# The state of functional safety in Industry 4.0


**VC Kumar**
*Embedded Processing,*
*Texas Instruments*

# Industry 4.0, or the fourth industrial revolution, typically refers to the evolution of the manufacturing industry to become “digitized” – to harness the power of collecting and using information in real time to create smart factories.

The goal is to sense and share factory, equipment and product status in real time with intelligent and self-aware machines (like robots) to drive increased efficiency and flexibility.


***Figure 1**. Functional safety standards in industrial applications.*

The digitization of the factory combines communications, information technology (IT) (including cloud storage and interaction), data and physical elements. Machines interact with humans as well as products and other machines. Integrated sensing delivers decision-critical data, and real-time information processing and communication drive profound changes in the entire industrial ecosystem. This “connected everything” environment enables companies to collect, store and use large amounts of data simultaneously; greatly enhances manufacturing processes; and creates a fully digital value chain [1].

### The implementation of Industry 4.0 in a factory or system must include [2]:

- Interoperability: people, machines, devices and sensors that connect and communicate with one another.
- Information transparency: the systems create a virtual copy of the physical world through sensor data to contextualize information.
- Technical assistance: both the ability of the systems to support humans in making decisions and solving problems, and the ability to assist humans with tasks too difficult or unsafe for them.

- Decentralized decision-making: the ability of cyberphysical systems to make simple decisions on their own and become as autonomous as possible.

This trend toward autonomous machine decision-making and operation as well as increased human-machine interaction in potentially dangerous factory environments means that functional safety is becoming more important in Industry 4.0.

This white paper will focus on what functional safety means for processors in factory floor automation subsystems and explore some of the options to enable functional safety.

## Functional safety requirements for Industry 4.0 in smart factories

Functional safety is a part of an overall safety structure that depends on a system or equipment to operate correctly in response to its inputs. In other words, functional safety is the ability to detect a potentially dangerous condition and activate a protective or corrective device or mechanism to prevent hazardous events from arising, or providing mitigation to reduce the consequence of the hazardous event [3]. Two main standards govern the requirements for and implementation of functional safety in factory automation: International Electrotechnical Commission (IEC) 61508 and International Organization for Standardization (ISO) 13849. **Figure 1** shows the standard landscape in some common industrial applications.

## IEC 61508 and derived standards in factory automation

IEC 61508 covers the complete life cycle of safety systems and demands a ground-up approach, starting from the design/development stage. It is purposefully generic and covers a broad swath of the smart factory value chain, from factory systems to equipment manufacturers – and by inference, impacting component providers such as semiconductor manufacturers.

IEC 61508 measures the confidence of safety implementation in a system via safety integrity levels (SILs), which indicate the relative level of risk reduction that a safety function provides. There are four levels defined by the standard, from 1 through 4. Level 1 is the lowest level and level 4 is the highest. Smart factory systems typically conform to SIL-2 or SIL-3. Systems that have catastrophic, large-scale failure consequences (such as nuclear reactors) conform to SIL-4.

IEC 61508 also addresses hardware fault tolerance (HFT) requirements. HFT is the ability of a component or subsystem to continue delivering a required safety-instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that, for example, there are two components in a system and the architecture is such that the dangerous failure of one of the two components does not prevent the safety action from occurring [4].

Different industries/applications have adapted IEC 61508 for their specific functional safety requirements through additional derived standards. The most common in factory automation include IEC 61131-6 for safe programmable logic controllers (PLCs), IEC 62061 for industrial machinery, IEC 61800-5-2 for variable speed drives and IEC 61511 for industrial process control. All of these standards have adopted the SIL methodology to measure safety levels.

## ISO 13849 in factory automation

For industrial machinery safety, ISO 13849 is the successor to the older machinery European standard (EN) 954-1 functional safety standard, and covers safety requirements (including software) through the life cycle of safety-related machinery and their components in control systems. The

process identifies the parts in the system that perform safety functions as well as the necessary safety performance level (PL) for the system. Each relevant component then needs to perform at a level equal to or greater than the requirement for the whole system, which when combined with the architectural category of the component (category [Cat] levels 1 through 4) arrives at a comprehensive set of safety requirements [5].

Performance levels (PL) go from a to e (in increasing order of reliability). Category designations (Cat) go from B, then 1 through 4 (on a scale of increasing safety requirements). Typical industrial machinery systems are Cat3 or Cat4, PLd and in some instances PLe.

For specific applications, such as with IEC 61508, additional standards will refer to ISO 13849 and provide further clarification and guidance (such as for correlating categories and PLs). Examples include ISO 10218 and American National Standards Institute (ANSI)/Robotic Industries Association (RIA) R15.06 (2012) for industrial robots and robot systems.

## IEC 62061 vs. ISO 13849

In industrial machinery systems that are electronic or programmable-electronic, there is no clear distinction or guideline on whether to use ISO 62061 or ISO 13849 for functional safety. The choice will depend on the end user requirements (PL or SIL methodology preference) and/or past design methodologies and comfort levels. For systems that are not electronic/electrical, ISO 13849 may be more appropriate [6].

Both IEC 62061 and ISO 13849 have published reports/addenda to the main standard (IEC/technical report [TR] 62061-1 and ISO TR 23849) that can help in making a decision between them.

## Safety systems requirements flow to processing/communication subsystems

A typical factory automation safety-related system consists of sensors (a data collection subsystem), a logic subsystem (data processing and communication, local or to the network) and actuators (a control subsystem). Of course, software implementations are a key piece. The logic subsystems typically have microcontrollers (MCUs) and/or processors and their design/architecture plays a role in the system's safety architecture. Designing a system where the processor takes functional safety requirements into consideration, both from a hardware and software standpoint, greatly reduces the cost and complexity of designing a functionally safe system.

As an example, for functionally safe (FS) PLCs, IEC 61131 is a product-specific implementation of the requirements of IEC 61508 [7]. Processor vendors should consider the functional safety and safety integrity requirements of an FS PLC system outlined in IEC 61131, in conjunction with their customer requirements.

## Processor/system-on-chip architectures for functional safety

Depending on the application, safety requirements, and the amount and complexity of data, there are various ways to implement a safety system with a controller or processor. The biggest priorities for safety architecture designers are:

- Targeted safety level.
- Simplicity of solution (previous design experience, time to market).
- Product cost (integration, form factor).
- Product application and testability/diagnostic capability.
- Certification time/cost.

The trend toward digitization and increased data collection/processing and communication (including over networks) means that functional safety architecture and implementation are also evolving. Functional safety addresses two categories of faults: systematic and random. These faults become failures when a fault results in a loss of safety function or violates a safety goal.

Systematic faults arise from errors in design/development, manufacturing or operational processes. Examples of systematic faults include design bugs coupled with a failure to verify designed functionality, manufacturing test escapes or operating a product outside of guaranteed parameters. Faults in software are also considered systematic, as software is fully deterministic. Managing systematic faults is possible through the implementation of robust processes that include checks and balances in development, manufacturing and operation – it's best if they're performed from the ground up.

Random faults, on the other hand, can occur unpredictably during the lifetime of a component, requiring a focus on diagnostics and safety mechanisms to detect and manage. Examples of random faults include the temporary corruption of static random access memory (SRAM) data due to a soft error, or brownout conditions due to voltage glitches shorting adjacent signals in an integrated circuit (IC) package.

Mechanisms for functional safety detect faults during normal operation, executing within the fault-tolerant time interval of the targeted system. This puts a premium on periodically executed or continuously operating diagnostics over those that can be executed only upon system startup or shutdown. As control-loop timing requirements are tighter in more modern systems, safety mechanisms may need parallel and continuously operating diagnostics.

## Functional safety architectures

Two of the most common architectures implemented to detect random faults are single- and dual-channel systems.

Single-channel systems are typically the simplest to implement and use existing processing, memory and data communication paths in the system. However, the reliability and diagnostic ability of most implementations are limited by the fact that the diagnostic functions run on the same data/power/clock lines as the main system. Simplicity has a price, and the safety and performance levels of such systems are typically limited to SIL-2 or below and Cat-2 systems with PLc or below.

Dual-channel architectures provide two completely independent data/logic processing and communication, voltage and clock paths throughout the system. Not only is there independent redundancy, but it's possible to execute and compare any necessary safety functions on both channels. It's extremely unlikely that the same error will occur on both. However, if the results between the channels don't match and an error is detected on one of them, both systems can be brought safely to a safe state.

Dual-channel architectures are more expensive to implement than single-channel architectures and more complex to design, but can achieve higher SILs/PLs. SIL-3 and Cat-3/Cat-4 PLd and PLe systems typically use this approach.

## The move toward integration

Traditional dual-channel safety system designs included two separate processing ICs (not on the same piece of silicon). In most industrial applications, this is still true. The main processing element is increasingly responsible for not just safety diagnostic and compare functions but also for some combination of data analysis, control and

communication functions. The “checker” processing element is a separate chip with its own data, clock and power paths.

With the trend toward miniaturization and lower cost, over the past five years there has been a corresponding movement toward the integration of safety functions, driven first within the automotive industry. Both processing elements are integrated on the same piece of silicon.

An example of this approach is the Hercules™ MCU platform from Texas Instruments (TI). The Hercules MCUs functional safety architecture concept is called a “safe island” approach. The basic concept involves a balance between the application of hardware and software diagnostics to manage functional safety while balancing cost concerns. In the safe island approach, a core set of elements are allocated to continuously operating hardware safety mechanisms. This core set of elements – including power/clock/reset, a central processing unit (CPU) (in this case, an Arm® Cortex®-R5F real-time MCU core), flash memory, SRAM and associated interconnect – guarantees the functionally correct execution of software.

In addition to the elements noted above, software executing on these elements can provide software-based diagnostics for other device elements such as peripherals. This concept has been proven viable through multiple generations of safety-critical products in the automotive passenger vehicle space [8]. Combined in a system with a complementary power-management IC (PMIC), this approach enables safety levels as high as SIL-3. Meeting an HFT equal to 1 or SIL-4 with this approach would require two Hercules controllers or the use of augmented traditional dual-channel solutions.

## The evolution of processor capabilities in a digitized factory

Given the ever-increasing complexity of factory automation systems, next-generation processors are integrating more system-level requirements on-chip. This includes high-speed communication interfaces, multiple processor cores to handle the data processing (with real-time cores to perform tight control-loop functions) and security functions on the same piece of silicon.

Having multiple types of processing cores (such as Arm Cortex-A, Cortex-R5F and Cortex-M) and implementing the right functional safety capabilities (isolated power and clock domains for different cores, hardware diagnostic functions) can give system designers a lot of flexibility in implementing their safety architecture, either by:

- Using one of the processing cores on-chip for safety functions (with an external checker) while partitioning the rest of the processor to perform control, processing and/or communications.
- Implementing a safety island on the processor with two processing cores and saving additional printed circuit board (PCB) space and bill-of-materials cost.

The safety island concept offers more integration on a single piece of silicon, a lower failure-in-time (FIT) rate (vs. multiple ICs) and lowers PCB footprint. But at the same time, it can also complicate the unambiguous determination of dependent and common-cause failure modes, a key requirement for functional safety. Simplicity is often favored in safety certifications; therefore, it is important to balance the need for cost, footprint and safety certification efforts.

TI's new AM65x family of Sitara™ processors offers factory automation vendors the flexibility to choose the best architecture for their system. It offers multiple processing cores for both performance and real-time processing needs. It is also includes the necessary safety architecture and diagnostic features to enable functional safety systems for Industry 4.0 factories. The AM65x supports both an independent dual-channel approach with an external checker processor/MCU, as well as an integrated safety island option with the lockstep approach and an external PMIC (**Figures 2, 3** and **4**).

## Making certification easier

System-/equipment-level certification can benefit from component-level certification and/or FIT/failure injection data to reduce cycle time and certification complexity. Again, a system that needs to meet a certain safety or performance level must have all safety-critical components meet or exceed that level. This includes information to address both systemic and random fault scenarios.

### Deliverables from the IC vendor that can help include:

- *Documentation:*
  - o A component safety manual detailing the product safety architecture and recommended usage.
  - o A safety analysis report summary, with a summary of the FIT rate along with failure modes, effects and diagnostic analysis (FMEDA) at the component level for IEC 61508.
  - o A detailed safety analysis report, with full details of all safety analysis executed down to the module (IP) level for IEC 61508, as well as a software tool for customizing the analysis results to the specific application.
  - o A safety report summarizing compliance to IEC 61508.
  - o A third-party assessment of development flow in accordance with IEC 61508.
  - o Component-level certification.

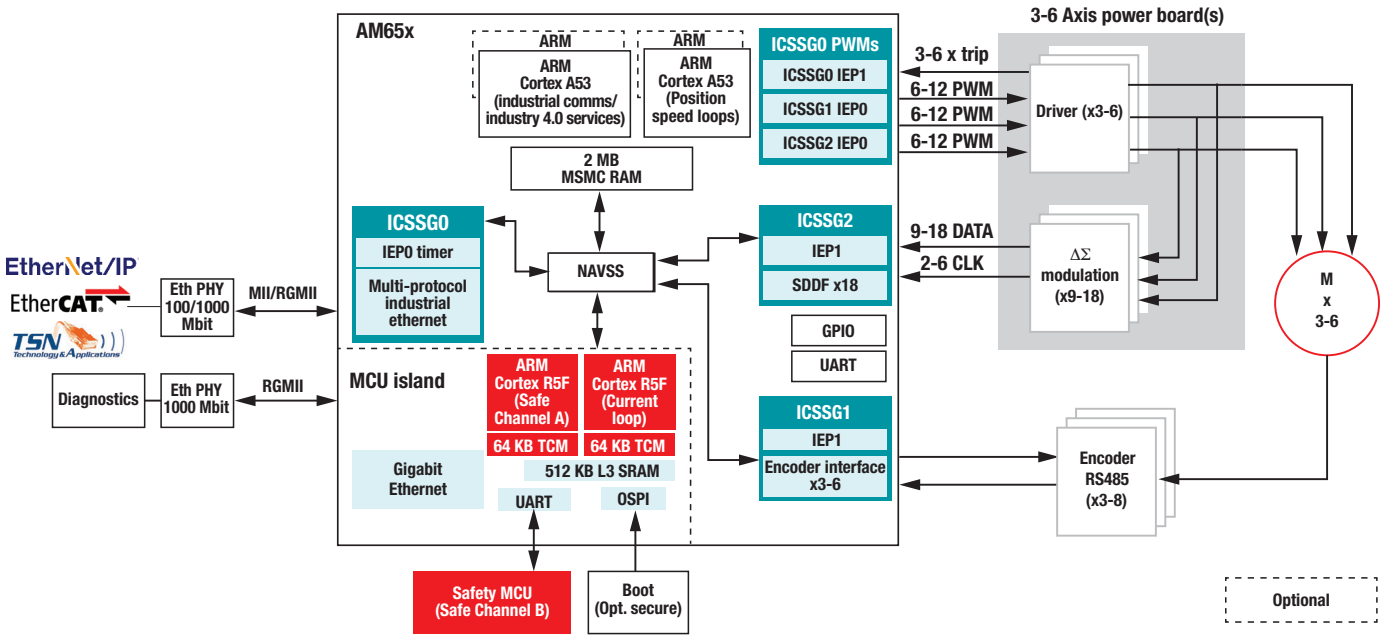


***Figure 2**. AM65x – Centralized smart servo drive.*

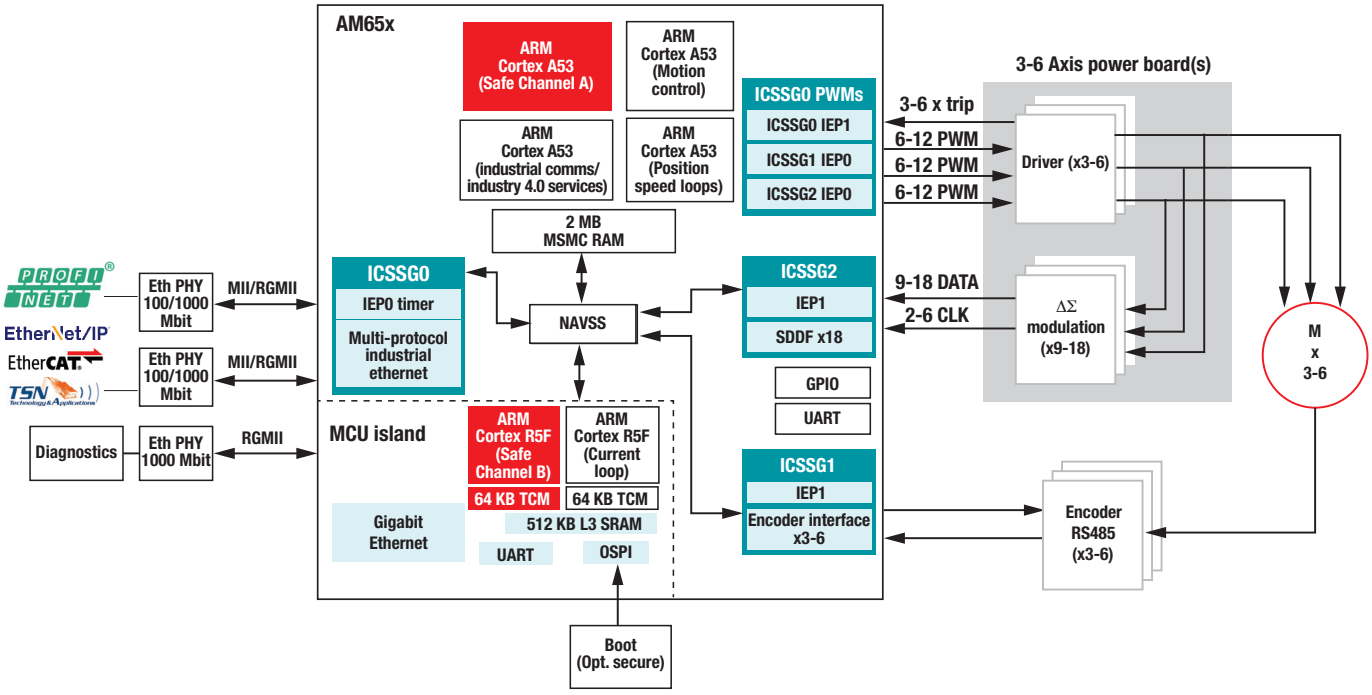


***Figure 3**. AM65x – Integrated robot CPU board.*

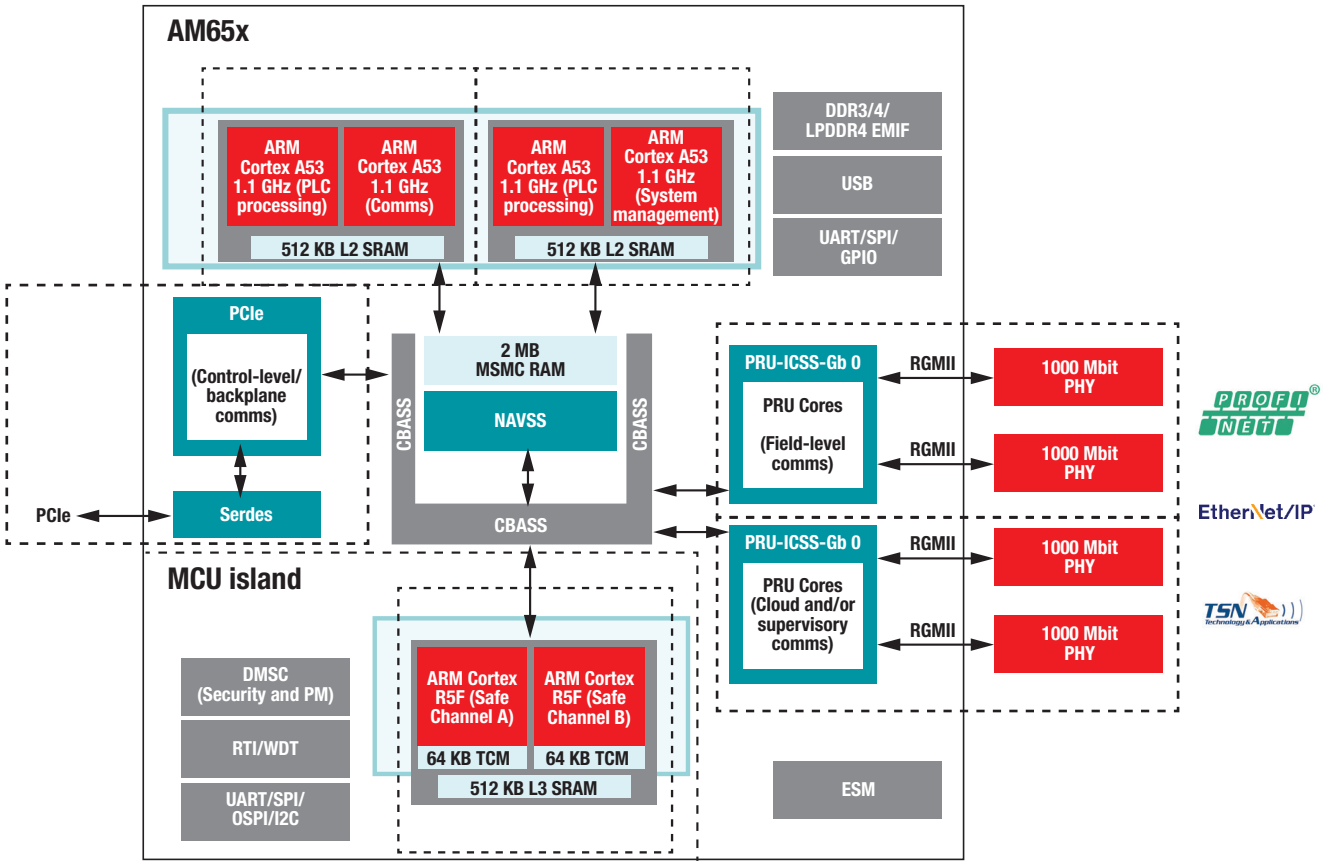


***Figure 4**. AM65x – Safe PLC - PLC Controller CPU.*

- *Software:*
  - o A safety compliance support package according to IEC 61508, including software documentation and testing to assist in compliance with functional safety standards. The package includes safety requirements documents, code review and coverage reports, unit test results and software safety manuals – and ideally also includes unit test capability using tools such as a Liverpool Data Research Associates (LDRA) unit.
  - o Safety tool documentation and qualification according to IEC 61508 that assists in the qualification to functional safety standards, including a tool classification report, tool qualification plan and report, tool safety manual, and test automation unit.
  - o A safety diagnostic library that provides interfaces and a framework for initializing and enabling safety diagnostics/features, fault injection to allow the testing of application fault handling, a handler callback routine, and profiling for measuring time spent in diagnostic test/fault handling.
  - o Development tools assessed and/or certified as suitable for use with IEC 61508, including integrated development environments and compilers and Joint Test Action Group emulators/traces.

The AM65x family of industrial processors will have this comprehensive design support package.

## Summary

Industry 4.0 is driving increased needs for functional safety. Component-level needs are increasing and architectures are evolving to meet the future needs of a digitized smart factory. Processor vendors have a key role to play to support the demanding needs of new products, approaching safety from the ground up and offering innovative and flexible architectures, as well as a support infrastructure to enable system-level certifications. TI has been a leader in delivering processing solutions for applications demanding functional safety, and the AM65x family will continue that trend.

## References


1. Accenture. 2018. Industry X.0.
2. Marr, Bernard. 2016. "What Everyone Must Know About Industry 4.0."
3. International Electrotechnical Commission. 2018. Functional Safety.
4. Generowicz, Mirek. 2015. "Achieving Compliance in Hardware Fault Tolerance."
5. Nix, Doug. 2017. "ISO 13849-1 Analysis – Part 3: Architectural Category Selection."
6. TÜV SÜD. 2018. "SIL or PL? What is the difference?"
7. PLCopen. 2018. Introduction into IEC 61131-6 functional safety.
8. Texas Instruments. 2011. "Hercules™ Microcontrollers: Real-time MCUs for safety-critical products."

# IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), 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, regulatory 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 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.

TI objects to and rejects any additional or different terms you may have proposed.

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