Functional Safety for Industrial and Automotive Applications, Part 1

EUF-IND-T0589

Roger Ungerer | Field Application Engineer

JUNE 2014
Agenda

• Primary MCU Family for Functional Safety
  - Qorivva MCUs: Born for the Road

• Qorivva MCUs: Driving Industrial Safety

• Qorivva MCUs: Meets Some of the Safety Products

• SafeAssure: Functional Safety

• SafeAssure Program
A **Global Leader** in 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**

**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*
Qorivva MCUs: Born for the Road
Freescale has shipped over 200 million 32-bit Power Architecture™ MCUs, helping make cars smarter and safer
We help put
160,000 new cars
on the road every day
The Auto Industry is Evolving Rapidly

New technologies
- Electrification of powertrain
- Active vehicle safety
- The connected car

Microcontroller performance requirements accelerating rapidly
- Multicore processing for safety and performance
- Integrated memory doubling every technology generation

Safety requirements across many new applications
- Fault tolerant/ fault recognition systems for braking, steering, powertrain and all the newest advanced driver assist solutions

Reducing power consumption becoming critical
- Up to 100+ ECUs having an impact
Automotive System Trends for ASIL Levels

Source: Freescale: Expectations based on global customer feedback
Qorivva Means…

**Designed for Automotive**
Built on industry-leading Power Architecture technology, Qorivva MCUs offer performance leadership.

**Unprecedented Scalability**
The Qorivva portfolio offers scalable solutions for powertrain, body and chassis & safety applications, enabling streamlined tools and development environments.

**Qorivva MCUs built on Power Architecture**

**Innovation**
With our newest MCUs built on 55nm process technology, you get triple- and quad-core devices that significantly improve power efficiency and quality, plus configurable peripheral sets to design exactly what you need.

**High-Quality Portfolio**
Choose from hundreds of 32-bit Power Architecture MCUs with peripheral sets optimized for a full range of automotive applications and a focus on quality and long-term reliability.

**Scalable, highly integrated solutions built on the industry’s most powerful automotive architecture**
Largest portfolio with automotive qualification grade
High temperature for space constraint applications
• Fuel, oil, water pumps, sensor and actuators…

125°C

All Freescale Automotive MCU are certified AEC Q100
support up to 125°C ambient temperature

Low PPM
Benefit of one of the lowest PPM levels in the industry targeting zero defects

Extended temperature up to 135°C+ ambient on several product lines (S08SG, S12G, S12ZV, Qorivva)
Qorivva MCUs: Driving Industrial Safety
Challenges for Complex Industrial Control Applications

• Advanced control algorithms
• Safety regulations
• Harsh conditions
• Quality and reliability
• Improved efficiency
• Reduced development time
• Lower system cost
• Component longevity

Motion control, power generation, clinical medical, aerospace and defense, motor drives, renewable energy, robotics and more
### The value proposition of Freescale Industrial MCUs

#### Broad Portfolio
- S08 MCUs
- 16/32bit DSC
- 32bit Kinetis
- 32bit Qorivva

#### Mark Leading IP
- Analogue
- Wireless IP
- Low Power
- Memory Technology

#### Enablement
- MQX RTOS
- CodeWarrior IDE
- Freemaster Analysis Tool
- Bare Metal stacks, Drivers, Libraries
- 3rd Parties
- SafeAssure Program (Qorivva)
- Reference Designs & Demos
- Freescale Tower System

#### Product Longevity

#### Design Support

#### Quality

---

**External Use** | **14**
Qorivva MCUs: Meet Some of the Safety Products
MPC5643L (90nm)

- **Core**
  - 120MHz PowerPC ISA Dual e200 zen4 core
  - 4K 2-way / 4-way I-cache
  - Safety enhanced Cores + SPE + VLE + MMU
  - Dual Parallel or Lock Step configuration + HW/SW monitoring

- **Memory**
  - 1MByte RWW Flash with ECC
  - 128 KByte SRAM with ECC
  - EE emulation
  - Dual crossbar with MPUs

- **I/O**
  - 2 x FlexCAN (32 message buffers each)
  - 1 x FlexRay (64 msg. buffers)
  - 2 x LINFlex
  - 3 x DSPI
  - 1 x External clock output
  - 2 x FlexPWM (2 x 12 channels)
  - 3 x eTimer modules (3 x 6 channels)
  - Dual ADC (16 channels each, 12bit), 1 S/H per ADC
  - 1 x Cross-triggering unit for motor control

- **System**
  - 2 x 16 Channels eDMA
  - Autonomous Fault Collection and Control Unit
  - CRC computing unit
  - Software watchdog timer (inc. window mode, flow monitoring)
  - 2 x Junction temperature sensor
  - Nexus debug interface (up to N3)
  - FM-PLL + FlexRay PLL
  - 3.3 V Single supply with external and internal ballast transistor
  - 3.3 V I/Os (ADC 5 V capable)
  - 144 LQFP / 257 MAPBGA 14 x 14 0.8mm pitch
  - Tj = 150°C
MPC5744P (55nm)

- **Core**
  - Dual up to 200 MHz PowerTM ISA e200 zen4 core (Z420)
  - 32 bit Reg File, 64 bit BIU with E2E ECC
  - 64kB RAM of D-LMEM with MPU for fast context switch + local data
  - 8KB 2-way I-cache / 4KB 2-way D-Cache
  - 1x Scalar FPU (compiler supported) per core
  - Safety enhanced Cores – VLE only
  - No Signal processing unit extension + NO MMU
  - Delayed Lock Step configuration only

- **Memory**
  - 2.5 MBytes NVM with ECC (with add. Safety measure for address)
  - 64kB EEE (Data Flash) available incl. ECC
  - Up to 384 Kbyte global system SRAM with ECC (Addr + Data)

- **I/O**
  - 3 x FlexCAN (64+2x32 message buffers)
  - 1 x FlexRay (Dual Channel 64 msg. buffers)
  - 2 x LINFlex (Uart/Lin protocol driver)
  - 4 x DSPI (4 cs each)
  - 2x FlexPWM (2x 12ch for 2 independent Motors Controlled)
  - 3 x eTimer modules (18 channel total)
  - 4 x SAR ADC – 1MS/s target 5V input capable
  - 2 x Cross-triggering unit for motor control automatism
  - 2x SENT
  - Ethernet (257BGA only)

- **System**
  - Interprocessor I/F SIPI (~ approx 300Mbaud)
  - Safe DMA
  - Fault Collection unit, WDG, T-sens, & CRC computing unit
  - Nexus debug interface – Aurora
  - Dual-PLL (Peripheral + System Core)
  - 3.3 V Single supply: internal regulator with external power stage or External supply
  - 3.3 V I/Os (ADC 5V capable)
  - 144 LQFP / 257 MAPBGA 0.8 mm pitch
  - Tj = 150°C. Extended Temperature at 165°C Option (separate P/N)
SafeAssure: Functional Safety
• Functional safety is the **absence of unreasonable risk** due to hazards caused by malfunctioning behavior of electrical/electronic systems
  - **Hazards**: potential source of harm
  - **Harm**: physical injury or damage to the health of people

- **Systematic**: failures, related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or manufacturing process, operational procedures, documentation or other relevant factors
- **Random**: failures that can occur unpredictably during the lifetime of a hardware element and that follow a probability distribution
Auto Example: Body System Architecture – Window Lift

- Arbeitskreis ‘Lieferanten’ V3
  - Gefaehrdungsanalyse und Risikoeinschaetzung der Wesentliche PKW-Funktionen
- One of the working groups set up to standardize electronic systems and products in the automotive industry
  - Made up of system developers
  - Carried out a Hazard Analysis and Risk Assessment of vehicle systems
  - AK_L_2009_06_07 Referenzliste
- Two hazards and their ASIL rating were identified for window lift (and sunroof)
Auto Example: The Body System Architecture – Window Lift

- Function: central closing of all windows
- Scenario: car is moving, window is slightly open, fingers are in the opening, all windows suddenly close
  - Light or moderate injuries possible (severity: S1)
  - Can happen on any journey, but fingers in slightly open window only to be expected occasionally (exposure: E2, 0.01)
  - Unlikely to be able to react quickly enough (controllability: C3, 1)
- According to the ISO 26262 standard (Table 4, ISO26262-3 Concept Phase), this leads to a QM rating for this function
  - no explicit functional safety requirements
What is Functional Safety?

Functional safety refers to the ability to avoid the risk of physical injury due to incorrect system operation in response to system inputs.
2006/42/EC Machine Directive

(Legal document incorporated across member states of EU)

Harmonized standards supersede all others from end of 2011 onwards (see Official Journal of the European Union for list)

EN ISO 13849-1/-2 (PLa – PLe)

EN IEC 61508

EN IEC 62061 (SIL1 – SIL3)

Cites IEC 61508 up to SIL 3

This relates to electronic and micro processors

European Union

United States of America

EN ISO 13849-1/-2

EN IEC 61508
Machine Directive: European Impact Only?

EEA – European Economic Area (EU + Iceland, Liechtenstein & Norway)
## 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>ISO 26262</th>
<th>IEC 61508</th>
<th>ISO 13849</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automotive</strong> Industry standard, adaptation of IEC 61508 for electrical / electronic systems within road vehicles</td>
<td><strong>Generic</strong> Industry standard, applicable to electrical / electronic / programmable electronic safety-related systems.</td>
<td>One of two European Standards to achieve compliance with the Machinery Directive 2206/42/EC</td>
</tr>
<tr>
<td>Safety Integrity Levels</td>
<td>Safety Integrity Levels</td>
<td>Performance Levels</td>
</tr>
<tr>
<td>ASIL A, ASIL B, ASIL C, ASIL D</td>
<td>SIL 1, SIL 2, SIL 3, SIL 4</td>
<td>a, b, c, d, e</td>
</tr>
<tr>
<td>Publication date</td>
<td>Publication date</td>
<td>Categories</td>
</tr>
<tr>
<td>15 Nov 2011</td>
<td>Ed. 2.0 – Apr 2010</td>
<td>B, 1, 2, 3, 4</td>
</tr>
<tr>
<td></td>
<td><em>Ed. 1.0 - More than 10 years ago</em></td>
<td></td>
</tr>
</tbody>
</table>

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

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

**Tier 1**
- Safety Architecture
- Safety Concept
- ASIL Classification of Functions

**Tier 2 Supplier - Freescale**
- HW / SW offering

**Safety Manual & Safety Analysis**
- Safety Requirements & DIA

**Product Safety Measures** (implemented in offering, described in Safety Manual, quantified/qualified by Safety Analysis)
- Development Process & Methods
- Quality & Quality Data

Freescale
- Functional Safety Focus
- Safety Element out of Context

ISO 26262
- Relevant scope of ISO 26262 high
- Relevant scope of ISO 26262 medium
MCU HW Component Developed as SEooC

**SEooC Hardware Component Development**

<table>
<thead>
<tr>
<th>3</th>
<th>Concept Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5</td>
<td>Considered not In scope of HW SEooC development</td>
</tr>
</tbody>
</table>

**Item Development**

| 3 | Concept phase |

---

**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

---

**Reference ISO 26262-10:2012**
Functional Safety Process – Definition to Test
First ISO 26262 Certified MCU – Qorivva MPC5643L

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

Released on 6th September, 2012
ISO 26262 Assessment and Audit Summary

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

<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 quality at component level. Functional safety is addressed at system level</td>
<td>addresses quality &amp; functional safety at component level</td>
</tr>
<tr>
<td><strong>Deliverables available to customers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Analysis of Architecture</td>
<td>Safety FMEA or FTA</td>
<td>FMEDA, CCF or FTA</td>
</tr>
<tr>
<td>Software</td>
<td>QM software, e.g. AUTOSAR OS and MCAL, Self Test Software, Complex Drivers</td>
<td>Software developed to ISO 26262, e.g. AUTOSAR MCAL, Self Test Software</td>
</tr>
<tr>
<td>Production readiness evidence:</td>
<td>PPAP</td>
<td>Functional Safety Assessment, PPAP</td>
</tr>
</tbody>
</table>

- 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)
**Functional Safety Standards**

**Automotive**
- ISO 26262
- Generic Industry standard, applicable to electrical/electronic/programmable electronic safety-related systems.
- Integrity levels: SIL 1, SIL 2, SIL 3, SIL 4
- Pub date: More than 10 years ago

**Industrial**
- IEC 61508
- Generic Industry standard, applicable to electrical/electronic/programmable electronic safety-related systems.
- Integrity levels: SIL 1, SIL 2, SIL 3, SIL 4
- Pub date: More than 10 years ago

**Safety Support**
- ISO 26262
- Automotive Industry standard, adaptation of IEC 61508 for electrical/electronic systems within road vehicles.
- Integriy levels: ASIL A, ASIL B, ASIL C, ASIL D
- Pub date: Target end 2011

**Safety Hardware**
- Microcontrollers
- Lockstep Cores, ECC on Memories, Redundant Functions, Internal Monitors, Built-In Self Test, Fault Collection & Control

- Analog and Power Management
- Voltage Monitors, External Error Monitor, Advanced Watchdog, Built-In Self Test

- Sensors
- Timing Checker, Digital Scan of Signal Chains, DSS3 or PSIS Safety Data links

**Safety Software**
- IEC 61508
- Automotive Industry standard, adaptation of IEC 61508 for electrical/electronic systems within road vehicles.
- Pub date: Target end 2011

**Safety Process**
- Microcontrollers
- Lockstep Cores, ECC on Memories, Redundant Functions, Internal Monitors, Built-In Self Test, Fault Collection & Control

- Analog and Power Management
- Voltage Monitors, External Error Monitor, Advanced Watchdog, Built-In Self Test

- Sensors
- Timing Checker, Digital Scan of Signal Chains, DSS3 or PSIS Safety Data links

- Organization
- Safety is an integral part of the Freescale world-wide organization

- Project Management
- Configuration & Change Management, Quality Management, Requirements Management, Architecture & Design, Verification & Validation

- Quality Management
- ISO TS 16949 Certified Quality Management System
- Hardware - Zero Defects
- Software – SPICE Level 3

**Freescale Quality Foundation**

**People**
- Regional functional safety experts

**Documentation**
- Safety Application Notes / Safety Manual / FMEDA

**Automotive Software**
- AUTOSAR OS & MCAL
- Core Self Test
- Device Self Test, Complex Drivers

**Software Partnerships**
- Partnering with leading third-party software providers for automotive and industrial

**Safety Analysis**
- Selected products defined & designed from the ground up with safety analysis being done at each step of the process

**Assessments / Audits**
- Safety Confirmation Measures

**Continuous Improvement**
- Process evaluation, assessments / audits and gap-analysis exist to ensure processes are continually optimized
## SafeAssure Products

<table>
<thead>
<tr>
<th>Target Market</th>
<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>Automotive</td>
<td>Microcontrollers</td>
<td>Coriiva MPC5768G</td>
<td>Battery Monitoring High End Body Control Module Infotainment Gateway Central Gateway / In-Vehicle Networking</td>
<td>ISO 26262 ASIL B</td>
<td>Integrated Safety Architecture e.g.: Multicore, e2ECC, LBIST &amp; MBIST, clock and under voltage monitoring, FCCU</td>
<td>FMEDA Safety Manual</td>
</tr>
<tr>
<td>Automotive</td>
<td>Microcontrollers</td>
<td>Coriiva MPC5679X</td>
<td>77 GHz RADAR System Front View Camera</td>
<td>FSL QM</td>
<td>Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU</td>
<td>FMEDA Safety Manual</td>
</tr>
<tr>
<td>Automotive</td>
<td>Microcontrollers</td>
<td>Coriiva MPC5610L</td>
<td>77 GHz RADAR System Electric Power Steering (EPS) Braking and Stability Control</td>
<td>ISO 26262 ASIL D</td>
<td>Integrated Safety Architecture e.g.: Dual core, lockstep or dual parallel processing, replicated peripherals, FCCU</td>
<td>FMEDA Safety Manual</td>
</tr>
<tr>
<td>Automotive</td>
<td>Microcontrollers</td>
<td>Coriiva MPC5610P</td>
<td>Airbags Electric Power Steering (EPS)</td>
<td>FSL QM</td>
<td>Integrated Safety Architecture e.g.: Single core, SECDED ECC, Clock Monitoring Unit, Low Voltage Detector, FCCU</td>
<td>FMEDA Safety Application Note</td>
</tr>
<tr>
<td>Automotive</td>
<td>Analog and Power Management</td>
<td>MC33907</td>
<td>Electric Power Steering (EPS) Safety critical motor control Vehicle dynamic and chassis control</td>
<td>ISO 26262 ASIL D</td>
<td>Integrated Safety Architecture e.g.: Voltage Monitoring and Fail Safe state Machine (ASIB, LBIST), FCCU Monitoring for Dual Core Lock Step Mode, Several HW diagnostic to cover SP, LT</td>
<td>Safety Manual FMEDA System Level Application Note</td>
</tr>
</tbody>
</table>

*To view the latest SafeAssure product table visit [www.freescale.com/SafeAssure](http://www.freescale.com/SafeAssure)*
ISO 26262 Assessment – Clarification…

Q: Do we need to assess every MCU for ISO 26262 compliance?
A: No. **Selected** MCUs will need to be compliant with ISO 26262, for these we need to have a **positive assessment report** and completed **Safety Case** prior to releasing the product for production.
- Process updated: ISO 26262 update made to the Automotive MCU CAB gate.
- Selected MCUs will continue to be developed to target QM
- Some QM developed MCUs will be enabled with additional safety collateral (safety analysis, SW etc) to simplify integration into safety systems
- Selection between QM or ISO26262, based on market demand

Q: Do we need to have an external company (**Exida / TUV**) assess each MCU?
A: No. ISO 26262 does not require that we are assessed/certified by a 3rd party. However, ISO 26262 does require that there is a certain level of independence between the assessor and the MCU development team.
- Process update: Quality organization has agreed to take on the Audit and Assessment role for ISO 26262. Similar as is done today to ensure compliance with ISO TS 16949 / ISO 9001.
Functional Safety Standards Focus

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

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

**Freescale** has strengthened its product development cycle, making functional safety an integral part of the process.
**Functional Safety Standards Focus**

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

---

**Freescale** has strengthened its product development cycle, making functional safety an integral part of the process.
FSL QM Products - Typical Deliverables

- Safety Analysis of Architecture: Safety FMEA or FTA
- User Guide: Safety Application Note
- Development Process evidence: PPAP, Quality Plan (Mapping to ISO 26262 / IEC 61508 checklists)

ISO 26262 or IEC 61508 Products – Typical Deliverables

- Safety Analysis of Architecture: FMEDA, CCA or FTA
- User Guide: Safety Manual (baseline is ISO26262, IEC61508 additions included for certain products)
- Development Process evidence: PPAP, Safety Plan, Certificates

Local Support

- Functional Safety Field Experts

Learning

- Field Training / workshops – delivered by Local Functional Safety FAE Experts
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, STM, SRAM, Processing Unit…

Work flow and result

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

Objective
- Enables customers to extract the full value of Freescale’s functional safety offering
- Simplify integration of Freescale’s safety products into applications
- A comprehensible description of all information relating to FS in a single entity to ensure integrity of information and links with datasheet

Content
- SoC Safety Concept description
- System level assumptions of use (Safety specific usage considerations)
- Pseudo-code or C-Code to simplify adoption of safety application requirements
- FMEDA results
  - Latent Fault Matrix (LFM)
  - Single Point Fault Matrix (SPFM)
  - Probabilistic Metric for random Hardware Failures (PMHF)
- Provisions against Dependent Failures
Safety 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 Bus Chip in automotive electronic/electrical systems that target the ISO26262 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 ISO26262 solutions, that form part of the Freescale Safety Assurance 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 D02044 core of Application (AS) safety platform with a safety concept targeting ISO26262 ASIL D integrity level. In order to minimize additional software and hardware-level features to reach this target, on-chip redundancy is offered for the critical components of the MCU (CPU, DMA controller, Interrupt controller, crossbar bus system, memory protection unit, Flash memory and RAM controller, peripheral bus bridge, system timer, and watchdog timer). ASIL D redundancy control and check unit (RCCU) is implemented as each output of the SoC. RCCU 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 safety state control.

B. Power Supply Requirements

The analog voltage regulator module provides the following features: Single high supply requirement; nominal 3.3V. An external rail translator is used to reduce isolation capacitance at high temperature but can be used if power dissipation is maintained within package dissipation capacity (lower frequency of operation). All I/Os are at same voltage.
SafeAssure MCU Product: MPC5744P

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, Self tests, SW safety manual

Safety enablement provided by Freescale
- Safety manual
- FMEDA
- System-level Application Note
ISO 26262 ASIL D
- Safety measures of analog architecture and development process (ISO 26262) helps to reduce effort and time on ECU functional safety assessment
  - FCCU (dual core lock step) monitoring

Integrated Safety Architecture (ISA)
- Saves development effort and time as no additional SW required (only 1 main MCU)
  - Independent voltage monitoring and fail safe state machine
  - High HW diagnostic to cover SPF, LT, CCA

Secured SBC & MCU SW interactions
- Multiples registers to help SW diagnostics, including safe state machine
  - Safety mechanisms to secure SPI
  - Advanced watchdog challenger to secure MCU timing monitoring

Safety enablement provided by Freescale
- Application recommendations to combine MC33907 and MPC5643L
  - Safety manual, FMEDA and complete ecosystem to ease development, save time
Industrial MCUs Built on Power Architecture™ Performance and Safety in Motion

• The Freescale Qorivva MCUs, based on the e200 Power Architecture core, offers **exceptional performance** and **integration** for complex industrial applications

• With embedded safety architecture, new MCUs **simplify safety approvals**

• Proven **leadership** with respect to quality, reliability and technical support

• Advanced **development is simplified** with run-time software, modeling tools, advanced debug capabilities and rapid prototyping
Making the World a Smarter Place.