



# How to Use Functional Safety Manual and **Dynamic FMECA** to Design Your Safe System

EUF-ACC-T1555

Mathieu Blazy-Winning | Automotive MCU

JULY.2015



External Use

Freescale, the Freescale logo, AllWin, C-S, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C-Ware, the Energy Efficient Solutions logo, Kinetic, MagniV, motorGT, PEG, PowerQUICC, Prosecc Expert, QorIQ, QorIQ Qonverge, Qorivos, Ready Plus, SafeAssure, the SafeAssure logo, StarCore, Synchrify, Vortige, Vybrid and Xilinx are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. AirMat, BeeKit, BeeStack, CoreNet, Flexis, LayerStack, MXC, Platform on a Package, QUICC Engine, SMARTMO25, Tower, TurboLink and UMEMS are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2015 Freescale Semiconductor, Inc.













# Agenda

- Functional Safety at Freescale
- Freescale Development Process for ISO 26262
- MCU Safety Context and Safety Concepts
- Standard Deliverables to Enable the Customer
  - Safety Manual
  - Dynamic FMEDA

# Automotive MCU Product Leadership



Megatrend	Safer Travel 		Electrification Going Green 	Connectivity 	Electrification Emerging Markets 	
Application	Radar (#1**)	Vision (#2**)	Powertrain (#2*)	Gateways (#1*)	General Body and Chassis (#2*)	Actuators and Sensors
						
Key Technology	High perf. ADC and DSP	Image processing	CPU/timer performance and instrumentation	Communication interfaces Security	ARM Cortex Software and Tools	MagniV with HV analog (#1**)
Value Proposition	Highest performance and system integration	Leading image processing AND functional safety	Leading performance architecture	Highest networking bandwidth AND security	Reduce our customers R&D and time-to-market	Reduce system size and manufacturing cost

\*On Revenue, \*\*On Design Wins




# SafeAssure - *Simplification*

- SafeAssure products are conceived to **simplify** system level functional safety **design** and cut down time to **compliance**
- Component safety measures **augment** system level safety measures
- Key functional safety activities addressed
  - Safety analysis (*FMEA, FTA, FMEDA*)
  - Hardware integration (*Safety Manual*)
  - Software integration (*Safety Manual*)
  - Support interface (*Roles & Responsibilities*)



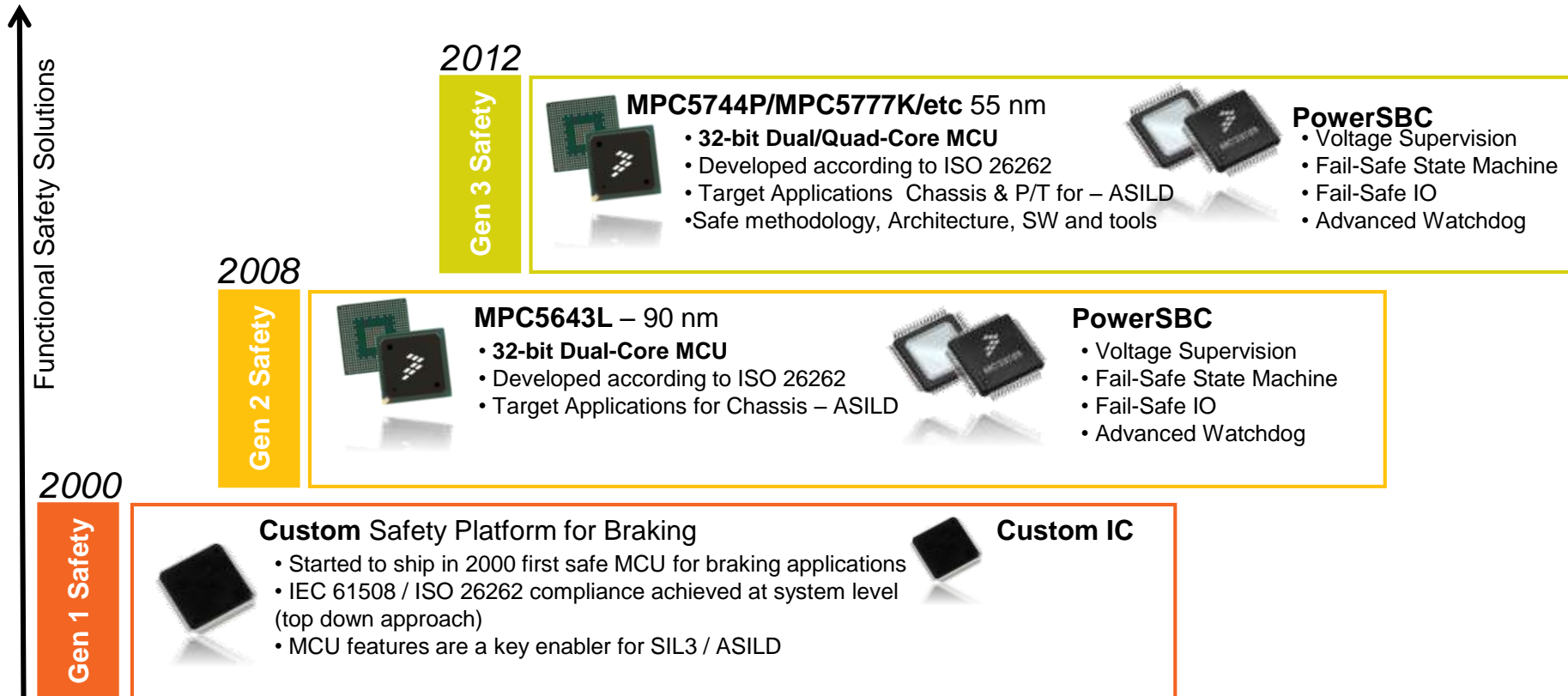
# The World of Functional Safety Standards

	1980	1985	1990	1995	2000	2005	2010	2015
Aeronautic	DO 178 DO 178A		DO 178B ARP 4754	ARP 4761	DO 254		DO 178C ARP 4754A	
Rail Transport				EN 50155	IEC 61508 EN 5012X EN 50159			
Generic Standard IEC61508					IEC 61508		IEC 61508 Ed. 2.0	
Industrial Automation					IEC 61508 IEC 61511 IEC 62061	ISO 13849	IEC 61508 Ed. 2.0	
Automotive					(IEC 61508)		ISO 26262	
Medical							IEC 60601 Ed. 3.0	


 Select Freescale products are being defined and designed from the ground up to comply with ISO 26262 and enabled for IEC 61508 Ed. 2.0 & ISO 13849

# 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



# Freescale Development Process for ISO 26262



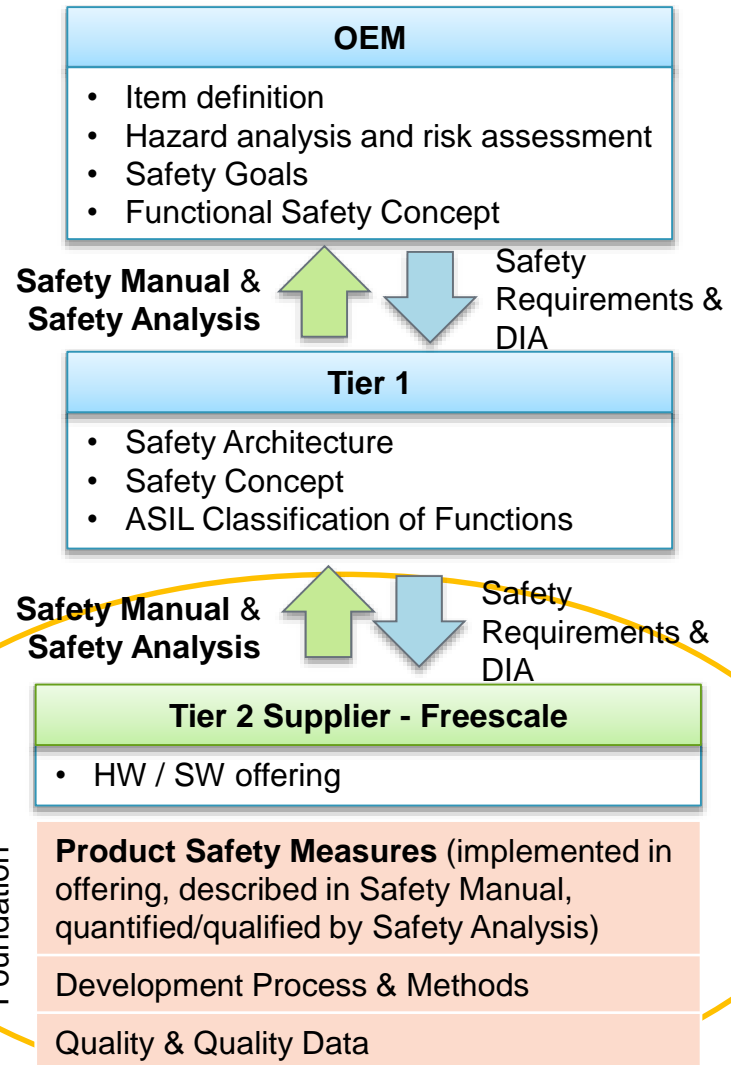
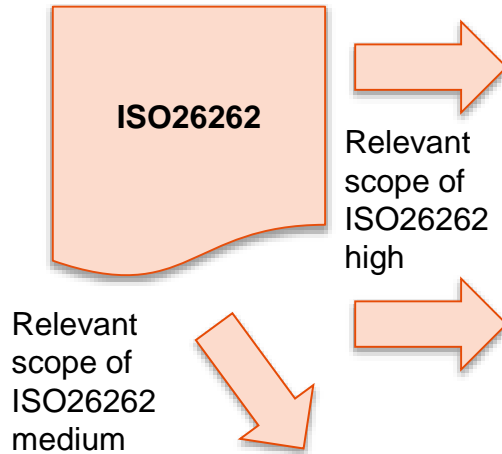
# Freescale Development Process for ISO 26262

- Freescale is **committed** to addressing the requirements of **ISO 26262**
- Freescale MPC564xL is the first MCU to achieve a formal certificate for ISO 26262 ASIL D, as **certified** ([Link](#)) by exida in 2012.
- **Selected products** are developed as a Safety Element out of Context (**SEooC**) where Functional Safety Management and Quality Management are integrated in the development process
- **ISO 26262 Deployment** completed across Freescale during 2011 - 2014
  - Functional Safety Management
  - Development Processes
  - Product Architecture
- **Standard Process**
  - All safety activities and deliverables required by ISO 26262 are integrated in the Freescale Quality Maturity System (QMS), used to plan and track ISO 26262 compliance per product development.



# Example Interaction Between Car OEM, Tier 1 & Tier 2 (Freescale)

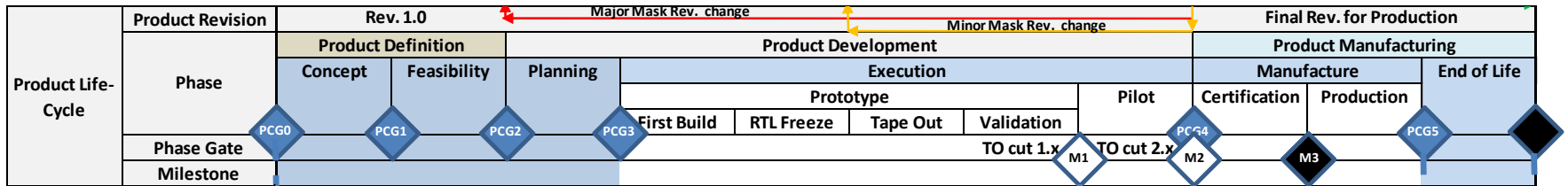
Overall ISO 26262 compliance is achieved together, we each own a piece of the puzzle



**Freescale**  
 Functional Safety Focus  
 Safety Element out of Context



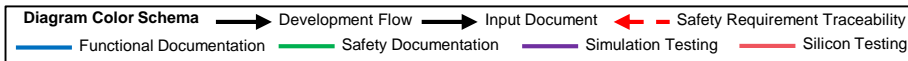
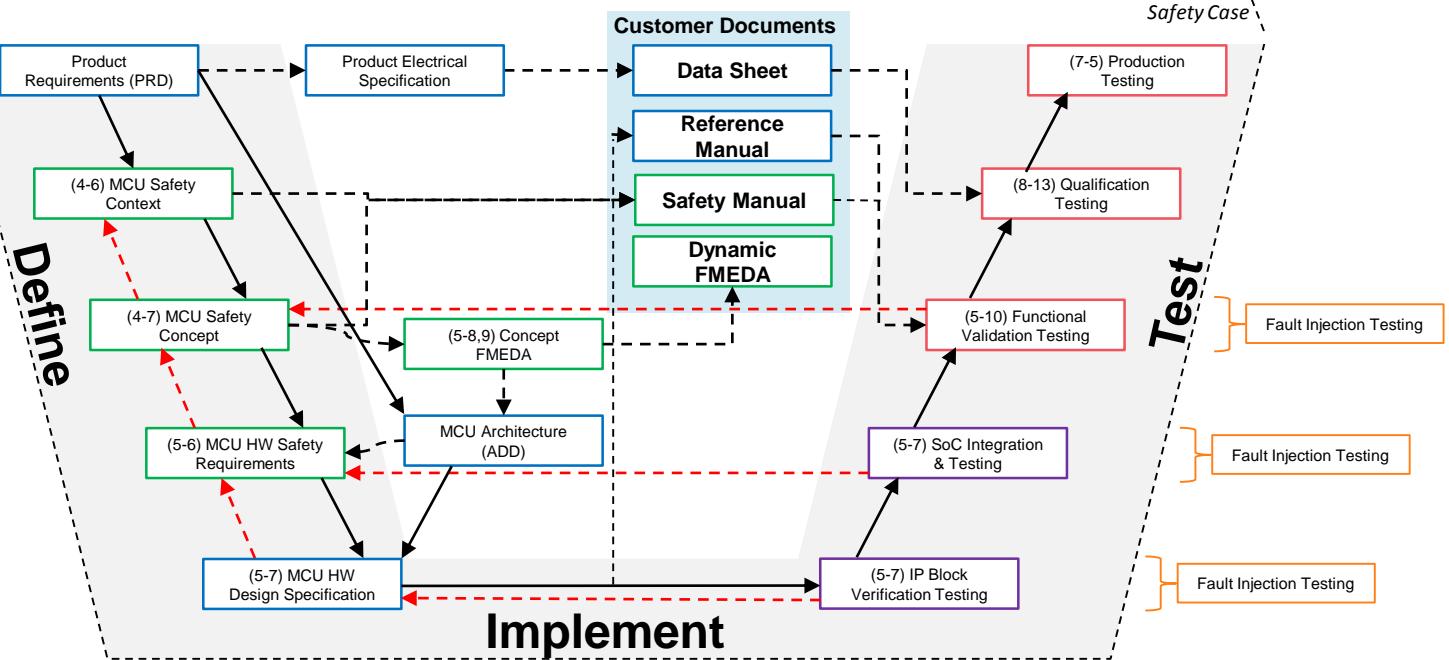
# Functional Safety Process – Definition to Test



Start Lifecycle  
Defining product type  
QM of ISO26262

Alpha Functional Prototypes  
Beta Specification Compliant  
Certified Product  
Start EOL  
EOL

Input Requirements  
Standard  
Customer  
Marketing  
Internal



# Freescale Processes Aligned with ISO 26262

- Freescale standard ISO 26262 process complies with **all** applicable ISO 26262 **ASIL D** requirements for MCU SEooC development

ISO 26262	Freescale Process	ASIL A	ASIL B	ASIL C	ASIL D
<b>Part 2</b> Management	Safety Plan, Safety Case, Confirmation Measures	Yes			
<b>Part 3</b> Concept	<i>OEM / Tier 1 responsibility</i>	NA			
<b>Part 4</b> System	System assumptions & MCU Safety Requirements – HW/SW	Yes, only partially applicable			
<b>Part 5</b> Hardware	MCU HW – Safety requirements traced to implementation and testing	Yes			
<b>Part 6</b> Software	MCU SW – Safety requirements traced to implementation and testing	Yes			
<b>Part 7</b> Production	Standard processes, aligned with ISO 26262	Yes			
<b>Part 8</b> Processes	Standard processes, aligned with ISO 26262	Yes			
<b>Part 9</b> Analysis	FMEDA & DFA	Yes			
<b>Part 10</b> Guideline	MCU SEooC Development & application of ISO 26262 to Microcontrollers	Yes, MCU SEooC development			

- **One process for all products**, regardless of safety architecture ASIL target
- Only **difference** is for Confirmation Measures which are tailored to ASIL target

# Freescale ISO 26262 Confirmation Measures

- Freescale performs ISO 26262 Confirmation Reviews (CR), Audit and Assessment as required by ISO 26262 for MCU SEooC development

Confirmation Measures	ASIL A	ASIL B	ASIL C	ASIL D
CR Safety Analysis	Yes	Yes	Yes	Yes
CR Safety Plan		Yes	Yes	Yes
CR Safety Case		Yes	Yes	Yes
CR Software Tools			Yes	Yes
Audit			Yes	Yes
Assessment			Yes	Yes

- Confirmation Measures (CM) performed depending on ASIL
  - All checks executed with **independence level I3** by Freescale Quality organization
  - Freescale Assessors **certified** by SGS-TÜV Saar as *Automotive Functional Safety Professional (AFSP)*
  - Freescale CM process **certified** ([Link](#)) by SGS-TÜV Saar as ISO 26262 ASIL D
    - Included as part of Freescale Analog & Sensor HW certificate

Note: The following confirmation reviews are not applicable: hazard analysis and risk assessment, item integration and testing, validation plan & proven in use argument

# MCU Safety Context and Safety Concepts



# Hazard Analysis and Risk Assessment (HARA)

- Identify and categorize the hazards that can be triggered by malfunctions in the system
- The Risk Assessment is carried out using three criteria
  - Severity – how much harm is done?

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

- Exposure – how often is it likely to happen?

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

- Controllability – can the hazard be controlled?

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable



# Determination of ASIL and Safety Goals

- For each Hazardous event, determine the ASIL based on Severity, Exposure & Controllability
- Then formulate **safety goals** to prevent or mitigate each event, to avoid unreasonable risk

Table 4 — ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Reference ISO 26262-3:2011

# Target Metrics for ASIL

- Associate the following target metrics to each **safety goal**
  - Single-point fault metric (SPFM)

Table 4 — Possible source for the derivation of the target “single-point fault metric” value

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

- Latent-fault metric (LFM)

Table 5 — Possible source for the derivation of the target “latent-fault metric” value

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

- Probabilistic Metric for random Hardware Failures (PMHF)

Table 6 — Possible source for the derivation of the random hardware failure target values

ASIL	Random hardware failure target values
D	$<10^{-8} \text{ h}^{-1}$
C	$<10^{-7} \text{ h}^{-1}$
B	$<10^{-7} \text{ h}^{-1}$

Reference ISO 26262-5:2011



# Where the Failures Come From

- Typically, dangerous failures in a safety system come from a combination of the following
  - **Development bugs – Software or hardware**
  - **Insufficient system safety architecture**
  - **Transient failures** in semiconductors, primarily **SRAM** – very high rate of occurrence
  - **Permanent failures** in hardware
- For a MCU the break down of Failures is typically:

Failure Type	per hour	FIT	%
MCU SRAM Transient Failure rate	7.00E-07	700	70.00%
MCU FF Transient Failure rate	2.00E-07	200	20.00%
MCU Package Permanent Failure rate	8.00E-08	80	8.00%
MCU Die Permanent Failure rate	2.00E-08	20	2.00%
MCU Total Failure rate	1.00E-06	1000	100%

## Residual Failure rate

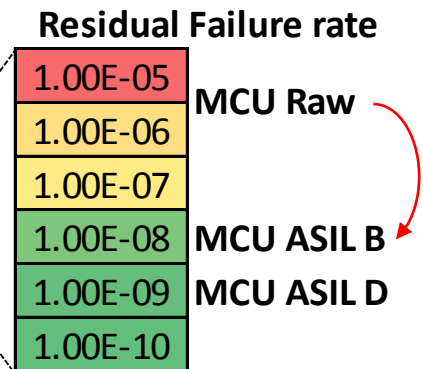
1.00E-05	MCU Raw
1.00E-06	
1.00E-07	
1.00E-08	MCU ASIL B
1.00E-09	MCU ASIL D
1.00E-10	

Note: Assumption - MCU is allocated only 10% of System ASIL target

# MCU Safety Context

- Applications have different safety requirements driven by different safety contexts, but the need for safe SW execution is common across all
- The objective is to make SW execution safe to achieve **ASIL B**

		ASIL B	ASIL D
Detect incorrect operation during runtime	Fault Detection Time Interval	10 ms	
	Diagnostic Coverage (transient & permanent faults)	90%	99%
	Residual Failure rate	$1 \times 10^{-8} / \text{h}$	$1 \times 10^{-9} / \text{h}$
Start-up / Shut-down periodic test	Diagnostic Coverage (permanent faults)	60%	90%
MCU HW to support SW Independence		MPU	



Note: Assumption - MCU is allocated only 10% of System ASIL target

# Defining the MCU Safety Concept

- Objective
  - Define how MCU ASIL targets will be achieved between a mix of on-chip HW safety measures and system level safety measures (HW/SW)
- ISO 26262-5 Annex D – Elements related to MCU
  - Low application dependency: Power, Clock, Flash, SRAM & Processing Unit
  - High application dependency: Digital IO & Analogue IO

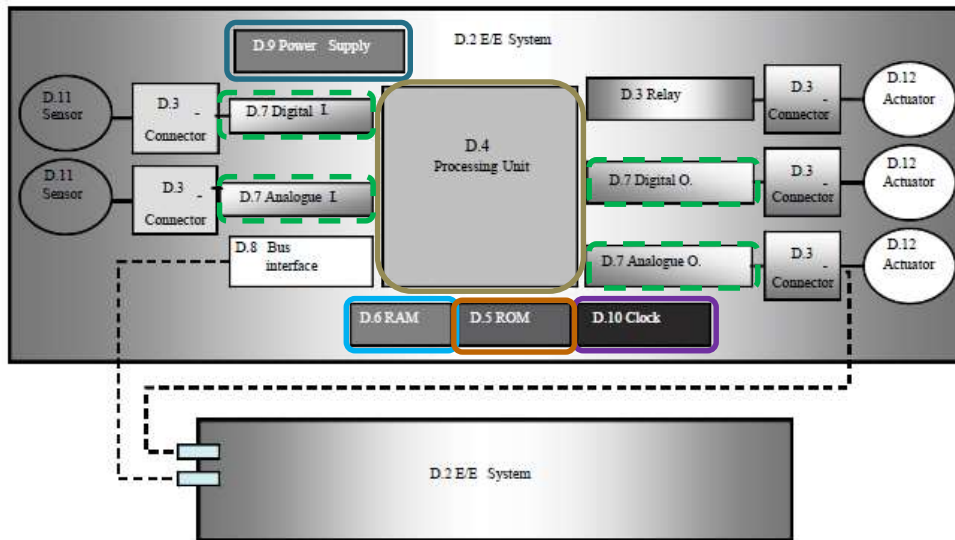


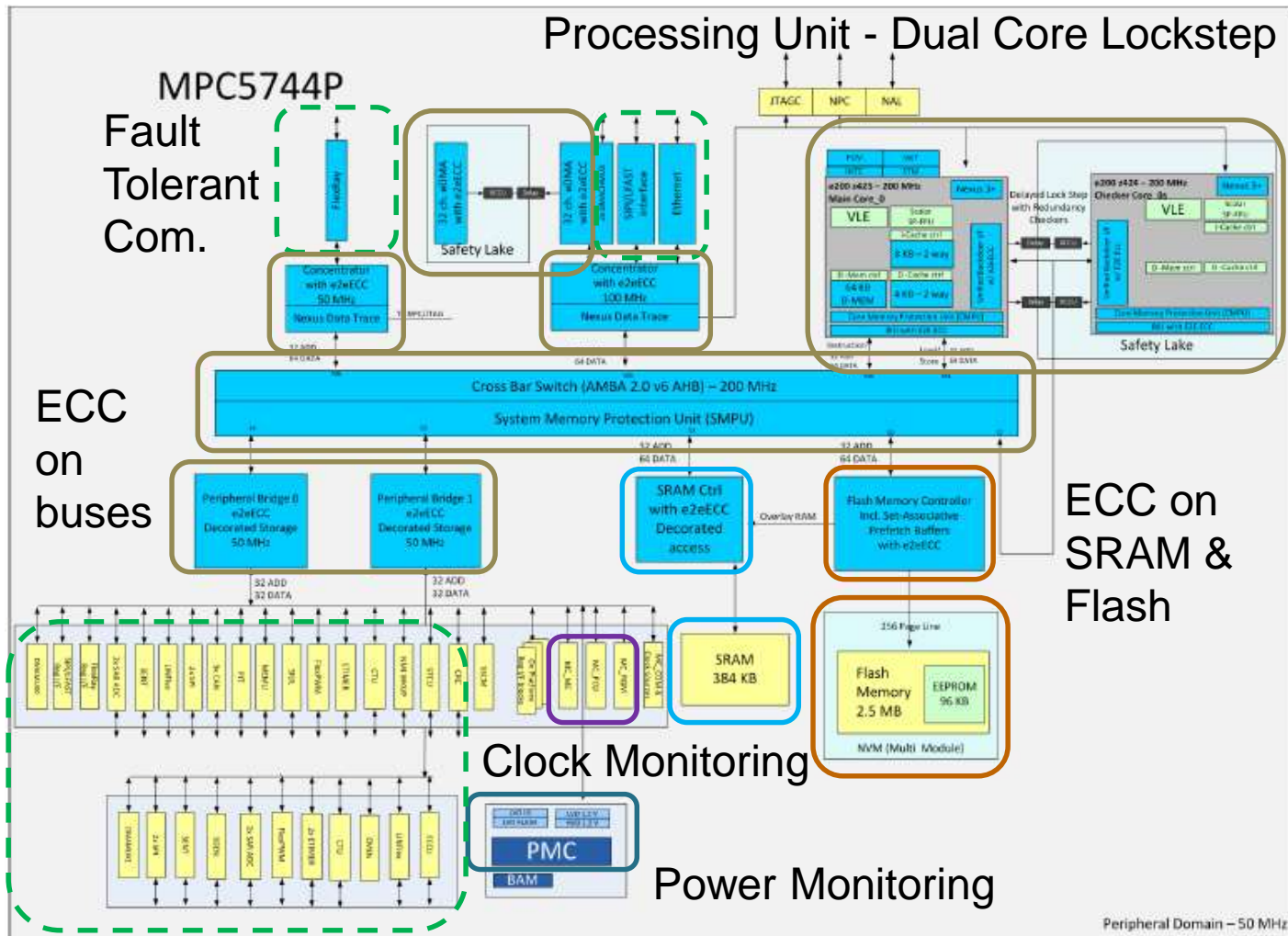
Figure D.1 — Generic hardware of a system Reference ISO 26262-5:2011

# Module Classification - Safety

- Each module on the MCU is classified as Safety Related or Not Safety Related

Elements in ISO 26262-5, Table D.1	MPC5744P FMEDA	MPC5744P Module	Part of Software Execution Function	Safety Mechanism	Comments
Power Supply	Power	Power Management Controller (PMC)	YES		
		Power Control Unit (MC_PCU)	YES		
Clock	Clock	Phase Lock Loop (2 x PLL)	YES		
		Clock Monitor Unit (5 x CMU)		YES	
		Clock Generation Module (MC_CGM)	YES		
		External Oscillator (XOSC)	YES		
		Internal RC Oscillator (IRCOSC)	YES		
Non-Volatile Memory	Flash	Embedded Flash Memory (c55fmc)	YES		
		Flash Memory Controller (PFLASH)	YES		
		End-to-end Error Correction Code (e2eECC)		YES	
Volatile Memory	SRAM	System SRAM	YES		
		RAM Controller (PRAMC)	YES		
		End-to-end Error Correction Code (e2eECC)		YES	
Processing Unit	Core	Main Core_0 (e200z4251n3)	YES		
		Checker Core_0s (e200z424) ( <i>Delayed Lockstep</i> )		YES	
		Crossbar Switch (XBAR)	YES		
		JTAG Controller (JTAGC)			Not Safety Related module - Debug logic
		Nexus debug modules (NXMC, NPC, NAL & NAP)			Not Safety Related module - Debug logic
		Cyclic Redundancy Check (CRC)		YES	
		Fault Collection and Control Unit (FCCU)		YES	
		Memory Error Management Unit (MEMU)		YES	
		Self-Test Control Unit (STCU2) ( <i>includes MBIST &amp; LBIST</i> )		YES	
Register Protection (REG_PROT)		YES			
Communication (External)	Peripheral	CAN (3 x FlexCAN)			Peripheral module - High application dependency (failure rates only)
		Serial Interprocessor Interface (SIPI)			Peripheral module - High application dependency (failure rates only)
		10/100-Mbps Ethernet MAC (ENET)			Peripheral module - High application dependency (failure rates only)
Peripheral Bridge (2 x PBRIDGE)				Peripheral module - High application dependency (failure rates only)	
System Integration Unit Lite2 (SIUL2)				Peripheral module - High application dependency (failure rates only)	
Analog to Digital Converter (4 x ADC)				Peripheral module - High application dependency (failure rates only)	
Analogue I/O and Digital I/O		Wakeup Unit (WKPU)			Peripheral module - High application dependency (failure rates only)

# Realizing the MCU Safety Concept - MPC5744P



Redundant use of IO & Application checks



# Standard Deliverables to Enable the Customer



# What You Get

To support the customer to build his safety system, the following deliverables are provided as **standard** for **all** ISO 26262 developed products.

- **Public Information available via Freescale Website**

- Freescale Quality Certificates ([Link](#))
- Safety Manual
- Reference Manual
- Data Sheet

- **Confidential Information available under NDA**

- Safety Plan
- ISO26262 Safety Case
- ISO26262-10 Table A.8 Checklist
- Permanent Failure Rate data (Die & Package) - IEC/TR 62380 or SN29500
- Transient Failure Rate data (Die) - JEDEC Standard JESD89
- FMEDA & Report
- DFA & Report
- PPAP
- Confirmation Measures Report (summary of all applicable confirmation measures)



# Safety Manual





# Safety Manual

## Objective

- Enables customers to build their safety system using the MCU safety mechanisms and defines system level HW & SW assumptions
- 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

## Content

- MCU Safety Context
- MCU Safety Concept
- System level hardware assumptions
- System level software assumptions
- FMEDA summary
- Dependent Failures Analysis summary

## 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 Manual: Structure



- **MCU Safety Context**
  - Safe states, Fault tolerant time interval
- **MCU Safety Concept**
  - Describes the safety concept of the device (what is implemented and how does it work)
- **System level hardware assumptions**
  - Describes the functions required by external hardware to complement the MCU safety concept (Error out monitor)
- **System level software assumptions**
  - Description of necessary or recommended sw mechanisms for each module (Initial checks, configuration & runtime checks)
- **Failure Rates and FMEDA**
  - Short introduction to FMEDA
- **Dependent Failure Analysis**
  - $\beta$ ic – IEC 61508 Ed. 2.0 part 2, Annex E: Analysis of dependent failures
  - Countermeasures against common cause failures on chip level



# 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 Base 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 Safe-Assure 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 e200e4d 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 (RCU) 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 (PFCU) 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



# Dynamic FMEDA



# 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
  - $\beta$ ic – IEC 61508 Ed. 2.0 part 2, Annex E
- Dynamic FMEDA covers elements with low application dependency: Clock, Power Supply, Flash, SRAM, Processing Unit...

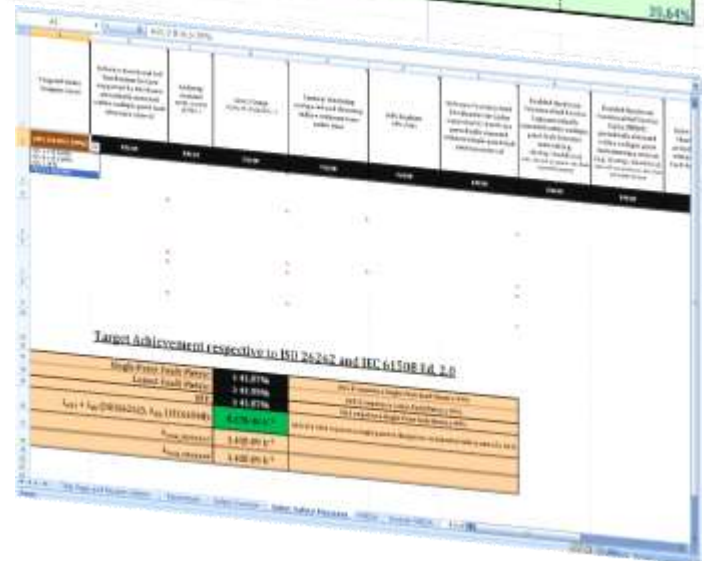
## Work flow and result

- Customer specifies the failure model (dependent on Safety Integrity Level) required by their application, and then confirms the Safety Measures that will be used or not 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 T <sub>average</sub> in h	Temperature		Logic Gate failure acceleration GATE	SIL failure acceleration
	T <sub>max</sub>	T <sub>ambient</sub> in °C		
0 h	-30 °C	-40 through -20	4.03E-07	1.84E-01
80 h	-15 °C	-20 through 0	5.57E-08	5.75E-02
400 h	0 °C	0 through 40	1.47E-04	8.12E-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	3.74E-02	4.10E-01
1700 h	110 °C	100 through 120	1.29E-01	5.89E-01
300 h	130 °C	120 through 140	3.73E-01	7.05E-01
420 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%



# ISO 26262-5 (Elements and Failure Models)

Table D.1 — Analyzed faults or failures modes in the derivation of diagnostic coverage

Element	See Tables	Analyzed failure modes for 60 %/90 %/99 % DC		
		Low (60 %)	Medium (90 %)	High (99 %)
<b>General semiconductor elements</b>				
Power supply	D.9	Under and over Voltage	Drift Under and over Voltage	Drift and oscillation Under and over Voltage Power spikes
Clock	D.10	Stuck-at <sup>a</sup>	d.c. fault model <sup>b</sup>	d.c. fault model <sup>b</sup> Incorrect frequency Period jitter
Non-volatile memory	D.5	Stuck-at <sup>a</sup> for data and addresses and control interface, lines and logic	d.c. fault model <sup>b</sup> for data and addresses (includes address lines within same block) and control interface, lines and logic	d.c. fault model <sup>b</sup> for data, addresses (includes address lines within same block) and control interface, lines and logic
Volatile memory	D.6	Stuck-at <sup>a</sup> for data, addresses and control interface, lines and logic	d.c. fault model <sup>b</sup> for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model <sup>c</sup> for bit cells	d.c. fault model <sup>b</sup> for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model <sup>c</sup> for bit cells
Digital I/O	D.7	Stuck-at <sup>a</sup> (including signal lines outside of the microcontroller)	d.c. fault model <sup>b</sup> (including signal lines outside of the microcontroller)	d.c. fault model <sup>b</sup> (including signal lines outside of the microcontroller) Drift and oscillation
Analogue I/O		Stuck-at <sup>a</sup> (including signal lines outside of the microcontroller)	d.c. fault model <sup>b</sup> (including signal lines outside of the microcontroller) Drift and oscillation	d.c. fault model <sup>b</sup> (including signal lines outside of the microcontroller) Drift and oscillation

FMEDA Supply

FMEDA Clock

FMEDA Flash

FMEDA SRAM

Failure Rate Table



# ISO 26262-5 (Elements and Failure Models)

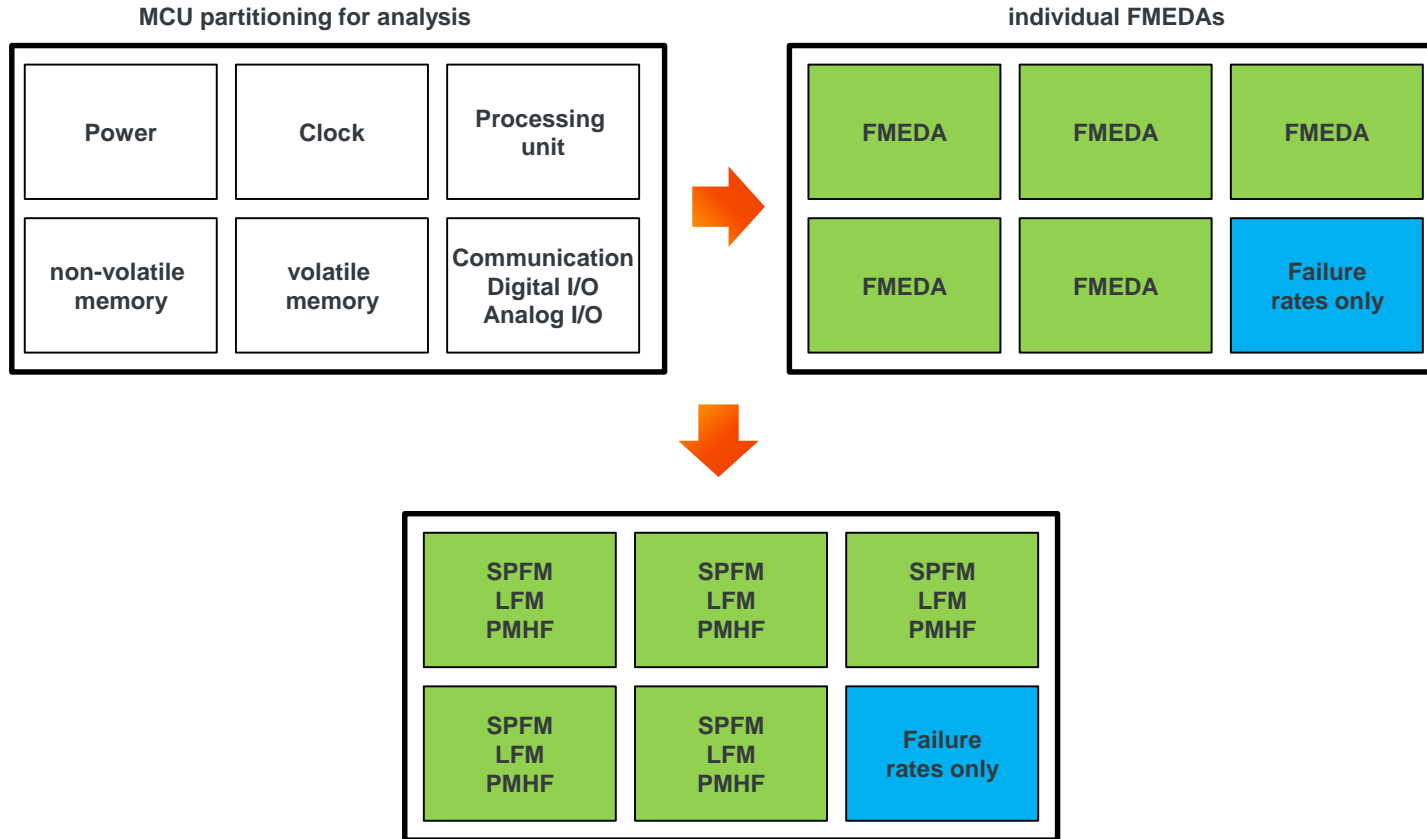
Table D.1 — Analyzed faults or failures modes in the derivation of diagnostic coverage

Element	See Tables	Analyzed failure modes for 60 %/90 %/99 % DC			
		Low (60 %)	Medium (90 %)	High (99 %)	
<i>Specific semiconductor elements</i>					
Processing units	ALU - Data Path	D.4/D.13	Stuck-at <sup>a</sup>	Stuck-at <sup>a</sup> at gate level d.c. fault model <sup>b</sup> Soft error model <sup>c</sup> (for sequential parts)	
	Registers (general purpose registers bank, DMA transfer registers...), internal RAM	D.4	Stuck-at <sup>a</sup>	Stuck-at <sup>a</sup> at gate level Soft error model <sup>c</sup> d.c. fault model <sup>b</sup> including no, wrong or multiple addressing of registers Soft error model <sup>c</sup>	
	Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	D.4/D.5/D.6	Stuck-at <sup>a</sup>	Stuck-at <sup>a</sup> at gate level Soft error model <sup>c</sup> (for sequential parts)	d.c. fault model <sup>b</sup> including no, wrong or multiple addressing Soft error model <sup>c</sup> (for sequential parts)
	Interrupt handling	D.4/D.10	Omission of or continuous interrupts	Omission of or continuous interrupts Incorrect interrupt executed	Omission of or continuous interrupts Incorrect interrupt executed Wrong priority Slow or interfered interrupt handling causing missed or delayed interrupts service
	Control logic (Sequencer, coding and execution logic including flag registers and stack control)	D.4/D.10	No code execution Execution too slow Stack overflow/underflow	Wrong coding or no execution Execution too slow Stack overflow/underflow	Wrong coding, wrong or no execution Execution out of order Execution too fast or too slow Stack overflow/underflow
	Configuration Registers	D.4	—	Stuck-at <sup>a</sup> wrong value	Corruption of registers (soft errors) Stuck-at <sup>a</sup> fault model
	Other sub-elements not belonging to previous classes	D.4/D.13	Stuck-at <sup>a</sup>	Stuck-at <sup>a</sup> at gate level	d.c. fault model <sup>b</sup> Soft error model <sup>c</sup> (for sequential part)

FMEDA  
Processing  
Unit



# Dynamic FMEDA Metrics



- FMEDAs must **individually** fulfill the target relative metrics (SPFM, LFM)
- **Sum** of individual PMHF must fulfill the absolute target



# Dynamic FMEDA

- Failure Mode, Effect and Diagnostic Analysis
- A systematic way to **identify** and **evaluate failure modes**, **effects** and **diagnostic techniques**, and to **document** the system.
- FMEDA can be **tailored** to **application** use-case:
  - FMEDA allows adaptation of temperature profile and ASIL level
  - FMEDA allows selection of package used
  - FMEDA allows selection / de-selection of modules
  - FMEDA allows selection / de-selection of diagnostic measures
  - FMEDA allows to change particular DCs

**Called “Dynamic FMEDA”**

- FMEDA can generate a specific (static) “**customer FMEDA**”

# Dynamic 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 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), $\lambda_{DU}$ (IEC61508):	2,18E-10 h <sup>-1</sup>	ASIL D & SIL3 requires a single point or dangerous undetected failure rate of ≤ 1E-8
$\lambda_{total\_ISO26262}$ :	1,38E-07 h <sup>-1</sup>	
$\lambda_{total\_IEC61508}$ :	1,38E-07 h <sup>-1</sup>	

## 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

# Supporting Material for Functional Safety

- SafeAssure @ [www.freescale.com/SafeAssure](http://www.freescale.com/SafeAssure)
- Certification Package under NDA
- App-Notes, White Papers, Articles
- On-demand Training





[www.Freescale.com](http://www.Freescale.com)