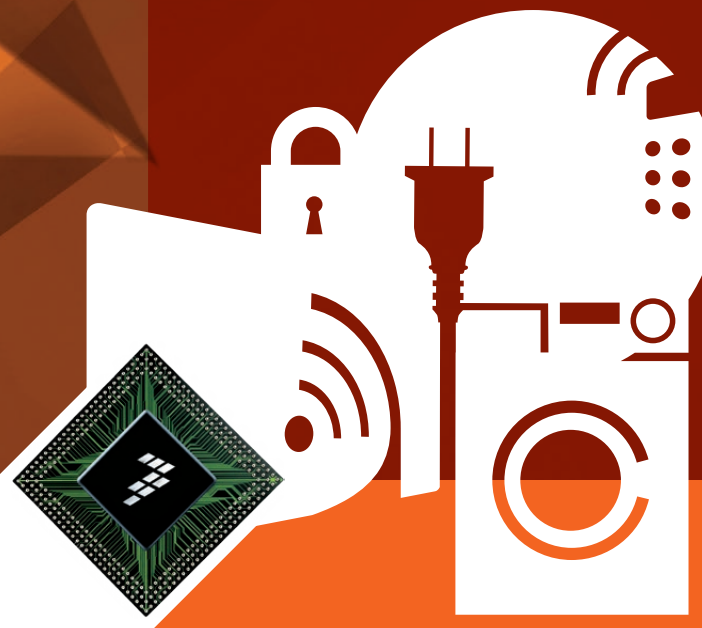


Safety Electronics

A New Approach

freescale™

SAFE ASSURE™ by Freescale

freescale.com

A New Approach

Overview

In order to determine how safe a system needs to be, you have to look at the risk for a given event that will lead to the hazard. In addition, you have to take into account the probability of exposure to this event and the potential severity. These steps will lead to the safety requirements of the system. Once the safety requirements are defined, the designer then has to determine how to reduce any resulting risk of all potential hazards below the acceptable risk level. The use of redundant systems for increasing the safeness of a system is standard procedure, but the design and implementation of the redundancy often requires some creativity. Electronic systems are not an exception.

The Situation

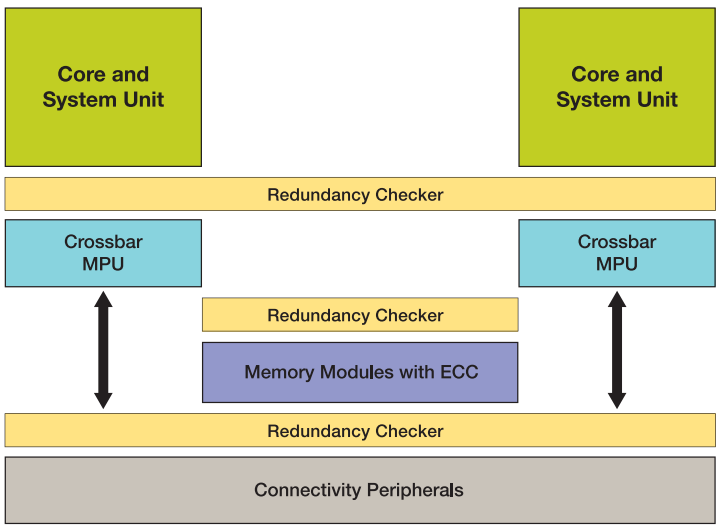
Traditionally, the only choice functional safety systems designers had for electronics processing design was a multi-chip system. Designers would pick the processors, memory modules, timers, watchdogs and other peripherals, and integrate them to create the redundancy and monitoring needed for safety applications. While these multi-chip systems do work they are quite laborious to create. Creating the hardware designs and implementing the software on multi-chip systems is significantly more complex and time consuming than on a single-chip system. While every designer knows this is true, single-chip systems did not offer the redundant architecture needed for safety applications. That is, until recently. There is a new approach for electronics processing in functional safety applications: a single-chip dual-core MCU.

The Approach

Freescale's Qorivva MPC5643L family of 32-bit Power Architecture® MCUs takes a new approach to addressing design needs for safety applications by integrating key safety functions on a single chip. The Qorivva MPC5643L, a Freescale SafeAssure solution, utilizes a dual-core safety platform with an innovative safety concept targeting systems with IEC61508 SIL 3 safety integrity levels. This is possible by offering on-chip redundancy for the critical components of the MCU, including: 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. Lockstep redundancy is then used for each output in this sphere of replication for redundant processing and calculations. On- board flash and RAM are protected with error correcting code, further reducing faults, and a fault collection and control unit monitors the integrity status of the device and provides flexible safe state control. The MPC5643L MCU also has the necessary performance and integration to handle the complexities of safety applications with up to 120 MHz dual-core operation, up to 1 MB of on-board flash memory, and dual motor control capabilities.

Besides reducing design time, the system footprint and bill of materials, there are several other advantages of a single-chip dual-core safety solution when compared to traditional multi-chip systems. One of the key advantages is that a single-chip solution will be implemented the same way over many applications while the design and implementation of multi-chip systems will change with each application. This allows for single- chip solutions to be pre-certified for use in functional safety applications. This saves significant time during certification as the system designer does not have to concentrate on the standard compliance of the MCU. Another advantage to single-chip

Qorivva MPC564xL Family Sphere of Replication



SafeAssure Safety Diagram

solutions is that internal communication is much faster because all components are on the same chip. This allows for many more safety checks per cycle through the same chip hardware in contrast to software checks on multi-chips systems. Software and debugging are also simplified as the redundancy of the cores in lockstep mode requires only one software image simplifying software programming and debugging efforts.

The Resolution

Achieving functional safety system compliance is time consuming and therefore, any simplification of functional safety compliance will save a company time and money. This is what the Freescale SafeAssure functional safety program is designed to do.

Freescale launched the SafeAssure program in September 2011 to help system manufacturers more easily achieve compliance with functional safety standards, including IEC 61508 and ISO 26262 for the industrial and automotive markets. Our approach is accomplished by focusing on four main areas outlined in the diagram on this page.

Functional safety requirements begin with the way a company designs and implements a functional safety solution—the Safety Process. Freescale has made functional safety an integral part of its product development process to align to the rigorous requirements of IEC 61508 and ISO 26262. In addition, select Freescale products, like the Qorivva MPC5643L, 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 offers a variety of MCUs, analog and power management, and sensors in the SafeAssure program to serve a broad range of functional safety applications. The MPC564xL devices are the first MCUs for industrial applications to be included in the SafeAssure program and cover a wide variety of functional safety applications. Since hardware and software must seamlessly integrate to provide comprehensive coverage of safety requirements, Freescale has partnered with leading third-party software provider Green Hills Software for industrial functional safety. For applications that require high reliability or certified functional safety, Green Hills Software offers the pre-certified INTEGRITY or certifiable u-velOSity-based safety BSPs, safety-qualified development tools and Embedded Expert safety consulting—enabling the highest levels of ISO 61508 SIL3 (industrial), ISO 26262 ASIL-D (automotive), DO-178B Level A (avionics) and EN 50128 SWIL4 (railway).

INTEGRITY's unique separation architecture enables reduced certification effort and program risk, faster time to market and lower costs of goods and certification through consolidation of multiple levels of criticality onto a single CPU.

For applications demanding the smallest footprint or a single level of software criticality, the IEC 61508-certifiable u-velOSity RTOS is a good fit. Both are optimally supported with the MULTI integrated development environment that combines record breaking compilers that produce the fastest and smallest code on the Power Architecture e200 core, a powerful multicore trace debugger, MISRA C coding standards enforcement, analysis tools, runtime error checking, instruction set simulator and other integrated productivity tools. For functional safety applications, the MULTI compiler and code generation tools are qualified for ISO 26262, IEC 61508 and EN 50128.

The fourth area of Freescale's functional safety approach is robust Safety Support, with the goal of easing system-level integration and functional safety standard compliance. Freescale capabilities extend from customer-specific training and system design reviews regarding functional safety architecture to extensive safety documentation and technical support. A failure modes effects and diagnostic analysis is available for the MPC5643L and offers customer-tailored product failure metrics. A safety manual describing how to use the functional safety features on the Qorivva MPC5643L is also offered.

Functional safety will always include an extra level of complexity but, with the Freescale SafeAssure approach and the Qorivva MPC564xL MCUs integrated functionality, simplification is within your reach.

How to Reach Us:

Home Page:
freescale.com

SafeAssure Information:
freescale.com/SafeAssure

Qorivva MPC564xL Product Information:
freescale.com/MPC564xL

e-mail:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
1-800-521-6274
480-768-2130
support@freescale.com

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014
+81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For more information, visit freescale.com/SafeAssure

Document Number: SFTYELCTRCWP REV 2