Enhancing Robust SEU Mitigation with 28-nm FPGAs

WP-01135-1.0 White Paper

Systems designed with FPGAs benefit from significant improvements over ASICS, such as rapid-process technology scaling and design innovation, which permit the use of FPGAs in high-availability, high-reliability, and safety-critical systems. However, along with technology scaling come other effects such as increased susceptibility to soft errors that previously could be ignored. These soft errors, caused by single event upsets (SEUs), are nondestructive and can be corrected without system downtime. This white paper explains how the SEU mitigation enhancements developed for Altera® Stratix V® FPGAs provide a strong roadmap to address soft-error system challenges.

Introduction

The benefits of FPGAs over ASICs become more and more compelling as rapid-process technology scaling and innovation provides ever-greater speed, density, and power improvements. However, along with this technology scaling come other effects that previously could be ignored. One of the accompanying effects of higher density is increased susceptibility to SEUs, which in turn causes soft errors. Although careful IC design and layout techniques have decreased the soft-error rate per bit at 65 nm and 40 nm, each process-technology generation offers twice the logic density, bringing with it a corresponding doubling in the number of configuration RAM (CRAM) bits.

A secondary effect of FPGAs becoming denser and more capable is that they now tend to sit at the heart of the system, often in the data path; this offers the designer an unprecedented level of system integration with Stratix series FPGAs. With this change, FPGAs are now a primary silicon choice for many systems, including those that fall into the high-availability category such as telecom, storage, and data-processing systems. These application areas demand high reliability, and consequently, modern high-end devices, such as Altera's 28-nm Stratix V FPGAs, must offer robust SEU mitigation including correction without any system downtime.

Single Event Upsets

SEUs are nondestructive events caused by ionizing radiation strikes in the junction of transistors in CMOS devices, which discharge the charge in storage elements such as configuration memory cells, user memory, and registers. Within terrestrial applications, the two ionizing radiation sources of concern are alpha particles emitted from package materials and high-energy neutrons caused by the interaction of cosmic rays with the earth's atmosphere. The most common effect observed in digital CMOS devices is the soft error, where the amount of charge caused by the SEU, when acting on the storage nodes of an SRAM cell, can cause the bit to flip its state. Soft errors, like their cause (ionizing radiation),

101 Innovation Drive
San Jose, CA 95134
www.altera.com

are random and happen according to a probability related to energy levels, flux, and cell susceptibility. An important consideration of soft errors is that they can always be recovered simply by rewriting a cell with the correct value. No power cycle is needed because no silicon latch-up or any form of hard failure has been observed in SEU testing in several generations of Altera FPGAs.

Altera understands the effects of SEUs very well and focuses on keeping the native soft-error rate of SRAM cells within FPGAs low, as well as providing solutions for the mitigation of soft errors when they occur, to help designers meet their system reliability goals. By characterizing and studying SEUs for every technology node and product family, Altera makes continuous enhancements in next-generation products. As a result, the native soft-error rate has improved or is at least flat over the last few technology generations. To help designers meet their system reliability goals, Altera also focuses on providing solutions for the mitigation of soft errors when they occur. With Stratix V FPGAs, system designers can first rapidly detect and correct SEU errors and later classify the errors.

Lowering the Upset Rate

The sensitivity of a SRAM cell can be expressed in failures in time (FIT) per Mb or as a neutron cross-sectional area. The most consistent metric for neutron sensitivity in the industry is the >10 MeV neutron cross-section area as measured at the Los Alamos Weapons Neutron Research (WNR) facility. This metric provides an apples-to-apples comparison between process technologies, and is not subject to scaling factors that can be used to offer seemingly better FIT numbers.

Through process techniques and careful CRAM cell physical design- and circuit-level techniques, Altera has reduced the per-bit upset rate with advanced process generations. In addition, potentially damaging effects such as latch-up have been eliminated in process technologies, meaning mitigation of soft errors is the only remaining concern. To understand the effects of soft errors, it is important to understand which building blocks within a FPGA are most likely to contribute to functional errors. Because registers, flip flops, and I/O registers are least likely to contribute errors, Altera's focus is on SEU mitigation for the CRAM cells and user RAM cells.

Logic, Routing, and Hard IP CRAM Cells

With over 250 Mb of CRAM size for the largest Stratix V FPGAs, logic, routing, and hard intellectual property (IP) CRAM cells represent the largest proportion of SRAM cells on chip. Since these SRAM cells directly control the functionality of the FPGA, their integrity is of prime importance. In reality, though, only a small percent of these bits typically affect a given design due to low routing utilization even in full designs.

On-Chip Memory RAM Cells

Stratix V FPGAs offer over 50 Mb of user memory, and consequently, unmitigated user memory can be a significant contributor to the soft-error rate in an FPGA. The M20K memory blocks in Stratix V FPGAs have hard error correction coding (ECC) built in with enhanced multibit detection and correction capability. Enhanced multibit correction, coupled with physical separation of bits in a word (commonly referred to as interleaving) provides robust mitigation for multibit upsets in user memory.

Registers and Flip Flops in the Device Core

Registers and flip flops are present within the Stratix V adaptive logic modules (ALMs), digital signal processing (DSP) blocks, pipelining, and memory ports. Since these cells have a smaller neutron cross section (in other words, a higher critical charge) than typical SRAM cells, their contribution to the FIT rate is very low and statistically insignificant in a SRAM-based FPGA.

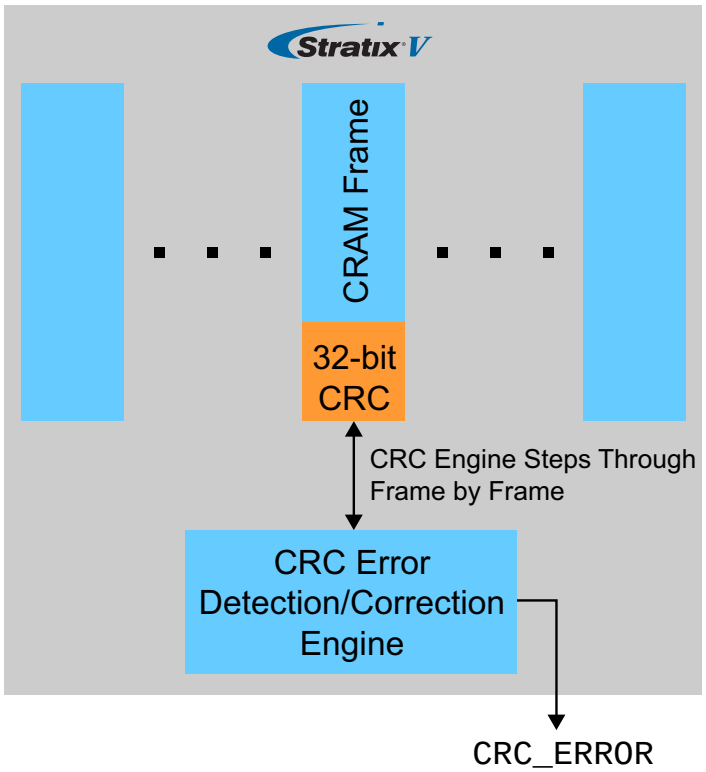
I/O Registers

I/O registers are built in the periphery of the chip, which operates at a higher voltage. These registers are designed to be very robust from a SEU mitigation point of view. Also, because the number of I/O registers is comparatively low, they consequently make no contribution to the FIT rate. No upset has ever been observed within the registers during SEU testing.

Configuration RAM Soft-Error Mitigation

Since the 130-nm process generation, Altera has included background error detection circuitry in all FPGAs using a cyclic redundancy check (CRC) hard engine to enable continual verification of the CRAM contents during device operation. The 32-bit CRC circuit (Figure 1) in Stratix V FPGAs is enhanced to provide nine 9s (99.9999999767 %) of error detection. The CRC circuit is also guaranteed to correct single-bit and double-adjacent multibit upsets. The benefit of integrating this circuitry on-chip in hard gates is that the circuitry is robust and not susceptible to soft errors. In addition, the CRC engine is a self-contained block and is enabled simply by checking the compilation options box in Altera's Quartus® II development software.

Figure 1. Stratix V Integrated Configuration CRC



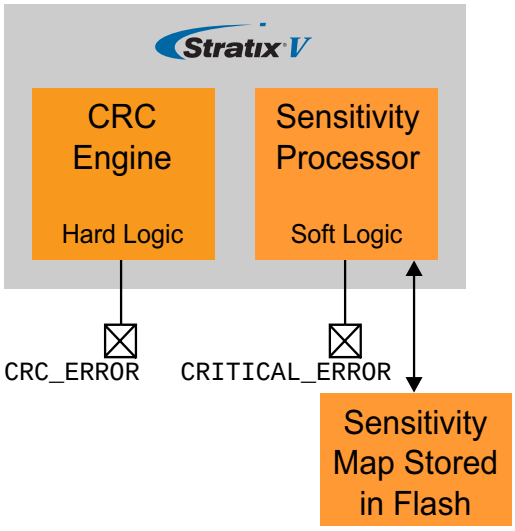
Whereas previous generations used a single 16-bit CRC value per frame, Stratix V FPGAs use an enhanced 32-bit CRC polynomial that has close to 100% error-detection capability. This, combined with a faster clock, translates to a lower error detection time compared to previous generation and competing solutions. In addition, simultaneous soft errors in separate frames can be detected and located due to the isolation of the frames and their corresponding CRC registers. Table 1 summarizes the CRC enhancements through several generations of Stratix series FPGAs.

Table 1. CRC Enhancements in Stratix Series FPGAs

Stratix Series FPGA Family	CRAM CRC of Entire CRAM	CRAM CRC of CRAM Frame	CRAM Error Location	Injection of CRAM SEU Errors for Testing	Error Classification	CRAM Error Correction	On-Chip Memory Error Checking
Stratix, Stratix GX	Yes						
Stratix II, Stratix II GX	Yes						
Stratix III		Yes	Yes	Yes	Yes		Yes
Stratix IV E, Stratix IV GX, Stratix IV GT		Yes	Yes	Yes	Yes		Yes
Stratix V E, Stratix V GX, Stratix V GT		Enhanced	Yes	Enhanced	Yes	Yes	Enhanced

With the soft-error location capability, the ability to determine the sensitivity of an error is further enhanced through software tools. Because only a small percent of configuration errors typically affect the FPGA functionality, being able to ignore "don't care" configuration soft errors brings a decrease in the actual FIT rate because the decision to continue operating the FPGA can be made without experiencing a functional interrupt. The critical error detection capability, shown in Figure 2, is implemented in soft logic using a megafunction integrated in Quartus II software.

Figure 2. Critical-Configuration Soft-Error Detection Within Stratix V FPGAs



The operation of the critical error detection solution takes the following steps:

1. Detect and locate the configuration soft error using the built-in soft-error detection circuitry. This asserts the `CRC_ERROR` pin.
2. The soft logic takes the error information and uses it to calculate an address within a file containing a map indicating which of the configuration bits are "care" or "don't care."
3. Using a user-specified memory interface, such as the active serial configuration port, the soft logic accesses the appropriate bit in a sensitivity map file to determine if the particular configuration soft error is critical to the design currently configured in the FPGA.
4. If the configuration soft error is a "don't care," then the FPGA can continue operating without a functional error. If the configuration soft error is a "care" and may be affecting functionality, then the `CRITICAL_ERROR` pin is asserted and the appropriate action can be taken within the system, such as reconfiguring the FPGA. The sensitivity map file, which contains the map of "care" and "don't care" bits, is automatically generated by the Quartus II software for a particular design according to resource usage and the utilized routing. This means partially full designs also benefit from a further FIT-rate decrease because configuration soft errors within unused resources will not cause a critical error.

Because the sensitivity processor for determining the "care" or "don't care" nature of the pin is implemented in soft logic, triple-mode redundancy techniques can be employed in both the interface signals and control logic. These techniques retain reliable operation in case the configuration soft error affects that particular part of the FPGA. High-reliability systems require this type of advanced mitigation but, importantly, also require the ability to test the system through the injection of configuration soft errors. This removes the need to take a system to a suitable ionizing radiation source to test system behavior when reacting to a soft error.

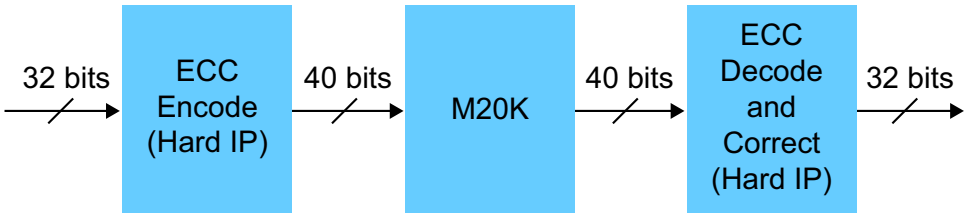
Stratix V FPGAs enhance the error injection capability by allowing the user to inject multiple single-bit errors as well as multibit errors. This capability is typically required when hardware has already been developed. Consequently, Stratix V FPGAs offer this capability via the JTAG port, allowing running systems to be tested easily and mitigation strategies verified.

User RAM Soft-Error Mitigation

In addition to configuration memory checking, Stratix V devices offer the ability to check the integrity of on-chip memory. Stratix V FPGAs offer two sizes of user memory, each of which has the option of using a ninth memory bit per byte as a parity bit to enable error detection and correction. With this extra storage, along with automatically generated ECC circuits, both the 640-bit MLAB and the 20-Kb M20K blocks provide SEU mitigation.

As shown in Figure 3, the M20K block has a hard ECC circuit with double error correct/triple error detect (DECTED) code. Furthermore, the memory blocks are carefully laid out so that the logical bits in a single data word are physically separated. This technique, known as "interleaving," is a standard best practice in memory design. Enhanced multibit detection and correction capability combined with interleaving provides maximum SEU mitigation for multibit upsets.

Figure 3. Stratix V Automatic ECC for M20K User Memory



Configuration of the ECC is made simple by Altera's MegaWizard® Plug-In Manager, which provides this functionality without extra design effort. Soft-error mitigation within user memories of Stratix V FPGAs can be tested using the system-memory content editor capability of Altera's SignalTap™ logic analyzer, which allows modification of the memory contents from Quartus II software via a JTAG connection.

In a case where external memory is interfaced to Stratix V FPGAs, Altera's memory interface IP also includes support for ECC. The controller features error logging and interrupt management to allow the system to monitor soft errors in external memories.

Methods of Mitigation

Having a low soft-error rate with robust and powerful mitigation features is essential to those users designing for high-end FPGAs within high-availability, high-reliability, and safety-critical systems. For the reliability engineer, mitigation features represent tools to meet the system reliability goals. There is a wide range of mitigation strategies possible depending on the requirements and the environment in which the system is operated.

Often the first step is to establish a target, such as MTBF, downtime, or desired failure mode. In many cases, it can be proved that the target reliability can be achieved with minimal effort. For example, considering a mid-density Stratix V FPGA with the integrated CRC engine enabled and "reconfigure on error" mitigation strategy, fractional downtimes of 10^{-11} are easily achievable and are several orders of magnitude better than the five 9's 99.999% availability required from telecommunication infrastructure equipment. However, the whole system should be taken into account, especially if there is a large bill of materials or the FPGA contains significant amounts of complex IP.

Certification of the processor and operating system, as well as software coding practices, heavily influence the reliability figures in a real system, as most system designers will already be aware. In the case of soft errors within digital ICs, any component containing volatile memory also needs to be included in the analysis. For example, if a large DDR1/2/3 SDRAM is included, then this will become the largest contributor to the system's soft-error rate, and techniques such as ECC within the memory controller should be considered. System partitioning can also make a significant difference to reliability, such as how much of the system is critical to core operation or, in the case of system redundancy, the granularity at which redundancy is implemented (generally the larger the granularity, the better).

Multiple approaches exist for dealing with soft errors, including ensuring the downtime following a soft error is less than a critical parameter, such as mean time to repair. Other examples of system soft-error mitigation behaviors range from executing a system-context save, reset, and restore, to simply flagging the soft error in a log and resetting the system at the earliest convenient time. Following a soft error in a critical-

configuration SRAM bit, the system functionality may be erroneous for a period of time before being corrected in an open-loop fashion. The danger in this case is that incorrect data has already been processed by the FPGA and will have propagated outwards into the rest of the system. While the same issue exists with any FPGA error detection technique, it is almost always best to recognize at a system level that a soft error has occurred so the incorrect data can be labeled as such.

Mitigation Options

When designing FPGAs, Altera's focus on a combination of low per-bit soft-error rate of the CRAM cells and mitigation techniques, such as critical error detection, provides a large improvement in reliability. When it comes to on-chip RAM soft-error mitigation, the well-understood and well-utilized ECC technique offers very good protection with only minimal cost in terms of silicon area and performance. Using ECC means that the memory is checked and corrected automatically at system speeds.

For designers who need the ultimate in terms of soft-error mitigation, ASICs offer the best solution. Altera's HardCopy® ASICs offer seamless migration from the prototype FPGA to a pin-compatible ASIC without heavy investment in design tools, chip design, or board redesign. No other ASIC offers the ability to delay the tape-out decision until the complete system, including PCB, is proven by the FPGA prototype. Because HardCopy ASICs contain no SRAM configuration cells, the logical functionality is immune to soft errors as the metal programming is not susceptible to SEUs. The only susceptible parts of the chip are the user memories, which are correctable using ECC, and the core registers, which have an extremely low upset rate. For example, in HardCopy ASICs, the logic registers are built from HCells.

During testing at Los Alamos WNR, it was found that in lower densities no upset was observed for logic registers. Using statistical analysis, the FIT rate is estimated to be <100 FIT per million registers with a 95% confidence level. A number of technical innovations, such as increased feedback-loop gate strength, an isolated master and slave stage, and improved node capacitance through via programming, are responsible for these FIT rates that are orders of magnitude lower than any commercially available FPGA. HardCopy V ASICs, prototyped using Stratix V FPGAs, use similar techniques offering the highest soft-error immunity of any ASIC.

Summary

Stratix V FPGAs offer a strong roadmap to address SEU system challenges through mitigation features from simple configuration soft-error detection to the capability of determining the difference between a functional or "don't care" configuration soft error. Stratix V FPGAs offer several SEU mitigation features, including built-in devices and tools that enable:

- Fast error detection built into the silicon
- Immediate error correction built into the silicon
- Improved error classification enabled by improved tools
- Fault injection enabled by silicon and tools
- ECC on user RAM built into the silicon

Combined with automated on-chip and external memory soft-error correction, systems designed using Stratix V FPGAs benefit from significant reliability improvements permitting the use of FPGAs in high-availability, high-reliability, and safety-critical systems.

Further Information

- Stratix V FPGAs: Built for Bandwidth: www.altera.com/products/devices/stratix-fpgas/stratix-v/stxv-index.jsp
- Literature: Stratix V Devices: www.altera.com/literature/lit-stratix-v.jsp
- Single Event Upsets: www.altera.com/support/devices/reliability/seu/seu-index.html
- Application note: *Error Detection & Recovery Using CRC in Altera FPGA Devices*: www.altera.com/literature/an/an357.pdf
- For Altera FPGA SEU test reports, please contact your sales representative: www.altera.com/corporate/contact/con-index.html

Acknowledgements

- Manoj Roge, System Architect, Product Planning Group, Altera Corporation

Document Revision History

Table 2 shows the revision history for this document.

Table 2. Document Revision History

Date	Version	Changes
July 2010	1.0	Initial release.