White Paper

Industries Made Safe: Qorivva MPC564xL MCUs by Freescale

Abstract

As the technology and industries that propel civilization's advancement increase in complexity, so increases the potential for catastrophic failures. Industrial explosions, crashes, fires and destruction are not uncommon. Governments, industry leaders and the public all stress the importance of holding companies accountable for industrial safety and standards. Enter functional safety and IEC 61508.

Table of Contents

freescale™

What Is Functional Safety and What Does IEC 61508 Cover?

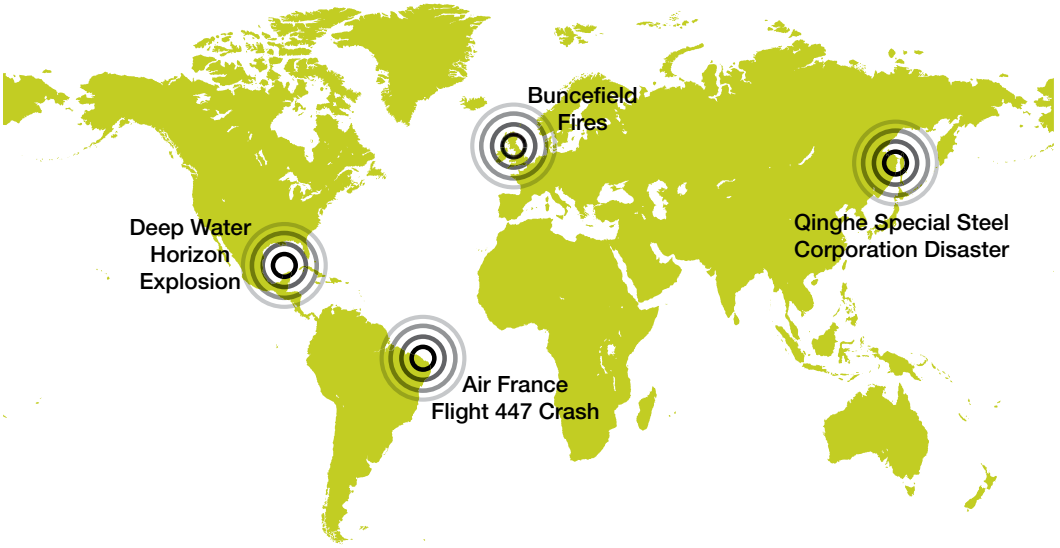
According to the IEC 61508 standards committee, functional safety is avoiding unacceptable risk of physical injury or damage to health of people, either directly or indirectly as a result of damage to equipment or to the environment where it operates.[1]

IEC 61508 is the leading international functional safety standard for general industrial applications and covers machinery, process industries, rail, nuclear power and automotive.

Functional safety is also becoming more prevalent and stringent in markets such as solar energy and aviation, as well as FDA Class III medical. Some examples of products requiring functional safety are:

- Safe PLCs
- Solar inverters
- Elevators and lifts
- Medical ventilators
- Aviation controls

Figure 1: History of Industrial Disasters



**Industrial disasters happen, have happened and will happen.
Robust safety systems are a key to prevention.**

Electronic safety systems, with their direct impact on human well being, are experiencing increasingly stringent requirements. Designing safety systems while meeting state-of-the-art functional safety requirements can be a challenging job for system designers—especially when they are also managing increased application complexity combined with time-to-market urgency.

The challenge for system engineers is to architect their system in a way that prevents dangerous failures or at least sufficiently controls them when they occur. Dangerous failures may arise from:

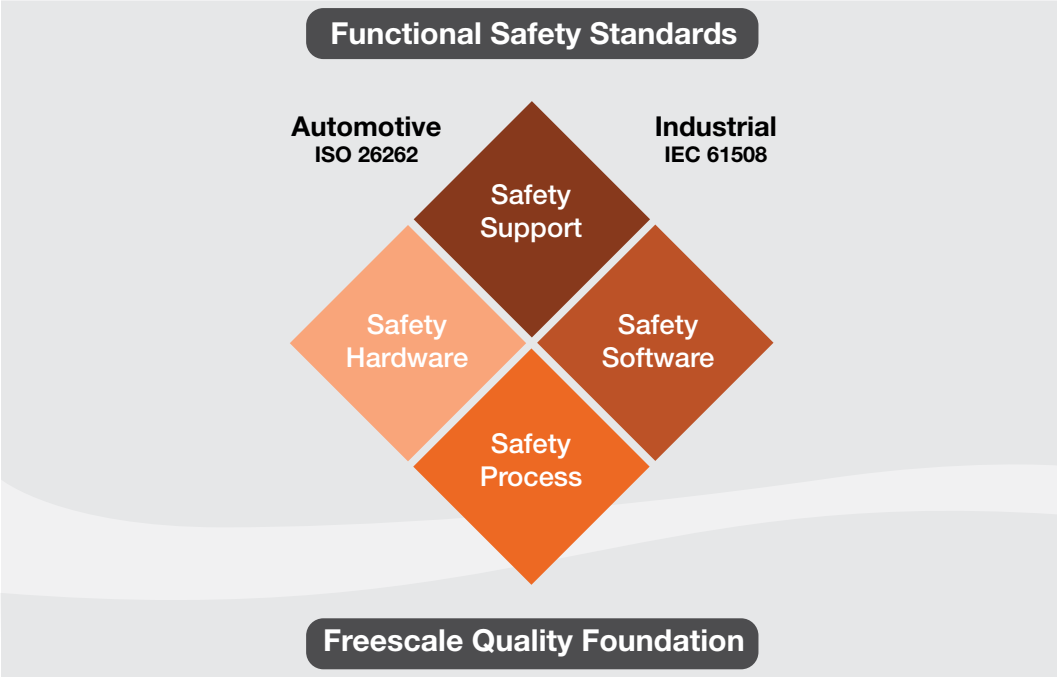
- Random hardware failures
- Systematic hardware failures
- Systematic software failures

Freescale's Solution for Functional Safety

The Qorivva MPC564xL family of 32-bit Power Architecture® dual-core MCUs targets industrial applications which require compliance with IEC 61508 SIL3 safety standard. It reduces design complexity and component count by putting key functional safety features on a single chip with a dual-core, dual-issue architecture, which can be statically switched between lockstep mode (redundant processing and calculations) to decoupled parallel mode (independent core operation). The performance of the MPC564xL family is rarely experienced in an MCU, with over 600 DMIPS possible.

The Qorivva MPC564xL family is part of Freescale's SafeAssure program. The SafeAssure program is designed to help system manufacturers comply with IEC 61508 functional safety standard with greater ease. System designers can count on the solutions included in Freescale's SafeAssure program to stand up to rugged conditions and be supported by the necessary documentation and safety expertise, reducing the time required to develop safety systems.

Figure 2: Freescale Functional Safety Diagram



Freescale Safety Foundation

Freescale's functional safety approach covers four key areas: Safety Process, Safety Hardware, Safety Software and Safety Support.

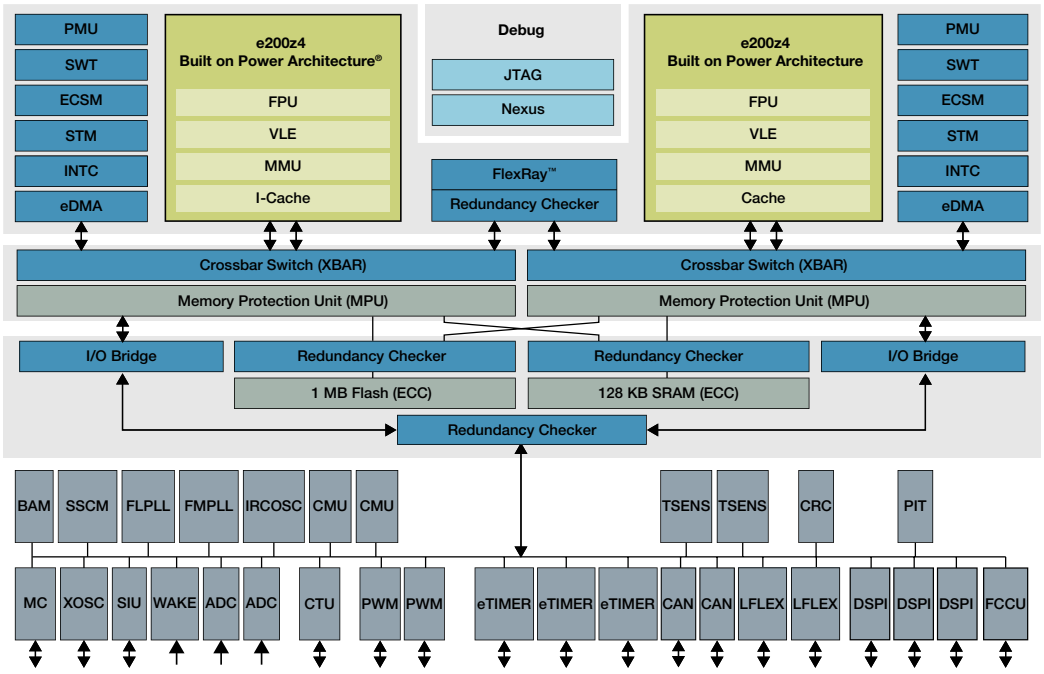
- Functional safety requirements begin with the way a company designs and implements a functional safety solution—the Safety Process
- Select Freescale products are being defined and designed from the ground up to comply with the standards, with safety analysis done at each step of the development process and additional confirmation measures taken to help ensure safety requirements are fully met

Freescale's Safety Hardware concept focuses on detecting and mitigating random hardware failures. This is achieved through built-in safety features, including self-testing, monitoring and hardware-based redundancy in Freescale MCUs. In industrial markets, MPC564xL MCUs are leading the way by targeting various industrial functional safety applications, including industrial automation and motor control.

The Qorivva MPC5643L contains two "channels," each consisting of a core, bus, interrupt controller, memory controller and other core-related modules. Instead of using two MCUs for safety-critical applications, the dual-core MPC5643L offers simplified system-level design, reducing complexity and cutting down development time for industrial functional safety systems.

To achieve system-level functional safety goals, hardware and software must seamlessly integrate to provide complete coverage of the safety requirements. To that end, the third key area of Freescale's functional safety approach is Safety Software. Freescale is partnering with leading third-party software providers to offer prevalidated Safety Software solutions.

Figure 3: Qorivva MPC5643L Dual-Core Sphere of Replication



Green Hills Software is offering support for the MPC564xL family with IEC61508 SIL 3 precertified INTEGRITY RTOS, certifiable µ-velOSity™ RTOS and MULTI Integrated Development Environment. Sciopta's IEC61508 SIL 3 precertified safety kernel is available for the MPC564xL family.

The fourth area of Freescale's functional safety approach is robust Safety Support, with the goal of easing system-level integration and functional safety standards compliance. Freescale's capabilities extend from customer-specific training and system design reviews regarding functional safety architecture to extensive safety documentation, such as a comprehensive safety manual and a Failure Modes, Effects and Diagnostics Analyses.

Figure 4: Freescale e200 Core Family Built on Power Architecture Technology

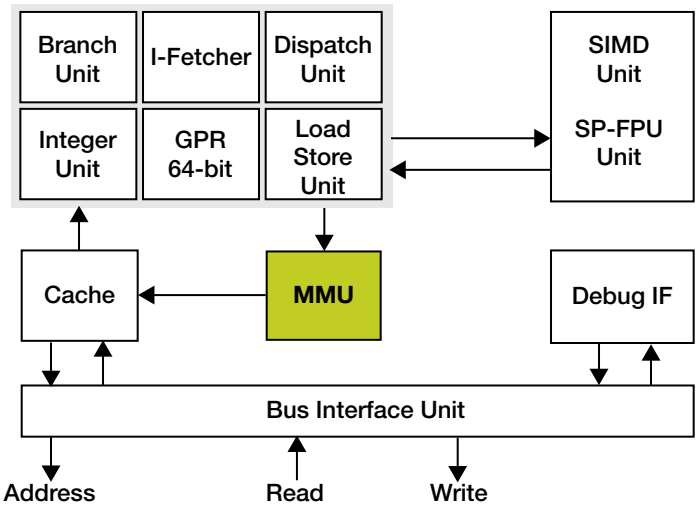


Figure 5: Memory and Crossbar Safety in a 32-bit Qorivva MCU

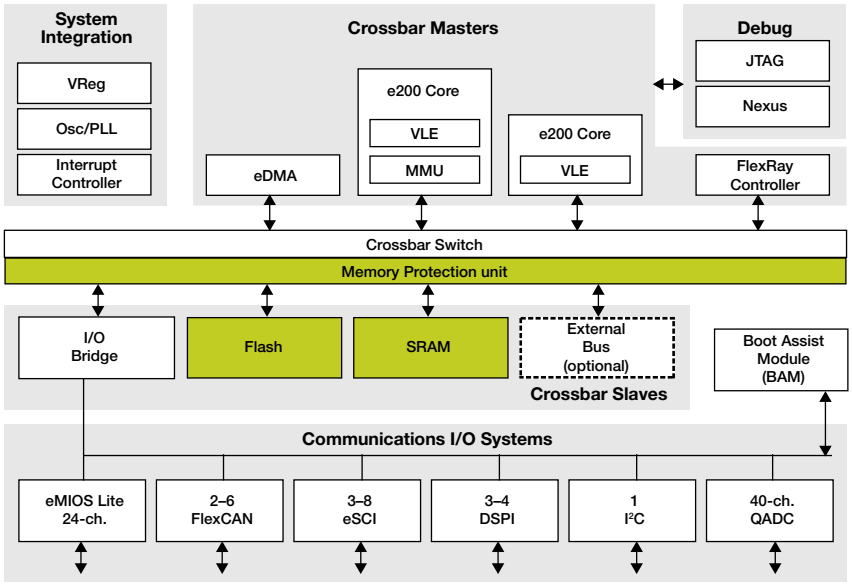
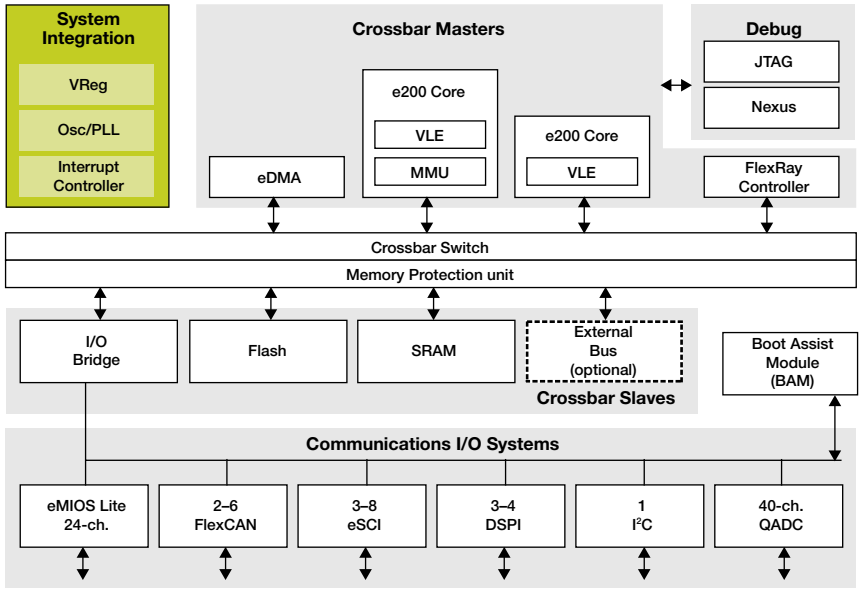


Figure 6: Power Supply and Clock Safety in a 32-bit Qorivva MCU



Robust Safety Systems

- Dual CPU cores with lockstep and decoupled parallel modes of operation
- Error correction (ECC) on memory systems with all single error correction and dual error detection
- Memory management and protection units monitor bus transfers and protect all bus transactions

Processor Core Safety

Example: Memory Management Unit (MMU)

- Optimization of self-test coverage by using different virtual addresses without relocating customer application data and code
- MMU can be used to protect accesses due to occurrence of faults in the core (exception generation)

Example: Multiple Input Shift Register (MISR)

- Method for verifying all intermediate results of a set of architected registers at the end of an instruction stream
- Introduction of MISR improves observability of the core resulting in:
  - Increased self test coverage
  - Faster detection of dormant faults

Memories and Crossbar Safety

Example: Memory Protection Unit (MPU)

- Monitors all system bus transactions and evaluates the appropriateness of each transfer
- Preprogrammed region descriptors define memory spaces and associated access rights
- Unmapped references are terminated with a protection error response

Example: Error-Correcting Code

- Used to detect failures of flash/SRAM stored data
- Typical solution for correcting bit flips caused by soft error rate (SER) impact
- ECC module (64 data bits + eight ECC bits) can:
  - Correct all single-bit errors
  - Detect all dual-bit faults
  - Detect several faults affecting > two bits

Power Supply and Clock Safety

Example: Power Suppy

- Monitoring of internal and external voltages—internal and external power supply
- Over- and under-voltage detection
- Testing capability of monitoring circuitry for detection of dormant faults

Example: Clock and Monitoring

- Clock monitoring for system and periphery clock:
  - Loss of crystal or PLL clock
  - PLL frequency higher/lower than reference
- Redundant clock generation with internal RC oscillator
- Glitch filtering with on-chip PLL

Reduce Your Safety-Critical Application Development Time

- Integrated features simplify safety approvals for IEC 61508 SIL3, FAA DO-178B Level A and FDA Class II to III
- Design for what you need today and in the future with our Tower System, a modular development platform that allows you to save time through rapid prototyping and tool reuse
- Self test with documented test coverage and fault graded
- System monitors for power supply and system clocks, with redundant clock generation

Conclusion

Functional safety will remain an important criterion while designing industrial control systems. The Freescale Qorivva MPC564xL family of industrial MCUs addresses the critical safety standards and requirements for industrial control systems, delivering robust safety features and exceptional performance.

References

1. “IEC 61508: Functional Safety—IEC 61508 Explained.” Welcome to IEC - International Electrotechnical Commission. International Electrotechnical Commission. Web. 02 Nov. 2011.

SAFE ASSURE by Freescale

For more information, visit freescale.com/power

Document Number: PWRARBYNDBITSIMS REV 2