Functional Safety
for Industrial Applications

freescale.com

freescale™

Designing for Safety

As functional safety is required in a continuously increasing amount of industrial applications, more companies are realizing the challenges associated with safety standard compliance. When designing a safety system, great value can be added by suppliers who understand the process and requirements that are needed to fulfill functional safety certification requirements. With an industry-leading quality and reliability foundation, deep automotive and appliance safety experience, vast resources for development and innovation, and strategic alliances with third-party experts, Freescale is the optimal choice for functional safety. Freescale offers hardware, software, development tools and documentation to provide a complete solution for your functional safety application.

SafeAssure

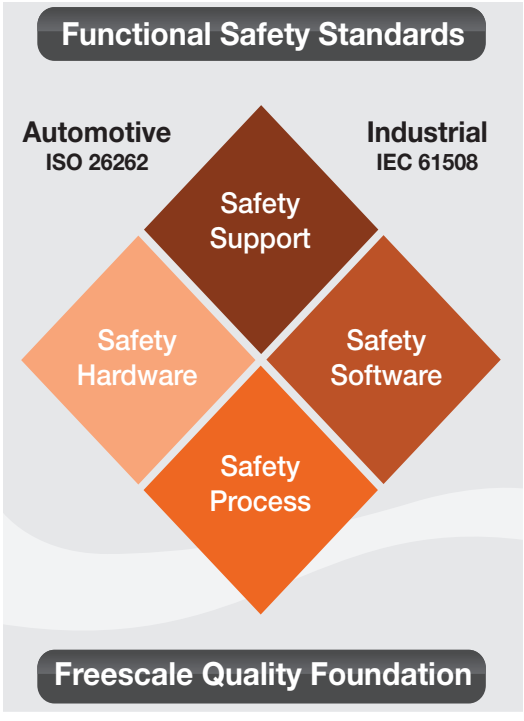
Functional safety. Simplified.

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 (SIL), 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



SAFE ASSURE™ by Freescale

freescale.com/SafeAssure

Safety Process

Safety through quality

Applications

Process Industries:
Refineries, boilers, chemical, pharmaceutical

Factory Automation:
PLCs, I/O control

Machinery:
Elevators, lifts

Medical:
Ventilators and respirators, anesthesia machines, surgical robots, FDA Class III devices

Aviation and Defense:
Safety-critical flight systems

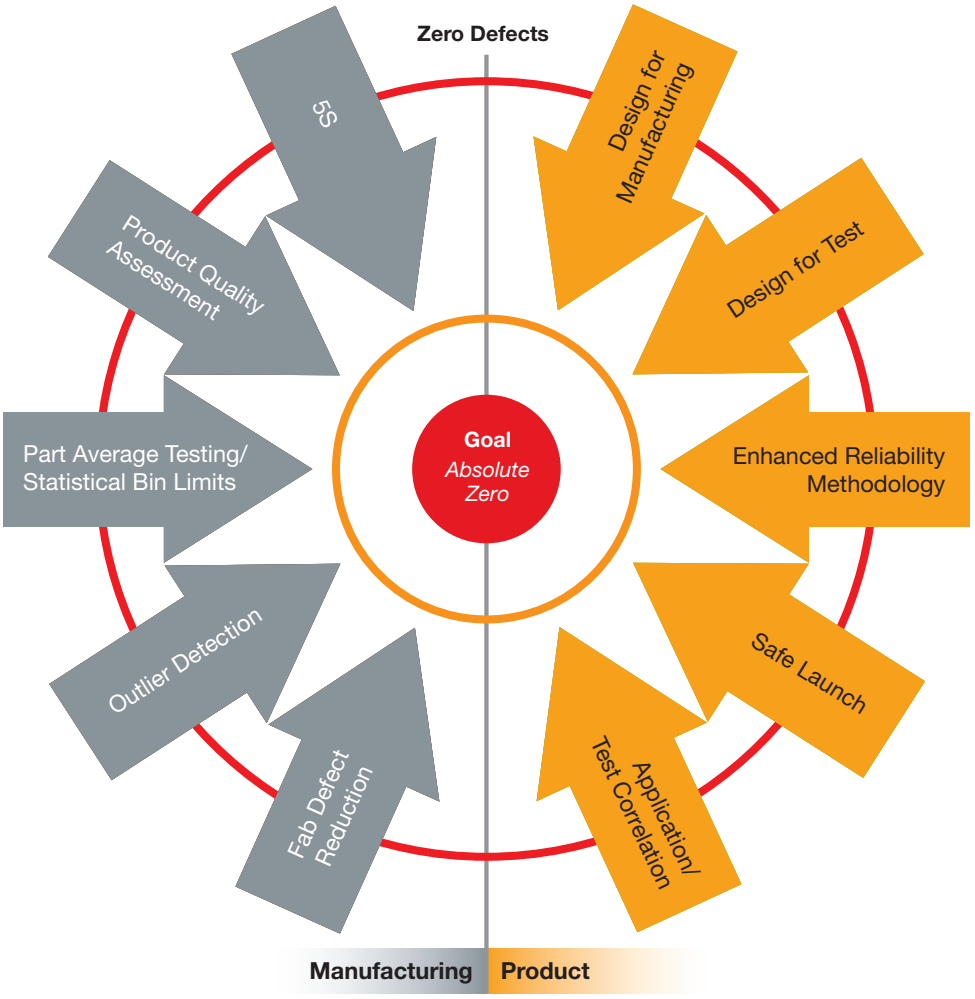
Industrial Transportation:
Rail, tractors, heavy machinery

Energy:
Power plants, wind, nuclear

Quality Processes

Strategies	Initiatives
Customer PPM and Incident Reduction	• Customer centric quality metrics • NPI problem parts containment/corrective action focus
Flawless New Product Introductions	• Technology certification/design robustness • Advanced test methodologies • Safety project manager
Quality Culture	• ISO/TS quality systems process excellence • Revitalizing 6 Sigma problem solving and continuous improvement

Zero Defect Methodology



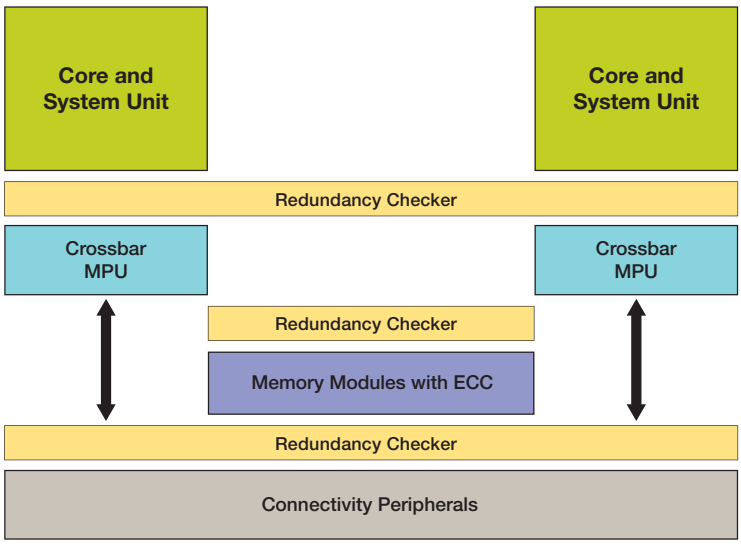
Safety Hardware

The PXS family

The PXS family of 32-bit Power Architecture® dual-core MCUs specifically targets industrial functional safety applications, including process industries, machinery, medical, aviation, power and industrial transportation.

All devices in this family are built around a dual-core safety platform with an innovative safety concept targeting systems with IEC61508 and SIL3 safety integrity levels. In order to minimize additional software and module level features, on-chip redundancy is offered for the critical components of the MCU. These include the 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. Lock step redundancy checking units are implemented at each output of the sphere of replication (SoR). The SoR allows for reduction of software safety checks, which simplifies the software and results in decreased functional safety certification efforts. With over 600 DMIPs of performance possible and up to 2 MB of on-chip flash memory, the PXS family can handle even complex safety controls.

PXS Family Sphere of Replication



Advantages of Single-Chip Dual-Core Safety Solutions

- Easier system-level certification
- 40 times more checks per cycle
- Simplified design and maintenance with only one software image
- Decreased debug complexity
- >99 percent diagnostic coverage of the cores

Features

- Dual processing spheres, including CPU, DMA, interrupt controller, crossbar and MPU
- Dual CPU architecture provides performance needed to address real-time applications and cross-checking functions common in many safety strategies, reducing hardware and software complexity required for multiple MCU designs. Architecture can be run in two statically configurable modes of operation
- Fault collection and control unit manages MCU behavior in the event of internal MCU logic faults and signals these to external system components
- Key functional safety features on a single chip reduces design complexity and component count
- Built-in flexible hardware self-test capabilities provide diagnostic coverage both at logic and memory level

PXS Family Portfolio (Temperature Range: -40°C to +105°C: Select Parts +125°C)

Product Number	Speed	Flash/RAM	Package
MPXS2005VLQ80	80 MHz	512 KB/128 KB	144 LQFP
MPXS2010VLQ80	80 MHz	1 MB/128 KB	144 LQFP
MPXS2010VLQ120	120 MHz	1 MB/128 KB	144 LQFP
MPXS2010VMM80	80 MHz	1 MB/128 KB	257 MAPBGA
MPXS2010VMM120	120 MHz	1 MB/128 KB	257 MAPBGA
MPXS3010VMM150	150 MHz	1 MB/256 KB	257 MAPBGA
MPXS3015VMS180	180 MHz	1.5 MB/384 KB	473 MAPBGA
MPXS3020VMS180	180 MHz	2 MB/512 KB	473 MAPBGA

Safety Software and Support

Partners and tools

Freescale is partnering with industry-leading software providers to offer a complete suite of software, including a safety-certified RTOS and tool chains to system level code generation and functional safety project management software.

Green Hills Platform for Industrial Safety

For customers seeking the highest levels of software safety, security and reliability in industrial, railway, medical, automotive, IT security or aerospace, Green Hills offers various platform solutions of pre-certified software with trusted advisor services.

One of these solutions, the Green Hills Platform for Industrial Safety, provides a complete cost-effective, end-to-end risk-managed product development solution covering every aspect of the product development life cycle from product and certification planning, training, architectural roadmap and full system development to final certification of safety levels IEC/EN 61508 SIL3 (industrial) or CENLEC EN 50128 SWIL4 (railway).

The Green Hills solution incorporates the following pre-integrated components to help you increase productivity and drastically reduce product cost, risk and time to market:

- Off-the-shelf INTEGRITY real-time OS, pre-certified to SIL3/SIL4
- Integrated OS middleware
- Highly integrated development and verification tool set for all phases of the software life cycle, including software changes
- Trusted Advisor system/software consulting, safety BSP development and certification support services

SCIOPTA

SCIOPTA Systems develops, sells, supports and maintains systems software for safety-critical applications. This includes real-time OS, network software, file systems, software for interface bus systems, and board support packages. SCIOPTA is a message-based real-time OS with many built-in safety functions. SCIOPTA is certified by TÜV to IEC61508 at Safety Integrity Level 3.

SCIOPTA includes high-value diagnostic test functions for all kernel internal data. Internal data is stored twice, normal and inverted, and validated at every read operation. A DC of 99.2 percent has been achieved. The same techniques are offered for user data by providing safe data type functions. However, SCIOPTA is more than just as an RTOS, and offers a new and modern approach to designing embedded systems. The direct message passing method allows easy and efficient design of robust and secure systems. Applications based on the SCIOPTA method can cover small static SoC designs to large dynamic systems.

LDRA

LDRA specializes in providing software standards certification solutions which automate requirement-based software verification, source code analysis, run time error prevention and test management. LDRA covers the full embedded software development life cycle from requirements engineering to testing on the target.

Safety Certification Kit

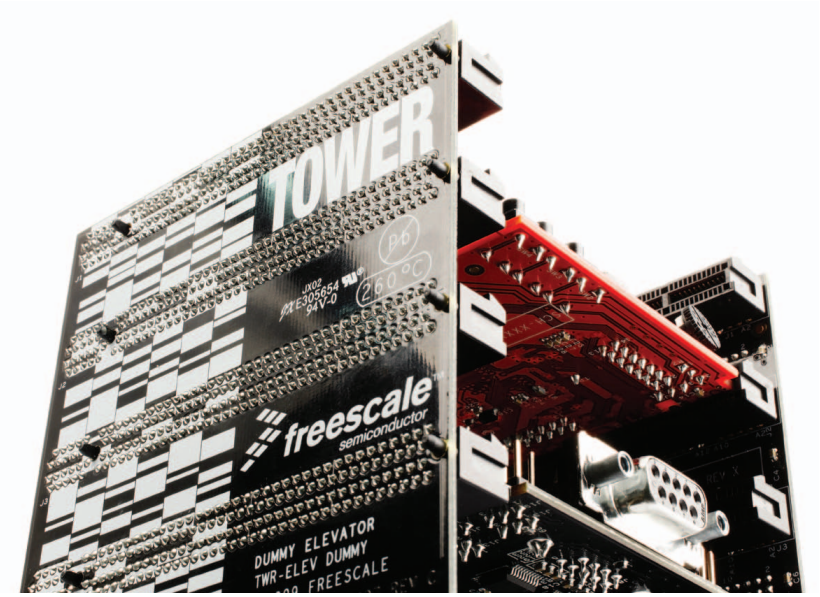
Collateral	Purpose
Safety Manual	• Shows how to use hardware and software features to maximize device functional safety potential
Failure Mode, Effects and Diagnostic Analysis	• Accurate product failure metrics • Dynamic and customizable: Calculates product-level failure rates
Failures in Time Report	• Low FIT rate reflects high quality and proves low part failure rates needed for functional safety

Freescale Support

Software and tools

MQX™ Software Solutions

Accelerate your design success with complimentary RTOS, TCP/IP and USB stacks provided by MQX software solutions. Available on Freescale processors for more than 15 years, MQX software solutions offer a straightforward API with a modular architecture, making it simple to fine tune custom applications and offering scalability to fit most requirements. The combination of our market-proven Freescale MQX software solutions and silicon portfolio provides a streamlined, powerful platform by creating a comprehensive source for hardware, software, tools and services needs.



RAppID

Our graphical development tool for the PX family enables the user to quickly and easily configure the controller, plus generate complete documentation. It can also be used as a learning tool to gain an understanding of the controller and its peripherals. RAppID not only generates C code for initializing the registers, but also provides a system initialization function that brings the controller up in an orderly sequence. Use RAppID to save time and become an expert on the PX series.

FreeMaster

FreeMASTER is a user-friendly real-time debug monitor and data visualization tool for application development and information management. FreeMASTER supports completely non-intrusive monitoring of variables on a running system. The data is then displayed as multiple variables changing over time on an oscilloscope-like display, or in traditional text form. FreeMASTER also supports additional capabilities and targets with an on-target driver for transmitting data from the target to the host computer.

Tower System

The Tower System is a modular development platform for 8-, 16- and 32-bit MCUs and MPUs that enables advanced embedded development through rapid evaluation and prototyping. Featuring multiple development boards or modules, the Tower System provides designers with building blocks for entry-level to advanced application development.

Motor Control Development Toolbox

The motor control development toolbox includes Mathworks Simulink plug-in libraries which provide controls engineers with an integrated environment and toolchain for configuring and generating all the necessary software, including initialization routines, device drivers, and a real-time scheduler, to execute motor control algorithms on any PXS hardware platform. The toolbox includes the automotive math and motor control library set developed by Freescale's renowned Motor Control Center of Excellence. The motor control library includes dozens of blocks optimized for fast execution on Freescale MCUs. The results are bit-accurate and comparable to a Simulink simulation using single-precision math.

freescale™ MQX

RAppID

SAFE ASSURE™
by Freescale

Learn more at freescale.com/PXseries
and freescale.com/SafeAssure

Document Number: BRFNCSFTYIND REV 0

BUILT ON Power™

freescale™