Functional Safety Compliance
Throughout the Vehicle with SafeAssure Solutions

FTF-AUT-F0009

Richard Soja  |  Automotive MCU Systems Engineer

A P R . 2 0 1 4
Agenda

• Functional Safety at Freescale

• Functional Safety and Microcontrollers

• MCU Safety Context and Safety Concepts

• Dynamic FMEDA

• Safety Manual
Microcontrollers and Digital Networking Processors

Five Core Product Groups

- Microcontrollers
- Digital Networking
- Automotive MCU
- Analog
- RF

Four Primary Markets

- Automotive
- Networking
- Industrial
- Consumer

>50 Year Legacy
>5,500 Engineers
>6,100 Patent Families
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

**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
The Right Technology Partner

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

Typical Safety System

<table>
<thead>
<tr>
<th>Sensors</th>
<th>MCUs</th>
<th>Analog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hi-Aspect Ratio SOI MEMS</td>
<td>Embedded Control</td>
<td>Hi-Performance Analog</td>
</tr>
<tr>
<td>SiGe Radar</td>
<td></td>
<td>Power Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connectivity</td>
</tr>
</tbody>
</table>
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** \(\Rightarrow\) **Certified ISO 26262**!
- **Gen 3 Safety** From 2012, multiple MCUs in Body, Chassis and Powertrain are being designed and developed according to ISO 26262

### 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

### 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

### 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
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**
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

**Aeronautic**
- 1980: DO 178
- 1985: DO 178A
- 1990: DO 178B
- 1995: ARP 4754
- 2000: ARP 4761
- 2005: DO 254
- 2010: DO 178C
- 2015: ARP 4754A

**Rail Transport**
- 1980: EN 50155
- 1985: IEC 61508
- 1990: EN 5012X
- 1995: EN 50159
- 2000: IEC 61508
- 2005: IEC 61508
- 2010: IEC 61508 Ed. 2.0

**Generic Standard**
- 1980: IEC 61508
- 1985: IEC 61508
- 1990: IEC 61508
- 1995: IEC 61508
- 2000: IEC 61508
- 2005: IEC 61508
- 2010: IEC 61508 Ed. 2.0
- 2015: ISO 13849

**Industrial Automation**
- 1980: IEC 61508
- 1985: IEC 61508
- 1990: IEC 61511
- 1995: IEC 62061
- 2000: ISO 13849
- 2005: ISO 13849
- 2010: ISO 13849
- 2015: ISO 26262

**Automotive**
- 1980: (IEC 61508)
- 1985: (IEC 61508)
- 1990: (IEC 61508)
- 1995: (IEC 61508)
- 2000: (IEC 61508)
- 2005: (IEC 61508)
- 2010: ISO 60601 Ed. 3.0
- 2015: ISO 60601 Ed. 3.0

**Medical**
- 1980: ISO 13485
- 1985: ISO 13485
- 1990: ISO 13485
- 1995: ISO 13485
- 2000: ISO 13485
- 2005: ISO 13485
- 2010: ISO 13485
- 2015: ISO 13485

---

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.
**Comparison of Functional Safety Standards**

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

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Safety Integrity Levels</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262</td>
<td><strong>Automotive</strong> Industry standard, adaptation of IEC 61508 for electrical / electronic systems within road vehicles</td>
<td>ASIL A, ASILB, ASIL C, ASIL D</td>
<td>15 Nov 2011</td>
</tr>
<tr>
<td>IEC 61508</td>
<td><strong>Generic</strong> Industry standard, applicable to electrical / electronic / programmable electronic safety-related systems.</td>
<td>SIL 1, SIL 2, SIL 3, SIL 4</td>
<td>Ed. 2.0 – Apr 2010</td>
</tr>
<tr>
<td>ISO 13849</td>
<td>One of two European Standards to achieve compliance with the Machinery Directive 2206/42/EC</td>
<td></td>
<td>Ed. 1.0 - More than 10 years ago</td>
</tr>
</tbody>
</table>

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

ISO26262

Relevant scope of ISO26262 high

Relevant scope of ISO26262 medium

Freescale

Functional Safety Focus

Safety Element out of Context

OEM

- Item definition
- Hazard analysis and risk assessment
- Safety Goals
- Functional Safety Concept

Safety Manual & Safety Analysis

Safety Requirements & DIA

Tier 1

- Safety Architecture
- Safety Concept
- ASIL Classification of Functions

Safety Manual & Safety Analysis

Safety Requirements & DIA

Tier 2 Supplier - Freescale

- HW / SW offering

Product Safety Measures (implemented in offering, described in Safety Manual, quantified/qualified by Safety Analysis)

Foundation

Development Process & Methods

Quality & Quality Data
MCU HW Component Developed as SEooC

Safety Manual includes all HW & SW requirements on system level (Assumptions) as well as MCU Safety Concept description.

(4-6) MCU Safety Context

(4-7) MCU Safety Concept

MCU SEooC Safety Plan

(5-6) MCU HW Safety Requirements

(5-7) MCU HW Design Specification

(5-7) Simulation Testing

(5-8,9) MCU FMEDA

(5-10) Silicon Testing

Applicable to MCU HW Component developed as SEooC

Reference ISO 26262-10:2012
### Functional Safety Process – Definition to Test

<table>
<thead>
<tr>
<th>Product Life-Cycle</th>
<th>Product Definition</th>
<th>Product Development</th>
<th>Product Manufacturing</th>
<th>End of Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Concept</td>
<td>Planning</td>
<td>Execution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Prototype</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>First Build</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RTL Freeze</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tape Out</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Validation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pilot</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Certification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Production</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Start EOL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>EOL</td>
</tr>
</tbody>
</table>

#### Milestone
- PCG0
- PCG1
- PCG2
- PCG3
- PCG4
- PCG5
- M1
- M2
- M3

#### Start Lifecycle
- Define product type
- QM or ISO26262

#### Define
- Input Requirements
  - Standard
  - Customer
  - Marketing
  - Internal
- Product Requirements (PRD)
- Product Electrical Specification
- (4-6) MCU Safety Context
- (4-7) MCU Safety Concept
- (5-6) MCU HW Safety Requirements
- (5-7) MCU HW Design Specification
- MCU Architecture (ADD)
- (5-8,9) Concept FMEDA

#### Implement
- Dynamic FMEDA
- (5-7) SoC Integration & Testing
- (5-7) IP Block Verification Testing

#### Test
- (7-5) Production Testing
- (8-13) Qualification Testing
- Fault Injection Testing

#### Customer Documents
- Data Sheet
- Reference Manual
- Safety Manual
- Dynamic FMEDA

#### Diagram Color Schema
- Development Flow
- Input Document
- Safety Requirement Traceability
- Functional Documentation
- Safety Documentation
- Simulation Testing
- Silicon Testing

---

**External Use** | 14
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.

Covering the whole range efficiently …
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)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Products enabled for functional safety</th>
<th>Products developed according to ISO 26262</th>
</tr>
</thead>
<tbody>
<tr>
<td>What does the development process address?</td>
<td>addresses <strong>quality</strong> at component level. Functional safety is addressed at <strong>system</strong> level</td>
<td>addresses <strong>quality &amp; functional safety</strong> at <strong>component</strong> level</td>
</tr>
</tbody>
</table>

**Deliverables available to customers**

<table>
<thead>
<tr>
<th>Software</th>
<th>QM software, e.g. AUTOSAR OS and MCAL, Self Test Software, Complex Drivers</th>
<th>Software developed to ISO 26262, e.g. AUTOSAR MCAL, Self Test Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production readiness evidence:</td>
<td>PPAP</td>
<td>Functional Safety Assessment, PPAP</td>
</tr>
<tr>
<td>Safety Analysis of Architecture</td>
<td>Safety FMEA or FTA</td>
<td>FMEDA, CCF or FTA</td>
</tr>
</tbody>
</table>
# SafeAssure Products

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Product</th>
<th>Target Applications</th>
<th>Safety Process</th>
<th>Safety Hardware</th>
<th>Safety Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MCU</strong></td>
<td>MPC5746M</td>
<td>Diesel Engine Management, Direct Injection Engine, Electronically Controlled Transmissions, Gasoline Engine Management</td>
<td>ISO 26262</td>
<td>Integrated Safety Architecture e.g.: Multi core, delayed lockstep, e2e ECC, replicated peripherals, LBIST &amp; MBIST, FCCU</td>
<td>FMEA, Safety Manual</td>
</tr>
<tr>
<td></td>
<td>MPC574xP</td>
<td>Electric Power Steering, Braking and Stability Control, Advanced Driver Assistance Systems (ADAS), Safety Domain Control</td>
<td>ISO 26262</td>
<td>Integrated Safety Architecture e.g.: Dual core, delayed lockstep, e2e ECC, replicated peripherals, LBIST &amp; MBIST, FCCU</td>
<td>FMEA, Safety Manual</td>
</tr>
<tr>
<td></td>
<td>MPC567xK</td>
<td>77 GHz RADAR System</td>
<td>FSL QM</td>
<td>Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU</td>
<td>FMEA, Safety Application Note</td>
</tr>
<tr>
<td></td>
<td>MPC564xL</td>
<td>77 GHz RADAR System, Electric Power Steering, Braking and Stability Control</td>
<td>ISO 26262</td>
<td>Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU</td>
<td>FMEA, Safety Manual, System Level Application Note</td>
</tr>
<tr>
<td></td>
<td>MPC560xP</td>
<td>DSIAirbag System, PSIS Airbag System, Electric Power Steering</td>
<td>FSL QM</td>
<td>Single core, SEC/DED ECC, Clock Monitoring Unit, Low Voltage Detector, FCCU</td>
<td>FMEA, Safety Application Note</td>
</tr>
<tr>
<td><strong>Analogue and Power</strong></td>
<td>MC33906</td>
<td>Safety Critical Motor Control, Electric Power Steering</td>
<td>ISO 26262</td>
<td>Integrated Safety Architecture e.g.: Independent Voltage Monitoring and Fail Safe state Machine (ARIST, LBIST), FCCU Monitoring for Dual Core Lockstep Mode, Several HW diagnostic to cover SPF, LT</td>
<td>Safety Manual, FMEA, System Level Application Note</td>
</tr>
<tr>
<td></td>
<td>MC33739</td>
<td>PSIS Airbag System</td>
<td>FSL QM</td>
<td>4xPSIS Host, Safety Block</td>
<td>Safety FMEA</td>
</tr>
<tr>
<td></td>
<td>MC33926</td>
<td>Valve control in Powertrain applications</td>
<td>FSL QM</td>
<td>Output state flag, Thermal Shutdown</td>
<td>Safety FMEA</td>
</tr>
<tr>
<td><strong>Sensors</strong></td>
<td>MMA16xx</td>
<td>DSIAirbag System</td>
<td>FSL QM</td>
<td>DSI2.5 safety bus, Triggered self test, Over-damped MEMS</td>
<td>FTA</td>
</tr>
<tr>
<td></td>
<td>MMA26xx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MMA51xx</td>
<td>PSIS Airbag System</td>
<td>FSL QM</td>
<td>PSIS safety bus, Triggered self test, Over-damped MEMS</td>
<td>FTA</td>
</tr>
<tr>
<td></td>
<td>MMA52xx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MMA65xx</td>
<td>PSIS Airbag System</td>
<td>FSL QM</td>
<td>SPI w/ CRC, Triggered self test, Over-damped MEMS</td>
<td>FTA</td>
</tr>
<tr>
<td></td>
<td>MMA66xx</td>
<td>Electric Power Steering (EPS)</td>
<td>FSL QM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MMA69xx</td>
<td>Braking and Stability Control</td>
<td>FSL QM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agenda

• Functional Safety at Freescale

• Functional Safety and Microcontrollers

• MCU Safety Context and Safety Concepts

• Dynamic FMEDA

• Safety Manual
Functional Safety – Risk definition

**Risk**: Combination of the probability and extent of damage

Reference TÜV SAAR Training  Module K3
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

*Reference ISO 26262-3:2011*
Target Metrics for ASIL

- Associate the following target metrics to each **safety goal**
  - Single-point fault metric (SPFM)
  - Latent-fault metric (LFM)
  - Probabilistic Metric for random Hardware Failures (PMHF)

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

<table>
<thead>
<tr>
<th>Safety Level</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-point fault metric</td>
<td>≥90 %</td>
<td>≥97 %</td>
<td>≥99 %</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Safety Level</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latent-fault metric</td>
<td>≥60 %</td>
<td>≥80 %</td>
<td>≥90 %</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Safety Level</th>
<th>Random hardware failure target values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&lt;10⁻⁸ h⁻¹</td>
</tr>
<tr>
<td>C</td>
<td>&lt;10⁻⁷ h⁻¹</td>
</tr>
<tr>
<td>B</td>
<td>&lt;10⁻⁷ h⁻¹</td>
</tr>
</tbody>
</table>

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**

**MCU Module Classification**

<table>
<thead>
<tr>
<th>Category</th>
<th>Module</th>
<th>SF1</th>
<th>SF2</th>
<th>SF3</th>
<th>SF4</th>
<th>PRL</th>
<th>HSM</th>
<th>NSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core and system modules</td>
<td>Main Core, IIC</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ClkCore, CPU</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DDR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Memories and memory controllers</td>
<td>Flash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>uSD/MMC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MC_PCU</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power management module</td>
<td>MCU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clocking module</td>
<td>MC_CSM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>PLL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CMU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MC_CGM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MICS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RDM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Reference ISO 26262-5:2011
Realizing the MCU Safety Concept – Qorivva MPC5744P

Redundant use of IO & Application checks

- Clock Monitoring
- Power Monitoring
- ECC on buses
- ECC on SRAM & Flash
- Fault Tolerant Com.
- Dual Core Lockstep

Processing Unit - Dual Core Lockstep

MPC5744P
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
    ▪ $\beta$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
What is an FMEDA?

FMEDA calculates absolute:

- Uncontrolled Failure per hour

FMEDA calculates and relative values:

- Controlled / Total Failure per hour

Each gate may have various possible failure modes

Uncontrolled Failure per hour

Failure avoided by design or usage

Failure detected by diagnostic

Failure switches to safe state

Unused by safety function

Catastrophic event

Gates
How to setup FMEDA - Template

Approach used in FMEDA Template

DC assessed by engineering judgment or analytic calculation

Diagnostic coverage measures 1
Diagnostic coverage measures 2
Diagnostic coverage measures 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

divide circuitry in elements

elements listed in ISO26262-5 Table D.1
## ISO 26262-5 (Elements and Failure Models)

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

<table>
<thead>
<tr>
<th>Element</th>
<th>See Tables</th>
<th>Analyzed failure modes for 60% / 90% / 99% DC</th>
<th>Low (60%)</th>
<th>Medium (90%)</th>
<th>High (99%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>D.9</td>
<td>Under and over Voltage</td>
<td>Drift</td>
<td>Under and over Voltage</td>
<td>Drift and oscillation</td>
</tr>
<tr>
<td>Clock</td>
<td>D.10</td>
<td>Stuck-at(^a)</td>
<td>d.c. fault model(^b)</td>
<td>d.c. fault model(^c)</td>
<td>d.c. fault model(^d)</td>
</tr>
<tr>
<td>Non-volatile memory</td>
<td>D.5</td>
<td>Stuck-at(^a) for data and addresses and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>control interface, lines and logic</td>
<td>d.c. fault model(^e) for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>data and addresses (includes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>address lines within same</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>block) and control interface,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lines and logic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volatile memory</td>
<td>D.6</td>
<td>Stuck-at(^a) for data, addresses and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>control interface, lines and logic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>d.c. fault model(^f) for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>data, addresses (includes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>address lines within same</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>block and inability to write</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>to cell) and control interface,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lines and logic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Soft error model(^g) for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bit cells</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital I/O</td>
<td>D.7</td>
<td>Stuck-at(^a) (including signal lines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>outside of the microcontroller)</td>
<td>d.c. fault model(^h) (including</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>signal lines outside of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>microcontroller)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analogue I/O</td>
<td></td>
<td>Stuck-at(^a) (including signal lines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>outside of the microcontroller)</td>
<td>d.c. fault model(^i) (including</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>signal lines outside of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>microcontroller)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*References: ISO 26262-5:2011*
## ISO 26262-5 (Elements and Failure Models)

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

<table>
<thead>
<tr>
<th>Element</th>
<th>See Tables</th>
<th>Analyzed failure modes for 60 %/90 %/99 % DC</th>
</tr>
</thead>
</table>
| ALU - Data Path                              | D.4/D.13   | Stuck-at*  
Stuck-at* at gate level  
d.c. fault model  
Soft error model (for sequential parts) |
| Registers (general purpose registers bank, DMA transfer registers...), internal RAM | D.4        | Stuck-at*  
Stuck-at* at gate level  
Soft error model (for sequential parts)  
d.c. fault model including no, wrong or multiple addressing of registers  
Soft error model (for sequential parts) |
| Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces) | D.4/D.5/D.6 | Stuck-at*  
Stuck-at* at gate level  
Soft error model (for sequential parts)  
d.c. fault model including no, wrong or multiple addressing  
Soft error model (for sequential parts) |
| Interrupt handling                           | D.4/D.10   | 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* wrong value  
Stuck-at* fault model |
| Other sub-elements not belonging to previous classes | D 4/D.13   | Stuck-at*  
Stuck-at* at gate level  
D.c. fault model  
Soft error model (for sequential part) |
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

<table>
<thead>
<tr>
<th>Software Functional Self Test Routine for Core supported by Hardware periodically executed within Fault Tolerant Time Interval</th>
<th>Lockstep enabled 33GCM_STATUS(LOM) = 1</th>
<th>Safety Relevant Core 2 Usage 33GCM_STATUS(LOM) = 0</th>
<th>Temporal Core and DMA Redundancy (recalculate on same core or doubles move with same EMMA)</th>
<th>Window and Logical Monitoring Watchdog implemented and detecting failure within Fault Tolerant Time Interval</th>
<th>MPU Enabled MPU_FGDs</th>
<th>MMU Enabled T,R0,0,T,0,F,0,F</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diagnostic Coverage of Self Test Routine</th>
<th>Reciprocal comparison</th>
<th>Diagnostic Coverage of Reciprocal comparison</th>
<th>Reciprocal comparison</th>
<th>Window Monitoring Watchdog configured</th>
<th>Logical Monitoring Watchdog configured</th>
<th>50% diagnostic coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>30% diagnostic coverage</td>
<td>TRUE</td>
<td>100% diagnostic coverage</td>
<td>Replicated Software use different SRAM block</td>
<td>TRUE</td>
<td>TRUE</td>
<td>50% diagnostic coverage</td>
</tr>
<tr>
<td>Software Test within Fault Tolerant Time Interval</td>
<td>TRUE</td>
<td>FALSE</td>
<td>Reciprocal comparison within Fault Tolerant Time</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Software Test supported by hardware</td>
<td>TRUE</td>
<td>FALSE</td>
<td>50% diagnostic coverage</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

**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 ≥ 99% |
| SF: λ | ≥ 99.84% | SIL 3 requires a Single-Point fault Metric ≥ 99% |
| λ_SFP + λ_RF (ISO26262), λ_Du (IEC61508) | 2.18E-10 h⁻¹ | ASIL D & SIL 3 require a single point or dangerous undetected failure rate of ≤ 1E⁻8 |
| λ_total_ISO26262 | 1.38E⁻⁰⁷ h⁻¹ |
| λ_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

• 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: 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)
  - $\beta$ic – 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]
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 Bosch 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 32-bit Arm® Cortex®-R4 core Safety Reduced Instruction (SRI) safety platform with a safety concept targeting ISO 26262 ASIL D integrity level. In order to maximize 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, processor bus system, memory protection unit, flash memory and RAM controller, paralleled bus bridges, system timers, and system watchdog timer). A Redundancy control and checker unit (RCCU) is implemented at each output of the SRI. RCCU is built to handle both on-chip RAM and flash memories.

The programmable Fault Collection and Control Unit (FCCU) monitors the integrity status of the device and provides fault isolation control.

B. Power Supply Requirements

The principal voltage regulator module provides the following features: Single high supply requires nominal 3.3V. An external diode transistor is used to reduce dissipation capacity at high temperature. An external resistor is used to reduce dissipation capacity at lower frequency of operation. All I/Os are at same voltage.
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

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

SW deliverables provided by Freescale and partners
- Enable support for ASIL D applications with minimized performance degradation
- sMCAL & sOS, Selftests, SW Safety Manual

Safety enablement provided by Freescale
- Safety Manual
- FMEDA
- System Level Application Note
Supporting Material for Functional Safety

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