ARTERIS IP

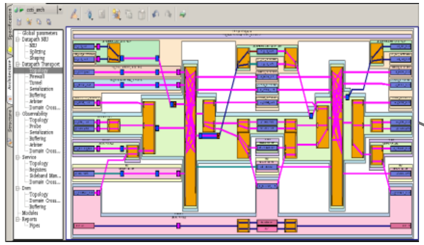
# Resilient Interconnect for Functionally Safe Automotive SoCs

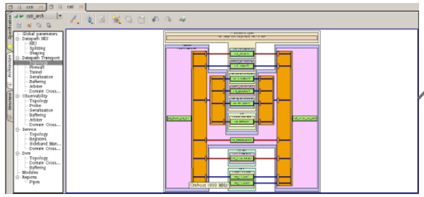
MPSOC CONFERENCE, JULY 2017, ANNECY FRANCE

K. CHARLES JANAC

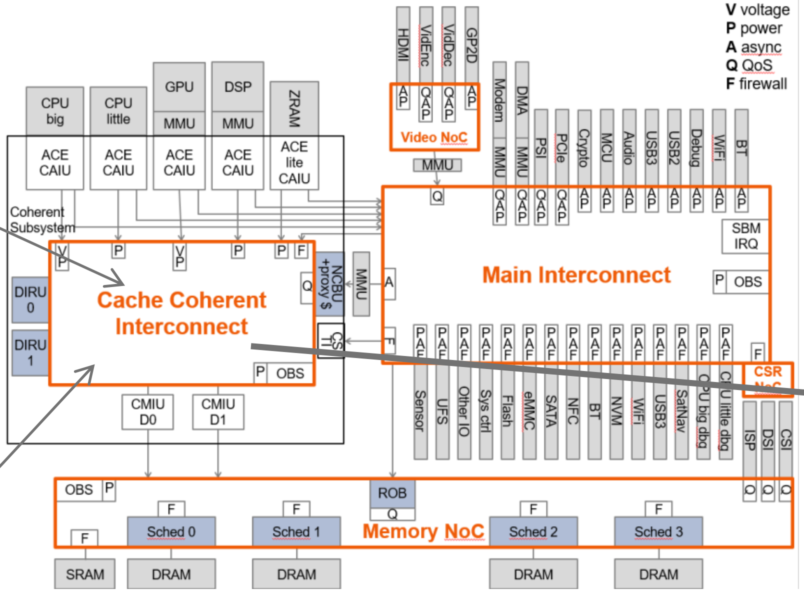
President and CEO

# SoCs Are now Assembled from IP Blocks

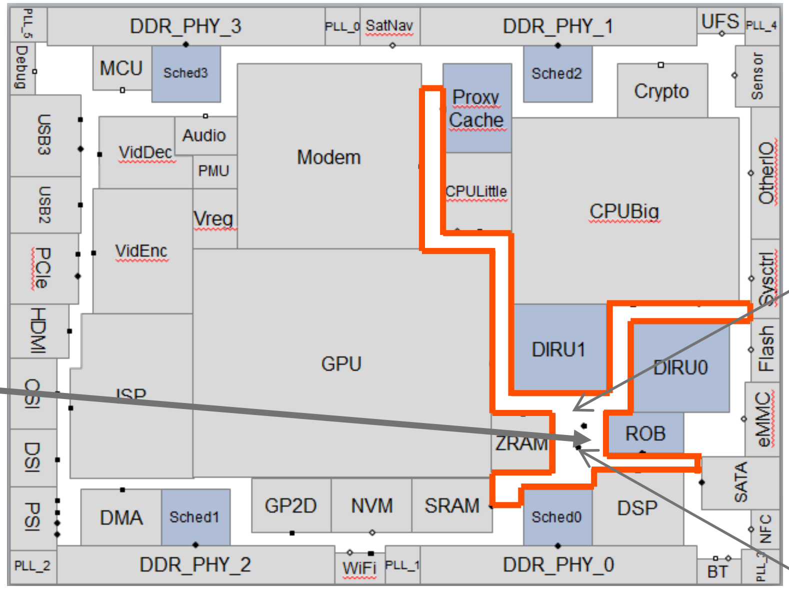


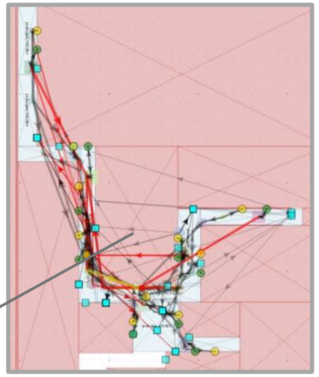


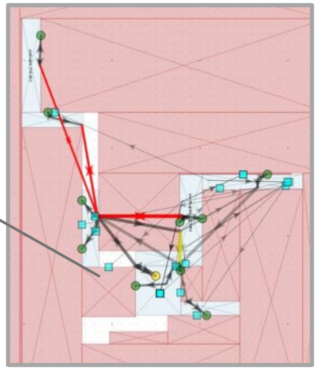
Architectural IP Connections



Physical IP Floorplan for SoC







- Large SoCs have multiple classes of interconnect IPs
  - Non-coherent, Coherent, Control/Status, Observability, etc.
- All interconnects must be converted from architectural IPs to Physical Ips
- There are many requirements for PPA, Flexibility, Productivity, Safety & Security

ARTERIS IP

# Resilience for Mission Critical Electronics

AUTOMATED VEHICLES REPRESENT THE NEXT GREAT GROWTH SEMICONDUCTOR MARKET

# Automated Driving Potentially Solves Major Problems

- Fatalities: Globally 1.25M people die each year due to traffic accidents (WHO 2016), 20-50M injuries/year (WHO 2016)
  - 94% of the causes are at least partially due to human error (NHTSA 2016)
  - Economic cost is 2-3% of a country’s GDP (WHO 2015)
- Automated Driving Opportunity: cut accidents per year by 80-90%, potentially saving 80-90% of $871B/yr. **cost in USA alone** (NHTSA 2014) or ~$700+B/year
- Use of Assets; Cars idle 80% of the time, Automated driving makes more efficient use of cars, roads and parking spaces – another 10s of Billions benefit
- Societal impacts cannot be fully predicted but will be large

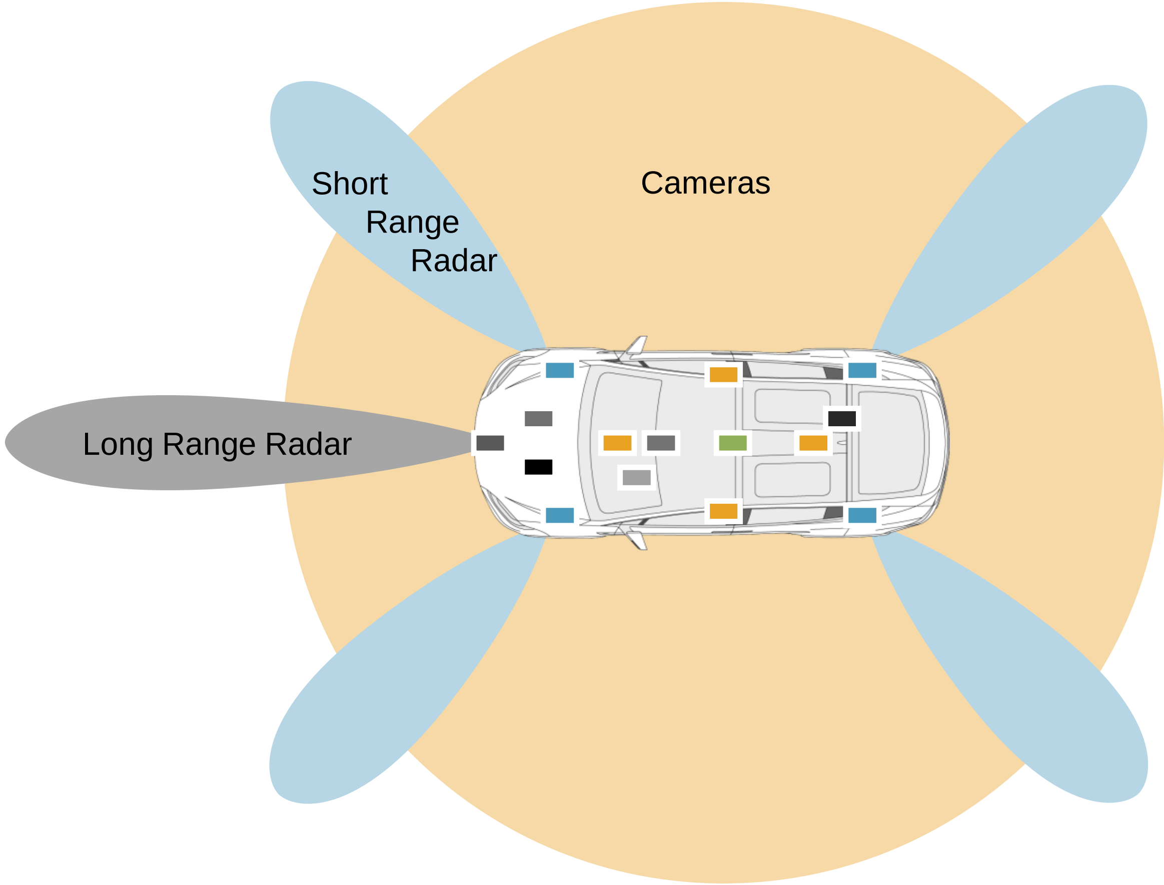
# Automated Driving Challenges

- Getting to level 4 automated driving technology (where car can manage the entire driving experience)
  - Sensor fusion for near realtime image recognition, machine learning for corner case management, optimization and queuing algorithms – need super computer performance
  - **Functional safety and security of both hardware** and software
  - Cost needs to be brought down to what customer is willing to pay
- Mixing manual and automated driving - Transition to automated driving is a challenge
- Road infrastructure not designed for automated driving
- Many will be saved but few people are going to die because of automated driving technology
- Questions of insurance and legal liability, regulation and documentation

# Delivering Resilient SoCs

## AND AUTOMOTIVE REQUIREMENTS

# Automotive SoCs in Automated Driving Vehicles



| | | |
|---|---|---|
| **Vision Camera (8)** | 🟧 | Mobileye<br>Toshiba<br>Texas Instruments<br>nextchip |
| **ADAS / Machine Learning (1-2)** | 🟩 | Mobileye<br>Not Public<br>NXP<br>ST life.augmented<br>Dream Chip<br>Cambricon<br>Movidius an intel company |
| Dashboard / HUD (2) | ■ | NXP<br>Renesas |
| Infotainment (1) | ■ | NXP<br>Not Public<br>Texas Instruments |
| RFCMOS Radar or LIDAR (4) | ■ | Not Public |
| Long Range Radar (1) | ■ | |
| Chassis Control (2) | ■ | |
| Engine Control (2) | ■ | ST life.augmented |
| V2X / WAN Modem (1) | ■ | Sequans Communications<br>Not Public |

*Notes: Numbers in parentheses are the number of "complex" SoCs per function. Logos and company names are publicly announced Arteris customers as of 1 Apr 2017.*

Source: Arteris, Inc.

# ISO 26262 Functional Safety

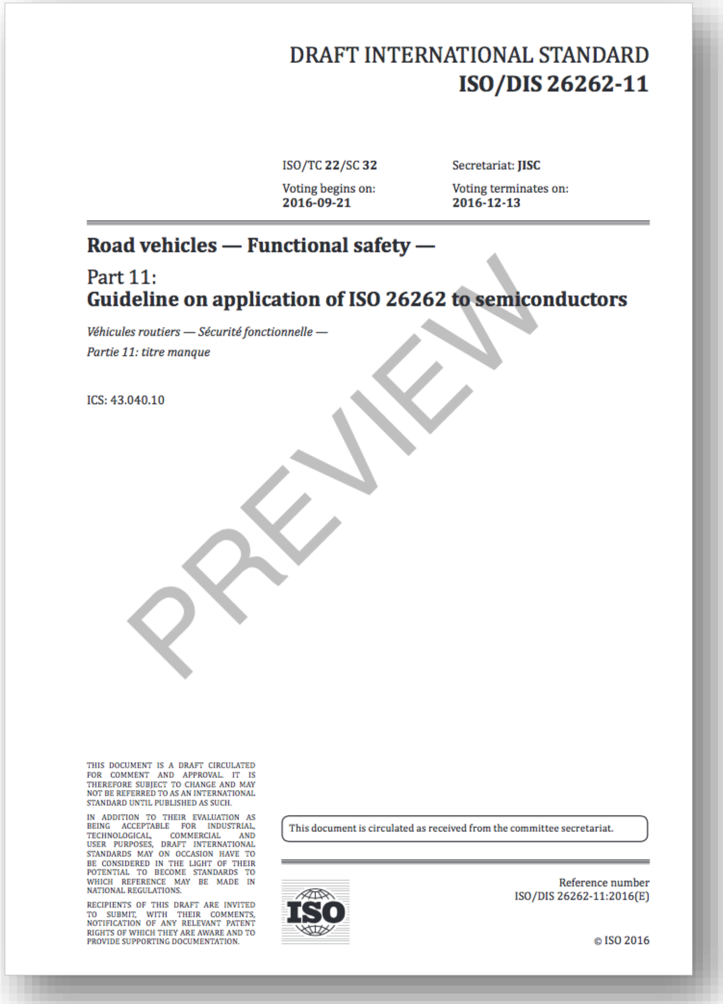
LET’S ADD EVEN MORE COMPLEXITY…

# ISO 26262 and Automotive Functional Safety

- Safety throughout supply chain (IP, HW, SW, processes)
- Functional safety risks include:
  - Random hardware faults
  - Systematic faults
- Multiple safety systems
  - Active – accident prevention
  - Passive – accident mitigation

International Organization for Standardization

SAE INTERNATIONAL



DRAFT INTERNATIONAL STANDARD
**ISO/DIS 26262-11**

ISO/TC **22**/SC **32** Secretariat: **JISC**

Voting begins on: **2016-09-21** Voting terminates on: **2016-12-13**

**Road vehicles — Functional safety —**

Part 11:
**Guideline on application of ISO 26262 to semiconductors**

*Véhicules routiers — Sécurité fonctionnelle —*
*Partie 11: titre manque*

ICS: 43.040.10

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

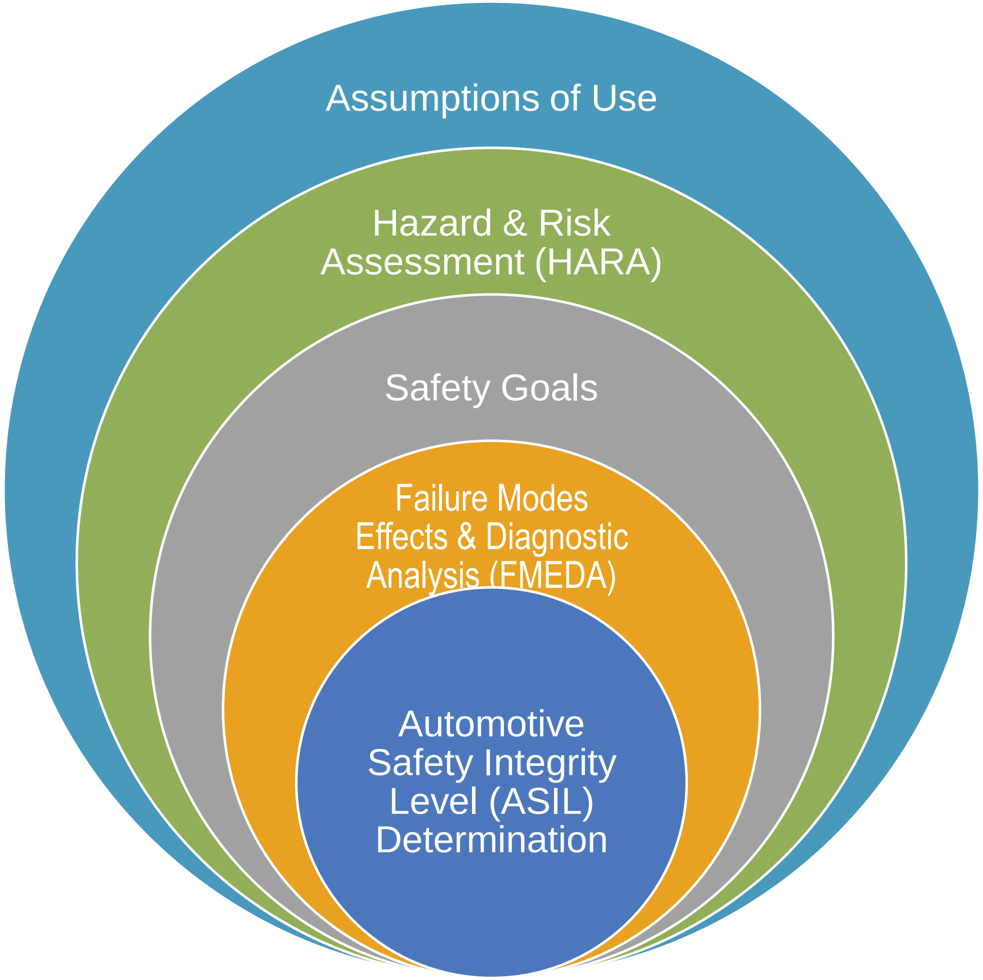
IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 26262-11:2016(E)

# The Safety Process (simplified)



Assumptions of Use

Hazard & Risk Assessment (HARA)

Safety Goals

Failure Modes Effects & Diagnostic Analysis (FMEDA)

Automotive Safety Integrity Level (ASIL) Determination

# What is an ASIL (Automotive Safety Integrity Level)?

| | When | ASIL B | ASIL C | ASIL D |
|---|---|---|---|---|
| SPFM<br>Single Point Fault Metric | Operating | > 90 % | > 97 % | > 99% |
| LFM<br>Latent Fault Metric | Key-on | > 60 % | > 80 % | > 90 % |
| FIT<br>Failure in Time | Operating | - | < 100 | < 10 |

## Ramifications

Hardware protection in SoC interconnect (rules of thumb)

- **ASIL B** = fault detection (ECC/parity, SW)
- **ASIL C/D** = unit duplication for key logic

**Built-in Self Test (BIST)** and **checkers** required for HW safety mechanisms!

## Definitions

**Single Point Fault Metric (SPFM)** - % coverage by safety mechanisms

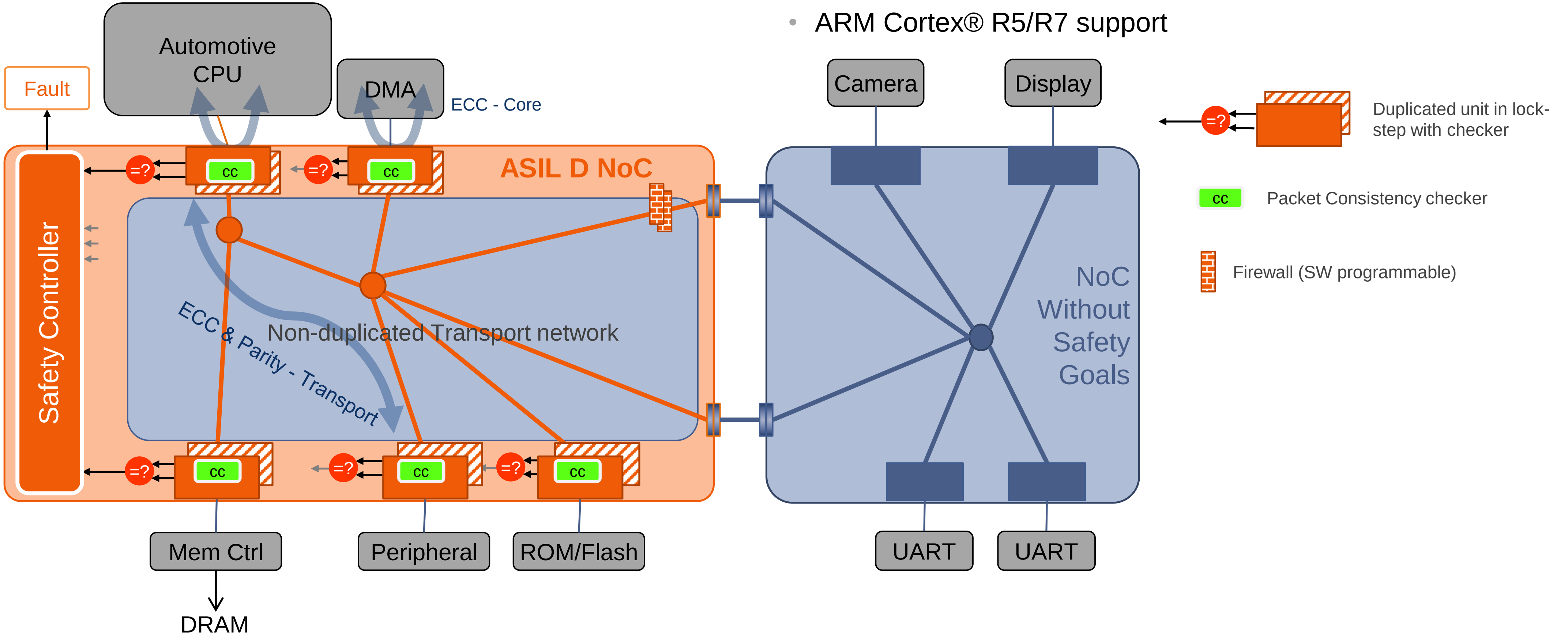
**Latent Fault Metric (LFM)** - % coverage by safety mechanisms of multi-point faults

**Failure in Time (FIT)** - # of expected failures in one billion hours (114,155 years)

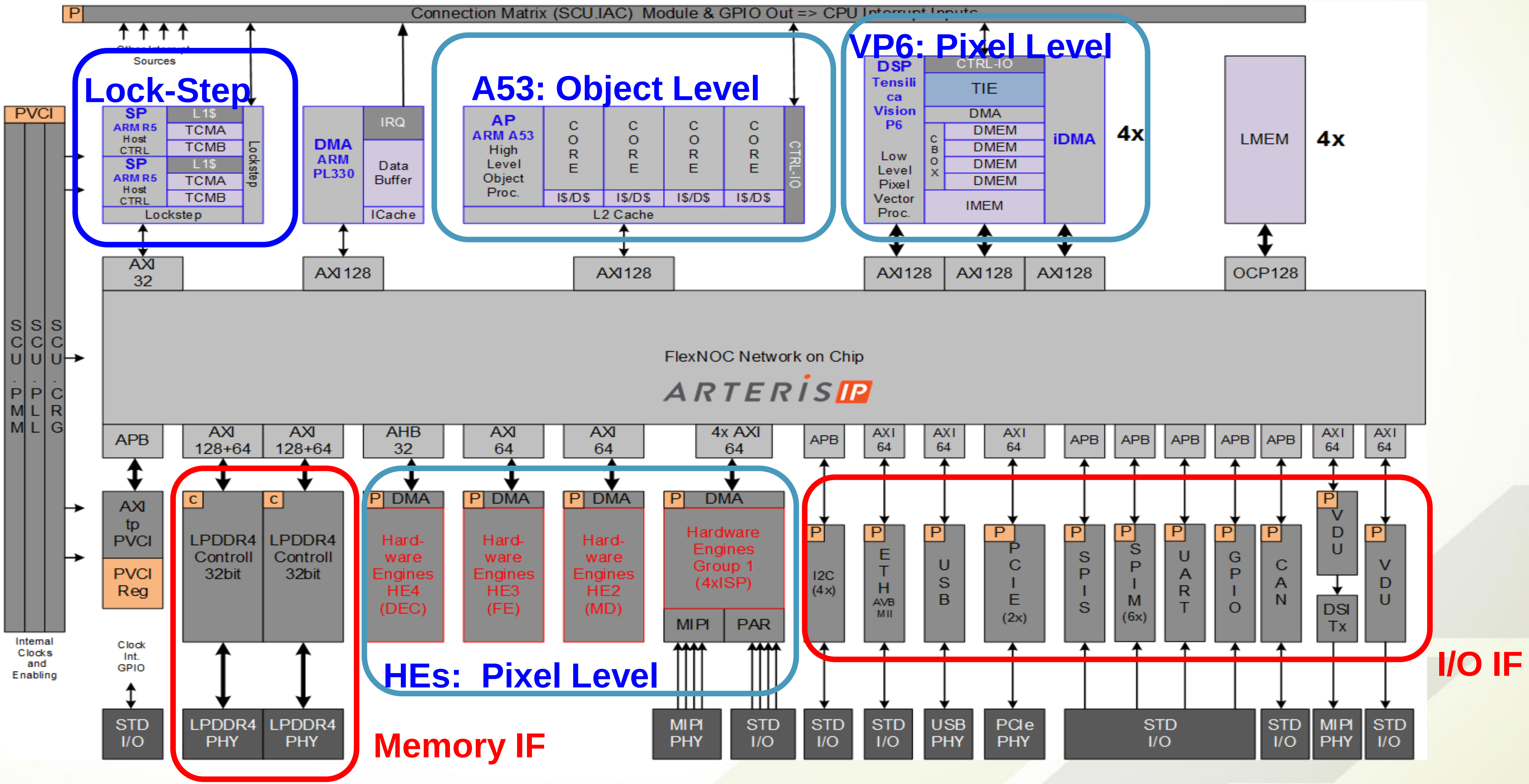
# FlexNoC Main Interconnect with Resilience Support

- Unit duplication - fault detection
- ECC at interface & in-transport
- Packet Consistency checkers

- Safety Controller
- Fault reporting logic BIST
- Multi ASIL Level Support
- ARM Cortex® R5/R7 support



# Low Power CNN Architecture



# For Safe, Scalable Automotive SoCs

## CAPABILITIES

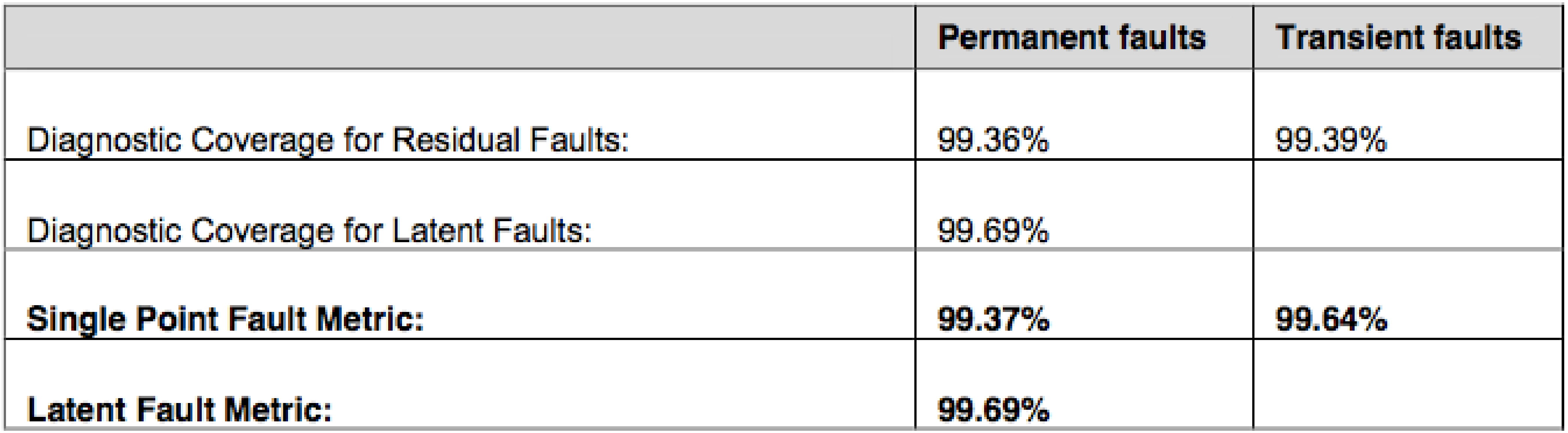
- **Resilience:** Data link protection, intelligent HW unit duplication, fault controller
- ASIL B – ECC, Parity Bit
- ASIL C – ECC, Parity Bit and Packet Integrity Check
- ASIL D - ECC, Parity Bit, Packet Integrity & Unit Duplication

## BENEFITS

- Achieve higher ASILs than feasible through software
- Simplify software by protecting hardware
- Easier FMEDA
- Easier integration of multiple processing elements, whether coherent or non-coherent
- Simplified software for NN systems, especially Recurrent (RNN)
- More flexible and area- and power-efficient

Need Resilient Interconnect for Functionally Safe Vehicles

# Quantitative Safety Analysis Results for FlexNoC Interconnect



| | Permanent faults | Transient faults |
|---|---|---|
| Diagnostic Coverage for Residual Faults: | 99.36% | 99.39% |
| Diagnostic Coverage for Latent Faults: | 99.69% | |
| **Single Point Fault Metric:** | **99.37%** | **99.64%** |
| **Latent Fault Metric:** | **99.69%** | |

**Architectural metrics related to ASIL D case**

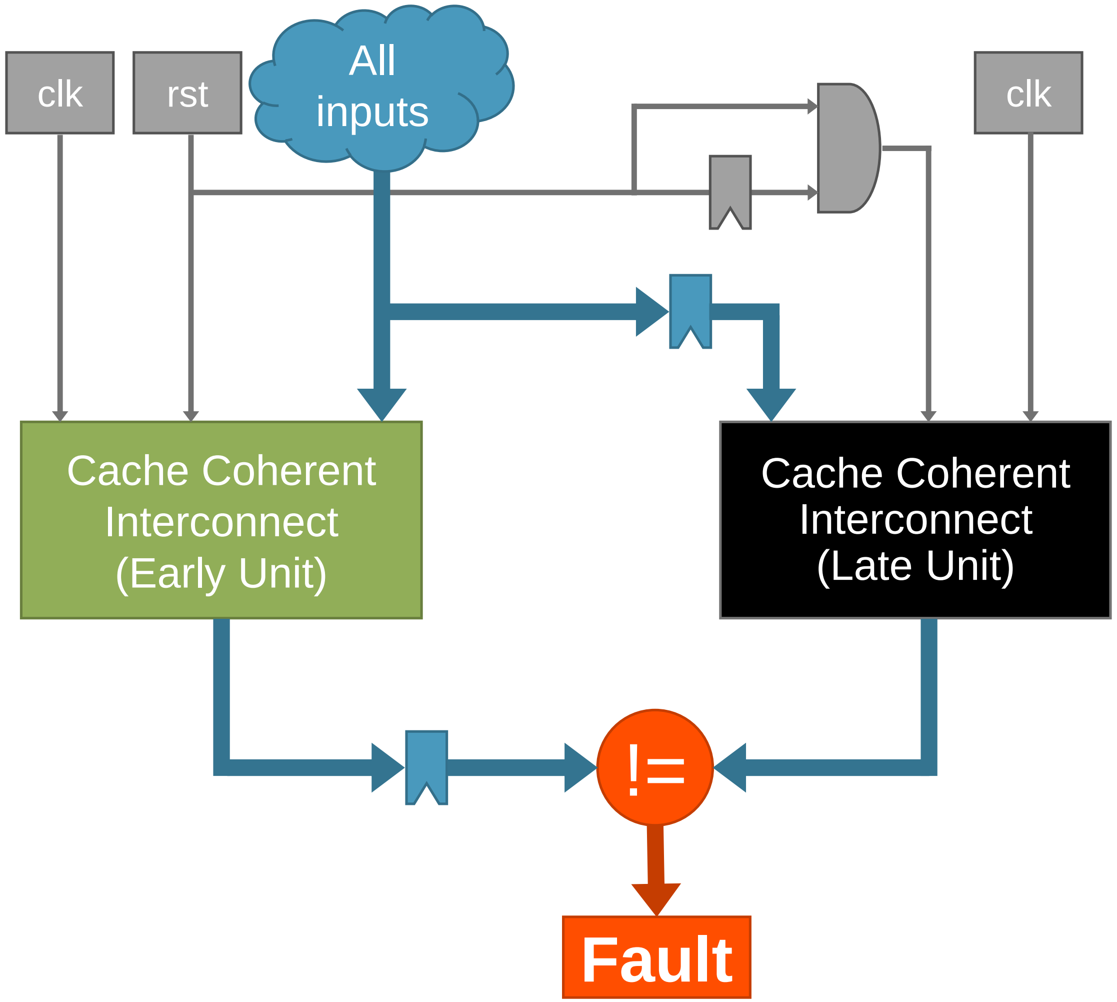
Analysis of the FlexNoC interconnect shows it can reach ASIL D on all ISO26262 Metrics
Source: Yogitech

# But What About Cache Coherency?

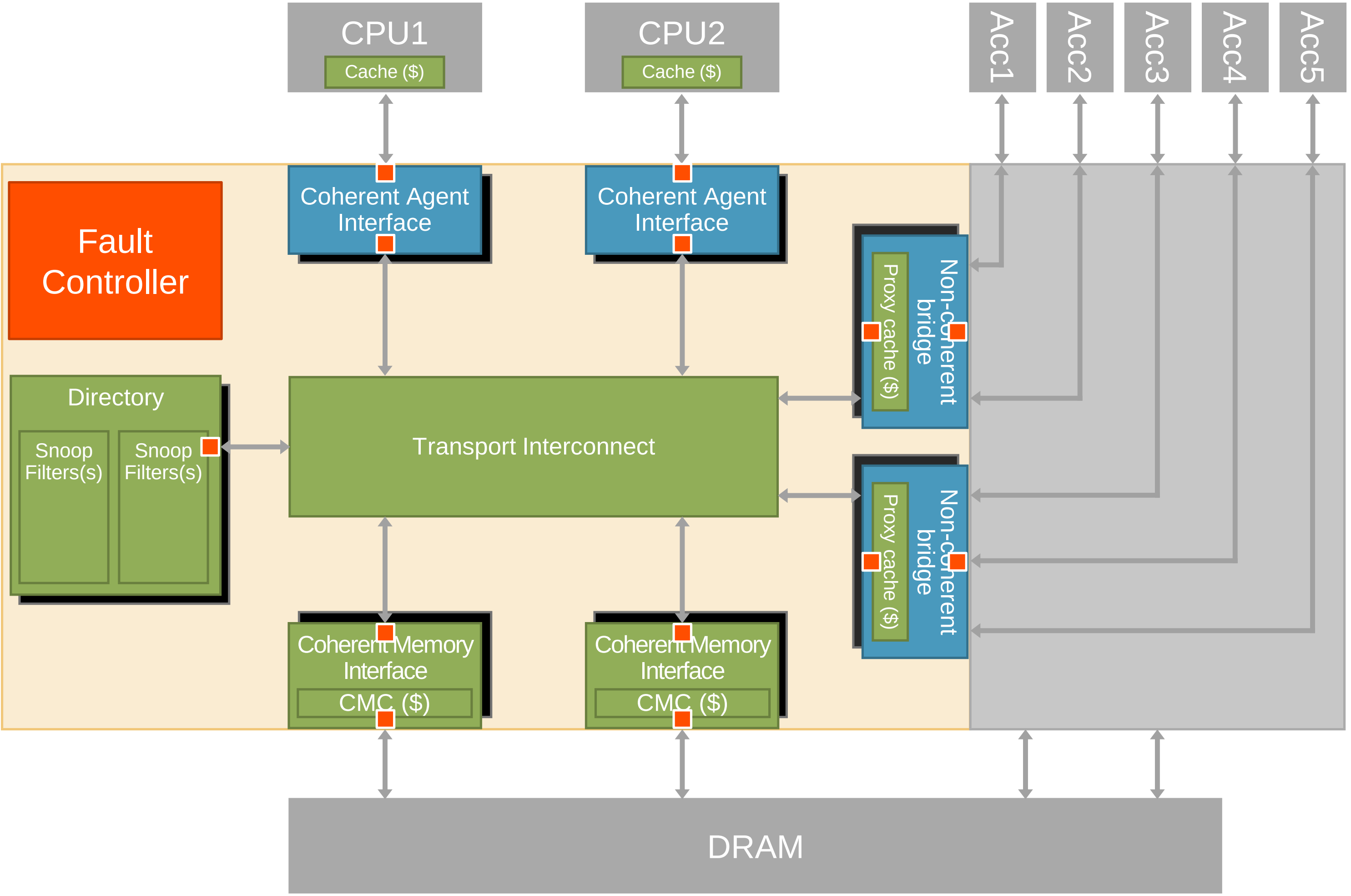
### The Brute Force Approach

- Duplicate the entire interconnect, run in lockstep
- Why is this wasteful?
  - Blows up design area fast ~120% overhead
  - Not power efficient
  - More integration work
  - Complexity inversely proportional to safety

Can we do better?


clk
rst
All inputs
clk
Cache Coherent Interconnect (Early Unit)
Cache Coherent Interconnect (Late Unit)
!=
Fault

# Ncore Cache Coherent Interconnect with Resilience



- **Data protection (at rest & transit)**
  - Parity 8 data path protection
  - ECC memory protection
- **Intelligent Ncore hardware unit duplication**
  - Don’t duplicate protected memories or links
  - Only duplicate HW that affects packets
  - Integrated checkers, ECC/parity generators & buffers
- **Fault controller with BIST**

# What is Next for Resilient Interconnect?

FAIL OPERATIONAL

# Fail Operational

# Autonomous HW requires safer, smarter SoCs

- All functions such as power management, security and QoS must work with Resilience
- Resilience has a cost so must minimize power, performance and area penalties
- All types of interconnect IPs must be made resilient; coherent, non-coherent, subsystems
- Resilience must be supported by documentation, safety verification and certification
- All autonomous vehicles will contain some form of Resilient Interconnect
- ISO26262 compliance is “table stakes” to thrive in the autonomous vehicle SoC market
- Resilience is the path to Fail Operational SoCs

NoC Interconnect for autonomous hardware SoCs

# Thank you

CHARLIE.JANAC@ARTERIS.COM