AUTOMOTIVE

FRANCISCO J. CAZORLA, JAUME ABELLA

EPI Tutorial/Barcelona/17-07-2019

SAFETY-CRITICAL SYSTEMS

- Failure or malfunction may result in
  - Death or serious injury to people
  - Loss or severe damage to equipment/property
  - Environmental harm
- Exhaustive Verification and Validation (V&V) process to guarantee the safety goals are met
- Each domain has its own guidelines and regulations for SW and HW

DO178C

ISO26262

EN50126/8

AUTOMOTIVE DOMAIN

- High-performance needed but… within specific domain requirements
  - Reliability
    - Harsh operating conditions due to Electro-Magnetic Interference (EMI), humidity, vibration, etc.
  - Safety
    - Development process subject to functional safety standards
      - Design
      - Verification and validation
  - Security
    - Connectivity
    - Updates

AUTOMOTIVE COMPLIANT MCU

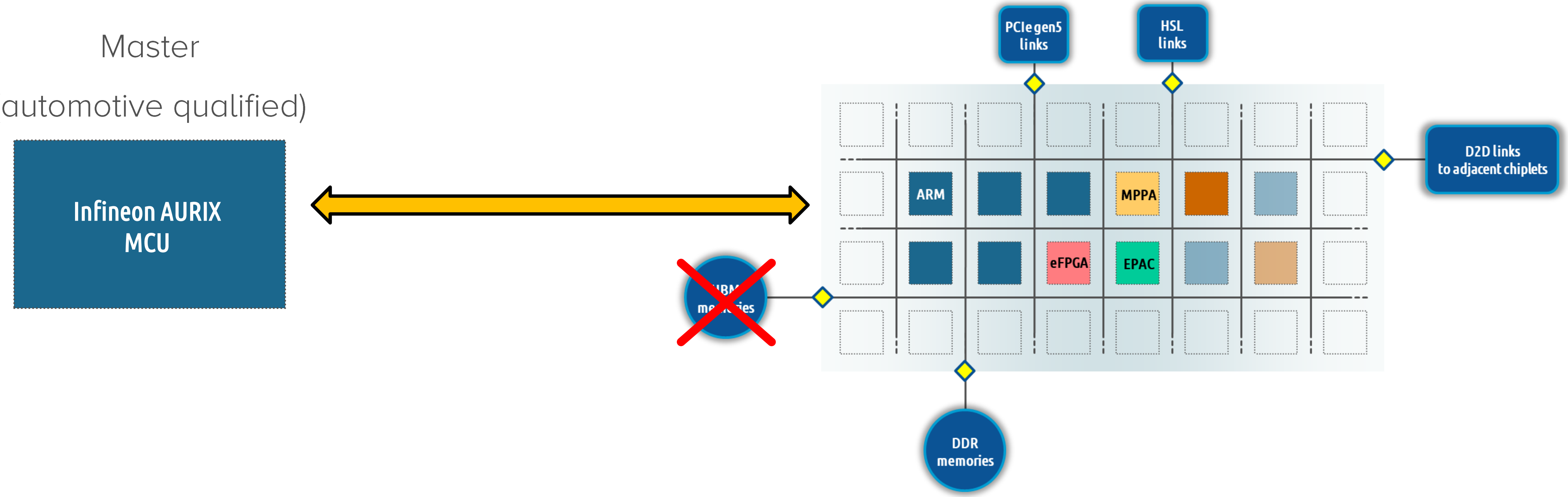
- Specifically designed to meet automotive requirements for any safety integrity level
  - E.g. Infineon AURIX processor family
- But insufficient performance for some ADAS and AD applications
  - ADAS: Advanced Driver Assistance System
  - AD: Autonomous Driving
- GPP can deliver performance needed
  - … but must also meet automotive requirements

THE EPI APPROACH: EMBEDDED HPC ARCHITECTURE

Master

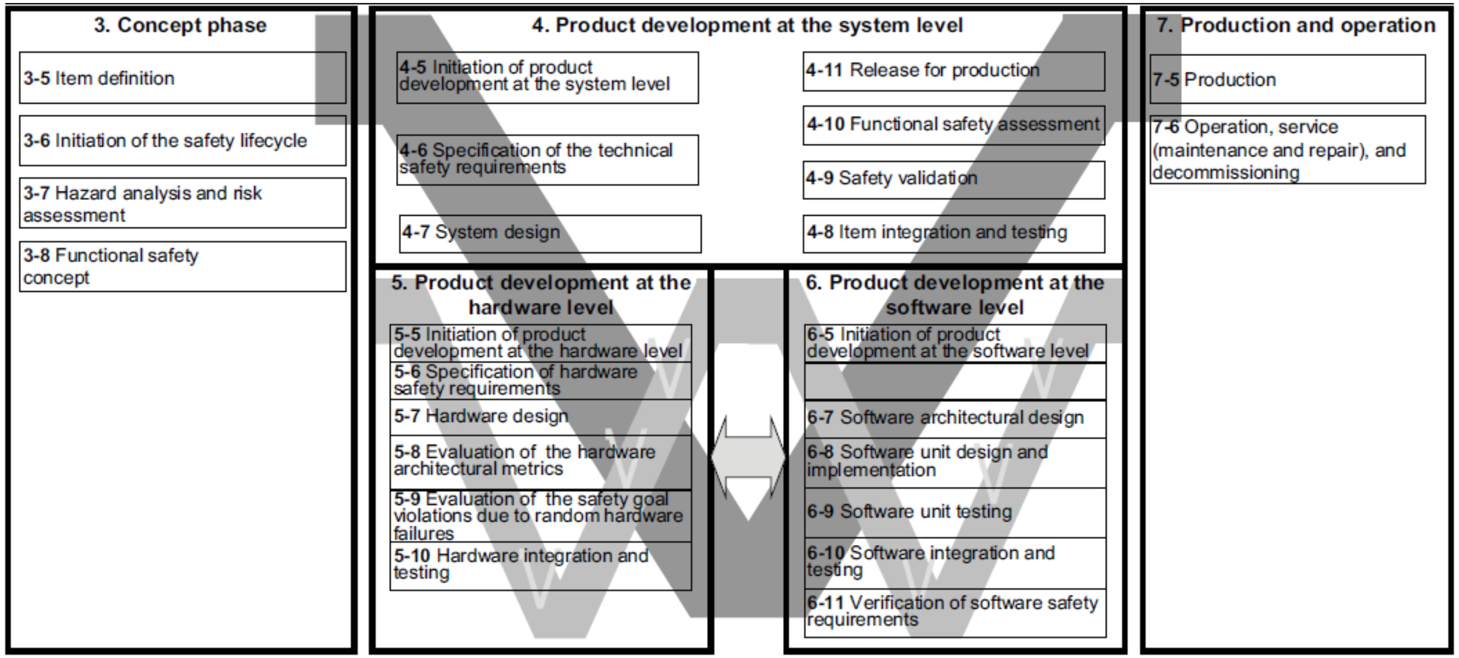
(automotive qualified)

Slave



SAFETY LIFECYCLE (ISO26262)

- Safety lifecycle intended for items designed to offer appropriate safety measures
  - Observability, controllability, diverse redundancy, watchdogs, etc
- GPP is, by nature, against some of these requirements
  - Target: average case, not worst case
  - Few safety measures
- Fitting automotive safety lifecycles is a complex challenge



3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development at the system level

4-5 Initiation of product development at the system level

4-6 Specification of the technical safety requirements

4-7 System design

4-11 Release for production

4-10 Functional safety assessment

4-9 Safety validation

4-8 Item integration and testing

5. Product development at the hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Evaluation of the hardware architectural metrics

5-9 Evaluation of the safety goal violations due to random hardware failures

5-10 Hardware integration and testing

6. Product development at the software level

6-5 Initiation of product development at the software level

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

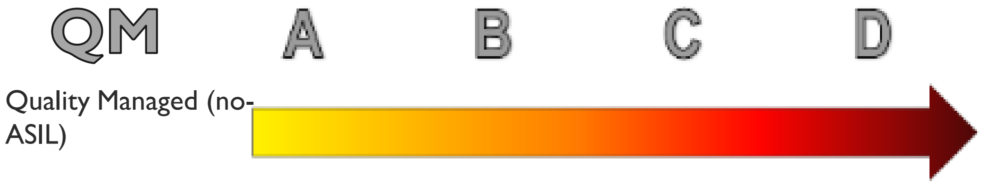
7. Production and operation

7-5 Production

7-6 Operation, service (maintenance and repair), and decommissioning

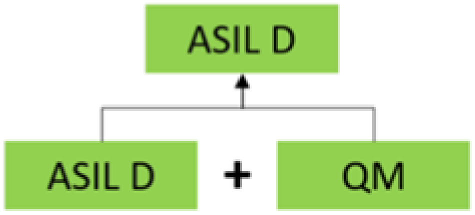
AUTOMOTIVE SAFETY REGULATIONS: ISO26262 AND SOTIF

- Functionalities are classified in different Automotive Safety Integrity Levels (ASIL) based on:
  - Severity
  - Exposure
  - Controllability upon failure
- Higher levels implies stricter design and V&V process
  - Increase costs
  - More difficult to achieve



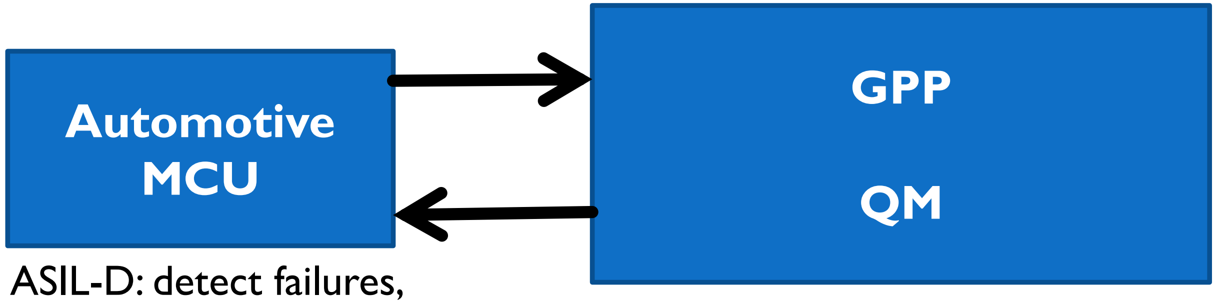
REQUIREMENTS FOR ADAS

- An ADAS unavailable system is a safe system
  - No fault tolerance needed
  - Just detect faults and reach a safe state timely
- ASIL-D MCU monitoring QM GPP
  - No safety requirements for GPP



✓ Fail-safe

✗ Fail-operational

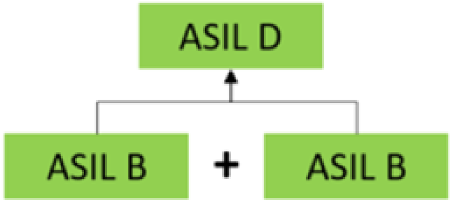


ASIL-D: detect failures, transfer control to the driver (e.g. lane detection)

QM: can be switched off upon a failure

REQUIREMENTS FOR AD

- An AD system must remain always available
  - Fault tolerance needed (no safe state!!)
  - Detect and recover from faults timely
- GPP must also reach ASIL-D (potentially with some help of the MCU)

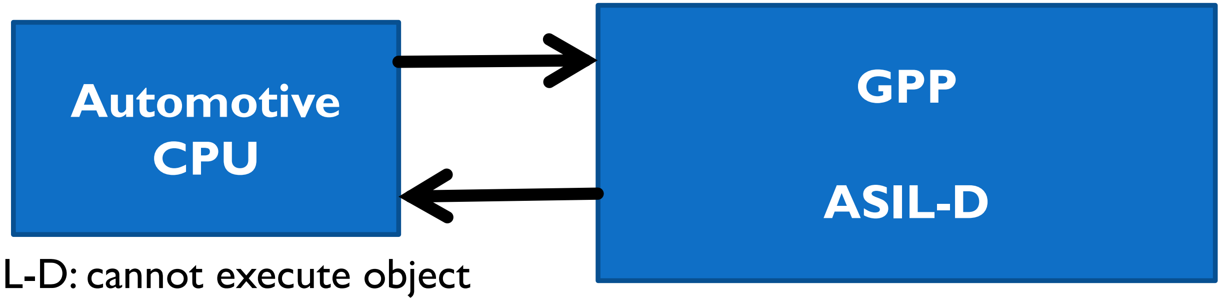


ASIL D

ASIL B + ASIL B

✓ Fail-safe

✓ Fail-operational



Automotive CPU

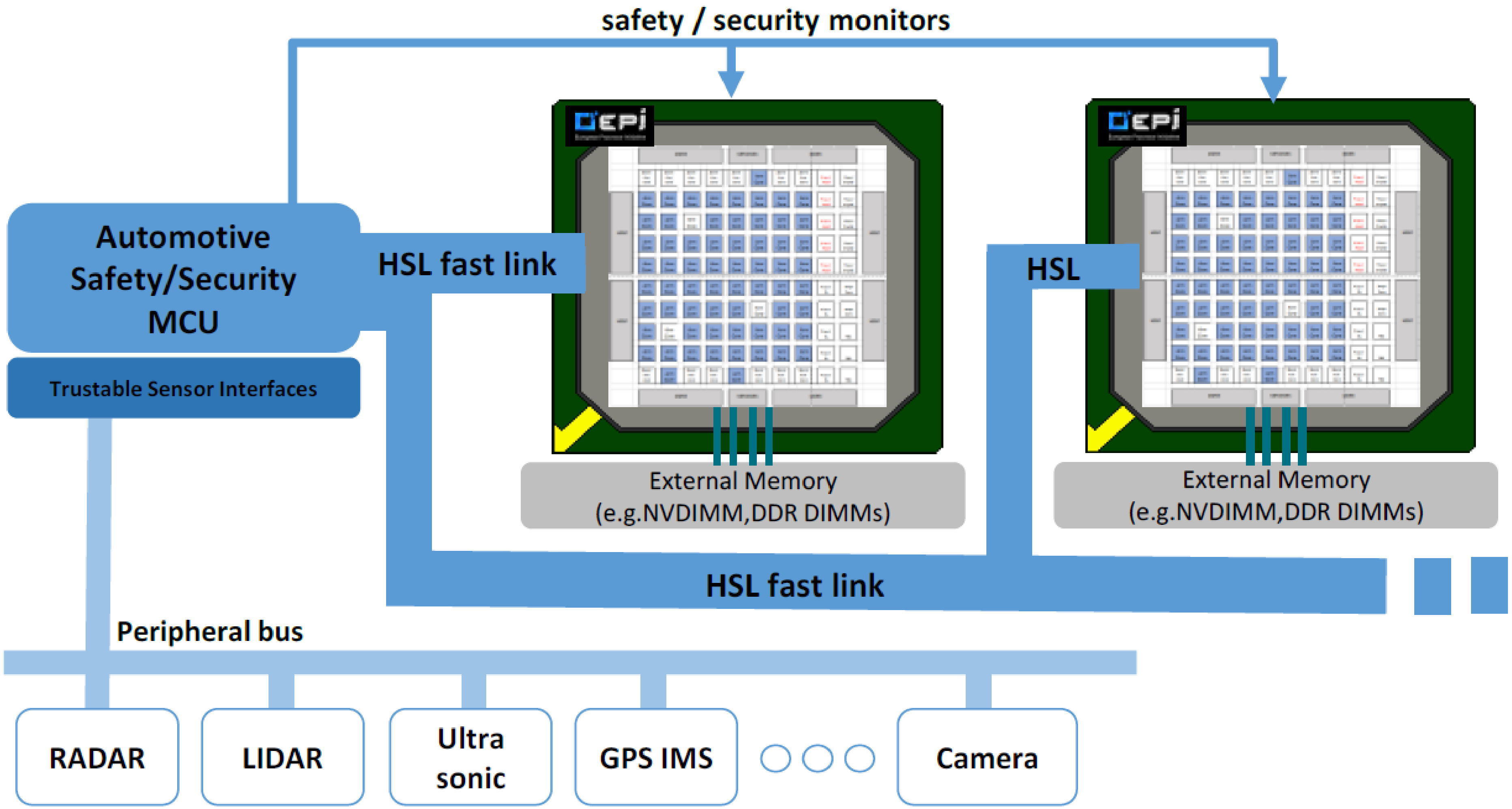
GPP

ASIL-D

ASIL-D: cannot execute object detection (too much performance needed)

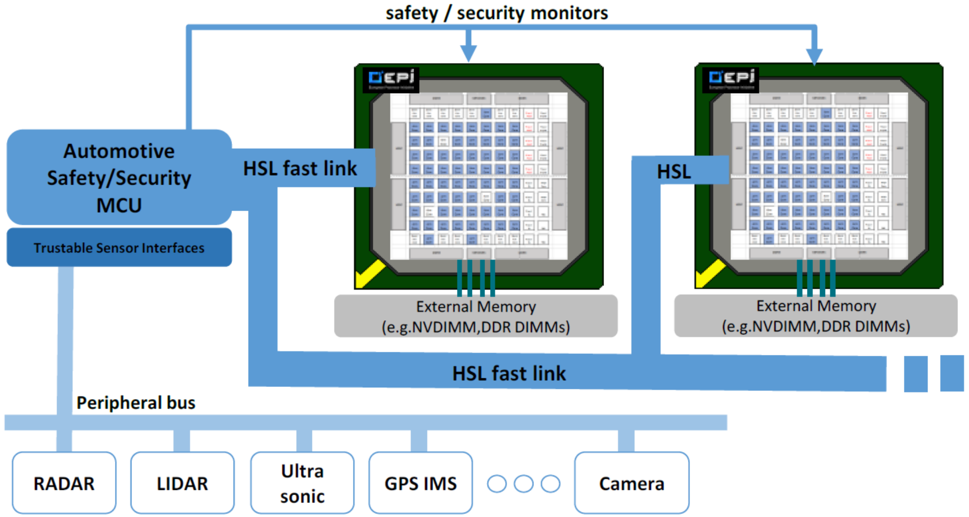
ASIL-D: no driver to transfer control, must be fault-tolerant

AUTOMOTIVE EPI ARCHITECTURE DETAILS


safety / security monitors
Automotive Safety/Security MCU
Trustable Sensor Interfaces
HSL fast link
HSL
External Memory (e.g.NVDIMM,DDR DIMMs)
External Memory (e.g.NVDIMM,DDR DIMMs)
HSL fast link
Peripheral bus
RADAR
LIDAR
Ultra sonic
GPS IMS
○○○
Camera

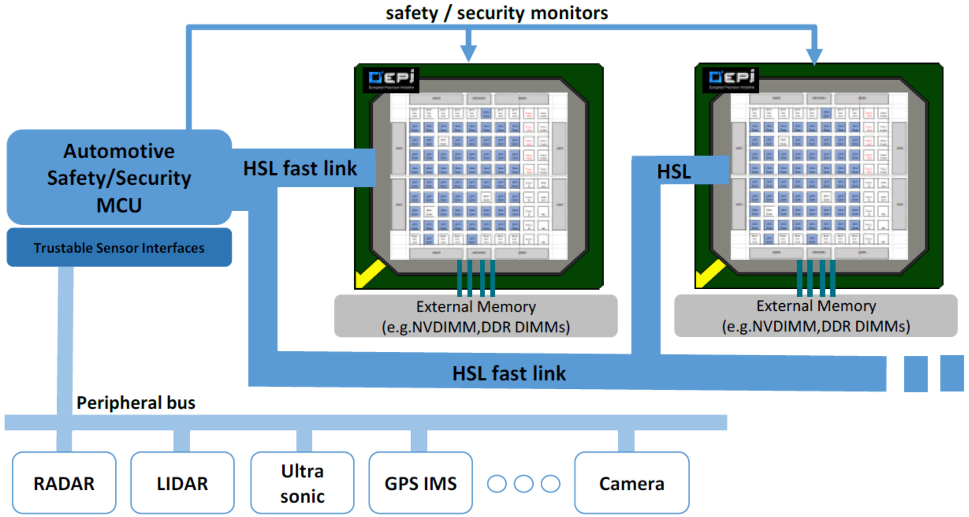
AUTOMOTIVE EPI ARCHITECTURE DETAILS

- Preferably a single GPP
  - As for automotive MCUs due to efficiency, reliability,…
- I/O managed by the MCU
  - As in today's systems
- Performance-demanding functionalities offloaded onto the GPP
  - Build upon interfaces compliant with auto reliability requirements
- MCU monitors execution in the GPP
  - No safety or security violations
  - E.g. no resource flooding, no resource overutilization


safety / security monitors
Automotive Safety/Security MCU
Trustable Sensor Interfaces
HSL fast link
HSL
External Memory (e.g.NVDIMM,DDR DIMMs)
External Memory (e.g.NVDIMM,DDR DIMMs)
HSL fast link
Peripheral bus
RADAR
LIDAR
Ultra sonic
GPS IMS
Camera

AUTOMOTIVE EPI SOFTWARE STACK

- Build upon AUTOSAR (AUTomotive Open System ARchitecture)
  - Standardized SW architecture
  - Defines interfaces, architecture of apps (SW components, runnables, tasks), diagnosis mechanisms
- MCU with classic AUTOSAR
  - Well stablished practice
  - Legacy SW, any app with sufficient performance in the MCU
- GPP with Adaptive AUTOSAR
  - Scale up to the challenge of complex platforms
  - High-performance CPU
  - Advanced communication with environment
  - Etc


safety / security monitors
Automotive Safety/Security MCU
Trustable Sensor Interfaces
HSL fast link
HSL
External Memory (e.g.NVDIMM,DDR DIMMs)
External Memory (e.g.NVDIMM,DDR DIMMs)
HSL fast link
Peripheral bus
RADAR
LIDAR
Ultra sonic
GPS IMS
○○○
Camera

CHALLENGES AHEAD

- Meet automotive requirements preserving performance
  - A single design meeting the requirements of HPC and automotive markets
- Reliability in harsh environments
  - Only reliable components implemented with reliable technology processes
- Sufficient degree of observability and controllability
  - MCU monitors GPP, and must detect faults quickly
  - MCU must have means to take corrective actions on the GPP to preserve fault tolerance
- Deliver performance needed for AD with fault tolerance
  - No safe state
  - HW design must meet not yet fully understood requirements of complex and changing SW systems

QUESTIONS?