Robust SEU Mitigation With Stratix III FPGAs

Introduction

The benefits of FPGAs over ASICs become ever more compelling as rapid-process technology scaling and innovation provide ever-greater speed, density, and power improvements. However, along with technology scaling come other effects that previously could be ignored. One of the accompanying effects is increased susceptibility to soft errors caused by single event upsets (SEUs). Although through careful IC design the soft error rate per bit decreases at 65 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 integration of a system into a programmable chip. With this change, FPGAs are now a primary silicon choice for many systems, including those that fall into the high-availability category such as telecoms, storage, and data-processing systems. These application areas demand high reliability, and consequently modern high-end FPGAs, such as Altera's 65 nm-based Stratix® III, must offer robust SEU mitigation. This is especially the case where the operating environment has a high neutron flux, such as within avionics systems.

SEU Background

SEUs are nondestructive events caused by ionizing radiation strikes in the junction of transistors in CMOS devices. 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), 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 since there is no silicon latch-up.

Altera understands these effects 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.

Keeping the Upset Rate Low

The sensitivity of a SRAM cell can be expressed in failures in time (FIT) per Mbit or as a neutron cross-sectional area. The most consistent metric for neutron sensitivity in the industry is the >10MeV 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 careful process technology selection and SRAM cell physical design- and circuit-level techniques, Altera has reduced the per-bit upset rate with decreasing process geometries. In addition, potentially damaging effects such as latch-up have been eliminated in process technologies up to and including 65 nm, meaning mitigation of soft errors is the only remaining concern.

To understand the effects of soft errors, it is important to understand the building blocks within a FPGA. These, in order of descending contribution to functional errors, are as follows.

Logic, routing, and hard IP CRAM cells: With counts as high as 120 Mbits for the largest Stratix III devices, 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 10 percent of these bits typically affect a given design due to low routing utilization in even full designs.

On-chip memory RAM cells: Stratix III FPGAs offer over 17 Mbits of user memory, and consequently, unmitigated user memory can be a significant contributor to the soft error rate in an FPGA.

Registers and flip flops in the device core: These are present within the Stratix III adaptive logic modules (ALMs), digital signal processing (DSP) blocks, pipelining, and memory ports. Since these cells have a smaller neutron cross section than typical SRAM cells and have a relatively low count (less than 1 Mbit even on the largest Stratix III devices), their contribution to the FIT rate is very low and statistically insignificant in a SRAM-based FPGA.

I/O registers: These registers are built in the periphery of the chip, which operates at a higher voltage. Since the number of I/O registers is very low (<10,000 on the largest Stratix III device), they consequently make no contribution to the FIT rate. No upset has ever been seen within the registers during testing by Altera.

Consequently, Altera's focus is on SEU mitigation for the CRAM cells and user RAM cells.

Stratix III Configuration RAM Soft Error Mitigation

Since the 130-nm process generation, Altera has included background error detection circuitry in all FPGAs using a cyclical redundancy check (CRC) engine to enable continual verification of the CRAM contents during device operation. The CRC is guaranteed to detect up to a maximum of three bit errors. 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 a box in the Quartus® II compilation options. Stratix III FPGAs include an enhanced CRC capability, which extends the functionality compared with previous generations, as shown in Figure 1.

*Figure 1. Stratix III Integrated Configuration CRC*
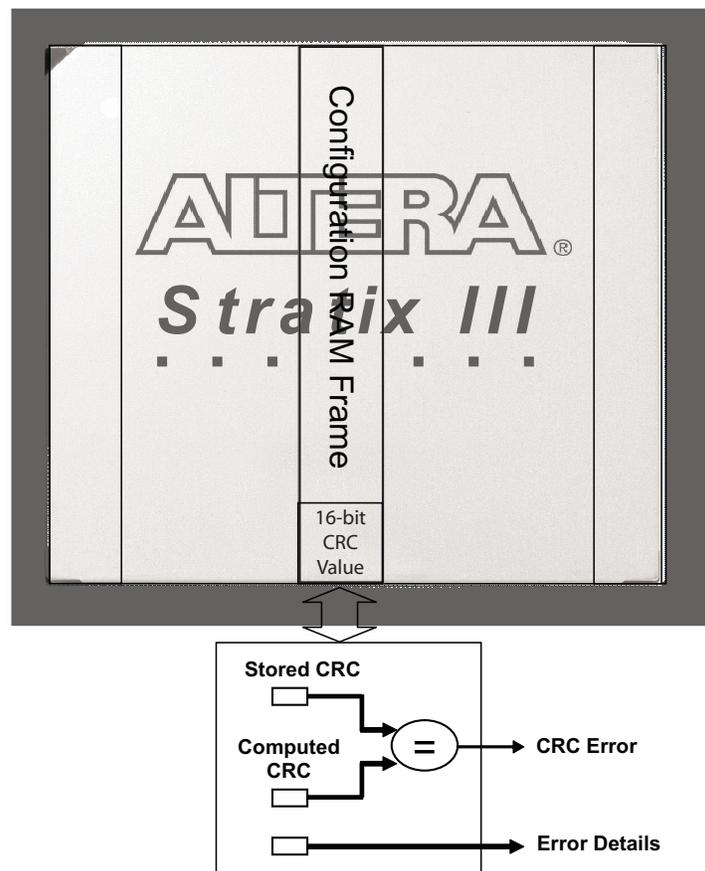
Whereas previous generations used a single 32-bit CRC value for the entire device, Stratix III FPGAs employ a 16-bit CRC value per frame, which brings multiple benefits. First, the error detection circuitry doesn't need to wait until a CRC has been calculated for the entire device before a soft error is detected. This translates to a lower soft error detection time. The second benefit is that a greater number of CRC bits on-chip means that enough information is contained to locate the soft error, be it a single soft error or a double-bit soft error in adjacent bits. A further benefit is that simultaneous soft errors in separate frames can be detected and located due to the isolation of the frames and their corresponding CRC registers.

With the soft error location capability of Stratix III FPGAs, the capability to determine the sensitivity of an error is enabled. Since only 10 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 since the decision to continue operating the FPGA can be made without experiencing a functional interrupt.

The critical error detection capability is implemented in soft logic using a reference design that will be supported from Quartus II software version 7.2 onward. Figure 2 shows how this critical bit detection system works.

Figure 2. Critical Configuration Soft Error Detection Within Stratix III FPGAs
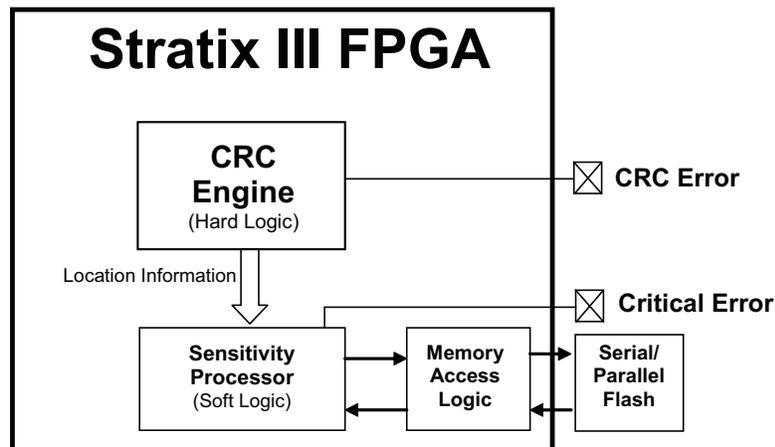
The operation of the critical error detection solution is as follows:

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 then takes the error information and uses it to calculate an address within a file containing a map indicating which 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 then accesses the appropriate bit in a sensitivity map file to determine if the particular configuration soft error is critical to the design currently configured into 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 file containing the map of "care"/"don't care" bits is automatically generated by the Quartus II design 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.

Since the sensitivity processor reference design for determining the "care" or "don't care" nature of the pin is implemented in soft logic, triple-mode redundancy techniques are employed in both the interface signals and control logic to 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 III FPGAs enhance the error injection capability of Stratix II FPGAs by allowing the user to inject multiple single bit errors as well as multiple double adjacent bit errors. This capability is typically required when hardware has already been developed. Consequently, Stratix III FPGAs offer this capability via the JTAG port, allowing running systems to easily be tested and mitigation strategies verified.

Stratix III User RAM Soft Error Mitigation

In addition to configuration memory checking, Stratix III devices offer the ability to check the integrity of on-chip memory. Stratix III FPGAs offer three sizes of user memory, each of which includes a ninth memory bit per byte. With this extra storage, along with automatically generated error correction coding (ECC) circuits, both the 640-bit MLAB and the 9-Kbit M9K blocks provide SEU mitigation. The 144-Kbit M144K blocks also offer this functionality, except that the ECC circuit is included in hard gates within the memory block (see Figure 3 for details).

Figure 3. Stratix III Automatic ECC for M144K User Memory
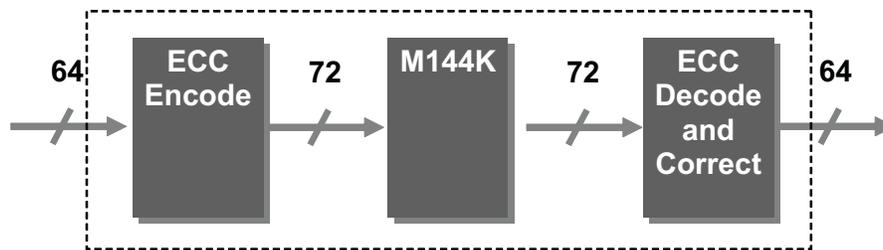
Using ECC, each of the three on-chip memory block types can detect up to two bit errors and correct single bit errors automatically in real time. Configuration of the ECC is made simple by the MegaWizard® Plug-In Manager, which means this functionality is provided without extra design effort.

One limitation of ECC arises in the case of two bit errors within a word, where the error can only be detected but not corrected. While this is better than not detecting the error, it means upper layers in the system need to manage the error using alternate methods, such as requesting the data affected to be resent. To lessen this effect, the logical bits within words in the larger memories in Stratix III FPGAs have been physically separated, reducing the probability of seeing logical multibit errors within a word, and thus enabling ECC to be effective even in the case of a multiple bit upset (MBU). Soft error mitigation within user memories of Altera® FPGAs can be tested using the system memory content editor capability of the SignalTap® logic analyzer. This allows modification of the memory contents from Quartus II software via a JTAG connection.

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

Mitigation Discussion

Having a low soft error rate with robust and powerful mitigation features is essential to those 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 midrange Altera FPGA with the integrated CRC engine enabled and "reconfigure on error" mitigation strategy, fractional downtimes of 10^{-11} are easily achievable; six orders of magnitude better than the 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 DDR SDRAM is included, then this will become the largest contributor to the system 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 to dealing with soft errors, including ensuring the downtime following a soft error is less than a critical parameter, such as the closed loop time constant of a control system. 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. Some techniques can even be dangerous, like the continuous background refreshing of the configuration data, also known as scrubbing. 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 labelled as such.

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 at little extra cost. Stratix III FPGAs offer a range of features that can be considered a collection of tools to help meet these goals. A summary of these is shown below in Table 1.

Table 1. Stratix III Configuration Soft Error Mitigation Options

Tool	CRC Only	Critical Error Detection
Detection Method	"CRC_ERROR" status pin	+ "Critical_ERROR" status pin
Bit Flip Knowledge	Somewhere in FPGA	Exact bit location
Mean Time Between Errors (MTTE)	1 (baseline)	1 / utilization factor
Bit Flip Correction	Reconfigure FPGA	Reconfigure FPGA only if flipped bit is critical
Design Cost	Monitor one pin	Monitor two pins Small amount of user logic + sensitivity map storage (reference design provided)
System Test Options	Error injection	Error injection Single or multiple errors

When it comes to on-chip RAM soft error mitigation, the well understood and utilized technique of ECC offers very good protection with only minimal cost in terms of silicon area and performance. The total width of memory needed (data bits and check bits) becomes more efficient for wider word widths, and 64-bit data with 8 check bits (72 bits total) is a widely accepted trade off. This ratio is demonstrated in server and cache applications and is the configuration supported by the M144K memory blocks in Stratix III FPGAs. Using ECC means that memory is checked and corrected automatically at system speeds.

For designers who need the ultimate in terms of soft error mitigation, ASICs, of course, offer the best solution. Altera's HardCopy® structured ASIC family offers seamless migration from the prototype FPGA to a pin-compatible

structured ASIC without heavy investment in design tools, chip design, or board redesign. No other structured ASIC offers the ability to delay the tape-out decision until the complete system, including PCB, is proven by the FPGA prototype. As structured ASICs, HardCopy devices contain no SRAM configuration cells. Consequently the logical functionality of the device is immune to soft errors as the metal programming is not susceptible to SEUs. The only parts of the chip that are susceptible are the user memories, which are correctable using ECC, and the core registers.

The core registers have an extremely low upset rate. For example, in HardCopy II structured ASICs, the logic registers are built from HCells. During testing at Los Alamos WNR, it was found that it was impossible to upset the registers at all. 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 this. The 65-nm HardCopy III structured ASICs, prototyped using Stratix III FPGAs, will use similar techniques offering the highest soft error immunity of any structured ASIC.

Summary

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

Further Information

- *Section IV: Design Security & Single Event Upset (SEU) Mitigation*, of the *Stratix III Device Handbook*:
  www.altera.com/literature/hb/stx3/stx3_siii5v1_04.pdf
- *AN 357: 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