Intelligent functional safety concept saves design time and costs

By Manfred Choutka, Infineon Technologies

The PRO-SIL SafeTCore package is a complete solution, including optimized semiconductors like the TriCore and XC2300 microcontrollers, safety and test software libraries, services and related documentation, and paves the way to a successful functional safety certification.

Figure 1. The 32-bit SafeTkit is the heart of an ASIL-D/SIL3 capable platform in an easy-to-configure and easy-to-use format. It is based on a TriCore evaluation board with the safety monitor chip CIC61508 and the SafeTcore test library.

Engineers are striving to achieve 100% fail-safe systems, but this utopia is very difficult to realize in practical implementations and a cost-effective way. Therefore a probabilistic and risk-based approach is normally adopted to define the level of functional safety required for safety-relevant systems, as in standards like ISO 26262 and IEC 61508. These standards define the (automotive) safety integrity levels (ASIL/SIL) which specify which attributes of a system have to be observed, and the degree of rigor of the engineering process that must be applied, to achieve the related certification of a system. This includes a safety concept defining the safety goals of the system and the tolerable error rate, followed by a safety architecture which distributes the functions into hardware and software functionality that constantly verify that the system is running correctly. Traditionally the safety software, hardware and tools were only island solutions, solving parts of the requirements but in a disjointed way. However there is now an integrated PRO-SIL concept which offers a complete solution to achieve functional safety in an efficient and integrated manner, minimize risk, save cost and reduce complexity.

The fundamental motivation for the development of safe systems is to ensure a safe operation and defined behavior in the event of defects. Against this background, the IEC 61508 standard was developed in the mid-1980s, and since then repeatedly revised. This standard defines the design of safe systems for electrical and electronic devices. Furthermore, derivatives of this general standard have been developed for the specific demands of process automation (IEC 61511), machinery automation (ISO 13849), drives (IEC 61800-5), nuclear (IEC 61513) and automotive (ISO 26262 draft). The measures to ensure IEC 61508 compliance depend upon the required safety integrity level for each hazard in the system (SIL 1 up to SIL 4 for automation applications and ASIL A to ASIL D for automotive applications).

In the last couple of years functional safety has moved from a system integrator's task to the component/software level. Simple electronic components as well as complex microcontrollers have to support IEC 61508. One of the most important and often time-consuming challenges for system designers is the requirement to ensure the safety of systems, and get the related certifications not only at the top level but also deep down in the hardware and registers of the machine. The IEC 61508 prescribes detailed requirements for hardware supervision and testing, which by its very nature is very hardware-specific. Writing safety-critical software to perform these functions is therefore time-consuming and expensive, and is not easily portable between devices.

With a single-channel architecture using one microcontroller the maximum safety integrity level was limited to SIL 2. Therefore SIL 3 or ASIL C/D systems and safety products were designed using multiple CPUs, to take care of the self-testing and ensure redundancy. But this is a complex and costly solution with a large PCB footprint, and coverage limited by synchronization and communication issues between the two CPUs. A new approach is to go beyond the limits of the stated medium diagnostic coverage (DC) by adding special external hardware blocks, and using a software library running on a standard dual-core 32-bit microcontroller. This solution makes the inclusion of safety in a related system fast and reliable, by reducing development effort and material costs to only one microcontroller, and using an intelligent safety concept with all related components including ready-to-use self-test functions developed according to IEC61508 / ISO26262.

Instead of using a second external core, to evaluate functional failures of the microcontroller, the TriCore already includes two cores - the TriCore CPU itself (microcontroller and DSP) and the peripheral control pocessor (PCP) - making the external second core for safety evaluation obsolete. There are already different solutions on the market to implement safety-critical applications. While most leading

Safety Integrity Level	High demand rate (Dangerous failures/hr)	Low demand rate (Probability of failures on demand)
SIL 4	$\geq 10^{-9}$ to 10^{-8}	$\geq 10^{-5}$ to 10^{-4}
SIL 3	$\geq 10^{-8}$ to 10^{-7}	$\geq 10^{-4}$ to 10^{-3}
SIL 2	$\geq 10^{-7}$ to 10^{-6}	$\geq 10^{-3}$ to 10^{-2}
SIL 1	$\geq 10^{-6}$ to 10^{-5}	$\geq 10^{-2}$ to 10^{-1}

Table 1. Safety integrity levels specifying what has to be observed to achieve the safety certification of a system according to IEC 61508 or ISO 26262

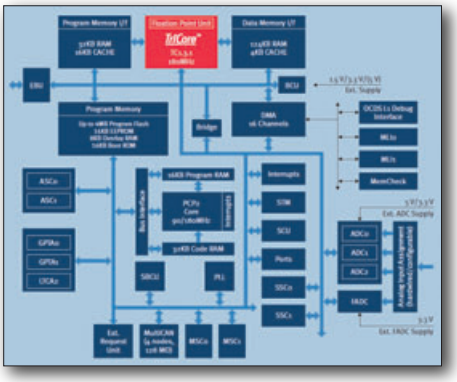

Figure 2. TriCore block diagram – the PCP implements self-test functions.

vendors offer related approaches for automotive applications, the availability to other application areas including industrial is constrained and the available device roadmaps are often limited. Leveraging its significant experience with the stringent safety requirements of automotive systems, Infineon has developed its PRO-SIL range of safety products to address the increasing needs of the industrial market with highly integrated safety solutions. The proven automotive solution is easily accessible for other applications, while a broad range of devices is offered. The PRO-SIL implementation is based on its 32-bit TriCore or 16-bit XC2300 microcontrollers and additionally includes the SafeTcore test library and the safety monitor chip, CIC61508. This fully verified implementation is in full compliance with the requirements according to IEC 61508.

The two most common types of safety control architectures are single channel (1oo1 or 1 out of 1) or dual channel (1oo2 or 1 out of 2) structures, with the latter based on two separate processing units. A 1oo1 structure provides cost-effective solutions with a safety integrity rating limited to SIL 2. The dual architecture (1oo2) enables high safety integrity to a rating of SIL 3 - but at higher cost and the need for more board space. The safety architecture used in the PRO-SIL concept is a 1oo1 structure with intelligent diagnosis (1oo1D).

The innovative safety concept is based on a challenge-response technique, while the PCP on the TriCore chip operates as the challenger and the main TriCore CPU executes the tests. Information is passed through a shared memory structure, while the data is kept diverse and redundant. Self-test functions are implemented on the PCP and this is additionally monitored by an external intelligent watchdog (CIC61508) which is connected to the TriCore chip via the SPI. The watchdog device is an effective measure to minimize common cause failures. The watchdog communicates with the TriCore chip in specified timing windows to check the clock, voltages and correct operation of the TriCore chip as defined in the standards. On the other side the TriCore monitors the power supply of the CIC 61508 and monitors it for correct operation via remote diagnostic measures. Error detection (hardware failure and task monitoring) is shared between the main TriCore CPU and the PCP.

The PCP software contains the PCP self test, the C/R (challenge/response) communication, the watchdog communication, a test execution monitor and a task monitor. The SafeTcore library running on the TriCore is a configurable framework that offers test functions to validate the processor and system integrity. Most of these tests are implemented so that they can run at the start time but also at runtime in the background. The typical diagnostic interval time is 6.4ms. The most complex test is the TriCore CPU self test. Using the innovative safety concept an overall diagnostic coverage of 96.5% for this opcode-based self test can be reached, which is significantly better compared to other instruction set tests and has the benefit of being interruptible and of low latency.

The SafeTcore package provides the tools to accomplish two things in parallel - a required certification from SIL1 - SIL3 (or ASIL B - D) and a demanding time-to-market schedule. The biggest challenges for certification are to achieve the required tests on the silicon level and to have the documentation to back up the safety case. The SafeTcore package delivers this through a highly-configurable driver library for the TriCore family of devices, combined with the availability of a full set of safety manuals, safety cases and requirements/traceability databases. By using the SafeTcore set of powerful self-test routines that run on the PCP both at startup and cyclically from within an application, the correct operation of the user software and the TriCore CPU itself can be verified and proven.

The core test features are combined with detailed peripheral tests and automatic support for the safety monitor chip. The set of software tests in the SafeTcore library also provides an operating system monitoring functionality to perform complex task and process flow monitoring, which enables a safe execution of code with diagnostic coverage of more than 99 percent. The SafeTcore package also includes a

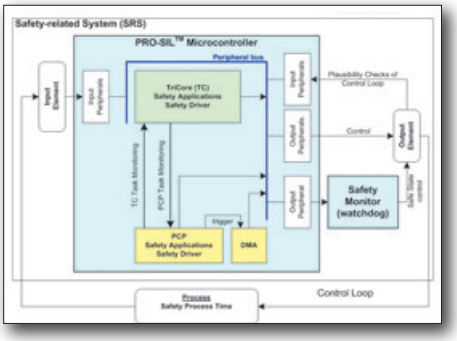

Figure 3. A safety-related system using a TriCore as the main controller

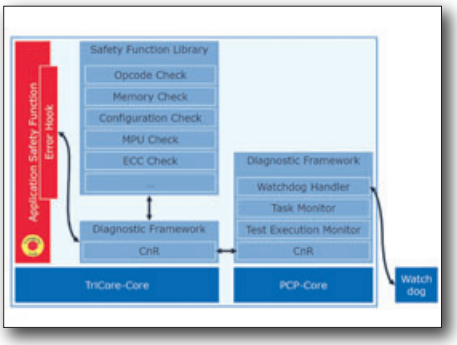

Figure 4. SafeTcore software partitioning

safety manual for the integration of the various library elements into the user application and the approval of the safety integrity level.

The CIC61508 can be integrated into various functional safety-relevant applications. The watchdog monitors the main microcontroller (e.g. TriCore chip) by providing features to detect common failure modes of clock, power supply and temperature which may lead to computational errors on the microcontroller. Thanks to its small TSSOP-38 footprint, the CIC61508 is a space-saving and cost-effective option for supporting safety applications. In a safety-related system using a TriCore MCU, the TriCore main core runs the SafeTcore test software with core and peripherals test, while the PCP monitors the TriCore main core. The CIC61508 external watchdog monitors both cores to identify common causes of failure. As the PCP has already implemented various self-test functions, the TriCore/CIC61508 combination needs only a subset of the functionality offered by the CIC61508.

The test features supported by the CIC61508 are stored in its ROM and include an internal opcode test scheduler/sequencer, which generates a sequence of test requests with specific data and checks the response against a user defined table. Other monitoring functions include the capability of detecting undervoltage and overvoltage in up to four power domains, the capability to monitor up to eight parallel data comparisons and verification functions, and an operating system task monitor to check the predefined dispatch sequence and execution budgets of all safety-critical tasks.

The PRO-SIL concept is based on the asymmetric dual-core architecture of the TriCore with an external watchdog as supervisor. Hardware features are combined with diagnostic software library, while the integrator can be free to focus on the application measures that are normally required. The concept supports IEC 61508 safety-related systems up to SIL 3. Industry acceptance is not only shown by the Embedded Award 2011 for the SafeTkit offered by Hitex, but also by the positive feedback from key accounts like Parker Hannifin, which successfully used the innovative safety package to design their latest safety products.

Parker Hannifin used the PRO-SIL concept for the development of an innovative new programmable hydraulics controller for use by OEMs and system integrators for the development of mobile and off-highway equipment. The design is based on a TC1197 and the complexity can be expressed by the following figures which faced the developers to create the IQAN-MC3: 687 design requirements: 674 lines of failure analysis in FMEDA, 2800 software and more than 500 hardware tests. Based on the PRO-SIL concept the company was able to finalize the complex design in a fast and secure manner. The new IQAN-MC3 enables both safety and operational functions to be controlled from a single module. This allows system design times and costs to be reduced significantly, while at the same time improving machine performance, safety and productivity.

The launch of the new controller coincides with growing demand from manufacturers of mobile and off-highway equipment for components and software, used in the production and development of safety systems, to offer improved performance and be certified to accepted functional safety standards, such as EN ISO 13849-1 (machinery directive) or IEC 61508. To make this possible, the IQAN-MC3 was designed to IEC 61508 using the PRO-SIL products and effectively enables the operation and performance level of all safety functions to be proven as part of a SIL2 methodology, or to be used as part of a PLD subsystem within EN ISO 13849-1.

A comprehensive service package is available in partnership with Hitex. The SafeTkit is a board-level solution which includes the TriCore MCU, CIC61508 and all relevant software and documentation. The complete safety solution makes it as easy as possible to certify applications in compliance with IEC61508 while saving design resources and reducing the time-to-market for the customers. The SafeTkit is based on a TriCore evaluation board with the safety monitor chip CIC61508. Besides the SafeTcore test library the supplied software package contains a complete tool chain including a free general-purpose TriCore compiler, a safety demonstration application and a test bench.

A comprehensive set of documentation including safety manuals and a quick-start guide complete the safety kit. All the major safety features are available and can be reconfigured to assess their effect on system behavior and gain an understanding of the concepts underlying them. SafeTcore test library and documentation for certification are currently available for the TC1767, TC1782, TC1797 and TC1387 processors and will shortly also be available for additional TriCore and XC2300 derivates. In addition Hitex provide comprehensive design support and offers related trainings and consulting services. ■

Name	Description	Name	Description
BCU	Bus control check	MPU	Memory Protection check
Boot ROM	Boot code integrity check	PCP CRC	PCP SafeTcore integrity check
CAN	CAN check	PCP ISR	PCP interrupt routine priorities
CAN LLC	CAN Link Layer Controller	PCP Protection	PCP memory access protection
Core SFR	CPU SFR configuration check	RAM	RAM check
DMA	DMA check	RAM	RAM Protection check
ECC Flash	ECC Flash check	SBST	Opcode test
ECC LMB	ECC system on LMB bus	SFR	Peripheral SFR check
ECC MultiCAN	ECC check MultiCAN RAM	Trap	Trap system test
FLX	FlexRay check	Watchdog	Internal watchdog test
FLX RAM	FlexRay RAM	ASIC	Connectivity to ext. watchdog
ICACHE	Instruction Cache check	APPL ADDR	User Application Address test
ISR	Interrupt structure	APPL RAM	User Application RAM test
MEMCHK	CRC32 check	APPL ROM	User Application ROM test

Figure 5. SafeTcore startup and shutdown tests