Designing embedded systems for high reliability with the 66AK2Gx DSP + ARM® processor

Texas Instruments

Mike Hannah
Senior Member of Technical Staff
Systems Engineer
Processors Business Unit

Neil Simpson
Embedded Processing
Design Quality Manager

Texas Instruments

Introduction

With the 21st century focus on efficiency and productivity, factory automation equipment manufacturers have joined the aerospace and defense industries reliability bandwagon, striving for little to no down time or failure on manufacturing floors. Subsequently, reliability design requirements are now often mandated by factory automation equipment manufacturers. Product engineers must not only focus on embedded solutions that meet cost and performance goals, but devices that will 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 made to remove these alpha-emitting particles on those first DRAM devices, alpha particles are still an issue that affect not only the reliability of DRAMs but also other silicon-based device memories today. 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 cause the device not to function correctly at any point during its expected lifetime. From a design for reliability perspective, this means designing the device to meet market-driven transient and permanent failure rate requirements.

Transient errors are random errors induced by an event which corrupts the data stored in a device (usually only a single 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
- These types of errors do not contribute to silicon failure metrics as the silicon is still functional.

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

- The root cause is due to physical damage to the circuit
- These types of physical errors contribute to silicon failure metrics

- Data is lost and data can no longer be restored to that location.
- Some examples of permanent failure mechanisms are Gate Oxide Integrity (GOI) and Electo-Migration (EM)

To minimize both transient and permanent errors in a complex SoC, reliability has to 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. And while performance and latency are always at forefront of requirements for an SoC, reliability has to 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, military and medical. To meet the reliability demands of those markets, TI has laid this reliability foundation with the design of the high-performance 66AK2Gx processor SoC.

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) accuracy, neutrons can also affect the reliability of the device. To assess the impact for a chip design such as the 66AK2Gx 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 66AK2Gx 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 market, the 66AK2Gx processor was designed for such and 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). So for the 66AK2Gx processor, the MTBF is greater than 400 years. This may seem like overkill for a device. However, if you consider 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 possibly millions of dollars in lost product manufacturing.

For the 66AK2Gx 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/or correct bit errors significantly reducing the SER across the device. The ECC method used in the 66AK2Gx processor is Single Error Correction and Dual Error Detection (SECDED). 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 parity on DSP Level 1 and Level 2 memories
- ECC and parity on A15 Level 1 and Level 2 memories
- ECC on Multicore Shared Memory Controller (MSMC) L2
- ECC on Queue Manager
- ECC on Network Coprocessor
- Software Cyclic Redundancy Check (CRC) in the Network Subsystem (NSS)
- ECC on Power Management Microcontroller (PMMC)

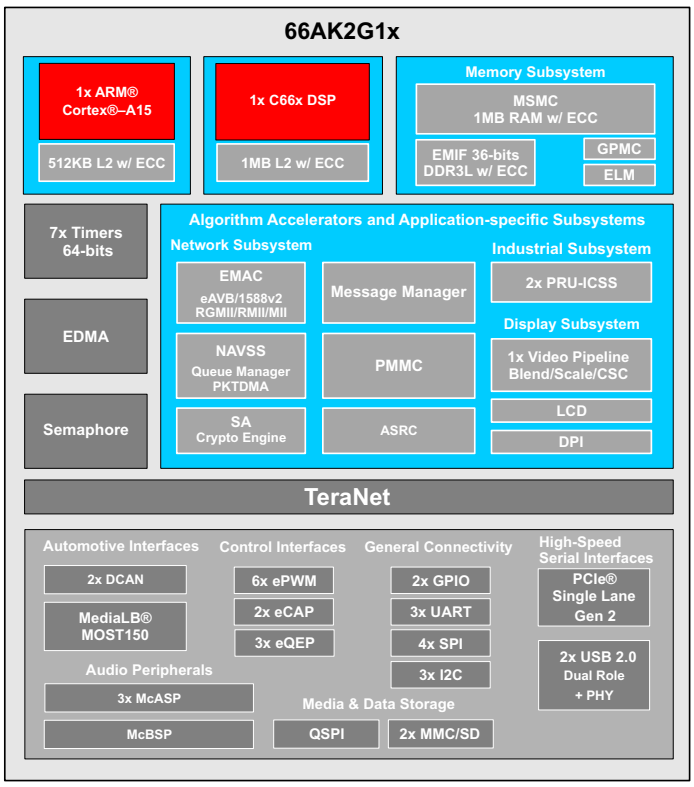

Figure 1: 66AK2Gx processor functional diagram

- ECC on DDR External Memory Interface (EMIF)
- ECC on Peripheral Component Interconnect express (PCIe) and Universal Serial Bus (USB)

In addition to the already low total SER on the 66AK2Gx processor, the actual SER for a specific use case may be reduced even further 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.

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.

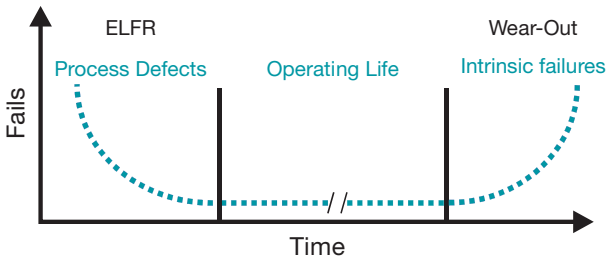

Figure 2: Reliability bathtub curve

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.

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 and / 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

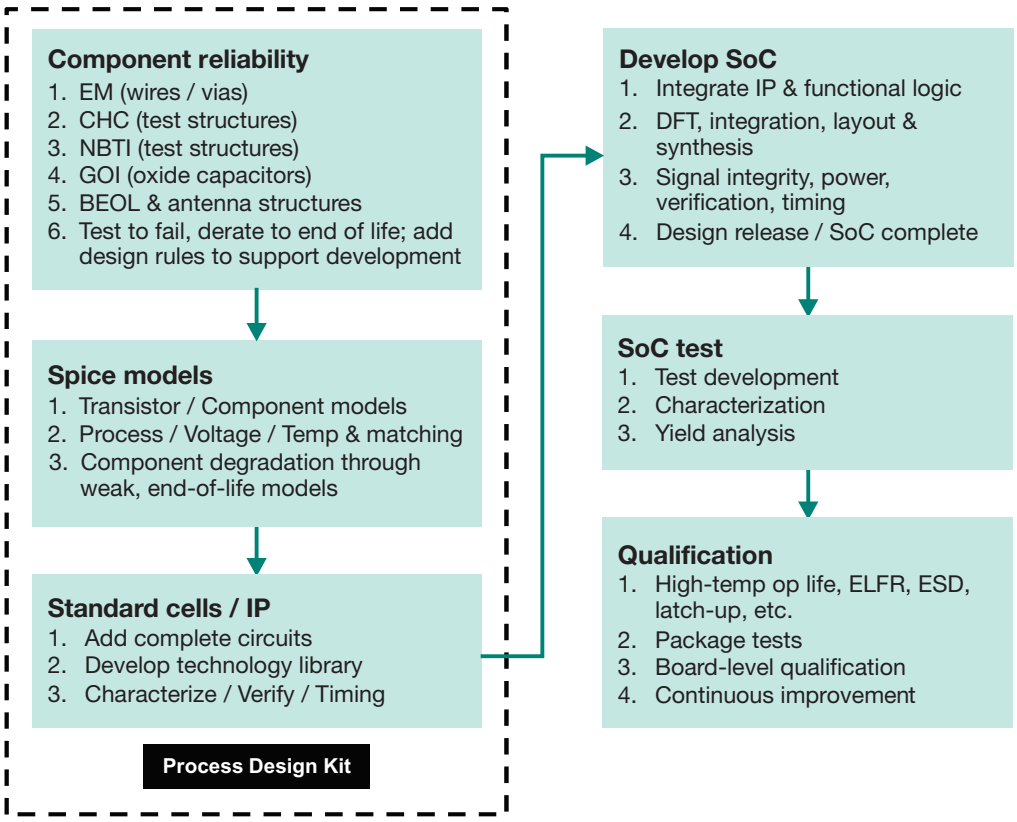

Figure 3: Design for intrinsic reliability process flow

the required level of reliability is designed in and is therefore correct by physical construction of the device. To achieve this, reliability requirements are defined and driven into the component / library level and then validated at the SoC design level as depicted in Figure 3 on the previous page.

For more information please see the Quality and Reliability section on TI.com:
www.ti.com/quality

The 66AK2G processor device was designed using TI's reliability process to ensure that it could meet the market-driven intrinsic failure rate requirements.

SoC reliability documentation and support

To assist customers who need to certify the reliability of their end product for a specific functional safety level, TI provides collateral to ease the burden of doing so with the 66AK2Gx processor. The 66AK2G processor is a Quality Managed (QM) product. A QM product is designed compliant to applicable quality standards such as ISO/TS 16949 or ISO 9001. However, it is not certified for applicable functional safety standards such as IEC 61508 or ISO 26262 to achieve a specific Safety Integrity Level (SIL) or Automotive Safety Integrity Level (ASIL) respectively. The 66AK2Gx processor by its design is intended to be used as an element in a specific 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.

TI delivers a 66AK2Gx processor Safety Architecture Manual (SAM) and a Failure Modes Effects and Diagnostic Analysis (FMEDA) for system-level certification efforts. The SAM describes the development process applied and the measures taken to avoid systematic failures. It provides an overview of the 66AK2Gx processor architecture and a breakdown of the design into sub-elements to support customer safety analysis. It includes a description of functionality, operating states and any features supporting error management. The SAM also includes details of diagnostic measures supported to detect faults in each design sub-element.

The FMEDA is constructed in accordance with the requirements specified by the ASIL ISO 26262 and SIL 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 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 vs. 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 control over the relative safety mechanism coverage. Package pin-level tailoring allows for control over which pins need to be considered in the analysis and diagnostic coverage control for each pin.

Finally, TI provides a **detailed quality and reliability section** on the TI website which discusses quality and reliability for all TI devices including the 66AK2Gx processor. 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.

In summary, the 66AK2Gx processor is designed for high-reliability applications providing low transient failure rates and estimated active lifetimes of more than 10 years. And while the 66AK2Gx processor is not safety certified, TI offers the tools and guidance to assist customers interested in achieving specific SIL or ASIL certifications for their products at the system level. With an ARM® Cortex®-A15 and C66x DSP cores, the 66AK2Gx processor offers significant performance that is also reliable and consistent. Whether the application is an automotive audio amplifier or a PLC managing numerous critical operations in networked 21st century factory, the 66AK2Gx processor is a reliable choice for the application.

For a broad overview of the 66AK2Gx processor read "**Getting personal with 66AK2Gx DSP**."

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

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