Single-Event Upsets (SEUs) and Medical Devices

December 2010

Abstract

As process nodes for integrated circuits (ICs) continue to shrink, their susceptibility to single-event upsets (SEUs) due to high-energy particles rises. Specifically, it is the static RAM structures within these devices that pose the greatest concern. The awareness of these risks has long been known in the space community, and that knowledge has spread to other industries, such as networking, avionics, automotive, and now medical. Medical devices are not only susceptible to nature's cosmic rays, but also must operate in radiation environments found in modern medical facilities. As evidence of these effects mounts, designers of medical devices must now also consider SEU susceptibility when choosing the technology that will form the basis for their products. This paper defines what the risks are and explains ways to mitigate and avoid these risks within programmable logic.

Introduction

CMOS memory structures such as static RAM cells and flip-flops are susceptible to upset (change of state) when bombarded with high-energy particles. These particles can be alpha particles, neutrons, protons or a wide-range of heavy ions, resulting from the collision of cosmic rays with particles in the upper atmosphere or secondary collisions with particles liberated by cosmic rays.

The cosmic ray shower is composed primarily of neutrons. Protons are the second significant component, being 7 to 32% of the neutron flux at the Earth's surface.

Additional sources for these particles are both the packaging and the silicon substrate itself. Packaging materials used for integrated circuits contain trace amounts of uranium and thorium. Both of these elements emit energetic alpha particles. Moreover, the element boron is used in polysilicon doping, substrate doping, or boro-phospho-silicate glass (BPSG) in large amounts. When one of the commonly occurring boron isotopes (^{10}B) is struck (referred to as neutron capture) by low-energy (thermal) neutrons, both a lithium ion and an alpha particle are created. This spectrum can be significant given both the amount of boron present in substrates plus the number of low-energy neutrons present in the cosmic shower. Because both of these sources are in the device itself, no amount of outside shielding can protect against these particles.

When these charged particles strike the silicon substrate of an IC, they leave an ionization trail. Similarly, when a high-energy particle, for example a neutron, strikes the substrate, they collide with atoms in the substrate, liberating a shower of charged particles which then leave an ionization trail. This ionization can result in a charge sufficient enough to overpower the gate and cause a change in state (bit flip) of the memory element. This change in state is referred to as a single-event upset (SEU), shown in Figure 1 on page 3.

These upsets are temporary in nature and are cleared the next time the memory structure is written to or reset (for example, by cycling the power). No long-term damage to the circuit resulting from SEUs has been demonstrated.

The susceptibility of memory circuits to SEUs is increasing with each new generation of devices. As process geometries decrease, the following also occurs:

- Supply voltages also decrease, lowering the threshold for SEUs.
- Gate area shrinks and causes capacitance to decrease, lowering the critical charge required to cause an upset to decrease.
- Cell area shrinks, reducing the cross section and, therefore, lowering chances of a particle impact.

As a consequence, memory element sensitivity to SEUs is increasing. What was once only a concern in space applications is now a design concern even at ground level for any high-reliability design such as medical equipment.

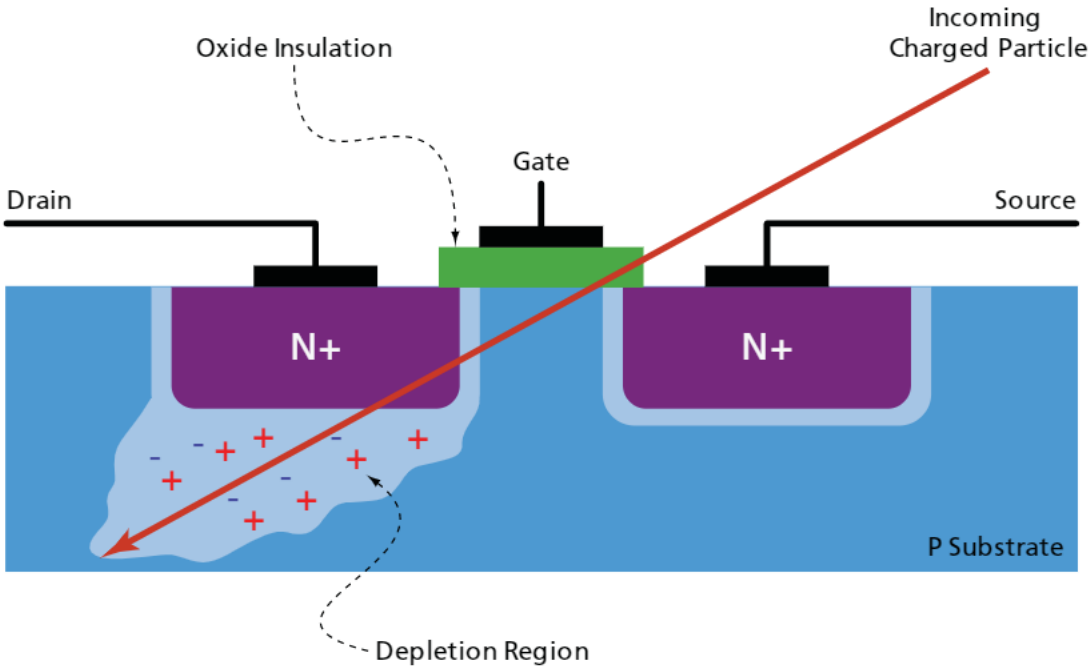


Figure 1: **Charged Particle Causing an SEU**

FPGA Technology and Susceptibility to SEU

All FPGAs share many common traits. All have an array of logic modules (referred to as the fabric of the FPGA), embedded memory blocks, possibly some specialized blocks such as multipliers or DSP, clock management circuits such as PLLs and all surrounded by a ring of programmable I/Os. One key area of differentiation between various families of FPGAs is their fabric. Families from different suppliers often differ in the exact structure of the logic modules and how these modules are interconnected or wired together. It is this interconnect that can pose a concern from an SEU perspective.

There are two aspects to FPGA routing: the wire (or metal trace) and the interconnecting via. The vias used in FPGAs are programmable—the basis of the entire technology. These programmable vias are also used to set the configuration of each logic module as well as the entire device. There are three via technologies used by FPGA industry: antifuse, flash and SRAM.

Antifuse

The antifuse via (programmable link) is a metal-to-metal programmable interconnect element that resides between the upper two layers of metal. Antifuses are normally open and when programmed form a permanent, passive, low-impedance connection. Because programming an antifuse requires multiple high-voltage pulses, they cannot be programmed (or unprogrammed) by high-energy particle impact.

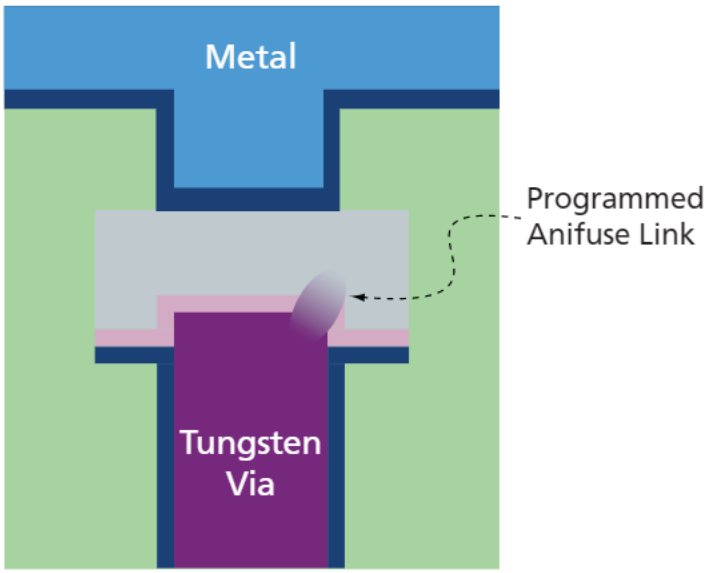


Figure 2: **Antifuse**

The major features of antifuse are as follows:

- Once programmed, it cannot be reprogrammed.
- Relatively high energies are required to program an antifuse.
- Programming is performed externally as a part of the OEM's manufacturing process.
- It is a static structure (persists after power is removed) involving no transistors.
- Is SEU immune.

Flash

The interconnect element used in flash-based FPGAs is a flash switch. As with all flash memory, the programmed state of the flash switch is nonvolatile. Programming/erasing a flash switch requires voltages and energy far in excess of that which can be generated by cosmic-ray-induced particles.

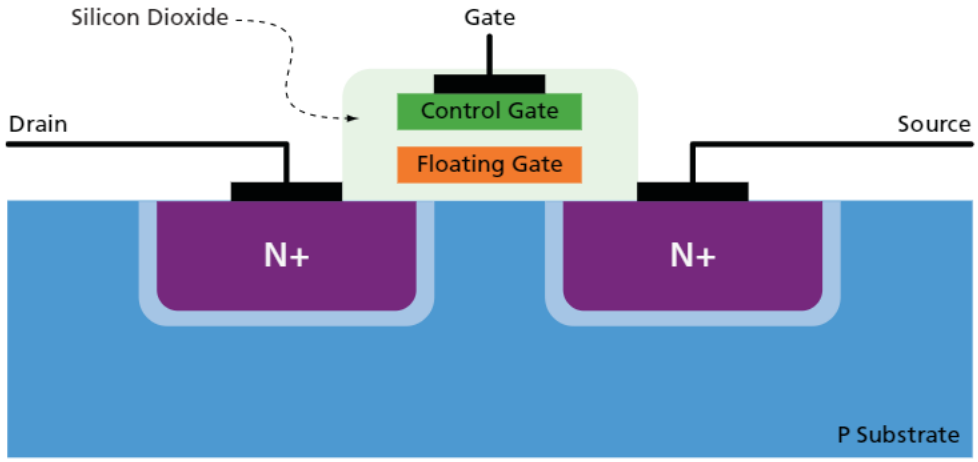


Figure 3: **Flash Switch**

The major features of flash are as follows:

- Reprogrammable
- Relatively high energies are required to program the interconnecting flash switches.
- It is a static structure (persists after power is removed).
- Is SEU immune.

SRAM

The basic programmable via in an SRAM-based FPGA is a single bit SRAM cell. The SRAM via is programmed and erased the same way as any other SRAM memory cell. Although more robust than block SRAM, the SRAM via can be easily programmed/erased by the charges created during the impact of cosmic-ray-induced radiation.

The major features of the SRAM via are as follows:

- Reprogrammable
- Relatively low energies are required to program the via.
- Programming is basically a memory write to the configuration vias.
- It is a volatile structure (is erased when power is removed) composed of multiple transistors.
- Is susceptible to SEUs.

SEUs — a Growing Concern for Medical Devices

As with other industries, there is a slow, but growing recognition of SEUs and their impact on medical equipment. For example, in 1998 Bradley and Normand reported on the incidence of SEUs in implantable cardiac defibrillators. This report presented the first clinical data set obtained indicating the effects of cosmic radiation on implantable devices.

Underscoring the Bradley ad Normand findings, in 2005, Canadian-based St. Jude Medical issued an advisory to doctors, warning that SEUs to the memory of its implantable cardiac defibrillators could cause excessive drain on the unit's battery.

While Bradley and Normand were investigating errors induced at ground level, modern medical equipment, such as portable infusion pumps, aircraft-based defibrillators, pacemakers, and implantable cardiac defibrillators, must also operate when flying in commercial aircraft (with the high neutron flux at altitude).

The error rate for a given circuit is generally proportional to the relative neutron flux of the operating environment. The neutron flux for aircraft operating at altitudes near 40,000 feet on near polar flight paths is roughly 600 times that at ground level at New York City (the reference point defined by JESD98A) — representing a significant increase in the risk of SEUs for devices operating on aircraft. As a result, the FIT rate for any device operating at this altitude near the poles is nearly 600 times greater than when operating at sea-level at lower latitudes.

However, cosmic rays and device materials are not the only sources of ionization radiation in the medical environment. With rise of new technologies such as radiation therapy, where ionizing radiation is used to target cancers, designers must also consider this locally generated flux. In fact, Guo, et al. investigated the flux generated by a Varian linear accelerator (LINAC) operating in high-energy mode, estimating that a typical radiation therapy room could experience 38 SEUs/MB/day. Given the memory content of modern electronics, the estimated error rate is indeed significant.

Mitigation versus Immunity

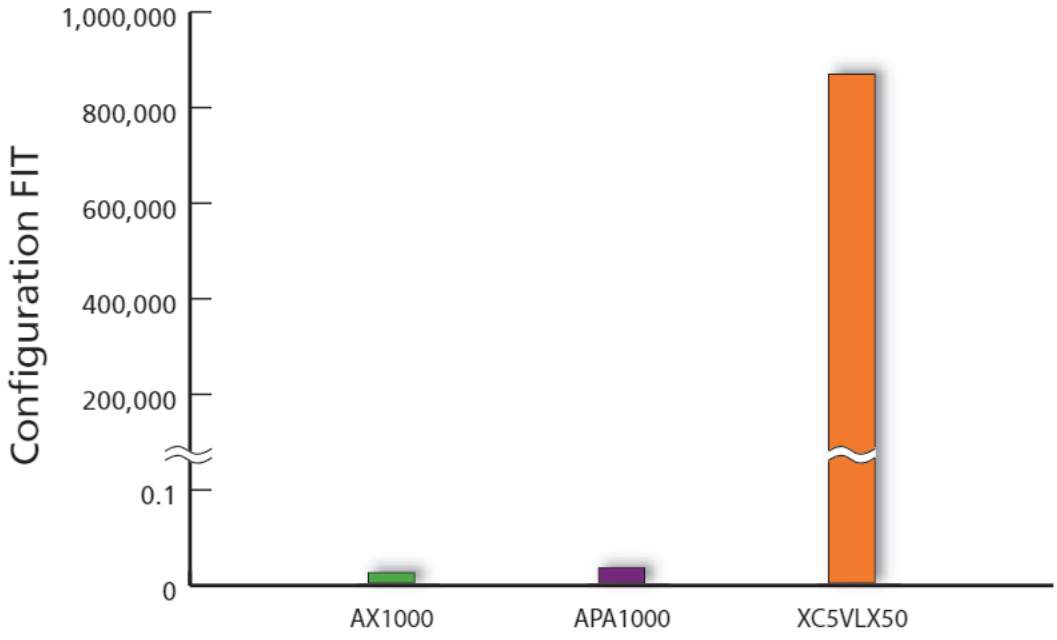
All FPGAs, whether SRAM, flash, or antifuse based, contain SRAM blocks and flip-flops which are susceptible to SEUs. Flip-flops are the most robust of memory structures are only upset in high-radiation environments (for example, space). Mitigating errors in flip-flops is well understood and straightforward; for example, mitigation can be done by using triple-module redundancy (TMR). Upsets to SRAM blocks can also be mitigated by the standard techniques used to detect and correct other errors, such as error detection and correction (EDAC) circuitry. Again, upsets to these structures are classed as soft errors, and when mitigated do *not* propagate to the rest of the system.

SRAM-based FPGAs have an additional area of concern regarding SEUs—the configuration memory of the device is essentially a large SRAM. As a result, an SEU to the configuration memory can result in a change in the functionality of the device in one of two ways:

- Altering the routing (connecting/shorting paths there were not connected before or breaking connections in the design)
- Changing the configuration and thus the function of logic cells and I/O structures (for example, changing an input to an output)

These errors are referred to as firm errors (in contrast to soft errors) as they impact the functionality of the device and cannot be corrected in real-time. Given the sheer number of configuration bits in an SRAM-based FPGA, the potential for SEUs represents a great impact on system reliability.

For example, Xilinx's own estimate for the configuration memory SEU rate for even a small Virtex®-5 device (XC5VLX50) operating in the neutron flux present at 40,000 feet is 570,125 to 809,971 FIT, translating to a mean time between failures (MTBF) of 1.23 to 2.61 months. Given that many systems can contain multiple FPGAs, the likelihood of a firm error occurring during a treatment session is significant.



Note: Chart represents predicted FIT rates at worst-case neutron flux at 40,000 feet based on terrestrial test data. No errors were observed for AX1000 and APA1000. The given FIT values for those devices represent the statistical upper bound for the given sample size.

Figure 4: **Predicted Configuration Upset Rates for Antifuse, Flash, and SRAM-based FPGAs**

Mitigating SEUs in SRAM-Based FPGAs

Because of the growing awareness of SEUs, manufacturers of SRAM-based FPGAs recommend various mitigation techniques. These techniques range from brute force to the more complex.

The simplest method is to simply reconfigure the FPGA at regular intervals, clearing any errors that have accumulated. For this method to be successful, the designer must determine the impact of potential errors, plus the length of time it takes for these errors to propagate. The idea is to reconfigure the FPGA inside this time. The errors still propagate, but the potential damage is limited by the reconfiguration. In addition, the function hosted in the FPGA is unavailable until the reconfiguration is completed.

With more recent generations of SRAM-based devices, the user can employ the built-in error detection scheme in the configuration engine. Using a configuration memory readback feature, the cyclic redundancy check (CRC) for each configuration frame is calculated and compared to a golden CRC. If a mismatch is detected, then an SEU has occurred, and the application can reconfigure the FPGA. Alternately, the application can attempt to correct the error and rewrite the frame in background. Again, the errors still propagate, but the time before they are corrected is greatly reduced.

Mitigation Does not Equal Immunity

Regardless of the methodology, mitigation is used to correct errors ***after*** the fact; in other words, mitigation attempts to lessen the impact of errors. In all cases, the correction schemes are only able to handle single-bit errors within a configuration memory frame. Any multi-bit errors require device reconfiguration. In addition, mitigation schemes require additional reliability analysis and engineering time to implement.

Mitigation should not be confused with immunity. With mitigation, the errors still occur, and can propagate in the system. The hope is that any errors can be detected and corrected before they have a noticeable impact.

Aside from the reliability concerns arising out of potential SEUs in a medical device (even with mitigation), potential errors raise a liability concern. If a manufacturer uses devices known to be susceptible to SEUs, then negligence could be argued. An example would be a LINAC suddenly malfunctioning and causing an overdose during a treatment. If the controlling circuitry were contained in an FPGA, it could be argued that an SEU caused the malfunction and the manufacturer was negligent in using a technology susceptible to such errors.

Using FPGAs immune to SEUs not only simplifies system design, but can also shield manufacturers from any potential legal implications.

In contrast, flash- and antifuse-based FPGAs are immune to configuration upsets (SEUs impacting the configuration), as demonstrated by Olmos of iRoC Technologies. As a consequence, the designer does not have to analyze the potential impact of these errors to the system, nor design and test mitigation protocols.

Conclusion

SEUs have long been a concern in space applications, but awareness of the issue has grown in the medical device community as reports of issues have grown. By their very nature, the configuration memory of SRAM-based FPGAs is susceptible to SEUs, causing changes to the functionality of the design—functional changes that could impact patient safety. While various techniques exist to mitigate these errors in the configuration memory of SRAM-based FPGAs, the errors still occur and their implication to system reliability must be understood. In contrast, the configuration of flash- and antifuse-based FPGAs is immune to configuration upsets, providing a higher level of system reliability.

References

"Single Event Upsets in Implantable Cardioverter Defibrillators," Bradley, P.D. and Normand, E., *IEEE Transactions on Nuclear Science*. Vol. 45, Issue 6, 1998.

Cosmic Rays May Drain Batteries of Some Older Defibrillators, October, 9, 2005. http://health.dailynewscentral.com/content/view/0001746/42/, retrieved November 15, 2010.

"Single Event Effects in Radiotherapy," F.Q. Guo, Y Zhai, Z Chen, and R Nath, *Medical Physics*. Vol. 37, 3258, 2010.

Xilinx Application Note, XAPP1073, *NSEU Mitigation in Avionics Applications*, May 17, 2010.

Xilinx White Paper, WP286, *Continuing Experiments of Atmospheric Neutron Effects on Deep Submicron Integrated Circuits*, Lesea, A., May 22, 2009.

Radiation Results of the SER Test of Actel, Xilinx and Altera FPGA Instances, Olmos, M., iRoC Technologies, SA. October 25, 2004.

Microsemmi Corporate Headquarters
2381 Morse Avenue, Irvine, CA 92614
Phone: 949-221-7100 · Fax: 949-756-0308
www.microsemi.com

Microsemi Corporation (NASDAQ: MSCC) offers the industry's most comprehensive portfolio of semiconductor technology. Committed to solving the most critical system challenges, Microsemi's products include high-performance, high-reliability analog and RF devices, mixed signal integrated circuits, FPGAs and customizable SoCs, and complete subsystems. Microsemi serves leading system manufacturers around the world in the defense, security, aerospace, enterprise, commercial, and industrial markets. Learn more at **www.microsemi.com**.

55900124-0/12.10