

# Safety Analysis of NXP High-Performance Layerscape® Multicore Processors

Geoff Waters

Systems Engineer – NXP Digital Networking

---

October 2019 | Session #AMF-AUT-T3648



SECURE CONNECTIONS  
FOR A SMARTER WORLD

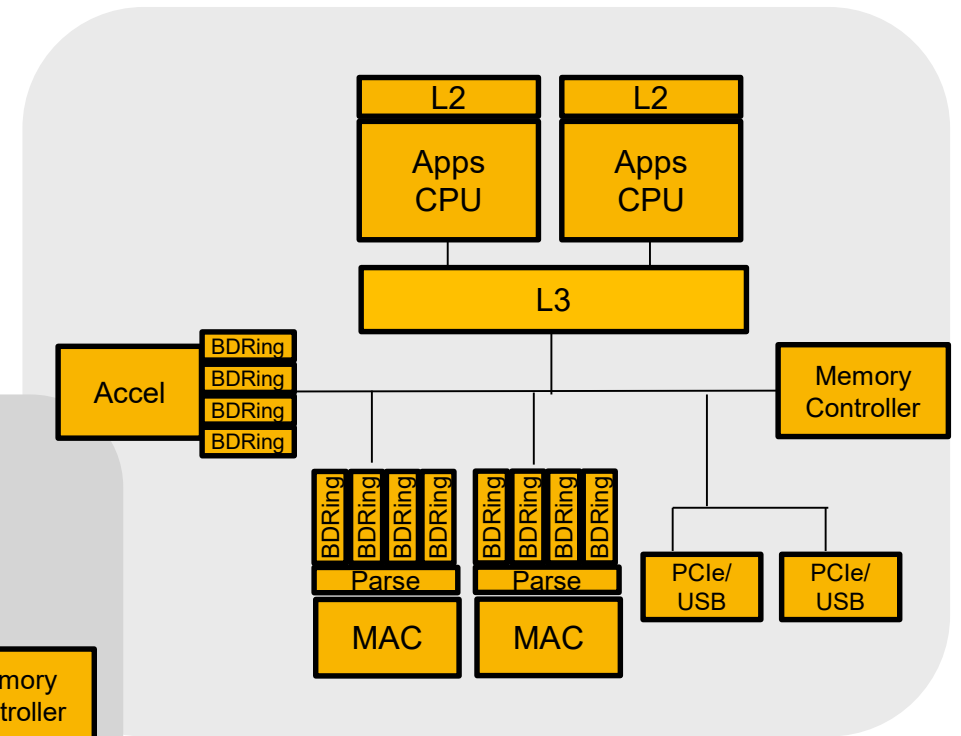
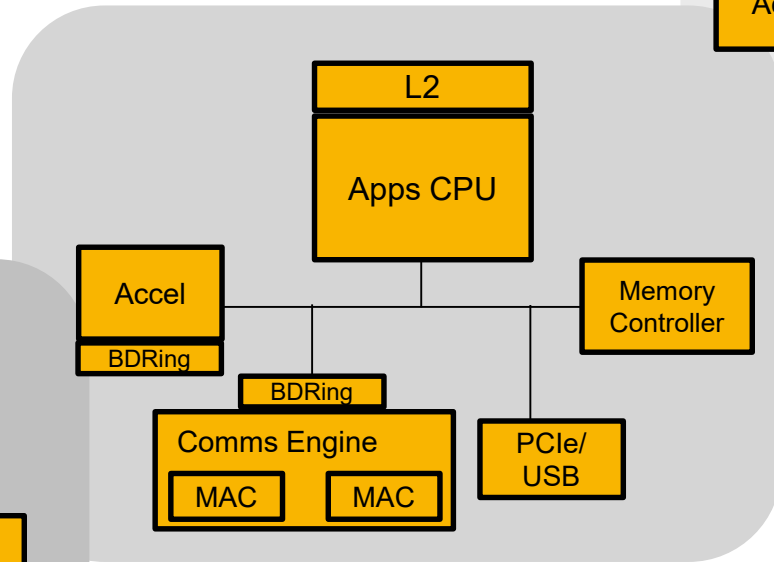
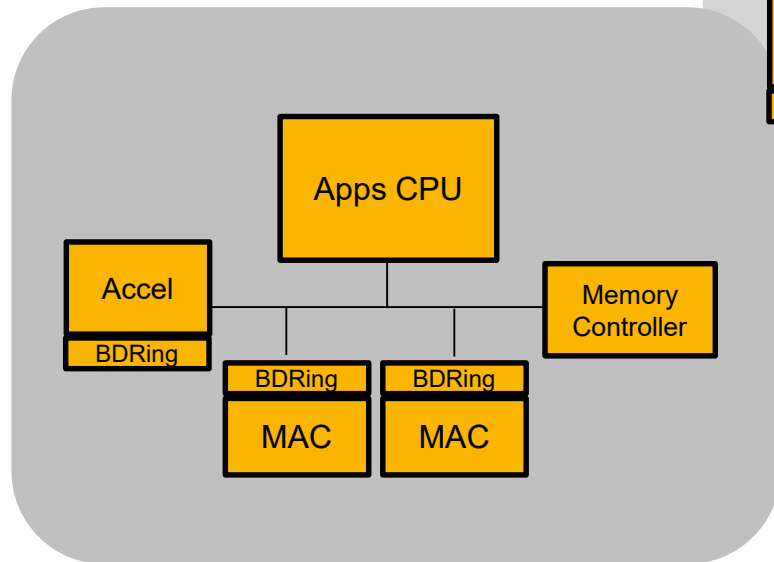
# Abstract

- High-performance processing in systems with high functional safety requirements has historically been a small segment in the overall processing market. Aerospace, high-end industrial, train & power grid control are traditional applications requiring high computing power with high fault detection coverage, and this 'niche' is exploding due to highly autonomous vehicles.
- This session will review the use of NXP's multicore processors in traditional safety critical applications, and the retroactive analysis of the Layerscape product family's fault detection mechanisms and coverage.

# The Safety Challenge of Complex Multicore SoCs

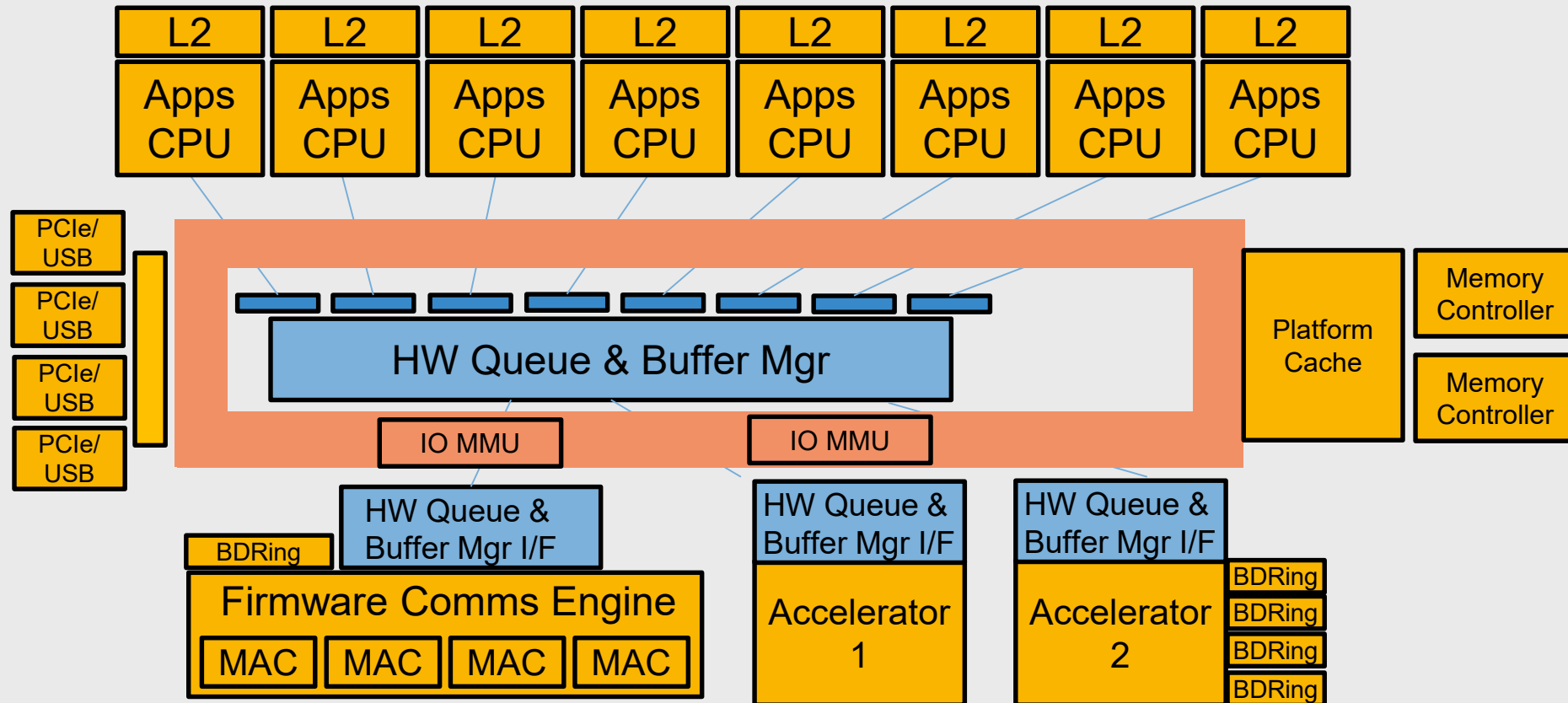


# Increasingly Complex SoCs



# P4080; NXP's First Many Core

Sampled 2008



# NXP Digital Networking SoCs in Safety Critical Applications

## Aerospace



Fuel Management, Main Flight Control, Secondary Flight Control, Aircraft Engine Management, Cockpit Display

## Railway



Traction Control, Railway Signaling Controller, Railway Communications, Brake Controller

## Factory Automation



Robotics Controllers, Motion Controllers, Multi-Axis Motor Controllers, Safety PLCs

## Power Grid



Power Distribution Relays, Smart Grid Communications

# Federated vs. Integrated Modular Avionics

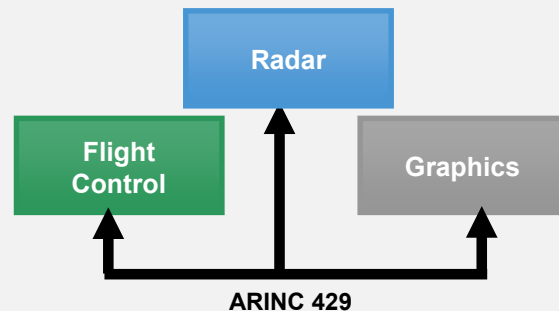
## Federated

### Advantages

- Independence of design and certification
- Well-understood methodology
- Established supply chain

### Challenges

- Greater space, weight, and power (SWaP) requirements
  - Each function is separate LRU
- Less software reuse
- Less portability, less modularity
- Cannot scale into larger platforms



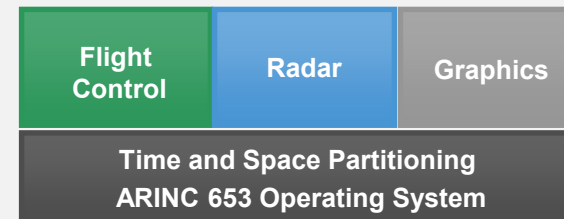
## IMA

### Advantages

- Lower SWaP requirements
  - Multiple functions on single LRU
- Better software reuse, refresh
- Better portability, modularity
- More efficient platform certification

### Challenges

- Greater complexity of system integration
- Greater complexity of design and certification
- Less experienced supply chain





# Federated vs. Integrated Modular Avionics

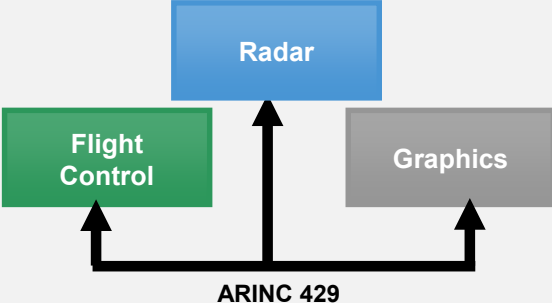
## Federated

**Advantages**

- Independence of design and certification
- Well-understood methodology
- Established supply chain

**Challenges**

- Greater space, weight, and power (SWaP) requirements
  - Each function is separate LRU
- Less software reuse
- Less portability, less modularity
- Cannot scale into larger platforms



The diagram illustrates a federated avionics architecture. It features three separate Linear Replaceable Units (LRUs): Flight Control (green), Radar (blue), and Graphics (grey). Each LRU is connected to a common ARINC 429 bus, which is represented by a horizontal line with three upward-pointing arrows leading to each LRU.

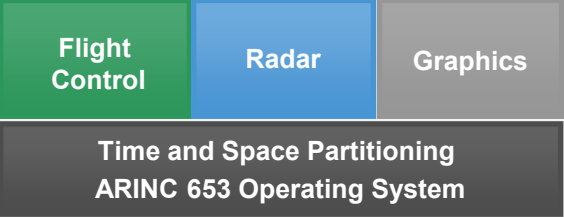
## IMA

**Advantages**

- Lower SWaP requirements
  - Multiple functions on single LRU
- Better software reuse, refresh
- Better portability, modularity
- More efficient platform certification

**Challenges**

- Greater complexity of system integration
- Greater complexity of design and certification
- Less experienced supply chain



The diagram illustrates an Integrated Modular Avionics (IMA) architecture. It shows three functions (Flight Control, Radar, and Graphics) integrated onto a single LRU. The functions are represented by colored blocks (green for Flight Control, blue for Radar, and grey for Graphics) stacked on top of a dark grey base labeled 'Time and Space Partitioning ARINC 653 Operating System'.

IMA with mixed criticality software requires proving adequate time & space separation



# Multicore for Avionics (MCFA) Working Group

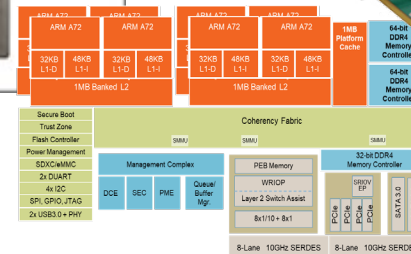
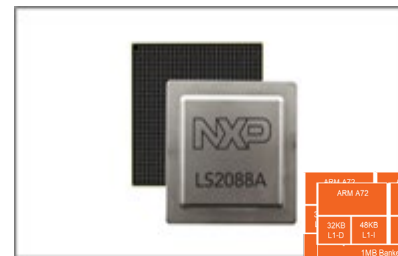
Objective: To assist avionics suppliers certify equipment which use NXP multicore SoCs

## MCFA Goals:

- Develop a partnership between NXP and the avionics industry
- Find industry consensus on NXP data to be requested
- Transfer basic SoC design and verification information to group members
- Allow review of other artifacts which are then summarized for the group
- Minimize SoC supplier effort by providing data to the whole group

## MCFA Does Not:

- Compel disclosure of NXP proprietary information
- Expect DO-254/EUROCAE ED-80 compliance from NXP
  - Multicore processors treated as COTS products under DO-254, Sect 11.2



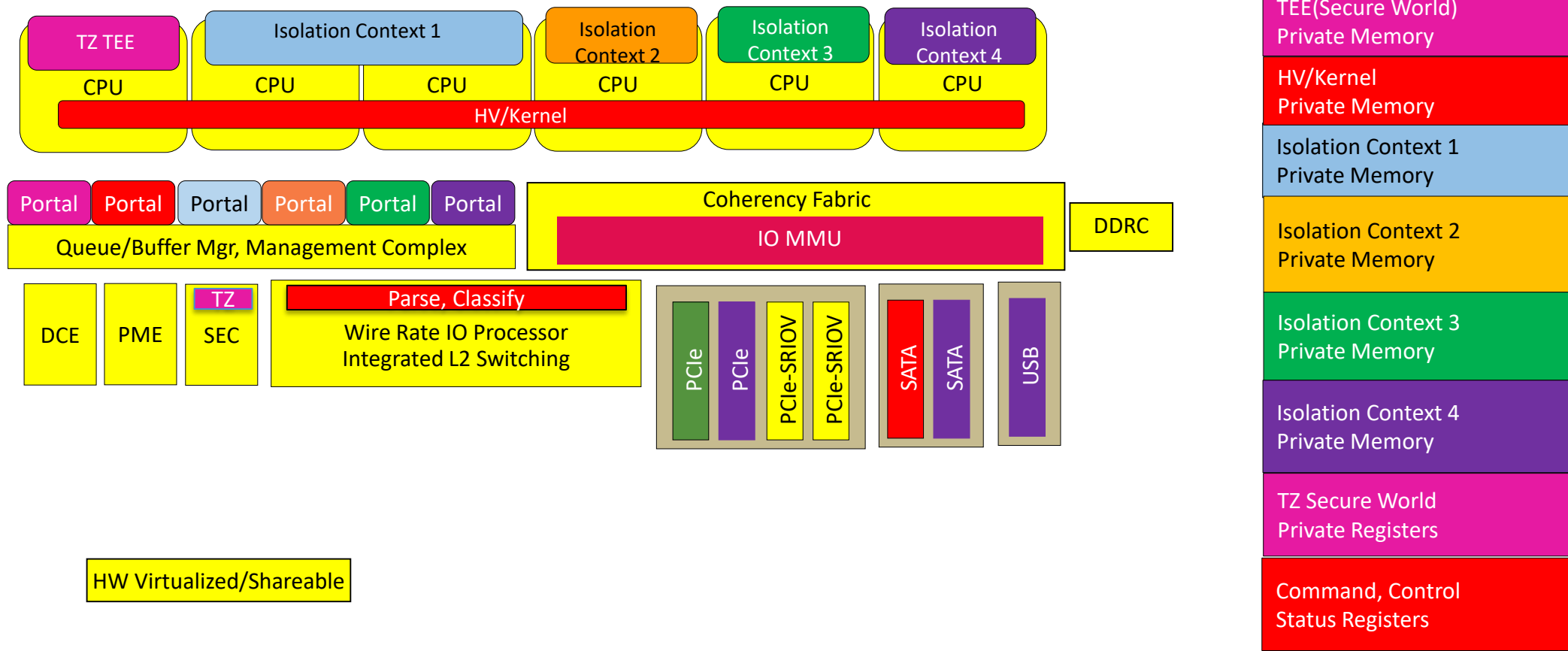
City/State

Date

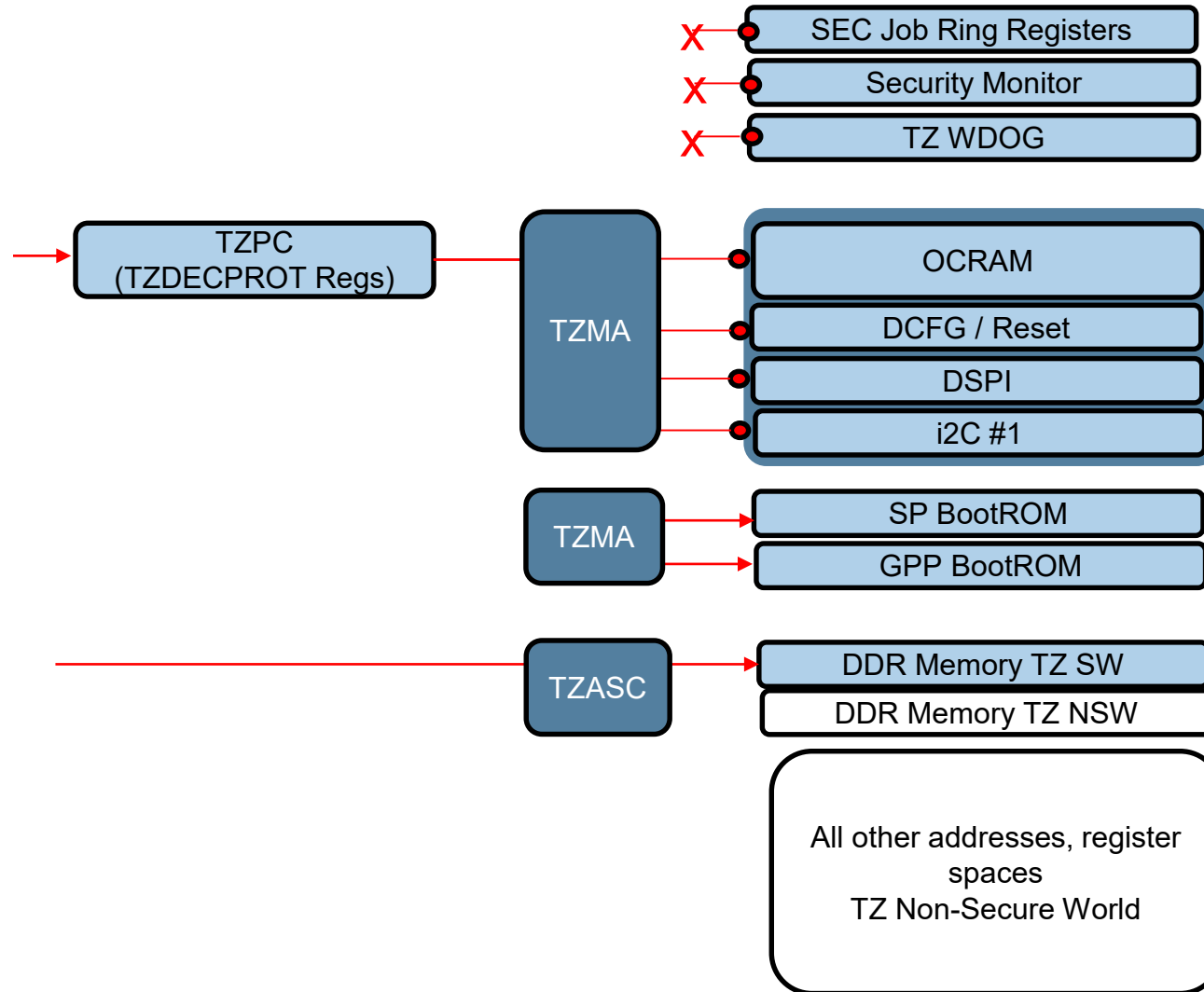
Austin | Texas

October 29-30

# Freedom from Interference Via Hardware Enforced Spatial Separation



# Protection of Critical Configuration Registers



LS2084 critical configuration registers are located in TrustZone Secure World memory space.

Only trusted firmware is able to access them.

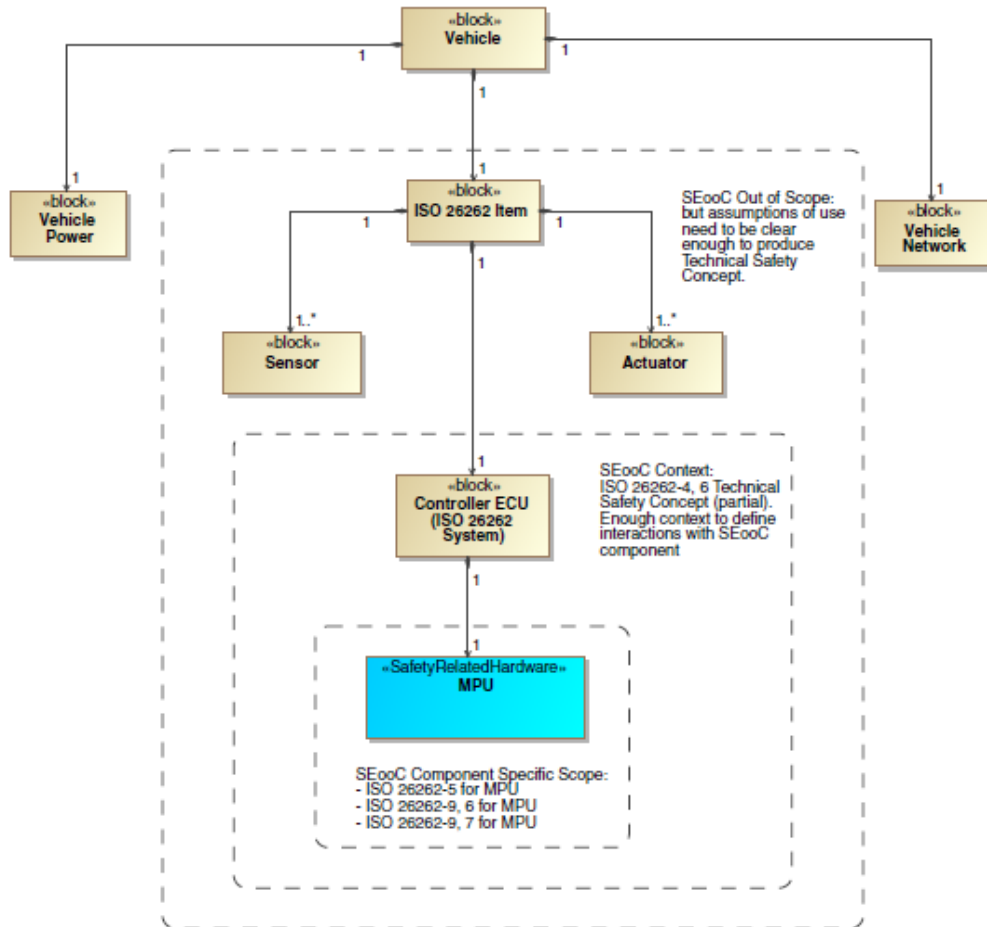
# Layerscape as ISO26262 SEooC



# Layerscape Safety Positioning

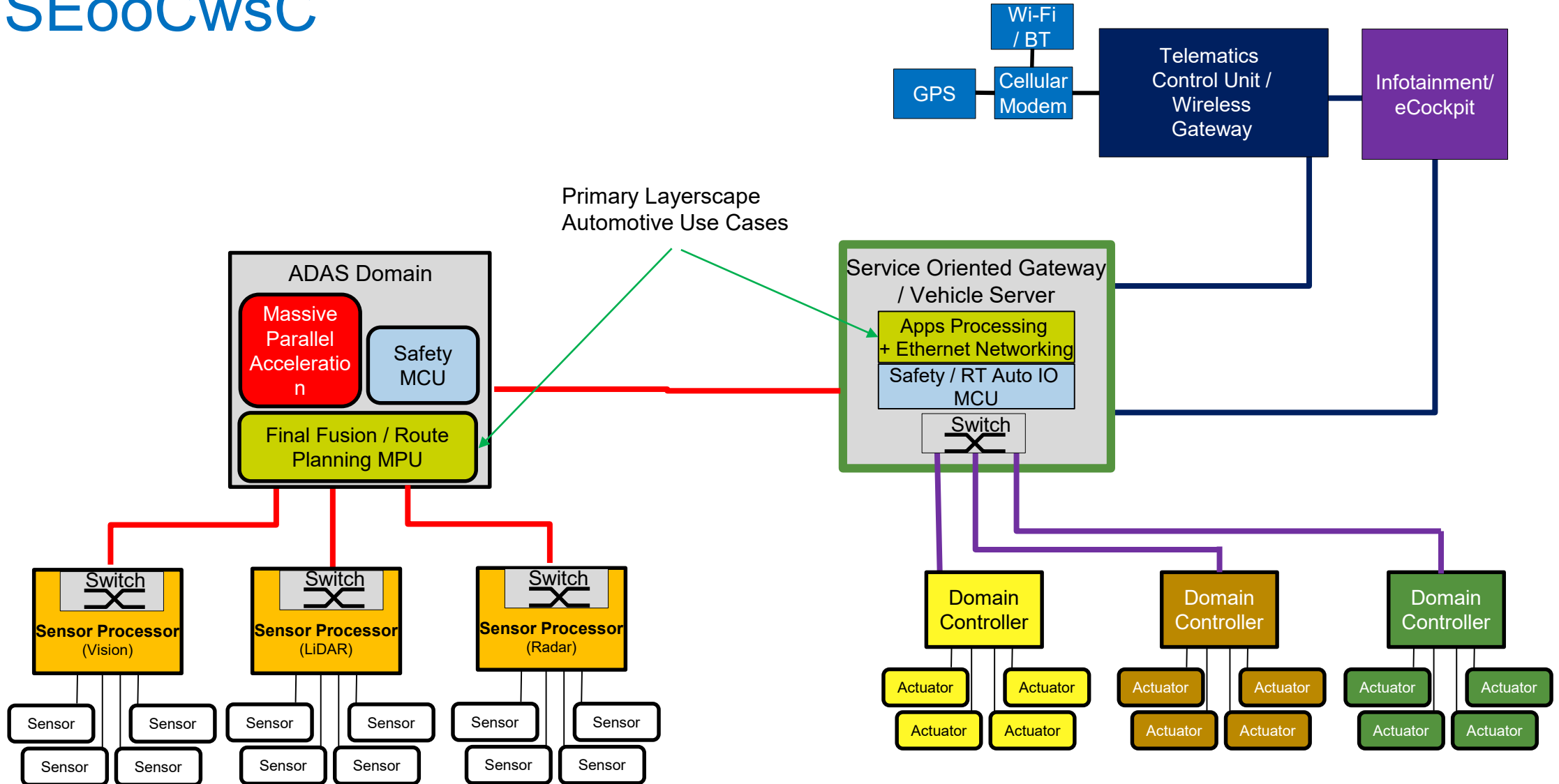
- Layerscape SoCs were not developed in accordance with ISO26262. All Layerscape safety analysis is retroactive, NXP does not have the auditable documentation trail from safety goals to implementation to validation normally available for automotive SoCs.
- This safety presentation introduces a reference application and outlines the systems engineering approach needed to use the LS2084A SoC in a QM(B) system. The approach here is based on the ISO 26262 “Safety Element Out of Context” (SEooC) development approach outlined in Part 10, Clause 9 of the standard.
- As in SEooC, the application presented here is notional. Actual deployment of a Layerscape SoC in a safety-critical application will require a full pass of safety analysis, validation, and verification using the actual design of the real system as a basis.

# SEooC Analysis Scope



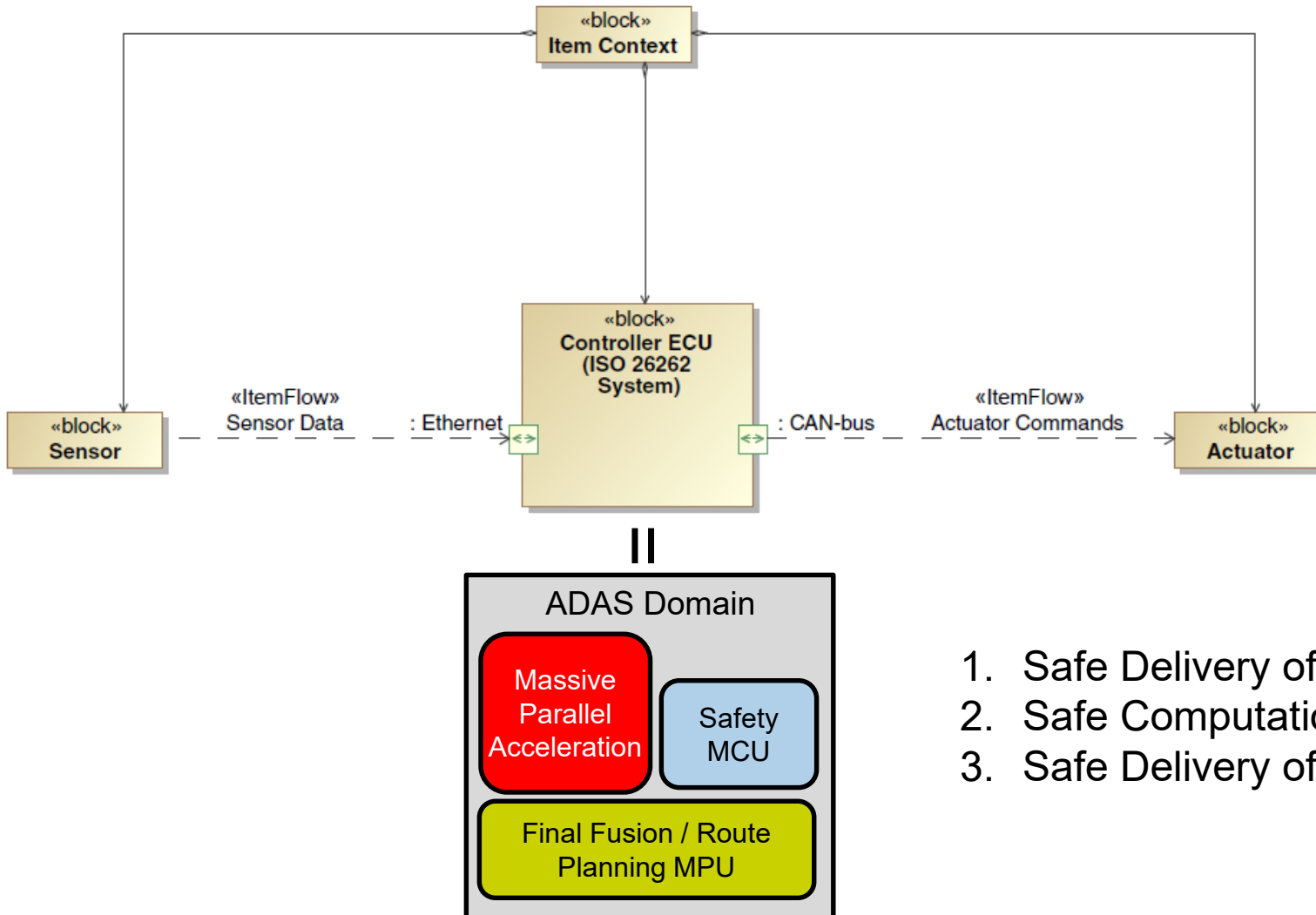
- Vehicle is out of scope.
  - Other systems in the vehicle such as power and networks that our SEooC interacts with are considered.
- The ISO 26262 “item” is out of scope.
  - Analysis makes assumptions allow development of the Technical Safety Concept.
- The electronic control unit (ECU) is the ISO 26262 “system” and is partially in scope.
  - We will develop enough of a technical safety concept to enable the safety analysis and concept for the MPU.
- The MPU is an ISO 26262 hardware component and is the focus of the SEooC safety analysis.

# SEooCwsC



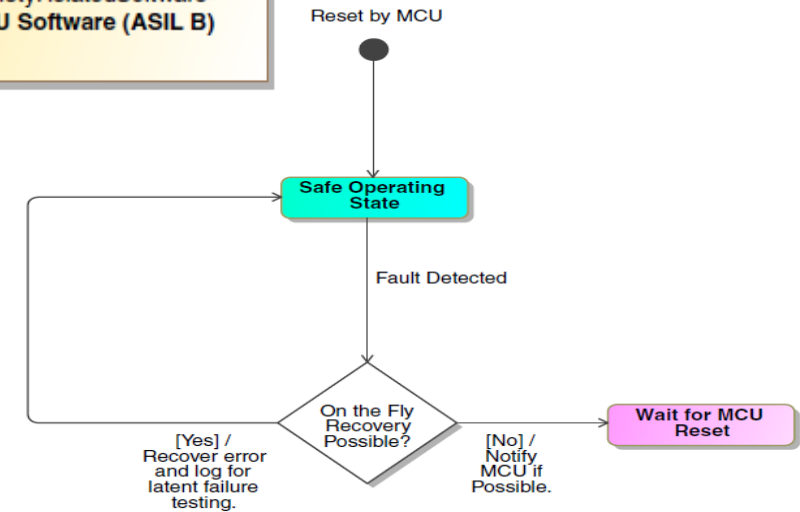
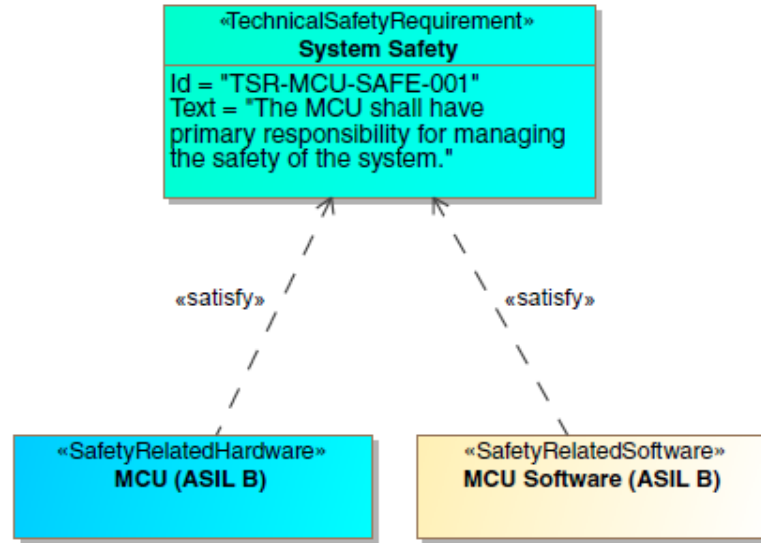
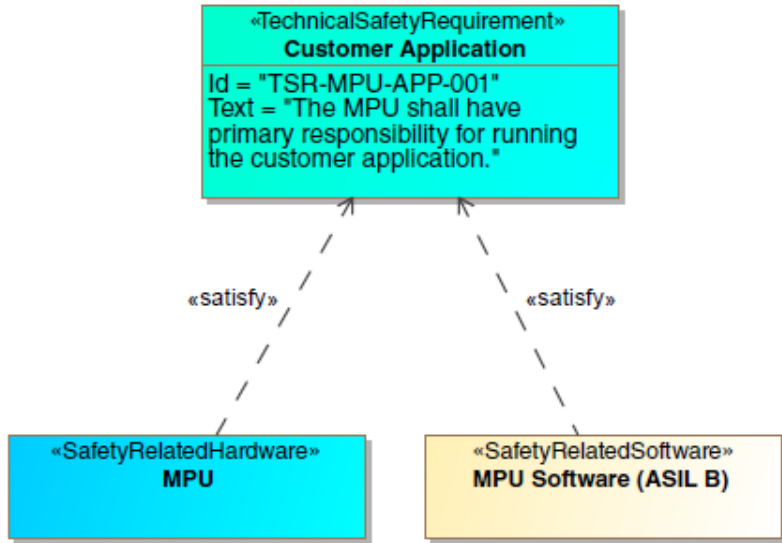


# Safety Goals

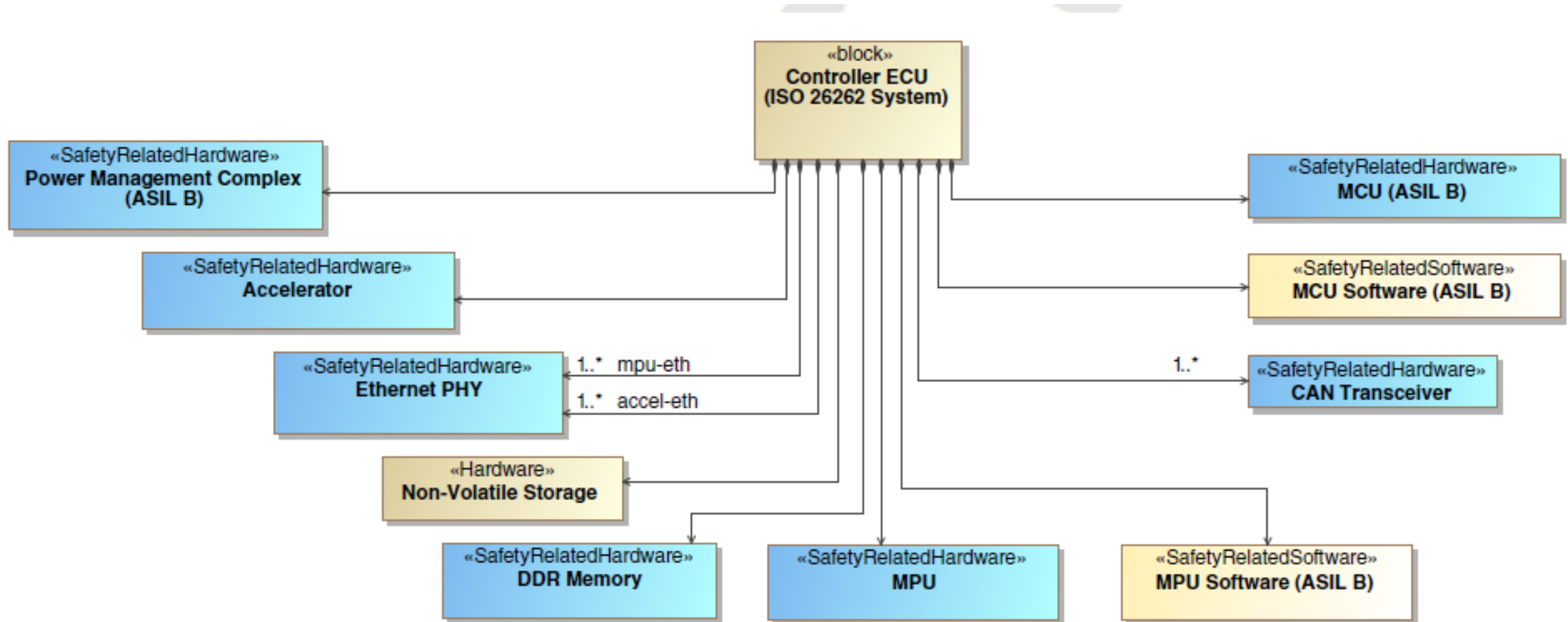


1. Safe Delivery of Sensor Data to Memory
2. Safe Computation
3. Safe Delivery of Command Messages to Actuators

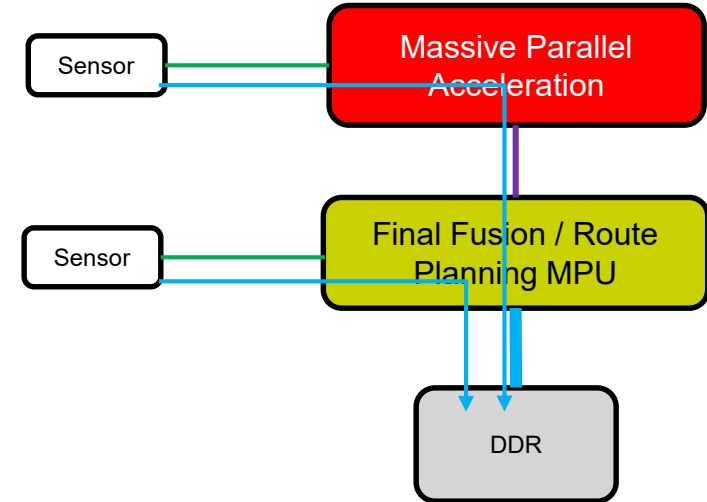
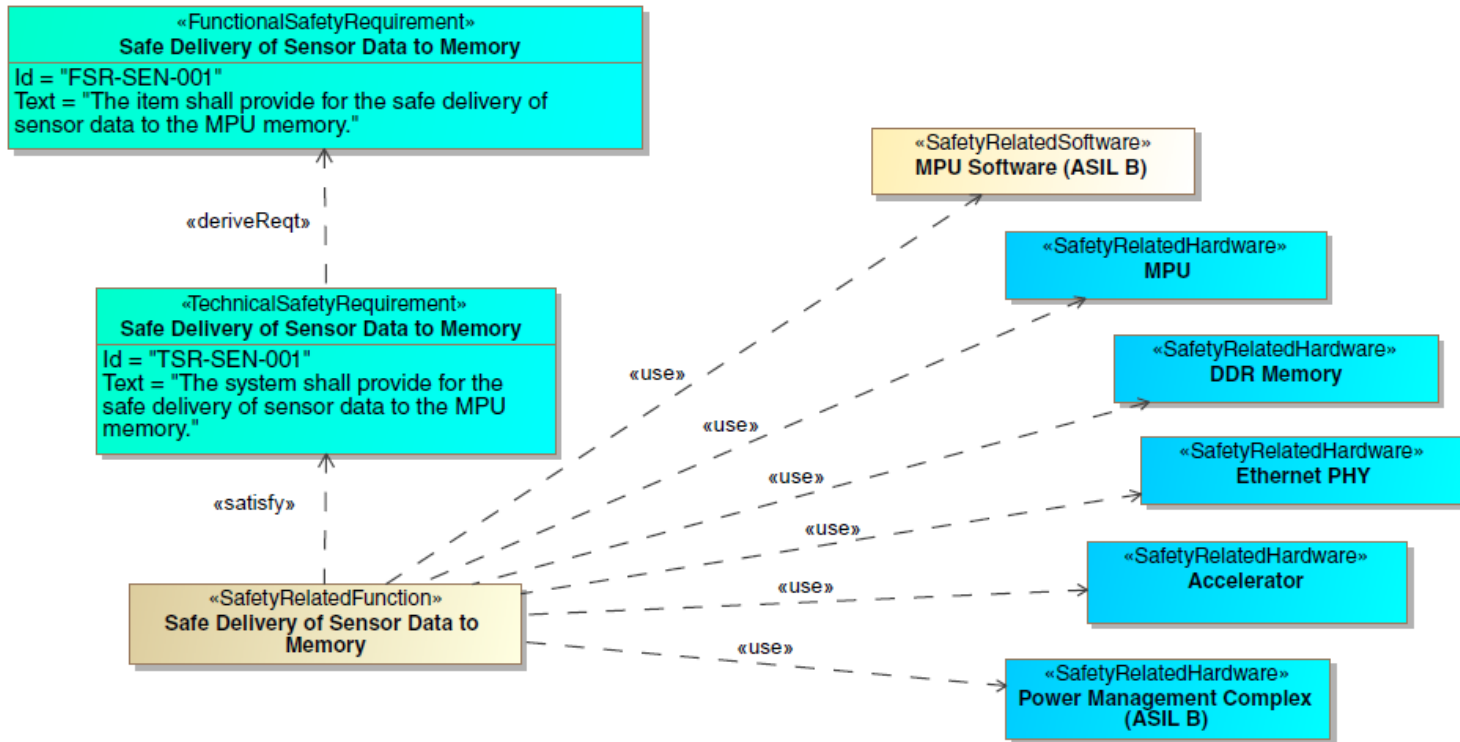
# General Safety Strategy



# ECU Components



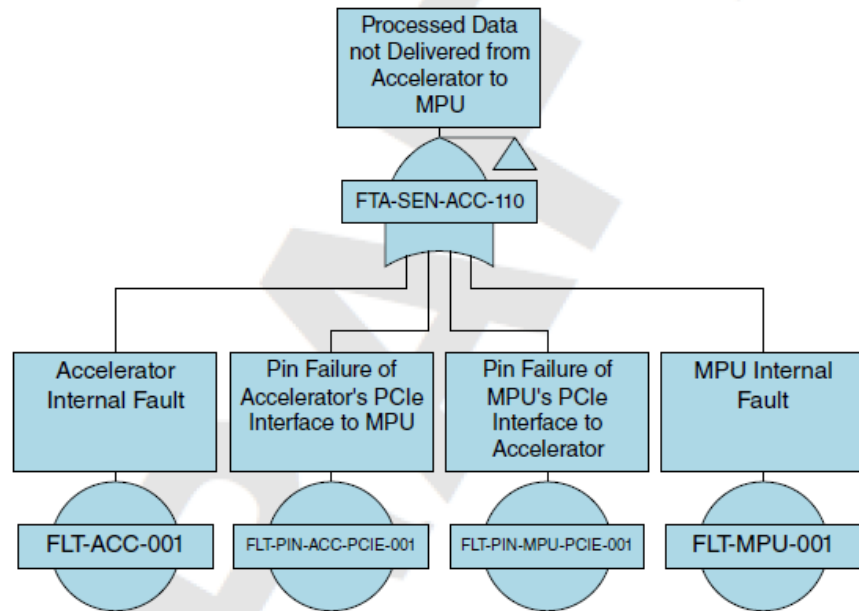
# FSR #1: Safe Delivery of Sensor Data to Memory



Paths analyzed;

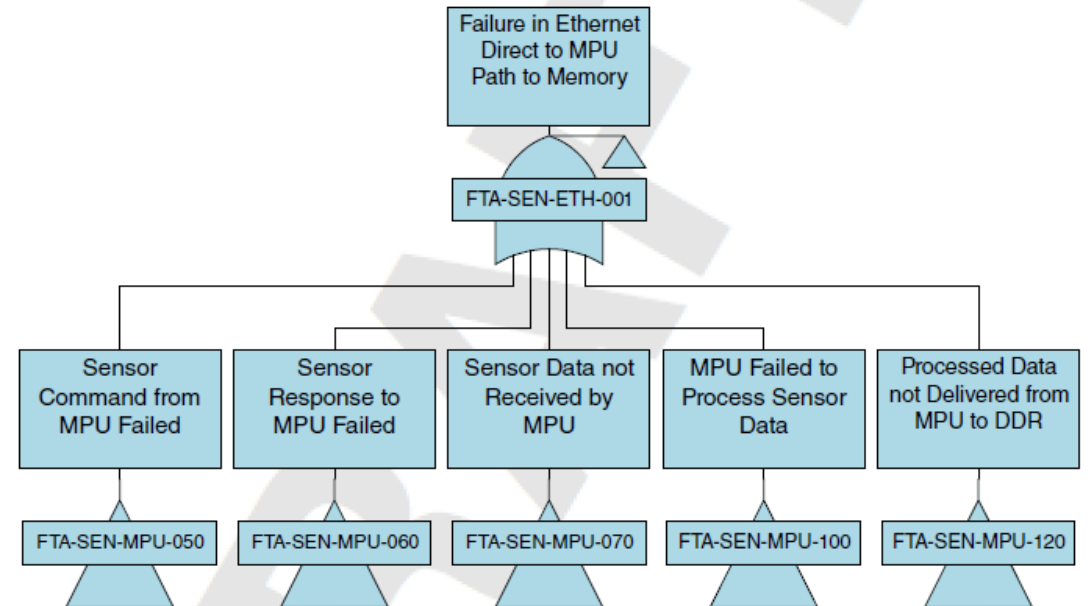
1. Sensor to accelerator (Ethernet), accelerator to MPU DDR (PCIe write)
2. Sensor to MPU DDR (Ethernet)
3. MPU/Accelerator commands to sensors (Ethernet)
4. Sensor command responses (Ethernet)

# Failure of Safe Delivery of Sensor Data to Memory



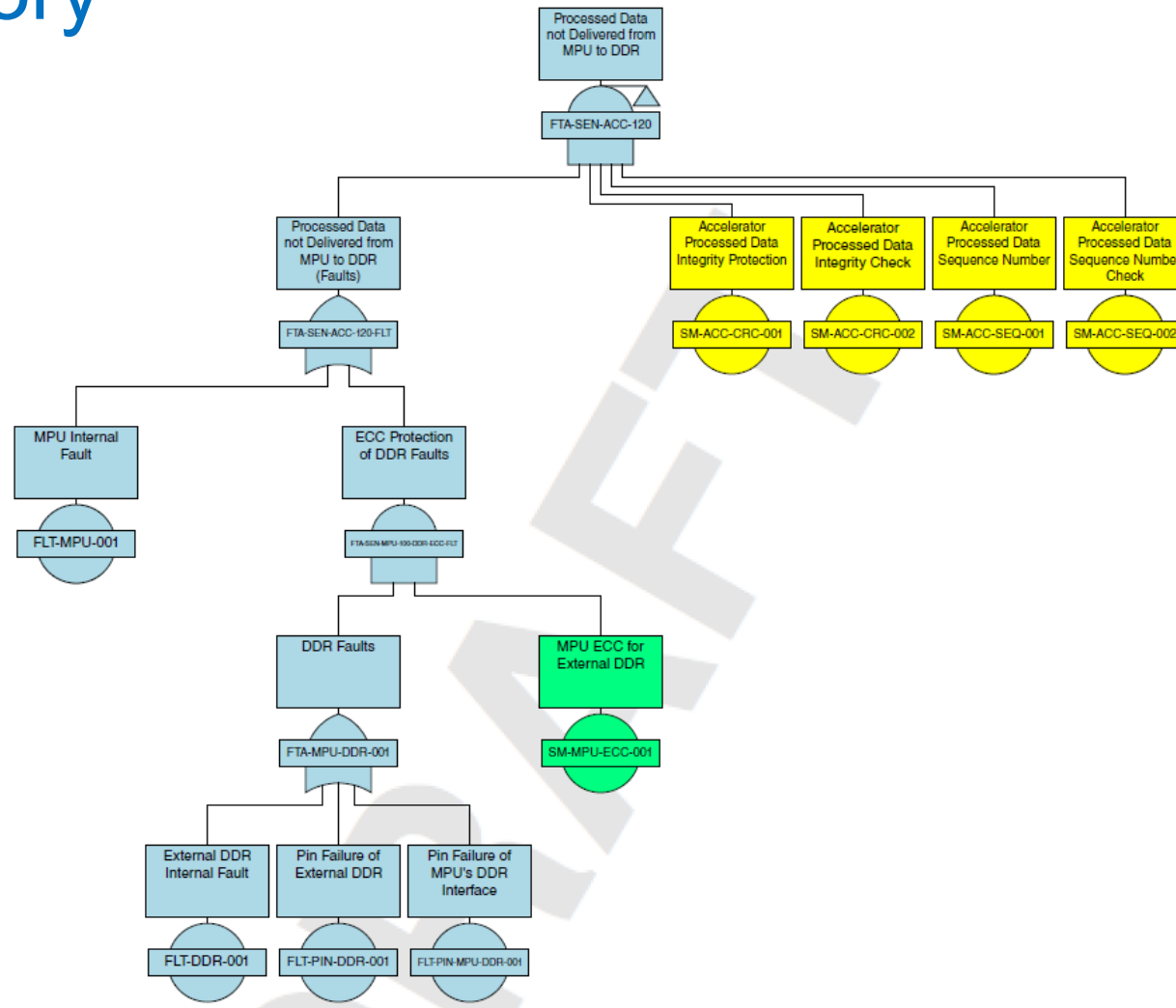
Additional scenarios;

1. Failure in accelerator path to memory
2. Sensor command from accelerator failed
3. Sensor response to accelerator failed
4. Sensor Data not received by Accelerator
5. Accelerator internal fault

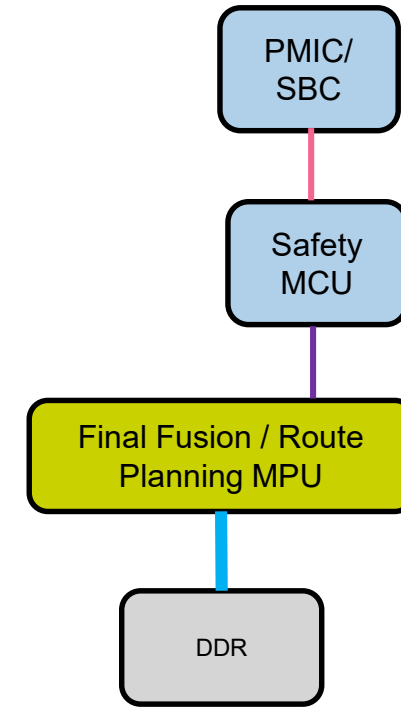
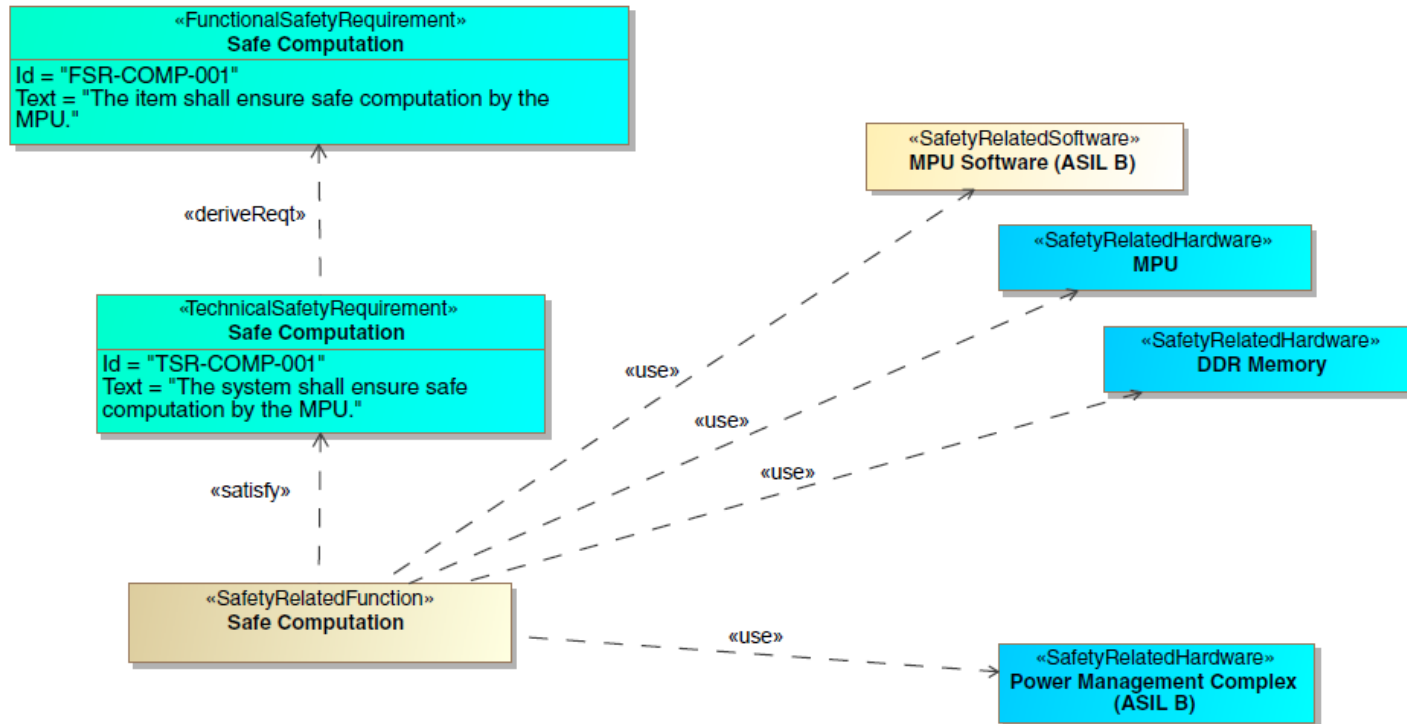


6. Processed data not delivered from MPU to DDR
7. Sensor Command from MPU Failed
8. Sensor response to MPU failed
9. Sensor data not received by MPU
10. MPU failed to process sensor data
11. Processed data not delivered from MPU to DDR

# Safety Mechanisms for Failure of Safe Delivery of Sensor Data to Memory



# FSR #2: Safe Compute

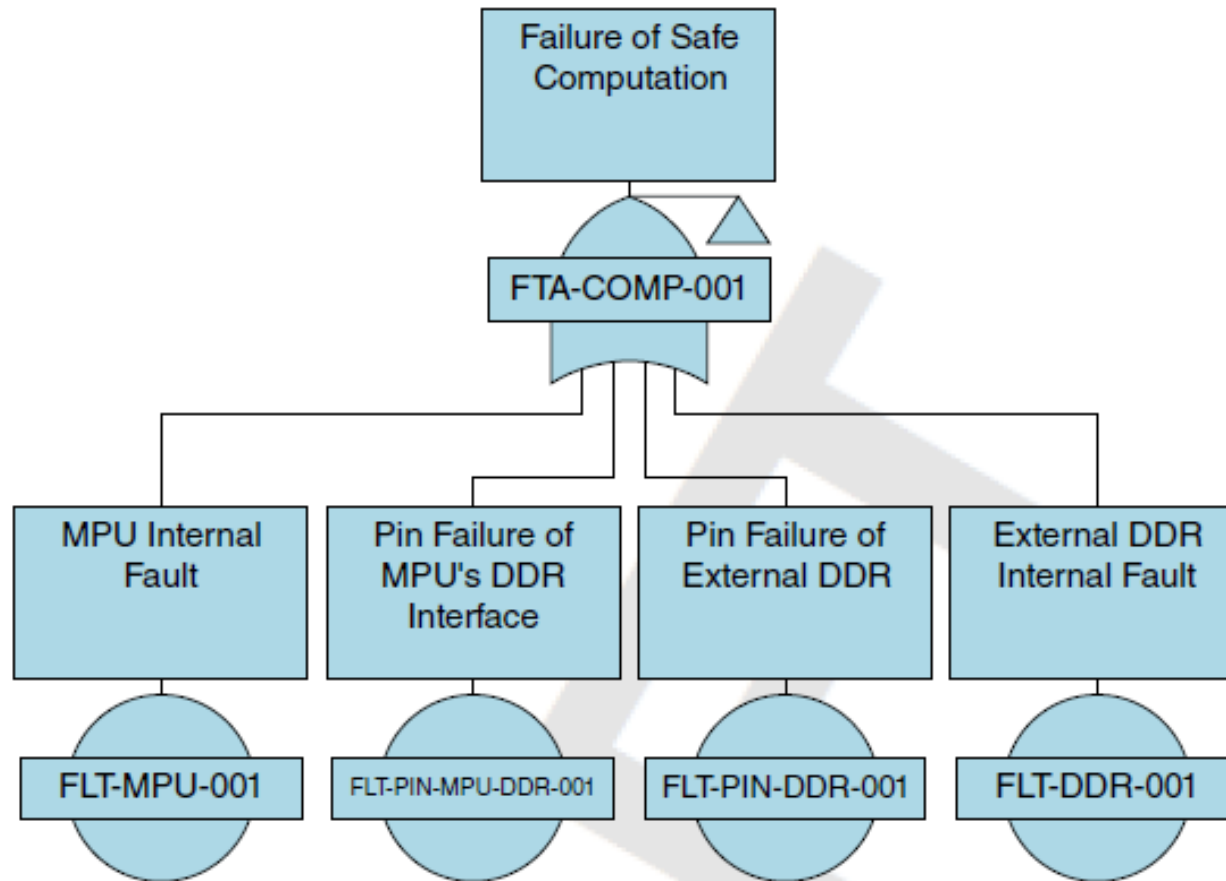


Paths analyzed;

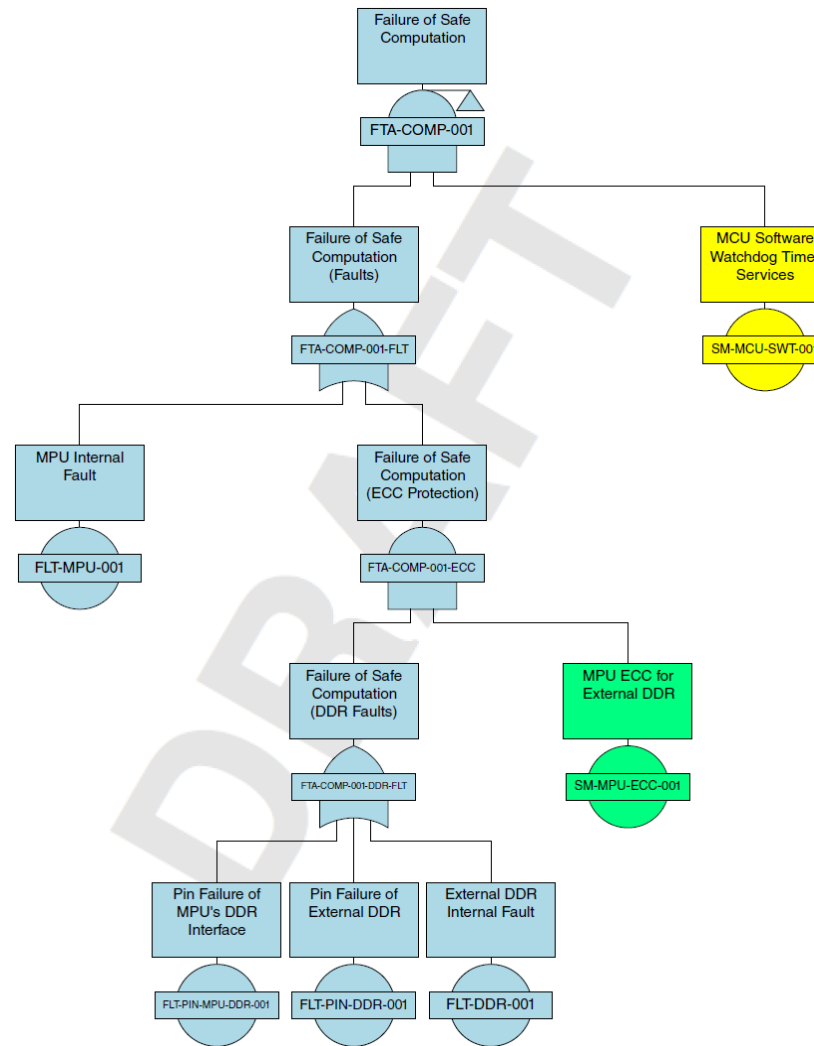
1. Instruction & data accesses (DDR) + internal computation
2. MPU interaction with safety MCU based watchdog (PCIe)
3. Safety MCU interaction with PMIC/SBC based watchdog (SPI)



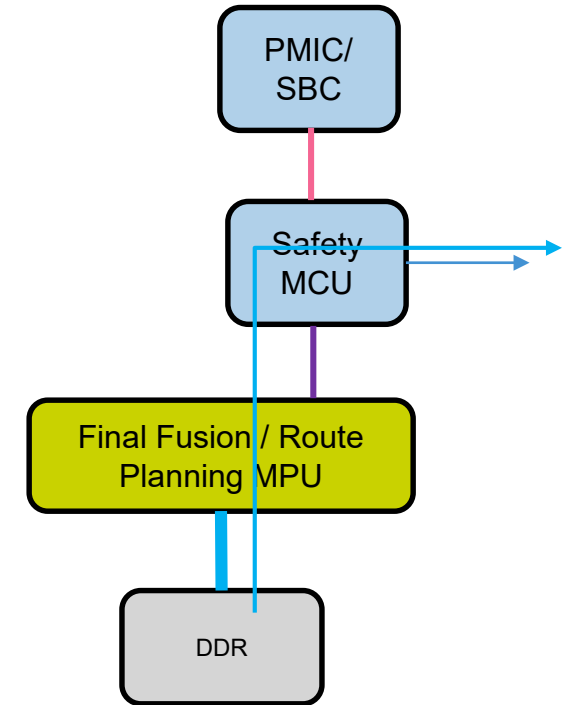
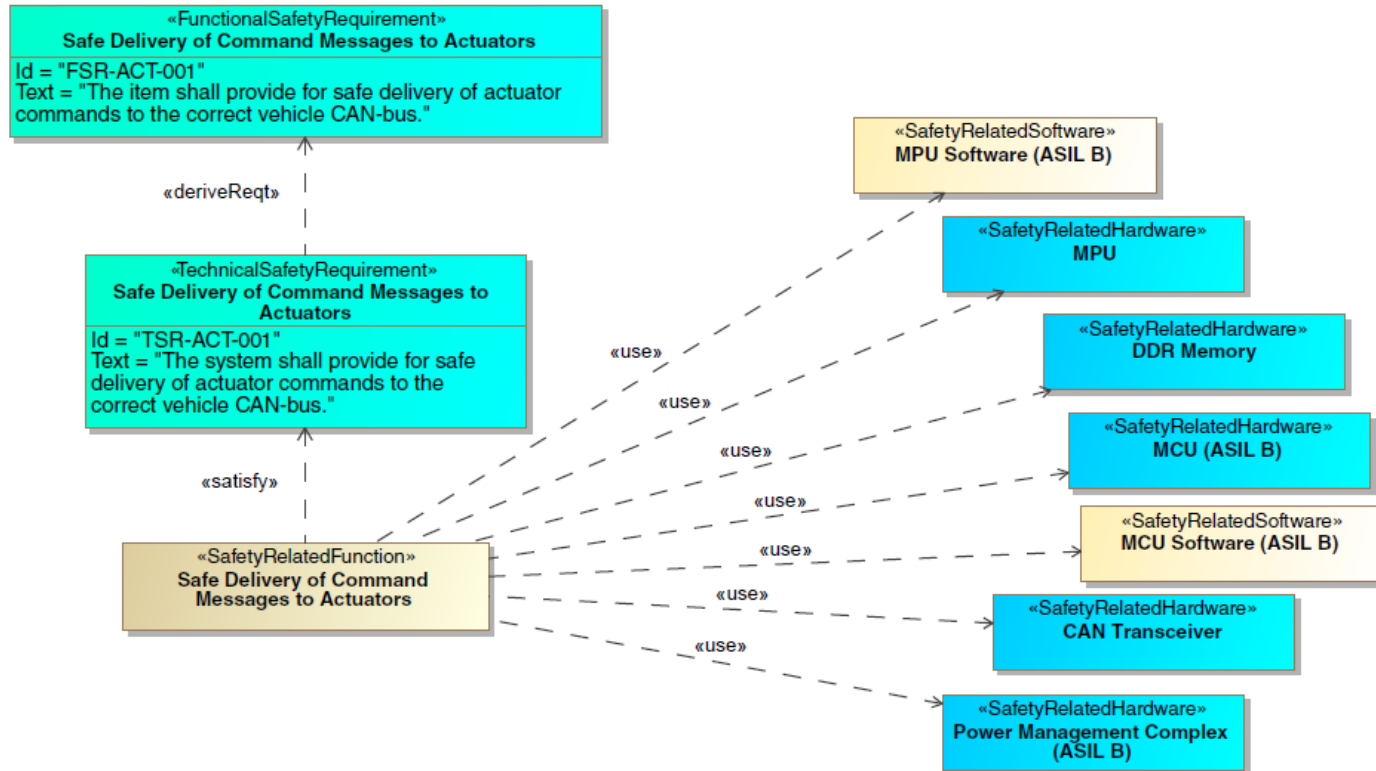
# Failure of Safe Compute



# Safety Mechanisms for Failure of Safe Compute



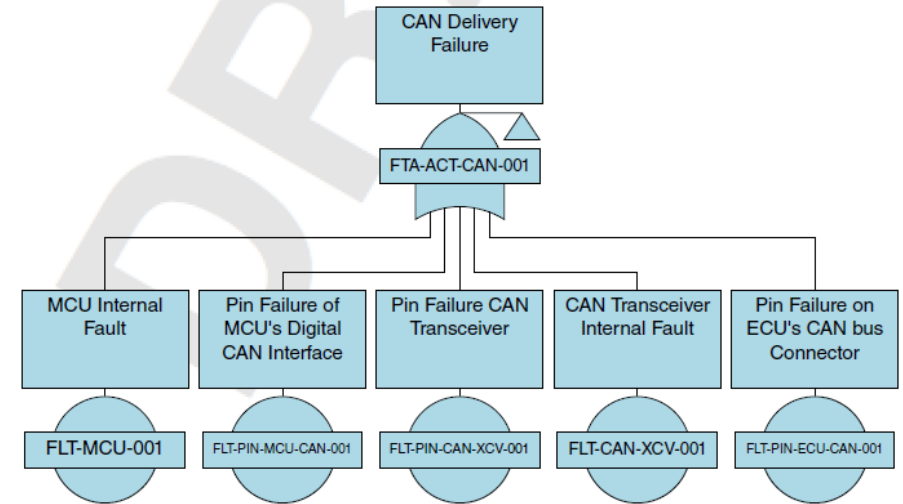
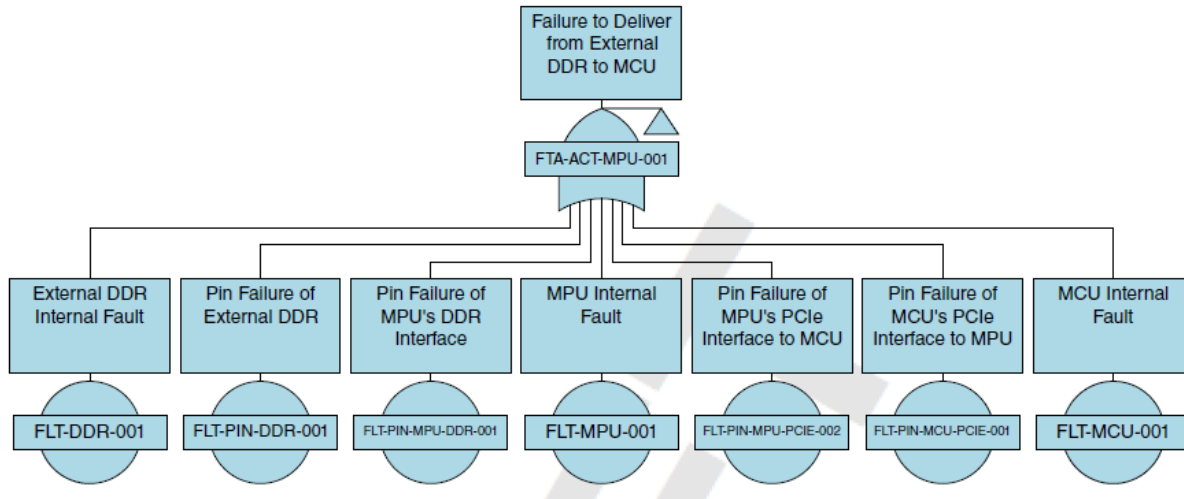
# FSR #3: Safe Delivery of Command Messages to Actuators



Paths analyzed;

1. MPU to Safety MCU (PCIe)
2. Safety MCU to actuators (CAN)

# Failure of Safe Delivery of Command Messages to Actuators

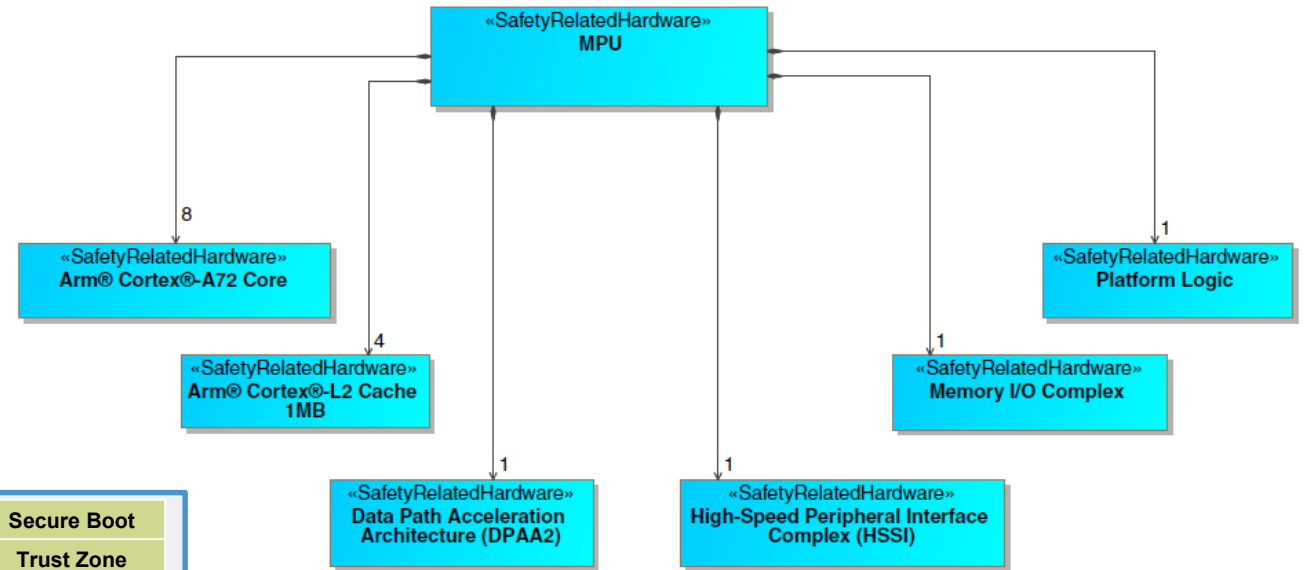
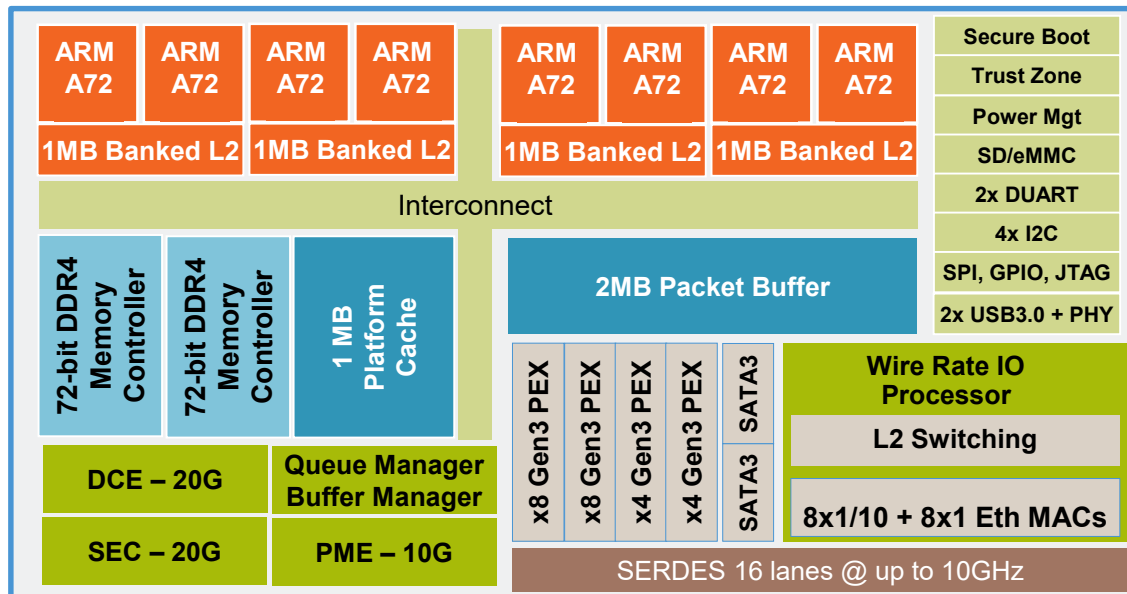


Additional scenarios;

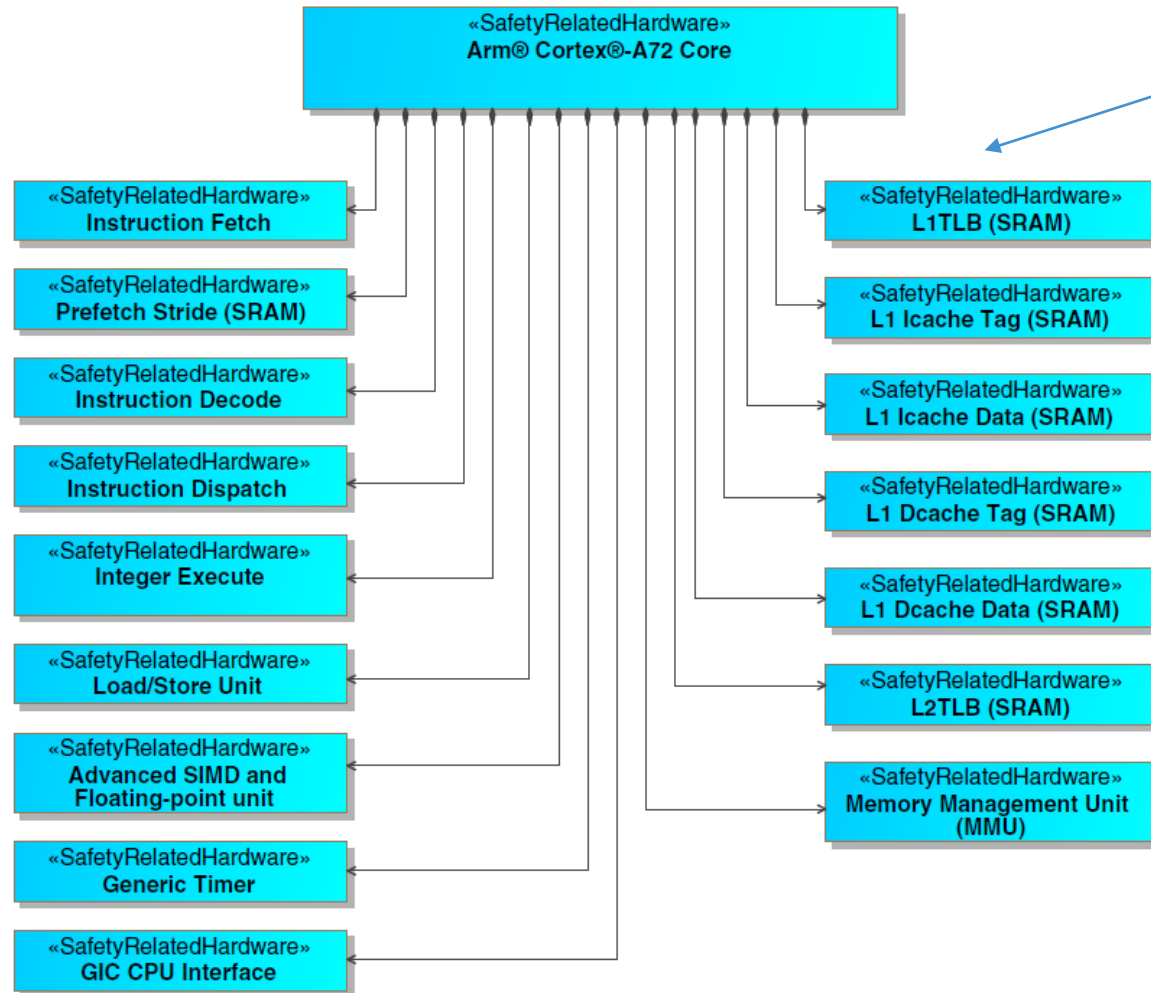
1. MCU failure to process

# MPU Components

## LS2084A

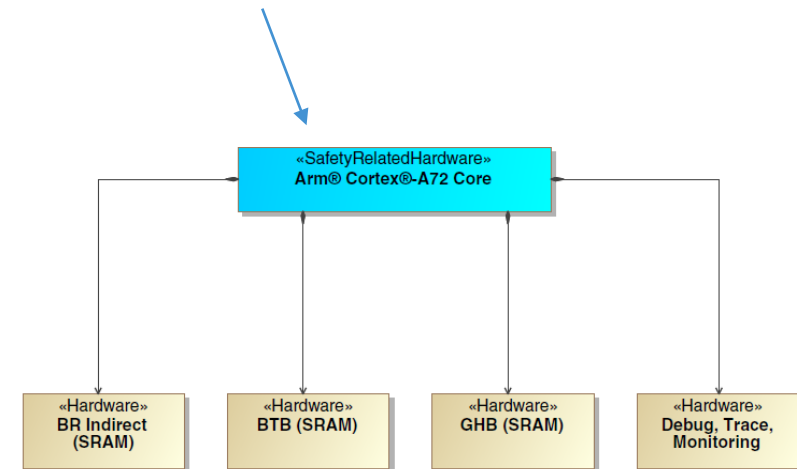


# MPU Part Safety Analysis



Faults in these A72 sub-parts lead to computation errors.

Faults in these A72 sub-parts don't impact computation, but may impact determinism.



# MPU On-Chip Safety Mechanisms

- **Detection of out of spec operating conditions**
  - Thermal Monitoring Unit
  - PLL loss of lock
- **Memory Corruption**
  - MBIST, error injection
  - All internal SRAMs have ECC or parity (only the smallest, most frequently read memories rely on parity)
  - DDR controller supports extra ECC data lines
    - Customers must provision boards with wider DRAM memories (x36 or x72) for the DDR controller to perform ECC
  - NVRAM corruption detection depends on the specific NVRAM interface.
    - Managed flash (ie QSPI) includes error detection.
- **Corruption within the interconnect (CCN-504); address||data parity on each 'flit'**
- **Hung/corrupted program execution**
  - Multiple watchdog timers (1 per core, plus TrustZone Secure World watchdog timer)
- **Freedom from interference (for partitioned systems)**
  - Memory access control
    - CPU MMU & IO MMU
    - Partitioning aware IO; Datapath acceleration architecture, PCIe SR-IOV



# Unsafe State Notification: Reset\_Request

Reset\_Req is used by LS to tell external logic that it is in an unrecoverable state and in need of reset.

Many unrecoverable errors are detected during SoC initialization, others are detected at runtime. Detection (and Reset\_Req assertion) can be triggered by hardware, firmware, or safety software.

## Sources:

- SERDES (PLL lock failure)
- Run Control Power Mgt (RCPM) Unit time-out
- POR BIST
- Multibit ECC Error
- Interconnect Misc Node
- Secure Debug Controller
- Security Monitor
- Service Processor
- Management Complex
- Integrated Flash Controller
- TrustZone Watchdog Timer
- Per CPU Watchdog Timers
- Any software with write access to Reset\_Ctl Register

# Communication Protocol Considerations

- Ethernet is not a reliable protocol. CRCs are used to detect corrupted frames, and these frames are discarded at the MAC.
  - Statistics are maintained on the number of discarded frames, thresholds can be set for generating interrupts if too many frames arrive corrupted.
- IP (OSI layer 3) is also an unreliable protocol. IPsec can be used to add cryptographic data integrity, encryption, and replay detection.
- OSI layer 4 options include UDP and TCP.
  - UDP/IP/Ethernet should be used where some packet loss is acceptable.
  - TCP/IP/Ethernet should be used where reliable transmission is required. If a portion of TCP data isn't delivered due to Ethernet frame corruption, the sending TCP stack will retransmit the missing data with sequence information, allowing the receiving TCP stack to reassemble the complete message.
- Application layer or middleware messaging (DDS) can implement reliable message delivery over reliable or unreliable network interfaces, or even over PCIe

# FMEDA

- **Permanent Failures in Logic Elements** - The methodology in (ISO 26262:11, 4.6.2) (which was adapted from the former IEC TR 62380) has been used to calculate an overall base failure rate for the die.
- **Allocation** - The overall die failure rate has been allocated to individual elements based on their ~die size as a % of the overall die.
- **Permanent Failures in SRAM Memories** - Same methodology used for logic elements is also used for SRAM memories.
- **Transient Failures in Logic Elements & SRAM memories** – Calculated by NXP process technology team using Fab data, backed by NXP’s own experimental results.
- **Package Failures** - The overall package failure rate is allocated to safety-related pins based on the number of safety-related pins divided by the total number of pins. Package failures are assumed to be permanent.
- **FFMi, safe** - Per (ISO 26262:10, 8.1.8, Figure 10, Note g) we have assumed  $F_{safe}$  of 0,5 (i.e. 50 %).
- **PMHF** - (ISO 26262:5, 9.4.2.2) requires that PMHF be calculated relative to safety goals. Safety goal violations cannot be directly identified in a SEooC analysis. Even in the context of an item with fully-defined safety goals, there are alternate methods of calculating PMHF which yield different results. LS FMEDA shows element failure rates and does not calculate an overall PMHF.
- **Diagnostic Coverage Assumptions** - Where possible, diagnostic coverage % assumptions are aligned with (ISO26262:5, Annex D):
  - Low = 30%, Medium = 60%, High = 90%
- **Use of Multiple Safety Mechanisms** - Not all safety mechanisms at the system level and at the MPU component level have been applied in the FMEDA. For each failure mode the safety mechanism with the highest diagnostic coverage has been applied. In a final in-context design, it may be possible to improve the metrics by applying secondary safety mechanisms and making a reasoned argument for a higher diagnostic coverage.

IEC 62380 Section	Integrated Circuits (Section 7)
Technology	MOS, BiCMOS (Low Voltage)
Technology Type Detail	MOS (Silicon, Standard Circuits)
MOS Type Detail	Micros, Digital Circuits, DSPs
Material Substrate	Epoxy Glass (FR4, G-10)
Package Failure Rate	Based on Number of Pins
Package Type	Epoxy (Plastic package)
Pin Type	PBGA
Thermal Resistance	Junction to Ambient
Thermal Package Type	BGA Plastic Package
Cooling Type	Fan assisted
Interface Circuits	Non Interfaces
Dissipated Power	37
Number of Transistors	~2B
Year of Manufacturing	2011
Number of Pins	1,292
Mission Profile	Standard Interior & Body Mounted

# Layerscape Mission Profiles

## Standard Networking Mission Profile

Detailed operating temperature data				
Junction Temperature (°C)	Time on T ( % )	Time on T ( h )	$\Delta T_{\text{self}}$	$T_a$ (or $T_{\text{case}}$ )
	100 % = 12000hrs			
-15 °C	2.0%	1752 h	20 °C	-35 °C
5 °C	3.0%	2628 h	20 °C	-15 °C
25 °C	4.0%	3504 h	20 °C	5 °C
45 °C	11.0%	9636 h	20 °C	25 °C
65 °C	15.0%	13140 h	20 °C	45 °C
85 °C	20.0%	17520 h	20 °C	65 °C
95 °C	25.0%	21900 h	20 °C	75 °C
105 °C	15.0%	13140 h	20 °C	85 °C
110 °C	5.0%	4380 h	20 °C	90 °C
Total	100%	87600 h		

Calculated  $T_a$  max-eff: 71C  
Calculated  $T_j$  max-eff: 91C

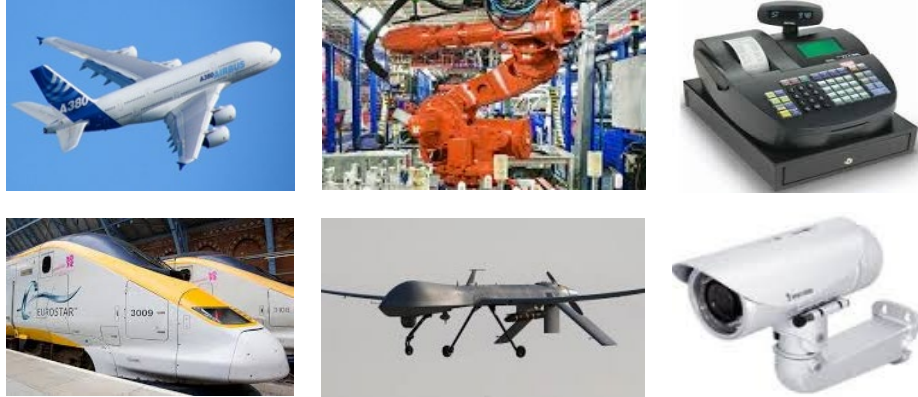
- NXP has certified 28nm technology for 187k power-on hours with an average of 105C  $T_j$ .
- Digital Networking's standard qualification is for 87k power-on hours, with an average of ~90C  $T_j$ .
- NXP's generic automotive mission profile has less power-on hours and a lower average temperature than the Digital Networking Mission Profile.
- Most Layerscape SoCs offered for automotive applications are qualified (AECQ100, grade 3). The mission profile is aligned with ZVEI Class 1, where the system is assumed to be mounted in the cabin or trunk.
- Other mission profiles are possible as well. The LS1043A supports AECQ100, grade 2.
- Note that Layerscape projected PPM is >1 for auto mission profiles.

## Standard Automotive Mission Profile

Detailed operating temperature data				
Junction Temperature (°C)	Time on T ( % )	Time on T ( h )	$\Delta T_{\text{self}}$	$T_a$ (or $T_{\text{case}}$ )
	100 % = 12000hrs			
-20 °C	6.0%	720 h	20 °C	-40 °C
43 °C	65.0%	7800 h	20 °C	23 °C
80 °C	20.0%	2400 h	20 °C	60 °C
120 °C	8.0%	960 h	20 °C	100 °C
125 °C	1.0%	120 h	20 °C	105 °C
Total	100%	12000 h		

Calculated  $T_a$  max-eff: 71C  
Calculated  $T_j$  max-eff: 83C

# Layerscape Longevity



Industrial & Automotive applications require product longevity

- Long product lifecycles
- Special product certification required

## NXP Application Processors

- 10 and 15 year supply longevity options
- Formal program with products listed at [www.nxp.com/productlongevity](http://www.nxp.com/productlongevity)



Digital Networking is still selling the (Motorola) 68302, a processor which was introduced in 1989. Many other products are still shipping after >20 years.

Any Layerscape product selected for a production vehicle will be guaranteed 10yrs supply, regardless of official start date of 10-15 year guarantee in longevity program.

# Layerscape for Automotive

- **Highest CPU and IO performance SoCs in NXP**
- **Scalability** – 1-16 ARM core SoCs
- **Quality & Longevity** – Best quality available in high performance processing. Many devices already on 15 year longevity program.
- **Safety** – We've demonstrated safety for mil/aero and other critical infrastructure applications. ISO26262 collateral (FMEDA, Safety Manual) available for selected devices.
- **Security** – Secure Boot, Secure Debug, Hardware Enforced Partitioning & Virtualization
- **Software** – SDKs with a very PC-like look & feel. Broad support in Linux, ecosystem of certified RTOS vendors.







**SECURE CONNECTIONS  
FOR A SMARTER WORLD**