Automotive Functional Safety: Options for **Fault Tolerant Systems**

AMF-ACC-T1659

John Cotner | Field Systems Engineer

S E P T . 2 0 1 5

External Use

Agenda

- Introduction
  - Fault Tolerance – Well Known
  - Fault Tolerance – The Challenge
- Microcontroller Random Hardware Faults
  - Fault Types
  - ADAS Aspects
- Fault Tolerance and Functional Safety Standards
  - IEC 61508
  - ISO 26262
- Solution Options
  - Safe States and Safe Sequences
  - Measures on Microcontroller Level
  - System Architecture Possibilities
- Summary

Evolution of Vehicle Safety Systems… And the Arrival of Functional Safety

Passive Safety

Active Safety

Predictive Safety

SAFE ASSURE™ by Freescale

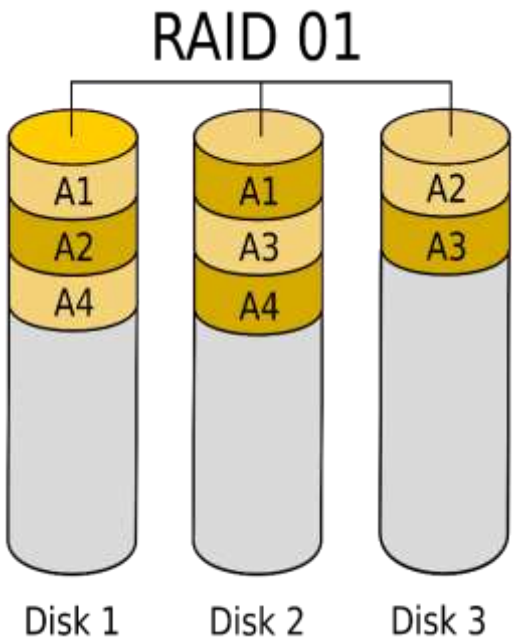
Functional Safety
Covers systems for
- Chassis & Safety
- Powertrain
- Body

Market trends
1. Vision zero - no fatalities
2. Safe Comfort & Asssistance
3. Green Technology
4. Automation

Injury Free	Accident Free	Semi Autonomous Driving
2000-2010	2010-2020	2020-2030

Introduction
Fault Tolerance

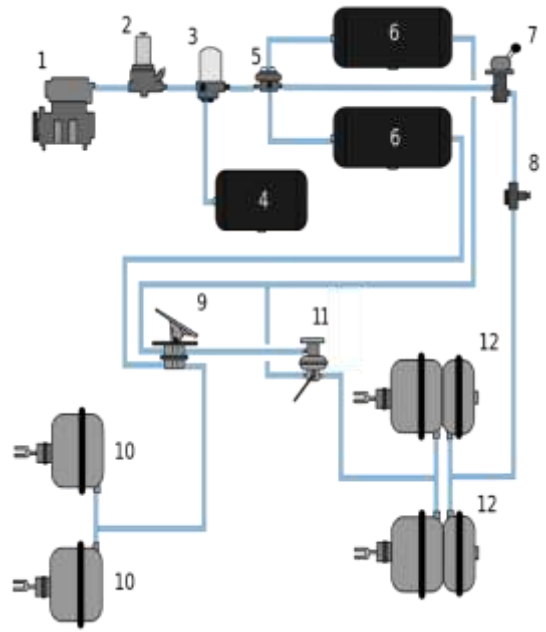
Fault Tolerance – Well Known – Non-Automotive



- Data storage:
  - RAID
- High performance computing:
  - Processing unit hot swap
- Networking:
  - Routing path reconfiguration
- Avionics:
  - High redundancy, FO-FO-FS

- Typical properties:
  - Hardware redundancy
  - No human interaction needed

Fault Tolerance – Well Known – Automotive Non-Electric

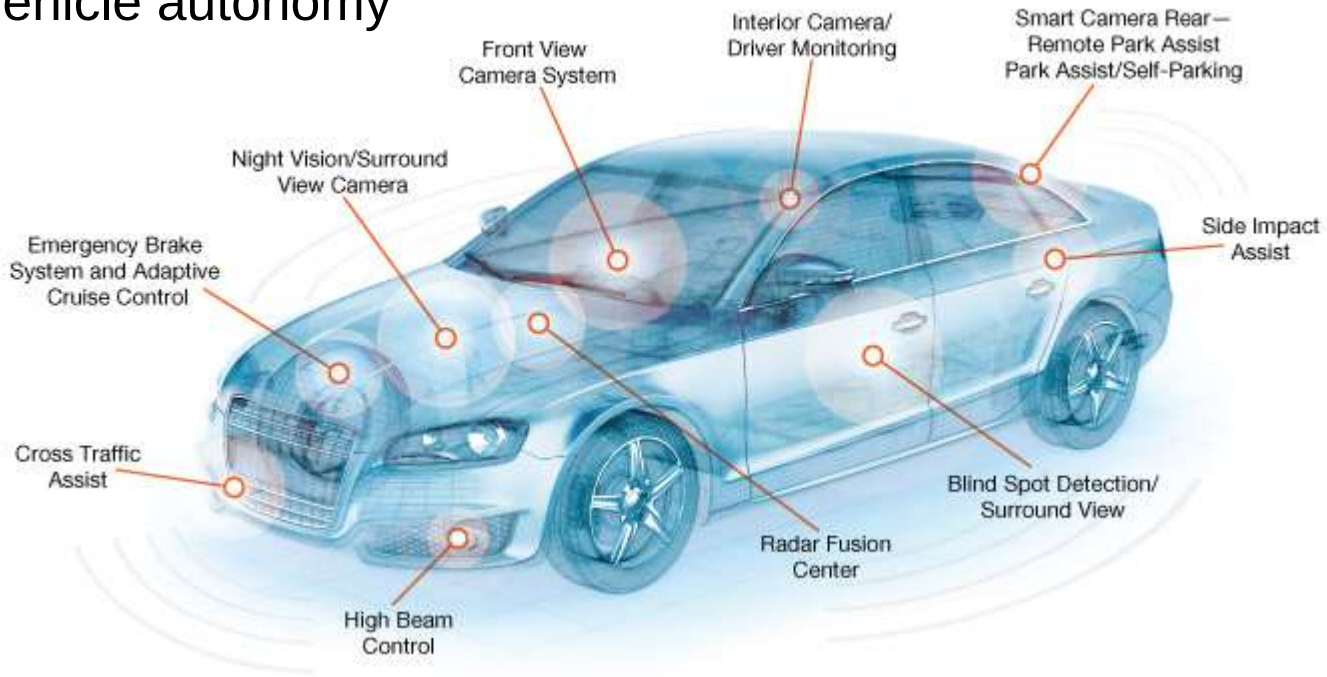


- Trailer hitch
  - Safety chains
- Tires
  - Run-flat option
- Brakes
  - Split brake system
- Power steering
  - Mechanical fallback

- Typical properties:
  - Simple physical principles
  - Robustness by design margins
  - Humans detect/control certain failures
  - Performance degradation

Fault Tolerance – The Challenge (1)

- Automotive ADAS roadmap:
  - More comfort functions
  - Stronger assist functions
  - More demanding regulations
  - Trend towards vehicle autonomy

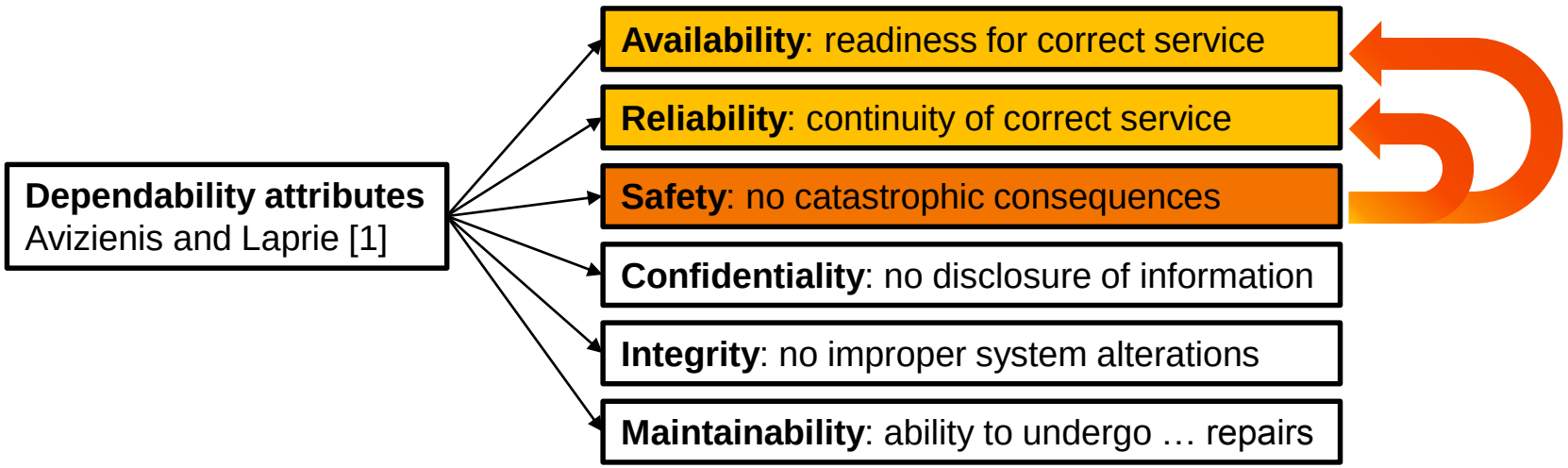


Fault Tolerance – The Challenge (2)

- Automotive roadmap – first order consequences:
  - More sensors, higher bandwidth sensors
  - Increasing use of high-performance microcontrollers
  - Increased number of technology elements
  - Growing software footprint
  - More functions on same or fewer microcontrollers
  - Fusion of comfort and safety functions
  - Complex control structures
  - Non-linear system behavior

Fault Tolerance – The Challenge (3)

- Automotive roadmap – second order consequences:
  - Hard to predict fault propagation
  - New and complex system failure modes
  - Humans incapable of handling complex failures
  - Fewer fallbacks on simple physical principles
  - **Shutdown of processing not safe**
  - **“Fail-silent” → “fail-operational” requirement**

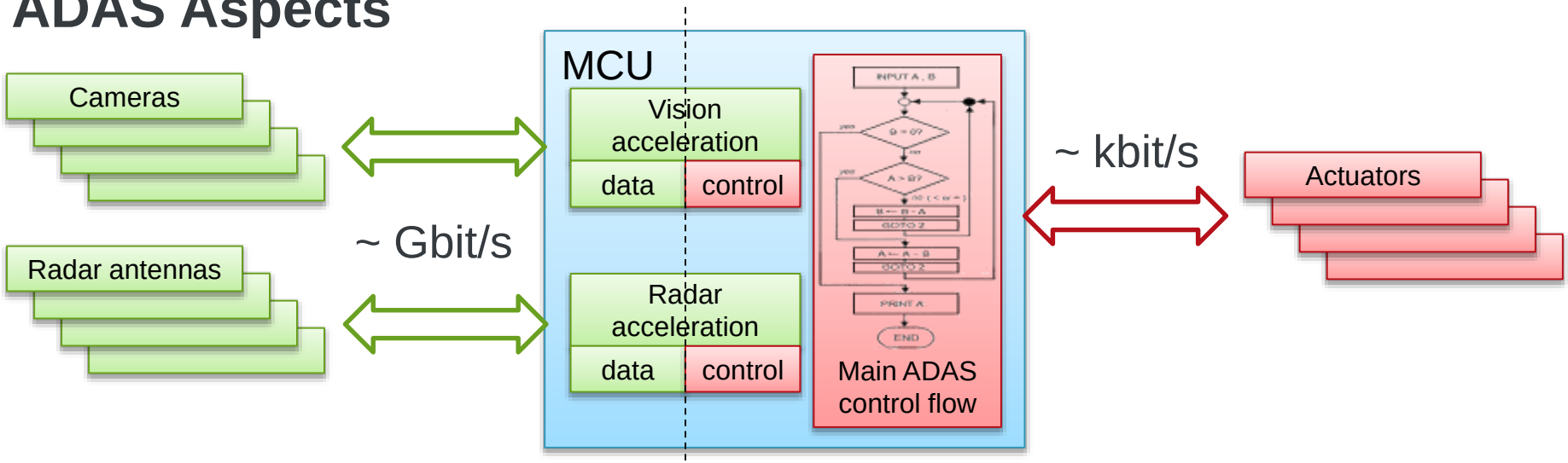


Microcontrollers
Random Hardware Faults

Semiconductor Random Hardware Faults

FAULTS	Transient, temporally limited	Intermittent, repeating	Permanent
Local, spacially limited	e.g. bit flip caused by radiation No physical damage High rate, ~constant over life time Fault detection ~~Shut-down~~ (not an option) Fault containment Fault removal	e.g. parametric drift by aging Potentially physical degradation Low rate, increasing towards end of life Fault detection ~~Shut-down~~ (not an option) Fault containment Fault removal + Fault monitoring + Part replacement	e.g. open/short by aging Physical damage Low rate, increasing at end of life Fault detection ~~Shut-down~~ (not an option) Fault containment ~~Fault removal~~ (not possible) + Fault localization + System reconfiguration + Part replacement
Non-local, affects big parts of die	e.g. clock/supply spike by noisy environment … clock/supply out of specification Often extrinsic root causes, failure rate is a composite of intrinsic and extrinsic causes, cannot be determined at component level Fault avoidance Robust design Redundancy with measures against common cause faults Fault detection Part replacement		

ADAS Aspects



Sensor data:

- Spacial redundancy
- Temporal redundancy
- Atomic frame processing
- Noise robust algorithms

Flow and actuator control:

- No native redundancy
- Vital for safe operation

→ Assessing dangerousness of faults essential for safety analysis
→ Mixed safety criticality on same microcontroller
→ **Freescale safety methodology enables use case specific analyses**

Freescale Approach to Functional Safety

The Four Elements

Safety process

- Integrating functional safety into product development process
- Select products defined and designed from the ground up to comply with the standards

Safety hardware

- Built-in safety functions (self-testing, monitoring and hardware-based redundancy) in Freescale microcontrollers (MCUs), power management ICs and sensors
- Additional system-level safety functionality from Freescale analog solutions (checking MCU timing, voltages and error management)

Safety software

- A comprehensive set of automotive functional safety software, including AUTOSAR OS and associated microcontroller abstraction layer (MCAL) drivers, as well as core self-test capabilities
- Partnerships with leading third-party software providers for additional safety software solutions

Safety support

- From customer-specific training and system design reviews to extensive safety documentation and technical support

Functional Safety Standards and Fault Tolerance

Functional Safety Standards – IEC 61508 Edition 2

- IEC 61508 = Generic parent standard for ISO 26262
- **Definition** (part 4):

> **3.6.3**
> **fault tolerance**
> ability of a functional unit to continue to perform a required function in the presence of faults or errors
> [ISO/IEC 2382-14, 14-04-06]

- **Metric** (part 2):

> **7.4.4.1.1** With respect to the hardware fault tolerance requirements
>
> a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics; and

- **Achievable Safety Integrity Level** (SIL, part 2):
- SIL 1 ~ ASIL A
  SIL 2 ~ ASIL B/C
  SIL 3 ~ ASIL C/D
  SIL 4 ~ n.a.

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	~~Not Allowed~~	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	~~SIL 4~~
≥ 99 %	SIL 3	~~SIL 4~~	~~SIL 4~~

Functional Safety Standards – IEC 61508 Edition 2

- **Reactions on fault detections** (part 2):

7.4.8.1 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem that has a hardware fault tolerance of more than 0 shall result in either:

a) a specified action to achieve or maintain a safe state (see Note); or

b) the isolation of the faulty part of the subsystem to allow continued safe operation of the EUC whilst the faulty part is repaired. If the repair is not completed within the mean repair time (MRT), see 3.6.22 of IEC 61508-4, assumed in the calculation of the probability of random hardware failure (see 7.4.5.2), then a specified action shall take place to achieve or maintain a safe state (see Note).

- **Semiconductor requirements** (part 2):

E.1 General

This annex is referenced by 7.4.2.2 b).

To allow the use of on-chip redundancy for ICs with one common semi-conductor substrate, a set of requirements is given below. For safety reasons this approach has a conservative nature, for example it is limited up to SIL 3 and a set of restrictive requirements have been specified. The following requirements are related to digital ICs only. For mixed-mode and analogue ICs no general requirements can be given at the moment. Common cause analysis (see IEC 61508-1, 7.6.2.7) may exclude the use of on-chip redundancy for an individual application. On-chip redundancy as used in this standard means a duplication (or triplication etc.) of functional units to establish a hardware fault tolerance greater than zero. According to 7.4.4.1.1 a) in determining the hardware fault tolerance no account is taken of measures that may control the effects of faults such as diagnostics.

A subsystem with a hardware fault tolerance greater than 0 can be realised using one single IC semi-conductor substrate (on-chip redundancy). In this case all of the following requirements a) to q) shall be fulfilled and the design of the E/E/PE system and the IC shall be such as to meet these requirements. An IC with on-chip redundancy shall have its own compliant item safety manual (see Annex D).

Functional Safety Standards – ISO 26262

- Not adopted from IEC 61508 for automotive domain:
  - "Hardware Fault Tolerance"
  - Dependency HFT → SIL

- Replaced in ISO 26262 by:
  - **"Fault Tolerant Time Interval"** property of the application, not of control system
  - **"Emergency operation"**

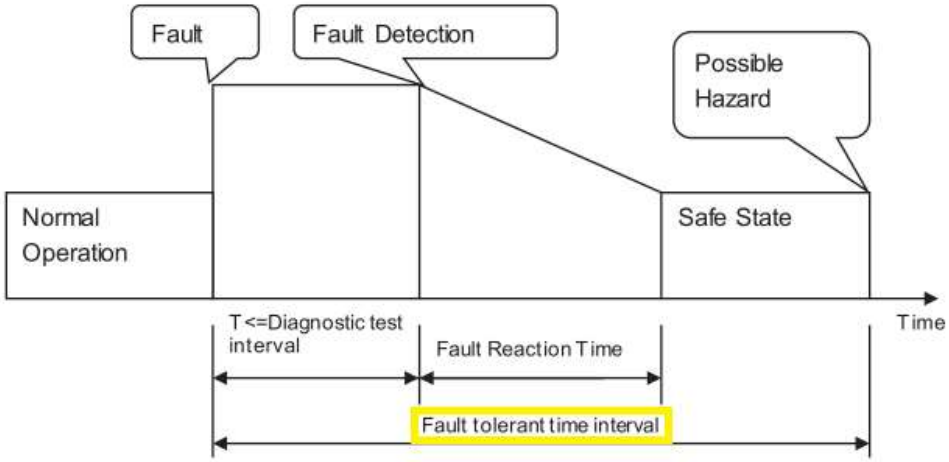


Figure 4 — Fault reaction time and fault tolerant time interval

1.34
emergency operation
degraded functionality from the state in which a **fault** (1.42) occurred until the transition to a **safe state** (1.102) is achieved as defined in the **warning and degradation concept** (1.140)

  - **"Warning and degradation concept"**

1.140
warning and degradation concept
specification of how to alert the driver of potentially reduced functionality and of how to provide this reduced functionality to reach a **safe state** (1.102)

Functional Safety Standards – ISO 26262

With regard to fault tolerance, ISO 26262 today …

- defines some terminology and concepts
- does not define how to apply metrics to a degradation chain
  - Probability Metric for Random Hardware Faults (PMHF rate)
  - Single Point Fault Metric (SPFM coverage)
  - Latent Fault Metric (LFM coverage)
- does not provide architectural guidance
- does not define clear architecture criteria or thresholds

Leading to …

- degree of freedom for system architects
- uncertainty regarding remaining risk quantification
- uncertainty regarding tolerable remaining risk

Functional Safety Standards – ISO 26262 Edition 2

- Semiconductor subgroup of ISO / TC 22 / SC 32 / WG 8 “Functional Safety”
  - Drafting of ISO PAS 19451 “Application of ISO 26262 to Semiconductors” included **preparatory work with regard to “fail-operation”**
  - ISO PAS 19451 “Application of ISO 26262 to Semiconductors” draft is approved for publication and commenting
    - Part 1: Application of concepts
    - Part 2: Application of hardware qualification
  - Preparatory work “fail-operation” was forked out and is fed into drafting of ISO 26262 Edition 2

- ISO / TC 22 / SC 32 / WG 8 “Functional Safety”
  - Life cycle of ISO 26262 Edition 2 started
  - **Incremental updates with regard to “fail-operation” (i.e. fault tolerance) planned**

- Freescale participation in ISO 26262 standardization:
  - 2 participants in German national body DIN/VDA
  - 2 participants in French national body AFNOR

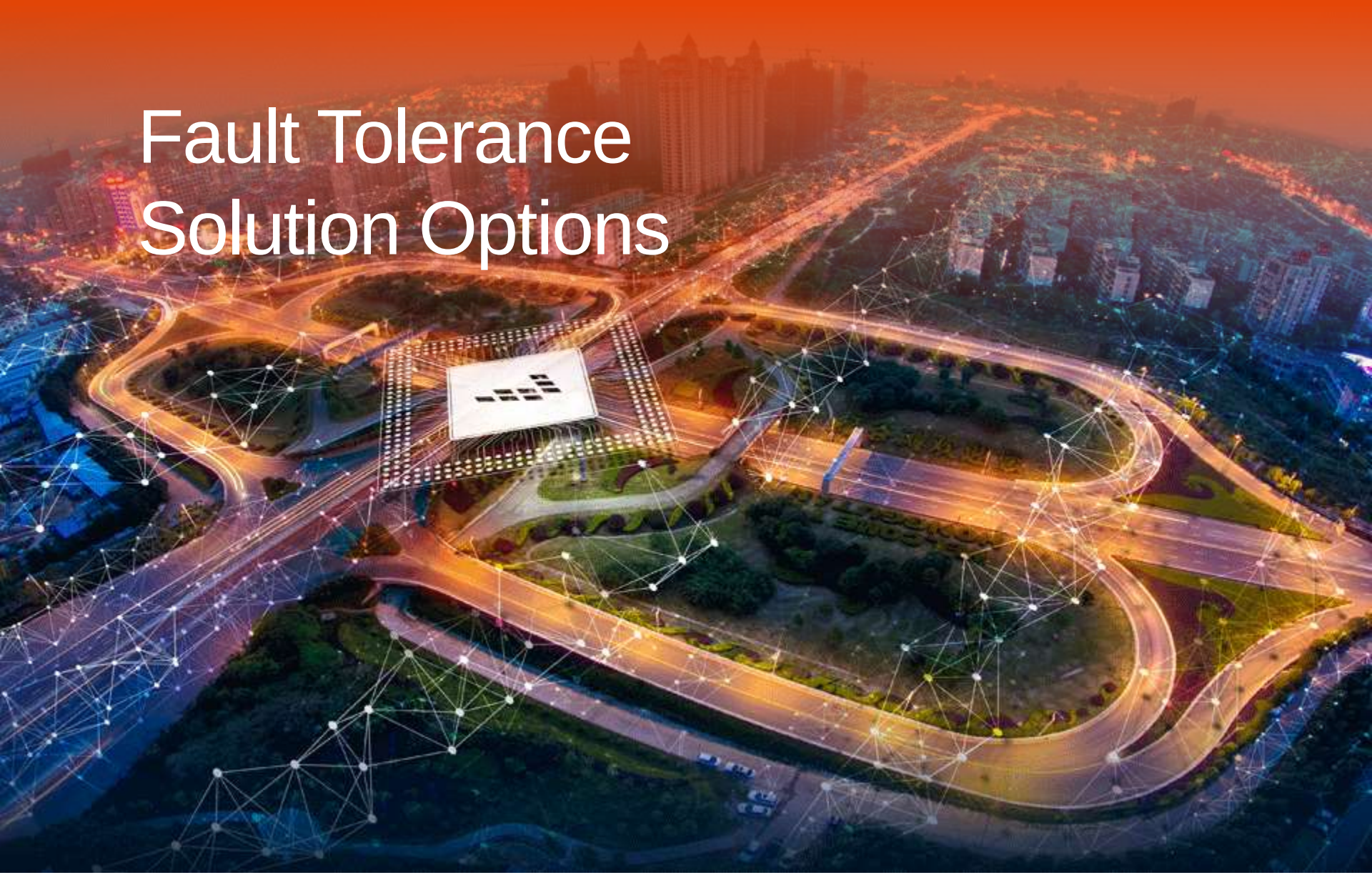
Options to Address Safety Standard Compliance

- **ISO 26262:2011-2012**
  Application of the generic requirements regarding "Warning and Degradation Concept"

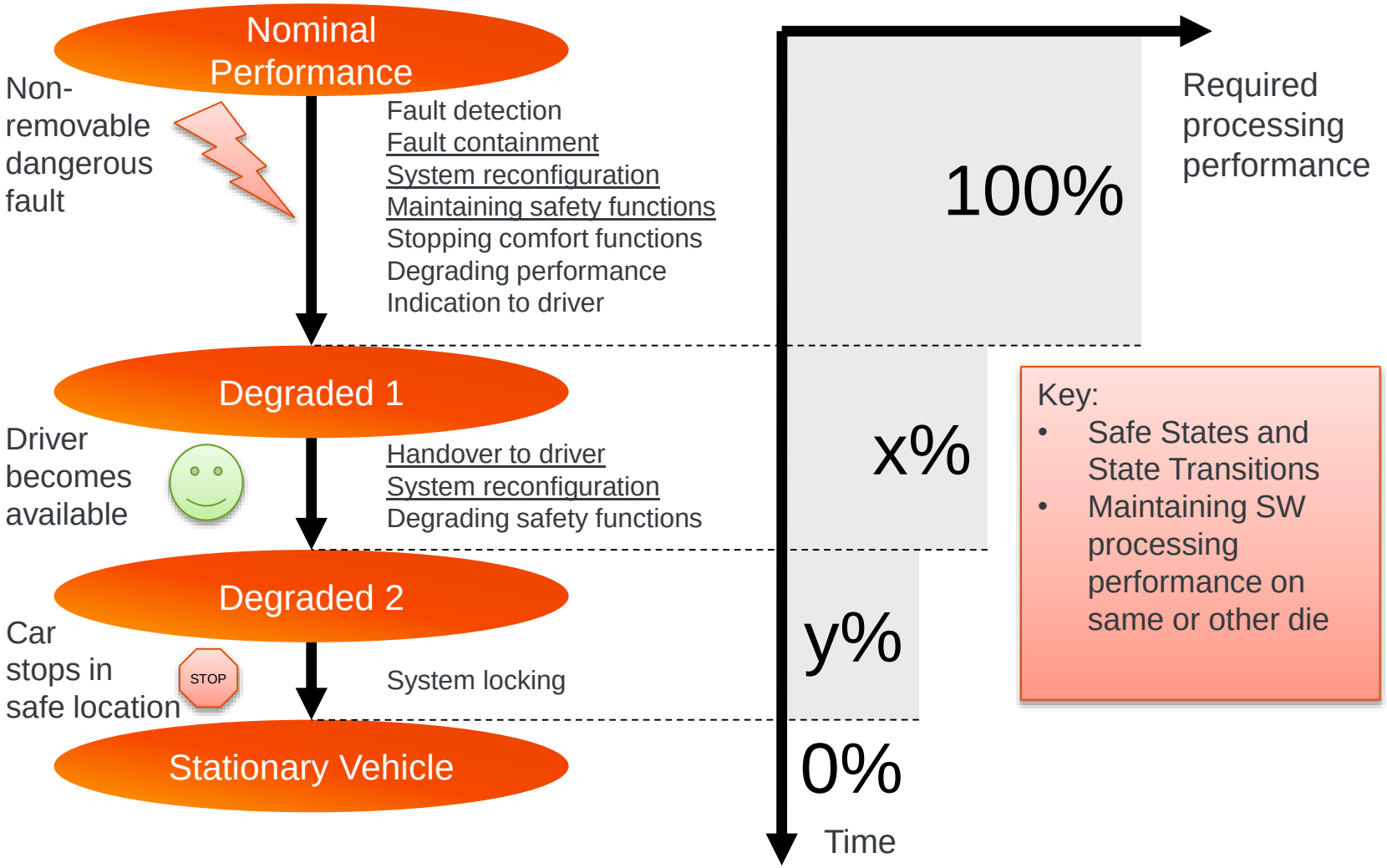
- **ISO 26262:2011-2012 + fallback on IEC 61508:2010**
  Application of "Hardware Fault Tolerance" levels and its influence on "achievable Safety Integrity Level"

- **ISO 26262 Edition 2**
  Application of first public draft of ISO 26262 Edition 2
  - Draft ~Q4, 2016
  - Final draft ~Q4, 2017
  - International Standard ~Q1, 2018

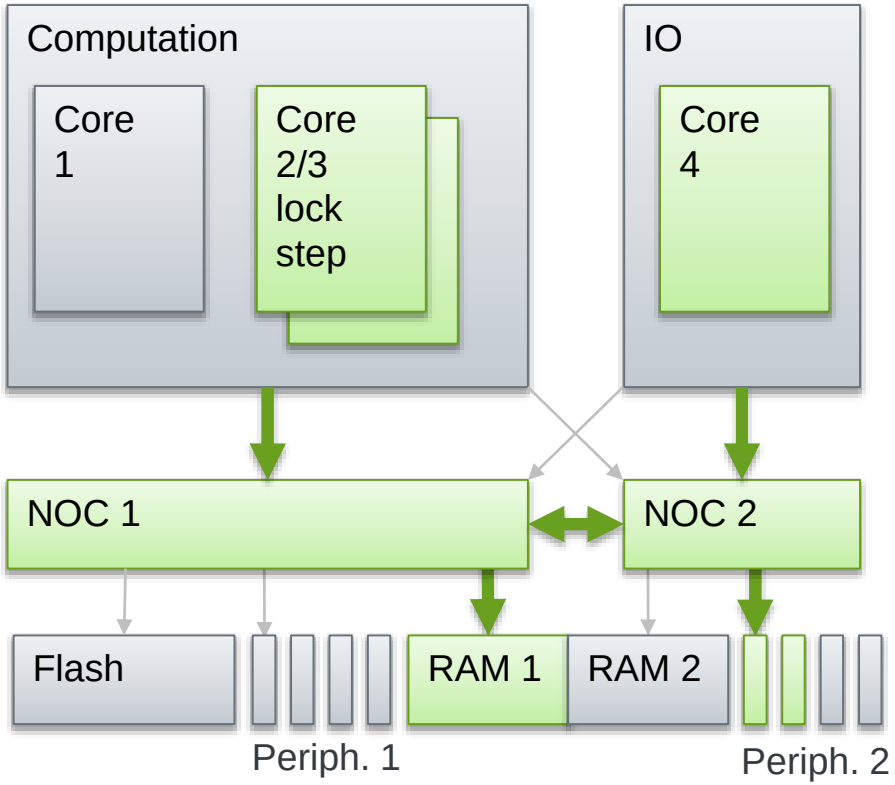
Fault Tolerance Solution Options



Safe Degraded States for ADAS – A Generic Example



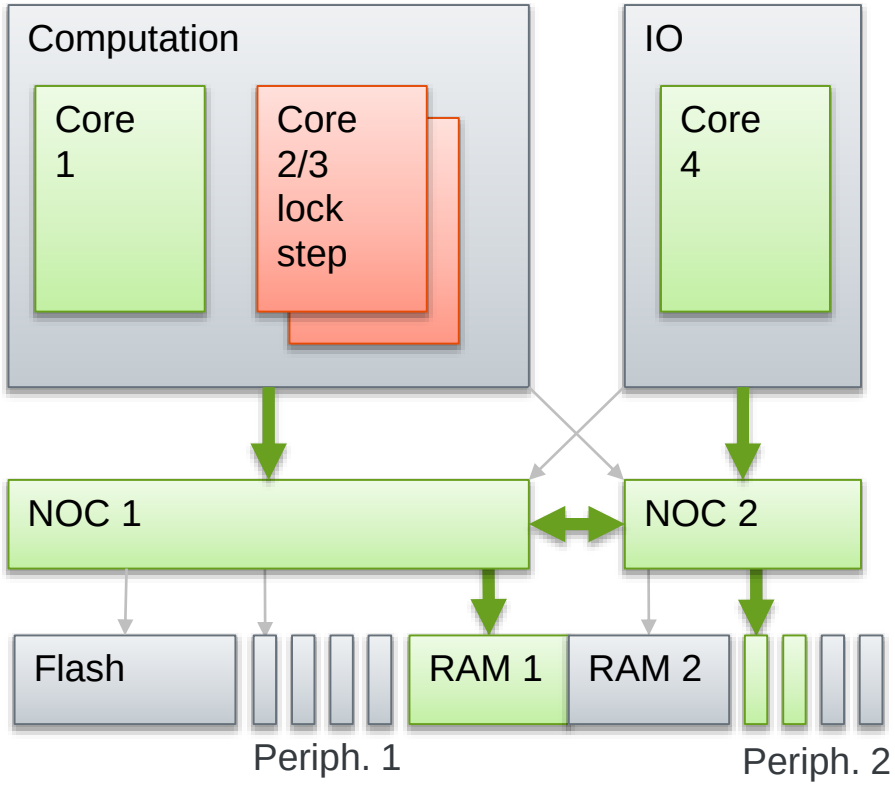
Architecture Options – On-Chip Degradation (1)



- Asymmetric multicore
- Networks on Chip
- Redundant peripherals
- Memory partitions
- Independent clocks
- Robust power distribution

- Hardware measures for
  - Fault localization (e.g. LBIST)
  - Fault removal (e.g. reset, ECC)
  - Fault containment (e.g. clock)
- Software measures for
  - Application reconfiguration

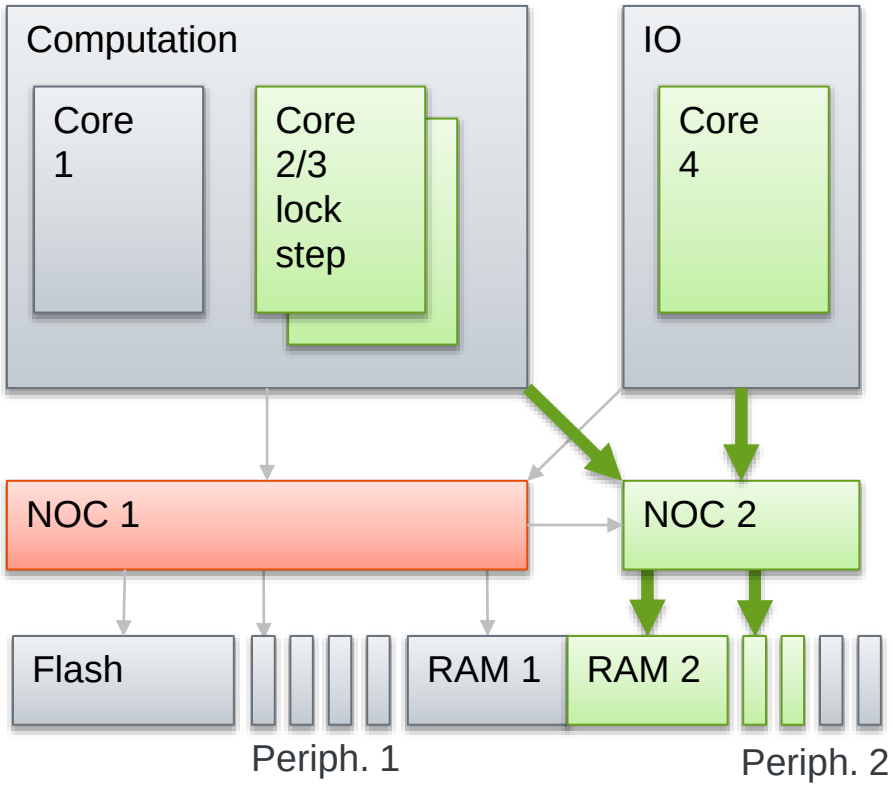
Architecture Options – On-Chip Degradation (2)



- Uncorrectable fault in core 2/3
- Core 1 takes over

- Degraded mode:
  - Comfort functions on core 1 stopped
  - Safety functions continued
  - Reduced diagnostics

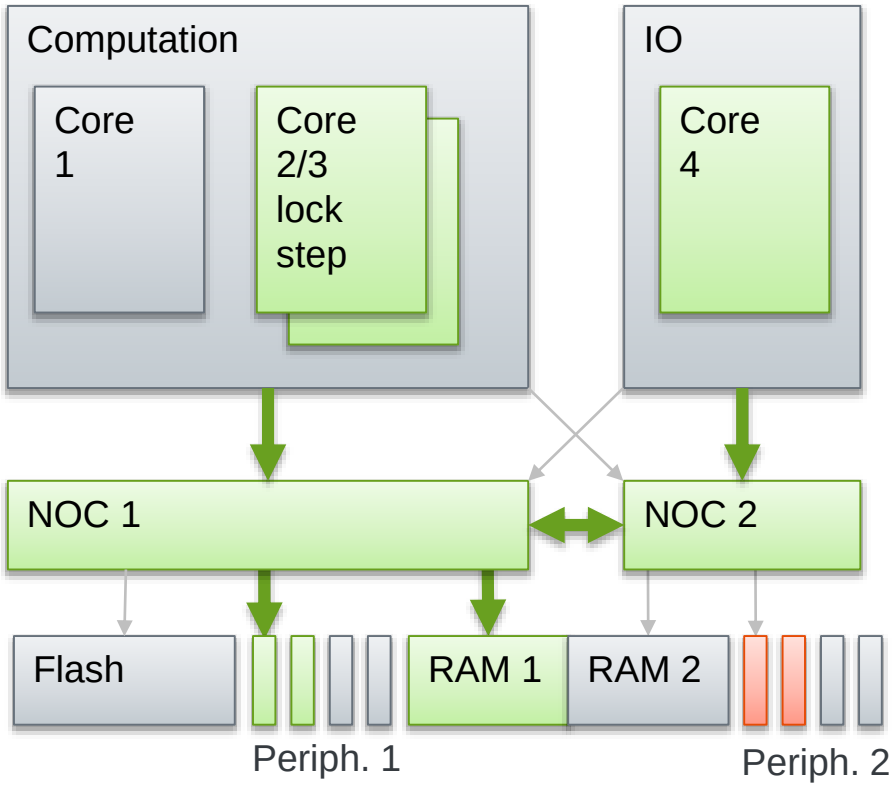
Architecture Options – On-Chip Degradation (3)



- Uncorrectable fault in NOC 1
- Alternative access via NOC 2
- Memory reconfiguration

- Degraded mode:
  - Reduced bandwidth
  - Comfort functions stopped
  - Safety functions continued

Architecture Options – On-Chip Degradation (4)



- Uncorrectable fault in perip. 2
- Periph. 1 takes over

- No degradation
- External components must adopt changed configuration

Architecture Options – On-Chip Full Redundancy (1)

- Started in a Continental + Freescale collaboration
- Press release from 11/13/2012:

Freescale and Continental Partner on Quad-Core 32-Bit Microcontroller for Advanced Stability Applications

11/13/2012

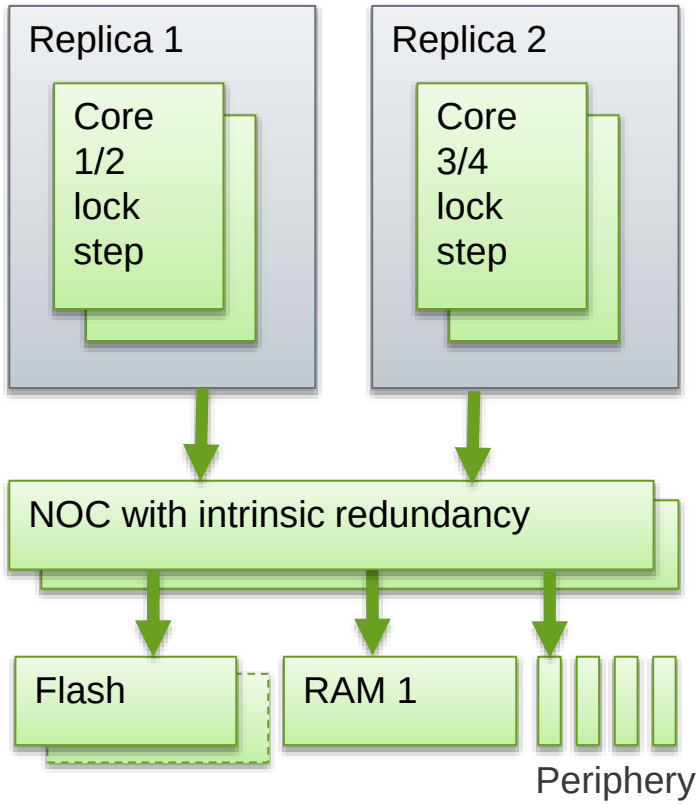
Automotive industry's first quad-core MCU with two pairs of redundant cores integrates Continental's "fault recovery" technology for safety-critical chassis control applications

MUNICH--(BUSINESS WIRE)-- Continuous developments in microelectronics are helping make advanced electronic braking systems (EBS) more reliable, responsive and affordable for mainstream vehicles. To enable the next generation of EBS and chassis control systems, Freescale Semiconductor (NYSE: FSL) and Continental have joined forces to design a high-performance, quad-core microcontroller (MCU) optimized for EBS applications.

The two automotive suppliers are collaborating on a custom MCU program called **Qu**ad-core microcontroller for **A**utomotive **S**afety **A**nd **R**eliability (**QUASAR**) designed to provide the processing intelligence for Continental's next-generation EBS products. The first device in the family integrates four e200z4 cores based on Power Architecture® technology, making it the industry's first quad-core automotive MCU with two pairs of cores in redundant lockstep

"The QUASAR device is de… …to be one of the most po… …d automotive MCU… …rian Traskov, IC Developmer… …Continental's Chassi… …complexity has… …ration bot…

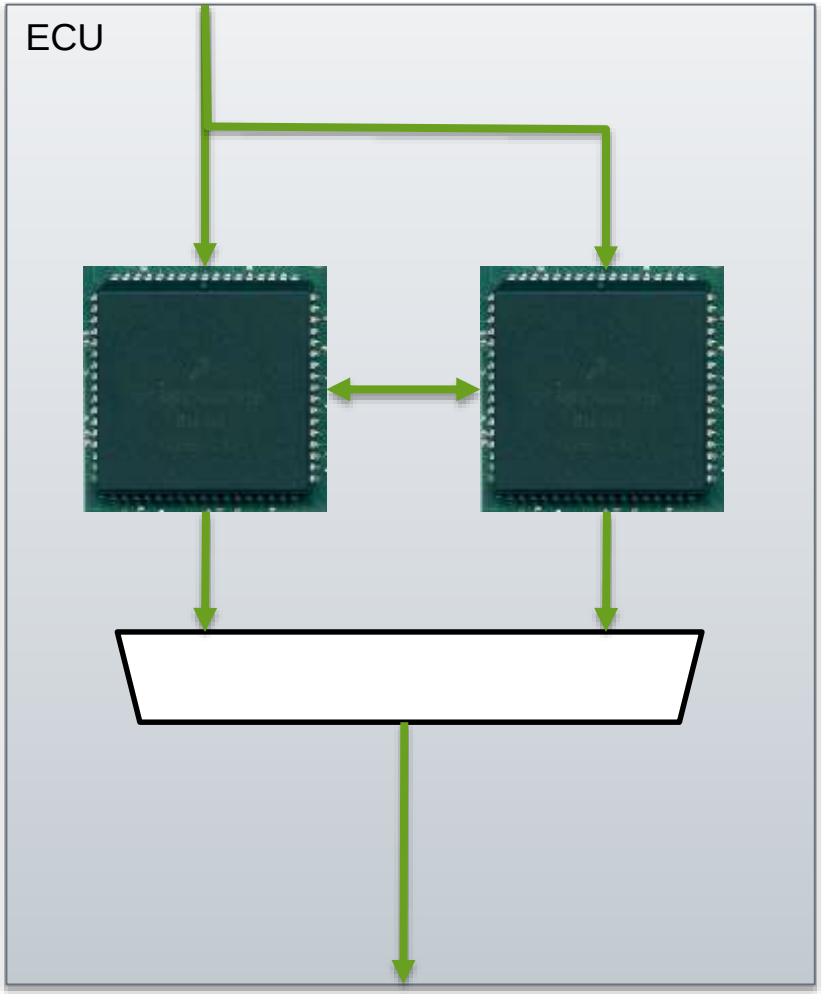
Architecture Options – On-Chip Full Redundancy (2)



- Based on commercial success story continues
- More products on roadmap

- Processing:
  - Hardware redundancy with strong independence
  - Potential software redundancy, diversity
  - Fault detection
  - Fault localization
  - Hardware support for auto reconfiguration
- NOC, peripherals, memories:
  - End-2-end error correction
  - Redundancy

Architecture Options – Two-Chip Redundancy



- Each MCU fail-silent
- MCU 1 master
- MCU 2 hot standby
- Mutual monitoring
- Highest independence

Architecture Options – Comparison

	On-chip degradation	On-chip full redundancy	Two-chip redundancy
SW effort	Very high	Medium	Low
HW cost	Optimized	Elevated	2x
Independence argumentation	Depending on HW measures, difficult	Depending on HW measures, manageable	Easy
Availability evaluation	Difficult	Manageable	Easy
Fault quantification	Difficult	Difficult	Easy
Architecture reuse	Low	High	High

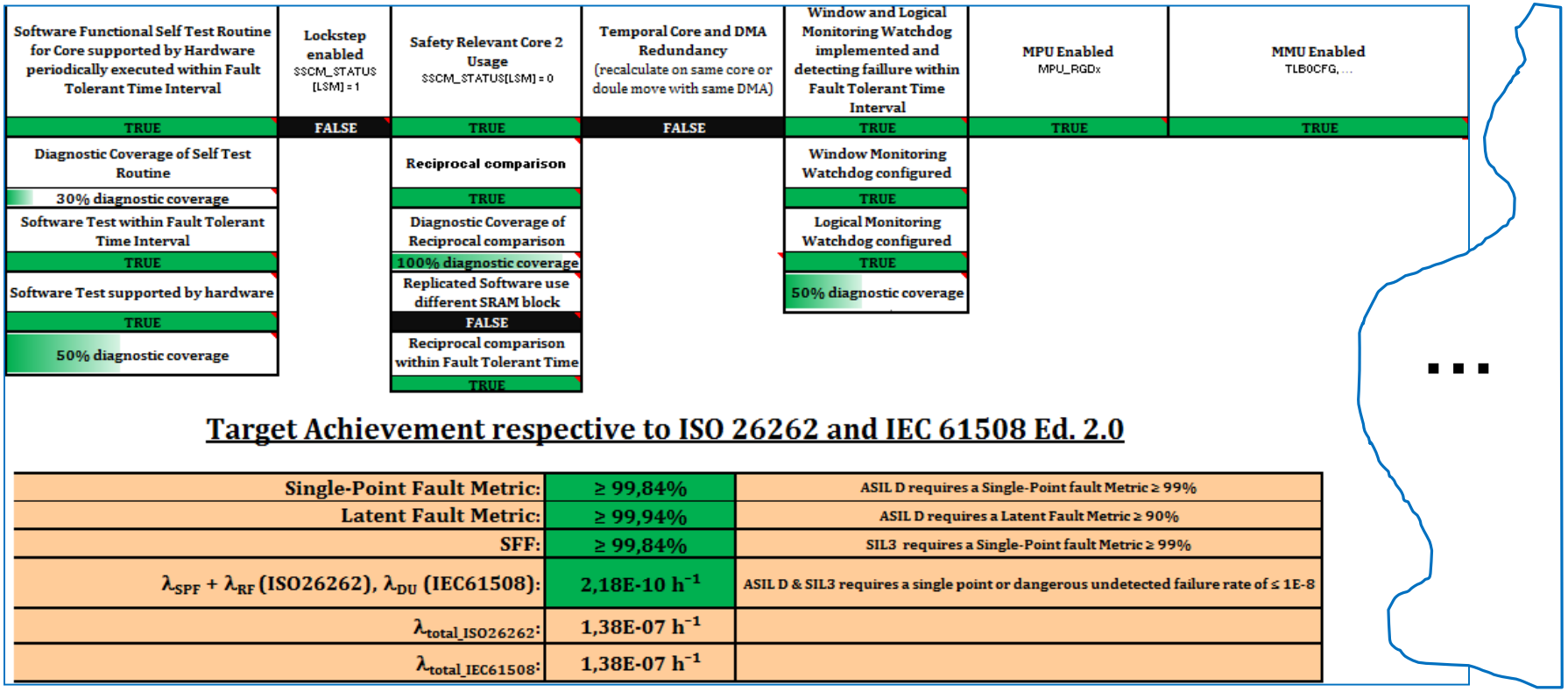
Functional Safety Enablement

Tailor Made FMEDA

- FMEDA enables **temperature profile** adaptation
- FMEDA enables selection of **package** used
- FMEDA enables selection of **enabled diagnostic measures** (tailor to application)
- FMEDA automatically **generates** a **specific customer FMEDA**

Dynamic FMEDA

- Additionally - FMEDA Report
  - Summarizing the assumptions and the method of the inductive functional safety analysis activities based on the FMEDA carried out for the MCU



Software Functional Self Test Routine for Core supported by Hardware periodically executed within Fault Tolerant Time Interval	Lockstep enabled SSCM_STATUS [LSM] = 1	Safety Relevant Core 2 Usage SSCM_STATUS[LSM] = 0	Temporal Core and DMA Redundancy (recalculate on same core or doule move with same DMA)	Window and Logical Monitoring Watchdog implemented and detecting faillure within Fault Tolerant Time Interval	MPU Enabled MPU_RGDx	MMU Enabled TLB0CFG, ...
TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
Diagnostic Coverage of Self Test Routine		Reciprocal comparison		Window Monitoring Watchdog configured		
30% diagnostic coverage		TRUE		TRUE		
Software Test within Fault Tolerant Time Interval		Diagnostic Coverage of Reciprocal comparison		Logical Monitoring Watchdog configured		
TRUE		100% diagnostic coverage		TRUE		
Software Test supported by hardware		Replicated Software use different SRAM block		50% diagnostic coverage		
TRUE		FALSE				
50% diagnostic coverage		Reciprocal comparison within Fault Tolerant Time				
		TRUE				

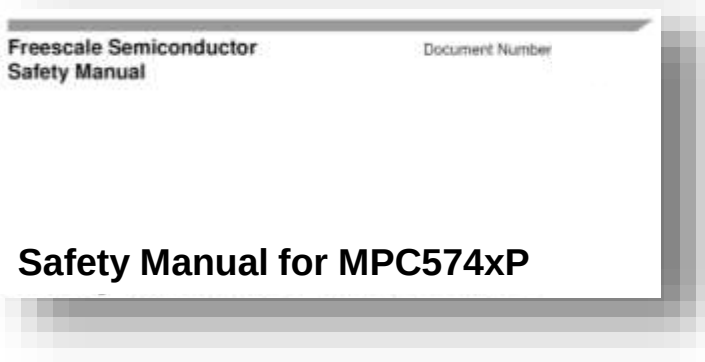
Target Achievement respective to ISO 26262 and IEC 61508 Ed. 2.0

Single-Point Fault Metric:	≥ 99,84%	ASIL D requires a Single-Point fault Metric ≥ 99%
Latent Fault Metric:	≥ 99,94%	ASIL D requires a Latent Fault Metric ≥ 90%
SFF:	≥ 99,84%	SIL3 requires a Single-Point fault Metric ≥ 99%
$\lambda_{SPF} + \lambda_{RF}$ (ISO26262), λ_{DU} (IEC61508):	2,18E-10 h^{-1}	ASIL D & SIL3 requires a single point or dangerous undetected failure rate of ≤ 1E-8
$\lambda_{total\_ISO26262}$:	1,38E-07 h^{-1}	
$\lambda_{total\_IEC61508}$:	1,38E-07 h^{-1}	

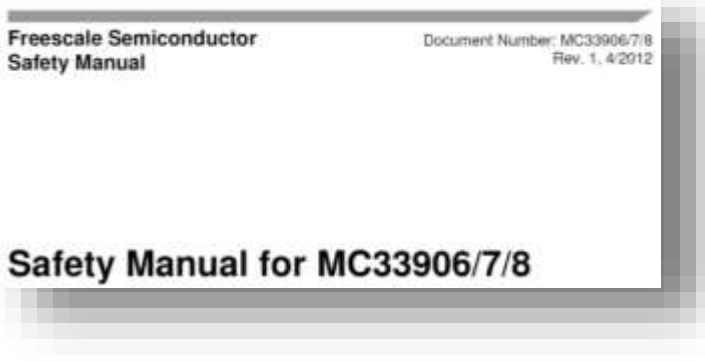
Safety Support – Safety Manual

- Objective
  - Enables customers to extract the full value of Freescale's functional safety offering
  - Simplify integration of Freescale's safety products into applications
  - A comprehensible description of all information relating to FS in a single entity to ensure integrity of information and links with datasheet
- Content
  - MCU Safety Context description
  - MCU Safety Concept description
  - System level hardware assumptions
  - System level software assumptions
  - Pseudo-code or C-Code to simplify adoption of safety software requirements
  - FMEDA summary
    - Full details provided in FMEDA Report
  - Dependent Failures Analysis summary
    - Full details provided in DFA Report

Safety Manual for MCU Solution



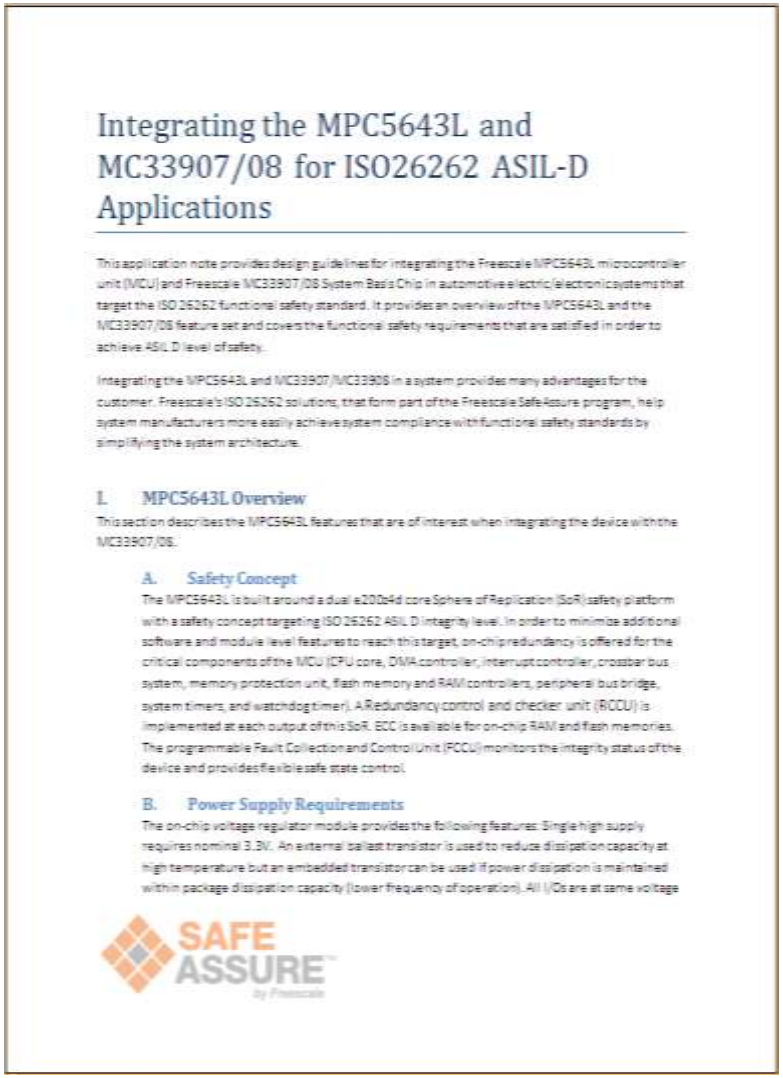
Safety Manual for Analog Solution



Safety Support – System Level Application Notes

Design Guidelines for

- Integration of Microcontroller and Analog & Power Management device
- Explains main individual product Safety features
- Uses a typical Electrical Power steering application to explain product alignment
- Covers the ASIL D safety requirements that are satisfied by using both products:
  - MPC5643L requires external measures to support a system level ASIL D safety level
  - MC33907/08 provides those external measures:
    - External power supply and monitor
    - External watchdog timer
    - Error output monitor



Integrating the MPC5643L and MC33907/08 for ISO26262 ASIL-D Applications

This application note provides design guidelines for integrating the Freescale MPC5643L microcontroller unit (MCU) and Freescale MC33907/08 System Basis Chip in automotive electric/electronic systems that target the ISO 26262 functional safety standard. It provides an overview of the MPC5643L and the MC33907/08 feature set and covers the functional safety requirements that are satisfied in order to achieve ASIL D level of safety.

Integrating the MPC5643L and MC33907/MC33908 in a system provides many advantages for the customer. Freescale's ISO 26262 solutions, that form part of the Freescale SafeAssure program, help system manufacturers more easily achieve system compliance with functional safety standards by simplifying the system architecture.

I. MPC5643L Overview

This section describes the MPC5643L features that are of interest when integrating the device with the MC33907/08.

A. Safety Concept

The MPC5643L is built around a dual e200z4d core Sphere of Replication (SoR) safety platform with a safety concept targeting ISO 26262 ASIL D integrity level. In order to minimize additional software and module level features to reach this target, on-chip redundancy is offered for the critical components of the MCU (CPU core, DMA controller, interrupt controller, crossbar bus system, memory protection unit, flash memory and RAM controllers, peripheral bus bridge, system timers, and watchdog timer). A Redundancy control and checker unit (RCCU) is implemented at each output of this SoR. ECC is available for on-chip RAM and flash memories. The programmable Fault Collection and Control Unit (FCCU) monitors the integrity status of the device and provides flexible safe state control.

B. Power Supply Requirements

The on-chip voltage regulator module provides the following features: Single high supply requires nominal 3.3V. An external ballast transistor is used to reduce dissipation capacity at high temperature but an embedded transistor can be used if power dissipation is maintained within package dissipation capacity (lower frequency of operation). All I/Os are at same voltage

SAFE ASSURE

Supporting Material for Functional Safety

- SafeAssure @ www.freescale.com/SafeAssure
- Certification Package under NDA
- App-Notes, White Papers, Articles
- On-demand Training

Summary

To meet the challenging fault tolerance requirements of Advanced Driver Assistance Systems and other automotive domains Freescale is an excellent supplier by providing:

- **Roadmap of devices for miscellaneous architecture options**
- **Experience in fault tolerant architecture definition**
- **Use case specific safety analysis methodology**
- **Standardization awareness and participation**

References

- [1] Avizienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C., "Basic concepts and taxonomy of dependable and secure computing," Dependable and Secure Computing, IEEE Transactions on , vol.1, no.1, pp.11,33, Jan.-March 2004

- Abbreviations:
  - ADAS: Advanced Driver Assistance Systems
  - ASIL: Automotive Safety Integrity Level, defined in ISO 26262
  - FO: Fail-operational
  - FS: Fail-safe
  - HFT: Hardware Fault Tolerance, defined in ISO 26262, ISO 2382
  - RAID: Redundant Array of Independent Disks
  - SIL: Safety Integrity Level, defined in IEC 61508

www.Freescale.com