Electronic Design

By RICK NELSON, Contributing Editor

Streamline Functional Safety Certification for Automotive, Industrial Apps

Sponsored by Texas Instruments: Selecting the right components and studying the relevant documentation can help meet the requirements of standards such as ISO 26262 and IEC 61508.

Whether you're designing equipment for use on the road or in the factory, you'll need to emphasize functional safety and obtain the necessary certifications. For automotive applications, you must meet the functional safety requirements of ISO 26262 when designing ADAS domain controllers, battery-management systems, inverters and converters, electric power-steering systems, camera and radar systems, hybrid instrument clusters, chargers, and vehicle control units.

Driven by Industry 4.0 and advanced robotics, industrial equipment is getting smarter and more efficient. To make sure it's also safer, you will want to meet the functional safety requirements of standards like IEC 61508 when designing analog input and output modules, digital output modules, safety guards, motor drives, and DIN rail power supplies.

For both automotive and industrial applications, you can efficiently achieve the necessary certifications using appropriate products, studying available documentation, and relying on knowledgeable safety experts.

Rigorous Requirements

Nevertheless, even when choosing appropriate parts and relying on expert information, meeting the requirements of functional safety standards such as ISO 26262 or IEC 61508 takes rigor and time. What these standards have in common is the concept of the safety integrity level (SIL). IEC 61508 defines a range from SIL 1 to SIL 4, with SIL 4 being the most stringent. Similarly, ISO 26262 has automotive SILs (ASILs) ranging from ASIL A to ASIL D, with ASIL D being the most stringent.

To achieve compliance, engineers must define hazardous con-

		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***			✓

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

**** Available for select products.*

Texas Instruments offers three categories of products for functional safety design.

ditions, identify ways to address those conditions, assess risk reduction, and ensure safety functions perform as intended. At the early stages of a typical development process, engineers examine system architectures, modules, and ICs. Functional safety standards define the information they need about the ICs so that they can conduct their own failure modes, effects, and diagnostic analysis (FMEDA).

Texas Instruments' approach to IC design provides you with the resources needed to accelerate functional safety system design. The table shows TI's three categories for products offered for functional safety designs.

The TI Functional Safety-Capable category includes relatively simple ICs developed using TI's standard quality-managed development flow. While these products lack comprehensive integrated safety functions, they remain important building blocks, and TI provides key information like functional safety failure-in-time (FIT) rates for designers to use in their own safety analyses.

The TI Functional Safety Quality-Managed category adds complex products with integrated diagnostic features. However, they're not developed in accordance with the certified functional safety development flow used for the Functional Safety-Compliant product category.

This third category includes products sufficiently complex to be systems unto themselves. TI developed these products using a functional safety development flow certified by agencies including TÜV SÜD, thereby helping to ensure that products in this category were developed following specifications prescribed by the relevant functional safety standards.

Products in the Functional Safety-Compliant category include the Automotive Electronics Council (AEC)-100-qualified Jacinto TDAx SoC for advanced driver-assistance systems; the TPS6594-Q1 multirail power-management IC (PMIC) for automotive and industrial markets; Hercules MCUs, which integrate sufficient safety and diagnostics features to enable engineers to aim for up to SIL 3; the DRV3245E-Q1 FET gate-driver IC for three-phase motor-drive applications; and the AWR1843 76- to 81-GHz automotive radar sensor with an onboard DSP, MCU, and radar accelerator.

Products in the Functional Safety-Compliant category come with dedicated functional-safety-related documentation covering topics such as functional safety FIT rate calculations, failure-mode distribution (FMD), FMEDA, and fault-tree analysis.

Understanding Failure Rates

Functional safety standards like IEC 61508 and ISO 26262 require that semiconductor makers address both systematic and random hardware failures. Systematic faults result from design inadequacies, and companies can mitigate or eliminate them through rigorous development processes and continuous process improvements.

Random hardware failures can't be eliminated even when companies adhere to specified quantitative metrics to meet hardware SILs or ASILs—in fact, all electronic systems will eventually fail. The goal is to detect random hardware failures and take some action; for example, alert a driver that a car's engine needs to be checked.

The base failure rate (BFR) quantifies the intrinsic reliability of an IC operating in normal environmental conditions. It forms the basis of the calculation of quantitative random hardware metrics, including safe failure fraction (SFF), probability of failure per hour (PFH) or per day (PFD), single-point fault metric (SPFM), latent fault metric (LFM), and probabilistic metric for random hardware failure (PMHF).

The classic bathtub curve represents random hardware failures over three periods of a product's lifetime. The early-life (infant mortality) period is characterized by relatively high failure rates, which can be addressed through techniques like burn-in and I_{DDQ} test. At the other end of the curve is the intrinsic wear-out period, where failures increase exponentially because of factors such as channel-hot-carrier effects, electromigration, time-dependent dielectric breakdown, and negative-bias temperature instability.

In between lies the normal life period, during which failure rates are low and constant. BFR estimations address this portion of a component's lifecycle, where the failure rate is quantified in FIT units—an estimate of the number of failures that could occur in a billion cumulative hours of product operation.

Various approaches can help estimate BFR, including observations of field failures and customer returns. However, this approach requires extensive record keeping—not all customers return all failed devices, and the approach can't be used for new product introductions. Empirical techniques include temperature-bias operating-life test, high-temperature operating-life test, and extended-life reliability test. Reliability guides including SN 29500 (the Siemens standard for the reliability prediction of electronic and electromechanical components) can provide an estimation for functional safety analysis.

Conclusion

Safety is critical in automotive and industrial applications, and many products will require functional safety certification. Choosing the appropriate parts for your design and availing yourself of accurate documentation and expertise can help smooth your road to success.