Streamlining Functional Safety Certification in Automotive and Industrial

Miro Adzan
General Manager
Industrial Systems
Factory Automation & Control
Texas Instruments

Arun Vemuri
General Manager
Automotive Systems
Body Electronics & Lighting
Texas Instruments

Functional safety design takes rigor, documentation and time to get it right. Whether you're designing for the factory floor or the highway, this white paper explains how TI's approach to designing integrated circuits (ICs) provides you with the resources needed to streamline your functional safety design.

Automation has increased the need for functional safety in both the industrial and automotive sectors. Functional safety is required across industrial applications but especially in factory automation and control systems.

In the automotive industry, while airbag and braking systems have included functional safety for years, increased electrification and autonomous driving features require systems that control battery management, sensor fusion and vehicle maneuvers, increasing the need for designs with functional safety.

Whether designing robotic systems for factories, appliances for homes or tomorrow's cars, design engineers are increasingly required to deliver projects that comply with the functional safety standard relevant for the application.

In applications that don't require standards compliance, designing a safer system has become a key differentiating factor against competitors.

Functional safety standards

Functional safety is part of the overall safety of a system and depends on responding in a predictable manner to certain inputs or a failure state. Functional safety standards accept that there is always a hazard, and that all systems therefore have an inherent failure rate.

Functional safety standards specify how to develop systems in a way that reduces the risk to a tolerable level. System designs that include functional safety must not only lower risk from improper operation, but detect faults and minimize their impact.

To achieve functional safety compliance, engineers must:

- Predict and define hazardous conditions.
- Identify safety functions that address these conditions.

- Assess the risk reduction that the safety functions achieve.
- Ensure that the safety functions perform to their design intent.

Functional safety standards defined by standards organizations, with participation from companies in the relevant industry, guide designers by helping define the safety functions in a system and setting specifications for assessing and rating safety levels. Texas Instruments' (TI) involvement in standards organizations helps ensure that the company develops products with functional safety in mind from the beginning.

Common safety standards include International Electrotechnical Commission (IEC) 61508 for industrial applications, International Organization for Standardization (ISO) 26262 for automotive applications and IEC 60730 for household appliances.

Safety standards have risk reduction and safety integrity levels (SIL) in common. For example, SILs as defined by IEC 61508 range from SIL 1 to SIL 4, with SIL 4 being the most stringent. SIL 1 requires a safety availability of 90% to 99%, a probability of failure on demand average (PFDavg) of 0.1 to 0.01 and a risk-reduction factor (RRF) of 10 to 100. SIL 4 demands >99.99% safety availability, a PFDavg of 0.0001 to 0.00001 and an RRF of 10,000 to 100,000.

ISO 26262 has similar SILs ranging from ASIL A to ASIL D, with ASIL D being the most stringent.

Functional safety process

A typical functional safety development process begins by deciding the hazards and functional safety goals. Engineers then typically start examining system architectures, modules and ICs. It is the ICs that then become the main building blocks of a functional safety standards-compliant system.

To predict system behavior, engineers must quantify and predict a module's operation. To accomplish this, they must conduct a structured qualitative safety analysis of the system as part of the development process in order to identify various failure modes—their causes as well as their effects.

Functional safety standards define the information engineers need about the ICs so that they can also conduct their own failure modes, effects and diagnostic analysis (FMEDA). Depending on the IC's complexity, a system safety analysis requires design-, die- and package-dependent information.

Choosing the right product from a reliable supplier is critical in this endeavor. TI has made it easier for engineers to find and use its products, whether in designs targeted to meet functional safety standards or in competitively differentiated safer systems.

Simplifying device selection with functional safety categories

Typical industrial and automotive applications require a large number of ICs that vary widely in complexity—one or more sensors and actuators, a microcontroller (MCU) or processor to process the data from the sensors, analog multiplexers, operational or instrument amplifiers, analog-to-digital converters (ADCs) and digital-to-analog converters that may or may not be integrated with the processor, DC/DC converters, low-dropout regulators or power-management ICs (PMICs), as well as driver components such as LED drivers,

		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***			✓

***Table 1**. TI's categories for products in functional safety design.*

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

**** Available for select products.*

motor drivers, solenoid drivers, field-effect-transistors (FET) and insulated gate bipolar transistor gate drivers, and power switches and load switches. In addition, the applications include communication interfaces such as RS-485, Controller Area Network (CAN), Ethernet, FPD-Link and Peripheral Component Interconnect Express (PCIe).

Table 1 shows TI's categories for products offered for functional safety designs, which reflects the logic behind standards-based IC complexity categories. The categories are TI Functional Safety-Capable, TI Functional Safety Quality-Managed and TI Functional Safety-Compliant.

Functional Safety-Compliant Products

These products are often complex enough to be systems in their own right, like MCUs and processors or analog motor drivers, and may have integrated safety features.

TI developed these products using a functional safety development flow certified by agencies like Technischer Überwachungsverein (TÜV) SÜD. This certification helps ensure that products in this category were developed following specifications prescribed by the functional safety standards, ISO 26262 and IEC 61508.

Take for instance, the following complex functional safety-compliant devices:

- Automotive Electronics Council (AEC)-100 qualified Jacinto™ TDAx systems on chip for advanced driver assistance systems integrate a mix of fixed- and floating-point TMS320C66x digital signal processor (DSP) generation cores, the Vision AccelerationPac embedded vision engine and dual ARM® Cortex®-M4 processors, as well as peripherals like multicamera interfaces for low-voltage differential signaling-based surround-view systems, displays, CAN and Gigabit Ethernet Audio Video Bridging. These devices support an extensive list of functional safety system requirements, including error correcting code (ECC)-protected M4, ECC-protected 32-bit double-data-rate interface, dedicated memory management

units for each central processing unit (CPU), memory protection units, temperature monitoring sensors and an eight-channel ADC for system monitoring.

- The TPS6594-Q1 multirail Power Management Integrated Circuits (PMIC) supports TI's Jacinto TDAx systems on chip in the automotive and industrial markets. High-accuracy, flexible PMICs that are suitable for automotive and industrial applications requiring functional safety and come with functional safety documentation. The TPS6594-Q1 provides a scalable power management solution for both the main domain and the MCU domain and support functional safety up to ASIL-D/SIL-3.
- Hercules™ MCUs integrate enough safety and diagnostics features to enable engineers to aim for up to SIL 3. This means that the MCU can attain about 99% fault coverage. For instance, integrating two Cortex-R CPUs in lockstep on the MCU enables comparison of the outputs every cycle and, in case of error, the generation of a nonmaskable interrupt. The CPU self-test can run at startup or in time slices for an industrial application.
- The DRV3245E-Q1 is a FET gate-driver IC for three-phase motor-drive applications. Its three half-bridge drivers can each drive a high- and low-side N-channel metal-oxide semiconductor FET. Designed to the applicable requirements of ISO 26262, this gate driver integrates diagnostics and protection for each internal block and provides support for common system diagnostic checks, each of which can be instantiated and reported through Serial Peripheral Interface. This flexibility of features allows the DRV3245E-Q1 to integrate seamlessly into many safety architectures.
- The TPS65381A-Q1 multirail PMIC supports TI's Hercules TMS570 and C2000™ MCU families in the automotive and industrial markets with dual-core lockstep or loosely coupled architectures. An asynchronous-buck switch-mode power-supply converter with an internal FET converts the input supply (battery) voltage to a 6-V preregulator output. The 6-V preregulator then supplies other regulators. Its monitoring and protection blocks, like a voltage monitor, analog built-in self-test, loss-of-clock monitor, junction temperature monitoring, current limiting for power supplies and MCU error signal monitor improve diagnostic coverage and decrease the undetected fault rate.
- TI offers many more devices in this category, such as C2000 real-time controllers and the AWR1843 76-GHz to 81-GHz automotive radar sensor with an onboard DSP, MCU and radar accelerator. All these products come with dedicated functional safety related documentation to support the system development process:
  - Functional safety failure in time (FIT) rate calculations.
  - Failure mode distribution (FMD).
  - FMEDA.
  - Fault-tree analysis.
  - A functional safety manual that explains the IC's safety functions and how to use external components to achieve certain fault coverage and diagnostics.
  - A functional safety product certificate.

Functional Safety Quality-Managed Products

This second category of products comprises complex products that have diagnostic features inside and are specifically designed for systems

requiring functional safety. However, this product category is not developed according to the certified functional safety development flow which is used for the Functional Safety-Compliant product category, but use the TI-wide standard quality-managed development flow.

Examples of products in this category include, but are not limited to:

- The TCAN4550-Q1 is an automotive system basis chip (SBC) with integrated CAN FD controller and transceiver. This highly integrated device simplifies CAN FD bus expansion by utilizing the existing SPI port, so that designers can maintain their current microcontroller-based architecture when upgrading to the higher-bandwidth CAN FD interface protocol.
- The LP87702-Q1 is a dual buck converter and 5-V boost with integrated diagnostic functions that are required in ASIL-compliant mmWave radar systems including a window watchdog and an independent voltage reference that monitors its own output supply, as well as two external power supplies.

As with the Functional Safety-Compliant devices, we supply an extensive set of documentation to help with functional safety system design, these include a functional safety FIT rate calculation, FMEDA and a functional safety manual, but unlike Functional Safety-Compliant devices, will not include fault-tree analyses or product certification.

Functional Safety-Capable Products

The third category of products is comprised of simper ICs that are developed using TI's standard quality-managed development flow, similar to the Functional Safety Quality-Managed product category.

Functional Safety-Capable products typically do not have integrated safety functions and therefore generally won't have internal monitoring and diagnostic features that are more common to devices in TI's other functional safety product categories.

Since the products do not have comprehensive safety functions integrated in them, they do not have the internal monitoring and diagnostic features common to devices in the other categories.

They still are important building blocks for functional safety systems, however, and TI therefore provides key information, like functional safety FIT rates and FMD, for designers to use in their safety analyses.

Products in this category include, but are not limited to:

- The industry's smallest linear thermistor, TMP61-Q1 popular for its < 1% long-term sensor drift and accuracy benefits over traditional thermistors. Our thermistor alternative, the TMP235-Q1, is a precision temperature sensor IC that achieves ±1.5°C without calibration.
- The TPS3840-Q1 voltage supervisor or reset IC. This AEC-Q100-qualified device can operate through a wide voltage range of 1.5 V to 10 V, and has a supply current of only 350 nA typical and 700 nA max.
- The TPS7A16A-Q1 AEC-Q100-qualified, 60-V, 5-µA quiescent current 100-mA low-dropout voltage regulator is designed for continuous or sporadic (power backup) battery-powered applications where ultralow quiescent current is important. This device is a good fit for generating a low-voltage supply from multicell solutions ranging from high-cell-count power-tool packs to automotive applications. Not only

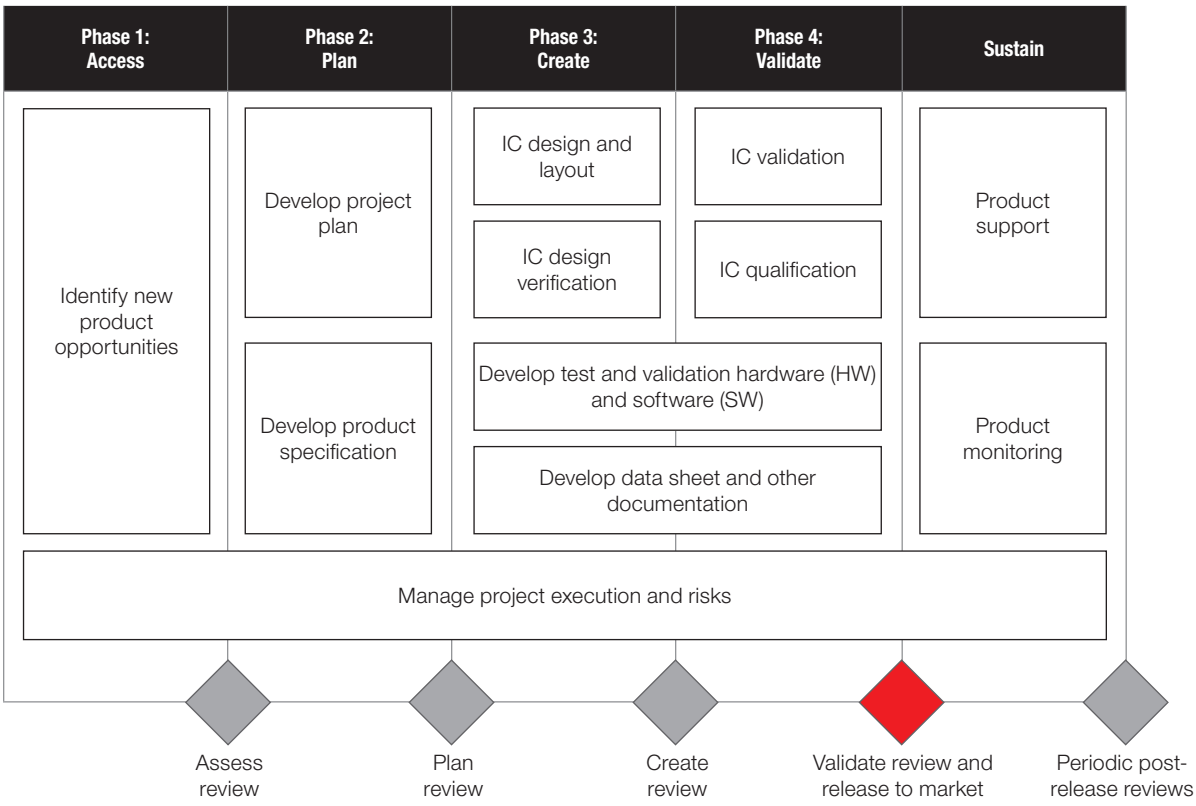

***Figure 1**. The standard quality-managed development process on which additional functional safety activities may be overlaid.*

can the TPS7A16A-Q1 supply a well-regulated voltage rail, it can withstand and maintain regulation during voltage transients.

TI's development process

Because of the complexity of functional safety development, you may need more information beyond the TÜV SÜD certification about a company's safety culture and process. That's why TI created a development process for the management of both systematic and random faults (see **Table 2** on the following page).

We follow a quality-managed development flow for all of our products to decrease the probability of systematic failures. This standard development process, as shown in **Figure 1**, features many elements necessary to manage systematic faults. Additionally, you can use the documentation and reports for these products to assist with compliance to a wide range of standards for end applications including automotive and industrial systems compliant to ISO 26262-4 or IEC 61508-2.

The process breaks the development into these phases:

- Assess.
- Plan.
- Create.
- Validate.

TI's functional safety development flow is derived from ISO 26262 and IEC 61508. We added several functional safety-specific activities to each phase of our standard new product development process to develop our three standards-based IC complexity categories.

As stated in Annex A of ISO 26262-2:2018, TI's development process supports and encourages the effective achievement of functional safety.

Assess	Plan	Create	Validate	Sustain and end-of-life
Determine if functional safety process execution is required	Define component target SIL/ ASIL capability	Develop component-level functional safety requirements	Validate functional safety design in SILicon	Document any reported issues (as needed)
Nominate a functional safety manager	Generate functional safety plan	Include functional safety requirements in design specification	Characterize the functional safety design	Perform incident reporting of sustaining operations (as needed)
End of phase audit	Verify functional safety case	Verify the design specification	Qualify the functional safety design (per AEC-Q100)	Update work products (as needed)
	Initiate functional safety case	Start functional safety design	Finalize functional safety case	
	Analyze target applications to generate system-level functional safety assumptions	Perform qualitative analysis of design (i.e. failure mode analysis)	Perform assessment of project	
	End of phase audit	Verify the qualitative analysis	Release functional safety manual	
		Verify the functional safety design	Release functional safety analysis report	
		Perform quantitative analysis of design (i.e. FMEDA)	Release functional safety report	
		Verify the quantitative analysis	End of phase audit	
		Iterate functional safety design as necessary		
		End of phase audit		

***Table 2**. Functional safety activities overlaid on top of TI's standard development process.*

The development process promotes exchange of functional safety related information among all teams involved in product development.

TI teams follow adequate standards to maintain organization-specific rules for functional safety, and TI's processes ensure resolution of identified safety anomalies. By following industry standards, TI supports its customers by maintaining a quality-management system that supports functional safety.

A growing functional safety portfolio

Functional safety design centers on planning for hazards, failures and mitigation right from the concept stage. It involves a standards-compliant analysis of a system for failures and the effectiveness of implemented diagnostic schemes. It revolves around data about every product that goes into building the system.

TI helps address this need by continuing to develop relevant products and making all of the necessary data and documentation about these products available to enable their use in functional safety applications.

Learn about TI functional safety technologies

Additional resources

- Video: Understanding Functional Safety and System-Level Fault Detection of an ADC.
- Video series: Functional Safety on C2000™ MCUs.
- White paper: Actuator Design Trends for Functional Safety Systems in Electric and Autonomous Vehicles.
- White paper: Leverage Jacinto™ 7 Processors Functional Safety Features for Automotive Designs.
- White paper: C2000™ MCU SafeTI™ Control Solutions: An Introduction to ASIL Decomposition and SIL Synthesis.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265