



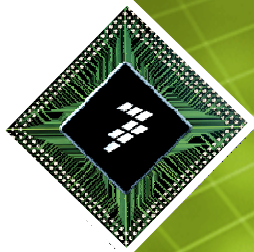
Functional Safety. Simplified.

Discover how we make it easier for you to attain system compliance >

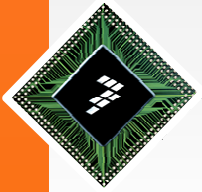
Freescale Forum **Funktionale Sicherheit** **Automotive MCUs**

Mark O'Donnell

Sr. Product Manager
Automotive Group

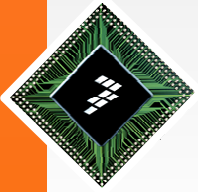


Freescale, the Freescale logo, Altivec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, the Energy Efficient Solutions logo, mobileGT, PowerQUICC, QorIQ, StarCore and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. BeeKit, BeeStack, ColdFire+, CoreNet, Flexis, Kinetis, MXC, Platform in a Package, Processor Expert, QorIQ, Qonverge, Qorivva, QIICC Engine, SMARTMOS, TurboLink, VortiQa and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2011 Freescale Semiconductor, Inc.



Agenda

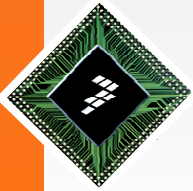
- Automotive Functional Safety Requirements
 - System level v sub component level (SEooC)
- Safety concepts of Freescale's Auto MCUs
- Safety Support
 - FMEDA
- Summary



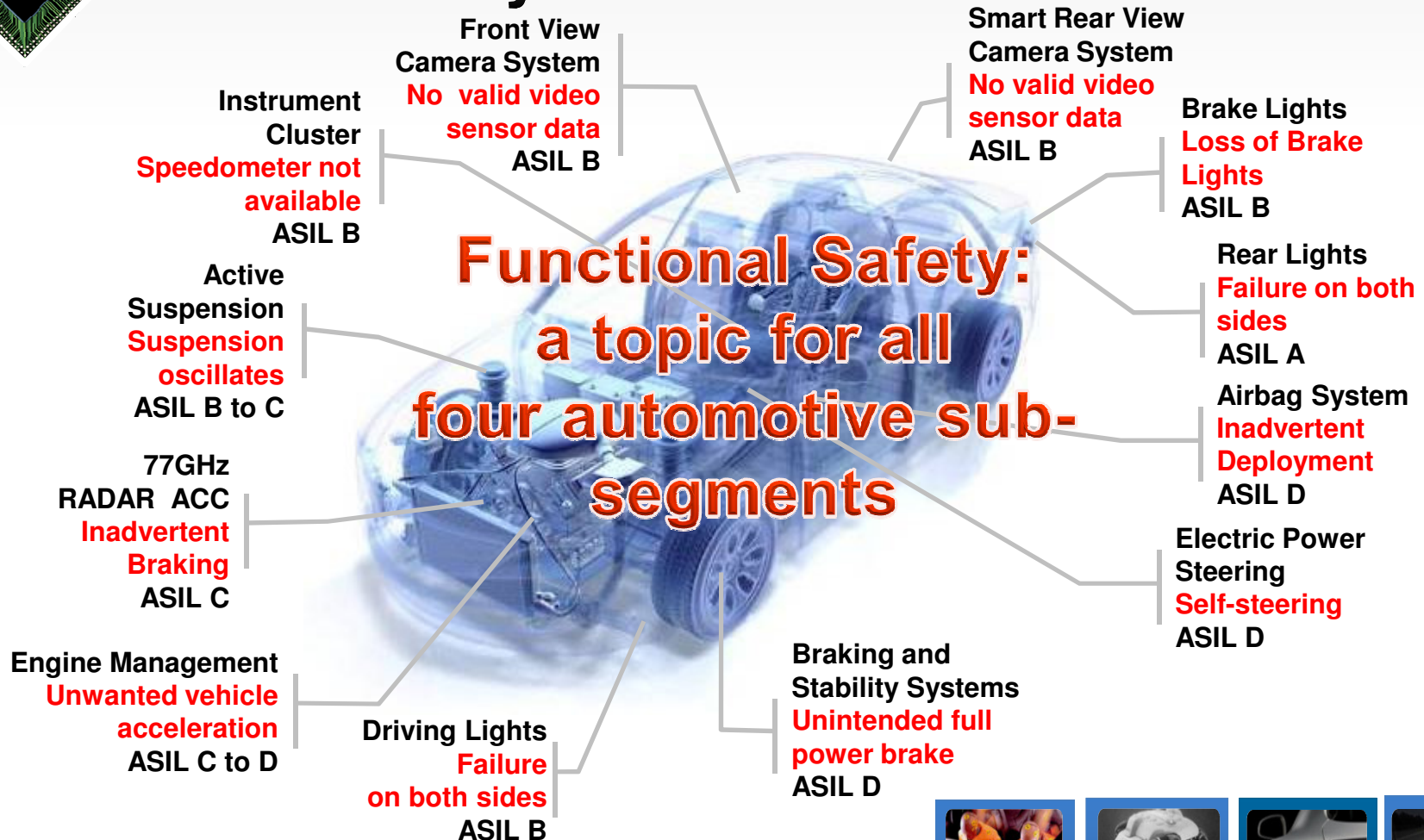
Functional Safety Defined



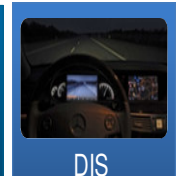
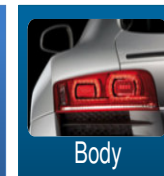
- Functional safety is the **absence of unreasonable risk** due to hazards caused by malfunctioning behavior of electrical/electronic systems
 - **Hazards**: potential source of harm
 - **Harm**: physical injury or damage to the health of people
- **Failures** are **main impairment** to safety:
 - **Systematic**: failures, related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or manufacturing process, operational procedures, documentation or other relevant factors
 - **Random**: failures that can occur unpredictably during the lifetime of a hardware element and that follow a probability distribution

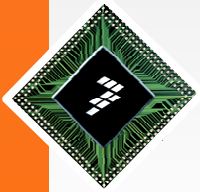


Automotive System Trends for ASIL Levels



Source: Freescale: Expectations based on global customer feedback





No “best” Safety Architecture exists!

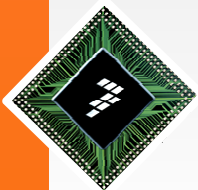
Every embedded application has its very specifics!

Microcontroller are successful due to the general purpose nature
(can be adapted to the specifics of an application)

Therefore **Freescal** provides products with
different Multi-Core safety architectures:

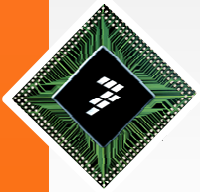
- **Monolithic** integration (safety system on chip)
- Multiple device **system level integration** (multiple chip ECU)
- **Distributed** system integration (multiple ECU system)
- ...

Customer may select their most suitable architecture!

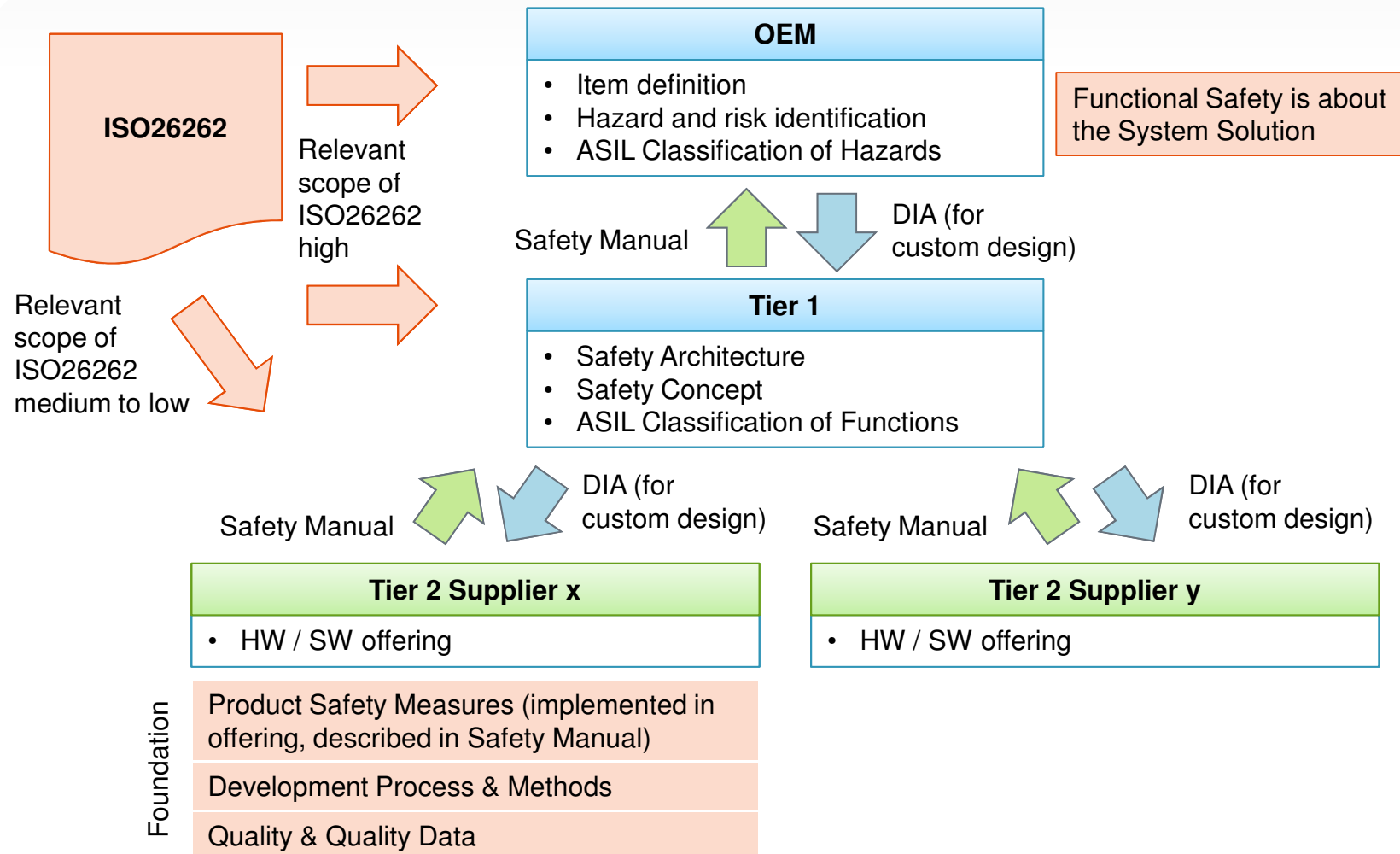


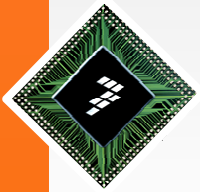
Safety Architecture Challenge

- ISO 26262 safety lifecycle defined as top down approach
 - Next level requirements result from previous level
 - In practice also “push-back” due to availability of products with desired functionality and safety measures
- Safety architecture needs to be defined such that it is safe and can be realized in an efficient way
 - Commission custom ASICs with application specific safety measures
 - Use off-the shelf components with an integrated safety architecture
 - Many new components emerging in light of ISO 26262 adoption
 - Define major elements of safety architecture at system level
 - Use “standard” off-the shelf components → discrete (component) safety architecture
 - Traditional way of designing a functional safety system



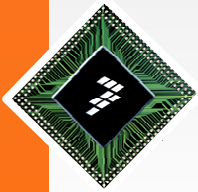
Top-Down Interaction from ISO26262 flow and dependancies





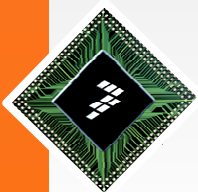
From Integrated to Discrete Safety Architecture

Integrated Safety Architecture		Discrete Safety Architecture
At system level and at component level	Safety Architecture	Resolved at system level
One or more devices contain dedicated safety measures based on an underlying safety concept	Device Level Safety Measures	No underlying safety concept at device level, typically, however, measures exploitable as safety measures available
Available for integrated safety measures	Device Level Safety Manual	None
FMEDA, DFA for dedicated safety measures	Device Level Safety Analysis	None, typically general supporting information sufficient
Safety case, with complete device level argument for ISO 26262 compliance at device level	Device Level Safety Argument	Qualification + optional evaluation of measures in development process against systematic faults



Safety Architectures

	ASIL A	ASIL B	ASIL C	ASIL D
Discrete Safety Architecture	✓	✓	✓	✓
Integrated Safety Architecture	✓	✓	✓	✓



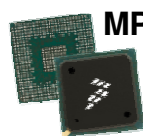
History of Auto MCU Functional Safety Solutions

- **Gen 1 Safety** More than 10 years experience of safety development in the area of MCU & SBC
- **Gen 2 Safety** First general market MCU, **MPC5643L** ⇒ **Certified ISO 26262!**
- **Gen 3 Safety** From 2012, multiple MCUs in Body, Chassis and Powertrain are being designed and developed according to ISO 26262

Functional Safety Solutions

2012

Gen 3 Safety



MPC5744P/MPC5777K/etc 55nm

- 32-bit Dual/Quad-Core MCU
- Developed according to ISO 26262
- Target Applications Chassis & P/T for – ASILD
- Safe methodology, Architecture, SW and tools

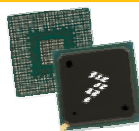


PowerSBC Gen 2

- Voltage Supervision
- Fail-Safe State Machine
- Fail-Safe IO
- Advanced Watchdog

2008

Gen 2 Safety



MPC5643L – 90nm

- 32-bit Dual-Core MCU
- Developed according to ISO 26262
- Target Applications for Chassis – ASILD



PowerSBC

- Voltage Supervision
- Fail-Safe State Machine
- Fail-Safe IO
- Advanced Watchdog

2000

Gen 1 Safety

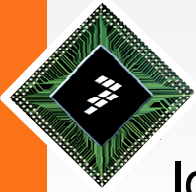


Custom Safety Platform for Braking

- Started to ship in 2000 first safe MCU for braking applications
- IEC 61508 / ISO 26262 compliance achieved at system level (top down approach)
- MCU features are a key enabler for SIL3 / ASILD



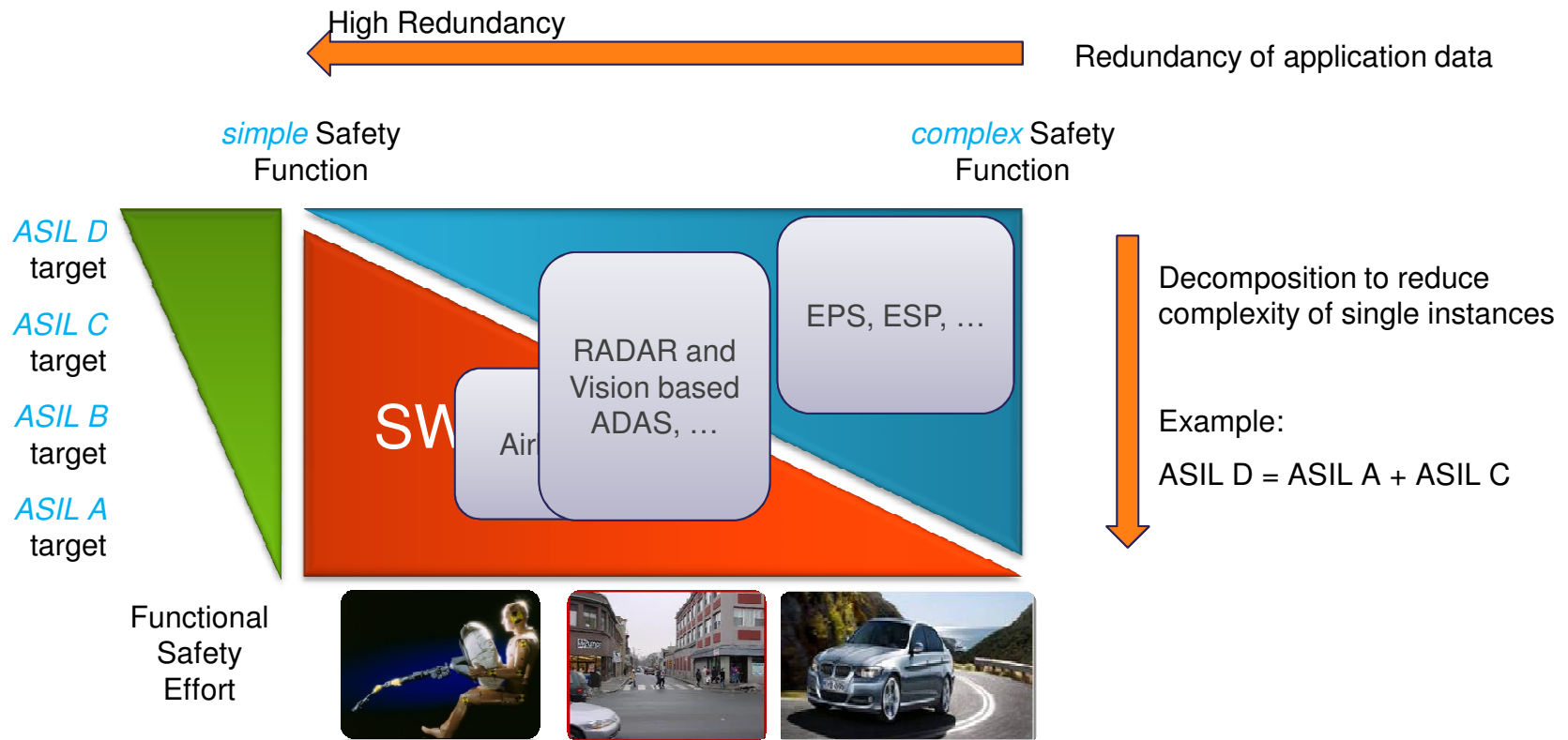
Custom IC

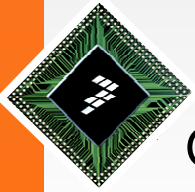


Our Vision in safety: know your context

Ideal partitioning between HW and SW measures dependant on ASIL target and complexity of safety function

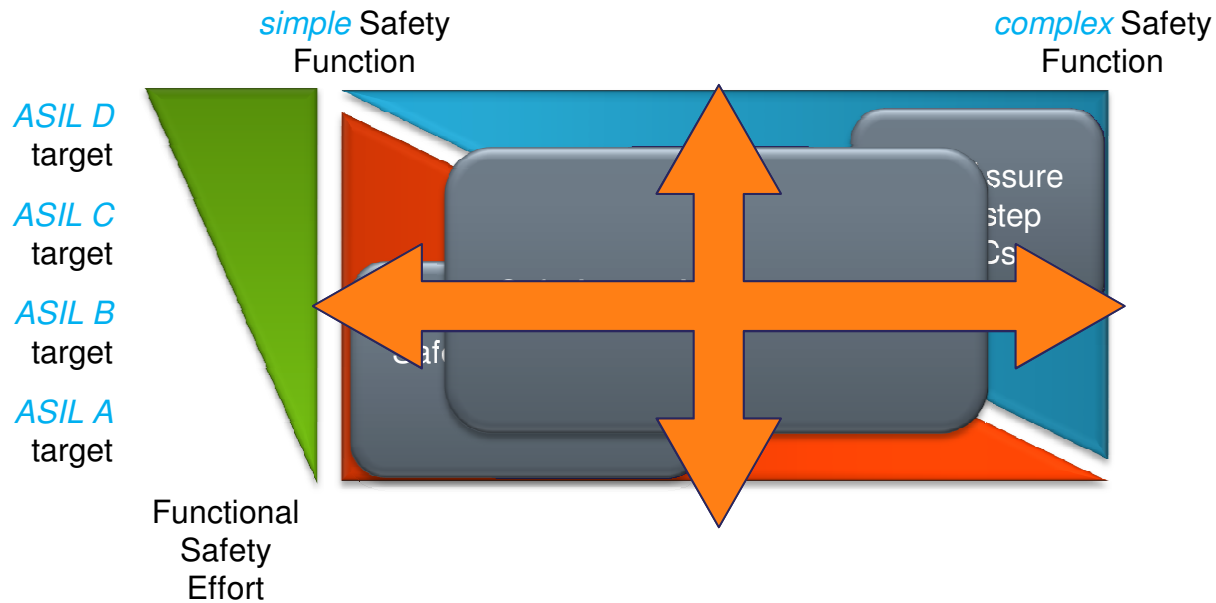
Example Safety Applications ...



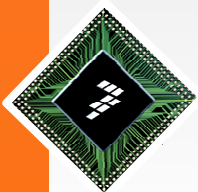


Our solution for safety: Balance and flexible

Offering products that scale to application specific safety requirements



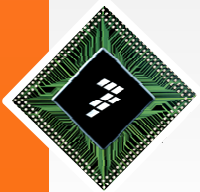
Spanning the **whole range efficiently ...**



SafeAssure Products

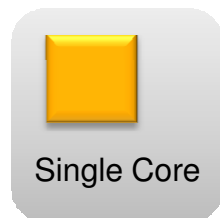
Target Market	Product Type	Product	Target Applications	Safety Process	Safety Hardware	Safety Support
Automotive	MCU	MPC5746M	Diesel Engine Management Direct Injection Engines Electronically Controlled Transmissions Gasoline Engine Management	ISO 26262 ASIL D	Integrated Safety Architecture e.g.: Multi core, delayed lockstep, e2eECC, replicated peripherals, LBIST & MBIST, FCCU	FMEDA Safety Manual
		MPC574xP	Electric Power Steering Braking and Stability Control Advanced Driver Assistance Systems (ADAS) Safety Domain Control	ISO 26262 ASIL D	Integrated Safety Architecture e.g.: Dual core, delayed lockstep, e2eECC, replicated peripherals, LBIST & MBIST, FCCU	FMEDA Safety Manual
		MPC567xK	77 GHz RADAR System	FSL QM	Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	FMEDA Safety Application Note
		MPC564xL	77 GHz RADAR System Electric Power Steering Braking and Stability Control	ISO 26262 ASIL D	Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	FMEDA Safety Manual System Level Application Note
		MPC560xP	DSI Airbag System PSIS Airbag System Electric Power Steering	FSL QM	Single core, SEC/DED ECC, Clock Monitoring Unit, Low Voltage Detector, FCU	FMEDA Safety Application Note
	Analog and Power	MC33906	Safety Critical Motor Control Electric Power Steering	ISO 26262 ASIL D	Integrated Safety Architecture e.g.: Independent Voltage Monitoring and Fail Safe state Machine (ABIST, LBIST), FCCU Monitoring for Dual Core LockStep Mode, Several HW diagnostic to cover SPF, LT	Safety Manual, FMEDA System Level Application Note
		MC33907	Electrical Power Steering Safety critical motor control applications Vehicle dynamic and chassis control	ISO 26262 ASIL D	Integrated Safety Architecture	Safety Manual, FMEDA System Level Application Note
		MC33908	Integrated Chassis Domain Safety critical motor control applications	ISO 26262 ASIL D	Integrated Safety Architecture	Safety Manual, FMEDA System Level Application Note
		MC33789	PSIS Airbag System	FSL QM	4x PSIS Host, Safing Block	Safety FMEA
		MC33926	Valve control in Powertrain applications	FSL QM	Output state flag, Thermal Shutdown	Safety FMEA
	Sensors	MMA16xx MMA26xx	DSI Airbag System	FSL QM	DSI2.5 safety bus, Triggered self test, Over-damped MEMS	FTA
		MMA51xx MMA52xx	PSIS Airbag System	FSL QM	PSIS safety bus, Triggered self test, Over-damped MEMS	FTA
		MMA65xx MMA68xx	PSIS Airbag System Electric Power Steering (EPS)	FSL QM	SPI w/ CRC, Triggered self test, Over-damped MEMS	FTA
		MMA69xx	Braking and Stability Control	FSL QM	SPI w/ CRC, Triggered self test, Over-damped MEMS	FTA
Industrial	MCU	PXS20	Aerospace Anesthesia Unit Monitor Input-Output Control (I/O Control) Process Control, Temperature Control Programmable Logic Control (PLC)	ISO 26262 ASIL D	Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	FMEDA
		PXS30	Motor Drivers Robotics Safety Shutdown Systems Ventilators and Respirators	FSL QM		Safety Application Note

- To view the latest SafeAssure product table visit www.freescale.com/SafeAssure



uC Architecture Evolution – Functional Safety Related

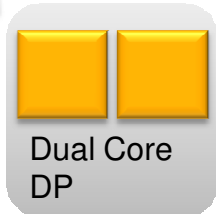
- Standard performance
- Less complex function / application



- Complex function / application



- Increased performance
- Less complex function / application



- Increased performance at low power (auto code)
- Multiple applications merged into one SoC (Hypervisor/Virtualization) (third party code, OEM and tier1 code separated, "rented cores")
- Increased availability
- Hybrid, Electrification, High end braking



- Increased performance at low power (auto code)
- Multiple applications merged into one SoC (Hypervisor/Virtualization)
- Increased availability
- Application specific safety
- Combustion engine, Sensor Fusion



- Dedicated Hardware accelerators
- Application specific safety
- ADAS (Vision, RADAR)

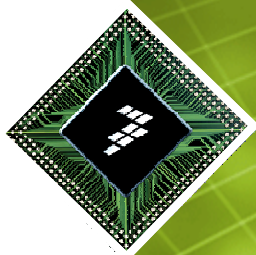


- Optional Dedicated Hardware accelerators
- Less complex function / application
- Application specific safety
- ADAS (Vision, RADAR)
- High End Body
- Sensor Fusion

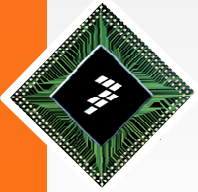
* A *complex* function (application) here refers to the combination of a *high computational* demand for the application combined with a *short control cycle*.



Safety Concept of an MCU with Integrated Safety Architecture

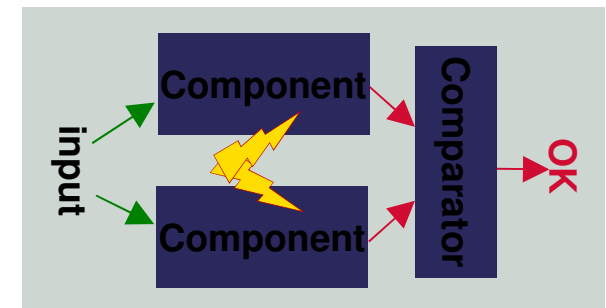
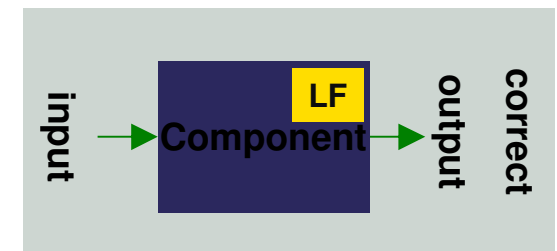
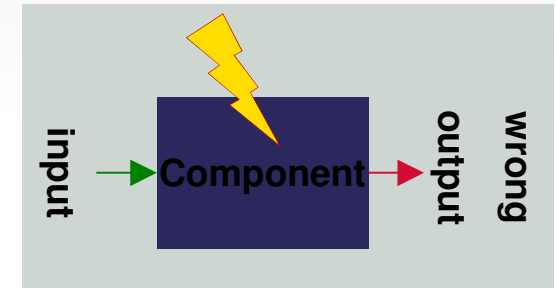


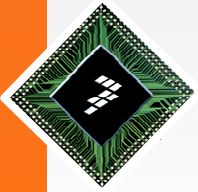
Freescale, the Freescale logo, Altivec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, the Energy Efficient Solutions logo, mobileGT, PowerQUICC, QorIQ, StarCore and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. BeeKit, BeeStack, ColdFire+, CoreNet, Flexis, Kinetis, MXC, Platform in a Package, Processor Expert, QorIQ, Qonverge, Qorivva, QUICC Engine, SMARTMOS, TurboLink, VortiQa and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2011 Freescale Semiconductor, Inc.



Random Failures and their Handling

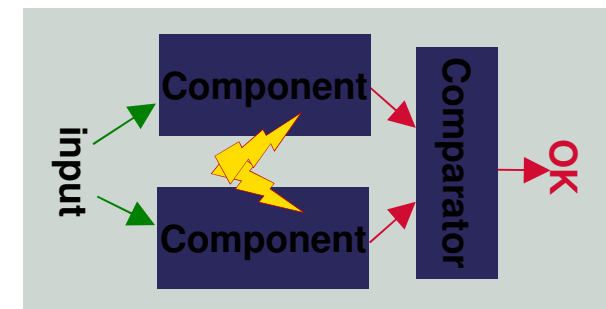
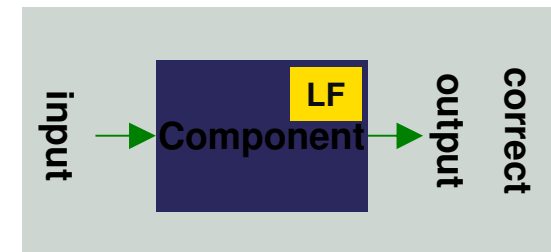
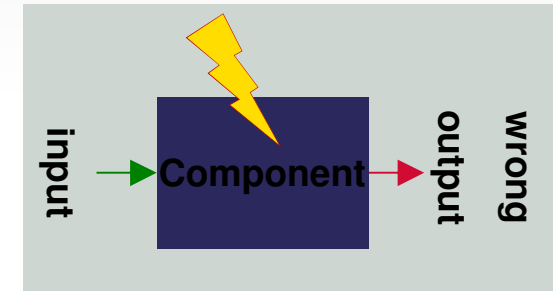
- Single Point Failure (SPF)
 - Immediate potential to cause a hazard
 - Quick detection or mitigation
- Latent Failure (LF)
 - Can become dangerous in conjunction with a second fault
 - Can aggregate
 - Periodic detection
- Common Cause Failure (CCF)
 - Causes several components to fail
 - Can possibly annul redundancy-based measures
 - Mitigation or quick detection

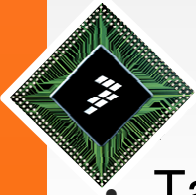




MCU Countermeasures for Failure Classes

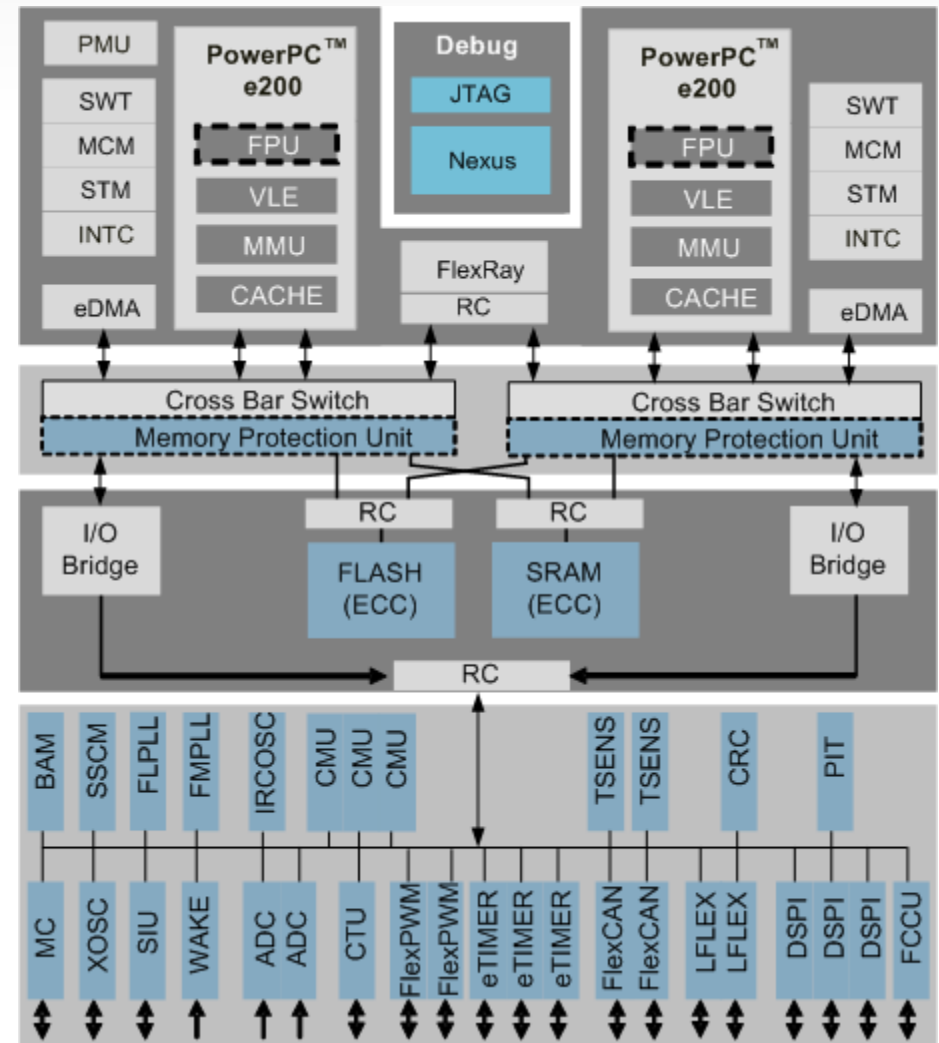
- Single Point Failure (SPF)
 - Structural redundancy
 - Core, DMA
 - Information redundancy
 - **E2E ECC**, EDC on Cache
- Latent Failure (LF)
 - HW-Self test
 - Memory, logic
 - 90% stuck-at
- Common Cause Failure (CCF)
 - Delayed Checker Core
 - Supervision of clock, power and temperature
 - Independent safety clock
 - Independent failure signaling

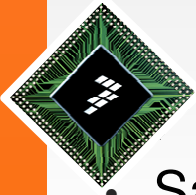




Safety Concept Example: MPC5643L (1)

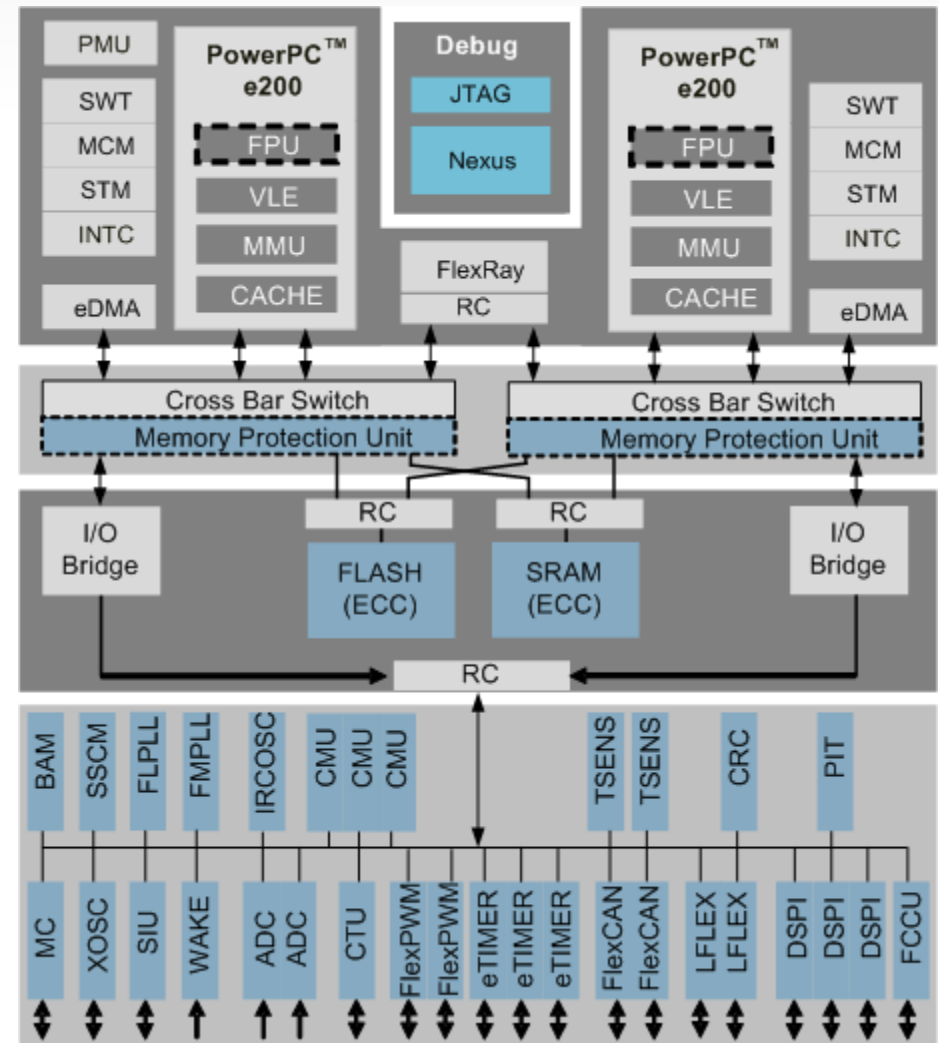
- Target applications
 - Safety applications that require a high safety integrity level, such as:
 - Electric power steering
 - Electronic stability control
- Item must be in safe state for modes of (non)operation:
 - Completely unpowered
 - Reset
 - Operating correctly
 - Indicating an internal error
- Safety mechanism: technical solution to detect faults or control failures in order to achieve a safe state

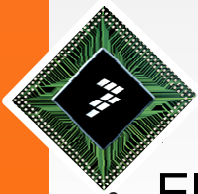




Safety Concept Example: MPC5643L (2)

- Safety mechanisms:
 - Built-in self tests (memory, logic, ADC)
 - Duplicate computational elements in lock-step
 - ECC for FLASH/SRAM
 - Temperature, clock and voltage monitors
 - Fault Collection and Control Unit (FCCU) with redundant fault notification path
 - Independent safety clock
 - eDMA and CRC
 - Access protection (MPU, register)





Safety Concept Example: MPC5643L (3)

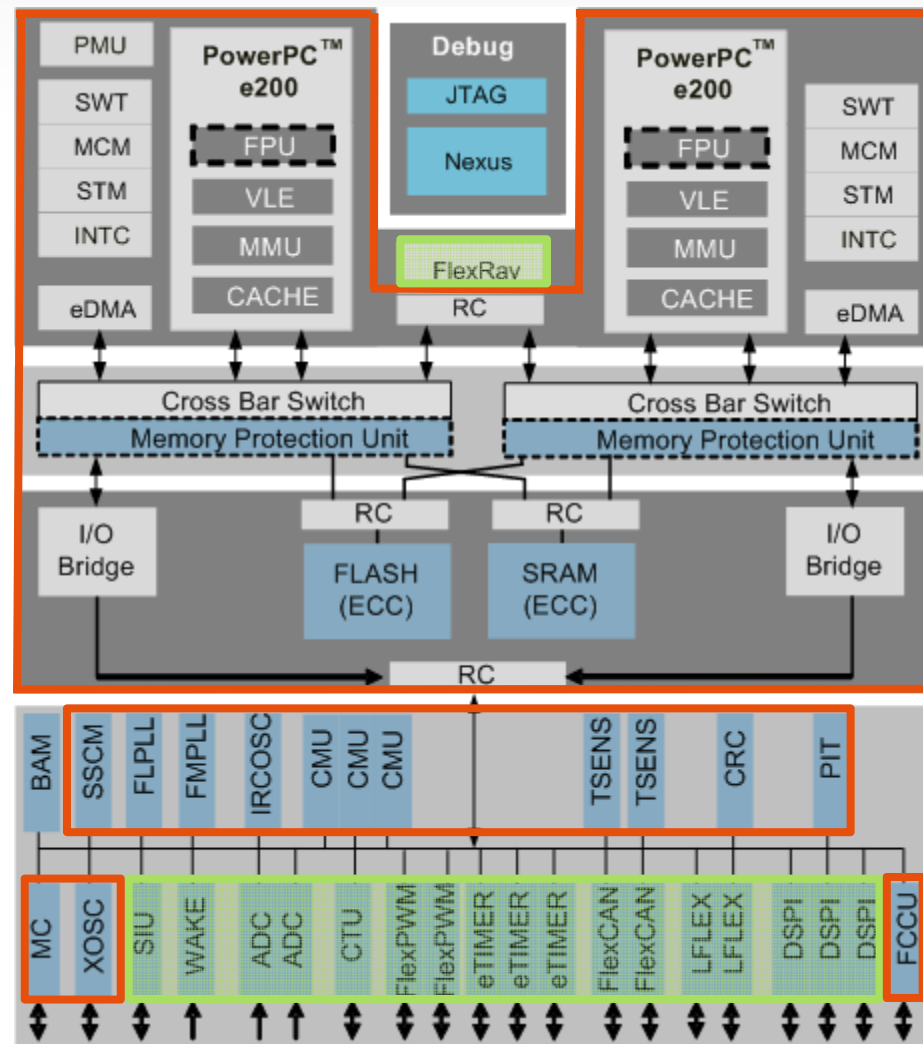
- Elements having low application dependency
 - Safety architecture may not interfere with application
 - Hardware driven

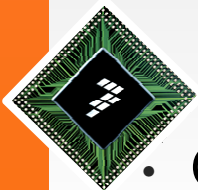
Computational Shell

System Safety mechanisms

- Elements having high application dependency
 - Functional safety of the periphery is ensured by system-level measures
 - Flexible usage within application software

I/O & Communication Peripherals





First ISO 26262 Certified MCU – Qorivva MPC5643L

- Certified by exida – an independent accredited assessor
- Certificate issued based on a successful assessment of the **product design and applied development and production processes** against all requirements and work product definitions of ISO 26262 identified as applicable to an MCU part
- **MPC5643L MCU certified for use for all Automotive Safety Integrity Levels (ASIL), up to and including the most stringent level, ASIL D**

Released on 6th September, 2012



The manufacturer may use the mark:



Reports:
Freescale 11/08-067-C
R009 V1 R0
Results of the ISO 26262
Functional Safety
Assessment

Validity:
This assessment is valid for
Microcontroller MPC5643L

This assessment is valid
until August 31, 2015.

V1 R1 September, 2012



Certificate / Certificat
Zertifikat / 合格証

FREESCALE 1108067 P0026 C001

exida Certification S.A. hereby confirms that the:

MICROCONTROLLER MPC5643L

FREESCALE Halbleiter Deutschland GmbH
Munich, Germany

Has been assessed per the relevant requirements regarding μ C development and verification & validation of:

ISO 26262 : 2011 Parts 2, 4, 5, 7, 8, 9 and 10 (to the extent applicable)

and meets requirements providing:

Systematic Integrity: ASIL D

Safety related function:
The μ C supports the execution of safety-related software by a dual-core lock-step architecture with memory protection and centralized fault collection and control unit.

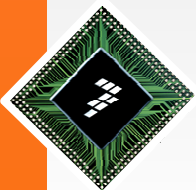
Application restrictions:
The microcontroller shall be used per the Safety Application Guide requirements.




 Evaluating Assessor

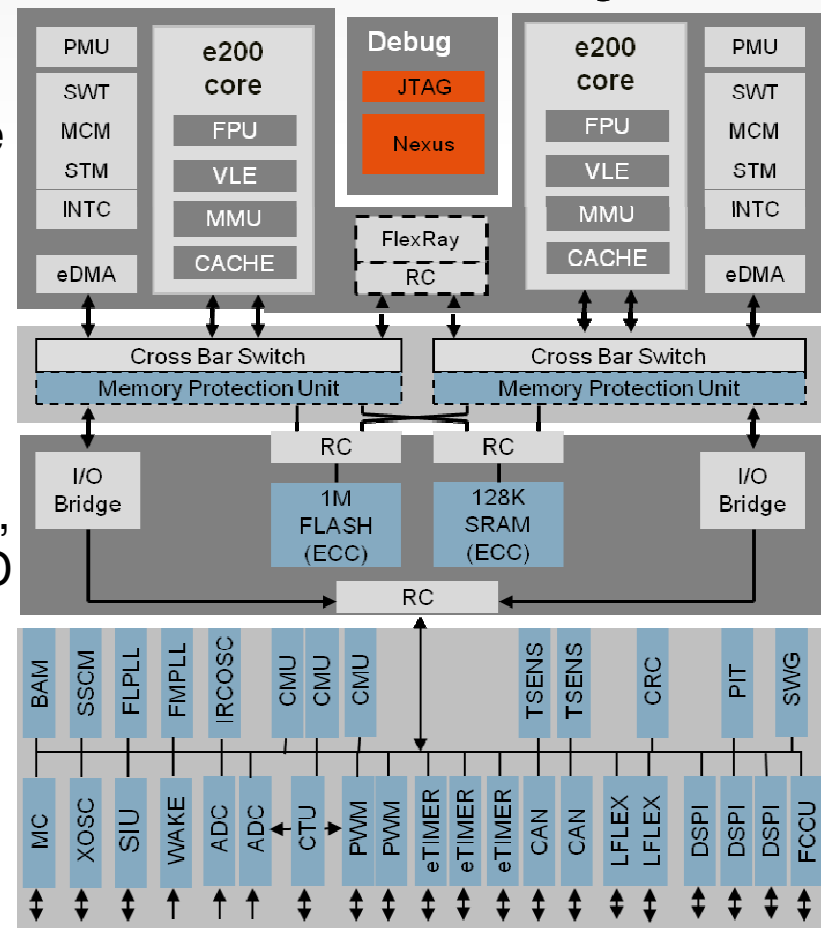
 Certifying Assessor

Page 1 of 2

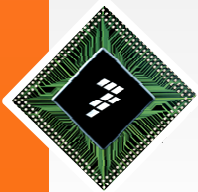


ISO 26262 Assessment and Audit Summary

- Assessment of the MPC5643L Safety Case
- Assessment and audit of Freescale's development processes used for the MPC5643L
- Assessment of the FMEDA (Failure Modes Effects and Diagnostic Analysis) of the MPC5643L to confirm it satisfies the SPFM, LFM and PMHF metrics required for ASIL D
- Assessment of the MPC5643L hardware design, implementation and verification activities
- Over 50 work products were provided to exida during the assessment and on-site audits

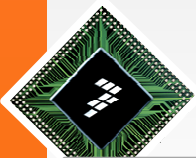


MPC5643L MCU



Safety concept btw. MPC5643L (90nm) & MPC5744P (55nm)

	MPC5643L	MPC5744P
ISO 26262, ASILD	Targeted	Targeted
Lock Step (DMA and RCCU)	Core and DMA using RCCUs for output signal comparison	A delayed lockstep (2 system clock cycles delay)
Lock Step (XBAR, SRAM and Flash)	XBAR, SRAM controller, flash controller are operating in lock step	E2E ECC is used instead to ensure correct bus transactions
Lock Step (PBRIDGE)	PBRIDGE was in lock step	two separated PBRIDGE blocks with a separate set of peripherals for redundant usage
ECC protection	N/A	extended for more memories (Flexray, FlexCAN and DMA)
Extended memory protection	N/A	Extended memory protection mechanisms (Core-MPU)
Logic BIST and memory BIST	to detect latent faults during start-up	to detect latent faults during start-up
ADC and PMU self-test	Available	Available
Temperature sensor, power and clock monitoring	Available	Available
Safety Application Guide	Available	New Safety Manual



SafeAssure MCU Product – MPC5744P

Safety Process

ISO 26262 ASIL D

- Safety assessment of MCU architecture and development process (ISO 26262)
- helps to reduce effort and time on ECU functional safety assessment

Safety Hardware

Integrated Safety Architecture (ISA)

- Saves development effort and time as no complex diagnostic SW required
- CPU processing power available for running applications
- High diagnostic coverage in HW to detect random faults

Safety Software

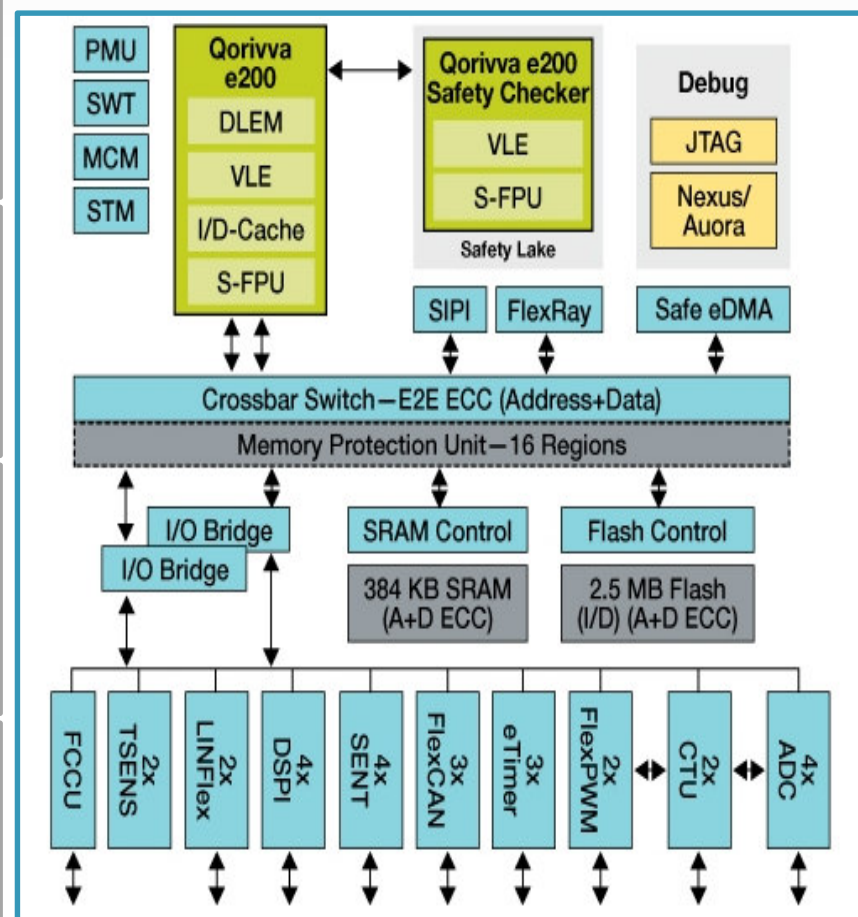
SW deliverables provided by Freescale and partners

- Enable support for ASIL D applications with minimized performance degradation
- sMCAL & sOS, Selftests, SW Safety Manual

Safety Support

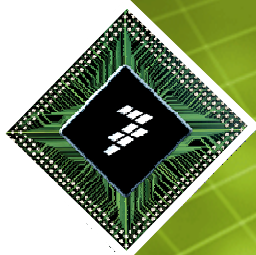
Safety enablement provided by Freescale

- Safety Manual
- FMEDA
- System Level Application Note

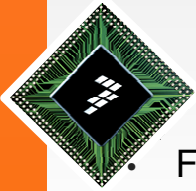




Safety Support - FMEDA



Freescale, the Freescale logo, Altivec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, the Energy Efficient Solutions logo, mobileGT, PowerQUICC, QorIQ, StarCore and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. BeeKit, BeeStack, ColdFire+, CoreNet, Flexis, Kinetis, MXC, Platform in a Package, Processor Expert, QorIQ, Qonverge, Qorivva, QUICC Engine, SMARTMOS, TurboLink, VortiQa and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2011 Freescale Semiconductor, Inc.

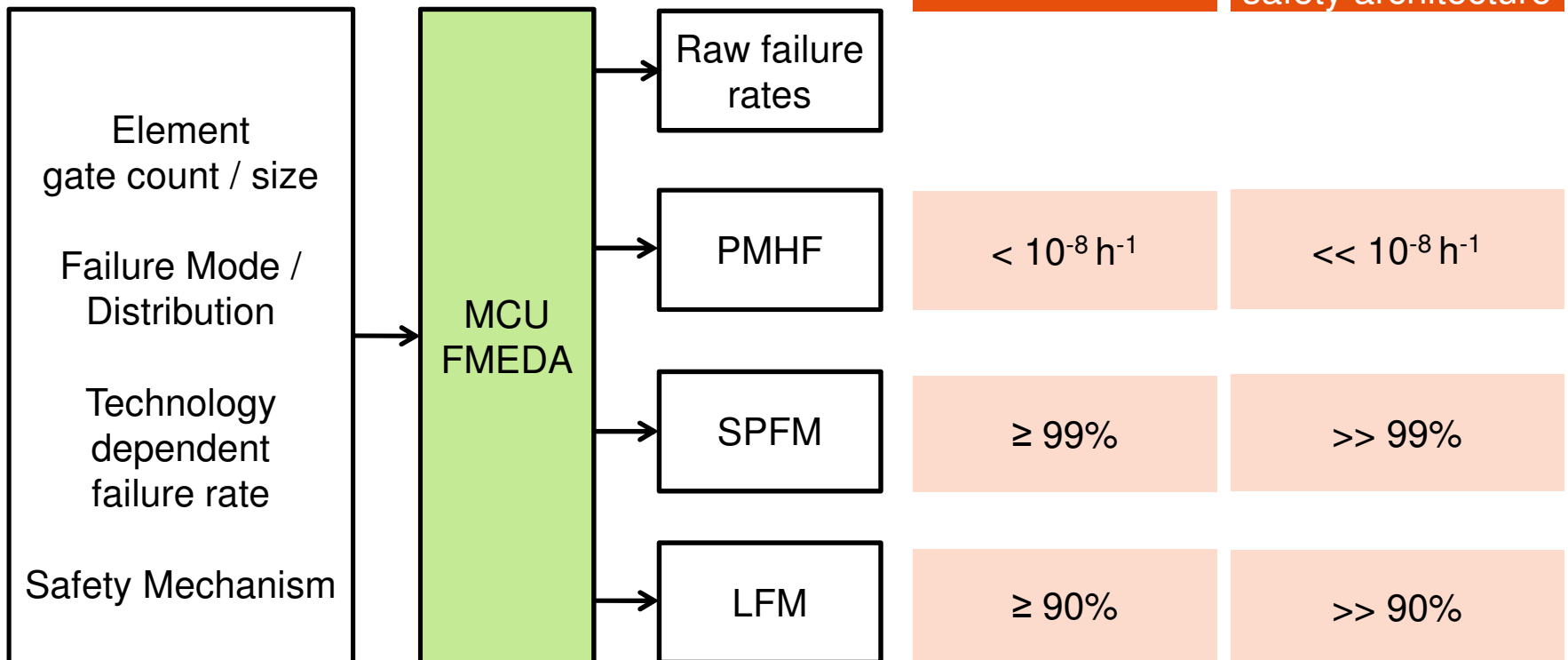


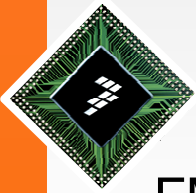
FMEDA: System-Level versus MCU

- Failure Mode, Effect and Diagnostic Analysis
- A systematic way to **identify** and **evaluate failure modes**, **effects** and **diagnostic techniques**, and to **document** the system.
- target values can be assigned to MCU
- FMEDA for MCU => for system-level FMEDA

ASIL D targets
for whole item

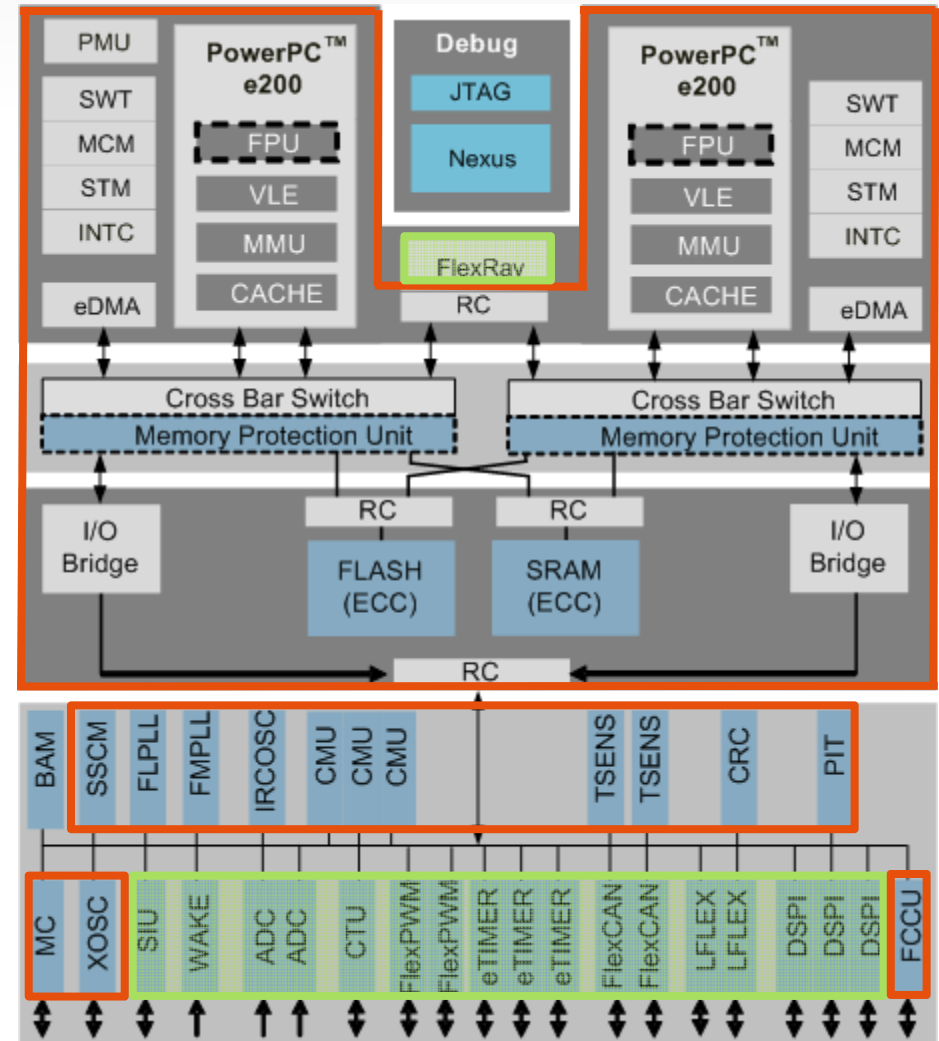
Typical results for
MCU with integr.
safety architecture

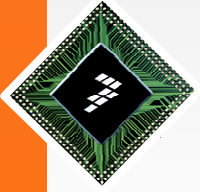




FMEDA Example: MPC5643L

- FMEDA for MPC5643L
 - Processing units (core, etc.)
 - Power supply
 - Clock
 - Non-volatile memory (FLASH)
 - Volatile memory (SRAM)
- Safety concept on system level not known
=> Raw failure rates for
 - Digital I/O
 - Analogue I/O
 - External communication

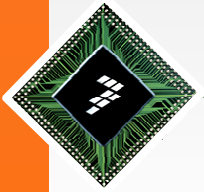




SEooC safety assumption inflexible

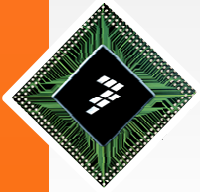
Old SEooC assumption forces system vendors to implement **unnecessary safety measures!**

- ✗ Example: First generation safety application guide for had 68 mandatory requirements



Tailoring SEooC safety assessment

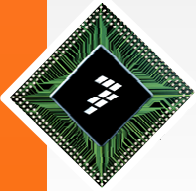
A new approach shall complement the safety measures of a context, not duplicate what the context already provides!



Dynamic FMEDA

Freescale introduces dynamic FMEDA approach:

- Customer communicates implemented safety measures and Freescale delivers respective tailored FMEDA (within e.g. 1 hour)
- E.g. MPC5675K has more than >1 million different FMEDAs in data base – so truly back to the world of general purpose!
- No longer applications have to fulfill FMEDA assumption but FMEDA tailors to application



Flexible FMEDA

Software Functional Self Test Routine for Core supported by Hardware periodically executed within Fault Tolerant Time Interval	Lockstep enabled SSCML_STATUS [LSM] = 1	Safety Relevant Core 2 Usage SSCML_STATUS[LSM] = 0	Temporal Core and DMA Redundancy (recalculate on same core or double move with same DMA)	Window and Logical Monitoring Watchdog implemented and detecting failure within Fault Tolerant Time Interval	MPU Enabled MPU_RGDx	MMU Enabled TLBOCFG, ...
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-9
$\lambda_{total_ISO26262}$:	1,38E-07 h ⁻¹	
$\lambda_{total_IEC61508}$:	1,38E-07 h ⁻¹	

FSL QM Products - Typical Deliverables

- ## ISO 26262 or IEC 61508 Products – Typical Deliverables

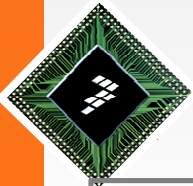
- ## Local Support

- # Learning

- Field Training / workshops – delivered by Local Functional Safety FAE Experts

The magnifying glass highlights the following content in the table:

Safety Support		Safety Process	Safety Hardware	Safety Support
Safety FMEA Safety Application Note	Target Applications	ISO 26262 ASIL D	Integrated Safety Architecture e.g. Multicore Deterministic, 32/64 ECC, replicated peripherals, LBST & MBST, FCCU	Dynamic FMEA Safety Manual
	Target Applications	ISO 26262 ASIL D	Integrated Safety Architecture e.g. Dual core, lockstep or dual parallel processing, replicated peripherals, LBST & MBST, FCCU	Dynamic FMEA Safety Manual
	Target Applications	FR, OM	Integrated Safety Architecture e.g. Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	FMEA Safety Application Note
	Target Applications	ISO 26262 ASIL D	Integrated Safety Architecture e.g. Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	Dynamic FMEA Safety Manual System Level Application Note
FMEDA Safety Manual (T) ISO 26262 compliance evidence	Target Applications	FR, OM	Single core, ASRC/ED ECC Clock Monitoring Unit, Low Voltage Detector, FCCU	FMEDA Safety Application Note
	Target Applications	FR, OM	4x PSR Node Safing Block	Safety FMEA
	Target Applications	FR, OM	CR22 safety bus Triggered self test, Over-damped MEMS	FTA
	Target Applications	FR, OM	SPW safety bus Triggered self test, Over-damped MEMS	FTA
Industrial	Target Applications	FR, OM	SPW safety bus Triggered self test, Over-damped MEMS	FTA
	Target Applications	ISO 26262 ASIL D	Integrated Safety Architecture e.g. Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU	Today, same as Automotive Equivalent products



Safety Support – Dynamic FMEDA

Objective

- Tailor FMEDA to match application configuration
- Enables customers, by supporting their system level architectural choices

Content

- FMEDA methods aligned with functional safety standards
 - SPFM & LFM, PMFH – ISO 26262
 - SFF & PFH- IEC 61508 ed-2.0
 - β_{ic} – IEC 61508 ed-2.0 part 2, Annex E
- Dynamic FMEDA covers elements with low application dependency: Clock, Power Supply, Flash, STM, SRAM, Processing Unit...

Work flow and result

- Customer specifies the Safety Integrity Level required by their application, and then confirms the Safety Measures that will be used
- A tailored FMEDA is then supplied to customer's for their specific application

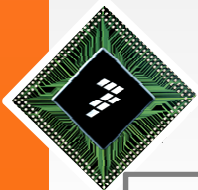
Temperature Profiles to calculate equivalent "average" temperature operation in hot climate				
time	temperature		Logic Gate	SEL
t_{exposure} in h	T_{reactor}	T_{ambient} in °C	failure acceleration GATE	failure acceleration
0 h	-30 °C	-40 through -20	4.01E-07	1.84E-02
80 h	-10 °C	-20 through 0	5.57E-06	3.75E-02
400 h	20 °C	0 through 40	1.47E-04	9.12E-02
1000 h	50 °C	40 through 60	2.12E-03	1.88E-01
1400 h	70 °C	60 through 80	9.67E-03	2.84E-01
3000 h	90 °C	80 through 100	9.74E-02	4.10E-01
1700 h	110 °C	100 through 120	1.25E-01	5.69E-01
300 h	130 °C	120 through 140	3.73E-01	7.65E-01
120 h	150 °C	140 through 160	1.00E+00	1.00E+00
0 h	170 °C	160 through 180	2.45E+00	1.28E+00
8000 h	100 °C		7.16%	39.64%
	131 °C			

ASIL D & SIL2 (99%)

Targeted Safety Integrity Level	Software Functional Failures (SFF) - Failures in the code supported by hardware (not including hardware failures)	Lockup - locked up (SFF) - Failures in the code supported by hardware (not including hardware failures)	Gate 2 Single - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)	System/Module - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)	PMU - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)	Software Functional Failures (SFF) - Failures in the code supported by hardware (not including hardware failures)	Embedded Hardware - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)	External Hardware - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)	Other - Single (SFF) - Failures in the code supported by hardware (not including hardware failures)
ASIL D & SIL2 (99%)	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL

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

Metric	Value	Requirement
Single-Point Fault Metric	2.41.89%	ASIL D requires Single-Point Fault Metric < 10%
Latent Fault Metric	2.41.55%	ASIL D requires Latent Fault Metric < 10%
SFF	2.41.89%	ASIL D requires SFF < 10%
$\lambda_{\text{SFF}} + \lambda_{\text{PMU}}$ (ISO 26262), Age (IEC 61508)	0.07E-10 h ⁻¹	ASIL D requires $\lambda_{\text{SFF}} + \lambda_{\text{PMU}}$ < 10%
λ_{PMU} (ISO 26262)	1.41E-09 h ⁻¹	ASIL D requires λ_{PMU} < 10%
λ_{SFF} (ISO 26262)	1.41E-09 h ⁻¹	ASIL D requires λ_{SFF} < 10%



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

- SoC Safety Concept description
- System level assumptions of use (Safety specific usage considerations)
- Pseudo-code or C-Code to simplify adoption of safety application requirements
- FMEDA results
 - Latent Fault Matrix (LFM)
 - Single Point Fault Matrix (SPFM)
 - Probabilistic Metric for random Hardware Failures (PMHF)
- Provisions against Dependent Failures

Safety Manual for MCU Solution

Freescale Semiconductor
Safety Manual

Document Number

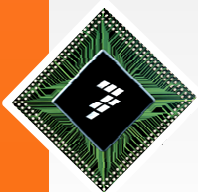
Safety Manual for MPC574xP

Safety Manual for Analog Solution

Freescale Semiconductor
Safety Manual

Document Number: MC33906/7/8
Rev. 1, 4/2012

Safety Manual for MC33906/7/8



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 MC33907/08 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-core 200MHz 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





Summary

- ISO 26262 has been widely adopted for Automotive functional safety
- Systems with safety goals according to ISO 26262 are no longer an exception
- Freescale support OEMs and Tier1s to achieve their ISO 26262 safety goals
 - Discrete and integrated safety architectures
- Combined with a range of Safety HW products, Freescale supports customers by providing A set of differentiating collateral that enable our customers and can significantly reduce their development time
 - Dynamic FMEDA, Safety Manual, System Level Application Notes



www.freescale.com/SafeAssure