FTF FREESCALE TECHNOLOGY FORUM 2014

Functional Safety Compliance Throughout the Vehicle with SafeAssure Solutions

FTF-AUT-F0009

Richard Soja | Automotive MCU Systems Engineer

APR.2014

freescale™

External Use

Freescale, the Freescale logo, AltiVec, C-5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C-Ware, the Energy Efficient Solutions logo, Kinetis, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, Qorivva, SafeAssure, the SafeAssure logo, StarCore, Symphony and VortiQa are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. Airfast, BeeKit, BeeStack, CoreNet, Flexis, Layerscape, MagniV, MXC, Platform in a Package, QorIQ Qonverge, QUICC Engine, Ready Play, SMARTMOS, Tower, TurboLink, UMEMS, Vybrid and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2014 Freescale Semiconductor, Inc.

Agenda

- Functional Safety at Freescale
- Functional Safety and Microcontrollers
- MCU Safety Context and Safety Concepts
- Dynamic FMEDA
- Safety Manual

Microcontrollers and Digital Networking Processors

>50 Year Legacy

>5,500 Engineers

>6,100 Patent Families

Five Core Product Groups	**Four** Primary Markets
Microcontrollers	Automotive
Digital Networking	Networking
Automotive MCU	Industrial
Analog	Consumer
RF	

Several Platforms Key to Making the World a Healthier, Safer Place

Health & Safety

Automotive

- Active Safety Systems
- Advanced Driver Assistance
- Radar, Vision Systems
- Functional Safety

Industrial

- Connected Home
- Portable Medical
- Factory Automation Systems

SAFE ASSURE™ by Freescale

We See a Healthier, Safer Population

Functional Safety. Simplified.

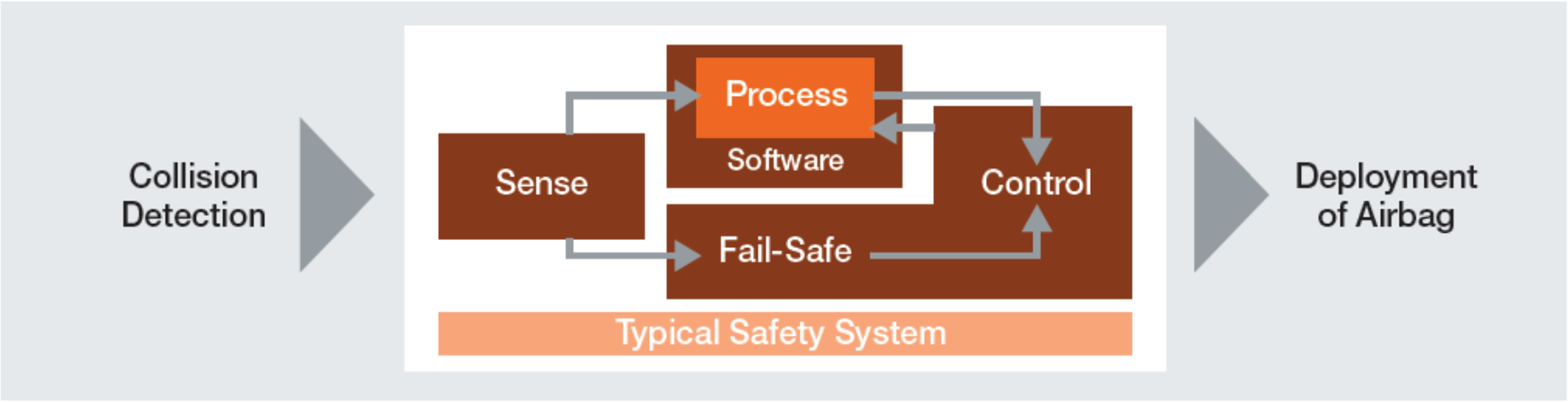
- **Simplifies the process** of system compliance, with solutions designed to address the requirements of automotive and industrial functional safety standards
- **Reduces the time and complexity** required to develop safety systems that comply with ISO 26262 and IEC 61508 standards
- **Supports the most stringent Safety Integrity Levels** (SILs),enabling designers to build with confidence
- **Zero defect methodology** from design to manufacturing to help ensure our products meet the stringent demands of safety applications

SAFE ASSURE™ by Freescale

The Right Technology Partner

Sensors		MCUs	Analog		
Hi-Aspect Ratio SOI MEMS	SiGe Radar	Embedded Control	Hi-Performance Analog	Power Management	Connectivity

Freescale is uniquely developing the end-to-end integrated system solutions.



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)*

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

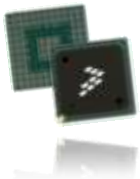
Gen 3 Safety

MPC5744P/MPC5777K/etc 55 nm
- **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
- Voltage Supervision
- Fail-Safe State Machine
- Fail-Safe IO
- Advanced Watchdog

2008

Gen 2 Safety



MPC5643L – 90 nm
- **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

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**, applied **development** & **production processes** against requirements and work products of ISO 26262 applicable to a MCU
- **MPC5643L MCU certified for use for all Automotive Safety Integrity Levels (ASIL), up to and including the most stringent level, ASIL D**

The manufacturer may use the mark:

exida CERTIFIED ISO 26262 ASIL D

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

exida CERTIFICATION

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 µC 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 µC 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

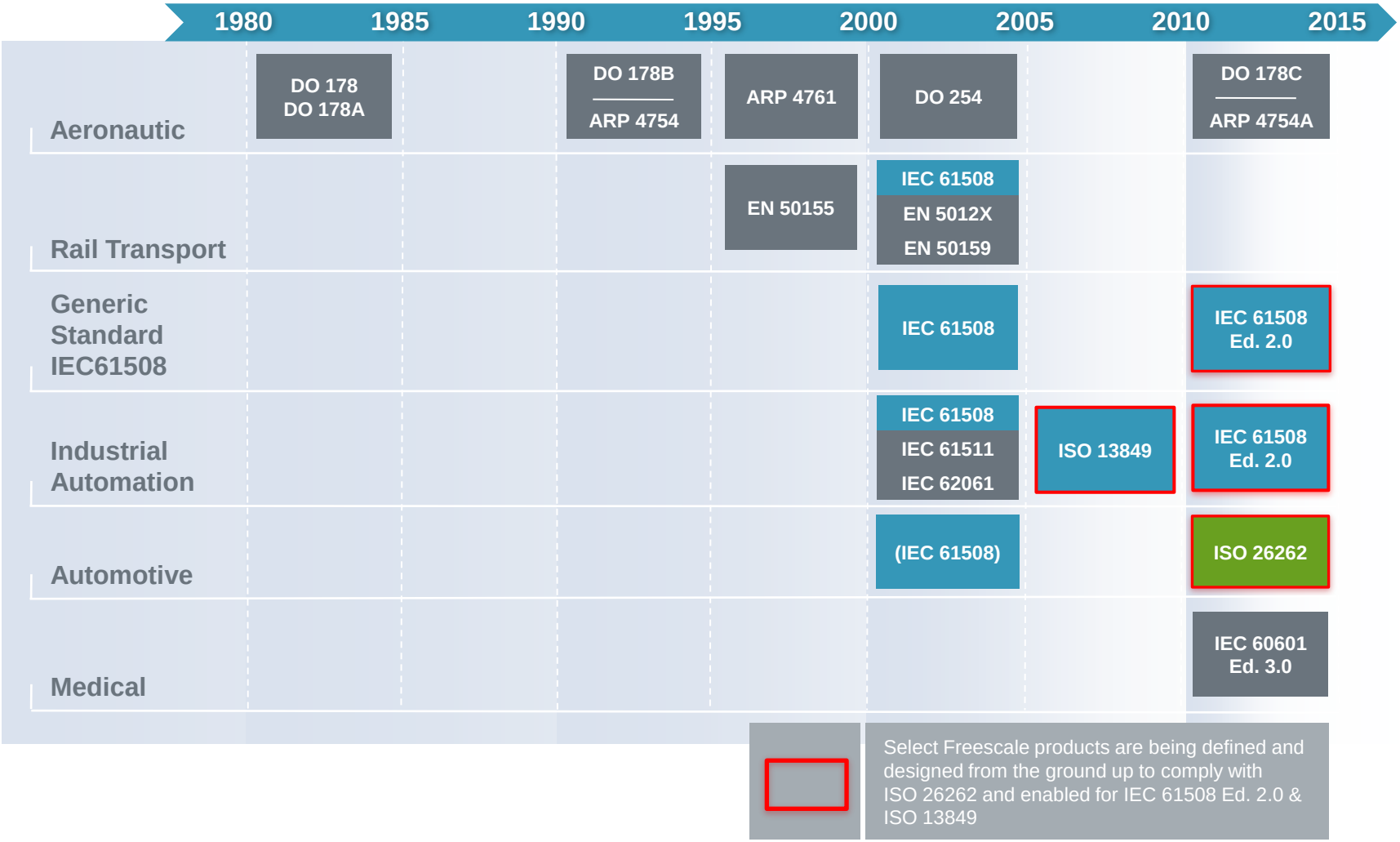
Certifying Assessor

Page 1 of 2

Agenda

- Functional Safety at Freescale
- Functional Safety and Microcontrollers
- MCU Safety Context and Safety Concepts
- Dynamic FMEDA
- Safety Manual

The World of Functional Safety Standards



Comparison of Functional Safety Standards

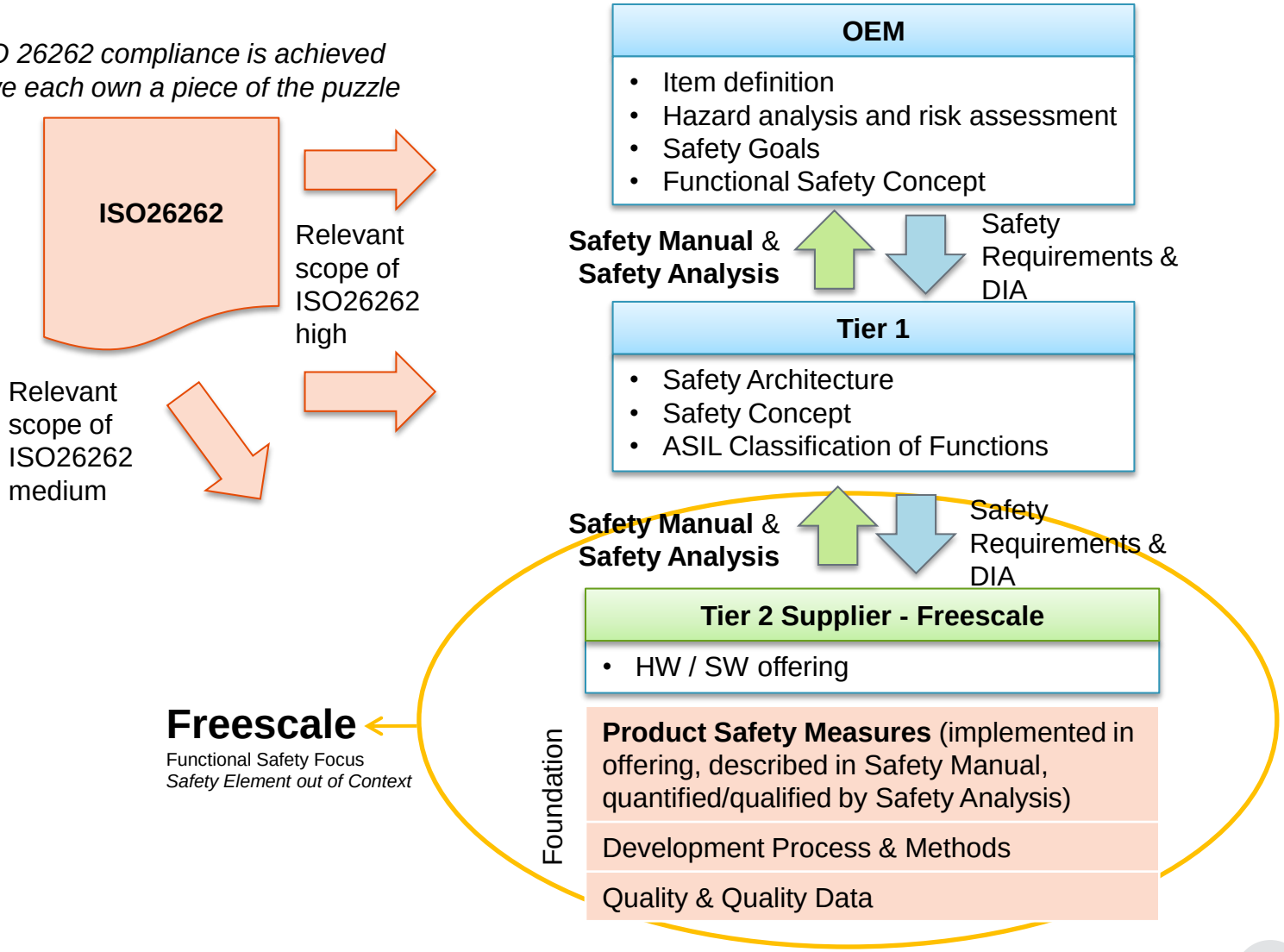
Functional Safety *is the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical / electronic systems*

ISO 26262	IEC 61508	ISO 13849
Automotive Industry standard, adaptation of IEC 61508 for electrical / electronic systems within **road vehicles**	**Generic** Industry standard, applicable to electrical / electronic / programmable electronic **safety-related** systems.	**One** of two European Standards to achieve compliance with the **Machinery Directive** 2206/42/EC
Safety Integrity Levels	**Safety Integrity Levels**	**Performance Levels**
ASIL A, ASILB, ASIL C, ASIL D	SIL 1, SIL 2, SIL 3, SIL 4	a, b, c, d, e
Publication date	**Publication date**	**Categories**
15 Nov 2011	Ed. 2.0 – Apr 2010	B, 1, 2, 3, 4
	Ed. 1.0 - More than 10 years ago	

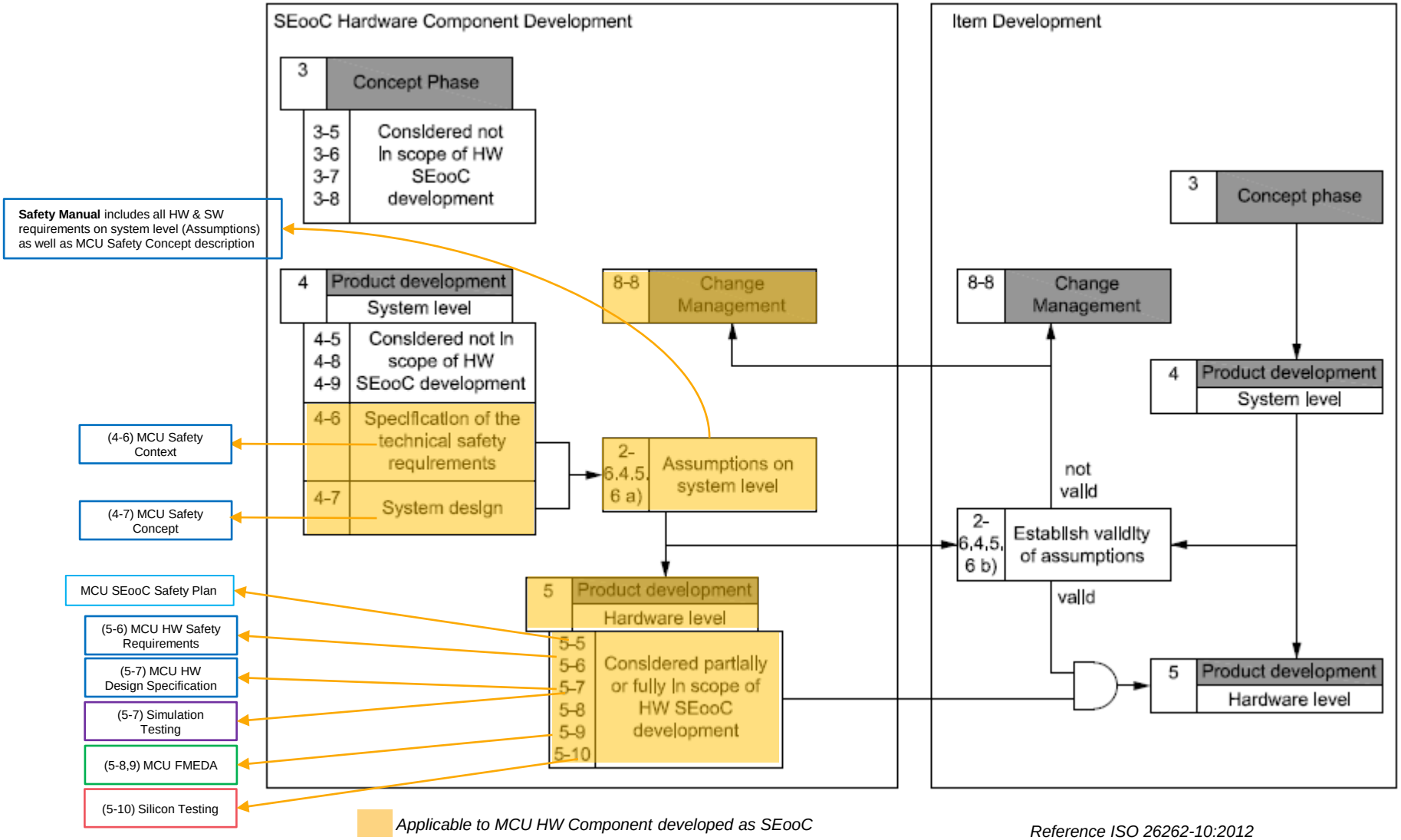
Freescale is strengthening its product development cycle, making functional safety an integral part of the process.

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



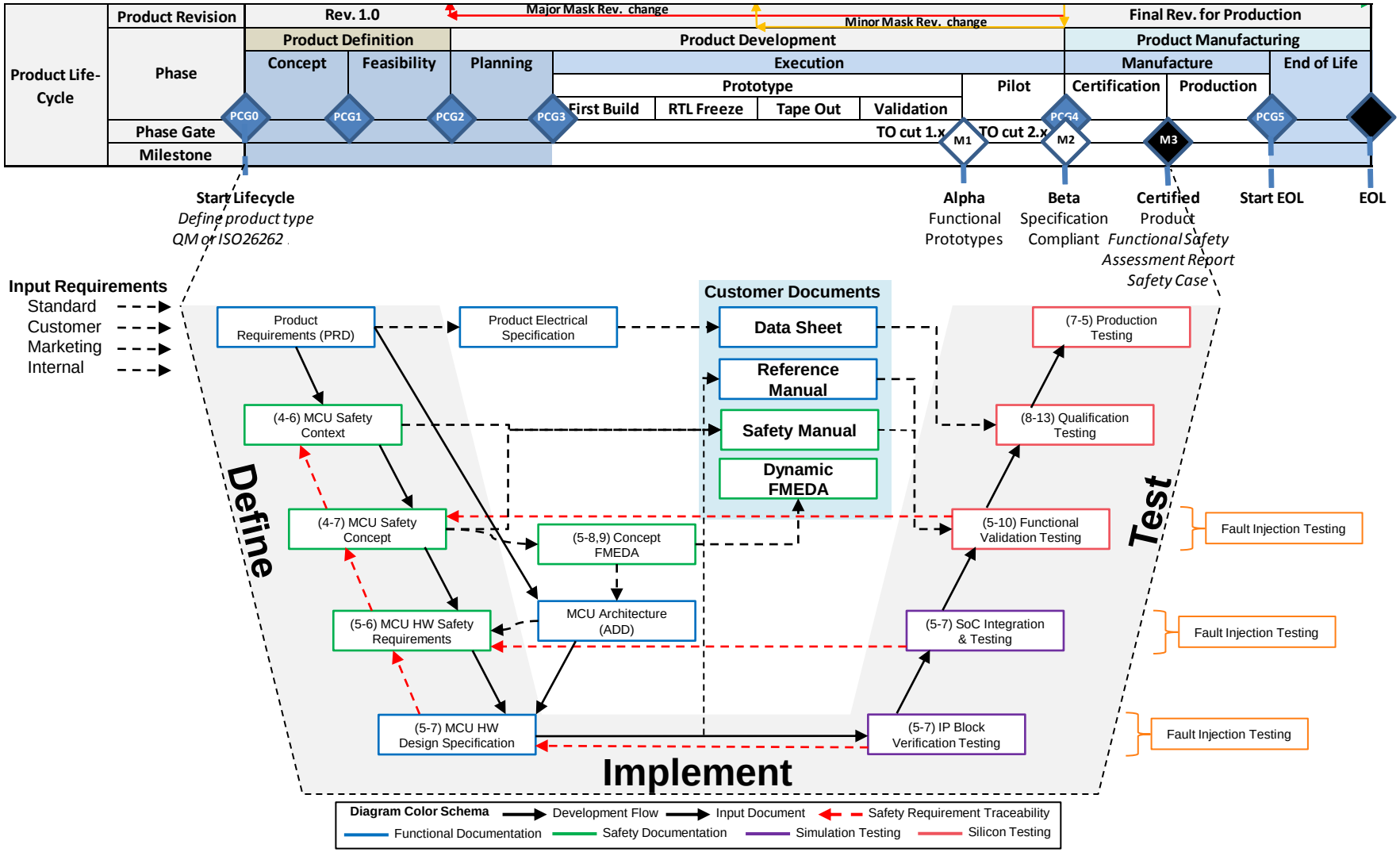
MCU HW Component Developed as SEooC



Applicable to MCU HW Component developed as SEooC

Reference ISO 26262-10:2012

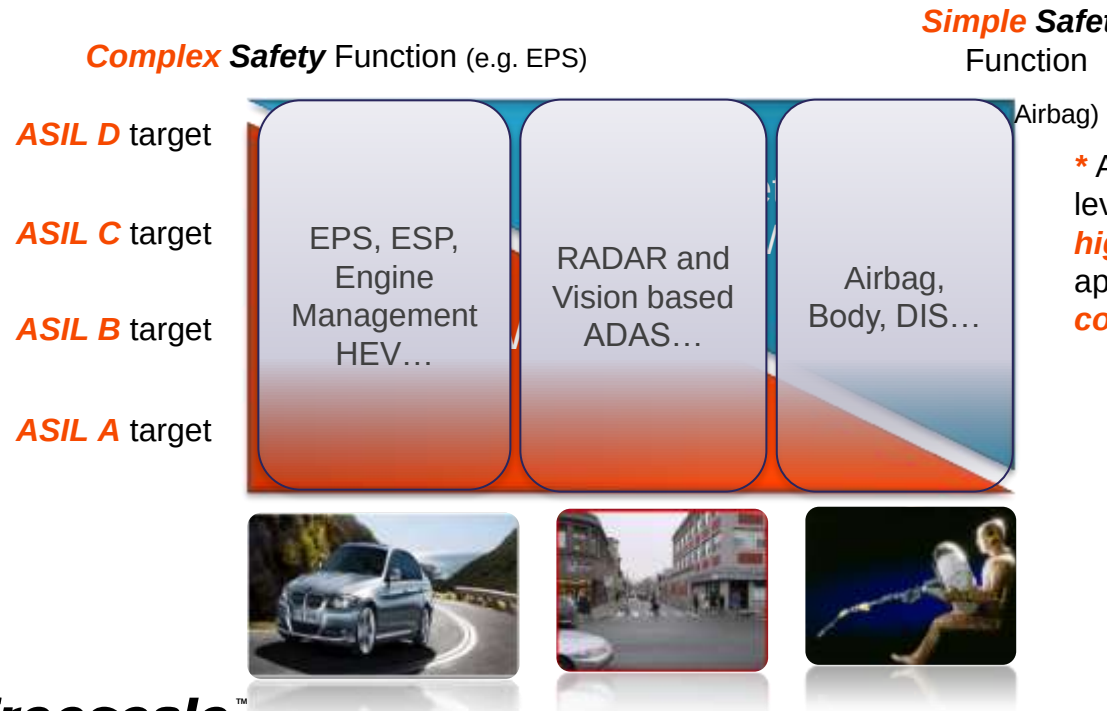
Functional Safety Process – Definition to Test



Know Your Safety System Context

How to make the system safe?

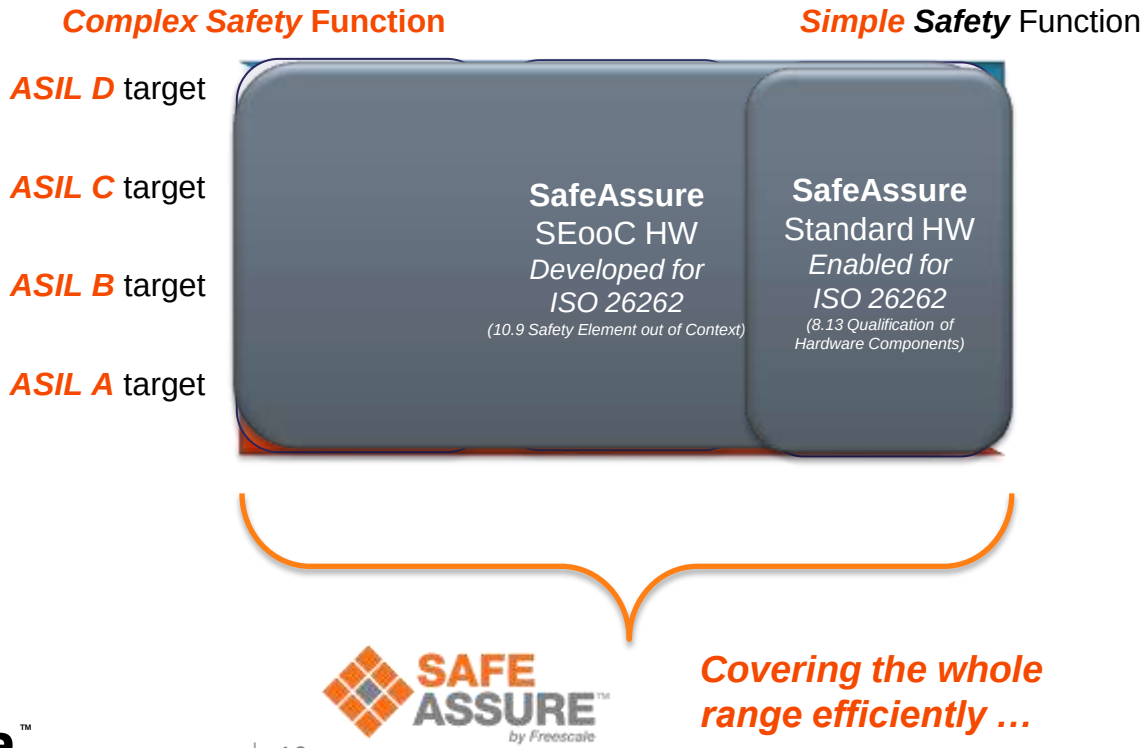
- Optimal partitioning between Safety System HW & SW measures scaled to complexity of vehicle safety function
  - ***Simple Safety*** Functions are implemented on a high abstraction level (vehicle & ECU)
  - ***Complex* Safety*** Functions are implemented using a combination of low (MCU HW) and high abstraction level (vehicle & ECU)



* A ***Complex Safety*** Function (vehicle level) here refers to the combination of a ***high computational*** demand for the application combined with a ***short control cycle***.

The Solution

- Offering **products scaled** to vehicle **safety function complexity** from across the Freescale product portfolio
  - **ISO 26262** developed products cover the complete range
  - **Standard** products cover systems with simple safety functions
    - Where we enable the customer to do the Qualification, testing and analysis to prove that our component is suitable for the purpose of his safety concept.



SafeAssure Product Types

- The SafeAssure program includes two main categories of product (in terms of Functional Safety):
  - **Products developed according to ISO 26262**
  - **Products enabled for functional safety;** e.g. additional collateral has been created to assist a customer when using a product within their system (which needs to meet a functional safety standard)

Criteria	Products enabled for functional safety	Products developed according to ISO 26262
What does the development process address?	addresses **quality** at component level. Functional safety is addressed at **system** level	addresses **quality** & **functional safety** at **component** level
Deliverables available to customers		
Safety Analysis of Architecture	Safety FMEA or FTA	FMEDA, CCF or FTA
User Guide	Safety Application Note	Safety Manual
Software	QM software, e.g. AUTOSAR OS and MCAL, Self Test Software, Complex Drivers	Software developed to ISO 26262, e.g. AUTOSAR MCAL, Self Test Software
Production readiness evidence:	PPAP	Functional Safety Assessment, PPAP

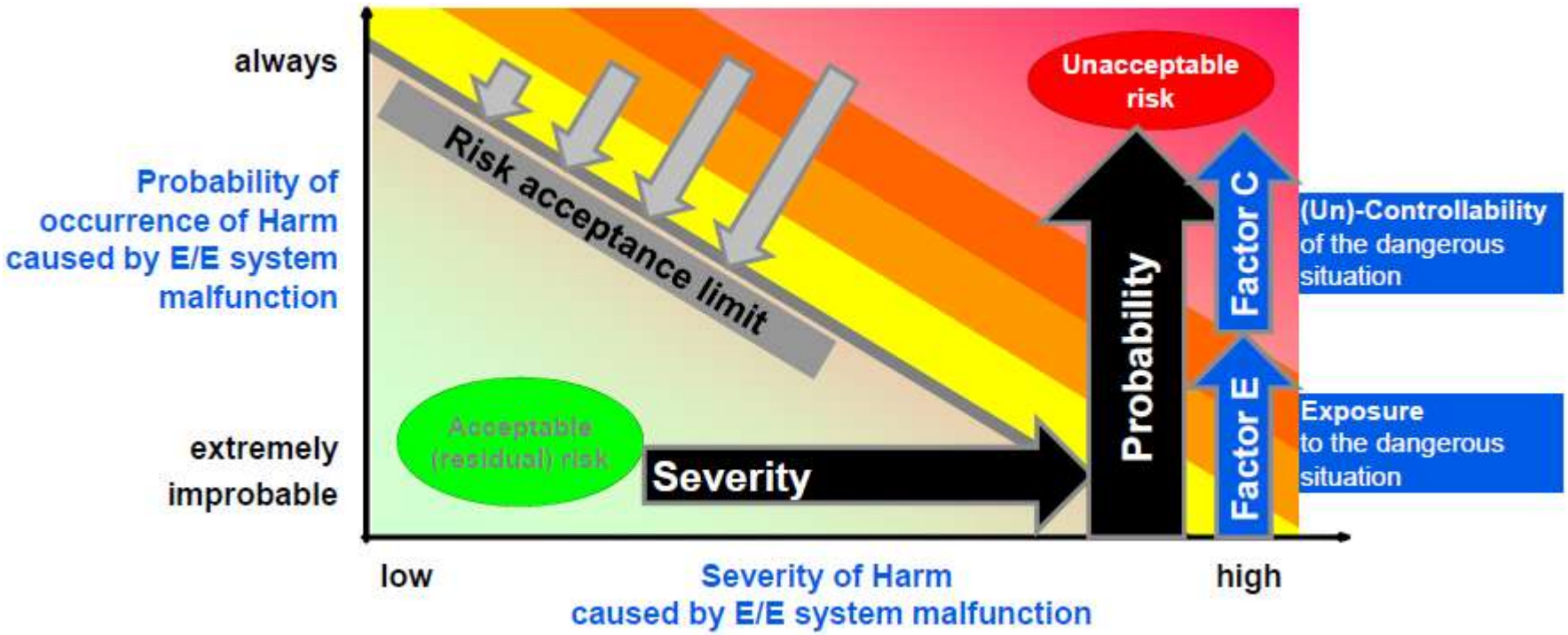
SafeAssure Products

Product Type	Product	Target Applications	Safety Process	Safety Hardware	Safety Support
MCU	MPC5746M	Diesel Engine Management Direct Injection Engines Electronically Controlled Transmissions Gasoline Engine Management	ISO 26262	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	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	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 PSI5 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	Integrated Safety Architecture e.g.: Independant 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	Integrated Safety Architecture	Safety Manual, FMEDA System Level Application Note
	MC33908	Integrated Chassis Domain Safety critical motor control applications	ISO 26262	Integrated Safety Architecture	Safety Manual, FMEDA System Level Application Note
	MC33789	PSI5 Airbag System	FSL QM	4x PSI5 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	PSI5 Airbag System	FSL QM	PSI5 safety bus, Triggered self test, Over-damped MEMS	FTA
	MMA65xx MMA68xx	PSI5 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

Agenda

- Functional Safety at Freescale
- Functional Safety and Microcontrollers
- MCU Safety Context and Safety Concepts
- Dynamic FMEDA
- Safety Manual

Functional Safety – Risk definition



Reference TÜV SAAR Training Module K3

Risk: Combination of the probability and extent of damage

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	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$

Reference ISO 26262-5:2011

Defining the MCU Safety Concept

- Objective
  - Define MCU ASIL derived from system level assumptions
- Application Assumptions
  - Safety Goals
    - Associated “mini” HARA, ASIL
  - Fault Tolerant Time Interval (FTTI / L-FTTI)
  - System Safe State

- MCU Assumptions
  - MCU Safety Functions
    - Associated ASIL from safety goal
  - Portion of FTTI
    - % of safety goal
  - Define portion of ASIL target allocated to each safety function
    - % of safety goal
  - MCU Safe State
    - Compatible with System Safe State

Example – EPS System

- Application Context
  - **Safety Goal 1** (SG1): The EPS does not apply unintended force to the steering system (**ASIL D**).
    - Hazard: Unintended steering assist
    - Risk Assessment
  - S3: Life threatening injuries (survival uncertain), fatal injuries
  - E4: High probability
  - C3: Difficult to control or uncontrollable

- MCU Assumptions
  - **Safety Function 1** (SF1): Execute software instructions, process data, write back result (**ASIL D**) -> mapped to SG1
  - Portion of FTTI: 10 ms
    - 50% of SG1 FTTI for HW safety measures
  - Define portion of ASIL target allocated to each safety function
    - **SPFM: 99%, LFM: 90%, PMHF: 10^{-10} hour^{-1}** (1% of safety goal ASIL target)
  - MCU Safe State (fail safe, fail indicate)
    - Reset, indicating an error

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 & Analog IO

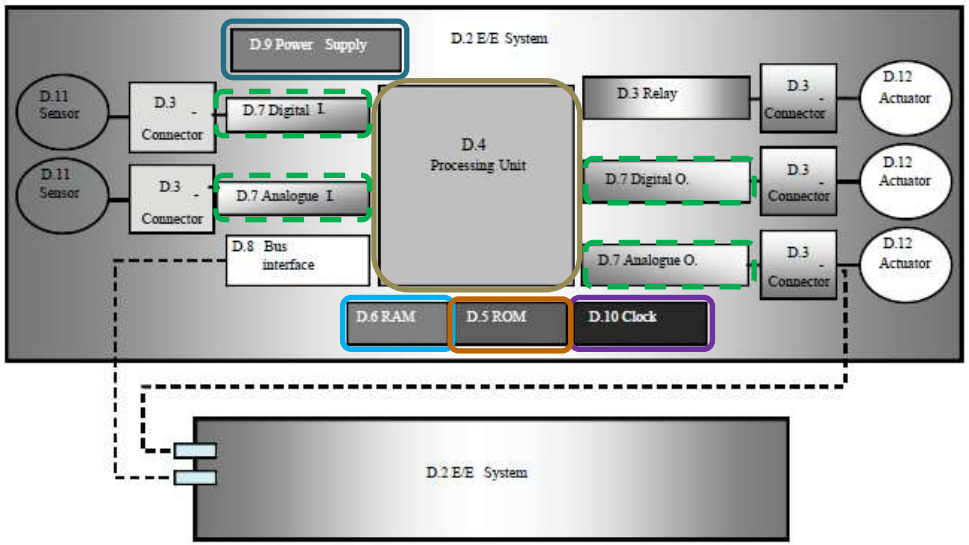


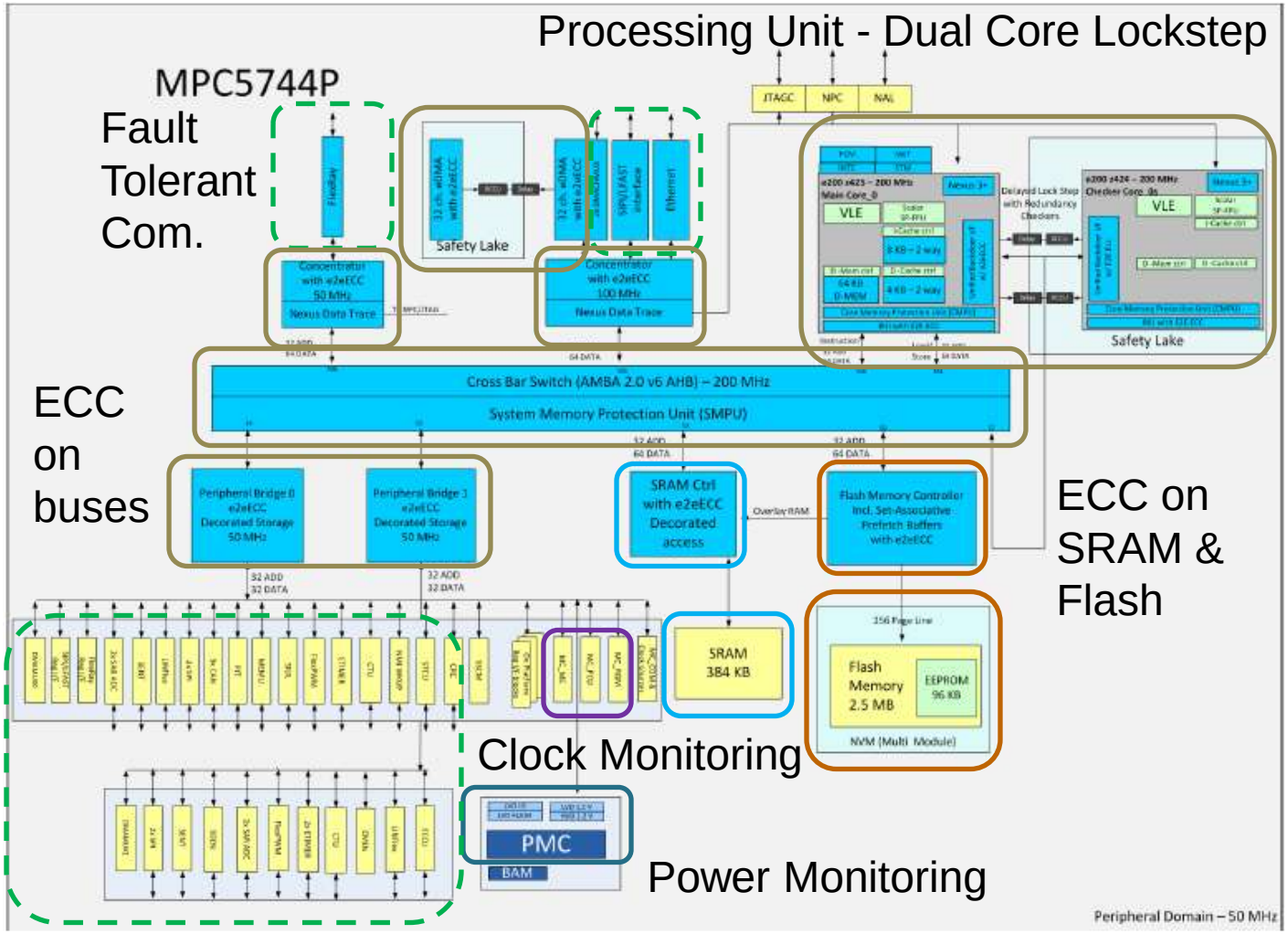
Figure D.1 — Generic hardware of a system *Reference ISO 26262-5:2011*

MCU Module Classification

Category	Module	SF1	SF2	SF3	SF4	PRL	HSM	NSR
Core and system modules	Main Core_0	x	x					
	Checker Core_0x						x	
	SUL2	x	x					
	XBAR	x	x					
	XBIC						x	
	AIPS-Lite					x		
	SMPU	x	x					
	MTC	x	x					
	eDMA	x	x					
	DMAMUX	x	x					
	EIM						x	
Memories and memory controllers	SRAM	x	x					
	Flash	x	x					
	eFlexECC						x	
	PRAMC	x	x					
	PFLASH	x	x					
	Flash OTP	x	x					
	DSMC	x	x					
Power management modules	PMC	x	x					
	MC_PCU	x	x					
	MC_ME	x	x					
Clocking modules	PLLDIG	x	x					
	CMU						x	
	MC_CGM	x	x					
	XOSC	x	x					
	RCOSC	x	x					

Realizing the MCU Safety Concept – Qorivva MPC5744P

Redundant use of IO & Application checks

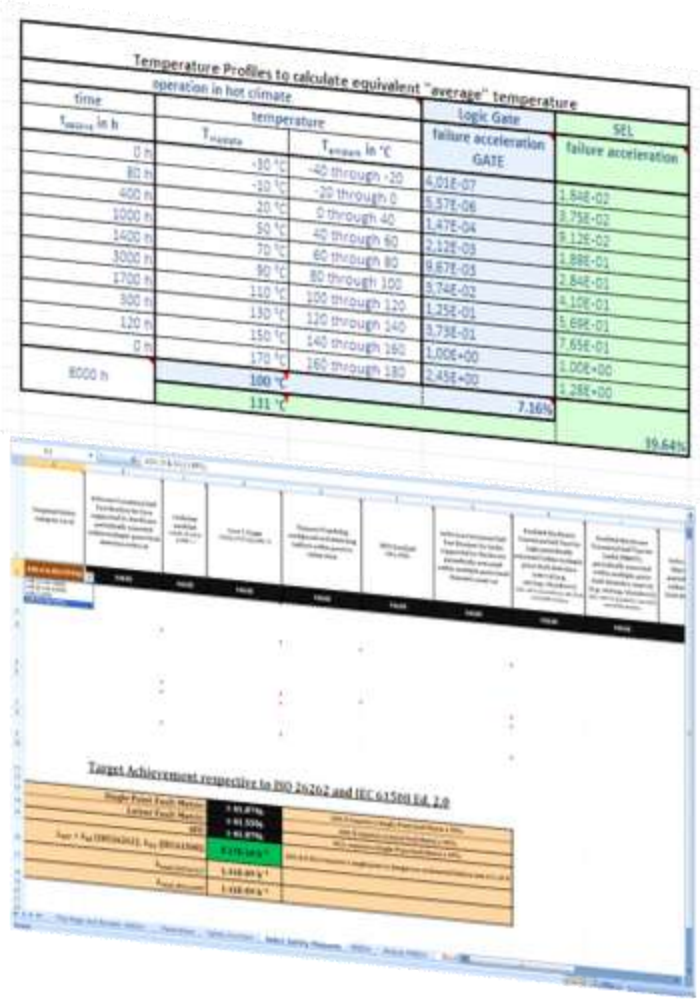


Agenda

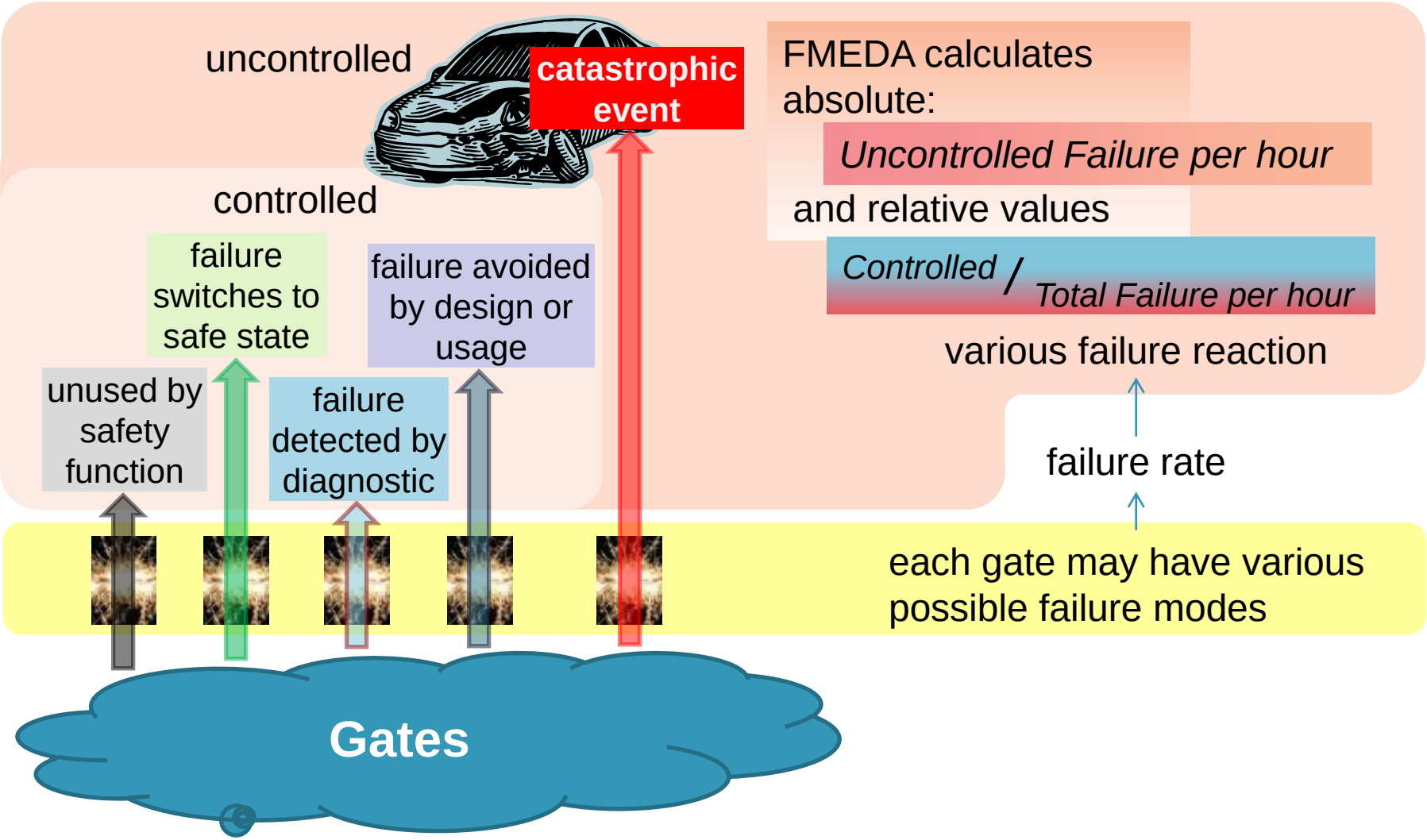
- Functional Safety at Freescale
- Functional Safety and Microcontrollers
- MCU Safety Context and Safety Concepts
- Dynamic FMEDA
- Safety Manual

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
    - βic – 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



What is an FMEDA?



How to setup FMEDA - Template

Approach used in FMEDA Template

DC assessed by engineering judgment or analytic calculation

Diagnostic covera measure

Diagnostic coverage measures 2

Diagnostic verage asures 3

Diagnostic coverage measures 4

apply for each failure model of an element typical diagnostic coverage

failure models listed in ISO26262-5 Table D.1

apply for each element typical failure modes

elements listed in ISO26262-5 Table D.1

divide circuitry in elements

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 %)
General semiconductor elements				
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[a]	d.c. fault model[b]	d.c. fault model[b] Incorrect frequency Period jitter
Non-volatile memory	D.5	Stuck-at[a] for data and addresses and control interface, lines and logic	d.c. fault model[b] for data and addresses (includes address lines within same block) and control interface, lines and logic	d.c. fault model[b] for data, addresses (includes address lines within same block) and control interface, lines and logic
Volatile memory	D.6	Stuck-at[a] for data, addresses and control interface, lines and logic	d.c. fault model[b] for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model[c] for bit cells	d.c. fault model[b] for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model[c] for bit cells
Digital I/O	D.7	Stuck-at[a] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation
Analogue I/O	D.7	Stuck-at[a] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation

FMEDA Supply

FMEDA Clock

FMEDA Flash

FMEDA SRAM

Failure Rate Table

Reference ISO 26262-5:2011

ISO 26262-5 (Elements and Failure Models)

FMEDA
Processing Unit

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 %)
	Specific semiconductor elements				
Processing units	ALU - Data Path	D.4/D.13	Stuck-at[a]	Stuck-at[a] at gate level	d.c. fault model[b] Soft error model[c] (for sequential parts)
Processing units	Registers (general purpose registers bank, DMA transfer registers…), internal RAM	D.4	Stuck-at[a]	Stuck-at[a] at gate level Soft error model[c]	d.c. fault model[b] including no, wrong or multiple addressing of registers Soft error model[c]
Processing units	Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	D.4/D.5/D.6	Stuck-at[a]	Stuck-at[a] at gate level Soft error model[c] (for sequential parts)	d.c. fault model[b] including no, wrong or multiple addressing Soft error model[c] (for sequential parts)
Processing units	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
Processing units	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
Processing units	Configuration Registers	D.4	—	Stuck-at[a] wrong value	Corruption of registers (soft errors) Stuck-at[a] fault model
Processing units	Other sub-elements not belonging to previous classes	D.4/D.13	Stuck-at[a]	Stuck-at[a] at gate level	d.c. fault model[b] Soft error model[c] (for sequential part)

Reference ISO 26262-5:2011

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**

Called "Dynamic 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}	

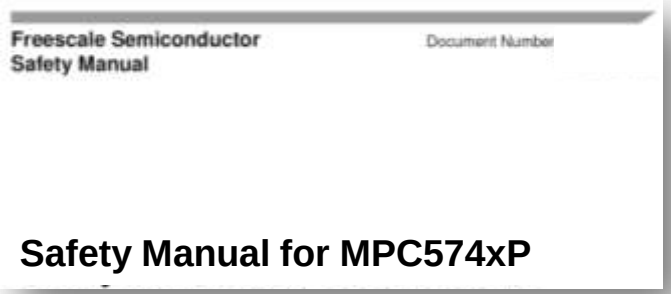
Agenda

- Functional Safety at Freescale
- Functional Safety and Microcontrollers
- MCU Safety Context and Safety Concepts
- Dynamic FMEDA
- Safety Manual

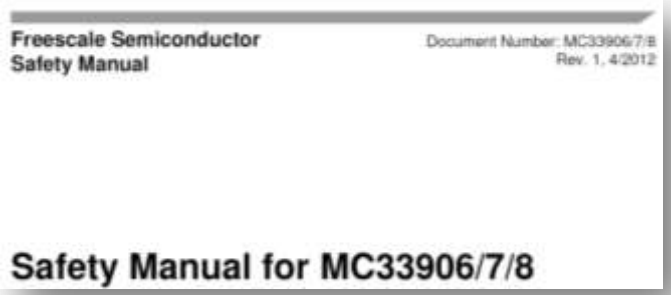
Safety Support – Safety Manual

- 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 Manual: Structure (1)

- **Preface & General Information**
  - Safe states, Fault tolerant time interval
- **Functional Safety Concept**
  - Customer should understand the safety concept of the device (what is implemented and how does it work together)
- **Hardware Requirements on System Level**
  - Description of all required (and optional) functions by external hardware to achieve the safety goal(s) on system level
- **Software Requirements on System Level**
  - Description of necessary or recommended sw mechanisms for each module
  - For each relevant module
    - Initial checks and configurations
    - Runtime checks

Safety Manual: Structure (2)

- **Failure Rates and FMEDA**
  - Short introduction and link to FMEDA

- **Dependent Failure Analysis (qualitative)**
  - βic – IEC 61508 Ed. 2.0 part 2, Annex E: Analysis of dependent failures
  - Countermeasures against common cause failures on chip level
  - Restrictions caused by countermeasures (e.g. peripheral usage)
  - Confidence-building measure

- **Code-examples / Pseudocode**
  - Give a more rigorous description of the SW interactions
  - Code fragments and examples (not intended for direct use)
  - Enable customer to develop safety SW as intended

Safety Specific Usage Considerations (1)

- **Assumption:**
  - An assumption being relevant for functional safety in the specific application under consideration. It is assumed that the user fulfills an assumption in his design.
- **Assumption under certain preconditions:**
  - An assumption being relevant under certain preconditions.
- **Recommendation:**
  - A recommendation is either a proposal for the implementation of a requirement, or a reasonable mechanism which is recommended to be applied if there is no requirement in place. The user has the choice whether or not to follow the recommendation.
- **Rationale:**
  - The motivation for a specific requirement and/or recommendation.
- **Implementation hint:**
  - Specific hints on the implementation of a requirement and/or recommendation. The user has the choice whether or not to follow it.

Safety Specific Usage Considerations (2)

- System integration: every requirement considered?
- Unique identifiers aid tracing of requirements, e.g.
  - Format: **[SM_*xxx*]** It is assumed that …. **[end]**

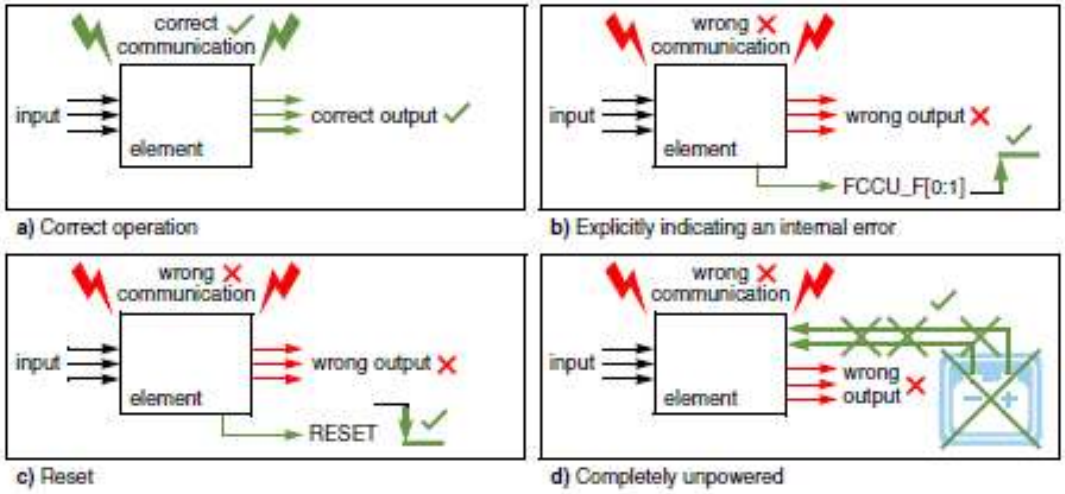


Figure 2-1. Safe state$_{MCU}$ of the MPC5643L

Assumption: [SM_086] It is assumed that the system transitions itself to a Safe state$_{system}$ when the MPC5643L explicitly indicates an internal error via its error out signal(s) (FCCU_F[0:1]).[end]

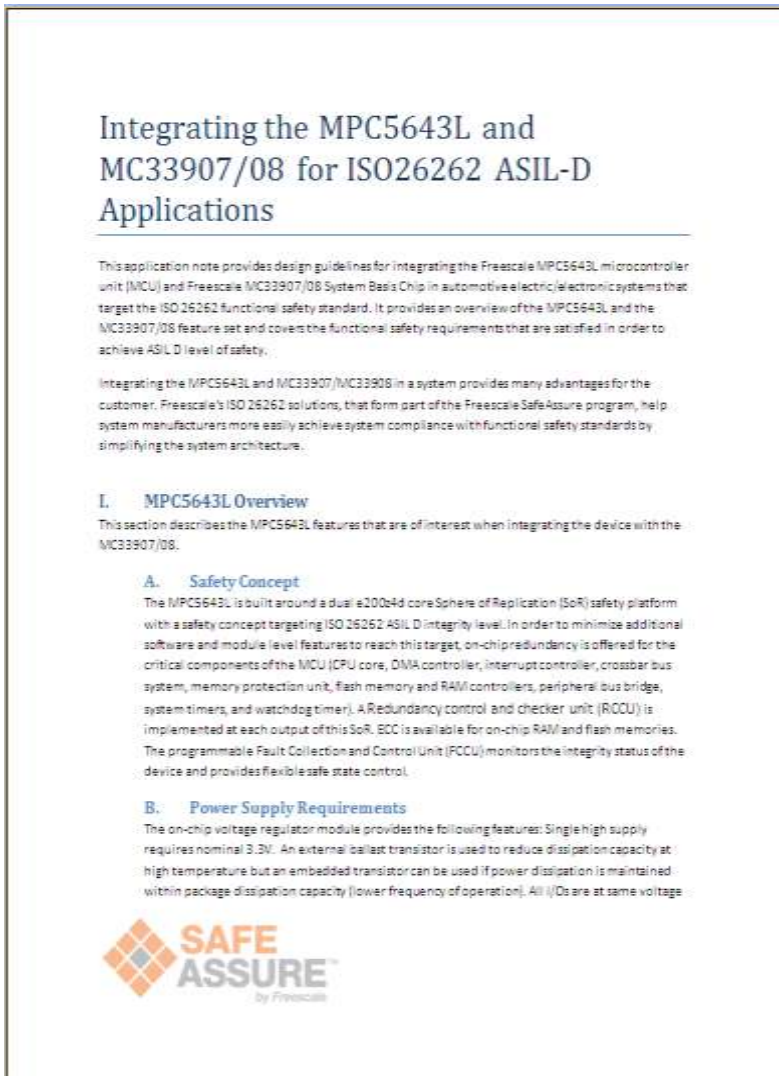
Assumption: [SM_703] It is assumed that the system transitions itself to a Safe state$_{system}$ when the MPC5643L is in reset state.[end]

Assumption: [SM_704] It is assumed that the system transitions itself to a Safe state$_{system}$ when the MPC5643L is completely unpowered.[end]

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 by Freescale

SafeAssure MCU Product – Qorivva 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

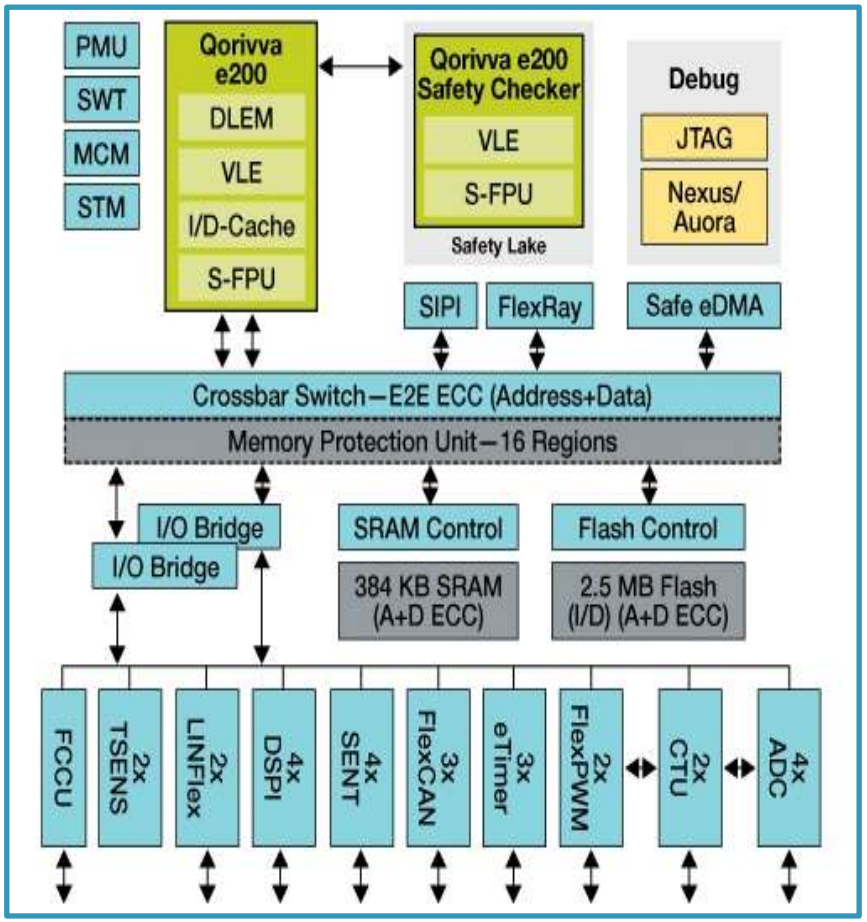
SW deliverables provided by Freescale and partners

- 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 Appication Note



Supporting Material for Functional Safety

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

www.Freescale.com

© 2014 Freescale Semiconductor, Inc. | ***External Use***