Electronic Design®

By RICK NELSON, Contributing Editor

Functional-Safety ICs and Reference Design Help Robots Meet IEC 61508

Sponsored by Texas Instruments: Three categories of ICs and an input-module design example give a boost to the functional safety of robotic and other factory-automation systems.

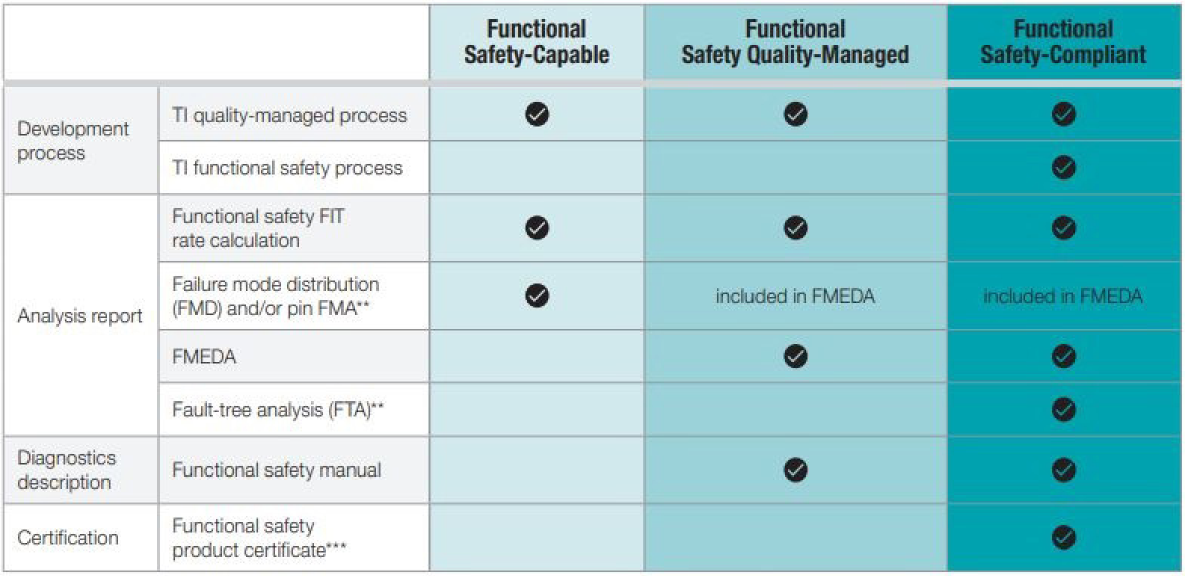
ntelligent robotic systems are bringing great gains in productivity to the factory floor. However, they also present collision hazards that could potentially injure humans or damage themselves, other equipment, or the product being manufactured.

Consequently, the need for functional safety is on the rise, and design engineers must increasingly deliver projects that comply with relevant standards like the International Electrotechnical Commission's IEC 61508 functional-safety standard. Even if a project doesn't require adherence to a particular standard, designing in accordance with function-al-safety requirements can be a key differentiator that pro-vides a competitive advantage.

Signal-Integrity Levels

Functional safety involves predicting hazardous conditions and identifying ways to address those conditions. Engineers must assess the risk reduction that any safety functions achieve and ensure they perform as intended. The goal is to meet the signal-integrity level (SIL) appropriate for the specific application as defined in the relevant standard.

IEC 61508 specifies four SILs, ranging from SIL 1 to SIL 4, with SIL 4 the most stringent. The SILs define required levels of risk-reduction factor (RRF) and probability of failure on demand average (PDFavg). The latter indicates the likelihood that a safety function will not work properly, resulting in a dangerous failure. SIL 1 requires an RRF of 10 to 100



		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA**	✓	included in FMEDA	included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)**			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate***			✓

Texas Instruments' product categories for functional-safety design.

*** May only be available for analog power and signal chain products.*

**** Available for select products.*

and a PDFavg of 0.1 to 0.01, while SIL 4 requires an RFF of 10,000 to 100,000 and a PDFavg of 0.0001 to 0.00001.

Functional-safety design begins with examination of potential system architectures and the required components. The next step is to obtain safety information about the components selected from their manufacturer.

With that information in hand, you can perform a failure modes, effects, and diagnostic analysis (FMEDA). FMEDA takes into account factors such as component failure modes, the effect of each possible failure mode on the end product's functionality, and the availability of diagnostic capabilities to identify failures.

Functional-Safety Product Categories

Texas Instruments offers three categories of products for functional safety designs *(see table)*. Functional-safety-compliant products include devices such as MCUs and analog motor drivers that are sufficiently complex to be considered systems in their own right. These devices may have integrated safety features.

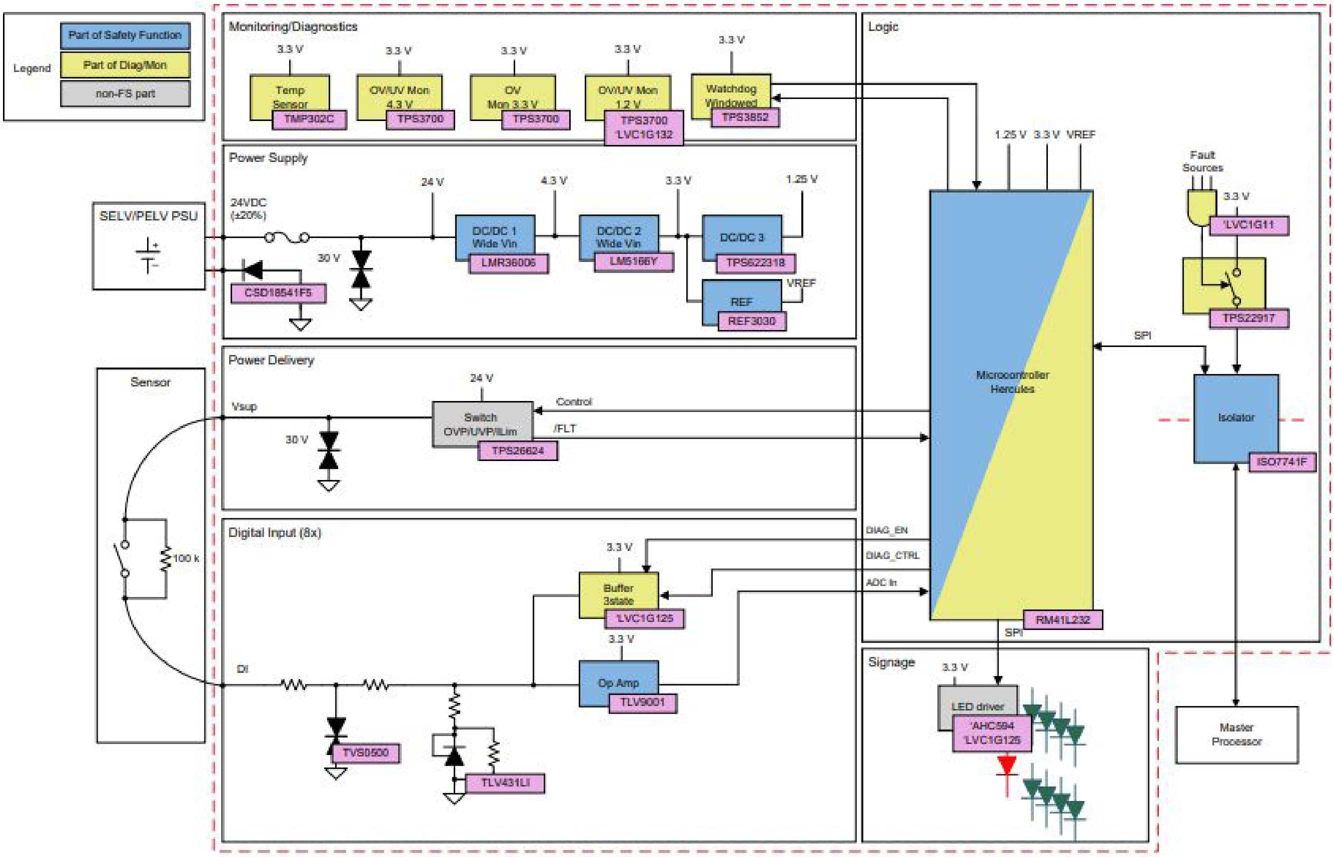
TI develops these products using a functional-safety development flow certified by agencies like Technischer Überwachungsverein (TÜV) SÜD. Such certification helps ensure that products in this category are developed following the requirements of IEC 61508 or other relevant standards.

In the second category are functional-safety quality-managed products, which include complex devices that may include diagnostic features. These products, though, are manufactured using the TI-wide standard quality-managed development flow—not the certified functional-safety development flow used for products in the first category. The third category includes functional-safety-capable products, which are simper devices developed using the TI standard quality-managed development flow.

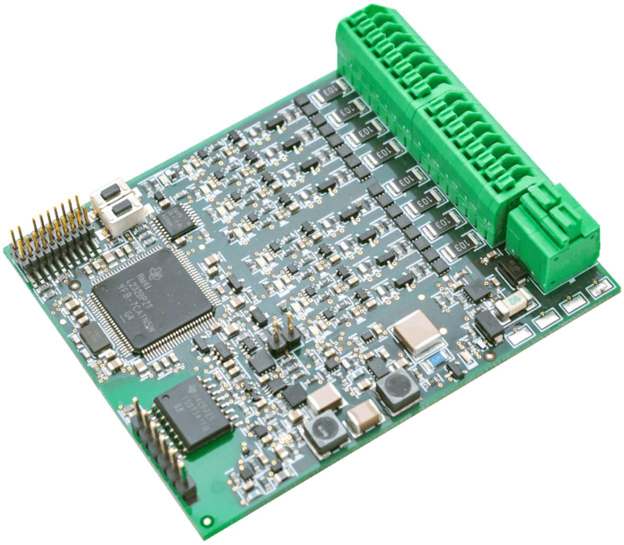
From PMICs to Real-Time MCUs

TI offers functional-safety-compliant products ranging from power-management ICs (PMICs) to real-time controllers for robotics and related factory-automation applications. For example, the TPS6594-Q1 multi-rail PMIC provides high accuracy and flexibility for industrial applications requiring functional safety up to SIL 3. They come with functional-safety documentation.

In addition, TI's Hercules MCUs integrate sufficient safety and diagnostics features to enable designs reaching up to SIL 3 for industrial applications. The MCUs integrate two Cor-



1. A Hercules microcontroller helps implement safety and diagnostics functions in the TIDA-010049 reference design.



2. The TIDA-010049 reference design yielded this fully assembled proof-of-concept board.

tex-R CPUs in lockstep to enable comparison of the outputs every cycle; in case of error, they generate a non-maskable interrupt. The CPU self-test can run at startup or in time slices.

TI also offers functional-safety compliant C2000 real-time MCUs, which are independently assessed and certified by TÜV SÜD to meet IEC 61508 SIL 2 requirements for components used in industrial applications. TI offers a tunable FMEDA and functional-safety manuals that provide sufficient information to enable customers to adapt the devices for use in compliant systems up to SIL 3.

Specific C2000 safety mechanisms include redundant sensing, communications, and actuation peripherals as well as dual oscillators to enable missing-clock detection. The devices also perform online temperature monitoring, ADC-to-DAC loopback test, hardware built-in self-test, and embedded real-time analysis and diagnostics.

Functional-Safety Reference Design

To help get you started on functional-safety projects, TI developed the TIDA-010049 reference design for an 8-channel group-isolated digital-input module *(Fig. 1)*. Such modules have flexible use cases and can serve as industrial robot digital I/O modules, which typically require highly efficient, isolated power supplies; a high-speed sampling rate; precision signal chains; and advanced protection and diagnostic capabilities.

Modules based on the reference design can also serve as ac drive control modules, linear-motor segment-controller modules, and servo-drive control modules. Sensors connected to the modules' inputs can range from switches monitoring door openings and closings to digital encoders that monitor a motor shaft's speed and position.

Note that a standard module designed without functional-safety assessment can exhibit permanent and random faults—for example, it can indicate that a switch is open when it's closed—that the module itself can't detect.

The TIDA-010049 design implements a diagnostic scheme that can help detect permanent and random faults *(Fig. 2)*. A Hercules microcontroller assists with both safety and diagnostics functions. Based on a design concept assessment by TÜV SÜD, TI expects that an actual module based on the design would meet IEC 61508 SIL 2 requirements.

Conclusion

An effective functional-safety design for an industrial robotic system or other factory-automation application requires identifying hazards and possible failure modes at the initial concept stage. It involves a standards-compliant analysis of a system and all of its components to determine the effectiveness of built-in diagnostic capabilities.

TI helps ensure successful functional-safety designs by developing functional-safety-capable, quality-managed, and compliant products, and by making all of the necessary data and documentation about these products available to enable their use in industrial applications.