Neutron-Induced Single Event Upset (SEU) FAQ

August 2011

Table of Contents

Overview . . . 3

Questions and Answers . . . 3

1. What are single event upsets? . . . 3
2. What causes SEUs? . . . 3
3. What are the types of radiation? . . . 3
4. What are the sources of ionizing radiation? . . . 3
5. What are the sources of neutrons? . . . 4
6. Where can neutrons be found? . . . 4
7. Is this a new problem? . . . 4
8. What is a soft error? . . . 4
9. Can soft errors be corrected? . . . 4
10. What are configuration memory upsets? . . . 4
11. Can configuration memory upsets be corrected? . . . 5
12. Can configuration memory upsets result in device damage? . . . 5
13. Have configuration memory upsets been reported in SRAM-based FPGAs? . . . 5
14. Are radiation effects at ground-level just a theoretical problem? . . . 5
15. Are there any widely reported incidents of errors due to charged particles? . . . 5
16. Are Microsemi's antifuse-based products resistant to configuration memory upsets? . . . 5
17. Are Microsemi's flash-based products resistant to configuration memory upsets? . . . 5
18. How do configuration memory upsets affect system reliability? . . . 6
19. How can configuration memory upsets be prevented in SRAM-based FPGAs? . . . 6
20. What about configuration memory mitigation techniques? . . . 6
21. What does this mean in the "real world?" . . . 6

Microsemi

Overview

This document provides a short background for the phenomenon of soft and configuration memory upsets in semiconductor devices caused by ionizing radiation. Further details can be found in the *Understanding Single Event Effects in FPGAs* white paper.

Questions and Answers

1. What are single event upsets?

A single event upset (SEU) is a bit flip in a memory element of a semiconductor device. These upsets are random in nature, do not normally cause damage to the device, and are cleared with the next write to that memory location or by power cycling the device.

The result of upsets is data corruption. Many systems can tolerate some level of soft errors; for example, corrupted data in a video or audio stream may or may not be noticeable or important to the user.

2. What causes SEUs?

When charged particles strike the silicon substrate of an IC, they leave an ionization trail. Similarly, when a high-energy particle such as a neutron strikes the substrate, it collides with atoms in the substrate, liberating a shower of charged particles which then leave an ionization trail.

If the resulting deposited charge from these particles is sufficient, it can change the state of a memory bit or flip-flop. Specifically, the charge (electron-hole pairs) generated by the interaction of an energetic charged particle with the semiconductor atoms corrupts the stored information in the memory cell.

3. What are the types of radiation?

Radiation (both particle and electromagnetic wave) is generally classified as being either ionizing or non-ionizing. The basic dividing line between the two is energy. Ionizing radiation has sufficient energy to strip electrons from atoms, thus creating ions (atoms with charge). Examples of ionizing radiation are alpha and beta particles, protons, X-rays, and gamma rays. Neutrons are not directly ionizing, but the resulting radiation from their collisions with nuclei is ionizing.

In contrast, non-ionizing radiation only has sufficient energy to change the energy state of electrons. Examples of non-ionizing radiation are visible and infrared light, microwaves and radio waves. Non-ionizing radiation cannot induce SEUs.

4. What are the sources of ionizing radiation?

These particles can come directly from radioactive impurities and cosmic rays or indirectly as a result of high-energy particle interaction with the semiconductor itself.

Galactic cosmic rays (GCR), comprised of high-energy particles, overwhelmingly protons, impact the Earth's atmosphere constantly. These particles, when they collide with molecules in the Earth's atmosphere, produce a wide range (and a high number) of particles, primarily neutrons and protons. Neutrons are particularly troublesome because they can penetrate most man-made construction (a neutron can easily pass through five feet of concrete).

Another source of ionizing radiation comes from the packaging. Packaging materials contain trace amounts of radioactive impurities which are strong alpha emitters. The eutectic lead solders used for the solder bumps in flip-chip packaging contain lead isotopes that later decay into alpha emitters. Although the penetration depth for alpha particles is small, the proximity of packaging materials to the silicon substrate make alpha emission a concern.

5. What are the sources of neutrons?

The primary source for neutrons in the atmosphere and the ground is the air shower caused by cosmic rays. Other sources are certain radioisotopes, nuclear reactors and particle accelerators.

6. Where can neutrons be found?

The flux of cosmic rays impacting the Earth's atmosphere is modulated by both the solar wind and the Earth's magnetic field. Combining these factors results in the neutron flux being a function of latitude, longitude, altitude and solar activity, with the greatest flux occurring at high altitudes over the poles during quiet periods of solar activity. For example, a resident of a northern sea-level city such as New York experiences twice the neutron flux as someone living near the equator in Singapore, but only about one-fourth that of Denver residents. On the other hand, airplane passengers experience nearly 600 times the neutron flux of New Yorkers.

7. Is this a new problem?

Initially, the SEU issue gained widespread attention in the late 1970s as a memory data corruption issue when DRAMs began to show signs of apparently random failures. Although the phenomenon was first noticed in DRAMs, SRAM memories and SRAM-based programmable logic devices are also subject to the same effects. Unlike capacitor-based DRAMs, SRAMs are constructed of cross-coupled devices, which have far less capacitance in each cell. The lower the capacitance of a cell, the greater the chance of an upset. As both the voltage and cell size are reduced with each new process generation, the SRAM cell capacitance continues to decrease, making the cell even more vulnerable to more types of particles, and to particles of lower energy.

8. What is a soft error?

A soft error is an SEU to data memory. The terms are sometimes used interchangeably but are not entirely synonymous.

9. Can soft errors be corrected?

Error-correction circuitry (ECC) can be added to memory devices and to embedded block memory in FPGAs. With this circuitry, single- and sometimes dual-bit errors can be corrected. For flip-flops, a technique know as triple-module redundancy (TMR) where the results of two good flip-flops overrule an upset flop can be used. However, the configuration memory of SRAM-based FPGAs presents a special case.

10. What are configuration memory upsets?

Although the physical phenomenon is often referred to as a soft error or as the soft error rate (SER), strictly speaking, this term only applies to memory elements used for data storage. An error in a memory element is considered soft because it only corrupts the data.

However, when an upset occurs in the configuration memory of an SRAM-based FPGA, it can alter the functionality of the device. If an upset occurs in a bit that controls routing or the configuration of a logic cell, it is referred to as a single event function interrupt (SEFI).

Generally, there are two classes of SEFIs in SRAM-based FPGAs:

- **Routing errors:** Occur when the bits controlling routing and look-up table (LUT) configuration are corrupted. This type of error results in a continuous functional error until new configuration data is reloaded. It can take a great number of clock cycles before the error is detected and recovery actions are initiated. During this time, the error can propagate to the rest of the system.
- **Persistent errors:** Occur when the weak keeper circuits within the device are corrupted. This error cannot be corrected by reconfiguration. The device must be completely reset and reinitialized, which may require a full system reset or even power cycling.

In contrast, both antifuse and flash-based FPGAs are immune to configuration memory upset.

11. Can configuration memory upsets be corrected?

Upsets to configuration memory can be corrected by reconfiguring the FPGA; however, any logic errors have already propagated. See "How can configuration memory upsets be prevented in SRAM-based FPGAs?" and "What about configuration memory mitigation techniques?".

12. Can configuration memory upsets result in device damage?

Normally configuration memory upsets can be cleared with a reconfiguration or system power cycling and have no lasting effect. However, configuration memory upsets can create illegal conditions within the FPGA, for example, creating high-current conditions due to contentions as a result of the misconfiguration. This high current draw may damage the device or the board on which it is mounted. If not corrected, configuration memory upsets that result in simultaneously enabling pull-ups and pull-downs or serious bus contention may physically damage the FPGA.

13. Have configuration memory upsets been reported in SRAM-based FPGAs?

In addition to numerous independent studies and testing, both Altera and Xilinx readily acknowledge the issue. In fact, Xilinx does continual SEU testing for all current device families, as detailed in WP286, *Continuing Experiments of Atmospheric Neutron Effects on Deep Submicron Integrated Circuits*. The phenomenon is prevalent enough that Xilinx publishes soft error rate data for each family, updated quarterly in UG116, *Device Reliability Report.*

Altera does acknowledge the problem but does not publish test data or FIT rates.

14. Are radiation effects at ground-level just a theoretical problem?

No, based on FIT rate data from Xilinx UG116, the largest Virtex®-6 device (XC6VLX760) with 184,823,072 configuration bits will have a nominal failures-in-time (FIT) rate of 176 at sea-level in New York. While this represents a mean time between failures (MTBF) of 648 years, a system comprised of 1,000 FPGAs would experience a failure every year. The same systems based in Denver would experience failures every few months.

15. Are there any widely reported incidents of errors due to charged particles?

Several incidents across many industries have been reported in recent years. Among these:

- In 2008, a Quantas Airbus A330-303 pitched downward twice in rapid succession, diving first 650 feet and then 400 feet, seriously injuring a flight attendant and 11 passengers. The cause has been traced to errors in an on-board computer suspected to have been induced by cosmic rays. Modifications were undertaken to mitigate such errors in the future.
- Canadian-based St. Jude Medical issued an advisory to doctors in 2005, warning that SEUs to the memory of its implantable cardiac defibrillators could cause excessive drain on the unit's battery.
- Cisco Systems issued a field notice in 2003 regarding its 1200 series router line cards. The noticed warned of line card resets resulting from SEUs.

16. Are Microsemi's antifuse-based products resistant to configuration memory upsets?

Configuration memory upsets are nonexistent in Microsemi’s antifuse-based products. The Microsemi antifuse is one-time programmable (OTP) and cannot be reprogrammed via radiation or any other means. For space applications, Microsemi offers the RTAX™ product family. This family provides SEU-hardened flip-flops to provide a robust solution for use in the space market, where radiation effects are particularly severe.

17. Are Microsemi's flash-based products resistant to configuration memory upsets?

Configuration memory upsets are nonexistent in Microsemi’s flash-based products. The Microsemi flash cell has been shown to be immune to ground and atmospheric particle effects.

18. How do configuration memory upsets affect system reliability?

To a system designer, configuration memory upsets are a more serious issue than data corruption. Once an upset occurs, that functional error remains (either "routing" or "persistent" in type) until the system is reconfigured or reinitialized, depending on the type of error. If this occurs, the system FIT rate essentially becomes infinite.

19. How can configuration memory upsets be prevented in SRAM-based FPGAs?

Configuration memory upsets are a fact of life in all SRAM-based PLDs; their occurrence cannot be prevented nor is shielding practical. For the sequential elements, tripling each portion of the design and voting out the error (TMR) may mitigate some of these effects. However, voting cuts the available gates by a factor of 4 or 5 and does not deal with static circuits (where voting does not fully protect against upsets). A system designer can further mitigate configuration memory upsets by adding detecting and reconfiguring routines into the system, although this can significantly reduce system availability and adds cost and complexity.

20. What about configuration memory mitigation techniques?

Upsets in configuration memory cannot be prevented; their effects can only be mitigated. Mitigating upsets in configuration memory involves a technique called scrubbing—the configuration memory is read in the background, and when an error is detected, the error is corrected and then written back to the configuration memory. Depending upon the control logic, the system may be alerted and a device reconfiguration initiated. There are a few limitations with this technique:

- The time to read and correct a configuration memory upset is on the order of 10 to 100 ms—more than enough time for the error to propagate through the system.
- The technique in most cases is only effective against single-bit errors. Some techniques can handle dual-bit errors. None can handle multi-bit errors that could result from a burst of particles.
- The mitigation control must be hardened to prevent configuration memory upsets, or must be hosted in an external SEU-immune device.

For critical applications such as financial transaction processing or dose rate metering in insulin pumps, mitigation is not option.

21. What does this mean in the "real world?"

While small ground-level systems with a single small SRAM-based FPGA may deem the risk of configuration memory upsets acceptable, high-reliability applications comprised of large network of systems or avionics systems must seriously consider the effects.

- A modern commercial airliner with 20 or more line-replaceable units (LRU) composed of multiple boards with multiple FPGAs could represent a collection 100 large FPGAs. Given that the neutron flux at altitude near the poles is nearly 600 times greater than at New York City, the resulting MTBF is on the order of every three or four days—for a single aircraft.
- With a fleet of 1,000 commercial airliners in operation, the fleet would experience one configuration memory upset every five minutes! While the result of every upset would not be catastrophic, the potential exists. Clearly, FPGAs based on SRAM technology are inherently unsuitable for any avionics applications due to the significantly increased occurrence of configuration memory upsets at higher altitudes.
- Designers cannot control the sources of soft errors and configuration memory upsets, but their effects can be mitigated through the use of careful design techniques and by utilizing SEU-immune programmable products.
- Although the underlying causes are the same, soft errors are transient errors in memories; configuration memory upsets are non-transient errors in SRAM-based programmable logic

devices. Unlike soft errors, configuration memory upsets remain until they are detected and corrected.

- Be aware of the hidden costs of configuration memory upsets, which include time lost in supporting and analyzing random field failures, reduced system availability and reliability, and reduced levels of customer satisfaction.
- Mission-critical applications at ground level are subject to unplanned outages due to configuration memory upsets unless preventative measures are taken. The reliability of ground-based systems using SRAM-based FPGAs varies significantly with altitude, latitude, and design complexity.
- While an individual product with just a single FPGA may have a relatively low probability of failure, when this same product ships in large quantities, there is a greatly increased risk of system outages in the field due to configuration memory upsets.
- Today's deep sub-micron-based programmable devices are already very susceptible to neutron and alpha particle induced errors. Shrinking geometries are making the problem increasingly worse with each new generation of SRAM-based FPGAs.
- Previous generations of CMOS technology had wider noise margins, while newer nanometer technologies will have only a few tenths of a volt noise margin. The combination of neutrons from above and locally produced noise will continue to challenge designers in the quest to build reliable systems.

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

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif., and has more than 2,700 employees globally. Learn more at **www.microsemi.com**.

© 2011 Microsemi Corporation. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.

55800021-0/8.11