Single Event Upset: An Embedded Tutorial

***Abstract*— With the continuous downscaling of CMOS technologies, the reliability has become a major bottleneck in the evolution of the next generation systems. Technology trends such as transistor sizing, use of new materials, and system on chip architectures continue to increase the sensitivity of a system to soft errors. These errors are random and not related to permanent hardware faults. Their causes may be internal (e.g., interconnect coupling) or external (e.g., cosmic radiation). To meet the system reliability requirements it is necessary for both the circuit designers and test engineers to get the basic knowledge of the soft errors. We present a tutorial study of the single event upset phenomenon, which is a major cause of soft errors. We summarize the concepts of basic radiation mechanisms and the resulting soft error in silicon. A soft error mitigation technique with time and space redundancy is illustrated. An industrial design example, the IBM z990 system, shows how the industry are dealing with soft errors these days.**

I. Introduction

From the beginning of the recorded history, man has believed in the influence of heavenly bodies on the life on Earth. Machines, electronics included, are considered scientific objects whose fate is controlled by man. So, in spite of the knowledge of the exact date and time of its manufacture, we do not draft a horoscope for a machine. Lately, however, we have started noticing certain behaviors in the state of the art electronic circuits whose causes are traced to be external and to the celestial bodies outside our Earth. The single even upset (SEU) phenomenon, as this non-permanent (i.e., random or soft) error behavior is termed, in digital systems affects the modern nanotechnology electronic devices. We believe SEU will assume greater importance in the future [12]. Sifting through the literature of the last half a century, we have collected the necessary material for a starter. Our aim is not to cram up these six pages with most information, but to provide the essentials that can be assimilated conveniently to prepare a reader to be an effective contributor. We begin with a definition.

> "**Single Event Upset (SEU):** Radiation-induced errors in microelectronic circuits caused when charged particles (usually from the radiation belts or from cosmic rays) lose energy by ionizing the medium through which they pass, leaving behind a wake of electron-hole pairs". - - - *NASA Thesaurus*

The objective of this tutorial is to familiarize the reader with the SEU in digital electronics – definitions and terms, causes (mostly experimental), measurement and estimation, reliability standards, and the related design methods. You should expect to get the complete, but not comprehensive, information. Looking over the Appendix on the last page will improve the comprehension as you read through this article.

We will present an up-to-date understanding of the SEU phenomena. Following the historical note of the following section, we summarize the concept of basic radiation mechanisms and how a soft error occurs in silicon in Section III. Examples of soft error mitigation techniques are presented in Section IV. In Section V, a case study of soft error detection and tolerance in IBM z990 system is given.

II. Historical Notes

Soft errors have been studied by electrical, aerospace, nuclear and radiation engineers for almost half a century. In the period 1954 through 1957 failures in digital electronics were reported during the above-ground nuclear bomb tests. These were observed as electronic anomalies in the monitoring equipment because they were random and their causes could not be traced to any hardware faults [25]. Perhaps the first paper concerning the role of cosmic rays on electronics is by Wallmark and Marcus [23]. As quoted in the recent literature [16], these authors predicted that cosmic rays would start upsetting microcircuits due to heavy ionized particle strikes and cosmic ray reactions when the feature size becomes small enough. Through 1970s and early 1980s, the effects of radiation received attention and more researchers examined the physics of these phenomena. Also from 1950s, theories of fault tolerance and self-repairing computing were being developed due to the increased reliability requirement of critical applications like the space-mission [22].

May and Woods of Intel Corporation [13] reported on alpha particle induced *soft* errors in the 2107-series 16-KB DRAMs. They showed that the upsets were observed at sea level in dynamic RAMs and CCDs. They determined that these errors were caused by the alpha particles emitted in the radioactive decay of uranium and thorium present just in few parts-per-million levels in package materials. This paper represents the first public account of radiation-induced upsets in electronic devices at the sea level and these errors were referred to as "soft errors". The term soft error was used to differentiate from the repeatable errors traceable to permanent hardware faults. Guenzer and Wolicki [9] reported that the error causing particles came not only from uranium and thorium but that nuclear reactions generated high energy neutrons and protons, which could also cause upsets in circuits. Because the title of their paper was "Single Event Upset of Dynamic RAMs by Neutrons and Protons", the term "SEU" has been in use ever since [9] (refer to [16]). In 1979, Ziegler and Lanford from IBM published an article in Science [26] in which they developed a method for predicting the number of cosmic-ray-induced soft fails in electronic circuit components. They predicted that cosmic rays could result in the same upset phenomenon in electronics (not only memories) even at the sea level. The paper presented solid evidence that, the electronic sensitivity to radiation-induced soft errors could become a nightmare for the future technologies.

Following the technology trend, nowadays, higher density of electronics components is fabricated in a chip and the size of transistors keeps shrinking. The radiation induced soft errors have become one of the most important and challenging failure mechanisms in modern electronic devices. Today, soft-error rate of commercial chips is controlled to within 100~1000 FITs (see Appendix). Compared to most hard failure mechanisms that produce failure rates on the order of 1~100 FIT, the soft error rate of a low-voltage embedded SRAM can easily be 1000 FIT/Mbit. Therefore, a four-phase approach to deal with them is in progress [10]:

1) Methods to protect chips from soft errors (prevention).
2) Methods to detect soft errors (testing).
3) Methods estimate the impact of soft errors (assessment).
4) Methods to recover from soft errors (recovery).

III. What is Soft Error?

A. Soft Error Categories

An electronic circuit, that bears no permanent hardware fault, may witness unexplained events resulting in single bit changes spontaneously in the system, and there is no way to repeat such failures. Within the computer industry such phenomenon is known as a “soft fail”, to differentiate from the “hard or permanent fail”, which may be repairable [26]. After observing a soft error, there is no implication that the system hardware is any less reliable than before because the soft fail is completely random. These soft fails may be caused by the well-known electronic noise sources such as a noisy power supply, lighting, and electrostatic discharge (ESD), or the thermal radiation from the galaxy, the radiation-emitting stars and the atmospheric gases. A soft or non-permanent fault is a non-destructive fault and falls into two categories [21]:

1) Transient faults, caused by environmental conditions like temperature, humidity, pressure, voltage, power supply, vibrations, fluctuations, electromagnetic interference, ground loops, cosmic rays and alpha particles.
2) Intermittent faults caused by non-environmental conditions like loose connections, aging components, critical timing, resistive or capacitive variations and noise in the system.

With advances in manufacturing technology, the issues like temperature fluctuations and noisy power supply can barely affect the sub-micron semiconductor reliability. The errors caused by cosmic rays and alpha particles are the dominant factors in an unstable electronic system.

B. Radiation Mechanisms in Semiconductors

Three key radiation sources cause soft errors in advanced semiconductor devices [2], [4]:

1) Alpha particles emitted by traces of uranium or thorium impurities in packaging materials were the dominant cause of soft errors in DRAM devices in the late 1970s. Alpha particles are emitted when the nucleus of an unstable isotope decays to a lower energy state. It contains kinetic energy in the range of about 4~9 MeV. There are many radioactive isotopes, however, uranium and thorium have the highest activity among the naturally occurring materials. In the terrestrial environment, major sources of alpha particles are radioactive impurities such as lead-based isotopes in solder bumps of the flip-chip technology, gold used for the bond wires and lid plating, aluminum in ceramic packages, lead-frame alloys and interconnect metalization [7].
2) High-energy (>1 MeV) neutrons from cosmic radiation can induce soft errors in semiconductor devices via secondary ions produced by the neutron reaction with silicon nuclei. Cosmic rays which are of galactic origin react with the Earth’s atmosphere to produce complex cascades of secondary particles. Less than 1% of the primary flux reaches ground level and the predominant particles include muons, neutrons, protons, and pions. Because pions and muons are short-lived and proton and electrons are attenuated by Coulombic interaction with the atmosphere, neutrons are the most likely cosmic radiation sources to cause SEU in deep-submicron semiconductors at terrestrial altitude. The neutron flux is dependent on the altitude above the sea level. The density of the neutron flux increases with altitude.
3) The third significant source of ionizing particles in electronic devices is the secondary radiation induced from the interaction of cosmic ray neutrons and boron. It is the radiation induced by low-energy cosmic neutron interactions with the isotope *boron-10* (^{10}B is commonly used as *p*-type dopant for junction formation in IC package). Specifically in BPSG (*Borophosphosilicate glass*) dielectric layer is commonly used to form insulator layers in IC manufacturing. Boron has two isotopes: ^{10}B and ^{11}B of which ^{10}B is unstable. The reaction scheme is shown in Figure 1. In the $^{10}B(n, \alpha)$ Li reaction the lithium nucleus is emitted with a kinetic energy of 0.84 MeV 94% of the time and 1.014 MeV 6% of the time. The gamma photon has energy of 478 KeV, while the alpha particle is emitted with an energy of 1.47 MeV [2]. This mechanism has recently been found to be the dominant source of soft errors in 0.25 and 0.18μ SRAM fabricated with BPSG. Modern microprocessors use highly purified package materials and this radiation mechanism is greatly reduced, making the high-energy cosmic rays the major reasons for soft errors. The SEU due to activation of ^{10}B can be mitigated by removing BPSG material from the process flow. For the future deep-submicron DRAM generations a greater suppression of *soft error rate* (SER) is expected for devices made with silicon-on-insulator (SOI) technologies [18].

C. Sensitive Regions in Silicon

A *single event transient* (SET) is caused by the generation of charge due to a single particle (proton or heavy ion) passing through a sensitive node in the circuit. SETs in linear devices differ significantly from other types of *single event effects* (SEE) like SEU in a memory and each SET has its unique characteristics like polarity, waveform, amplitude, duration, etc. Those unique properties depend on particle impact location, particle energy, device technology, device supply voltage and output load. In addition, an SET is normally

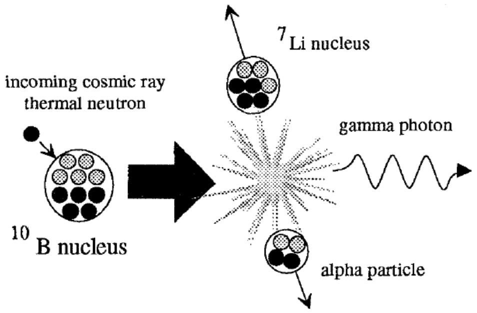


Fig. 1. Fission of ^{10}B induced by the capture of a neutron (commonly happened in SRAMs) [2]

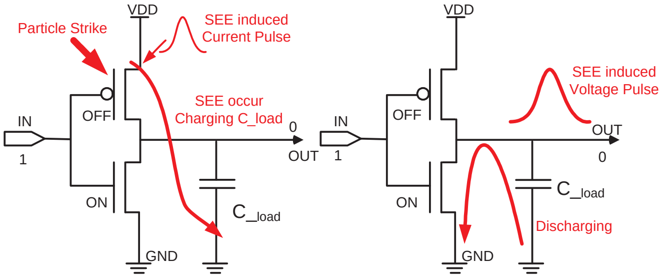


Fig. 2. Schematic view of how SEE-induced current pulse translates into a voltage pulse in a CMOS inverter.

non-destructive and may be corrected by “non-destructive” recovery methods. In CMOS circuits, the “off” transistors struck by a heavy ion in the junction area are most sensitive to SEU by particles with high enough LET (*linear energy transfer*; see Appendix) of around 20 $MeV-cm^2/mg$. When these particles hit the silicon bulk, the minority carriers are created and if collected by the source/drain diffusion regions, the change of the voltage value of those nodes occurs [20]. A particle can induce SEU when it strikes at the channel region of the off-NMOS transistor and the drain region of the off-PMOS transistor. The ionization can induce a current pulse in a p-n junction. When the charge injected by the current pulse at a sensitive node of a bistable data storage element exceed the critical charge (Q_{crit}), a SET is generated at the affected junction. The current transient typically lasts 200 picoseconds with the bulk of the charge collection occurring within 2~3 microns of the junction region for modern submicron CMOS technologies. These time constants depend strongly on the type of ion, its initial energy and the properties of the specific technology [3]. If enough charge is collected by a node the data state may change. The collected charge (Q$_{coll}$) is a function of the ionizing particle’s energy and trajectory, silicon substrate structure and doping, and the local electric field [3]. Conceptually, if Q$_{coll}$ is greater than the critical charge (Q$_{crit}$) then a soft error occurs.

D. Single Event Transient in CMOS inverter

A commonly used model for the transient current in the material caused by a particle with LET is given in a double-exponential form [15]. It gives an induced current with a rapid rise time but a more gradual fall time:

$$I(t) = \frac{Q_{coll}}{\tau_\alpha - \tau_\beta}(e^{-\frac{t}{\tau_\alpha}} - e^{-\frac{t}{\tau_\beta}}) \qquad (1)$$

where Q_{coll} is the collected charge in the sensitive region, τ_α is the collection time constant which is a process-dependent collection time constant of the junction, and τ_β is the ion-track establishment time constant which is relatively independent of the technology. Typical values are approximately $1.64 \times 10^{-10} sec$ for τ_α and $5 \times 10^{-11} sec$ for τ_β [6].

We simply choose $L = 2\mu$ for the bulk, and use approximated typical values $1.64 \times 10^{-10} sec$ for τ_α and $5 \times 10^{-11} sec$ for τ_β. We can compute the transient current pulse created by the particle strike from (1). Our interest is in the induced transient voltage pulse that may propagate through several levels of logic gates. Because a particle can induce an SEU when it strikes at the channel region of the off-NMOS transistor and the drain region of the off-PMOS transistor, for illustration, we only consider an off-PMOS drain area as the sensitive area. The critical charge depends not only on the total charge collected at the sensitive node, but also on the temporal shape of the current pulse and the device supply voltage. So, a parameter called “switching time (t_{th})” or “feedback time” is defined as the time that the gate voltage exceeds the threshold voltage at the affected node and must be evaluated for calculating the Q_{crit}. When the worst case impact occurs such that the off-PMOS drain region is affected by the particle strike, Q_{crit} can be calculated by integrating the current that flows at the sensitive node after the strike [8]. The conservation of charge requires the charge-current continuity equation to be satisfied. Ideally, charge collected at the node is integrated from 0 to infinite time. Because the voltage change across the capacitor is proportional to the instantaneous electric charge Q on the capacitor (2.b). From (2) we get the output SEE induced voltage caused by the particle strike at the off-PMOS drain region as given by (3):

$$\begin{cases} Q_{crit} = \int_0^{t_{th}} I_{drain}(t)dt & \text{(a)} \\ V = \frac{Q}{C} & \text{(b)} \end{cases} \qquad (2)$$

$$V = \frac{1}{C}\int_0^{t_{th}} I_{drain}(t)dt \qquad (3)$$

The pulse width of the voltage pulse depends on the value of the capacitance and the RC time constant of the discharging path. For example, in ami12 technology, when the output load capacitance is 100fF, the amplitude of the voltage pulse is $0.65pC/100fF = 0.65 \times 10^{-12}C/100 \times 10^{-15}F = 0.65V$. From these equations we can see that for the same charge collected in the sensitive area, the smaller the load capacitance it has, the larger is the amplitude of the SEE-induced voltage pulse. The discharge process can be modeled by the simple RC-circuit. So, the voltage as a function of time is $v(t) = v(0)^{\frac{-t}{RC}}$ and the smaller the RC value, the faster the discharge process. An schematic view of how the SEE-induced current pulse translates into an SEE-induced voltage pulse is illustrated in Figure 2.

IV. Soft Error Mitigation Techniques

The soft error tolerant techniques can be classified into two types: prevention and recovery. The methods to protect microchips from soft-errors are the prevention methods, used during the chip design and development. The recovery methods include on-line recovery mechanisms from soft-errors in order to achieve the chip robustness requirement. These include fault tolerant computing, ECC/parity, online-testing and redundancy. It is necessary to note that soft error is not the only reason why computer systems need to resort to a recovery procedure. Random errors due to noise, unreliable components, and coupling effects may also require the recovery mechanisms [10]. The need for a recovery mechanism stems from the fact that prevention techniques may not be enough for contemporary microchips, because the supply voltage keeps reducing, feature size keeps shrinking, and the clock frequency keeps increasing. Also, the cost of prevention techniques for a fault tolerant design may be too high. Because the error-tolerant computing is a broad area, here we concentrate on sample techniques that have been used for soft error mitigation.

A. Prevention Techniques

1) Purify the Fabrication Material: The significantly improvement in the SER performance of microelectronics can be achieved by eliminating or reducing the sources of radiation. To reduce the alpha particle emission in the final packaged IC, high purity materials and processes are employed. Uranium and thorium impurities have been reduced below one hundred parts per trillion for high reliability. Going from the conventional IC packaging to an ultra-low alpha packaging materials the alpha emission is reduced from 5~10 alphas/cm^2-hr to less than 0.001 alphas/cm^2-hr. To reduce the SER induced by the ^{10}B activation by low energy neutrons, BSPG is replaced by other insulators that don't contain boron. In addition, any processes using boron precursors is carefully checked for ^{10}B content before introducing them to manufacturing process [3]. When these measures are employed the SER of the IC is reduced dramatically, but the SER caused by the cosmic high energy neutron interactions cannot be easily shielded.

2) Radiation Hardened Process Technologies: SER performance can be greatly improved by adapting the process technology either to reduce the collected charge (Q_{coll}) or increase the critical charge (Q_{crit}) [24]. One approach is to use additional well isolation (triple-well or guard-ring structure) to reduce the amount of charge collected by creating potential barriers, which can limit the efficiency of the funneling effect and reduce the likelihood of parasitic bipolar collection paths [5].

Another approach replaces bulk silicon well-isolation with silicon-on-insulator (SOI) substrate material. The direct charge collection is significantly reduced in SOI devices because the active device volume is greatly reduced (due to thin silicon device layer on the oxide layer) [18]. Recent work shows a 10x reduction in SER achieved over conventional bulk devices when a fully depleted SOI substrate is used. Unfortunately, SOI substrates are more expensive than conventional bulk substrates and phenomena like parasitic bipolar action limit further reduction of SER [3]. Circuit-level solutions such as the addition of cross-coupled resistors and capacitors to decrease bit-line float time are also employed.

B. Recovery Techniques

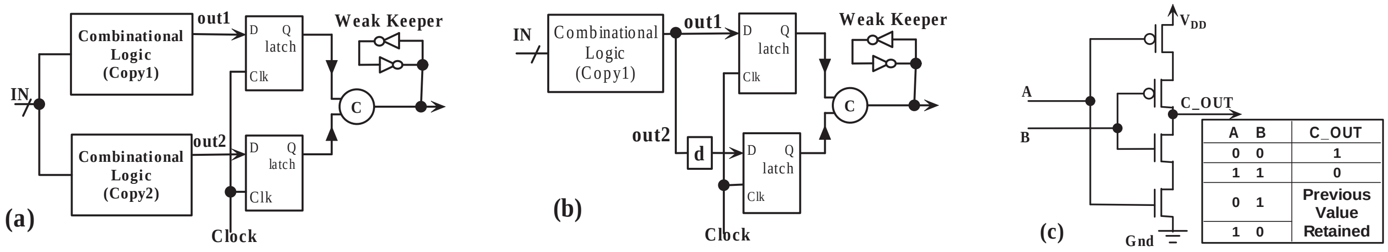
Fault-tolerant computing methods, in the literature for quite some time [22], have seen renewed interest due to the SEU phenomenon. On-line testing techniques are frequently used as recovery solutions for soft error mitigation. The concept of on-line testing is to execute a self-checking function, like detection, and correction, concurrently within the normal function execution cycle. Specific techniques includes self-checking design [19], concurrent error detection for FSMs by signature monitoring, error detection and correction (EDAC) code, and redundancy.

1) Redundancy: The basic idea of redundancy in design is to gain higher system reliability by sacrificing the minimality of time or space or both. The redundancy is favorite fault-tolerant design method exploited by electronic designers for half a century. The classic triple modular redundancy (TMR) with a majority voter [1] continues to be widely used.

Mitra *et al.* [17] combine a self-checking design with time redundancy based on the C-element gate to compare two samples of the outputs signal from a combinational circuit at times t_0 and t_0+d. The C-element has the ability to eliminate glitches at combinational outputs. Their error correction structure is illustrated in Figure 3. The space redundancy and time redundancy are often combined together to meet high fault-tolerance requirement with reduced hardware overhead, such as duplication and comparison instead of TMR.

2) ECC and Parity: Memories have a significant role in modern systems. Because of very high density of storage cells, a large memory is more sensitive to ionized particles than the logic. A simple solution for protecting a memory is to add a parity bit to each memory word. During each write operation, a parity generator computes the parity bit of the data to be written and the data, together with the computed parity bit, are then written in the memory. If a particle strike alters the state of 1 bit of a memory word, the error can be discovered by checking the parity code during the read operation. Because this scheme can only detect error but not correct it, it must be combined with a system-level approach for error recovery [19]. For example, if the memory is an instruction cache or a write-through data cache, then all data in the cache can also be found in the main memory. Thus, the error can easily be recovered by simply activating the *miss* signal of the cache each time the parity checker detects an error. In most situations, however, the error recovery in a memory is more complex so protection of the memory by means of codes, like error correcting code (ECC), is preferable.

Error correcting codes were first developed for reliable communication of digital information. Error detection and correction (EDAC) codes play an important role in many successful SEU mitigation schemes, both at the system level



A	B	C_OUT
0	0	1
1	1	0
0	1	Previous Value Retained
1	0	

Fig. 3. Error correction using duplication, (a) space redundancy structure, (b) time redundancy structure, and (c) C-element [17].

TABLE I

SAMPLE EDAC METHODS FOR MEMORY OR DATA DEVICES [11].

EDAC Method	EDAC Capability
Parity	Single Bit Error Detect
Hamming Code	Single Bit Error Correct, double bit detect
RS Code	Correct consecutive and multiple bytes in error
Conventional Encoding	Corrects isolated burst noise in a communication stream
Overlying Protocol	Specific to each system implementation

and at the chip level [16]. Table I summarizes sample EDAC methods for memory, data and systems [11].

V. A CASE STUDY

The IBM eServer z990 system is designed to detect and recover from both soft and permanent errors [14]. This system introduced a new nodal technology that supports concurrent capacity upgrade. The z990 contains up to four pluggable nodes connected through a planar board in a daisy chain interconnect structure. Each node contains up to 64 GB physical memory and 32 MB L2 cache for a system capacity of 256 GB memory and 126 MB L2 cache.

The memory and L2 cache across these nodes are fully ECC protected. ECC is also used to protect most of the system data and control buses. Parity is used in many other places to allow for the detection of errors and many of the detected errors are recovered using instruction or operation re-executed (timing redundancy). If the retry is not successful, the processors may be forced to checkstop and a spare processor may be used (space redundancy). In rare cases when the system is operated under severe environment, the whole system may be checkstopped to protect against silent data errors. The instruction and execution units within the microprocessor are duplicated and results compared in order to achieve a higher level of protection in processor cores. Techniques of checkpointing (saving critical states of the processor over time) and rollback (restoring those critical states in the presence of errors) allow recovery from soft errors. Soft error mitigation techniques used in each component of z990 system are:

- ***Memory*** The memory is protected by (140/128) single symbol correction/double symbol detection (SSC/DSD) with 2-bit symbols.
- ***L2 Cache*** The L2 cache has (39/32) SEC/DED to protect against hard and soft errors.
- ***Other SRAMs and Register Files*** The remaining SRAMs in the system are either protected by ECC or parity.
- ***Dataflow*** Most dataflow throughout the system control element is protected by ECC.
- ***Center Processor Fetch Data Bus and I/O Buses*** The CP fetch data bus is parity protected. ECC on this bus is not needed because the L1 cache is store-thru. When a parity error is detected on the fetch bus, the processor is sent into checkpoint recovery and the entire L1 cache can be cleared and refetched as needed from the L2 and memory.
- ***Store Address Stacks*** The Center Processor address stacks, which are made up of register arrays on the SCC chip, are protected. When a parity error is detected in the store address stack, the processor is sent into instruction processor damage recovery mode to indicate that the store could not be processed.
- ***Microprocessor Recovery in Logic Paths*** The recovery strategy for z990 is to maintain an architectural checkpoint on every hardware instruction boundary, so that once an error is detected, the in-flight operations can be purged, the error cleared, the last checkpoint restored, and the instruction processing resumed from the last checkpoint.

Overall, in IBM z990 system, microarchitecture-level SEU mitigation features include: extensive use of ECC and parity with retry on data and controls; full SRAM ECC and parity protection; operational retries; microprocessor mirroring, checkpointing and rollback, and some hardware derating techniques. These approaches may be useful for future mainframe, general purpose, and application-specific computing systems.

VI. CONCLUSION

Soft error rate in logic and and memory chips will continue to increase as devices become more sensitive to soft errors even at sea level. The logic FIT rate is expected to increase faster due to internal phenomena such as cross coupling, ground bounce and delay faults, becoming comparable to the prevailing FIT rate of memory. The IBM z990 system provides an illustration of how the soft error issue might be handled in the industry. Open soft error issues are in the areas of EDA tools, radiation tests and measurement, analysis of newer radiation mechanisms, device hardening, soft error rate analysis, and error mitigation methods, on which research is being conducted. We hope we have given a running start to our reader.

APPENDIX

Definitions and Terminology[1]

Collected Charge: The charge collected by a particular device node during the passage of a particle. The collected charge is dependent on the geometry and doping of the node, the particle property like mass, energy and trajectory, and the density and type of material in the volume being penetrated by the incident radiation.

Cross Section (σ): The device SEE response to ionizing radiation.Normally, the units for cross section are $cm^2/device$ or cm^2/bit.

Critical Charge (Q$_{crit}$): The minimum amount of charge that when collected at any sensitive node will cause the node to change state. The critical charge is usually generated by incident radiation and, it is dependent on the linear energy transfer effective which is usually a function of the angle of incident particle radiation.

flux density: The time rate of flow of particle energy emitted from or incident on a surface, divided by the area of that surface. The flux density is usually expressed in particles per square centimeter second (N/cm^2-s) or particles per square centimeter hour (N/cm^2-h).

LET: Linear Energy Transfer. LET is a measure of the energy transferred to the device per unit length as an ionizing particle travels through a material. The common unit is MeV-cm^2/mg of material (Si for MOS devices).

LET$_{th}$: LET threshold (LET_{th}) is the minimum LET to cause an effect at a given particle fluence.

SEE: Single Event Effect. Any measurable or observable change in state or performance of a microelectronic device, component, subsystem or system resulting from a single energetic particle strike. SEE include SEU (Single Event Upset), SEL (Single Event Latchup), SEB (Single Event Burnout) and SEFI (Single Event Functional Interrupt).

Sensitive Volume: A region, or multiple regions affected by SEE-induced radiation. The sensitive volume is determined by the angle of the incident radiation, the mass and energy of the incident particles and the density, type of the material in the volume being penetrated by the incident radiation. Is is not easy to know the geometry of the sensitive volume of the device but some information can be gained from the test cross section data.

Unit and Conversion Factors

Energy Unit: Electron Volt (eV) One eV is the energy gained by one electron in accelerating through a potential difference of 1 volt. Energy in radiation is usually in unit of MeV (10^{6}eV) or KeV (10^{3}eV). 1eV = 1.6$\times10^{-19}$ J, 1MeV = 1.6$\times10^{-13}$ J.

FIT: Failure in Time; the number of failures per 10^9 device hours. 1 year MTTF (Mean Time To Failure) = 10^9/(24×365) FIT = 114,155 FIT.

REFERENCES

[1] A. Avizienis, "Faulty-Tolerant Computing: An Overview," *Computers, IEEE Trans. Computers*, vol. 4, no. 1, pp. 5–8, 1971.

[2] R. Baumann, "Soft Errors in Advanced Semiconductor Devices-Part I: The Three Radiation Sources," *IEEE Trans. Device and Materials Reliability*, vol. 1, no. 1, pp. 17–22, 2001.

[3] R. Baumann, "Soft Errors In Commercial Integration Integrated Circuits," *International Jour. High Speed Electronics and Systems*, vol. 14, no. 2, pp. 299–309, 2004.

[4] R. Baumann, "Soft Errors in Advanced Computer Systems," *IEEE Design & Test of Computers*, vol. 22, no. 3, pp. 258–266, 2005.

[5] D. Burnett, C. Lage, and A. Bormann, "Soft-Error-Rate Improvement in Advanced BiCMOS SRAMs," in *Proc. 31st Annual IEEE Reliability Physics Symp.*, Mar. 1993, pp. 156–160.

[6] V. Carreno, G. Choi, and R. K. Iyer, "Analog-digital simulation of transient-induced logic errors and upset susceptibility of an advanced control system," in *NASA Technical Memo 4241*, 1990.

[7] C. L. Claeys and E. Simoen, *Radiation Effects in Advanced Semiconductor Materials and Devices*. Springer, 2002.

[8] C. Detcheverry, C. Dachs, E. Lorfevre, C. Sudre, G. Bruguier, J. M. Palau, J. Gasiot, and R. Ecoffet, "SEU Critical Charge and Sensitive Area in A Submicron CMOS Technology," *IEEE Trans. Nuclear Science*, vol. 44, no. 6, pp. 2266–2273, 1997.

[9] C. S. Guenzer, E. A. Wolicki, and R. G. Allas, "Single Event Upset of Dymanic RAMs by Neutrons and Protons," *IEEE Trans. Nuclear Science*, vol. 26, pp. 5048–5052, Dec. 1979.

[10] S. Kundu, G. Rajesh, N. Vijaykrishnan, R. Raina, and S. Pia, "Is the Concern for Soft-Error Overblown?," in *Proc. InternationalTest Conf. (Panel Discussion)*, 2005.

[11] K. L. LaBel, P. W. Marshall, J. L. Barth, E. Stassinopoulos, C. Seidleck, and C. Dale, "Commercial Microelectronics Technologies for Applications in the Satellite Radiation Environment," in *Proc. 1996 IEEE Aerospace Applications*, (New York), 1996, pp. 375–390.

[12] J. Maiz and N. Seifert, "Introduction to the Special Issue on Soft Errors and Data Integrity in Terrestrial Computer Systems," *IEEE Trans. Device and Materials Reliability*, vol. 5, no. 3, pp. 303–304, Sept. 2005.

[13] T. C. May and M. H. Woods, "A New Physical Mechanism for Soft Errors in Dynamic Memories," in *Proc. 16th Annual Reliability Physics Symp.*, 1978, pp. 33–40.

[14] P. J. Meaney, S. B. Swaney, P. N. Sanda, and L. Spainhower, "IBM z990 Soft Error Detection and Recovery," *IEEE Trans. Device and Materials Reliability*, vol. 5, no. 3, pp. 419–427, 2005.

[15] G. C. Messenger, "Collection of Charge on Junction Nodes from Ion Tracks," *IEEE Trans. Nuclear Science*, vol. 29, no. 6, pp. 2024–2031, 1982.

[16] G. C. Messenger and M. Ash, *Single Event Phenomena*. Chapman & Hall, 1997.

[17] S. Mitra, Z. Ming, S. Waqas, N. Seifert, B. Gill, and K. S. Kim, "Combinational Logic Soft Error Correction," in *Proc. International Test Conference*, 2006, pp. 1–9.

[18] O. Musseau, "Single-Event Effect in SOI Technologies and Devices," *IEEE Trans. Nuclear Science*, vol. 43, no. 2, pp. 603–613, 1996.

[19] M. Nicolaidis, "Design for Soft Error Mitigation," *IEEE Transactions on Device and Materials Reliability*, vol. 5, no. 3, pp. 405–418, 2005.

[20] M. Omana, G. Papasso, D. Rossi, and C. Metra, "A Model for Transient Fault Propagation in Combinatorial Logic," in *Proc. 9th IEEE On-Line Testing Symp.*, 2003, pp. 111–115.

[21] A. J. van de Goor, *Testing Semiconductor Memories: Theory and Practice*. Wiley, 1991.

[22] J. von Neumann, "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components (1959)," in A. H. Taub, editor, *John von Neumann: Collected Works, Volume V: Design of Computers, Theory of Automata and Numerical Analysis*, Oxford University Press, 1963, pp. 329–378.

[23] J. T. Wallmark and S. M. Marcus, "Minimum Size and Maximum Packing Density of Non-Redundant Semiconductor Devices," *Proc. IRE*, vol. 50, pp. 286–298, Mar. 1962.

[24] Q. Zhou and K. Mohanram, "Gate Sizing to Radiation Harden Combinational Logic," *IEEE Trans. CAD*, vol. 25, no. 1, pp. 155–166, 2006.

[25] J. F. Ziegler, "IBM Experience in Soft Fails in Computer Electronics (1978-1994)," *IBM Jour. Res. and Dev.*, vol. 40, no. 1, pp. 3–18, 1996.

[26] J. F. Ziegler and W. A. Lanford, "Effect of Cosmic Rays on Computer Memories," *Science*, vol. 206, no. 4420, pp. 776–788, Nov. 1979.

[1] These miscellaneous definitions and terms are collected from JEDEC standard and relevant papers.