White Paper

Managing Machine Safety and Productivity with QorIQ Multicore Processors

By John Ralston, Industrial System Architect

Table of Contents

Abstract

In most parts of the world there is now legislation which defines the common minimum requirements for health and safety of work equipment and machinery. In the European Union (EU) this is encompassed in the “Machine Directive,” which has been enacted in all members’ countries laws.

These directives represent the mandate with which all new work equipment must comply in terms of design and construction before it can be deployed. This ensures that the equipment can be used safely and without harm.

While the legislation covers the complete system, the sensors, the programmable logic control function and the actuation sub-systems, this paper focuses on the control sub-system. We will review the impact of the safety requirements on the control sub-system architecture, and make a proposal based on QorIQ multicore processors that not only addresses safety, but also helps maintain or improve machine productivity.

Introduction

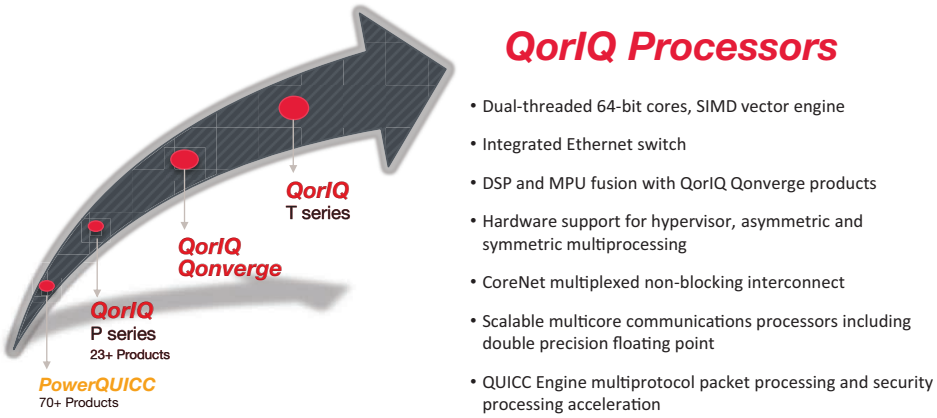
In North America and Europe, the UL or CE marks are probably familiar sights in most households. Less widely known is what these marks stand for and the stringent process that manufacturers must follow to qualify for those marks.

A key motivation behind these stringent processes is safety, which applies to equipment or machinery ranging from handheld power tools, elevators, railway systems and robots on the factory floor to nuclear, oil or gas installations. Safety is paramount in the latter group, but similar care and attention are also given to equipment that people use on a daily basis.

The objective behind what the industry calls “functional safety” is to remove any risk of physical injury or impact on health to people operating or using equipment or machinery. Not only must equipment operate correctly in response to its inputs, but it must also safely manage any operator errors, hardware failures or environmental changes.

While functional safety covers the end-to-end system, for the sensors, the programmable logic control function and the actuation sub-systems, we focus on the control sub-system. This paper covers the functional safety impact on the control sub-system architecture, and how a QorIQ multicore processing solution can address safety requirements more efficiently by improving machine productivity.

Figure 1: QorIQ Platform: Built for Performance, Reliability and High-Availability



QorIQ Processor Benefits

For product specific information on QorIQ P and T series processors, visit **freescale.com/QorIQ**.

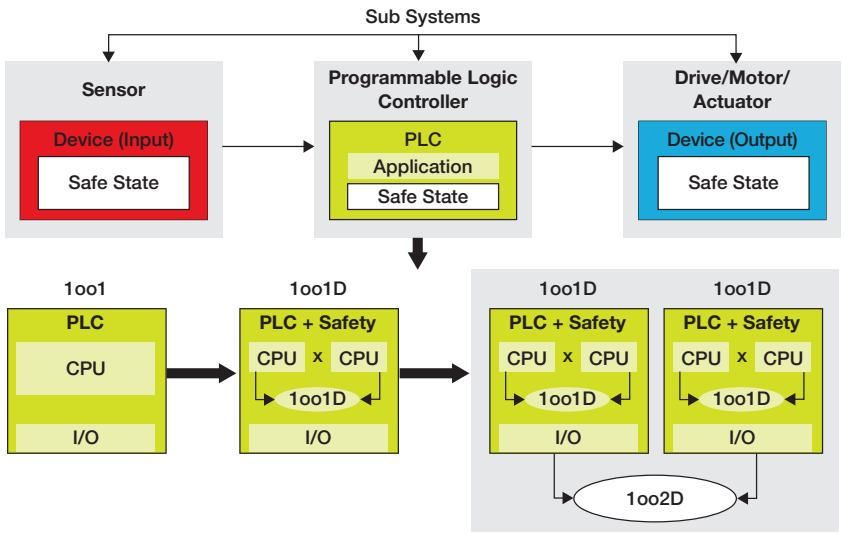
For advanced information on QorIQ Layerscape Architecture, visit **freescale.com/Layerscape** and read the “Layerscape Architecture, A Look Inside the Next-Generation QorIQ LS Series SoCs” white paper under the “Read More” section. Layerscape architecture is an evolution of the QorIQ P and T series processors—an infrastructure that supports sharing networking interfaces and accelerators by multiple CPUs, both Power Architecture® and ARM® cores, and the accelerators themselves.

Making Machines Safe

The standards covering functional safety are specified by the governing bodies in each country. For EU countries, the baseline is IEC 61508. In North America, the ISO specification ISO 13849 is enforced. The process of achieving certification involves a number of steps that identify the required safety functions, potential hazards and any risk-reduction required. This goes towards identifying the required safety integrity level (SIL). Other key factors in the process include the hardware fault tolerance (HFT, the number of faults that can be tolerated) and the safe failure fraction (SFF, the probability of the system failing in a safe state). The responsibility for these aspects lies with appropriately skilled engineers who, like the standards, have to take a holistic system approach. In this paper we will focus on the programmable control sub-system.

The HFT and SFF are significant in that they are a measure of the redundancy and diagnostic capabilities of the sub-system. The HFT depends on the amount of redundancy and voting policy used in the system. The SFF is a measure of the fail safe design and quality of the built-in diagnostics.

Figure 2: Safety and Productivity



Making a system safe requires additional processing performance and additional/duplicate hardware resources.

Figure 2 shows a dual-redundant system with one of two voting architecture and diagnostics (1oo2D). 1oo2D means two channels will process the same inputs and request a certain action. The voter will compare the request from both channels but only use the data from the channel with good diagnostics.

The diagnostics will report on software or random failures, incorrect operator inputs or common cause failures arising from environmental impact (a memory or data bus corruption caused by EMC, vibration, temperature or pressure changes). Making systems safe requires additional processing performance to deliver real-time computation and diagnostics. Duplicating hardware resources provides the system redundancy necessary to increase the probability of the system achieving a safe state in the event of a failure.

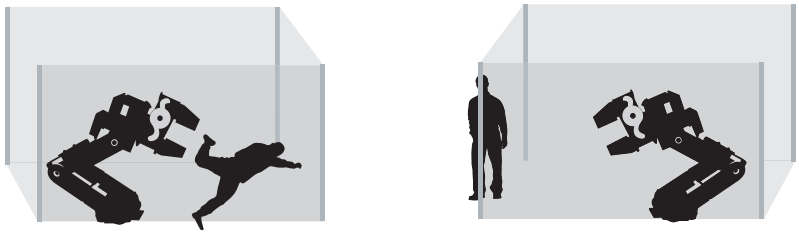
Redundancy and Real-Time Diagnostics

Herein lies the challenge for equipment or machine manufacturers: Adding redundancy has a direct impact on hardware costs, as it traditionally involves replicating controller modules or processor components.

- Can functional safety be provided without the replication of hardware?
- Can smarter and more integrated diagnostics help manage functional safety and productivity at the same time?

To illustrate the second question a little more, consider a robot on an assembly line. The robot is protected by light curtains.

Figure 3: Shut Down Versus Slow Down



a) Has fallen into the protected area

b) Has accidentally broken the light circuit without entering the protected area

There is a clear difference between figure 3a) and figure 3b). The first illustrates an incident where an operator is at risk of injury and the robot should de-energise or stop. This is not the case in the second illustration, where perhaps slowing the robot down would be sufficient. A system that can differentiate will improve productivity since it can maintain safety but also keep the production line going. In this situation an additional light curtain could be used to designate a ”buffer” zone and an ”operational” zone. A vision-based system might be the answer. In both cases there are now additional sensor inputs to be considered by the controller, and additional processing to be performed in real time.

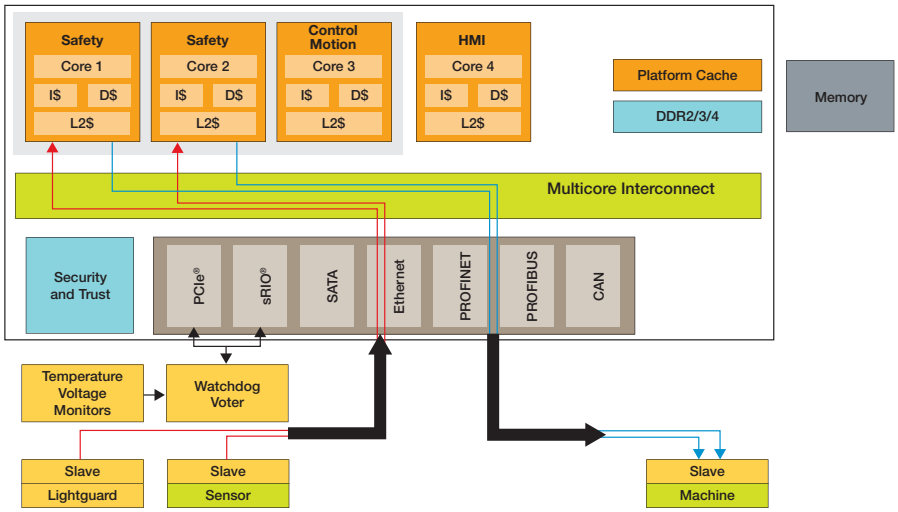
Solutions Based on QorIQ Multicore Processors

Part of the solution to both questions lies with QorIQ multicore processors, a family of multicore processing platforms ranging from single-, dual- and quad-core to multicore, all based on 32- or 64-bit Power Architecture cores that include integrated double precision floating point. The QorIQ multicore processing platform was designed for markets like telecommunications, enterprise and data center, as well as industrial where reliability and high availability are key. Design features at the core, interconnect, I/O and memory sub-architecture levels are as equally relevant to this discussion as they are those other markets.

Figure 4 shows how the programmable control and safety functions could co-exist on a single QorIQ multicore processor. The different functions can run on this architecture using shared or dedicated interconnect, memory and I/O resources. The hardware enforcement allows the difference functions to run without interference from other functions on other cores or on external hosts. The table that follows highlights each of the specific hardware features that make this possible.

This approach allows for consolidation of components or modules and the integration enables improved diagnostic capabilities, which can in turn support better machine availability or productivity.

Figure 4: Functional Mapping to QorIQ Multicore Processor



QorIQ Features and Benefits

The QorIQ series of control/communications processors provides flexible and scalable performance options ranging from single-, dual- and quad-core to multicore all based on 32- or 64-bit Power Architecture cores and including integrated double precision floating-point for motion control. The CoreNet multicore interconnect enables the processor cores and I/O controllers to maintain their workloads without interference. A wide range of I/O options are available, ranging from PROFIBUS (integrated PROFIBUS L2/FDL) via QUICC Engine, a range of serial interfaces (UART, SPI, I^2C, UART) and high-speed connectivity via Ethernet, PCI Express® and SRIO®. Extensive use of ECC and parity help maintain reliability while the security acceleration and trust architecture provide mechanisms to protect against misuse of equipment or theft of intellectual property.

For additional information on this specific topic and QorIQ multicore processors for industrial automation, please contact **john.ralston@freescale.com**.

Features and Benefits

	Feature	Benefit
Core	Parity and ECC	Provides ability to detect errors and with ECC correct single bit errors
	Integer and floating point (SP/DP)	For logic and motion control algorithms
	Supports three operating modes: User, supervisor and hypervisor	Supports symmetric and asymmetric multiprocessing with protected partitioning and vitalization
	Dedicated watchdog timer	Each core has its own watchdog
	Dedicated clock source and PLL	Each core has its own clock source
	Lock lines in L2 cache	Can operate as a local SRAM
	Dedicated or shared exception model	Each core can be programmed to manage or ignore exception events as required
Multicore Interconnect (CoreNet)	A multiplexed fabric (not a bus or ring)	• A non-blocking interconnect. Provides protected point-point connections between cores and memory or I/O resources. • Provides platform coherency and protection from incorrect memory transactions by peripherals and cores
	Provides the coherency in the system on a domain basis	
	Peripheral access management units (PAMU) protect against unauthorized write access by other internal/external masters	
	Large memory arrays protected by ECC/parity	
Memory L3 Platform Cache	Parity on control bits and ECC on data bits	Provides ability to correct single-bit errors and detect dual-bit errors
	Can be configured as SRAM	Can be configured as SRAM. Memory segregation protected by MMU, PAMU and CoreNet
Memory External DRAM	Parity on control bits and ECC on Data bits	Provides ability to correct single bit errors and detect dual-bit errors
I/O	QUICC engine	Offloads Ethernet-, HDLC- and UART- (PROFIBUS) based L2 processing Validates (e.g. CRC) frame prior to delivery to core
	Ethernet: Frame manager*	Offloads Ethernet based L2-L4 parsing. Validates (eg CRC) frame prior to delivery to core
	Ethernet: Queue manager*	Supports distribution of Ethernet frames to targeted cores
	Ethernet: Buffer manager*	Hardware buffer allocation and de-allocation
	PCIe/SRIO*	High-speed/bandwidth interfacing
	Security*	Cryptographic acceleration and trusted boot

*PAMU protection (see Multicore Interconnect section of table)

Support

Visit **freescale.com/support** for a list of phone numbers within your region.

For more product information on QorIQ multicore processors, please visit freescale.com/QorIQ

For more information on functional safety for industrial applications and Freescale solutions, please visit freescale.com/safeassure

Document Number: MACHSAFETYPRODWP REV 0