Application Report
SPRY324–October 2018

Designing Embedded Systems for High Reliability With Sitara™ AM6x Processors

Mike Hannah, Neil Simpson

ABSTRACT

TI has designed the K3 multi-core SoC architecture platform with a foundation of reliability. The Sitara™ AM6x processors are the first generation processors of this platform.

Contents

1 Introduction 2
2 Transient Errors 3
3 Permanent Errors 6
4 SoC Safety Documentation and Support 7
5 Conclusion 8

List of Figures

1 AM65xx Block Diagram 5
2 Reliability Bathtub Curve 6
3 Design for Intrinsic Reliability Process Flow 7

Trademarks

Sitara is a trademark of Texas Instruments.
Arm, Cortex are registered trademarks of Arm Limited.
All other trademarks are the property of their respective owners.

Copyright © 2018, Texas Instruments Incorporated

1 Introduction

With the increasing focus on efficiency and productivity, factory automation equipment manufacturers have joined the aerospace and defense industries' reliability bandwagon, striving to minimize manufacturing down time and failure. As a result, reliability design requirements are often mandated by factory automation equipment manufacturers. Other industrial markets, such as power grid infrastructure, building automation, and medical, are also starting to demand increased reliability for their products. Systems engineers must not only focus on embedded solutions that meet cost and performance goals, but on devices that help to assure overall end equipment reliability requirements. While integrated circuits have enabled quantum leaps in performance, size, and overall cost of embedded systems, the reliance on various memory elements and employment of small-geometry silicon process technologies introduce reliability challenges.

An issue with some of the first Intel Dynamic Random Access Memory (DRAM) chips in the early 1970s is described in an article in the December 2015 issue of *IEEE Spectrum* magazine. As densities of the memories grew from 1 KByte to 16 KBytes, the DRAMs started to exhibit a high number of bit errors. These errors impacted program execution and the reliability of the operational data. The source of the high number of bit errors was found to be caused by radioactive material that had found its way into the ceramic package. The radioactive material emitted alpha particles that caused bits to invert erroneously from the correct logical value.

Despite improvements in removing these alpha-emitting particles on those first DRAM devices, alpha particles are still an issue that affects not only the reliability of DRAMs but also other silicon-based device memories. Twenty-first century embedded System-on-Chip (SoC) devices with multiple processor cores, large internal caches and memories, and fixed-function logic dedicated to acceleration tasks are all susceptible to the same “soft” transient errors that can plague DRAMs.

Silicon device reliability requires managing failures that can prevent the device from malfunctioning at any point during its expected lifetime. From a design for reliability perspective, this means designing the device to meet market-driven failure rates that are acceptable for both transient and permanent faults.

Transient errors are random errors which are not persistent. They occur and then disappear. However, their effects may persist, by leaving the wrong value in a flip-flop or SRAM bit, and include the following characteristics:

- They affect both SRAM and logic.
- The device itself is not damaged, and the root cause of the error is often impossible to trace.
- The error is caused by external elements and not a physical defect on the silicon itself.

Permanent errors are repeatable errors induced by faulty device operation, and typically have the following attributes:

- The root cause is due to physical damage or a defect in the circuit.
- These types of physical errors contribute to silicon failure metrics.
- Data is lost and can no longer be restored to that location.
- Some examples of permanent failure mechanisms are Gate Oxide Integrity (GOI) and Electro-Migration (EM).

To minimize both transient and permanent errors in a complex SoC, reliability must be designed into the SoC from the ground up; it is not something that can be worked around or dealt with after the SoC is in production. While performance is always at forefront of requirements for an SoC, reliability must be an intrinsic part of the foundation if that device is to function properly for multiple years in reliability-critical applications, such as factory automation, transportation, defense, and medical. To meet the reliability demands of those markets, TI has designed the K3 multi-core SoC architecture platform with a foundation of reliability. The Sitara AM6x processors are the first generation processors of this platform.

Copyright © 2018, Texas Instruments Incorporated

2 Transient Errors

Over time, silicon device manufacturers have found that in addition to alpha particles causing transient errors in memory and logic (registers and latches), neutrons can also affect the reliability of the device. To assess the impact for a chip design such as the AM6x processor, alpha and neutron tests were run on TI or foundry test devices and were compliant with the JESD89A specification: “Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices.” For the alpha and neutron tests, the test chips were subjected to an alpha or neutron source to count the number of bit errors. The calculations for the alpha test were then used to determine the impact of alpha particles on the package. For the neutron tests, the calculations were used to determine the impact of neutron particles at different geographical locations and altitudes determined by the relative flux density.

Using the observed data collected from both the alpha and neutron tests, TI has developed a proprietary transient Soft Error Rate (SER) estimator tool. The tool estimates the SER for each functional sub-element in a device such as the AM6x processor for a cumulative total SER for the device. The SER tool uses the following inputs to accurately estimate the soft failure rate:

- Static Random Access Memory (SRAM) (Megabits) / Memory bit cell type
- Logic (Megabits – 1 register = 1 bit)
- Protection included (Parity or Error Correcting Code)
- Process technology
- Core voltage / Chip temperature
- Package type / # metal levels / # Bumps / Bump diameter
- Chip area
- Geographical factor (sea level altitude)
- Product lifetime

To address this high reliability requirement in today’s embedded systems marketplace, the AM6x processor was designed with specific reliability targets. TI set the goal of achieving an overall total SER of less than 250 Failures in Time (FIT) at New York City sea level and device temperature of 25 degrees Celsius. A single FIT—as calculated by the TI SER tool— is a single undetected failure in one billion hours of operation and the inverse of the FIT value is the Mean Time Before Failure (MTBF). Thus for the AM6x processor, the MTBF is greater than 400 years. This may seem like overkill for a device. However, if one considers a factory automation application like a Programmable Logic Controller (PLC), there may be close to a 100 PLCs controlling all of the operations in a large factory. If each PLC used a processor that had a MTBF of only 100 years, that would present the possibility of a device requiring reboot once each year due to a transient error. This would be intolerable in today’s factories, where minutes of downtime can mean millions of dollars in lost product manufacturing.

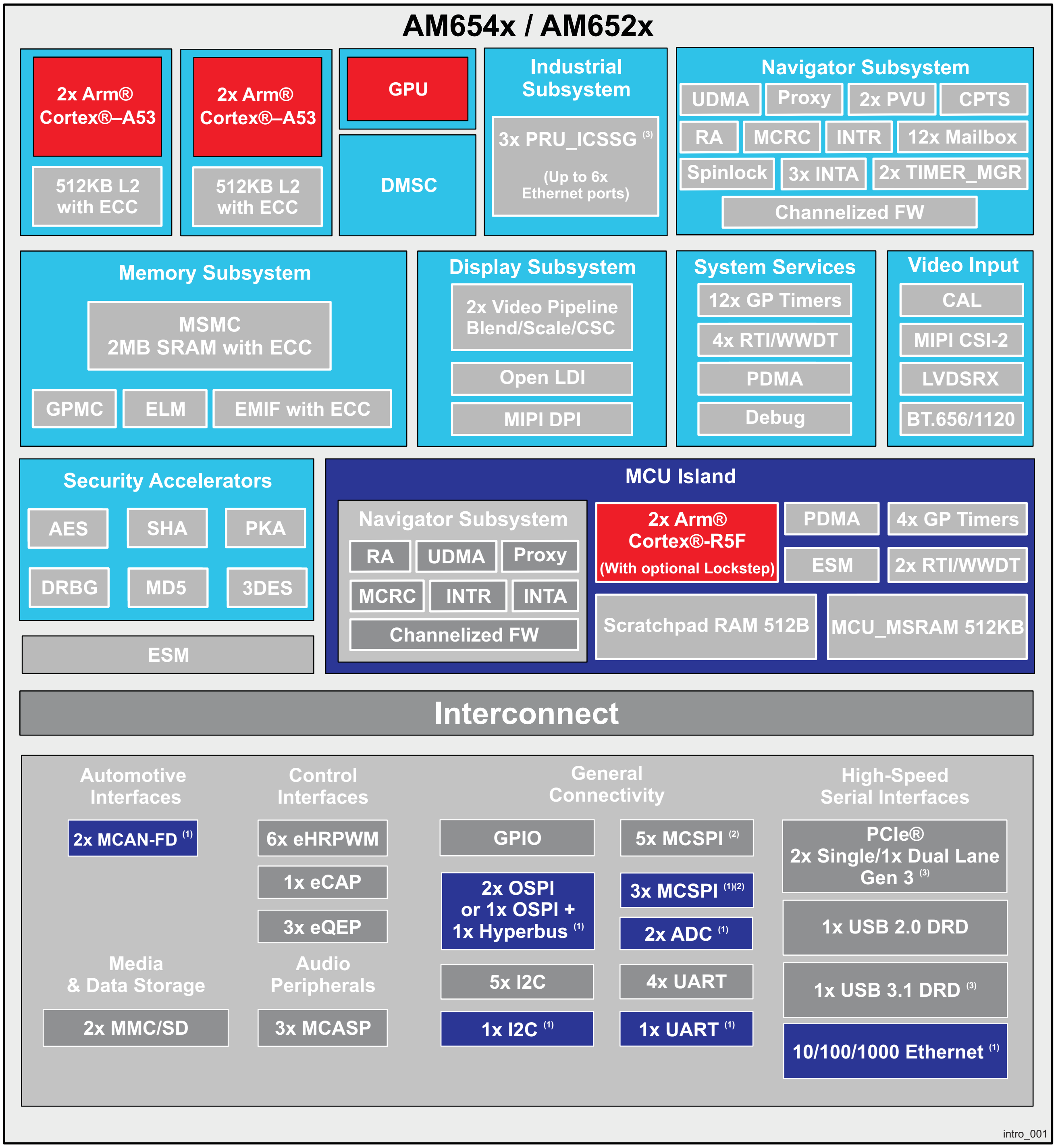
For the AM6x processor, careful design consideration was put into each functional block of memory and logic to ensure that the total SER was less than 250 FIT. Error Correcting Codes (ECC), parity bits, and Cyclic Redundancy Checks (CRC) were employed to detect and correct bit errors, significantly reducing the SER across the device. The ECC method used in the AM6x processor is Single Error Correction and Dual Error Detection (SECDED), and was heavily employed on nearly every block of memory in the device. Using SECDED, a single bit error is detected and corrected in hardware. For dual-bit errors, the errors are detected and the appropriate processor is signaled in the device to take action on the dual-bit error. A list highlighting some of the key functional blocks using these SER reduction techniques is given below and shown in Figure 1:

- ECC and/or parity on Arm® Cortex®-A53 Level 1 and Level 2 memories
- ECC on Arm Cortex-R5F caches and Tightly-Coupled Memory (TCM)
- ECC on MCU Subsystem (MCUSS) Scratchpad RAM, SRAM, Vectored Interrupt Manager (VIM) memory, and parity on Region-Based Address Translation (RAT) registers
- ECC on Multicore Shared Memory Controller (MSMC) memories, MSMC Data Routing Unit (DRU), and MSMC SRAM (can also be L3 cache)
- ECC on PRU-ICSS-Gb Instruction, Data, and Shared RAM and integrated CRC accelerators
- ECC support on DDR External Memory Interface (EMIF)
- Parity on Interconnect control registers

Copyright © 2018, Texas Instruments Incorporated

- ECC on Peripheral Component Interconnect express (PCIe) and Universal Serial Bus (USB)
- ECC on MMC/SD, HyperBus, Octal-SPI, MCAN-FD, and ADC memories
- ECC on Peripheral DMA (PDMA) memory
- ECC in several Navigator Subsystem (NAVSS) blocks
  - Peripheral Virtualization Unit (PVU) memory and parity on registers
  - Ring Accelerator (RA) proxy data buffers
  - Unified DMA (UDMA) memory
  - Timer Manager memory
  - Mailbox memory
- Memory Cyclic Redundancy Check (MCRC) accelerator in NAVSS
- ECC on Security Accelerator memory

Copyright © 2018, Texas Instruments Incorporated



Copyright © 2018, Texas Instruments Incorporated

(1) This interface is located on the MCU Island but is available for the full system to access.

(2) One port is internally connected only; not connected to any pins.

(3) SGMII, USB3.1 and PCIe share a total of two SerDes lanes.

Figure 1. AM65xx Block Diagram

In addition to the already low total SER on the AM6x processor, the actual SER for a specific use case may be further reduced by selectively removing the FIT contribution of unused functions in the device. TI can provide detailed information, under a non-disclosure agreement, to enable a customer to perform this selective derating procedure if desired. To request SER data, submit a request to the TI Support Center at http://www.ti.com/supportcenter.

To use the “Email TI” option for this case, select the following:

- The issue type would be “Quality, Reliability, Environmental.”
- In the description section, state the full orderable TI device part number.
- Include your company name.
- Include your project or product for which the information is needed.
- State what information is needed and why it is needed.

The Support Center will evaluate your request.

3 Permanent Errors

Reliability of an SoC is also impacted by “hard” permanent errors due to possible failure mechanisms in the device design and silicon process. From an overall failure mode perspective, the type of error is determined by where a device is within its lifecycle when compared to the traditional reliability “bathtub” curve view, as shown in Figure 2.

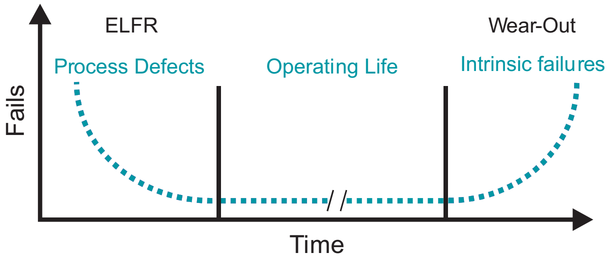


Figure 2. Reliability Bathtub Curve

The bathtub curve provides a simplified overview of the three primary phases of a semiconductor device product lifetime.

Early life failure rate (ELFR): This phase is characterized by a relatively higher initial failure rate, which decreases rapidly. The failures observed during this phase are extrinsic failures and are typically measured as “defective parts per million” (dppm). From a development perspective, these are removed by applying additional test screens or process updates.

Operating life: This phase consists of a relatively constant failure rate, which remains stable over the useful lifetime of the device. The failure rate is described in units of FITs, or alternatively as a Mean Time Between Failures (MTBF) in hours.

Wear-out phase: This represents the point at which intrinsic wear-out mechanisms begin to dominate and the failure rate begins increasing exponentially. The product lifetime is typically defined as the time from initial production until the onset of wear-out.

To manage the intrinsic failure rate, it is necessary to have a robust design process that ensures that the required level of reliability is designed in the physical construction of the device. To achieve this, reliability requirements are defined and driven into the component and library level, then validated at the SoC design level, as depicted in Figure 3 on the previous page.

Copyright © 2018, Texas Instruments Incorporated

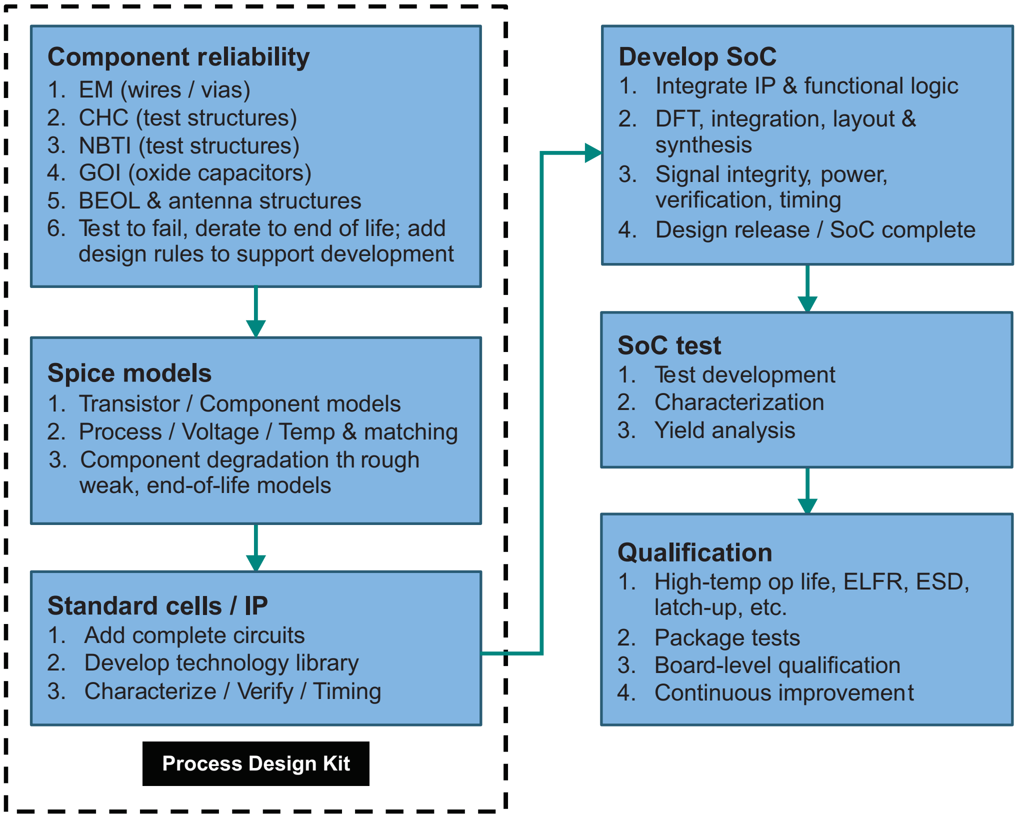

Component reliability
1. EM (wires / vias)
2. CHC (test structures)
3. NBTI (test structures)
4. GOI (oxide capacitors)
5. BEOL & antenna structures
6. Test to fail, derate to end of life; add design rules to support development
Spice models
1. Transistor / Component models
2. Process / Voltage / Temp & matching
3. Component degradation th rough weak, end-of-life models
Standard cells / IP
1. Add complete circuits
2. Develop technology library
3. Characterize / Verify / Timing
Process Design Kit
Develop SoC
1. Integrate IP & functional logic
2. DFT, integration, layout & synthesis
3. Signal integrity, power, verification, timing
4. Design release / SoC complete
SoC test
1. Test development
2. Characterization
3. Yield analysis
Qualification
1. High-temp op life, ELFR, ESD, latch-up, etc.
2. Package tests
3. Board-level qualification
4. Continuous improvement

Figure 3. Design for Intrinsic Reliability Process Flow

The AM6x processor was designed using TI's reliability process to ensure that it could meet the market-driven intrinsic failure rate requirements. Additionally, the AM6x was designed to operate up to an estimated 100k power-on hours (POH) at maximum frequency for all functional blocks and with Arm Cortex-A53 cores at 1.0 GHz. This can be achieved at maximum junction temperature of 105°C. By maintaining a slightly lower junction temperature of 95°C, the estimated operating lifetime can be doubled to 200k POH.

TI provides a detailed quality and reliability section on the TI website which discusses quality and reliability for all TI devices, including the AM6x processor: www.ti.com/quality

At this webpage, details can be found on TI's quality policies and procedures, environmental information, product shelf life, reliability and reliability calculators, certifications and standards, and other resources such as a quality and reliability FAQ.

4 SoC Safety Documentation and Support

To assist customers who need to certify their end product for a specific functional safety level, TI provides collateral to ease the burden of doing so with the AM6x processor. The AM6x is a Quality Managed (QM) product that is designed to be compliant to applicable quality standards such as ISO/IATF 16949 or ISO 9001. It is also in the process of being certified for functional safety standards such as IEC 61508 or ISO 26262, to achieve a Safety Integrity Level (SIL) or Automotive Safety Integrity Level (ASIL), respectively, as a Safety Element out of Context (SEooC). The AM6x by its design is intended to be used as an element in a functional safety design, but safety certification is contingent upon results of a system-level functional safety qualification activity. System-level qualification is the responsibility of the end customer, who owns the definition and design of the safety system.

Copyright © 2018, Texas Instruments Incorporated

TI delivers an AM6x Safety Manual and a Failure Modes Effects and Diagnostic Analysis (FMEDA) tool to assist in system-level certification efforts. The safety manual describes the development process applied and the measures taken to avoid systematic failures. It provides an overview of the AM6x processor architecture and a breakdown of the design into sub-elements to support customer safety analysis. It includes assumptions of use that were utilized in the Safety Element Out-of-Context (SEooC) analysis. It also includes a description of functionality, operating states, and any features supporting error management. The safety manual also includes details of diagnostic measures supported to detect faults in each design sub-element.

The FMEDA tool is constructed in accordance with the requirements specified by the ISO 26262 and IEC 61508 standards. For the transient faults, TI uses the lambda fail rates from the TI SER estimator tool. For the permanent faults, TI uses the lambda fail rates as defined by the IEC 62380 standard model. In addition to the detailed calculations, user control is provided for the following:

- Mission profile tailoring
- Function and diagnostic tailoring
- Package pin-level tailoring

Mission profile tailoring allows the selection of ambient temperature, duration, number of starts, and other factors per the IEC 62380 model. It also allows the user to tailor package type, life cycle (power-on hours), and safe versus non-safe faults. The function and diagnostic tailoring of transient and permanent faults allows selection of user-defined fraction of safe failures, safety hardware to be considered in the analysis, inclusion and definition of any safety mechanisms, and diagnostic coverage of the safety mechanisms. Package pin-level tailoring allows for control over which pins need to be considered in the analysis and diagnostic coverage control for each pin.

5 Conclusion

In summary, the Sitara AM6x processor is designed for high-reliability applications providing low transient failure rates and estimated active lifetimes of more than 10 years and in some use cases over 20 years. As the AM6x is in the process of being safety-certified, TI offers the tools and guidance that customers can leverage to achieve specific SIL or ASIL certifications for their end products at the system level. With multiple Arm Cortex-A53 cores and Arm Cortex-R5F cores, the AM6x offers significant performance that is scalable and dependable. Whether the application is an automotive gateway or a PLC managing numerous critical operations in networked 21st century factory, the AM6x processor is a reliable choice for the application.

For more details on the AM6x family of Sitara devices, visit www.ti.com/sitara.

Copyright © 2018, Texas Instruments Incorporated

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
Copyright © 2018, Texas Instruments Incorporated