Functional Safety has become an important topic not just in industrial machine building, but also in transportation, in passenger cars in particular. This high-volume market drives the development of dedicated micro-controllers featuring SIL-3 (safety integrity level) compatibility. These MCUs provide redundancy by some means, and, of course, CAN connectivity. CAN is by itself not functional safe. Additional communication software is required.

According to the IEC 61508 international standard, Functional Safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment. Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. The ISO 26262 international standard (to be published in 2011) specifying the Functional Safety for road vehicles defines Functional Safety as absence of unacceptable risk due to hazards caused by malfunctioning behavior of electrical and/or electronic systems.

In the beginning Functional Safety was realized on the system level. For some years, there has been a trend to implement Functional Safety on device (ECU) level. Furthermore, the chipmakers have started to provide on the component level micro-controllers with Functional Safety compliant to the international standards (see above).

The ISO 26262 standard defines the automotive safety integrity levels (ASIL) from A to D. They have equivalents to the SIL definition of IEC 61508 (see Table 1). The allowed failure rate is often expressed in “FITs”. One FIT (failure in time) is one failure per billion hours of operation (1 x 10^-9 failures/hour).

“Application of Functional Safety at MCU level is a complex topic.”
Texas Instruments

Most hardware safety designs are based on qualitative analysis techniques such as FMEA (failure mode and effect analysis). A qualitative analysis alone is not sufficient to determine compliance to either IEC 61508 or ISO 26262 safety standards. Quantitative analysis techniques, such as FMEDA (failure modes effects and diagnostic analysis) are needed to determine effectiveness of the safety architecture. These methods should be used as an iterative tool to evaluate and improve the product safety architecture until safety goals are met. Availability of component level failure rate data greatly simplifies the job of the system integrator.

Texas Instruments (TI) started already in 2007 with the development of the first TMS570 Cortex R4F based micro-controller with explicit compliance to the IEC 61508 standard. Recently, the chipmaker released the TMS570LS series featuring two identical CPUs on-chip. Both CPUs supporting floating point operation provide geometrical and timing diversity, in order to detect systematic failures. This dual-core ARM Cortex-R4F based micro-controller is compliant to SIL 3. It targets transportation safety applications including automotive chassis and stability control, electric power steering, hybrid and electric vehicles, aerospace, railway communications, and off-road vehicle engine control. The MCU is equipped with several peripherals including up to three CAN modules. Two of them provide 64 mailboxes, and the third one has 32 mailboxes.

“Functional Safety is a key paradigm of next-generation electronic vehicle systems.”
Freescale Semiconductors

The Lockstep mode implemented in the TI dual-core MCUs provides a high diagnostic coverage of the hardware. This technique is also implemented in the MPC5643L dual-core processors by Freescale. These MCUs are built on the Power Architecture technology, which includes additional instructions for digital signal processing. They are built around a dual-core safety platform with a safety concept targeting ASIL D and SIL-3 levels. In order to minimize additional software and device-level features to reach this target, on-chip redundancy is offered for the critical parts of the micro-controller (CPU core, DMA controller, interrupt controller, crossbar bus system, memory pro-
tion unit, flash memory and RAM controllers, peripheral bus bridge, system timers, and watchdog timer. The Lock Step Redundancy Checking Units are implemented at each output of this sphere of replication (SoR). ECC is available for on-chip RAM and flash memories. A programmable fault collection and control unit monitors the integrity status of the device and provides flexible safe state control. There are two FlexCAN modules on-chip with 64 message buffers. Each message buffer is configurable as receive or transmit buffer; all buffers support base and extended data and remote frame formats. The MCUs target especially the electric power steering and those applications requiring SIL-3 conformity.

“The two CPUs operate synchronously in lock-step mode with clock delay, executing identical instructions at different local times.”

Renesas Electronics

The V850 P-series by Renesas (formerly developed by NEC) provide as the above-mentioned micro-controllers the dual-core architecture. The MCUs are compliant to ASIL D and SIL 3. The family includes nine MCUs with a built-in flash memory ranging from 384KIB to 1MIB, assembled in 80- to 144-pin packages. One of the key elements guaranteeing the inherent safety is the redundant core that allows the function of the master CPU to be monitored permanently by a checker CPU. For the user, this function is totally transparent. Only the master CPU can access peripherals (e.g. two CAN modules) and memory and is visible to the user. The checker CPU operates invisibly in the background where with each clock cycle it monitors the operations of the master CPU.

“Pro-SIL supports users in putting Functional Safety features into devices conforming to IEC 61508 or ISO 26262.”

Infineon

To meet automotive system supplier requirements for intrinsic data and operating safety, two product series in the Audo Max family include Infineon’s Pro-SIL (safety integrity level) functionality. The product series TC179x and TC172x are designed for safety-critical systems like EPS (Electrical Power Steering), chassis controllers and suspension/damping as well as for specific control units used in hybrid and electrical vehicles. The micro-controllers are equipped with up to four CAN modules.

Pro-SIL supports automotive system suppliers and car manufacturers in putting safety features into practice and in designing systems conforming to the international IEC 61508 or ISO 26262. For example, Pro-SIL allows the implementation of a memory protection feature in order to separate the safety-critical software from the non-safety-critical software. Additionally, Pro-SIL allows implementation of error-code correction and checksum verification to ensure the integrity of calculations. The TriCore architecture, which includes a main processor and a coprocessor (peripheral control processor), can also be used as an asynchronous dual-core safety system.

For TriCore micro-controllers, Hitex has introduced the SafeTcore library, which is based on Infineon’s Pro-SIL security concept. The concept incorporates hardware and software aspects including the required safety documentation. The library was designed and programmed using a development process compliant to IEC 61508. By using a safety monitor independent from the micro-controller (CIC61508) required CPU’s and peripherals’, self-test functions can be controlled. Based on the long-experience in safety-critical micro-controller applications, Hitex not only offers support for the SafeTcore library’s utilization but also for integration into customer devices, execution of required tests including test documentation as well as achieving certification. Thus, SafeTcore along with the Hitex support provides a way to achieve SIL 3 or ASIL D certification for TriCore-based devices.

Hitex offers also the RiskCAT tool, which “measures” the achieved safety integrity level (SIL). The tool supports the correct application of IEC 61508, for example. The degree of obligation of each measure varies with the safety integrity level the system is supposed to achieve. This depends on the risk the system bears, i.e. the probability and the consequences of a system failure.

“Our tightly coupled fault supervisor configuration allows hardware and software size reductions.”

Toshiba

Toshiba developed a single core tightly coupled fault supervisor configuration, which requires less space compared to the dual-core implementations. German TÜV has certified these Cortex M3 core based micro-controllers supervised by a special micro-controller test chip for SIL 3 and ASIL D applications. This ‘white box’ approach has been developed in co-operation with the Italian Yokogtech company. The small supervisors provide architectural and functional diversity with respect to the MCU sub-block (e.g. CPU, memory) they supervise. Further peripheral functions on the chip are monitored by Toshiba’s own hardware diagnostic circuits. The run-

<table>
<thead>
<tr>
<th>Table 1: ASIL A to D and its SIL equivalents</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIL</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>D</td>
</tr>
<tr>
<td>C</td>
</tr>
<tr>
<td>B</td>
</tr>
<tr>
<td>A</td>
</tr>
</tbody>
</table>
time supervision guaranteed by the fRCPU hardware leads to high diagnostic coverage for transient faults while the short detection latency (achieved thanks to a dedicated interface between the ARM Cortex-M3 and fRCPU) allows fail operational reactions. There are also special measures on chip to avoid latent faults; for example through built-in self test of supervisor circuits or "scrub and repair" function against bit-flips in memories. Toshiba’s MCUs provide multiple CAN modules on-chip.

The trend to IEC 61508/ISO 26262 certified microcontrollers for automotive applications may influence other CAN application domains. In particular, industrial automation devices could benefit from those components. Implementing CANopen Safety on such certified micro-controllers would simplify device and system design. Other application domains requiring functional safety include off-road vehicles and construction machinery as well as rail vehicles. In all systems already using CAN networks, these certified micro-controllers are an interesting option.