Electronic Design

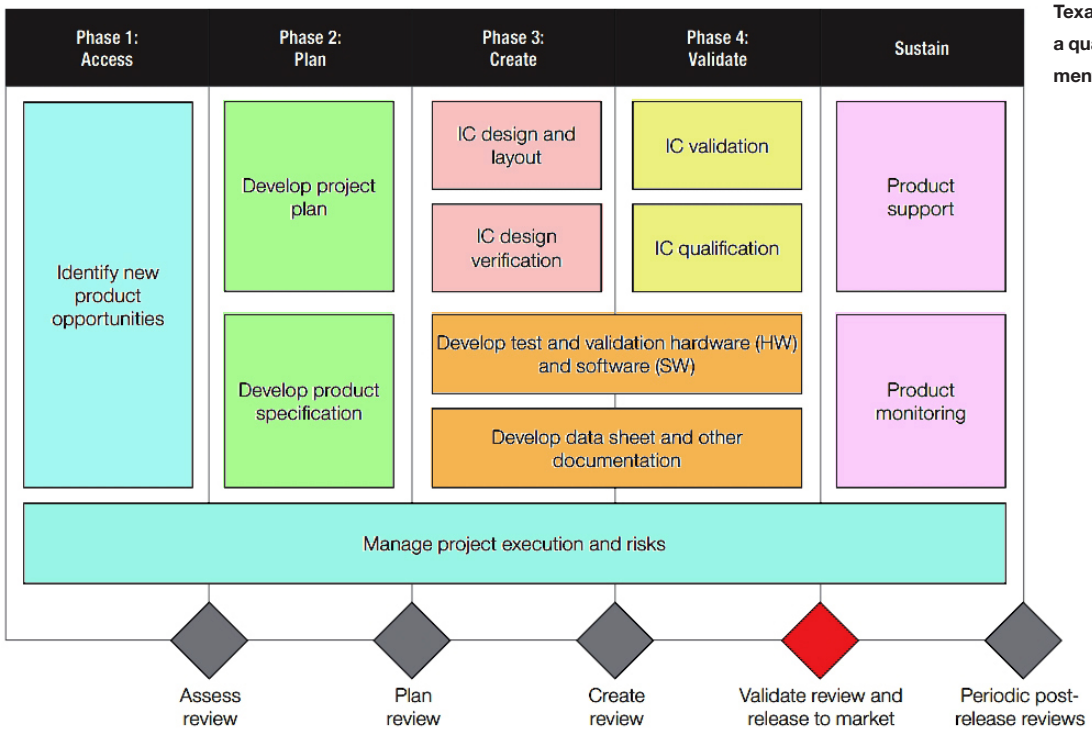
By RICK NELSON, Contributing Editor

Functional Safety Confers Competitive Advantage in Automotive, Industrial Apps

Sponsored by Texas Instruments: A rigorous development process overlaid with functional-safety activities streamlines functional-safety design for products ranging from ADAS domain controllers to industrial robotic systems.

From the highway to the factory floor, automation is driving the need for functional safety. Automotive airbag and braking systems have long incorporated functional safety. However, now the trend toward increasing vehicle electrification is extending the need for functional safety to autonomous driving and advanced driver-assistance system (ADAS) functions, battery-management systems, and systems employing sensor fusion. In addition, everything from industrial robotic systems to home appliances can benefit from functional-safety features.

Frequently, automotive and industrial products require certification in accordance with the IEC 61508 industrial and ISO 26262 automotive standards and their respective safety integrity level (SIL) and automotive SIL (ASIL) values. But even if your product doesn't require certification, building in functional safety can give you a competitive advantage.



Texas Instruments employs a quality-managed development flow.

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		

Functional safety activities overlaid on TI's standard development process.

Functional-Safety Categories

An effective functional-safety design begins with choosing the right parts and making sure your supplier can provide the necessary support. Texas Instruments has streamlined the process, offering products in three functional-safety categories along with access to engineering expertise and functional-safety-related documentation covering topics such as failure mode distribution (FMD); failure modes, effects, and diagnostic analysis (FMEDA); and fault-tree analysis.

The first of TI's three functional-safety categories, the Functional Safety-Compliant category, includes MCUs, processors, and analog motor drivers that may have integrated safety features. TI developed these products using a functional-safety development flow certified by agencies such as TÜV SÜD. Specific products in this category include Hercules MCUs, the TPS65381A-Q1 multi-rail power-management IC (PMIC), and the C2000 real-time controllers.

The Functional Safety Quality-Managed category includes devices specifically designed for systems requiring functional safety, yet they're fabricated using the TI-wide standard quality-managed development flow instead of a certified functional-safety development flow. Among the specific products in this category are the TCAN4550-Q1 automotive system-basis chip (SBC) with integrated CAN FD controller and transceiver as well as the LP87702-Q1 dual buck converter and 5-V boost converter/bypass switch with integrated diagnostic functions required in ASIL-compliant mmWave radar systems.

The Functional Safety-Capable category presents less-complex ICs that generally lack the internal monitoring and diagnostics features found in devices in the other two categories. Nevertheless, they come with key information such as failure-in-time (FIT) rates and failure-mode distribution (FMD) that engineers can use in their own safety analyses. Specific products include the TMP61-Q1 linear thermistor featuring < 1% long-term sensor drift; the TPS3840-Q1 voltage supervisor IC; and the TPS7A16A-Q1 AEC-Q100-qualified, 60-V, 5-µA quiescent-current, 100-mA low-dropout voltage regulator.

Development Process

To deal with the complexities of functional-safety development, you may need information about a company's safety culture and process beyond factors such as TÜV SÜD certification status. To help fill any information gaps, TI created a standard quality-managed development process *(see figure)*, which it overlays with several functional-safety-specific activities *(see table)*. The process decreases the probability of systematic failures and breaks development into four phases:

- The Assess phase involves identifying new-product opportunities and determining whether functional-safety process execution is required.
- The Plan phase defines component-level SIL or ASIL capabilities and results in a product specification.
- The Create phase involves IC design, layout, and design

verification as well as development of component-level functional-safety requirements.

• The Validate phase embodies IC validation and qualification and extends through the release of functional-safety documentation. You can use the documentation to help you comply with a range of automotive and industrial standards, including ISO 26262-4 or IEC 61508-2.

These four phases are followed by a Sustain period that involves product support and monitoring along with the documentation of issues through a product's end-of-life.

Random Faults and BFR

In addition to systematic failures, products are subject to the occurrence of inevitable random faults, often quantified by the base failure rate (BFR), which in turn is affected by factors such as temperature, voltage, and number of operating hours. BFR relates to other metrics, such as safe failure fraction (SFF), probability of failure per hour (PFH), single-point fault metric (SPFM), latent fault metric (LFM), and probabilistic metric for random hardware failure (PMHF). In addition, FIT is an estimate of the number of failures that could occur in a billion cumulative hours of a product's operation. ISO 26262 and IEC 61508 specify acceptable values of random hardware failure metrics for each ASIL and SIL value, respectively.

Several methods exist for generating estimates that can be used in functional-safety analysis, including those outlined in the Siemens SN 29500 standard for the reliability prediction of electronic and electromechanical components. SN 29500 includes lookup tables to find reference FIT rates and reference temperatures for component types including ICs, discrete semiconductors, passive components, switches, relays, lamps, and connectors.

The standard describes the calculations necessary to translate from a reference FIT rate to an adjusted FIT rate for the actual expected operating conditions. System integrators can refer to the SN 29500 standard to derive their application's specific FIT rate for a TI-supplied component.

Conclusion

Functional-safety considerations are increasingly important as automation pervades automotive and industrial applications. A careful functional-safety design can speed certification to standards such as IEC 61508 and ISO 26262. Even if your product doesn't require formal certification, functional safety can confer a competitive advantage. TI employs a quality-managed development flow overlaid with functional-safety activities to produce the ICs you need for the success of your functional-safety project.