Embedded Multi-Core Systems for Mixed Criticality Applications in dynamic and changeable Real-time Environments

EMC² Living Lab Automotive

Presentation at
3Ccar workshop
Eindhoven NL, 2016-11-15

Rutger Beekelaar, Robert Koffrie TNO, The Netherlands

Project Overview
Numbers

Embedded Multi-core Systems for Mixed-Criticality Applications in Dynamic and Changeable Real-Time Environments – EMC²

(Artemis Innovation Pilot Project (AIPP)

- AIPP 5: Computing Platforms for Embedded Systems
- Budget: 93.9 M€
- Funding: 15.7 M€ EU funding (Artemis)
  26.7 M€ National funding
- Resources: 9636 person months (803 person years)
- Consortium: 101 Partners (plus 1 associate partner)
- From: 16 EU Countries
- Project start: april 1st 2014

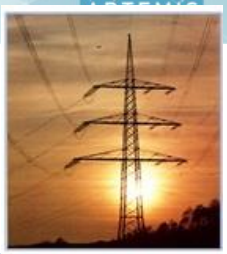
Motivation for EMC²

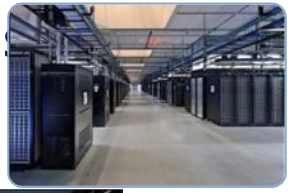
- Introduction

- Very fast technological advances of µ-electronics in past decades
- Amazing capabilities at lowered cost levels
- Systems quickly put together since the next technology generation is already waiting around the corner
- Today primarily exploited in consumer-oriented products
- Errors may be tolerated to a certain degree
- This (and similar) way(s) of handling errors acceptable for consumer products

Application innovation

- In professional areas the consumer approach is not feasible: **Automotive, Avionics, Space, Industry, Health care, Infrastructure**
- Need much higher level of operational reliability
- Higher HW/SW complexity
- Have to fulfill real-time safety requirements
- Dynamic priorities change during runtime
- Prime task of EMC² to bring two worlds together
  - Consumer world: use of advanced µ-electronic systems
  - Professional world: reliability, complexity, real-time



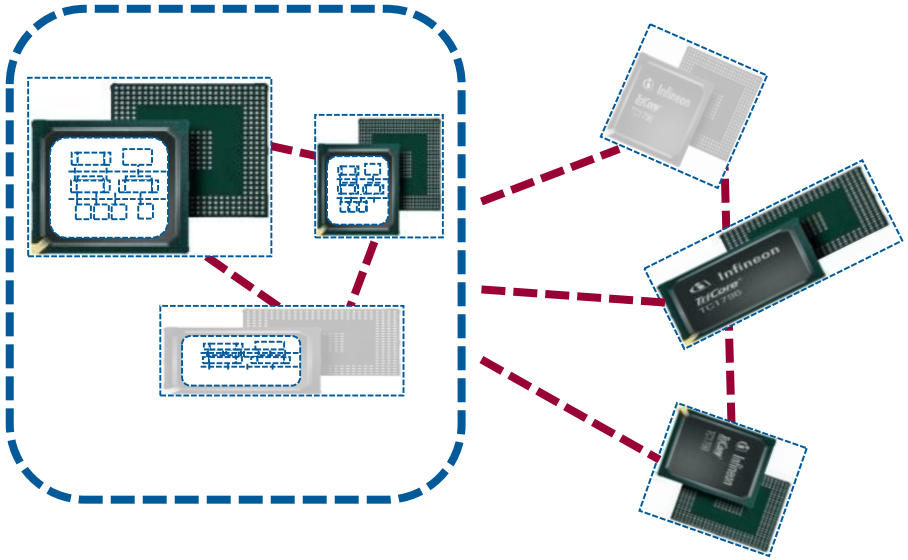







Technological innovation

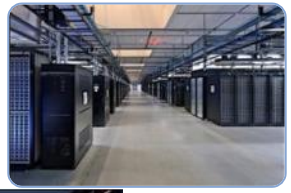
- Mixed Criticality
  - Handle applications with different ASIL levels
- Dynamic Re-configuration
  - Continuous dynamic changes on application level or priority
- Hardware Complexity
  - Variable number of control units at runtime



Applications

- EMC² - Embedded Multi-core Systems for Mixed-Criticality Applications in Dynamic and Changeable Real-Time Environments
- Applications: Automotive, Avionics, Space, Industry, Health care; Infrastructure
- Improve performance, lower cost
- Improve energy efficiency

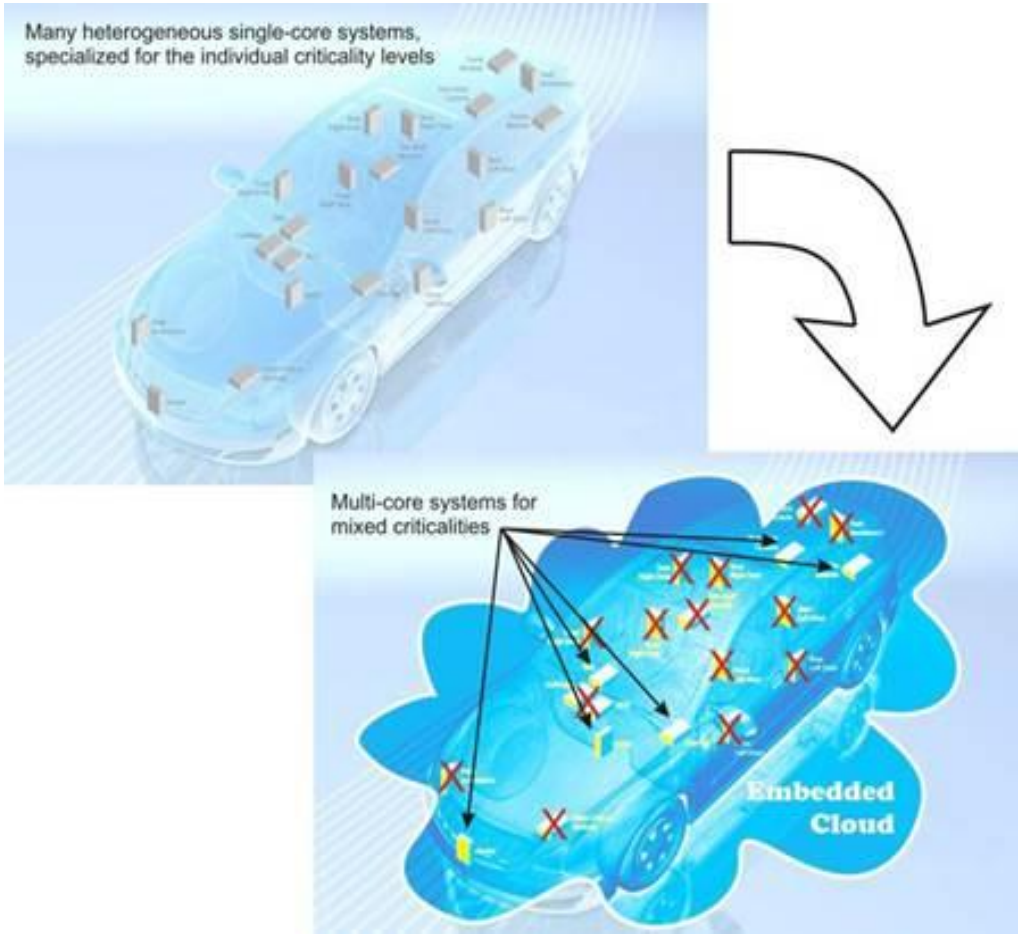






Automotive application (WP7)



By using multicore technology:

*** decrease the number of ECUs**

*** homogenous ECUs**

*** ECUs with the capability to execute applications of mixed criticality level**

*** increasing quality and decreasing cost**

We investigate the concept of Service-oriented Architecture for embedded systems

- **Embedded cloud services**
- **TCP/IP communication**
- **Late binding, dynamic system configuration**

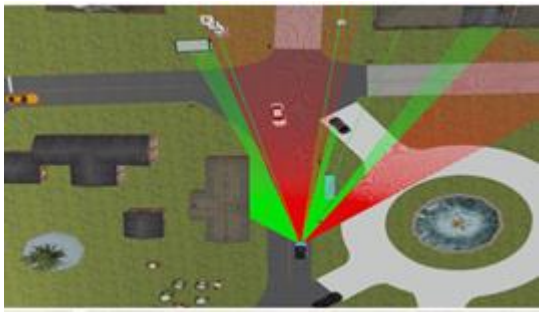
Automotive use cases

Living Lab Automotive (WP7) coordinated by

Thomas Söderqvist, VOLVO (Commercial vehicles), Sweden

Rutger Beekelaar, TNO, Netherlands

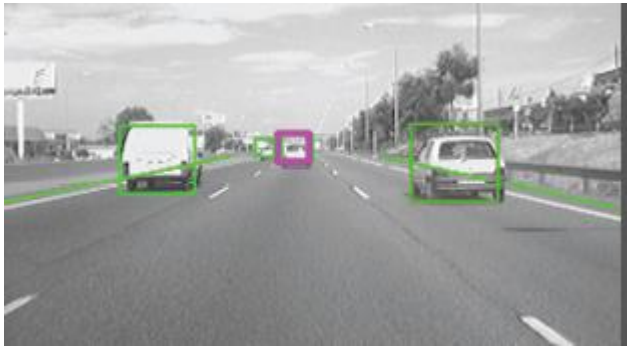
WP 7 contains 6 use cases



- **Use Case 1: ADAS and C2x**:
- Objective
  - To understand how/where/why and when EMC^2 multicore, mixed criticality, systems can have a beneficial impact on the development of Advanced Driver Assistance Systems (ADAS) as a waypoint to full AD.
  - To understand how the demands that ADAS places on existing vehicle s/w infrastructures can be accommodated by exploiting EMC^2 architectures.

Automotive use cases

- **Use case 2: Highly automated driving**
- use EMC² architectures and tools in real-life tests, using current advanced sensing, navigation and co-operation functionalities for highly automated vehicles.
  - Investigate, implement and evaluate an architecture that exploits the potential of existing technology around highly automated driving
  - EMC2 architecture and tools should enable the scheduling mixed time-critical high-performance functionalities
  - Evaluation will be performed in simulation for typical driving scenarios and with representative Hardware In the Loop (HIL)



Automotive use cases

- **Use Case 3: Design and validation of next generation hybrid powertrain / E-Drive:**
- The goal of this use case is the tailoring and further enhancement of the EMC² technologies for the design and validation of next generation hybrid powertrains and e-Drives.

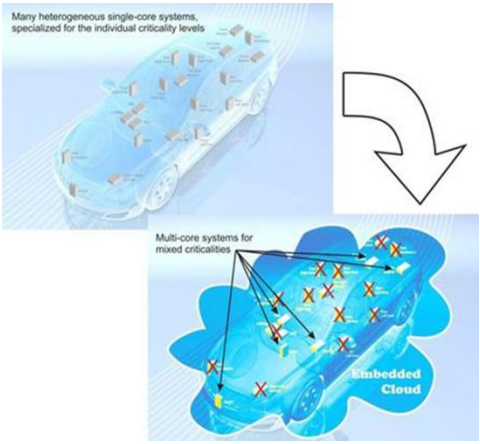
  This will be explained in more detail by Robert Koffrie
- **Use case 4: Modelling and functional safety analysis of an architecture for ACC system**:
- Objective: development of a tool chain for supporting the functional safety process (ISO 26262 conformant) applied to a safety mixed (safety/security) criticality systems, exemplified by an ACC system

Automotive use cases

- **Use case 5: Infotainment and eCall Multi-Critical Application**
- Development of a Multi-core Mixed-criticality Infotainment Platform
- Allow multi-core mixed-criticality functionality deployment
- Enable resource sharing among mixed-criticality functionalities

- **Use case 6: Next Generation Electronic Architecture for Commercial Vehicles**
- identify, apply and evaluate methods as well as tools to harvest the potential of multicores for mixed-critical applications for commercials vehicles. Main topics of interests are to explore the full potential of multicores based on the needs and requirements of the next generation Electrical and/or Electronic (E/E) architecture for commercial vehicles, for example, trucks and buses.

Summary, examples of common topics and technologies studied in the use cases



- Many single core ECUs → Fewer multicore ECUs
- Mixed criticality
- Support for mixed operating systems
- Freedom from interference (ASIL levels)
- Virtualization (during development and testing)
- Predictable, low latency, high bandwidth communication
- Service-oriented architecture

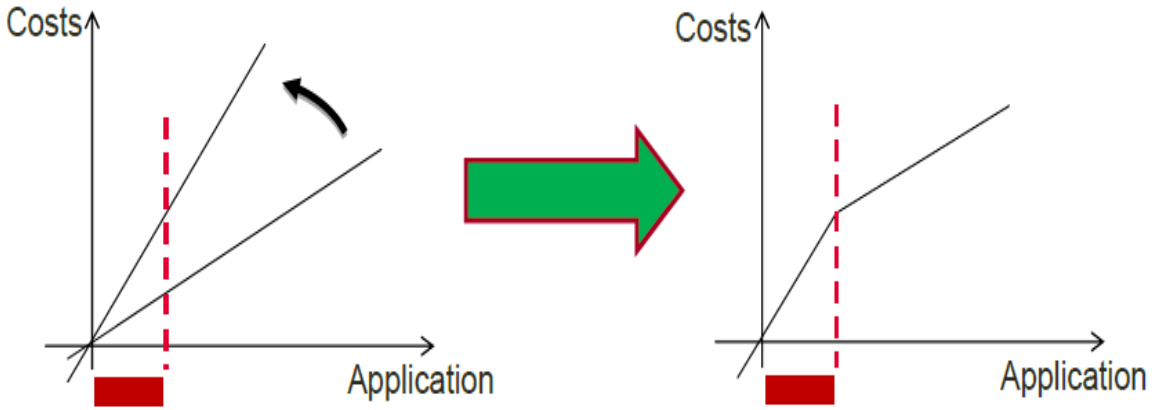
Use Case 3: Design and validation of next-generation hybrid powertrain / E-Drive

Automotive use cases
EMC² Problem overview

Costs are increasing due to (ever) increasing functionality and the desire to connect (more and more) systems with each other.

In the past dedicated devices (ECUs) were used for specific applications. However it is not practical, nor economically feasible, to allow the number of ECUs (in a car) to grow even further…

…therefore there is a need for scalable economically viable platforms, supporting mixed criticality and combined with development processes and tools.



Source: Infineon EMC2 introduction

Automotive use cases
EMC^2 goals

The following overall goals were stated in the DoW:

- Reduce cost for design by 15% (baseline 2012, towards 2020)
- Reduce effort and time required for re-evaluation of systems after making changes by 15% (baseline 2012, towards 2020)
- Achieve 15% reduction in development cycles –especially in sectors requiring qualification and certification- (baseline 2012, towards 2020)

Source: Infineon EMC2 introduction

Automotive use cases
WP7, UC 3: placed in context (1)

We are now "zooming in" on one of the Living Labs: LL1. There are however 6 living labs within EMC²:

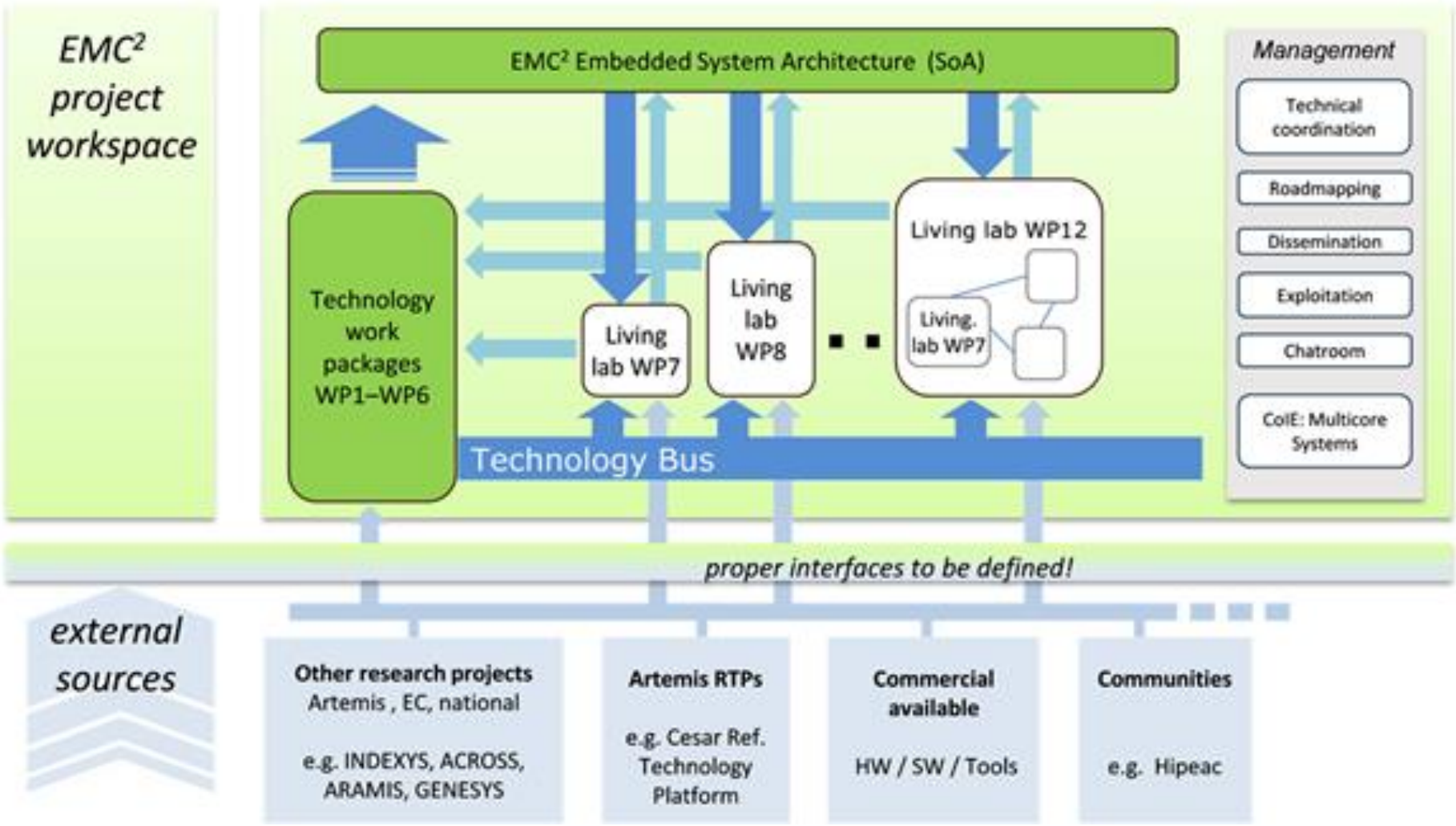
- LL1: Automotive applications (WP7)
- LL2: Avionics applications (WP8)
- LL3: Space applications (WP9)
- LL4: Optical payload applications (WP10)
- LL5: Industrial manufacturing and logistics (WP11)
- LL6: Internet of Things (WP12)

Automotive use cases
WP7, UC 3: placed in context (2)

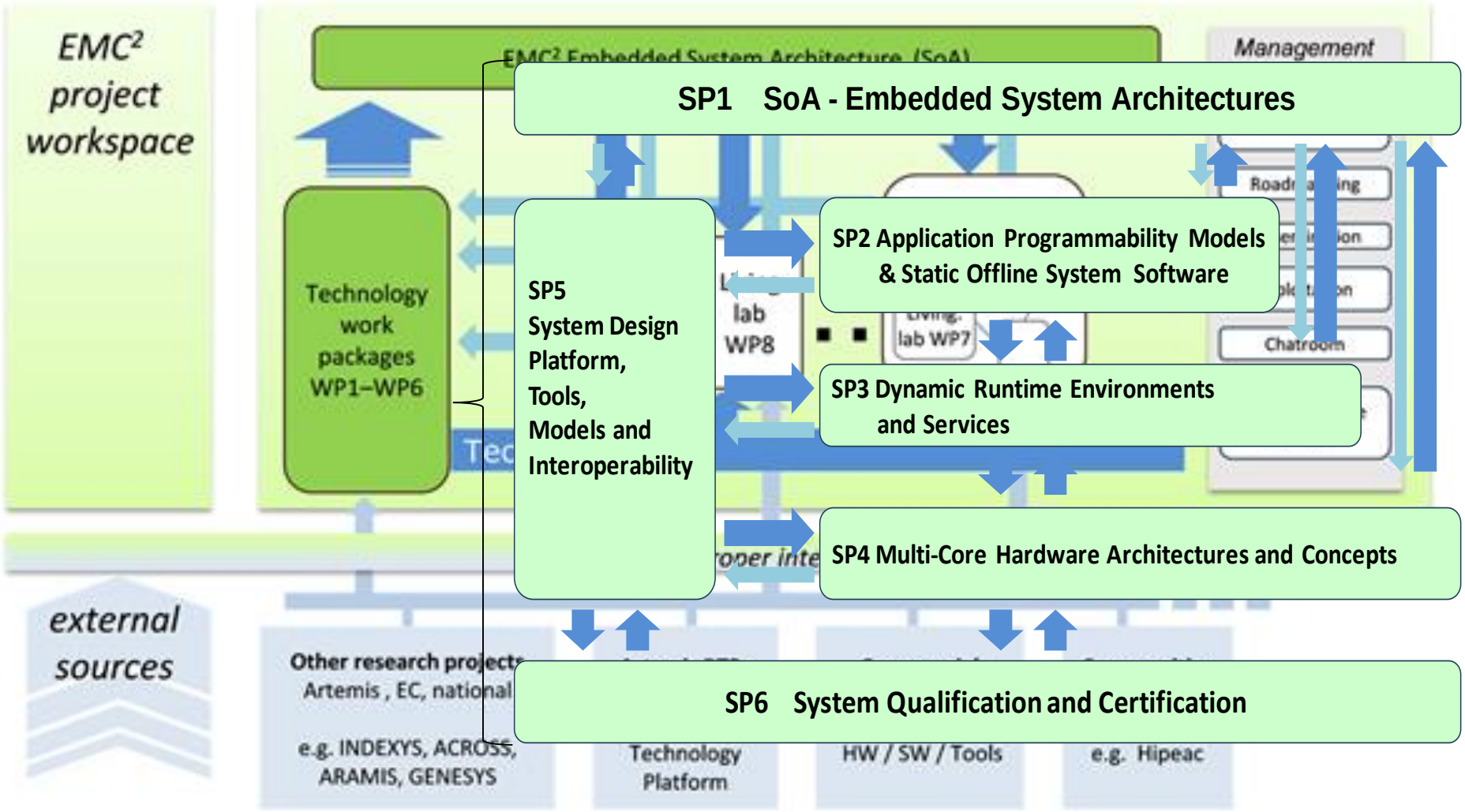
Next to the Living Labs, there are also 6 subprojects, focusing on methods, architectures and tools that will help reaching the EMC^2 goals:

- SP1=WP1: Service Oriented Architecture (SOA)
- SP2=WP2: Executable Application Models and Design Tools (for mixed critical, multi-core embedded systems)
- SP3=WP3: Dynamic runtime environments and services
- SP4=WP4: Multi-core hardware architectures and concepts
- SP5=WP5: System design platform tools, models and interoperability
- SP6=WP6: System qualification and certification

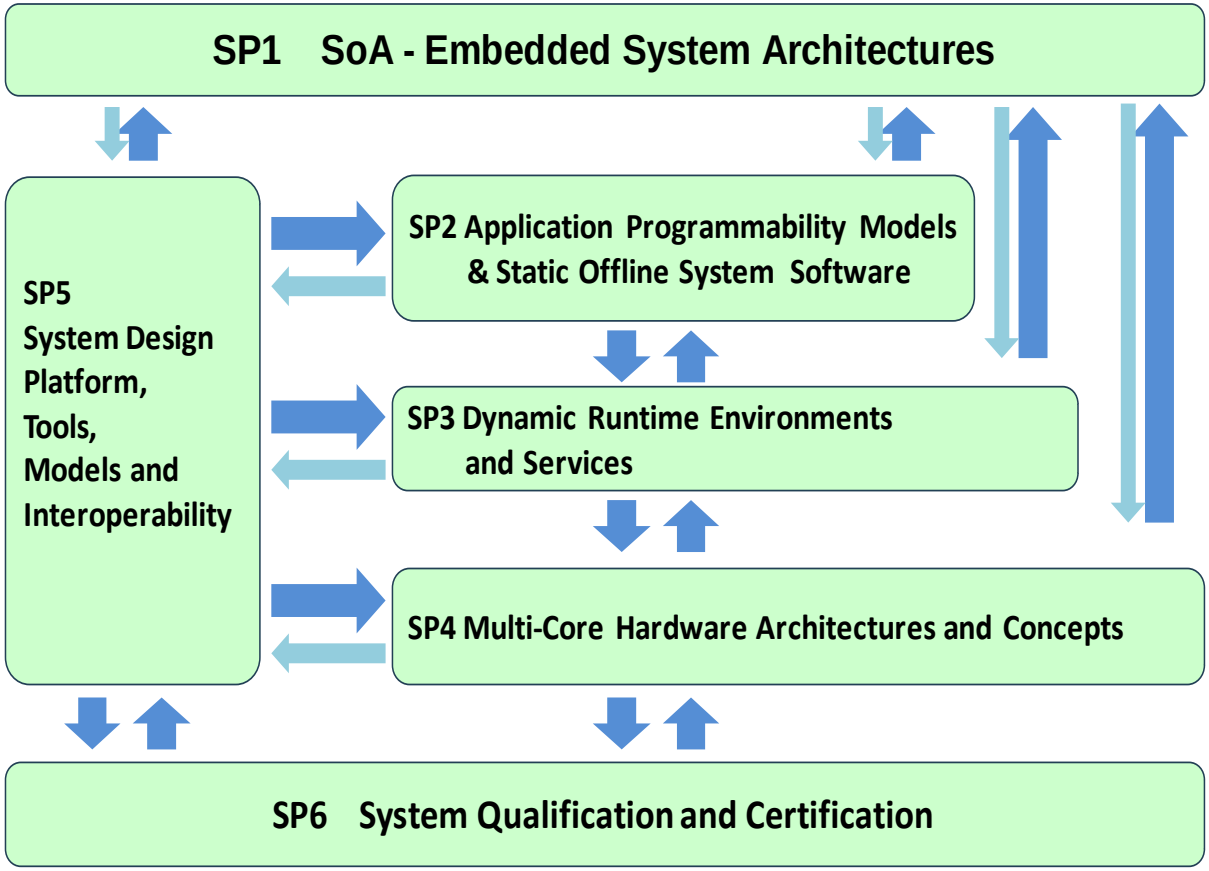
Automotive use cases
WP7, UC 3: placed in context (3)



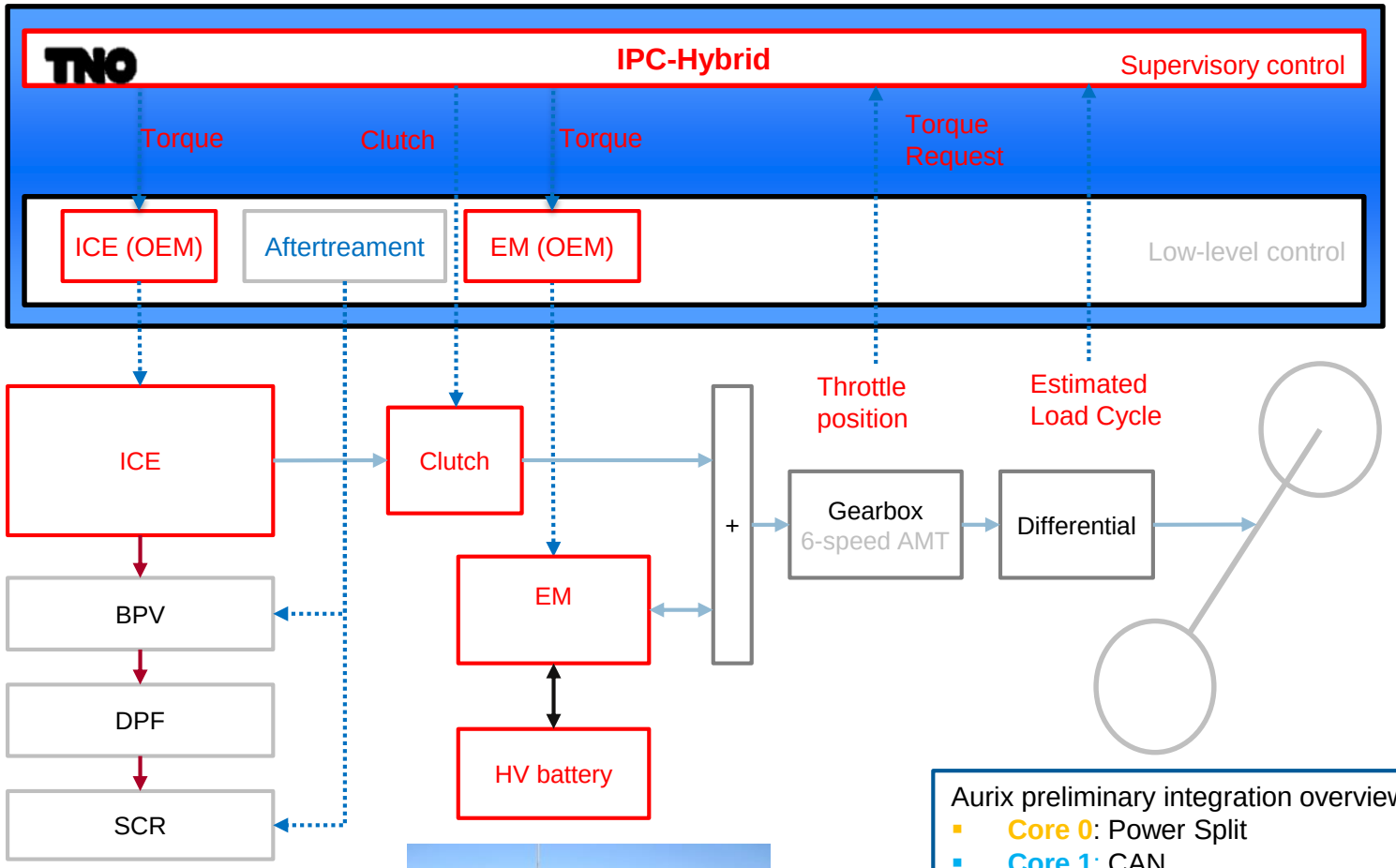
Automotive use cases
WP7, UC 3: placed in context (3)



Automotive use cases
WP7, UC 3: placed in context (3)

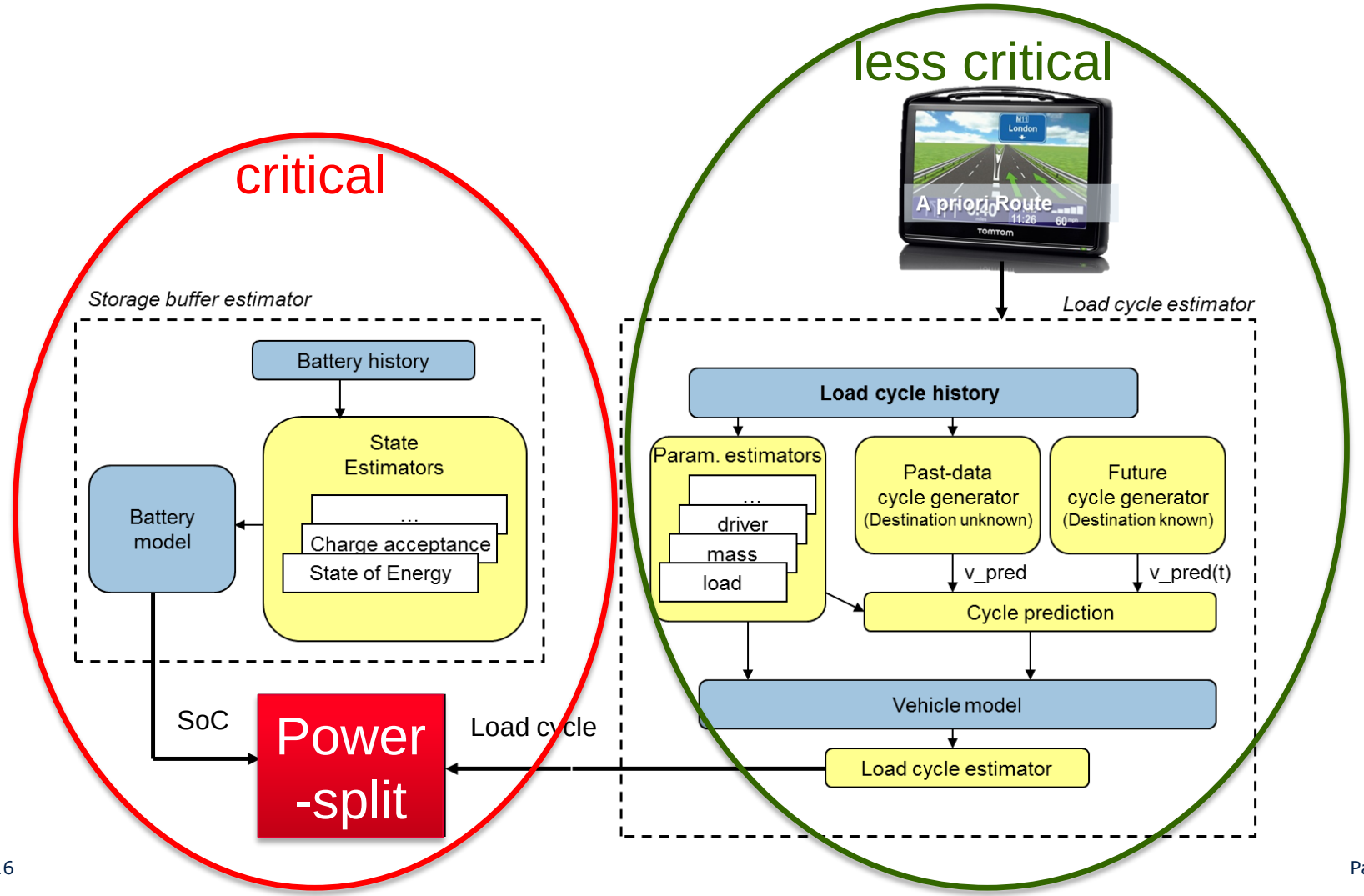


Automotive use cases
WP7, UC 3 TNO internal demo (1)



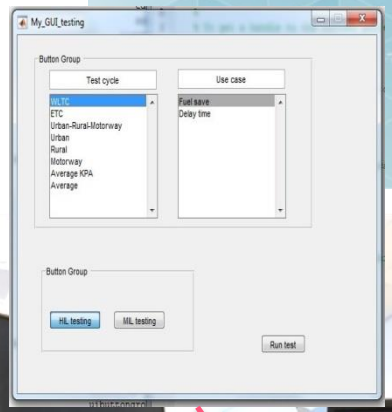
Aurix preliminary integration overview:
- Core 0: Power Split
- Core 1: CAN
- Core 2: Cycle and load prediction

Automotive use cases
WP7, UC 3 TNO internal demo (2)

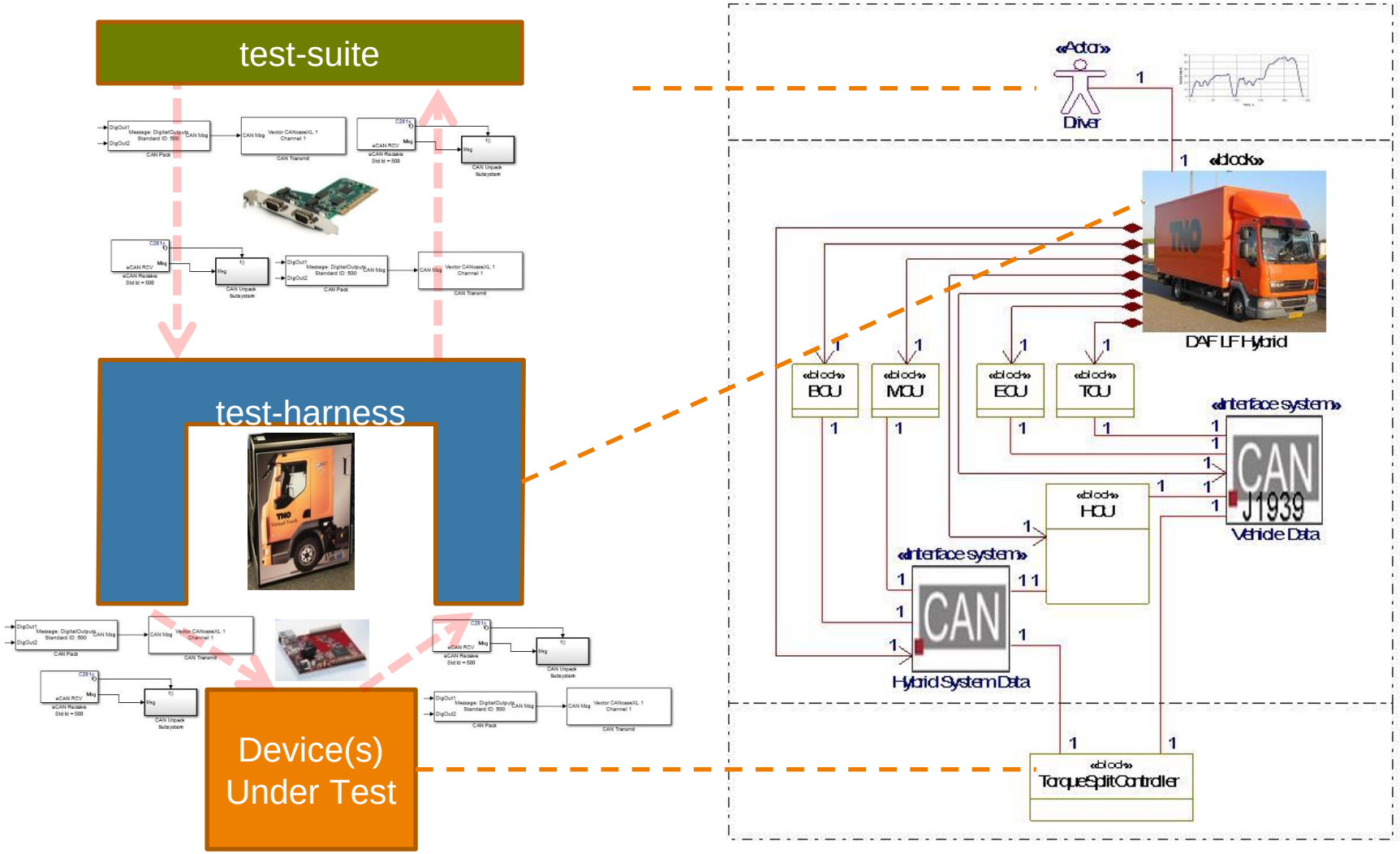


Automotive use cases
WP7, UC 3 TNO internal demo (2)

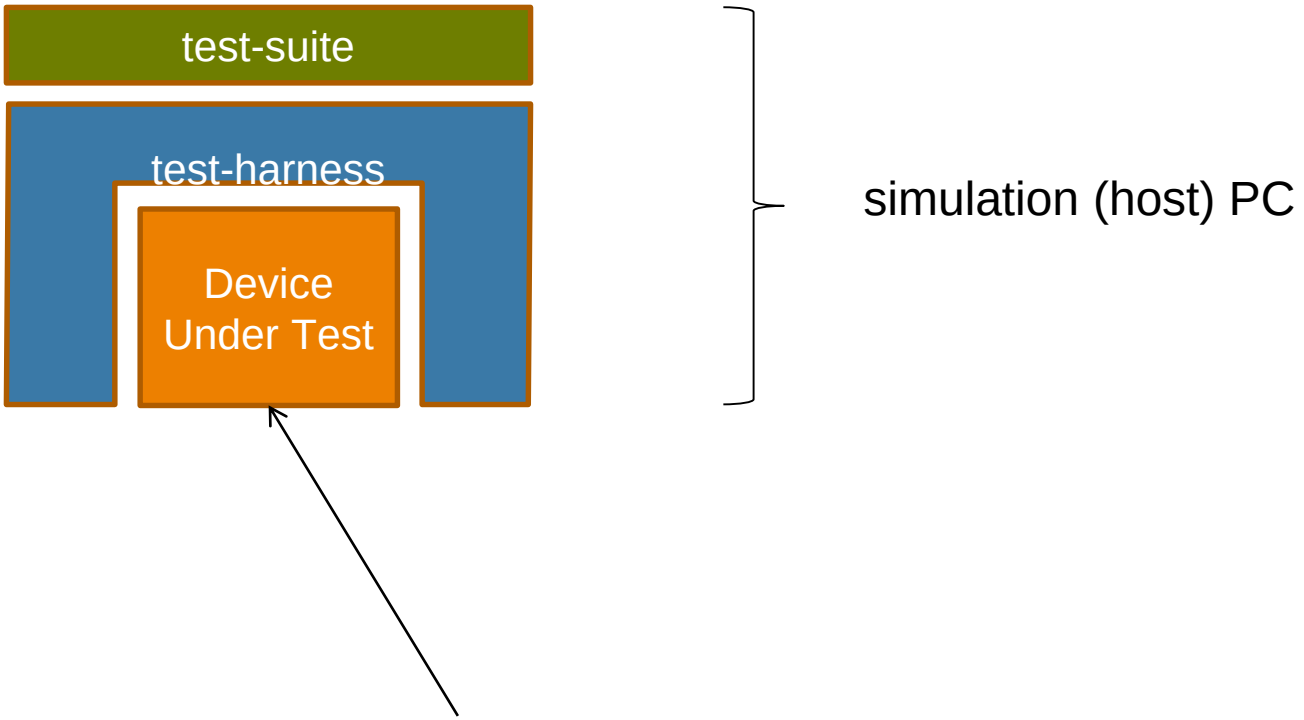
- TNO test-suite:
  - is running on a laptop;
  - is capable of running automated test scripts representing test scenario's;
  - provides an easy selection mechanism for this purpose:
- TNO test-harness:
  - Is running on a dedicated PC, using a dedicated OS (MathWorks Real-Time Windows Target)
- TNO DUT hardware:
  - The Aurix board



Automotive use cases
WP7, UC 3 TNO internal demo (3)



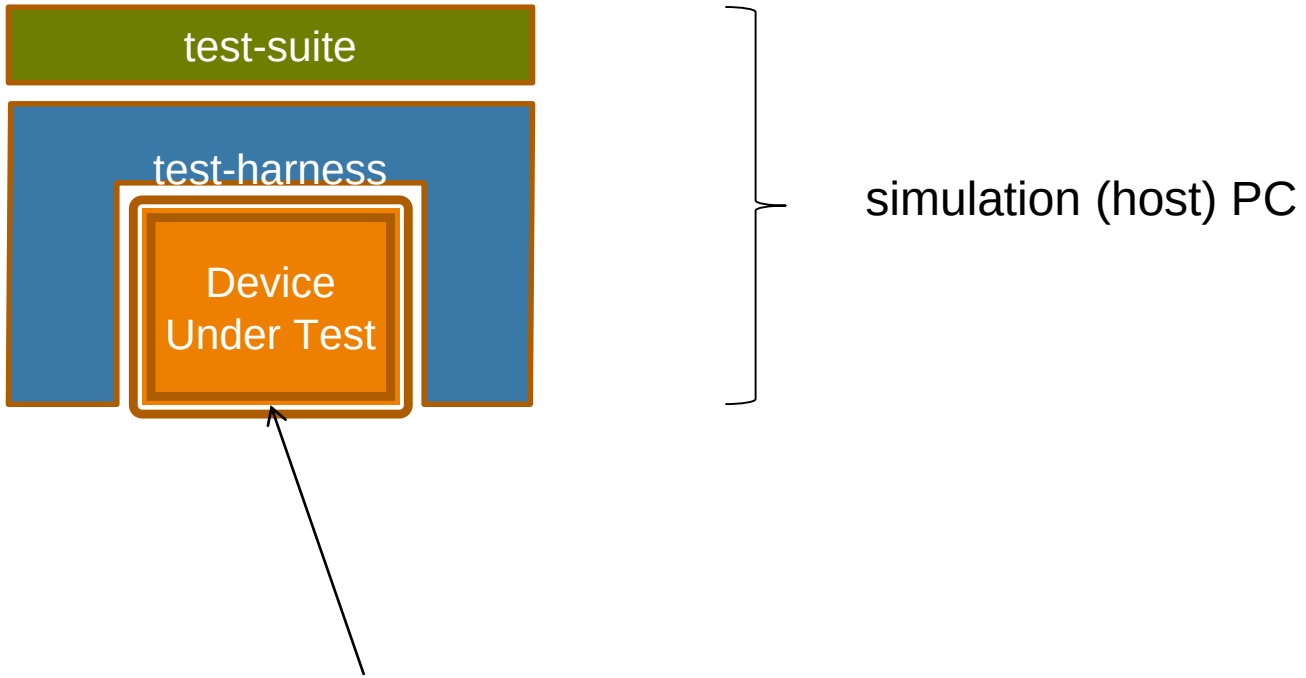
Automotive use cases
WP7, UC 3 TNO internal demo (4)
functional validation (MIL)



DUT still in Matlab/Simulink; algorithm however separated from test code

Goal: separation of concerns in preparation of mapping onto DUT HW

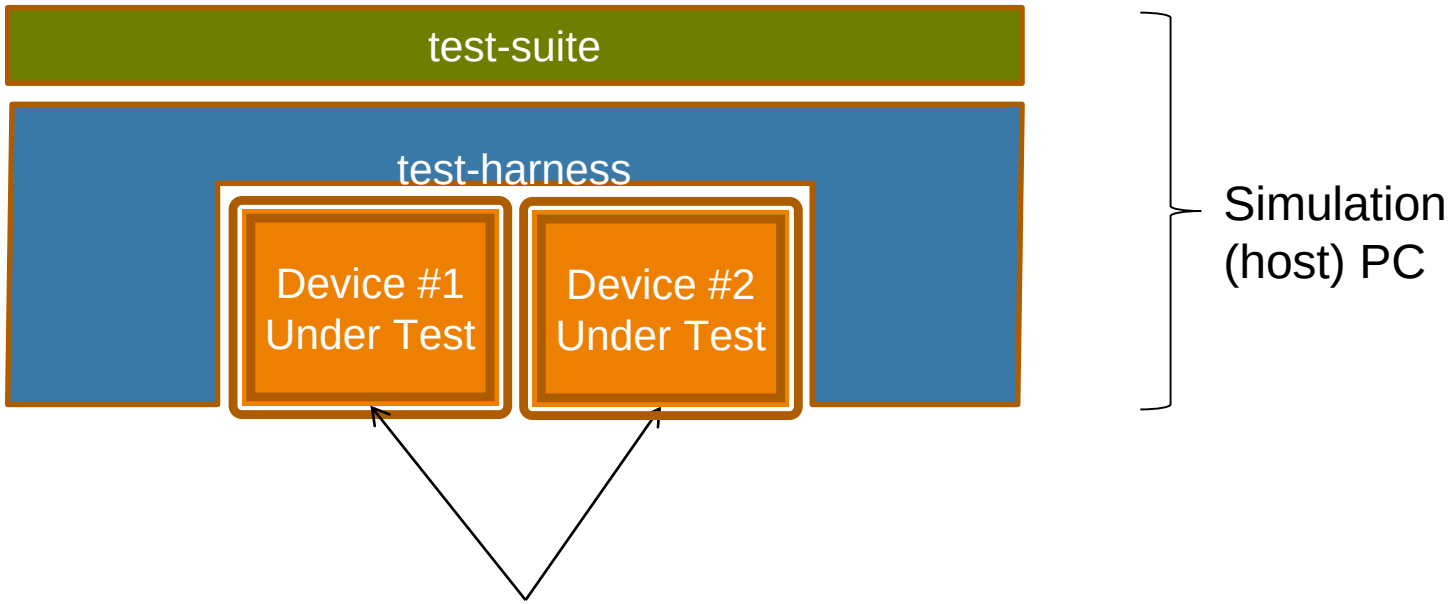
Automotive use cases
WP7, UC 3 TNO internal demo (5)
functional validation (SIL)



DUT exists of compiled code (presuming target HW constraints, such as fixed point parameters, target platform process scheduling, etc.)

Goal: verify whether the transition towards DUT SW caused regression

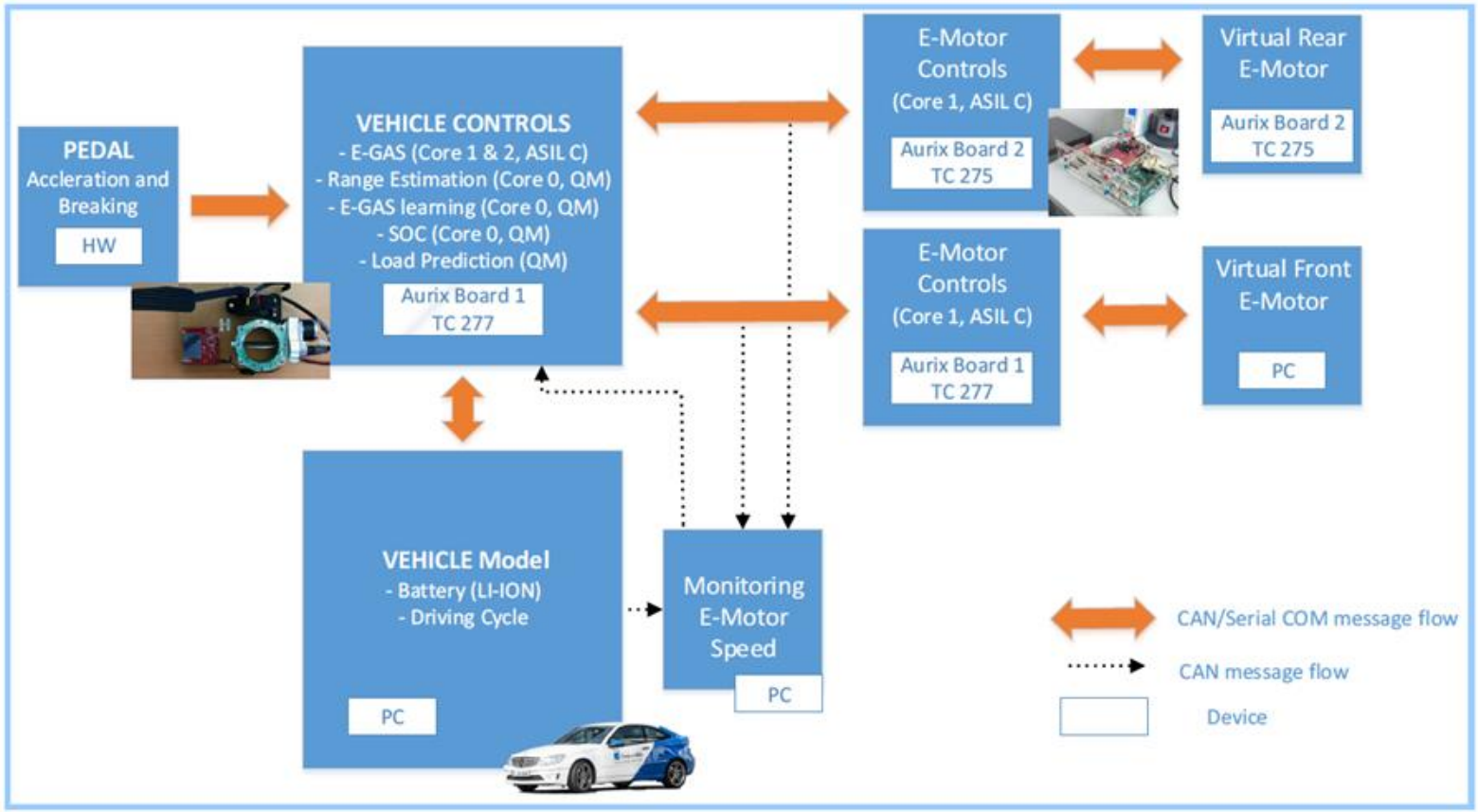
Automotive use cases
WP7, UC 3 TNO internal demo (6)
Multi-core functional validation



DUT exists of compiled code for each separate core (with a single test suite).

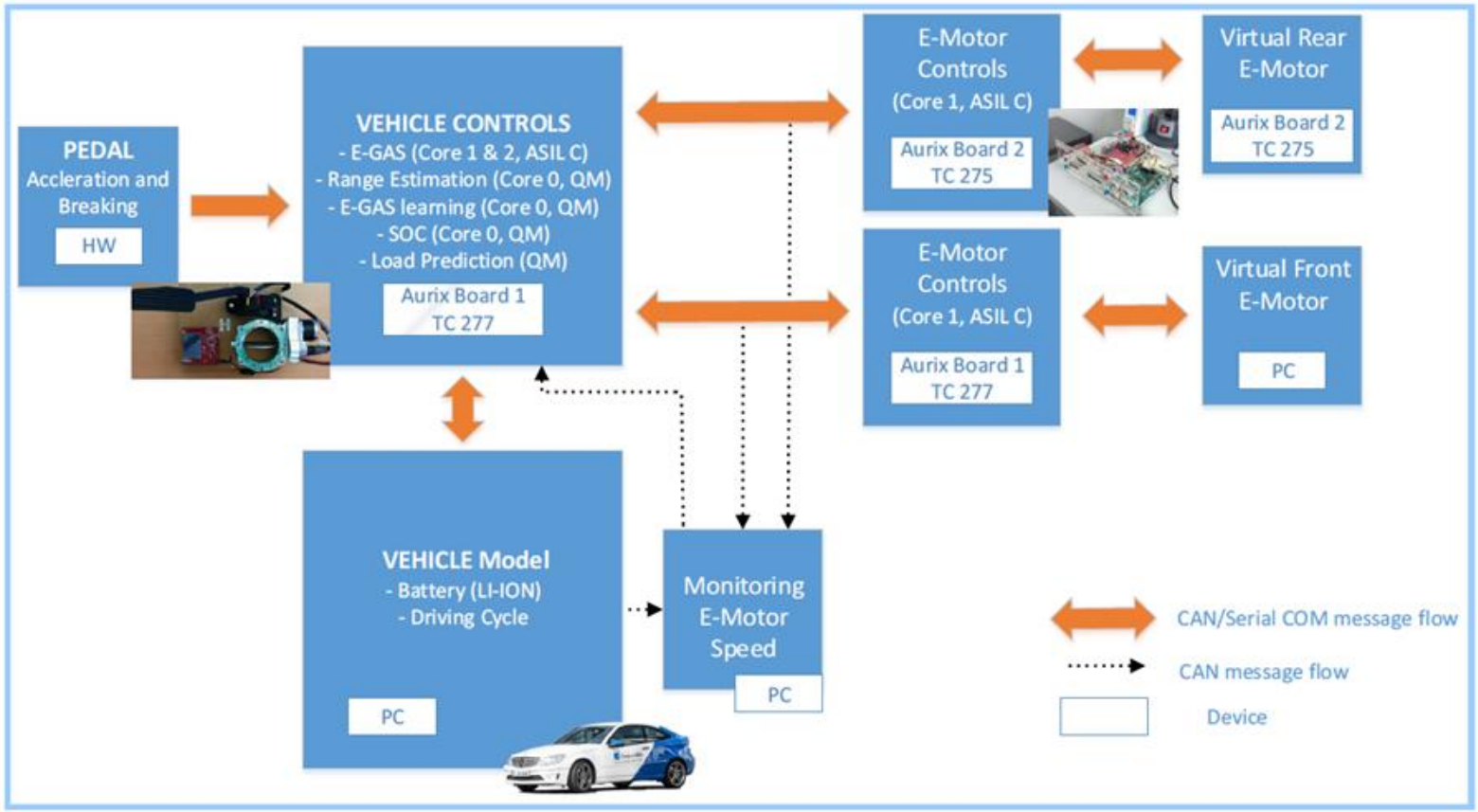
Goal: verify whether the transition towards DUT SW caused regression

Automotive use cases
WP7, UC 3 group demo: current status



Automotive use cases
WP7, UC 3 group demo: update

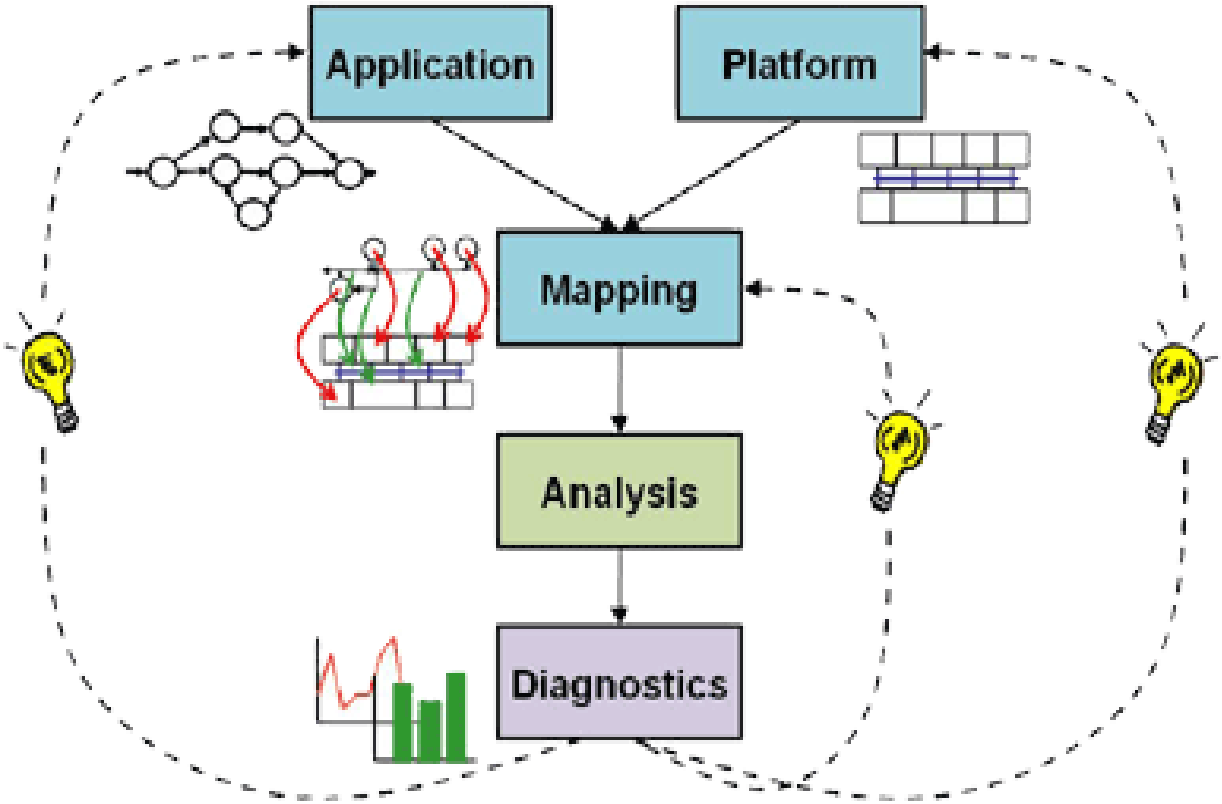
1) SP6 involvement: Apply Conditional Safety Certificates (ConSerts) to support the safety certification activities to be executed (automatically) at runtime in an act to support runtime adaptive systems;
2) SP2 involvement: (to be confirmed) Use the Y-chart design-space exploration approach for (a part of) this use-case in order to assess its applicability and presumed design efficiency improvements.



Automotive use cases

Questions?

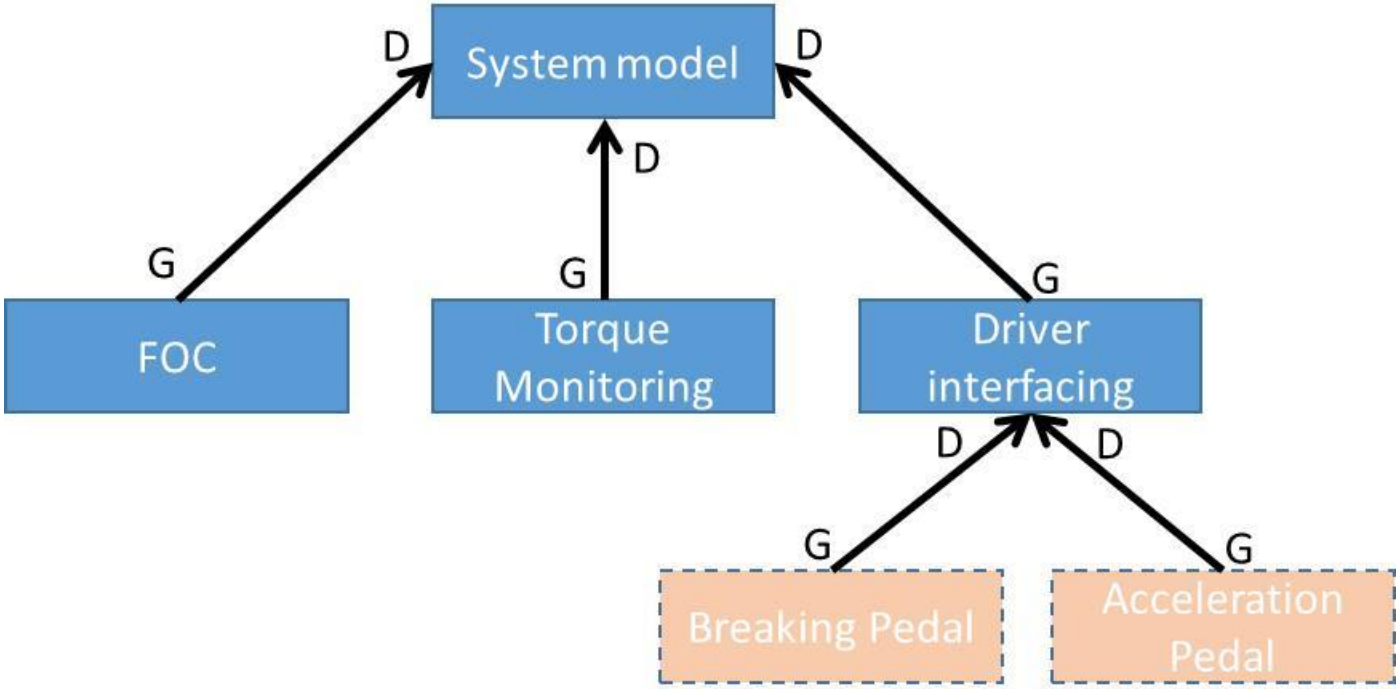
Automotive use cases
Y-chart design-space exploration



Design-space exploration typically involves the co-development of an application, a platform, and the mapping of the application onto the platform. Diagnostic information is used to (semi-automatically) improve application, platform, and/or mapping.

Source: TNO-ESI

Automotive use cases
ConSerts tree



Source: Fraunhofer

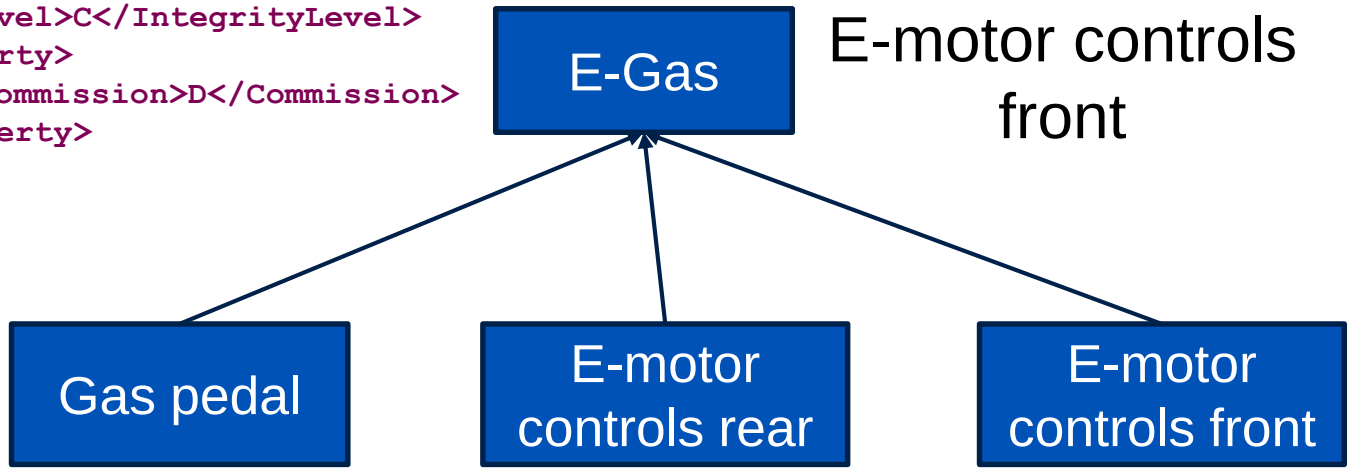
E-Gas (Horizontal demands)

```
<Horizontal_Demand>
        <ConfigurationName>setAcceleration</ConfigurationName>
        <IntegrityLevel>QM</IntegrityLevel>
        <SafetyProperty>
                <Commission>B</Commission>
        </SafetyProperty>
</Horizontal_Demand>
<Horizontal_Demand>
        <ConfigurationName>setTorqueFront</ConfigurationName>
        <IntegrityLevel>C</IntegrityLevel>
        <SafetyProperty>
                <Commission>D</Commission>
        </SafetyProperty>
</Horizontal_Demand>
<Horizontal_Demand>
        <ConfigurationName>setTorqueRear</ConfigurationName>
        <IntegrityLevel>C</IntegrityLevel>
        <SafetyProperty>
                <Commission>D</Commission>
        </SafetyProperty>
</Horizontal_Demand>
```

Gas pedal

E-motor controls rear

E-motor controls front

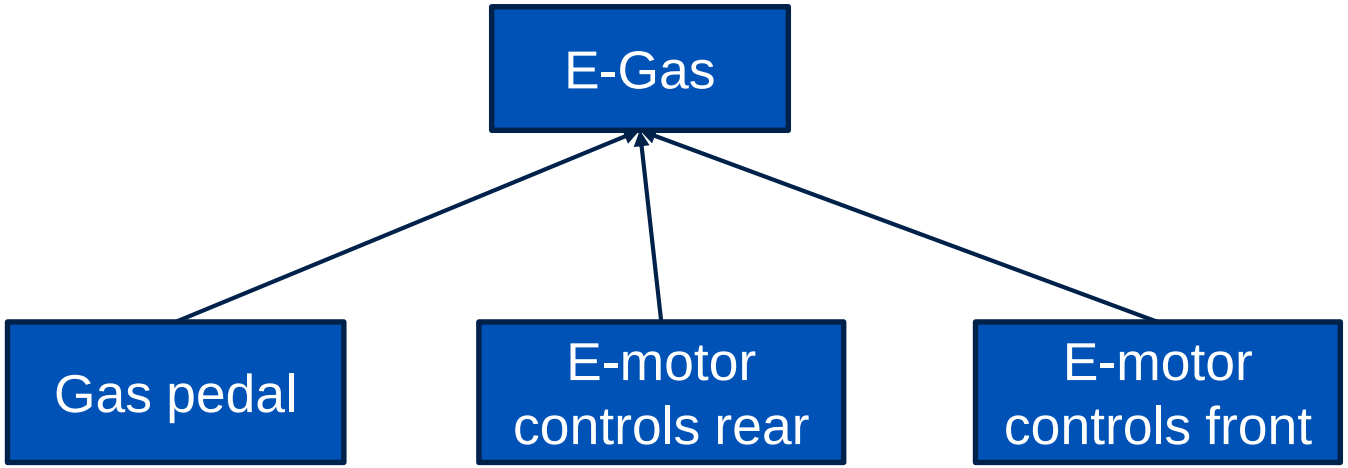


Source: Fraunhofer

Gas pedal (Horizontal guarantees)

```
<ComponentName>GasPedal</ComponentName>
<Horizontal_Guarantee>
    <ConfigurationName>setAcceleration</ConfigurationName>
    <IntegrityLevel>QM</IntegrityLevel>
    <SafetyProperty>
        <Commission>B</Commission>
    </SafetyProperty>
</Horizontal_Guarantee>
```

System type contract, no vertical demands.



Source: Fraunhofer

Automotive use cases
Use case 3: KPIs

No	Title	Description	Task/Use Case nr
01	Increased verification coverage by simulation	Increase verification coverage that can be performed in simulation by 10% for highly parallel applications and thus reduce the validation effort on target HW	T7.3.1, T7.3.5
02	Benefits of a seamless modeling method	Improve design specification maturity and consistency over the different domains, thus reducing cost and time for system design and safety recertification by 15%	T7.3.2
03	A collection of SW design and development guidelines for multicore platform	Prepare for each SW layer minimum 1 document including guidelines for the design and development of this component on multicore platforms, thus reducing training time for new SW engineers	T7.3.1, T7.3.3
04	Tailored safety architecture	Defined safety mechanisms for multicore to cover all automotive safety levels	T7.3.1, T7.3.2, T7.3.3
05	Decrease development time by use of integrated toolchain	Reduce development time at tool boundaries by 10% by efficient data transfer and consistency check	T7.3.1, T7.3.4, T7.3.5
06	Safety case generation	Reduction of effort for safety case generation by 20 %	T7.3.3, T7.3.4
07	Increased data throughput	Increase data throughputs of existing communication channels by the development and integration of new technologies such as CAN FD, Ethernet	T7.3.6
08	Data exchange and communication strategies	Maintain same configuration and handling efforts for communication complexity / load increase of 50%	T7.3.6

Automotive use cases
Use case 3