Aspects and Challenges on the Way to upcoming Automated Cars

Dr. Stefan Poledna

IFIP 10.4 WG June, 26th 2015

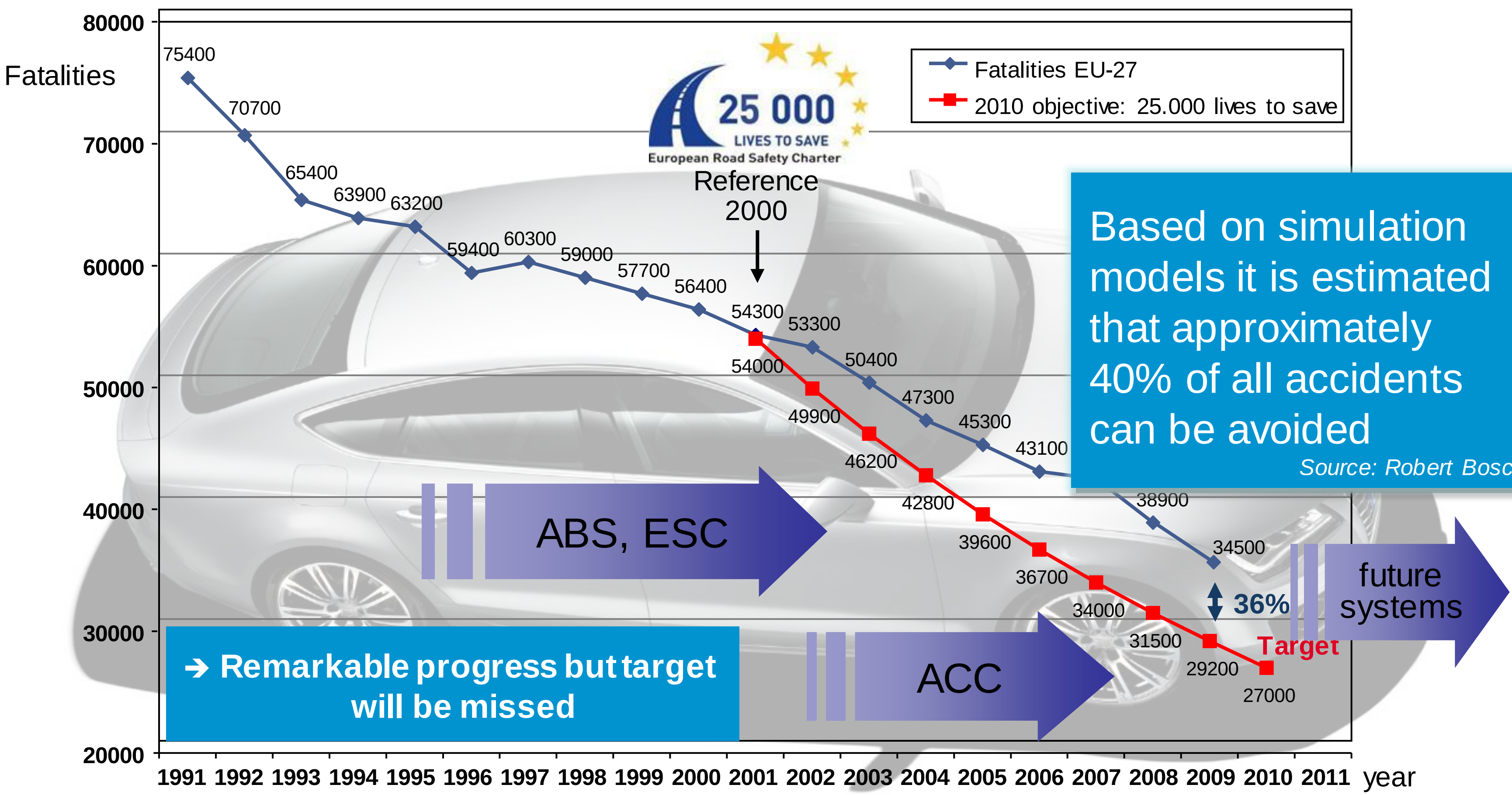
stefan.poledna@tttech.com

Content

Rationale for Autonomous Driving

Why Automated Driving: Safety

Evolution of European Road Fatalities (EU-27)



Source: CARE or national publications; EC Directorate General Energy and Transport December 2009

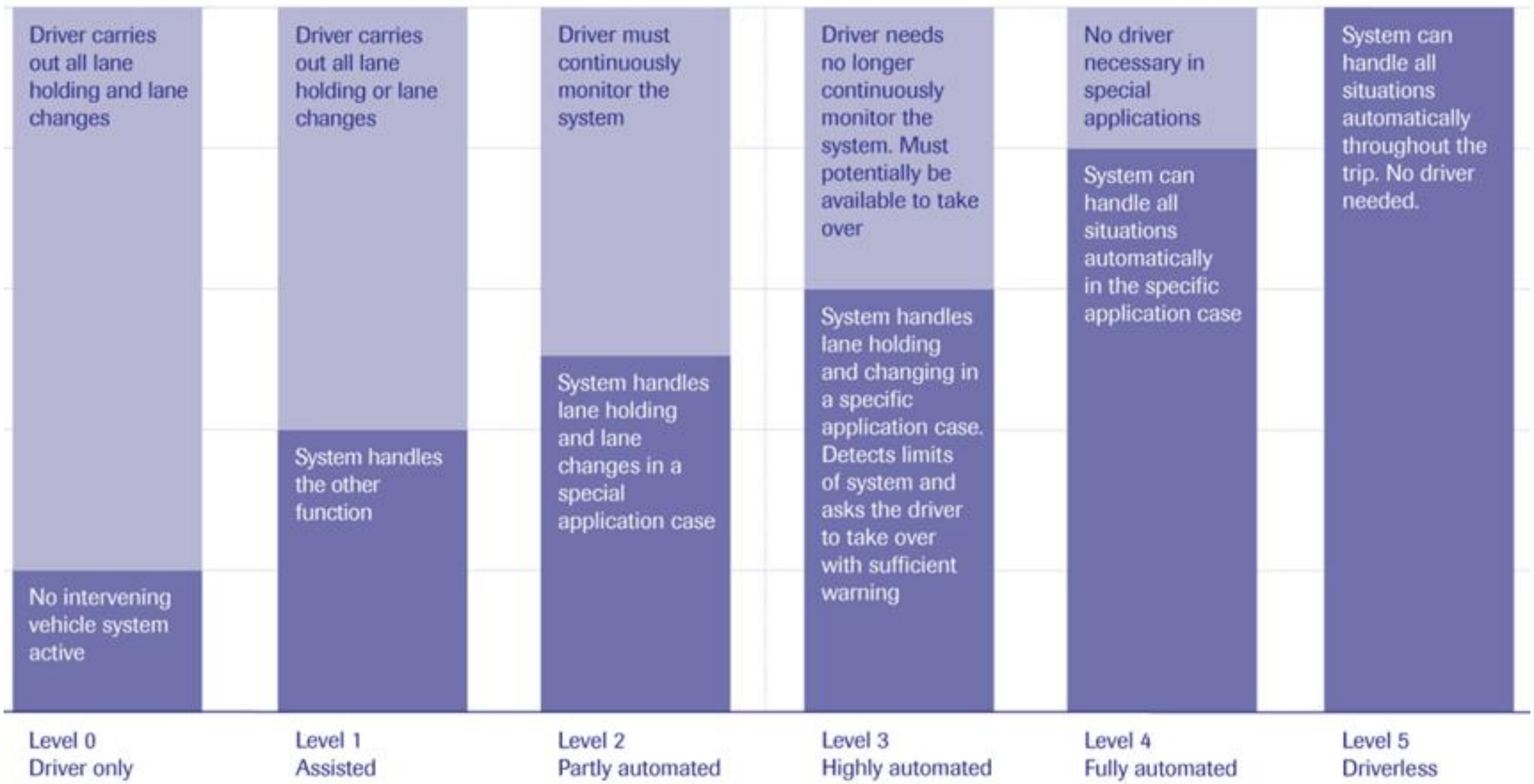
According to WHO: 50 million injuries in 2010, 1.2 million fatal injuries

Key Drivers: Quality Time & Economic Impact

System Classification

System Classification by VDA

TTTech



https://www.vda.de/de/themen/innovation-und-technik/automatisiertes-fahren.html

System Classification by NTSH

- **Level 0:** The driver completely controls the vehicle at all times.
- **Level 1:** Individual vehicle controls are automated, such as electronic stability control or automatic braking.
- **Level 2:** At least two controls can be automated in unison, such asadaptive cruise control in combination with lane keeping .
- **Level 3:** The driver can fully cede control of all safety-critical functions in certain conditions. The car senses when conditions require the driver to retake control and provides a “sufficiently comfortable transition time” for the driver to do so.
- **Level 4:** The vehicle performs all safety-critical functions for the entire trip, with the driver not expected to control the vehicle at any time. As this vehicle would control all functions from start to stop, including all parking functions, it could include unoccupied cars

"U.S. Department of Transportation Releases Policy on Automated Vehicle Development". *National Highway Traffic Safety Administration*. 30 May 2013. Retrieved18 December 2013

Level 3 is current challenge

TTTech

- **Level 0:** The driver completely controls the vehicle at all times.
- **Level 1:** Individual vehicle controls are automated, such as electronic stability control or automatic braking.
- **Level 2:** At least two controls can be automated in unison, such asadaptive cruise control in combination with lane keeping .
- **Level 3:** The driver can fully cede control of all safety-critical functions in certain conditions. The car senses when conditions require the driver to retake control and provides a "sufficiently comfortable transition time" for the driver to do so.
- **Level 4:** The vehicle performs all safety-critical functions for the entire trip, with the driver not expected to control the vehicle at any time. As this vehicle would control all functions from start to stop, including all parking functions, it could include unoccupied cars

State of the art

innovation

further out

"U.S. Department of Transportation Releases Policy on Automated Vehicle Development". *National Highway Traffic Safety Administration*. 30 May 2013. Retrieved18 December 2013

Challenges

Challenges ahead

- Safety – full authority over car by electronics
- Security – no unauthorized access or (software) change
- Fail-operational – cannot pass back control to driver immediately in case of component failures
- Software Integration – complex SW for different parties with different safety criticality level to be integrated on one ECU
- Re-use – Hugh invest in SW functionalities
- System complexity – system needs to be analyzable, understandable and evolvable
- Accelerated development – traditional automotive development process is too slow
- Addressing system cost

Automotive needs to go for Fail-Operational

TTTech

Driver takes over control

Driver needs some time to be prepared for take-over

- System is no longer fail-safe
- Fail-operational behavior for limited time required

or System needs to reach safe state

Sop car 0 km/h

Lane change to the side an stopping

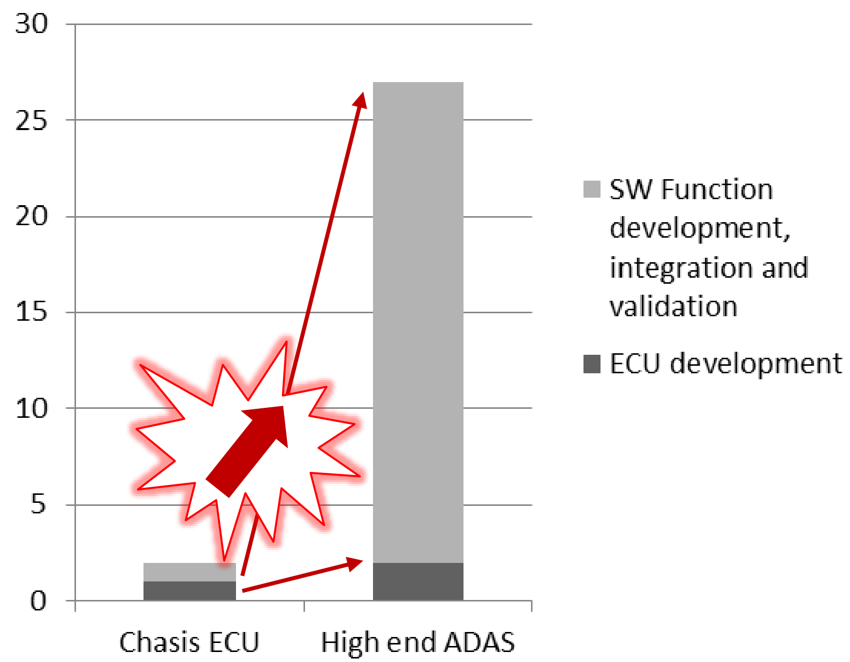
Reaching a safe state is limiting functions that can be automated

Cost Challenge is calling for Software Reuse

Cost shift from ECU hardware to SW function development.

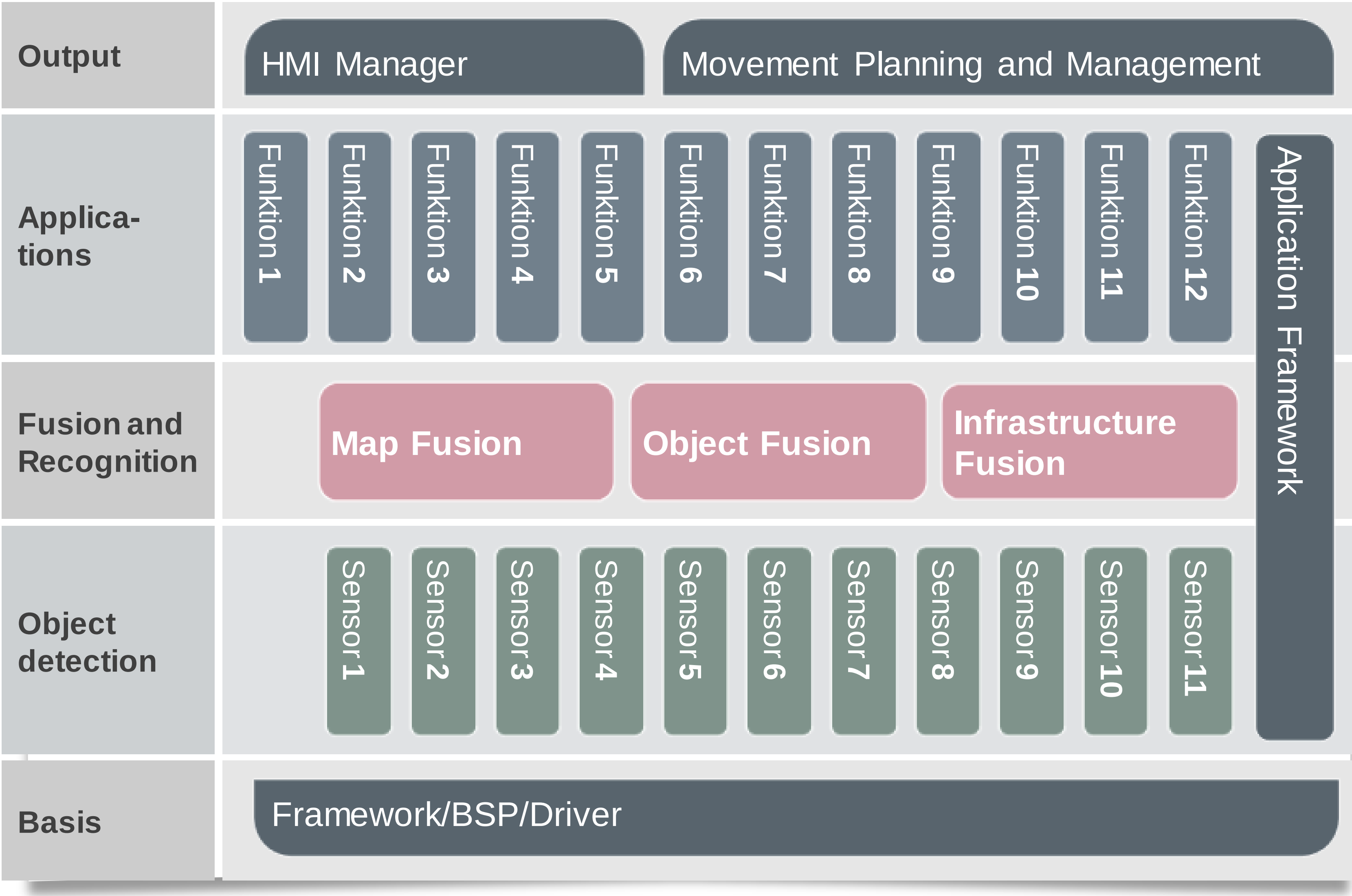
Development cost for advanced software functions, integration and validation is more than an order of magnitude higher than for conventional ECUs.

Comparison: ADAS Platform ECU vs. Chassis Control ECU

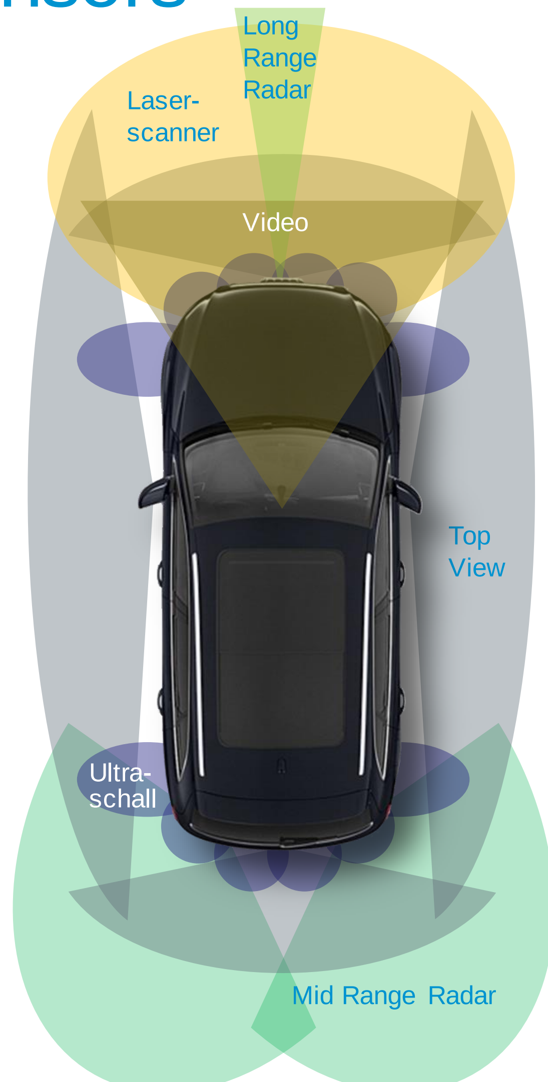


A Time-Triggered Platform Approach

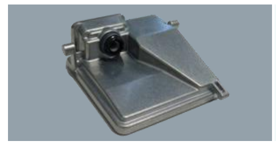
Layered Function Architecture with centralzed Fusion



Sensors



Long-Range-Radar (LRR 4)

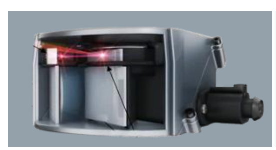


Video Camera

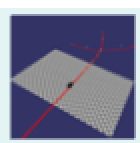
Top view Camera

Middle-Range-Radar (MRR)

Ultra Sonic



Laser Scanner

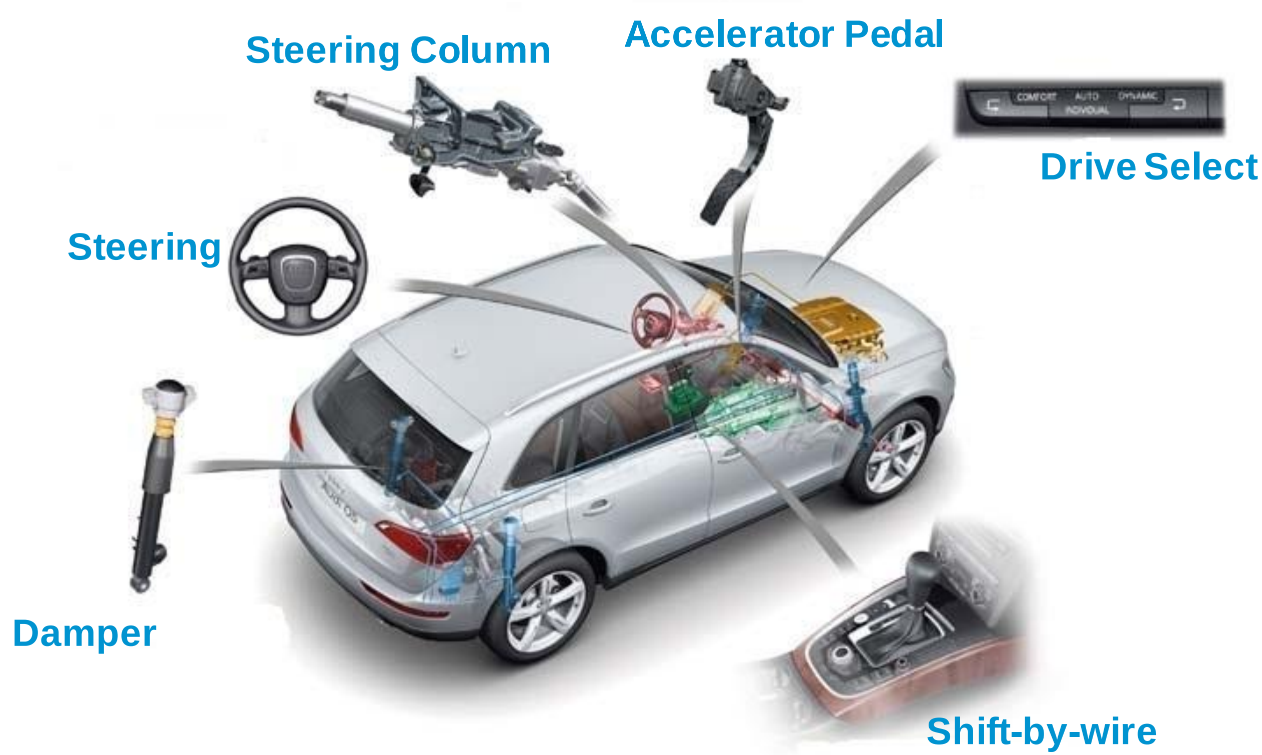


Predicitive Map Data
Car2x Connectivity

Actuators

Necessary Actuators for Automated Driving

- Electronic Stability Control
  - Hold management system
  - Decelleration management
- Powertrain Coordination
- Shift-by-Wire
- Electric Power Steering



Address Safety and Performance at the same time

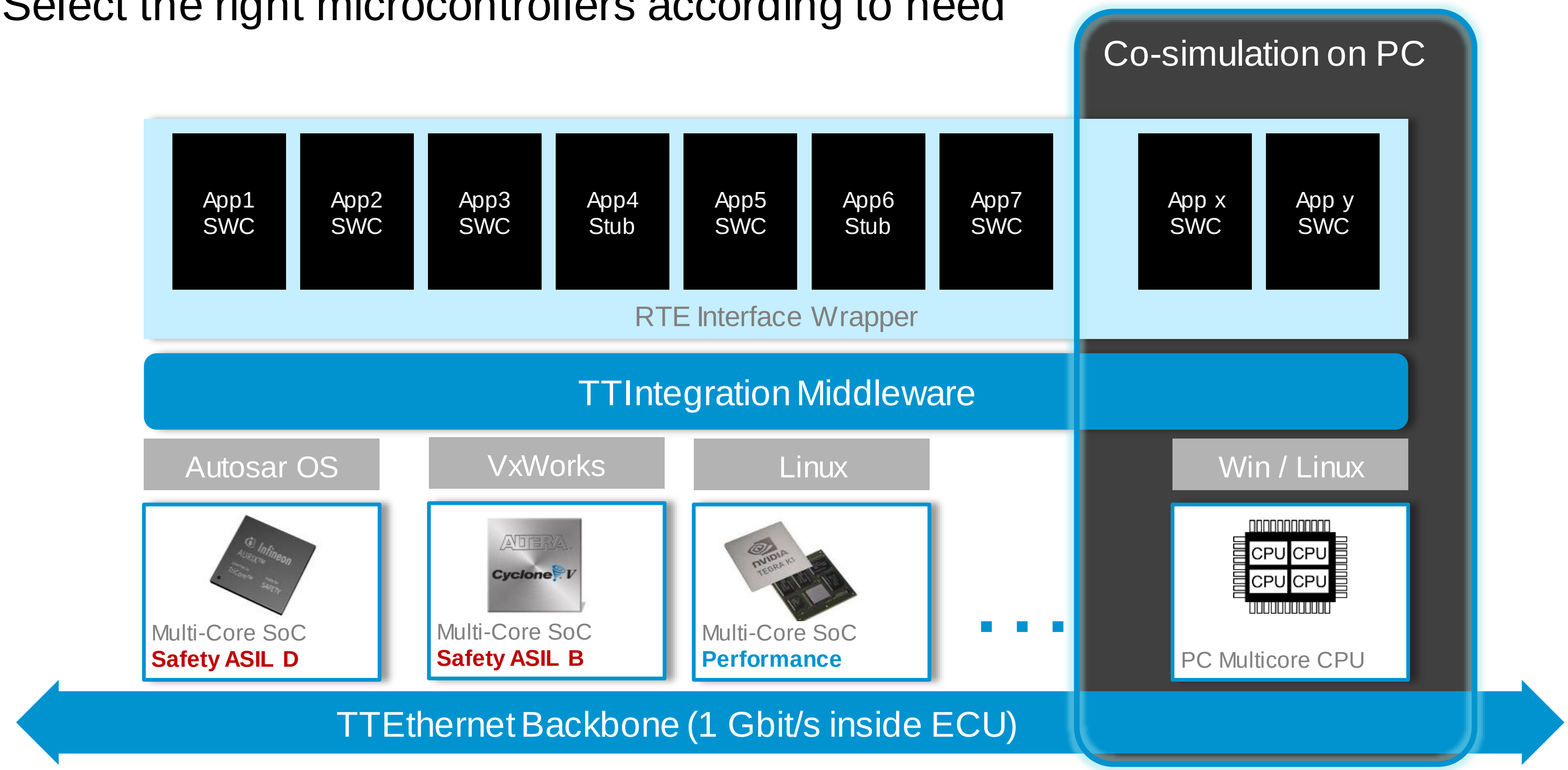
- Sensor processing and data fusion need highest performance
- Steering and braking require up to ASIL-D

Today's automotive safety micro-controllers do not fulfill the computing performance and memory requirements of high-end ADAS applications

zFAS Platform unites Safety *and* Performance

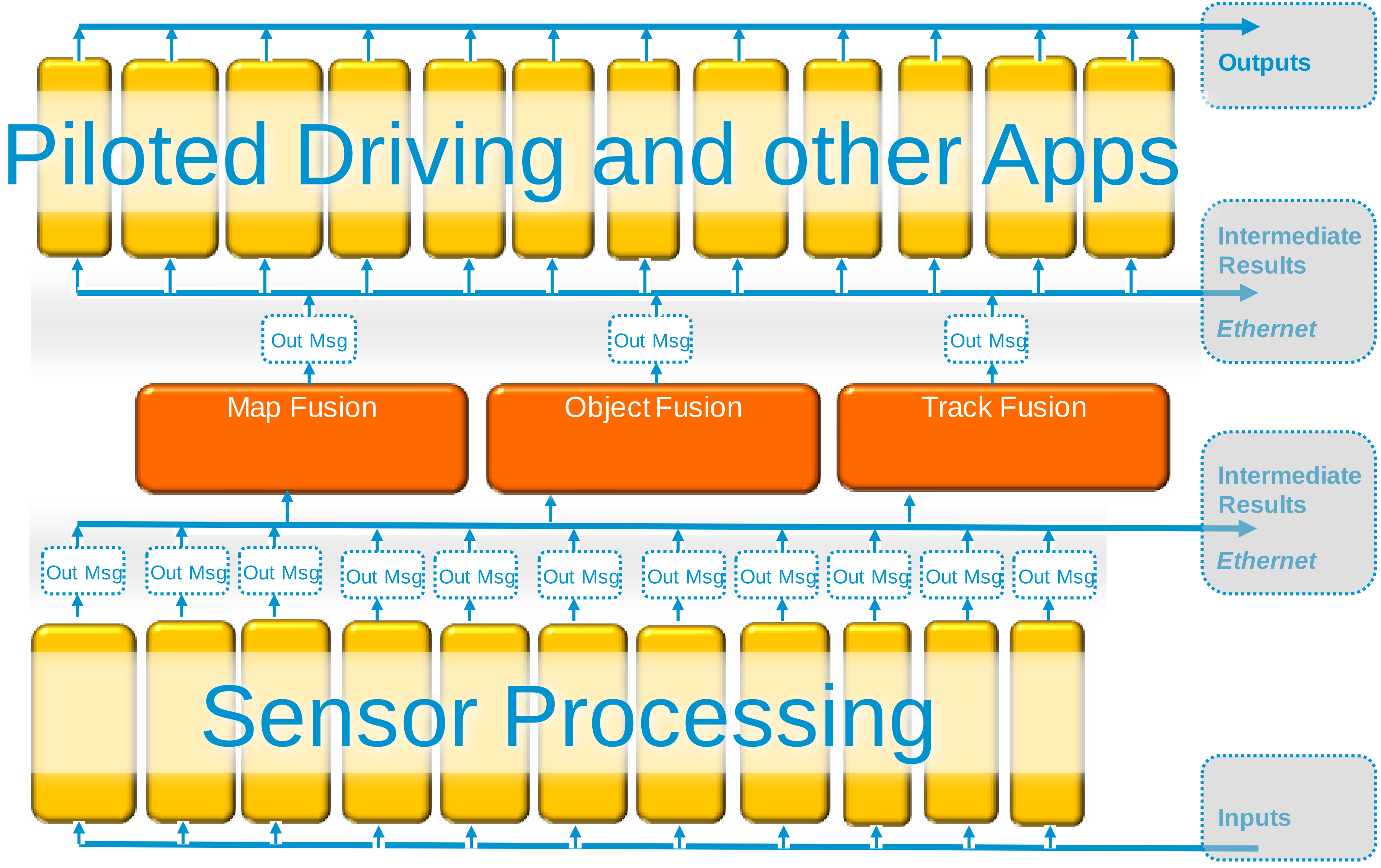
TTTech

Select the right microcontrollers according to need

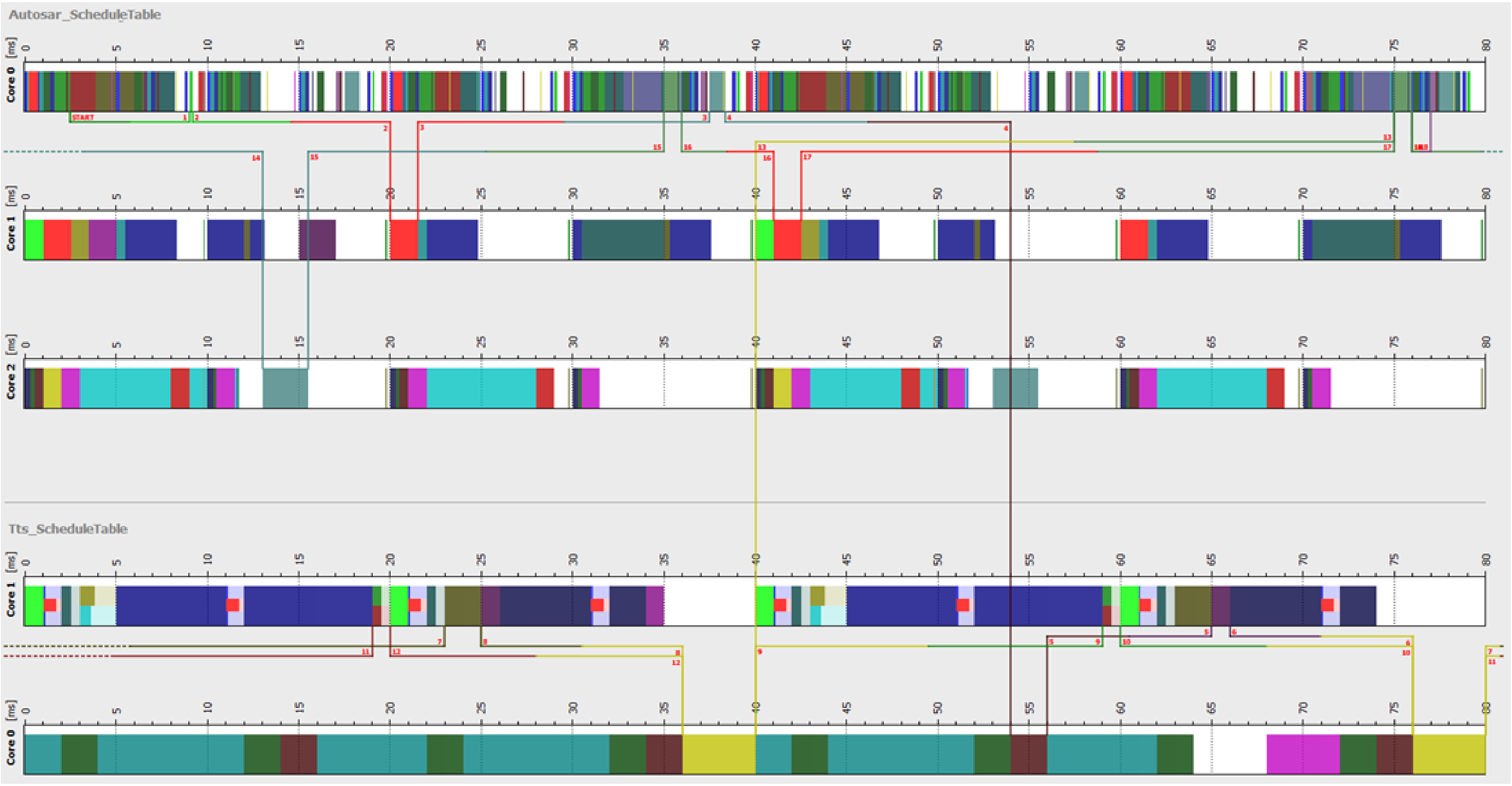


www.tttech.com

TTIntegration: Fully Location Transparent due to TTEthernet

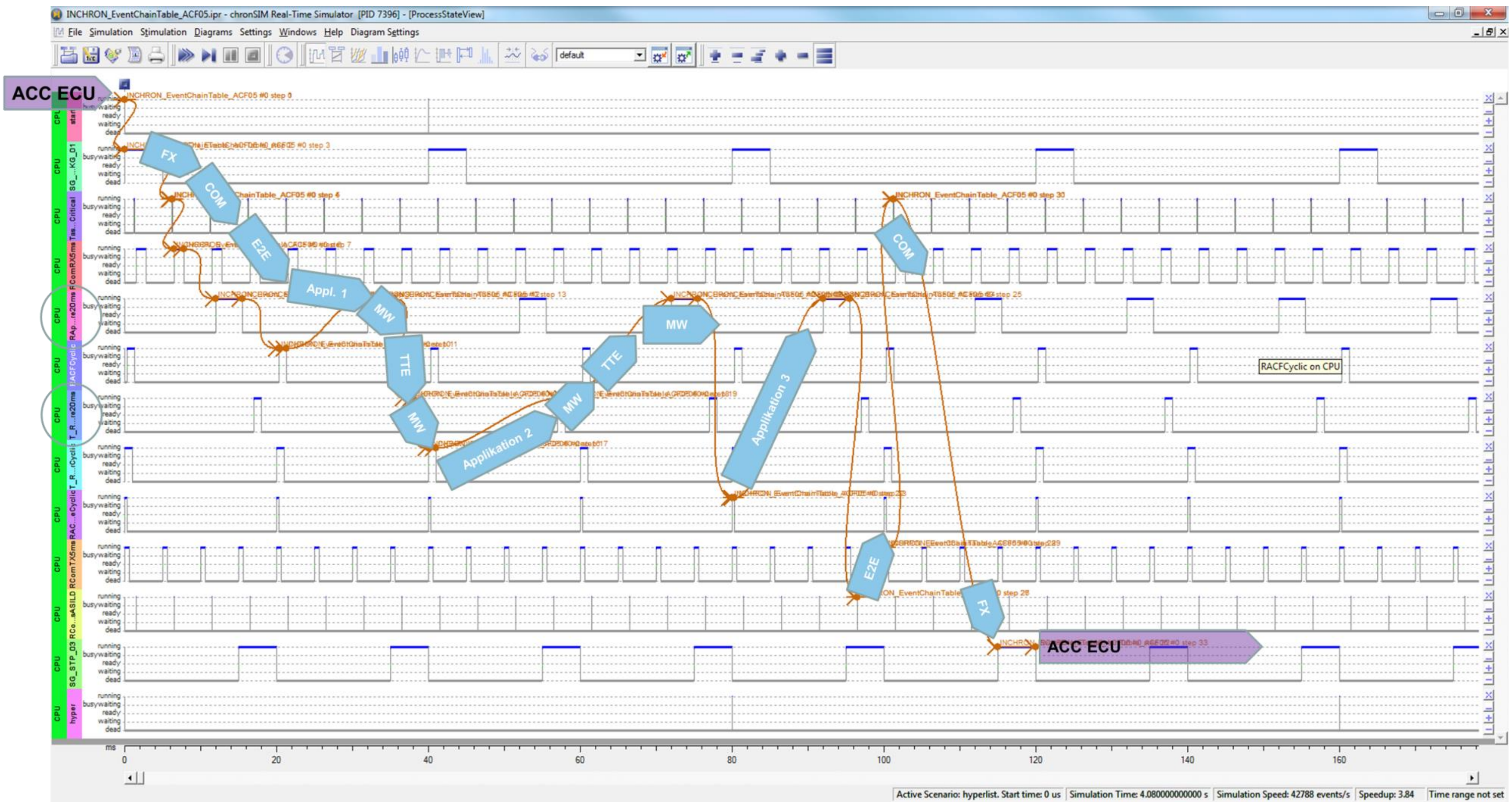


Time-Triggered Data Flows between Synchronous Cores

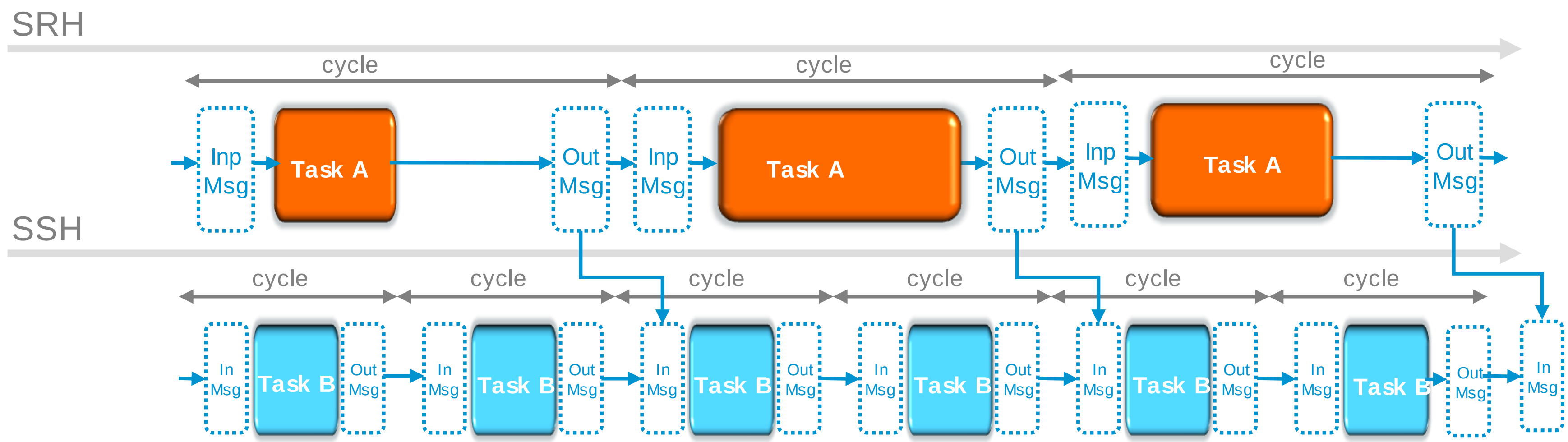


Time-Triggered Data Flow Example

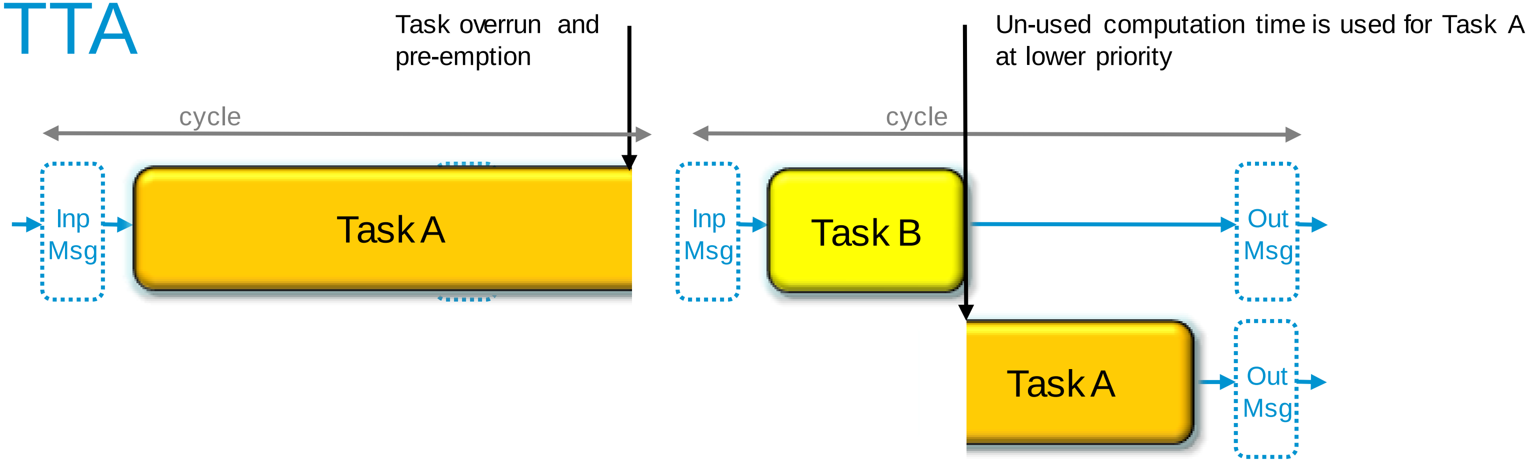
TTTech



TTIntegration: Scheduling and Communication based on TTEthernet



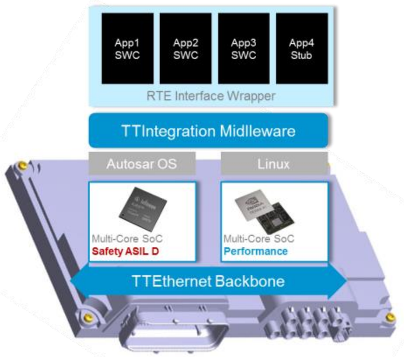
Soft TTA



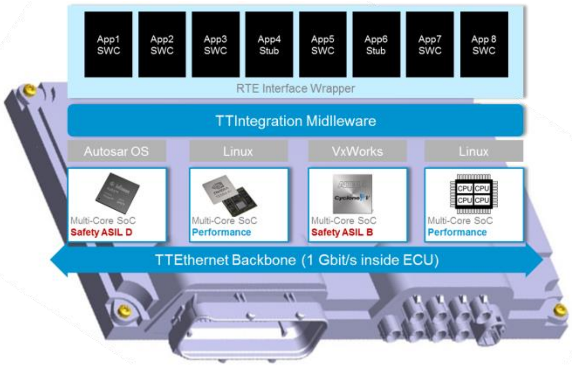
Scalability and Software Re-Use

The internal Ethernet backbone allows easy scaling between entry level and full featured versions as well as between single ECU and multi ECU versions.

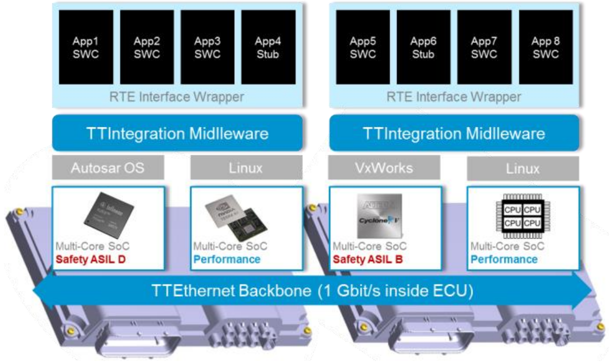
Small ECU – Reduced Functionality



Large ECU – Full Functionality



Split in two ECUs – Full Functionality



www.tttech.com

Integration of Software from several Sources

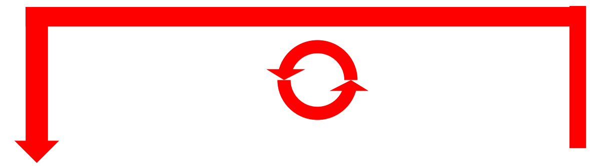
Requirements

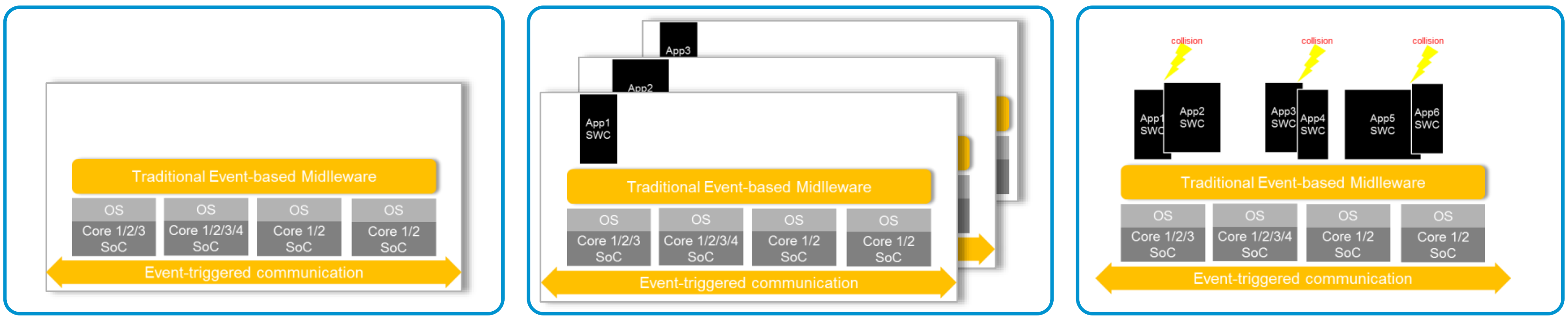
- Parallel development path for several teams developing application functions (OEM, Tier-1, SW providers)
- Seamless path between testing of individual SWCs SWCs
- Seamless path between SIL test and test on “real”
- Support of “Black-box integration process” for key a functions
  → IP-protection!

Traditional Integration Approach (best avoided)

TTTech

4. Conflicts are reported back to function SW suppliers, applications have to be modified to meet the system‘s timing restrictions





1. Integration of platform without configuring execution frames

2. Applications are integrated and tested individually by SWC suppliers without timing and memory restrictions

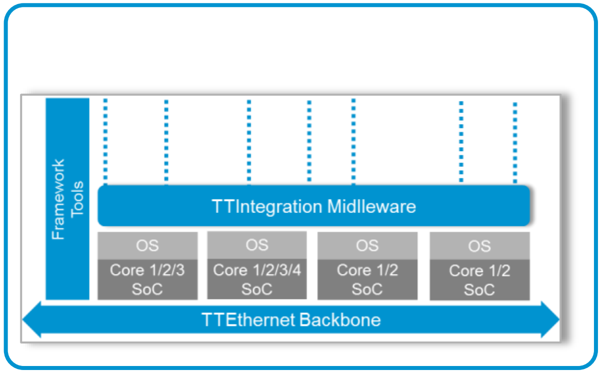
3. All applications are integrated by the SW-integrator on the platform; conflicts start immediately as it is not clear who is causing problems and why

www.tttech.com

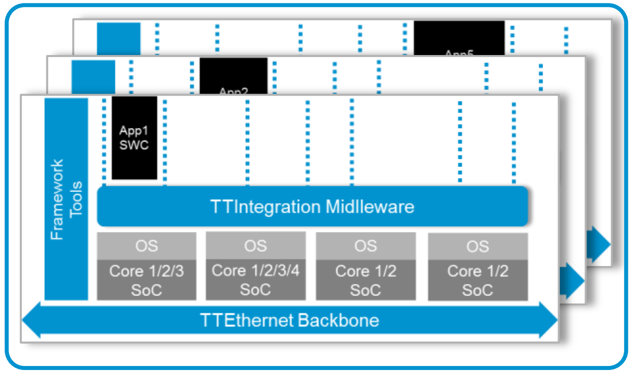
Robust Deterministic Integration

TTTech

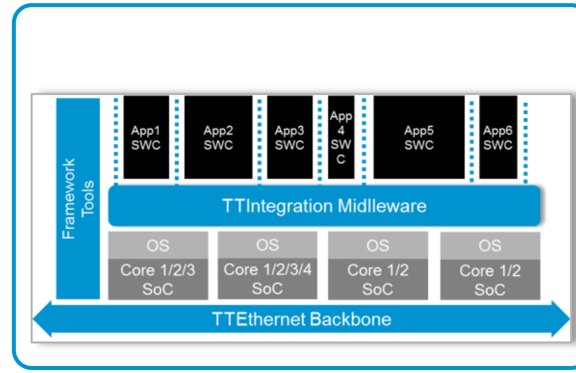
Robustness through clear allocation and monitoring of resources (memory, CPU, communication)



Parallel Integration to speed-up software development of multiple-software suppliers



Complete software integrated for functional testing

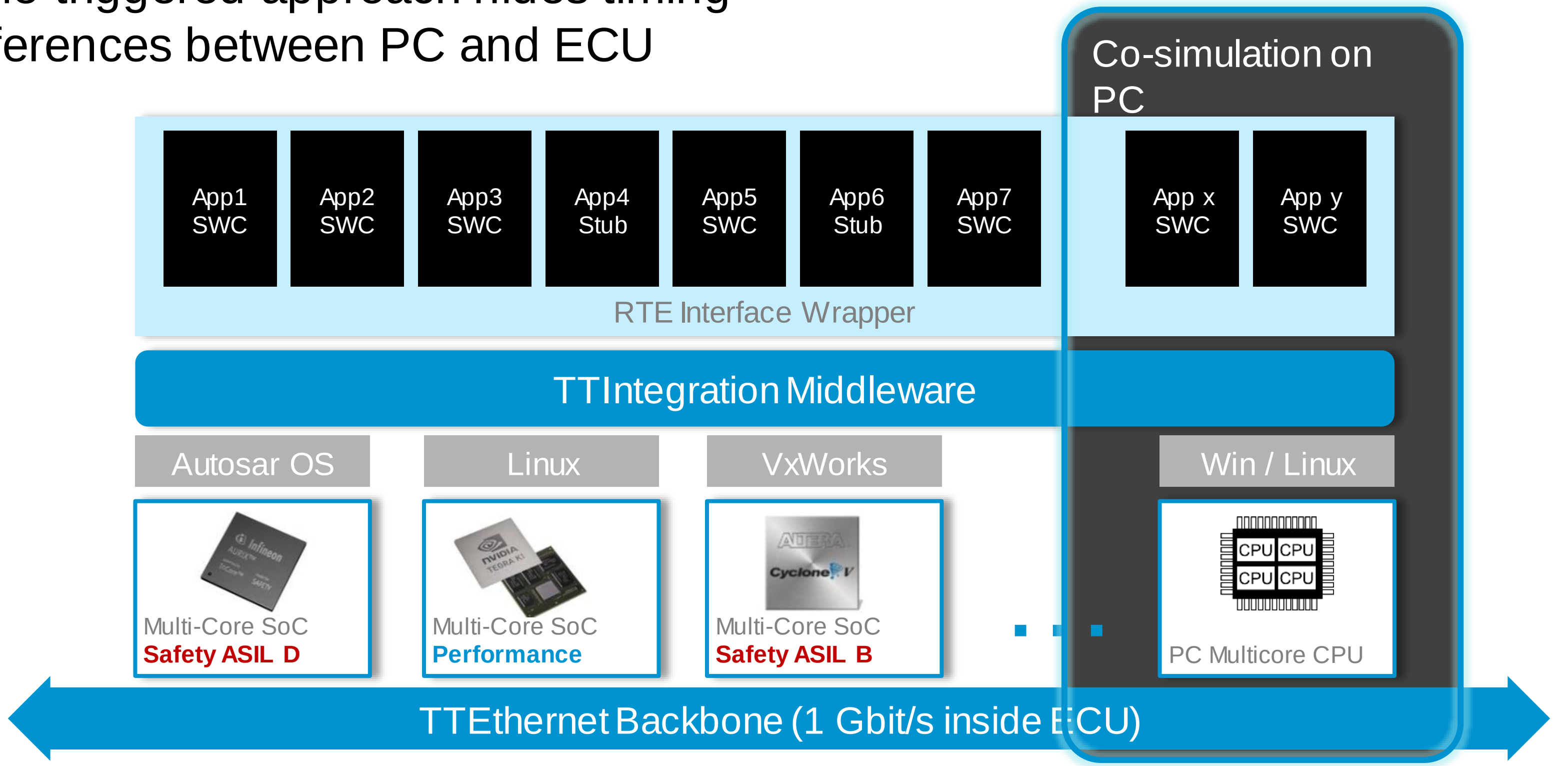


1. TTTech integrates the platform and configures the execution boundaries for the applications.
2. Applications are integrated and tested individually by the SWC suppliers into their respective execution boundaries.
3. All applications are integrated by TTTech and are immediately able to run together; violations by SWCs are detected easily.

www.tttech.com

Co-Simulation Support

- Ethernet backbone enables easy connectivity to PC's
- TTIntegration middleware available on PC
- Time-triggered approach hides timing differences between PC and ECU



www.tttech.com

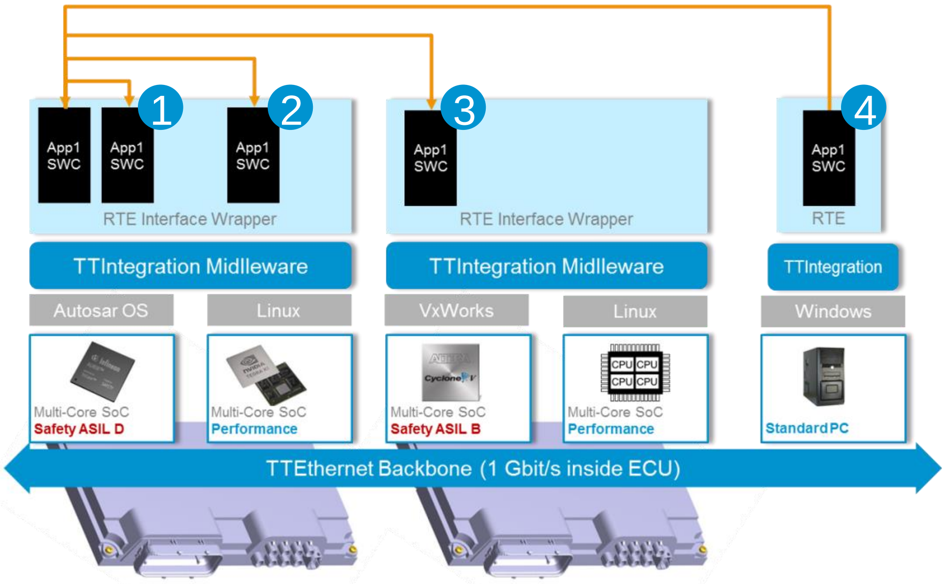
Multiple Levels of Software Re-Use

TTIntegration Middleware enables to

1. move SW-C between cores on the micro-controller
2. move SW-C between micro-controllers in the same ECU
3. move SW-C between ECUs
4. move SW-C between ECU and simulation PC

Minimal re-testing

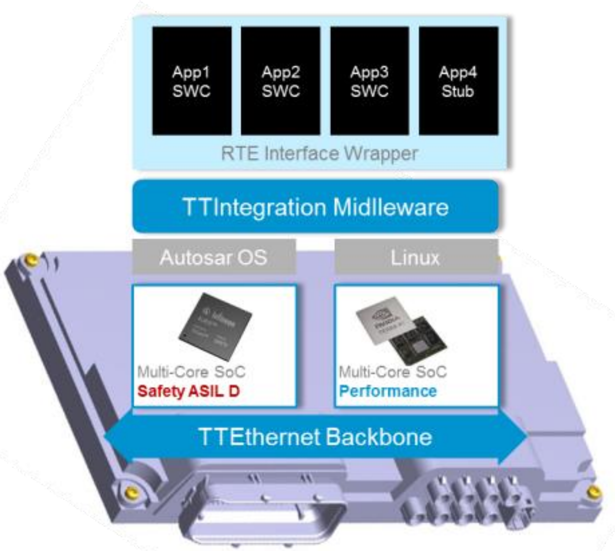
- no change in timing
- no change to source code necessary



www.tttech.com

Exhaustive Set of Features

- Time-synchronization (global / between SoCs)
- Scheduling (Time-Triggered, Soft-Time-Triggered, Event-Triggered)
- ECU lifecycle management
- Inter-ECU communication (FR, CAN, Ethernet)
- Intra-ECU communication
  (TTEthernet, Middleware, Key/Value Store)
- Diagnostics
- Software update – Multistage flashing
- Safety mechanisms (ASIL-A to ASIL-D)
- Debug and calibration features
- Software-in-the-loop / Co-simulation tools
- Data recorder
- …



www.tttech.com

Middleware Availability and Key Parameters today

Processing Units

- Infineon Aurix, Altera Cyclone 5, Nvidia Tegra K1
- Fully portable

Operating Systems

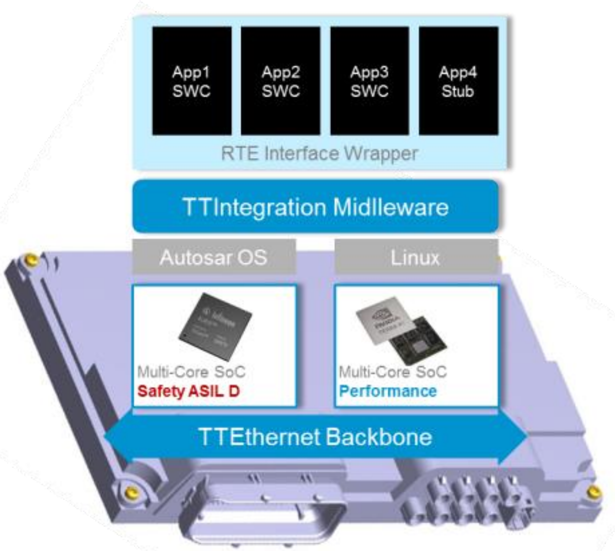
- AUTOSAR, VxWorks, Linux, Windows

Application Supplier Landscape

- 35 Application SW components from 12 suppliers

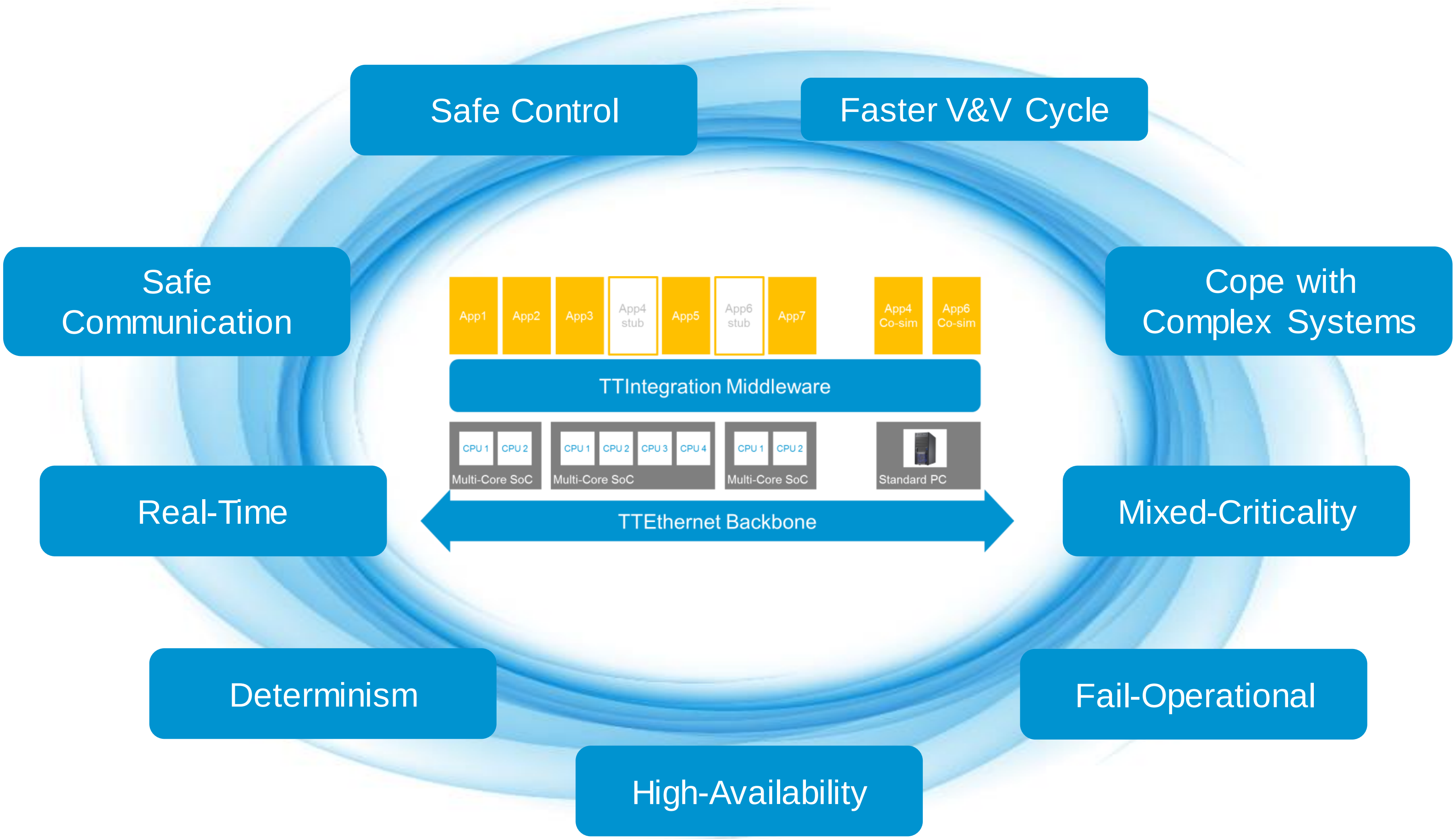
Tools

- Seamless ADTF integration
- All Linux-based debugging features on all hosts



www.tttech.com

Safety Platform Highlights



TTA-Drive
Fault-Tolerance Option

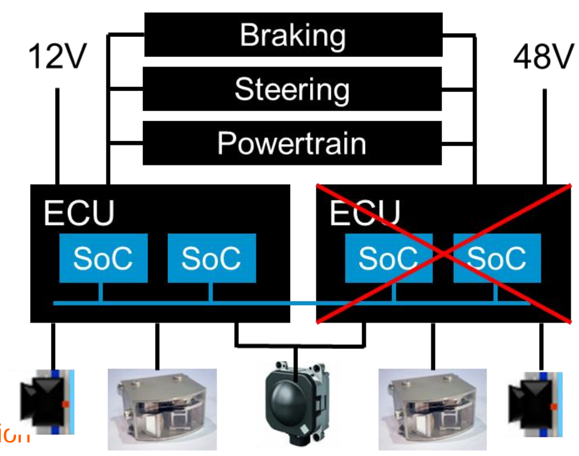
TTTech

No Single Point of Failure – No Common Mode Failures

- Power supply – e.g., 12V and 48V
- Communication – redundant connections, resource monopolization, ...
- Environment – mechanical stress, temperature, impact in case of accident, …
- Fault-Containment – faults do not propagate across the whole systems, …
- Steering and braking – need to be fail-operational

Two ECU´s can be combined with Ethernet to form a fault-tolerant system for automated driving

2 Fault-Containment Regions =
2 physically separated ECUs



Ensuring Reliable Networks TTTech

Piloted Driving & Piloted Parking based on our platform will be implemented in the next Audi A8

Further Challenges

Further Challenges

- Object classification and Sensor fusion for safety – classical safety processes, e.g., ISO 26262, are not suitable
- Standardization of semantic interfaces for sensor fusion – input from sensors to fusion and fusion results
- Consumer defined semiconductors – automotive is a much harsher environment calling for more reliability
- Validation – is 400.000 km enough, real-test cases vs. synthetic, Peta Byte data bases, HIL systems with accelerated real-time, …
- Interacting Systems SoS – strategy interaction between systems (human driven cars, automated cars)
- Legal – during automated driving responsibility is with the car

And Finally

Big data collection: **2 Gb/s**

- Street conditions
- Traffic conditions
- Weather conditions
- Construction work
- Traffic signs
- Where are drivers going, what are drivers doing
- What others do around the car
- ...

The Future?

TTTech

TTTech

Ensuring Reliable Networks

Vienna, Austria (Headquarters)
Phone +43 1 585 34 34-0
office@tttech.com

USA
Phone +1 978 933 7979
usa@tttech.com

Japan
Phone +81 52 485 5898
office@tttech.jp

China
Phone +86 21 5015 2925-0
china@tttech.com

www.tttech.com