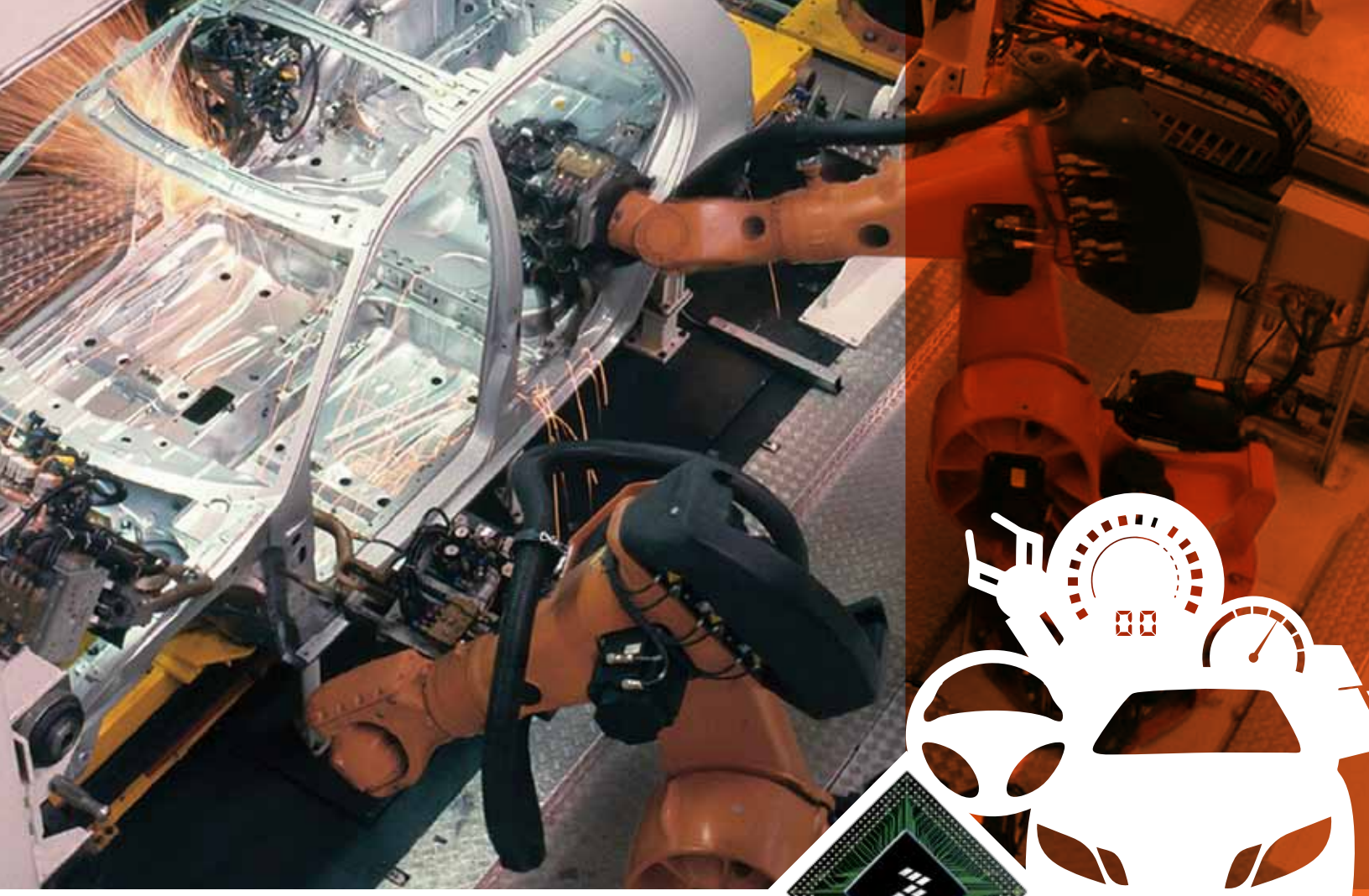


White Paper

Addressing the Challenges of Functional Safety in the Automotive and Industrial Markets

freescale™

SAFE ASSURE™ by Freescale

freescale.com/SafeAssure

Contents

Overview

Real-time control of safety-critical applications has been a longtime challenge for engineers. Application functions are becoming more complex and industry standards require more sophisticated functional safety concepts in both the automotive and industrial markets. Freescale has introduced its **SafeAssure** program to help system manufacturers more easily achieve compliance with the upcoming International Standards Organization (ISO) 26262 and existing International Electrotechnical Commission (IEC) 61508 standards. 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.

This white paper covers how functional safety requirements are changing the design game, the details behind Freescale's **SafeAssure** program and the hardware solutions targeting safety applications.

Functional Safety for Automotive and Industrial Applications

The focus on safety-critical applications in both the automotive and industrial markets is significantly growing, bringing new and added pressures to systems engineers as they work to solve safety challenges.

The automotive industry is under pressure to provide new and improved vehicle safety systems, ranging from basic airbag-deployment systems to extremely complex advanced driver assistance systems (ADAS) with accident prediction and avoidance capabilities. These safety functions are increasingly carried out by electronics, and ISO 26262 is intended to enable the design of electronic systems that can prevent dangerous failures and control them if they occur.

Recent industrial disasters have highlighted the need for improved safety, and an increasing number of industrial control systems are requiring IEC 61508 safety certification. Functional safety is also becoming more prevalent and stringent in markets such as solar energy and aviation, as well as FDA Class III medical. Electronics in industrial markets typically must operate with minimal faults in harsh environments.

The Increasing Complexity of Safety Applications

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

The functional safety standard IEC 61508 and its automotive adaptation ISO 26262 are applied to ensure that electronic systems in general industry and automotive applications are completely safe. The IEC 61508 document defines four general Safety Integrity Levels (SILs) with SIL 4 denoting the most stringent safety level. The ISO document defines four Automotive Safety Integrity Levels (ASILs) with ASIL D denoting the most stringent safety level. Each level corresponds to a range of target likelihood of failures of a safety function.

There is no direct correlation between the SIL and ASIL levels, but the ISO 26262 takes the safety process and requirements to a deeper level. From the beginning of the design process, evidence must be collected to show that the product has been developed according to regulation standards. Any potential deviations that have been identified must be documented to ensure that adequate mitigation is in place. New tools have been developed to support this additional element to automotive quality assurance.

Figure 1: Functional Safety Standards Details

Standards Defined

IEC 61508	Generic industry standard, applicable to electrical/electronic/programmable electronic safety-related systems	
	Integrity levels	SIL 1, SIL 2, SIL 3, SIL 4
	Publication date	More than 10 years ago
ISO 26262	Automotive industry standard, adaptation of IEC 61508 for electronic systems in road vehicles	
	Integrity levels	ASILA, ASILB, ASILC, ASILD
	Publication date	Target end 2011

Level Comparison

No direct correlation for SIL and ASIL levels

SIL (IEC)	ASIL (ISO)
4	D
3	C
2	B
1	A

Failure Measures

IEC 61508

SIL	Random HWFR target
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-4}$

ISO 26262

ASIL	Random HWFR target
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

New Policy

- **Information** is more structured in IS0 26262
- **Concept of safety culture** exists in IS0 26262
- **Terminology** is well defined in ISO 26262 (safety plan, safety case, work products, confirmation measure, etc.)
- **Roles and responsibilities** are better defined in IS0 26262, (PM, safety manager)

Freescale Safety Foundation

Freescale is a leading supplier of safety solutions with a history of design experience in dual-core controller technology for safety-critical applications. Freescale has expertise in developing custom microcontrollers (MCUs) and analog companion devices for functional safety systems used in the automotive safety and chassis market and has shipped more than 60 million units of MCUs and 30 million analog companion devices for applications such as electronic stability control and anti-lock braking.

In 2008, Freescale began developing its latest family of 32-bit devices, Qorivva 56xx automotive MCUs based on Power Architecture® technology. The devices are designed specifically to address the requirements of the ISO 26262 safety standards that are being applied to the growing number of safety-critical systems in road vehicles.

Freescale's safety portfolio also includes market-leading sensing solutions that have been operating in safety applications for more than a decade. The first MEMS-based inertial sensors for automotive airbags were introduced by Freescale in 1996.

At the heart of Freescale's safety solutions is a focus on quality. From design to manufacturing, Freescale employs the ISO TS 16949 Certified Quality Management System as well as a zero defects methodology to help ensure our products meet the stringent demands of safety applications and standards in the automotive and industrial markets. We also focus on continuous improvement with process evaluation, assessments/audits and gap analyses to ensure processes are continually optimized.

Figure 2: Program Pillars

SafeAssure Functional Safety Program from Freescale

Building on the company's safety heritage and expertise, Freescale's **SafeAssure** functional safety program enables system designers to develop with confidence and more efficiently achieve their system-level design goals and compliance with the IEC 61508 and ISO 26262 requirements. 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**. 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 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, analog and power management integrated circuits (ICs) and sensors. Freescale's analog automotive solutions provide additional functionality (such as checking MCU timing, voltages and error management) that helps improve system robustness and simplify electronic control unit designs. Freescale's Qorivva 56xx automotive MCUs and PXS family of industrial MCUs based on Power Architecture technology are designed specifically to address the requirements of the IEC 61508 and ISO 26262 safety standards. A number of devices in this family are already sampling, with some in full production. The lead product in the automotive family, the MPC564xL MCU, targets steering and braking applications and features a dual-core architecture that can be operated in lockstep mode. The PXS20 device is leading the way in the industrial market, targeting various industrial functional safety applications including industrial automation and motor control.

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 developing a comprehensive set of automotive functional safety software deliverables, including AUTOSAR OS and associated microcontroller abstraction layer (MCAL) drivers, as well as core self-test capabilities. To enhance its safety software portfolio for the automotive and industrial markets, Freescale partners with leading third-party software providers to offer additional safety software solutions.

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's capabilities extend from customer-specific training and system design reviews regarding functional safety architecture to extensive safety documentation and technical support.

SAFE ASSURE™ by Freescale

To guide you to the right product for your design needs, look for the Freescale **SafeAssure** solutions mark. It designates hardware and software that can be used in functional safety applications and in system engineers' IEC/ISO-compliant systems. The mark indicates products whose implementation of functional safety technologies is truly optimal and are fully enabled to facilitate system-level design and functional safety standard compliance, including support for failure analysis, hardware and software integration.

Freescale Functional Safety Hardware Solutions—Micros and More

Functional safety systems rely not only on MCUs or microprocessors, but also companion power management devices and sensors. Freescale is one of the few companies able to offer the full spectrum of system solutions—and all three product classes are available within the **SafeAssure** program, simplifying system design and standards compliance.

Freescale's safety hardware concept focuses on detecting and mitigating single-point faults, latent faults and dependent faults. This is achieved through built-in safety features, including self-testing, monitoring and hardware-based redundancy in Freescale MCUs, power management ICs and sensors.

Figure 3: Built-in Safety Features

Microcontrollers	Analog and Power Management	Sensors
Lock-Step Cores	Voltage Monitors	Timing Checker
ECC on Memories	External Error Monitor	Digital Scan of Signal Chains
Redundant Functions	Advanced Watchdog	DSI3 and PSI5 Safety Data Links
Monitors	Built-in Self-Test	ECC on Memories
Built-in Self-Test		Triggered Self-Test
Fault Collection and Control		

Microcontroller Assurance

Freescale has developed many innovations in its MCUs for functional safety applications that have seen wider adoption in the marketplace, such as the fault control and collection unit, the coherent safe core mechanism (patented) and the self-checking analog-to-digital converter (ADC).

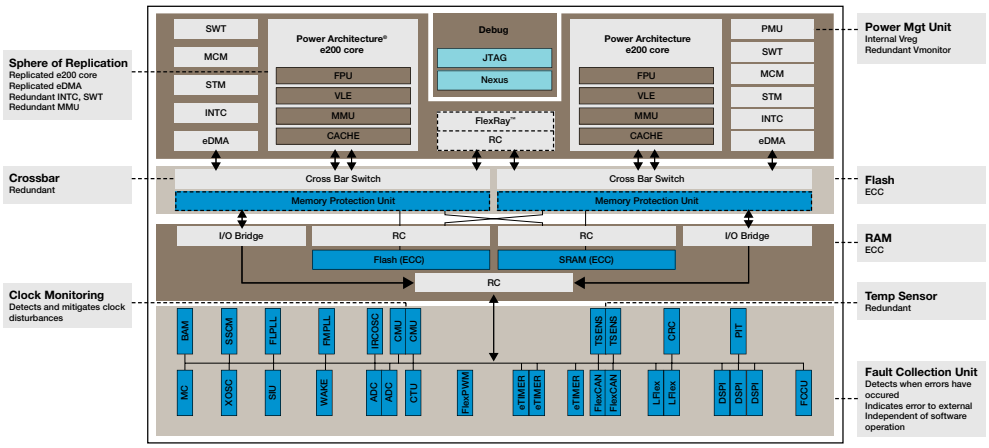
Additional Qorivva families of products have been introduced that target specific applications ranging from the single-core MPC560xP family used for airbag and ultrasonic park assist to true multicore high-performing advanced driver assistance systems (ADAS) with the MPC567xK family.

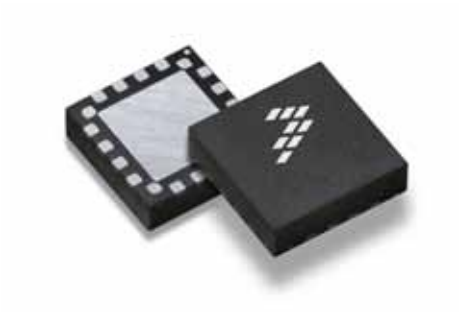
Freescale continues to develop lock-step (computational shell) based architecture products in next-generation technology nodes (55 nm and beyond), leveraging one of the strongest functional safety supplier legacies in the market today with an acute focus on airbag, steering, braking applications and the growing market of ADAS, power train applications, body controller applications and various industrial applications.

Freescale's extensive design experience in dual-core controller technology for safety-critical applications led to the development of two new 32-bit dual-core MCUs for safety-critical applications. They are the Qorivva MPC5643L, which specifically targets ISO 26262-compliant automotive applications, and the PXS20 for IEC 61508-compliant industrial applications.

The dual-core Qorivva MPC564xL and PXS20 contain 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 MPC564xL and PXS20 offer simplified system-level design, reducing complexity and development time, as well as ISO 26262-compliant automotive safety or IEC 61508-compliant industrial safety.

Figure 4: Qorriva MPC5643L Key Safety Features





Sensors for Safety

When a crash occurs, a vehicle rapidly decelerates while its structure absorbs the majority of the crash forces. Airbags supplement safety belts by reducing the chance that the occupant's head and upper body will strike some part of the vehicle's interior. They also help reduce the risk of serious injury by distributing crash forces more evenly across the occupant's body. From the onset of the crash, the entire deployment and inflation process takes only about 50 milliseconds, faster than the blink of an eye.

Because a vehicle changes speed so fast in a crash, MEMS sensors must detect the impact in a few milliseconds and airbags must inflate rapidly if they are to help reduce the risk of the occupant hitting the vehicle's interior. Freescale has several advanced Xtrinsic products that address the stringent requirements for airbag solutions, including the MEMS-based MMA5xxxW satellite crash accelerometers and the MEMS-based MMA68xxQ dual-axis crash sensors for the airbag ECU.

Freescale's Xtrinsic MMA5xxxW is the industry's first PSI5 X- or Z-axis satellite inertial sensor in a quad flat no-lead (QFN) package designed for a small footprint. The MMA5xxxW family enables small, robust front and side airbag satellite solutions and improved system reliability against parasitic vibrations due to Freescale's advanced overdamped transducer. Compatible with the PSI5 rev 1.3 standard protocol, these inertial sensors can easily be integrated as part of an overall PSI5 airbag system and include a bus-switch drive that simplifies daisy chain configurations.

The Xtrinsic MMA68xxQ digital inertial sensor family is designed as a main crash sensor or a safing sensor in airbag applications. The overdamped transducer coupled with a high resonant frequency package provides increased immunity to overload conditions induced by high-magnitude and high-frequency shocks encountered in crash detection applications. These features enable robust airbag designs.

Safety Companion: Analog and Power Management

To support a total system solution for functional safety applications, a class of companion power system basis chips (SBCs) with integrated safety measures matching the Freescale microcontroller families and combining both safety monitor role for the MCU and power supply generation has been developed and is available on the market.

Freescale's MC33789 SBC is a mixed-signal analog IC for airbag safety applications. The MC33789 SBC provides a flexible system IC solution partitioning across the range of airbag partitions used in cars and trucks. In order to protect vehicle occupants, the MC33789 includes a safing state machine to prevent unexpected events and enhance system functional safety. The safing concept involves the utilization of logic, independent of the MCU, to monitor both on-board

and remote satellite sensors and determine if a sufficient inertial activity is present to warrant deployment arming of the system. An on-board analog sensor self-test is often used to verify functionality and the connection between the sensor and the MCU. To facilitate the test without activation of the arming airbag outputs due to the possiblity of fault, the MC33789 SBC monitors the analog sensor self-test control signal from the MCU. It can be used to detect seat belt switch input states and communicate with remote crash sensors via new PSI5 master interfaces to meet industry standards. Allowing scalability across a wide range of firing loops while providing enhanced safety and system reliability, the MC33789 SBC is well suited for low- to high-end airbag safety systems.

Figure 5: Freescale's SafeAssure Hardware Solutions

Target Market	Product Type	Product	Target Applications
Automotive	MCU	Qorivva MPC567xK	Advanced Driver Assistance Systems (ADAS)
		Qorivva MPC564xL	Electronic Power Steering Electronic Stability Control ADAS
		Qorivva MPC560xP	Airbags Electronic Power Steering
	Analog and Power Management	MC33789	Airbags
	Sensors	Xtrinsic MMA16/26xx	Airbags
		Xtrinsic MMA51/52xx	Airbags
		Xtrinsic MMA65/68xx	Airbags
		Xtrinsic MMA69xx	Electronic Stability Control
Industrial	MCU	PXS20	Safety Shutdown Systems Solar Inverters, Motor Drives, Factory Automation, Aerospace Robotics
		PXS30	

Build Your Safety System Today

Designing safety-critical systems brings new challenges to the system designer: ensuring compliance with the IEC 61508 and ISO 26262 functional safety standards. Freescale's answer is the **SafeAssure** program, which covers how Freescale designs and implements a functional safety solution to our broad solution set, including MCUs, sensors and analog ICs along with our support of functional safety application design that extends to training, safety documentation and technical support. The **SafeAssure** program highlights selected solutions—including hardware and software—that are targeted for use in functional safety applications, enabling system designers to design with confidence and achieve their system-level design goals and standards compliance more efficiently.

How to Reach Us:

Home Page:
freescale.com

SafeAssure Program Information:
freescale.com/SafeAssure

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 Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447
303-675-2140
Fax: 303-675 2150
LDCForFreescaleSemiconductor@hibbertgroup.com

freescale™

For more information, visit freescale.com/SafeAssure

Document Number: FCTNLSFTYWP REV 0