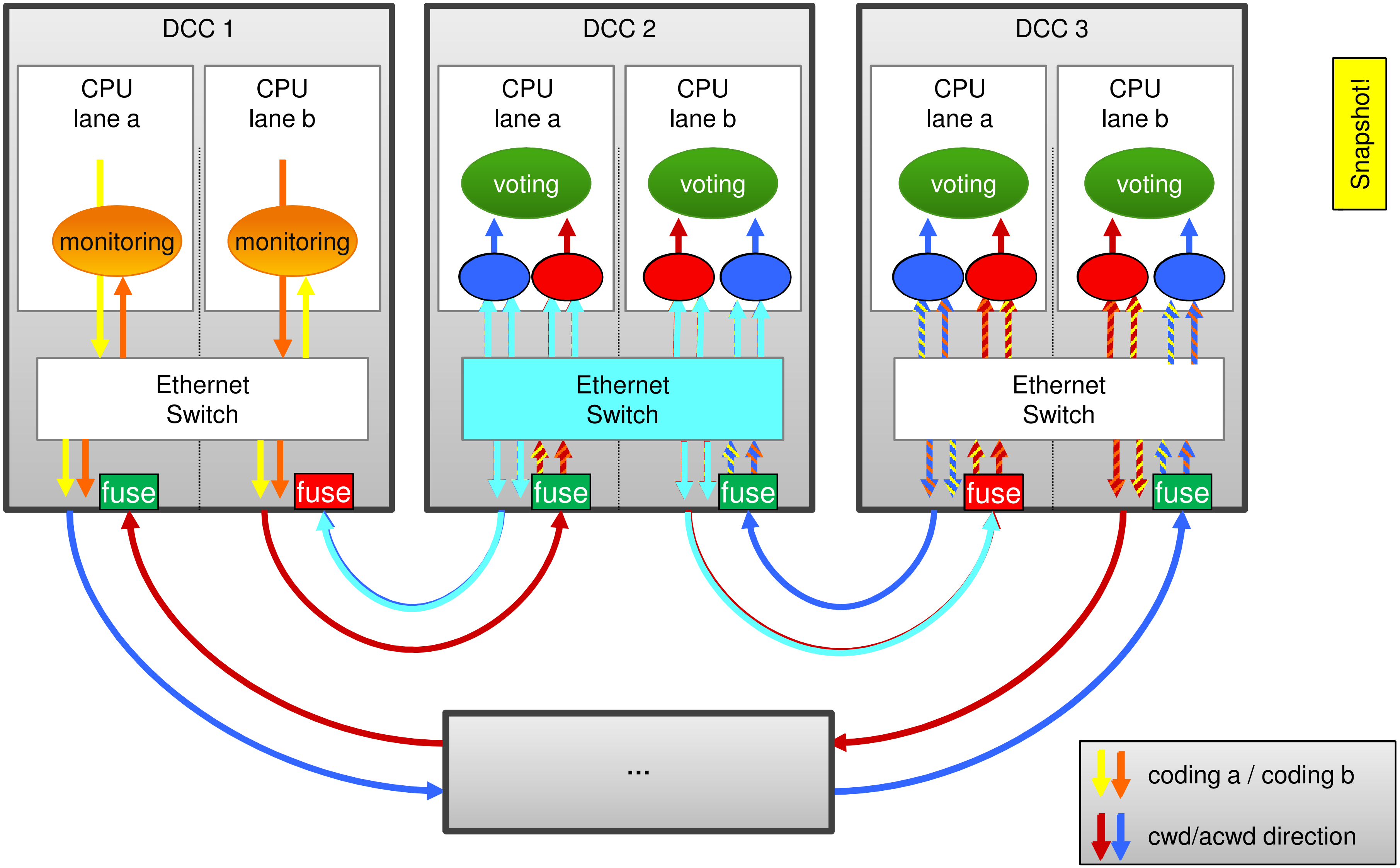


Snapshot!

↓↓ coding a / coding b

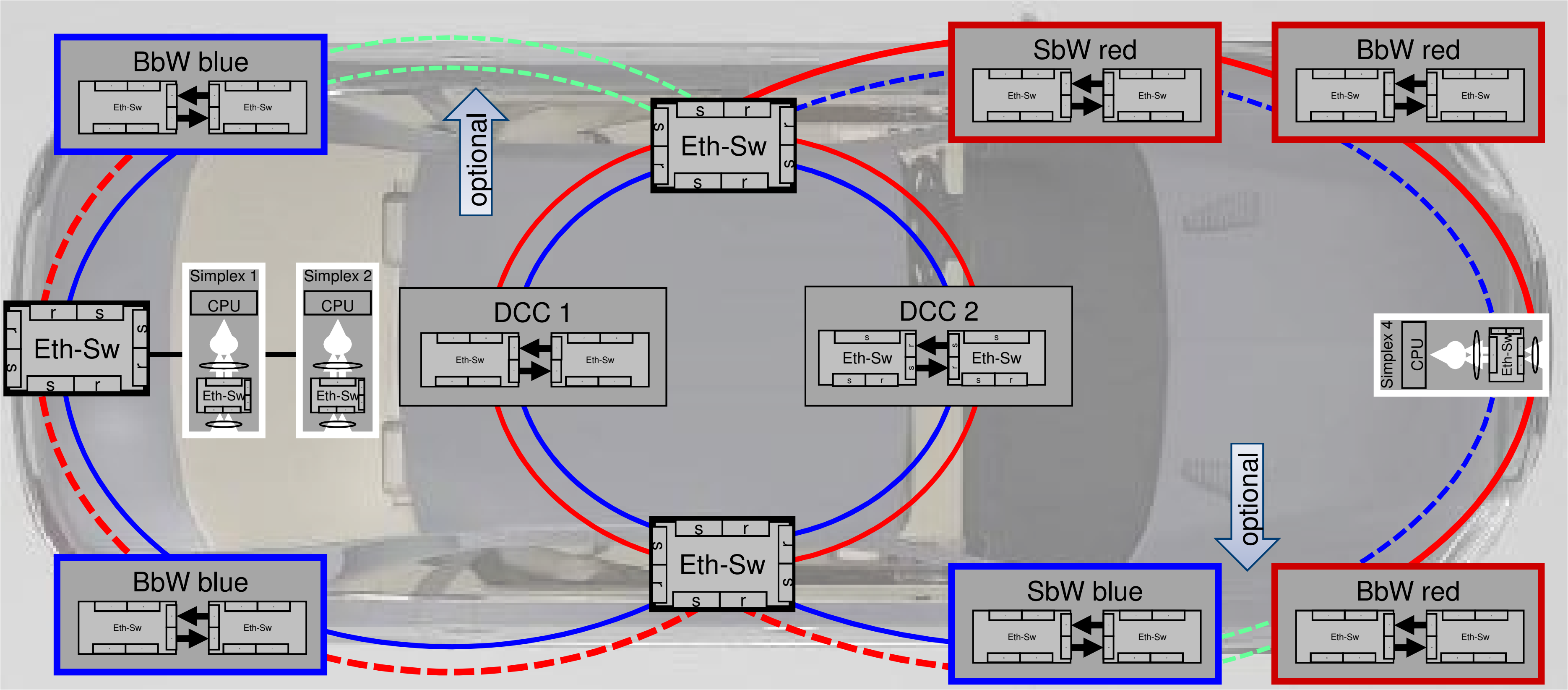
↓↓ cwd/acwd direction

Solution: Network Fuse



Snapshot!

Scalability for number of nodes and level of integrity



- Inner Ring with 2 to N DCCs
- Branches and/or outer rings for integration of aggregates
- Higher availability with low additional cabling effort

Thank you.

Andreas Zirkler,
Michael Armbruster,
Ludger Fiege,
Gunter Freitag,
Thomas Schmid,
Gernot Spiegelberg

Siemens AG Corporate Technology

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

race