Single Event Effects on Digital Integrated Circuits: Origins and Mitigation Techniques

Raoul Velazco
TIMA Laboratory - QLF Team
46, Avenue Félix Viallet
38031 Grenoble Cedex - FRANCE
Email: raoul.velazco@imag.fr

Francisco J. Franco
Facultad de CC. Físicas - Dep. Física Aplicada III
Universidad Complutense de Madrid
28040 Madrid - SPAIN
Email: monti@fis.ucm.es

***Abstract*— New generation electronic devices have become more and more sensitive to the effects of the natural radiation coming from the surrounding environment. These radiation sources are cosmic rays and radioactive impurities, able to corrupt the content of memory cells or to induce transient pulses in combinational logic. The growing sensitivity seems to be related to two main factors: the lower and lower charge needed to define the logic levels in advanced devices and the increasing number of basic components inside the modern integrated circuits. In this paper, are described state-of-art techniques to mitigate these effects as well as typical tests to verify the radiation-tolerance of the devices and/or systems.**

I. Introduction

Failure mechanisms induced in microelectronic devices as the consequence of the radiation interaction are divided into two classes, depending on the involved physical phenomenon. First, the damage can consist in the creation of vacancies, Frenkel defects, etc. in the Si lattice. This is the *displacement damage* [1], usually related to heavy ions or neutrons.

However, in other situations, the damage is caused by ionizing mechanisms and not by displacement. Gamma or X-rays, ions, etc., create free charge in the integrated circuit (IC). In some conditions, this charge can be trapped in the dielectric layers of the devices (e.g., in the MOSFET gate oxide), causing the so-called *Total Ionizing Dose (TID)* damage [2]. Obviously, neither of the damages excludes each other. For instance, protons contribute to both TID and displacement damage.

Sometimes, the free charge is created by a particle with a high ionizing power in the presence of an electric field (e.g., in a PN reverse biased junction). Charge is eventually drained out of the so-called *charge collection volume* where it was generated, this phenomenon being equivalent to a short-lived but intense current pulse that can modify the electric state of the nearby elements.

This is the scenario where a single event effect (SEE) occurs. These phenomena are characterized by the randomness, both in the location and in the temporal distribution. According to the kind of modification, the SEEs can be classified in several categories although, in this paper, we will focus on the single event upset (SEU), multiple bit upset (MBU) and single event transient (SET), the description of other SEEs being available in [3]–[9]. SEUs are the modification of the stored information in memory cells or flip-flops, to which the MBU is closely related since it consists in the simultaneous modification of neighbor cells. Finally, SETs are transient pulses potentially perturbing combinational networks.

Regarding the system level, SEEs can be divided into two classes. Indeed, in some cases, SEEs lead to the destruction of the device (*Hard errors*). A typical example is the single event latch-up (SEL) [4]. On the other hand, the system may just wrongly behave keeping its functionality (*Soft errors*). It is important to remark that, in some cases, a soft error can be as problematic as a hard one if it affects a critical part of the system that would eventually lead to a later fatal consequences (e.g., SEUs in the cache memory of a microprocessor controlling a currency transfer: The computer is not destroyed but there can be a significant loss of money).

Before going on the description of the SEEs, it is necessary to define some useful parameters. First of all, the *static cross section,* σ, is an estimation of the sensitivity to SEEs. In the case of memories, it is the inverse of the average number of particles needed to induce a bit flip in one cell. Thus, supposing that the device has been exposed to a fluence of N_P particles with known energy and N_{EV} events were observed, then $\sigma = N_{EV}/N_P$. The *soft error rate (SER)* is defined as the probability of an error in a device working at typical conditions. Usually, it is expressed in *FIT (Failures In Time)*, equivalent to 1 error every 10^9 hours. For instance, 180-nm SRAMs usually have SER values around 1000 FIT/Mb.

II. Sources of radiation

In the past, radiation effects were a concern only for applications devoted to operate in harsh environments such as space vessels or particle accelerators so they were not considered a critical problem for standard systems. However, there are two radiation sources that can affect any kind of electronic devices, wherever they may be: traces of radioactive elements and vestigial cosmic rays, mainly neutrons present in the Earth's atmosphere [10].

A. Radioactive impurities in electronic devices

During the manufacturing process, traces of radioactive elements can contaminate the production chain, the primary source being usually unpredictable. For instance, in 1987 IBM

had to face a too high SER, caused by a contamination with polonium, a non-natural α-emitter element. Finally, its origin was traced back to the cleaning of some phosphoric acid bottles with a ^{210}Po deionizer gadget, in a factory far from the point where the problem had arisen [11]. In other cases, impurities came from an old uranium mine, laid upstream of the creek where the ICs package factory collected the water, or from phosphorous extracted from the dropping of bats living in a cavern with uranium minerals [10].

Moreover, uranium and thorium minerals such as the pitch-blende are geologically associated with the seams of tin or lead ore. If the purification is not correctly done, tin and lead might contain traces of radioactive elements. Thus, usual solder balls become a source of α-particles. Fortunately, these particles only travels some micrometers so a careful placement of the solder balls as well as the use of ultra-purified metals would avoid the disastrous action of the alpha particles, as it has been reported in the literature [12].

B. Cosmic Rays

The second source of SEEs are the cosmic rays coming from the outer space. Electronic equipment on board space crafts is exposed to a shower of energetic particles (protons, heavy ions, ...) coming either from the Sun activity or from the galaxy core. Hence, SEEs have been the reason of some fails observed in satellites [13]. Most of these particles are repelled by the Earth's magnetic field and only very few of them reach the sea level. Unlike the exospheric cosmic rays, particles arriving to the ground mainly consist in neutrons and, less often, pions [14]. Indeed, only neutral particles manage to escape from the terrestrial magnetic shield.

Even though they do not have electric charge, neutrons ionize the matter by means of secondary mechanisms. Sometimes, the neutron hits an atom that immediately is thrown out, this one being the ionizing agent. In other situations, nuclear reactions take place. This option plays its most significant role in the case of thermal neutrons, with too little energy to induce an SEE but very likely to interact with a boron isotope, ^{10}B, with the release of a 1.47-MeV α-particle [15]. Unfortunately, boron is very used in electronic devices since it is a typical acceptor impurity and a component of the boron-polysilicon glass (BPSG), used for metallization layers [16].

The value of the neutron fluence depends on the altitude, latitude, sun activity and shielding materials. There is an empirical law linking the neutron fluence with the altitude [14] although, as a first approximation, we can accept that the neutron fluence is ten times higher every 3000 m of altitude, the saturation happening at 15-20 km at a value 100-200 times higher than that at sea level. Concerning the latitude, a law was proposed [17] setting that the neutron fluence is 5 times lower on the Equator than on the Poles. Under these circumstances, it should not be strange that New York City be usually chosen as the reference point because of being at sea level and at a latitude of 45, the neutron fluence being on the order of 15 n/cm^2/h. Values at elsewhere are usually referred to this figure.

Finally, the neutron flux decreases in the periods of intense Sun activity and if the system is protected by walls, by layer of rocks, etc. However, this protection is not very effective since a 1.5-m concrete layer reduces the neutron fluence only to $1/2$ of the initial value [18].

III. Neutrons and advanced technologies

One of the questions that can arise is why SEEs are now a problem. In following sections, some answers related to the decrease in the technology features (transistor's size and operating voltage) are offered.

A. Precedents of SEEs

In the early 70s, SEEs were observed in some satellites [19]. They were judged a scientific curiosity although, some years later, their actual relevance was discovered. Something similar is presently happening with the atmospheric neutrons. Years ago, nobody believed that those exotic phenomena could affect electronic systems operating at sea level. However, in the 90s problems began to come up in aircrafts [20], where the neutron flux is higher, and just some years later SEEs have become an important topic concerning commercial electronics.

Obviously, the probability of a basic device's undergoing an SEE is very low. Nevertheless, in the case of either very huge systems or a large set of equipments simultaneously working throughout the world, this probability is not negligible. As an example of the first scenario, SEEs in supercomputers are illustrated in [21]. On the other hand, pacemakers, on which a patient's life depends and where the allowed error margin is null, show the impact of radiation on largely-distributed systems [22]. Another interesting example is that of the computer servers and workstations [23], where massive devices and very serious operations such as money transfers are combined. Prior to 2000, sudden crashes happened in UNIX servers, finally attributed to SEUs in the cache memory of the microprocessors, oddly lacking error correction systems. The replacement of the problematic chips could cost millions of dollars [24]. A similar episode was observed on router servers, which showed a high sensitivity to cosmic rays [25].

B. Reasons of this trend

In the light of the previous examples, the altitude where SEUs affect electronic devices seems to decrease in proportion to the evolution of the technology integration. In other words, sensitivity is quickly increasing. Two factors are supposed to be the reason of this trend: First of all, in spite of the fact that most works in this field forecast a decrease of the sensitivity in proportion to the scaling because of the diminution of the charge collection volume [18], [23], [26], [27], it is also widely accepted that the probability of MBUs increases as the typical sizes goes down [28]. Nowadays, the ratio between MBUs and SEUs are on the order of 1-2% [29]–[31]. Besides, other papers predict a minimum at 100-200 nm followed by an immediate and quick increase [32] although this opinion is not widely accepted [18].

Finally, new generation devices are developed with the purpose of profiting from their full potential. In this case, all the estimations agree: if the probability of a fault in the whole system is studied instead of that of an isolated cell, the chance of an error is becoming higher as miniaturization continues [18]. E. g., even though a change from an old to a newer technology implies a reduction of the cell cross section to 50% of the initial value, the number of cells may be 4 times higher. Thus, the probability of an error, eventually leading to the crash of the system, soars.

C. Factors increasing the probability of an SEE

Microelectronic devices can undergo a reduction of their tolerance to the SEEs in several situations. First of all, the sensitivity depends on the power supply values: the lower the power supply value, the higher the probability of an SEU [27], [32], [33]. Besides, other works have found a little dependence on the temperature [34]. The clock frequency also influences the SER value although some experimental results disagree. Ref. [30] shows that this is secondary for some SRAMs but other works concerning PowerPC microprocessors highlight the importance of the frequency of operation [35].

IV. Techniques to mitigate SEEs

Prior to enumerating the different techniques to avoid the incidence of SEEs, it is necessary to specify the devices where the chance is higher. DRAMs, PSRAMs, ROM and NAND memories show a high tolerance [18], [23], [36], the most significant effects being forecasted in typical SRAM devices (SRAM modules, FPGAs, cache memory of microprocessors, etc.). SETs are expected to become a very important concern in the range of 90-nm technologies and it will affect all the logic networks, whether combinational or sequential blocks.

Three are the main lines to harden devices against SEEs: *Technology, Design and Redundancy.*

A. Mitigation by Technology

Some technologies seem to be more tolerant to effects of the radiation than others. Therefore, their use would increase the tolerance of the IC. Some options are the following:

1) Removal of BPSG layer: In the 90s, BPSG process became very popular since it reduced the Si stress during the metallization. Unfortunately, this layer contains 5-10% of boron, quite sensitive to thermal neutrons as it was previously highlighted. In fact, devices without BPSG seem to have an SER ten times lower than those incorporating this process [15].

Fortunately, technologies below 130 nm no longer make use of BPSG [37]. However, if the chip designer must use technologies with BPSG, there are still two tricks. First, purification: in its natural state, boron is actually a mixture of two stable isotopes, ^{11}B (80%) and ^{10}B (20%), so using only ^{11}B will inhibit the action of the thermal neutrons. The second option is the boron shields. Chips can be covered with a B_4Si_3 layer or their external packages be doped with boron. Thus, most of the thermal neutrons will interact with boron atoms very far away from the Si bulk, avoiding the daughter α-particles reach the critical nodes.

2) Silicon-on-insulator (SOI) Technology: Some papers have reported that SOI technologies show an SER several times lower than that of the same generation bulk technology [18], [38]. Nevertheless, partially depleted SOI technologies are sensitive to a specific SEE, called *snapback* [9], [39]. This problem is solved in more modern fully depleted SOI technologies with body ties, immune to this effect and showing an SER 50 times lower than that of the bulk technologies [40].

3) Managing the doping profile: If neither the SOI technologies nor the BPSG removal are available, another option is to implant a very doped layer below the internal devices. Thus, the charge collection volume shrinks and the SEE is dimmed. Usually, the sensitivity is reduced down to 25-50% of that of a non-hardened device. Nevertheless, this choice brings two drawbacks: First, an additional step is needed during the manufacturing process. Moreover, parasitic capacitors are added, dramatically worsening the frequency response [18].

B. Mitigation by Design

In these strategies, basic circuit cells are improved adding extra devices (resistors, transistors,...) with the purpose of dealing with the consequences of the single events.

Most of the works focus on SRAM cells. Such a classic cell consists in a couple of two inverters, their outputs connected to the input of each other. The first approach to mitigate SEUs was to include resistors between the output and the input of the inverters [41]. This is equivalent to add an LP filter to the structure so the penalty is that the IC speed plunges down. Many hardened-by-design structures were proposed in the related literature, all of them being based on the addition of extra transistors to provide a feedback and to restore the memory cell content in case of an SET: DICE [42], HIT [43] and other solutions described at [44]–[49]. These structures have between 12 and 16 transistors whereas a usual cell has only 6 so they have lesser integration capability and high power consumption.

C. Mitigation by Redundancy

Previous techniques are based on a redesign of the ICs in order to reduce their sensitivity to the SEEs. However, sometimes this is not a realistic choice since electronic equipment developers usually rely on available ICs in the market (COTS). In this case, are available some well-known techniques to mitigate SEEs that can be implemented in commercial devices.

1) Error correction codes: Additional bits are added to every word in order to detect and correct erroneous values (e.g., parity bits, Hamming code, etc.). This technique is useful to avoid SEUs on data storage devices such as memories. The correction can be done by software (coding the data before saving) or redesigning a new chip [50]. The drawbacks of this technique are several: First of all, the effective memory area decreases (e.g., a 64-bit word needs 72 cells). Secondly, codes are usually able to correct only a single error but in case of a multiple error the correction system fails (in previous sections, it was stated that 1-2% of single event effects are MBUs). Finally, if a SET occurs in the coder while coding or decoding, true data words are corrupted.

2) Interleaving bits: This technique complements the previous one to reduce the sensitivity to MBUs. The principle is simple: Given that MBUs affect adjacent bits, never should data be registered in contiguous cells [23]. The main drawback of this option is the dramatic reduction of the effective capacity of the memories because of the use of ghost bits. Also, the problem of fails inside the coder/decoder remains.

3) Periodical refresh and resetting: This technique is restricted to some reconfigurable devices (FPGAs, CPLDs, etc.). Sometimes, SEU can corrupt data that keep latent without immediate consequences. Or, in other cases, the devices belong to a large set of similar elements where the damaged device can be replaced by the unaffected twins (e.g., signal conditioners measuring the temperature of a huge system). In this case, a periodical reload of the source configuration from a *trustworthy* copy erases all the internal errors. Moreover, this technique is compatible with the usual updates of the internal digital code of these devices.

Very often, an SEU can hang a microprocessor or an FPGA so their outputs no longer change. In such a situation, watchdog devices must be used to detect breaks of the data stream. If no activity is observed for some seconds, the device starts to provide reset digital pulses to the main device until the watchdog detects again signs of operation.

Some examples of these techniques are found in [51], [52].

4) Triple modular redundancy: Usually known as TMR, this technique is the most popular among the designers of fault-tolerant digital systems. Instead of using only one system, the designer implements three copies, their outputs going to a voting system, which will perform a majority vote. Thus, even if one of the copies completely stops working, the system output keeps unaffected. Obviously, there is always the risk of the crash of two of the three blocks although this situation seems to be unrealistic due to the statistic laws.

The popularity of this technique springs from the ease to implement the design in FPGAs. Indeed, there are some tools to implement HDL (Hardware Description Language) designs in TMR mode [53]. Unfortunately, the handicaps are that the size of the system soars up to three times the initial one so, sometimes, only critical parts such as the latches used in sequential logic are triplicated. Moreover, even a TMR system is committed if a SET occurs in the combinational voting block. Finally, the speed of the system decreases due to the addition of a new stage. Some representative applications can be found at the literature [54]–[56].

5) Time redundancy: These techniques are based on periodically sampling the output signal to detect transients due to SEEs. Unlike TMR, this technique is mainly devoted to minimize the action of SETs on combinational logic.

A simple solution consists in delaying the signal for T_D ns and comparing the original and the delayed signals by means of a XOR gate. If a SET happens, the signals are not equal and the system can be warned.

Similar topologies can be implemented although all of them train the same drawbacks. First, if the SET keeps for longer than T_D, the system will end up believing that the anomalous situation is correct. Also, in case of an ordinary change in the input value, the warning system only accepts the trueness of the new value after T_D ns. Therefore, this strategy usually leads to a limitation of the frequency of work. Examples incorporating this technique can be found at [57]–[59].

6) Software redundancy: This technique is suitable to harden microprocessors-based architectures and consists in modifying the program running on the device to self-detect the potential errors. This goal is achieved adding check and correction capabilities [60], such as the duplication of data and instructions, temporal redundancy, etc.

The main advantage of this technique is that it allows hardening any kind of architecture having a set of instructions, from a simple PIC to a cutting-edge PowerPC. Nowadays, this technique was proven as being able to detect around 90% of soft errors provoked by the radiation. However, the drawbacks are quite obvious: First, the size of the program, which usually is 3-4 times larger than the equivalent unhardened version. Secondly, developing hardened versions of the programs requires the development of automatic tools.

V. Evaluating the sensitivity to SEEs

After designing a system supposed to be perturbed by radiation, a mandatory task is to get experimental results allowing evaluating the sensitivity to the various radiation effects. Such a task can be accomplished by means of suitable experiments such as *life tests, accelerated radiation ground tests*, *fault injection* and *analytical techniques*.

A. Life Tests

These tests consist in exposing the tested devices to the environment of the final application. Usually, the test platform gathers a high number of devices to increase the total number of SEEs and, this way, to obtain valid statistics. Their main advantages are that the devices are tested where they are supposed to work so the only actual and trustworthy results come from them. Unfortunately, it can be a really expensive option, due to the accumulated cost of all the samples, the power consumption and the necessity of devoted facilities. Moreover, usually a longtime (from several months to a year) must elapse before obtaining accurate results [10]. A detailed description of an experiment of this sort can be found at [61].

B. Accelerated Radiation Ground Tests

To increase the probability of an SEE, an option is to use as many particles as possible. This goal is achieved using different facilities such as particle accelerators, equipments using fission decay sources like ^{252}Cf or Th foils, and laser beams. Only a few samples are needed although the test set-up is more complex than that of the life tests.

Thus, in some hours, trustworthy statistical results can be deduced and validated by repeating the experiments. However, only experiments performed with particle accelerators are suitable to investigate the consequences of SEEs for a large scope of particle energies and a sufficient coverage of the sensitive area. Fission decay sources are usually used to

validate the test platforms prior to perform tests in particle accelerators. Finally, laser facilities are complementary tools providing means to investigate the consequences of SEEs, specifically SETs or SEUs, with the chance of aiming a tiny surface and so dealing with likely critical nodes of the IC.

In the case of the radiation facilities, samples are activated so they cannot be immediately handled after the test. Besides, devices must be decapsulated in order to straightly expose the silicon active area to the beam. Even, in some cases, flipped chips must be thinned to allow back-side irradiation. Other disadvantages are the differences between the radiation source and the natural particles, whether in composition and energy spectrum. Finally, only a few facilities exist in the world so the experiments must wait until the facility is available.

C. Simulated Fault Injection Experiments

These tests are valid for microprocessor-based architectures and FPGAs. Bit-flips supposed to be caused by radioactive environments can be injected in the device by hardware and/or software strategies. In this way, the behavior of the device undergoing radiation-induced SEUs can be deeply investigated avoiding of radiation accelerated tests.

One of the state-of-the-art strategies is the so-called *CEU (Code Emulated Upset)*, in which the bit-flips are injected as the consequence of the execution of a piece of code triggered by the assertion of a interrupt-like signal [62]. Both instants of occurrence and location can be explored either exhaustively or according to a random pattern . The expected results of such experiments is the number of injected bit-flips leading to an error in the native application. Such a result is usually known as *error rate*, $\tau_{inj} = N_{errors}/N_{Injected\ SEUS}$.

If the SEU static cross section is known, the SEU sensitivity, also called *dynamic cross section,* σ_{dyn}, of the studied application can be estimated as $\sigma_{dyn} = \sigma \times \tau_{inj}$. A great deal of experiments have proved that such an estimation is very close to real measure as well as that the strategy can be successfully applied to advanced processors [63].

The main advantages of this approach are obvious: accelerated tests give too pessimistic results as they count all the errors even though they happen on unused memory cells. Despite this fact, the complexity and duration of dynamic tests lead to the use of static cross section as the final application sensitivity. Proposed fault injection approach allows to obtain realistic estimations of figures of the sensitivity and can follow without cost the evolution and updates of the application.

Yet the drawbacks are also important. Some cells are not accessible to the instruction set although they are susceptible to undergo flips and should be explored. An alternate solution is to perform fault injection using an HDL model, which is not always available.

D. Analytical Techniques

This is an useful way to estimate the tolerance of an HDL design to be implemented in an FPGA. Once the HDL code is developed and compiled, it is necessary to create a gate-level netlist to be downloaded to the DUT by the JTAG protocol. However, this gate-level design can be opened and studied with appropriate computer tools.

Thus, the action of the radiation induced bit-flips can be simulated prior to the implementation and their final consequences forecasted [64]–[66]. Also, this technique allows to identify critical points to be hardened and, on the other hand, those parts where hardening is unnecessary. This way, the size of the final design is reduced.

The drawbacks of these techniques are that, in any case, the DUT must be exposed to a radiation source to be sure of the quality of the design. Also, there is not a universal kind of gate-level netlist so specific tools must be developed for every FPGA's manufactures.

VI. Conclusion

Advanced microelectronic technologies allow the release of more and more complex devices with a growing sensitivity to the natural radiation coming from the space or from radioactive impurities. Therefore, their reliability, dependability and security is threatened although some techniques allow mitigating the consequence of these phenomena. In any case, radiation ground tests are mandatory to get a feedback about the soft error rate and the potentially critical nodes.

Acknowledgment

The stay of F. J. Franco in TIMA was supported by the Secretaría de Estado de Universidades e Investigación of the Spanish MEC under a postdoctoral grant.

References

[1] G. C. Messenger, "A Summary Review of Displacement Damage from High Energy Radiation in Silicon Semiconductors and Semiconductor Devices," *IEEE Trans. Nucl. Sci.*, vol. 39, pp. 468-473, June 1992.

[2] T. Oldham and F. McLean, "Total Ionizing Dose Effects in MOS Oxides and Devices," *IEEE Trans. Nucl. Sci.,* vol. 50, pp. 483-509, Jun. 2003.

[3] A. E. Wasckievicz, J. W. Groninger, V. H. Strahan, and D. M. Long, "Burnout of power MOS transistors with heavy ions of californium-252", *IEEE Trans. Nucl. Sci.*, vol. 33, pp. 1710-1713, Dec. 1986.

[4] K. Soliman and D. K. Nichols, "Latchup in CMOS Devices from Heavy Ions," *IEEE Trans. Nucl. Sci.,* vol. 30, p. 4514-4519, Dec. 1983.

[5] B. A. Beitman, "N-channel MOSFET breakdown characteristics and modelling for p-well technologies," *IEEE Trans. Elec. Dev.,* vol. 35, pp. 1935-1941, Nov. 1988.

[6] C. Dufour et al., "Heavy Ion Induced Single Hard Errors on Submicronic Memories," *IEEE Trans. Nucl. Sci.,* vol. 39, pp. 1693-1697, Dec. 1992.

[7] M. R. Darwish, M. A. Shibib, M. R. Pinto, and J. L. Titus, "Single Event Rupture of Power DMOS Transistors," in *Proc. of the Electron Devices Meeting*, pp. 671-674, Dec. 1993.

[8] M. Ceschia et al., "Low Field Leakage Current and Soft Breakdown in Ultra-Thin Gate Oxides after Heavy Ions, Electrons or X-ray Irradiation," *IEEE Trans. Nucl. Sci.,* vol. 47, pp. 566-573, June 2000.

[9] P. Dodd et al., "Single-Event Upset and Snapback in Silicon-on-Insulator Devices and Integrated Circuits," *IEEE Trans. Nucl. Sci.,* vol. 47, pp. 2165-2174, Dec. 2000.

[10] J. F. Ziegler and H. Puchner, *SER-History, Trends and Challenges. A Guide for Designing with Memory ICs*, Cypress Semi., USA, 2004.

[11] —, *IBM Journal of Research and Development,* vol. 40, pp. 1-128, 1996.

[12] J. Wilkinson and S. Hareland, "A Cautionary Tale of Soft Errors Induced by SRAM Packaging Materials," *IEEE Trans. Dev. Mater. Reliab.,* vol. 5, pp. 428-433, Sep. 2005.

[13] B. E. Pritchard, G. M. Swift, and A. H. Johnston, "Radiation Effects predicted, observed, and compared for Spacecraft Systems," in *IEEE Radiation Data Workshop Rec.,* pp. 7-13, 2002.

[14] J. F. Ziegler, "Terrestrial Cosmic Rays," *IBM Journal of Research and Development,* vol. 40, pp. 19-39, 1996.

[15] R. C. Baumann and E. B. Smith, "Neutron-Induced Boron Fission as a Major Source of Soft Errors in Deep Submicron SRAM Devices," in *Proc. 38th Intern. Reliab. Physics Symp.,* pp. 152-157, 2000.

[16] R. C. Baumann and E. B. Smith, "Neutron-induced ^{10}B fission as a major source of soft errors in high density SRAMs," *Microelectron. Reliab.*, vol. 41, pp. 211-218, 2001.

[17] K. Johansson, "In-Flight and Ground Testing of Single Event Upset Sensitivity in Static RAMS," *IEEE Trans. Nucl. Sci.*, vol. 45, pp. 1628-1632, June 1998.

[18] R. Baumann, "Single-Event Effects in Advanced CMOS Technology," *Section II of the short course in the frame of the 2005 IEEE Nuclear and Space Radiation Effects Conference*, Seattle, USA, July 2005.

[19] D. Binder, E. C. Smith and A. B. Holman, "Satellite Anomalies from Galactic Cosmic Rays," *IEEE Trans. Nucl. Sci.*, vol. 22, pp. 2675-2680, Dec. 1975.

[20] J. Olsen et al., "Neutron-Induced Single Event Upsets in Static RAMS Observed at 10 km Flight Altitude," *IEEE Trans. Nucl. Sci.*, vol. 40, pp. 74-77, April 1993.

[21] K. W. Harris, "Asymmetries in Soft-Error Rates in a Large Cluster System," *IEEE Trans. Dev. Mater. Reliab.,* vol. 5, pp. 336-342, Sep. 2005.

[22] P. D. Bradley and E. Normand, "Single Event Upsets in Implantable Cardioverter Defibrillators," *IEEE Trans. Nucl. Sci.*, vol. 45, pp. 2929-2940, Dec. 1998.

[23] C. W. Slayman, "Cache and Memory Error Detection, Correction, and Reduction Techniques for Terrestrial Servers and Workstations," *IEEE Trans. Dev. Mater. Reliab.,* vol. 5, pp. 397-404, Sep. 2005.

[24] —, "Sun Screen", *Forbes*, available on *http://www.forbes.com/global/2000/1113/0323026a.html.*

[25] M. Santarini, "Cosmic Radiation comes to ASIC and SOC Design," *EDN*, pp. 46-56, May 12, 2005.

[26] P. Dodd, et al., "Neutron-Induced Soft Errors, Latchup, and Comparison of SER Test Methods for SRAM Technologies," in *IEEE Electron Dev. Meeting Digest,* pp. 333-336, Dec. 2002.

[27] P. Hazucha et al., "Neutron soft error rate measurements in a 90-nm CMOS process and scaling trends in SRAM from 0.25-μm to 90-nm generation," in *IEEE Int. Electron Dev. Meeting Technical Digest,* pp. 21.5.1- 21.5.4, Dec. 2003.

[28] N. Seifert et al., "Radiation-Induced Soft Error Rates of Advanced CMOS Bulk Devices," in *IEEE Intern. Reliab. Physics Symp.,* pp. 217-225, March 2006.

[29] K. Johansson et al., "Neutron Induced Single-word Multiple-bit Upset in SRAM," *IEEE Trans. Nucl. Sci.,* vol. 46, pp. 1427-1433, Dec. 1999.

[30] J. Maiz et al., "Characterization of Multi-bit Soft Error events in advanced SRAMs," in *IEEE Intern. Electron Dev. Meeting Technical Digest,* pp. 21.4.1- 21.4.4., Dec. 2003.

[31] A. D. Tipton et al., "Multiple-Bit Upset in 130 nm CMOS Technology," *IEEE Trans. Nucl. Sci.,* vol. 53, pp. 3259-3264, Dec. 2006.

[32] T. Granlund et al., "Soft Error Rate Increase for New Generations of SRAMs," *IEEE Trans. Nucl. Sci.*, vol. 50, pp. 2065-2068, Dec. 2003.

[33] J. M. Armani, G. Simon, and P. Poirot, "Low-Energy Neutron Sensitivity of Recent Generation SRAMs," *IEEE Trans. Nucl. Sci.*, vol. 51, pp. 2811-2816, Dec. 2004.

[34] J. George et al., "SEE Sensitivity Trends in Non-hardened High Density SRAMs with Sub-micron Feature Sizes," in *IEEE Radiation Effects Data Workshop Rec.,* pp. 83-88, July 2003.

[35] F. Irom and F. F. Farmanesh, "Frequency Dependence of Single-Event Upset in Advanced Commercial PowerPC Microprocessors," *IEEE Trans. Nucl. Sci.,* vol. 51, pp. 3505-3509, Dec. 2004.

[36] A. H. Johnston, "Scaling and Technology Issues for Soft Error Rates," in *Proc. 40th Annual Research Conference on Reliability*, pp. 1-9, 2000.

[37] M. Olmos et al., "Investigation of Thermal Neutron Induced Soft Error Rates in Commercial SRAMS with 0.35 μm to 90 nm Technologies," in *IEEE Intern. Reliab. Physics Symp.*, pp. 212-216, March 2006.

[38] E. H. Cannon, et al., "SRAM SER in 90, 130, and 180 nm bulk and SOI technologies," in *IEEE Intern. Reliab. Physics Symp.,* pp. 300-304, 2004.

[39] J. R. Schwank, et al., "Radiation Effects in SOI Technologies," *IEEE Trans. Nucl. Sci.,* vol. 50, pp. 522-538, Dec. 2003.

[40] J. Baggio, et al., "Neutron and Proton-Induced Single Event Upsets in Advanced Commercial Fully Depleted SOI SRAMs," *IEEE Trans. Nucl. Sci.,* vol. 52, pp. 2319-2325, Dec. 2005.

[41] H. T. Weaver, et al., "An SEU tolerant memory cell derived from fundamental studies of SEU mechanisms in SRAM," *IEEE Trans. Nucl. Sci.,* vol. 34, pp. 1281-1286, Dec. 1987.

[42] T. Calin, M. Nicolaidis, and R. Velazco, "Upset Hardened Memory Design for Submicron CMOS Technology," *IEEE Trans. Nucl. Sci.,* vol. 43, pp. 2874-2878, Dec. 1996.

[43] R. Velazco et al., "Two CMOS Memory Cells Suitable for the Design of SEU-Tolerant VLSI Circuits," *IEEE Trans. Nucl. Sci.,* vol. 41, pp. 2229-2234, Dec. 1994.

[44] L. R. Rockett, "An SEU-hardened CMOS data latch design," *IEEE Trans. Nucl. Sci.,* vol. 35, pp. 1682-1687, Dec. 1988.

[45] S. Whitaker, J. Canaris, and K. Liu, "SEU hardened memory cells for a CCSDS Reed Solomon encoder," *IEEE Trans. Nucl. Sci.,* vol. 38, pp. 1471-1477, Dec. 1991.

[46] J. Canaris, "An SEU immune logic family," in *Proc. of the Third NASA Symp. on VLSI Design*, pp. 2.3.1-2.3.12, 1991.

[47] M. N. Liu and S. Whitaker, "Low power SEU immune CMOS memory circuits," *IEEE Trans. Nucl. Sci.,* vol. 39, pp. 1679-1684, Dec. 1992.

[48] L. W. Massengill, "SEU-Hardened Resistive-Load Static RAMs," *IEEE Trans. Nucl. Sci.,* vol. 38, pp. 1478-1485, Dec. 1991.

[49] J. R. Hauser, "SEU-Hardened Silicon Bipolar and GaAs MESFET SRAM Cells Using Local Redundancy Techniques," *IEEE Trans. Nucl. Sci.,* vol. 39, pp. 2-6, Feb. 1992.

[50] D. Yu-Lam et al., "SEE-Hardened-by-Design Area-Efficient SRAMs," in *IEEE Aerospace Conference,* pp. 1-7, 2005.

[51] J. M.A. Rodriguez-Ruiz et al., "Rad-Tol Field Electronics for the LHC Cryogenic System", in *7th European Conf. on Radiation and its Effects on Components and Systems,*, pp. 653-657, 2003.

[52] V. Sridharan et al., "Reducing Data Cache Susceptibility to Soft Errors," *IEEE Trans. Dependable Sec. Comput.*, Vol. 3, pp. 353-364, Oct. 2006.

[53] Xilinx TMRTool, *http://www.xilinx.com/esp/mil_aero/.*

[54] G. L. Smith and L. de la Torre, "Techniques to Enable FPGA Based Reconfigurable Fault Tolerant Space Computing," in *IEEE Aerospace Conference,* 2006.

[55] S. Baloch, T. Arslan, and A. Stoica, "Probability Based Partial Triple Modular Redundancy Technique for Reconfigurable Architectures," in *IEEE Aerospace Conference,* 2006.

[56] L. Sterpone and M. Violante, "Analysis of the Robustness of the TMR Architecture in SRAM-Based FPGAs," *IEEE Trans. Nucl. Sci.,* vol. 52, pp. 1545-1549, Oct. 2005.

[57] D. G. Mavis and P. H. Eaton, "Soft Error Rate Mitigation Techniques for Modern Microcircuits," in *IEEE Intern. Reliab. Physics Symp.,* pp. 216-225, 2002.

[58] P. Mongkolkachit and B. Bhuva, "Design Technique for Mitigation of Alpha-Particle-Induced Single-Event Transients in Combinational Logic," *IEEE Trans. Dev. Mater. Reliab.,* vol. 3, pp. 89-92, Sep. 2003.

[59] J. E. Kim, et al., "Mitigation of Single and Multiple Cycle Duration SETs using Double Mode Redundancy (DMR) in Time," in *IEEE Aerospace Conference,* 2005.

[60] M. Rebaudengo, et al. "Coping with SEUs/SETs in microprocessors by means of low-cost solution," *IEEE Trans. Nucl. Sci.,* vol. 49, pp. 1491-1495, June 2002.

[61] A. Lesea et al., "The Rosetta Experiment: Atmospheric Soft Error Rate Testing in Differing Technology FPGAs," *IEEE Trans. Dev. Mater. Reliab.,* vol. 5, pp. 317-328, Sep. 2005.

[62] R. Velazco, S. Rezgui, and R. Ecoffet, "Predicting error rate for microprocessor-based digital architectures by C.E.U. (Code Emulating Upsets) Injection," *IEEE Trans. Nucl. Sci.*, Vol. 47, pp. 2405-2411, Dec. 2000.

[63] F. Faure, R. Velazco, and P. Peronnard, "Single-Event-Upset-Like Fault Injection: A Comprehensive Framework," *IEEE Trans. Nucl. Sci.,* vol. 52, pp. 2205-2209, Dec. 2005.

[64] L. Sterpone and M. Violante, "A New Analytical Approach to Estimate the Effects of SEUs in TMR Architectures Implemented through SRAM-Based FPGAs," *IEEE Trans. Nuc. Sci.,* Vol. 52, pp. 2217-2223, Dec. 2005.

[65] G. Asadi and M. B. Tahoori, "Soft Error Rate Estimation and Mitigation for SRAM-based FPGAs," in *Proc. 2005 ACM/SIGDA 13th Int. Symp. on Field Programmable Gate Arrays,* pp. 149-160, 2005.

[66] G. Asadi and M. B. Tahoori, "An Analytical Approach for Soft Error Rate Estimation in Digital Circuits," in *Proc. IEEE Int. Symp. Circ. and Systems, (ISCAS)*, Vol. 3, pp. 2991-2994, 2005.