

# Microcontroller platform provides assistance for safety-critical medical applications?

*Medical applications based on electronic components are characterised by a trend towards higher integration, resulting in the need to find the right balance between complexity, development overhead and usability.*

**T**here is also a growing tendency towards medical devices which can be used by patients at home. Therefore, these devices must be small, handy and portable.

Quite often, healthcare devices must meet tougher requirements than devices designed for other applications. After all, the health or even life of many people depends on the functional safety and reliability of these devices every single day. The functional safety standard EN 60601-1 was introduced to unify the functional safety requirements of electrical devices and systems for medical applications. As such, it defines the general safety requirements and the major performance features of

*"The EN 60601-1 standard was introduced to unify the functional safety requirements of electrical devices and systems for medical applications."*

electric devices designed for medical use. Europe is currently in a transitional phase from the second edition to the third edition of this standard. The third edition of the EN 60601-1 standard became effective on June 1, 2012. Electronic medical devices introduced after this date therefore must comply

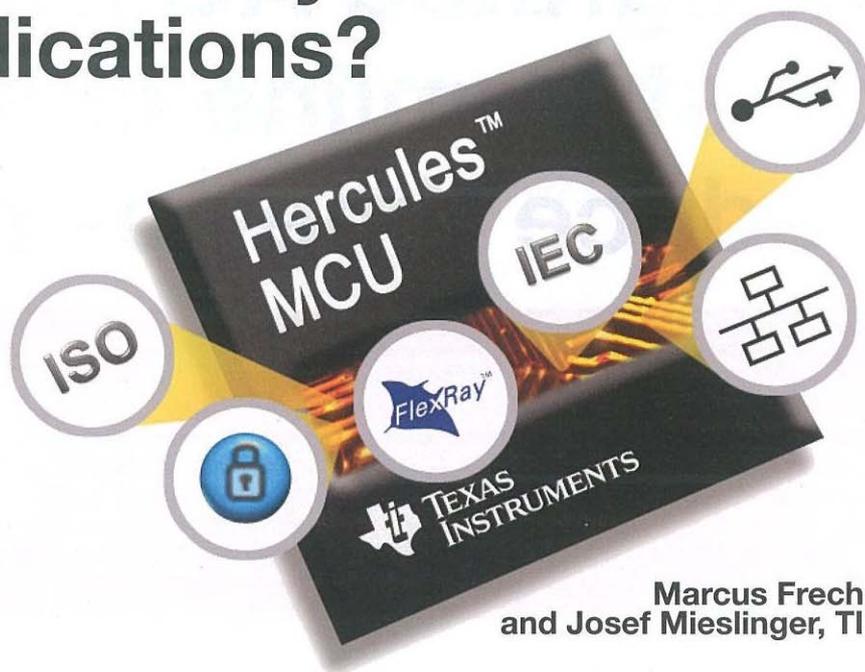
with this edition. Major modifications include the integration of a risk-management process and the fact that functional safety requirements were added to the safety concept. Developers of electronic systems for medical applications are therefore well advised to consider functional safety requirements starting at the early system concept stage. In particular, components should be selected with a special focus on their suitability for safety-critical applications. Some vendors already offer electronic components developed with functional safety requirements in mind. These include the Hercules safety microcontroller platform provided by Texas Instruments.

Hercules safety microcontroller platform is an ARM

Cortex-based family developed according to the IEC 61508 safety standard in order to avoid systematic errors. Random errors are quickly and reliably detected by the hardware-based diagnostic functions, making Hercules devices suitable for many safety-critical industrial and medical applications.

The Hercules RM4x Cortex-R4F lockstep family lends itself to medical applications including insulin pumps and lung ventilators. Today, the family includes devices supporting up to 220MHz for a broad spectrum of safety-critical applications.

Contrary to other microcontrollers with software-based safety implementation, Hercules microcontrollers include hardware-based safety diagnostics in order to achieve better error-detection rates with less software overhead. Hercules RM4x devices include two ARM Cortex-R4F CPUs in lockstep operation, resulting in a high level of on-chip diagnostic functionality. In the lockstep architecture, the program code is redundantly executed by both CPUs without additional software or memory overhead. So called "common cause" failures (CCF) are detected by the special hardware implementation of the lockstep architecture. Hardware-based comparison of the CPU signals enables an almost instant response to any program execution errors. System complexity and costs are also reduced by the lockstep architecture. Furthermore, the software must only be developed for



Marcus Frech  
and Josef Mieslinger, TI

a single CPU. Nonetheless, the application can benefit from the additional processing power which would otherwise be consumed by the safety software.

Apart from the lockstep architecture, the Hercules platform provides a lot of additional safety features, including error correction codes (ECC) protecting flash and RAM memories and busses. The ECC logic is directly embedded into the CPUs in order to avoid any performance degradations caused by additional wait states. Hardware-based self-test functions for the CPU logic



(LBIST) provide assistance for detecting potential CPU faults at run-time without the need for complex software algorithms. In contrast to software-based approaches, LBIST offers significantly improved diagnostic coverage and shorter execution times. All RAM can be tested using a hardware-based memory test (PBIST). Additionally, a memory protection unit (MPU) is available to separate safety-critical software from the non-safety-critical application code. Additional diagnostic functions have been included to monitor the internal clock signals and voltages. Furthermore, the diagnosis functions provided by the Hercules microcontrollers are linked to the central Error Signaling Module (ESM) which can notify the application in case of any serious internal faults.

The Hercules safety microcontroller platform was developed for usage in safety-critical systems requiring SIL3 according to IEC 61508 and was evaluated in a 'safety case'. Texas Instruments offers a safety manual and FMEDA information providing customers with development and certification assistance. The safety documentation delivered with the Hercules microcontrollers includes relevant information required for certification according to this standard and its industry-specific derivatives.

Texas Instruments has also developed the TPS6538x, 'safety companion' providing safety-monitoring and power-supply functions for the Hercules platform. In addition to providing voltages required for microcontrollers, transceivers and sensors, the TPS6538x also supports several diagnostic functions (including voltage, time and temperature monitoring) and self-test functions. The integrated safety features offered by the TPS6538x devices significantly reduce the component count and complexity of the hardware, resulting in shorter development times and lower system costs. The TPS6538x devices were designed to provide optimum support for the Hercules safety microcontroller platform and other microcontrollers.

## IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as "components") are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI's terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers' products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers' products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI's goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or "enhanced plastic" are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have **not** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

### Products

Audio	<a href="http://www.ti.com/audio">www.ti.com/audio</a>
Amplifiers	<a href="http://amplifier.ti.com">amplifier.ti.com</a>
Data Converters	<a href="http://dataconverter.ti.com">dataconverter.ti.com</a>
DLP® Products	<a href="http://www.dlp.com">www.dlp.com</a>
DSP	<a href="http://dsp.ti.com">dsp.ti.com</a>
Clocks and Timers	<a href="http://www.ti.com/clocks">www.ti.com/clocks</a>
Interface	<a href="http://interface.ti.com">interface.ti.com</a>
Logic	<a href="http://logic.ti.com">logic.ti.com</a>
Power Mgmt	<a href="http://power.ti.com">power.ti.com</a>
Microcontrollers	<a href="http://microcontroller.ti.com">microcontroller.ti.com</a>
RFID	<a href="http://www.ti-rfid.com">www.ti-rfid.com</a>
OMAP Applications Processors	<a href="http://www.ti.com/omap">www.ti.com/omap</a>
Wireless Connectivity	<a href="http://www.ti.com/wirelessconnectivity">www.ti.com/wirelessconnectivity</a>

### Applications

Automotive and Transportation	<a href="http://www.ti.com/automotive">www.ti.com/automotive</a>
Communications and Telecom	<a href="http://www.ti.com/communications">www.ti.com/communications</a>
Computers and Peripherals	<a href="http://www.ti.com/computers">www.ti.com/computers</a>
Consumer Electronics	<a href="http://www.ti.com/consumer-apps">www.ti.com/consumer-apps</a>
Energy and Lighting	<a href="http://www.ti.com/energy">www.ti.com/energy</a>
Industrial	<a href="http://www.ti.com/industrial">www.ti.com/industrial</a>
Medical	<a href="http://www.ti.com/medical">www.ti.com/medical</a>
Security	<a href="http://www.ti.com/security">www.ti.com/security</a>
Space, Avionics and Defense	<a href="http://www.ti.com/space-avionics-defense">www.ti.com/space-avionics-defense</a>
Video and Imaging	<a href="http://www.ti.com/video">www.ti.com/video</a>

### TI E2E Community

[e2e.ti.com](http://e2e.ti.com)