FPGA RADIATION HARDENING

SEMINAR REPORT

Submitted by

AJMAL M ALI

in partial fulfillment for the award of the degree

of

Master of Technology

in

VLSI AND EMBEDDED SYSTEMS

of

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF ELECTRONICS ENGINEERING

MODEL ENGINEERING COLLEGE

COCHIN 682 021

APRIL 2014

MODEL ENGINEERING COLLEGE

THRIKKAKARA, KOCHI-21

DEPARTMENT OF ELECTRONICS ENGINEERING

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that the SEMINAR report entitled

FPGA RADIATION HARDENING

Submitted by

AJMAL M ALI

is a bonafide account of the work done by him under our supervision

Dr. Jayasree V K

HOD &

Seminar coordinator

Mr. Jagadeesh Kumar P

Seminar guide

ABSTRACT

Continuous reduction in size and power of CMOS transistors have resulted in their increased sensitivity to radiation effects. With the amount of charge representing the stored information dropping at successive technology nodes, the sensitivity of CMOS devices to single particle charge collection is increasing. The configuration memories within reconfigurable components, such as EEPROM-based FPGA are particularly vulnerable to radiation-induced single event effects. The Seminar presents a Silicon on Insulator (SOI) based configuration memory system for use in a radiation hard reconfigurable system. A non-volatile storage cell, able to be manufactured in a standard single Polysilicon SOI CMOS process with no special layers, is combined with a Schmitt amplifier. A simple current detector of the type used in conventional RAM circuit allows the configuration memory to be setup to exhibit self-correcting, or "Auto Scrubbing" behaviour which results in a final structure that exhibit characteristics enhancing its resistance to radiation. Other circuit design techniques have been used to make systems more radiation tolerant, it is often difficult to justify the cost in terms of area and power compared to the level of extra robustness achieved by the techniques.

Acknowledgement

I would like to express my sincere thanks to our Principal, Dr. V.P Devassia, for his valuable support and advice.

I would also like to thank our HOD, Dr. Jayasree V. K for her valuable help and support. I am highly obliged to her for all the valuable suggestions and guidance she provided.

I am highly indebted to our Seminar Coordinator, Mrs Anjana Devi S for her guidance, support and constant supervision throughout the duration of the work as well as for providing all the necessary information regarding the seminar.

I express my heartfelt gratitude to our M-Tech VLSI and Embedded Systems coordinator Mr Jagadeesh Kumar P, for all his help, valuable suggestions and directions. I offer my sincere gratitude to all my friends for their support that helped me get through the tough phases during the course of this work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

SEU	Single Event Upset
TMR	Triple Modular Redundancy
SOI	Silicon On Insulator
SOS	Silicon On Sapphire
TID	Total Ionization Dose
SEE	Single Event Effects
MTBF	Mean Time Between Failure
FIT	Failure In Time
ICAP	Internal Configuration Access Port
LUT	Look Up Table
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failure

CHAPTER 1

INTRODUCTION

Scaling of MOS transistor dimensions is a key factor in the improvement of performance of CMOS technologies. For deep submicron technologies, the energy-delay product decreases approximately with the fourth power of the dimension scaling factor. This power efficiency can be attributed to a quadratic reduction of switching charge, linear increase in speed, and linear decrease in supply voltage. At the same time, transistor area decreases quadraticaly. The trend shows a slow increase in die area which means that the number of transistors increases at least quadraticaly.

Faults are becoming increasingly pronounced in emerging applications and technologies, from permanent faults arising from circuit processing at nanometre scales to transient soft errors arising from high-energy particle hits. Continuous reductions in size and power of Cmos transistors have resulted in their increased sensitivity to Radiation effects. At the same time, reconfigurable systems, such as field programmable gate arrays (FPGAs), are becoming increasingly attractive to system designers as they support flexible design and post manufacture upgrades. The expanded use of field programmable gate arrays (FPGA) in remote, long life, and system-critical applications requires the development and implementation of effective, efficient SRAM-based FPGA fault-tolerance techniques [4].

However, reconfigurable components, such as SRAM-based FPGAs are particularly sensitive to so-called single event upset (SEU) induced soft errors caused by cosmic radiation or the impact of high energy charged particles. As the circuit is defined via its configuration memory, any error in this memory may result in a range of potential effects—from nothing, to a change in the design functionality through to internal open or short circuits [1].

Various techniques have been developed to harden CMOS logic against SEU, both for the underlying hardware and at the design stage. Extensive work has been undertaken to improve the reliability of existing FPGA devices. While mitigation techniques, such as triple modular redundancy (TMR), scrubbing, and other circuit design techniques have been used to make systems more radiation tolerant, it is often difficult to justify the cost in terms of area and power compared to the level of extra robustness achieved by the techniques [4].

In silicon on insulator (SOI) technology, the active silicon layer, within which the transistors are created, is separated from an underlying substrate by a layer of insulating material. For example, silicon on sapphire (SOS) is a subclass of SOI technology where the insulating material is sapphire (Al_2O_3). As the region between active devices is etched away in this technology, and the devices sit on an insulating layer of sapphire, complete electrical isolation is achieved between active devices, as well as between the devices and the silicon substrate. Its inherent resistance to radiation, low gate and interconnect capacitance, high noise immunity and relative insensitivity to voltage variation makes CMOS/SOS a good solution for high radiation environments. Furthermore, because it lacks the parasitic PN junctions between the source/drain regions and the substrate, SOI supports a number of circuit techniques that are simply not possible in bulk CMOS [4].

In this seminar, we analyse a radiation hard EEPROM memory cell based on SOS technology for application in reconfigurable memory systems. In addition to its intrinsic radiation resistance, the cell can be set up to exhibit self-correcting, or auto-scrubbing behaviour.

CHAPTER 2

RADIATION EFFECTS

Radiation has been a major concern for the space and aviation electronics for almost half a century. Trapped protons and electrons, high energetic particles, cosmic radiation and solar flares all have their effects on electronic devices. These are now showing up at lower altitudes. Given the reduction in feature size and operating voltages accompanying developments in IC technology, the effect has become more severe and is becoming a concern even at sea level, potentially affecting both the physical structure of an electronic device, as well as its functionality. In general, the description of radiation effects can be divided into two general categories. Total ionization dose (TID) and single event effect (SEE) [3].

2.1 Total Ionization Dose (TID):

This represents the cumulative effect on a transistor circuit of long-term exposure to protons and neutrons. The effect occurs when high energy electrons or protons pass through a device and produce electron-hole pairs, which then interact with its gate and field oxide. Electrons resulting from ionization have high mobility in the oxide and are quickly swept out by the internal fields. Holes, on the other hand, have much lower mobility and only a fraction of them will be transported to the silicon/silicon-dioxide interface, where they will be trapped. This changes the threshold voltage and mobility of the transistors, thereby changing their characteristics. The more long-lasting of these effects can cause permanent or semi-permanent damage in the device, such as increased device leakage and power consumption, timing changes plus an overall decrease in functionality [3].

2.2 Single Event Effects (SEE):

SEE are not cumulative and (as suggested by the name) result from single energetic particles. It represents a change of state in a memory cell or register due to single ion/particle interaction with the storage device. Such soft errors occur when the node value or the device is disturbed sufficiently to change its switching value momentarily due to an external event, such as a particle strike. While not representing physical damage to the device, it is still quite serious as the effect can be long lasting compared to the information storage time and gate propagation delays causing an incorrect result to maintain for a relatively long period of time. This can be catastrophic as memory forms a significant portion of modern electronic systems in terms of its area as well as functionality. With the amount of charge representing the stored information dropping at successive technology nodes, the sensitivity of CMOS devices to single particle charge collection is also increasing. SEUs are now the biggest contributor to soft errors in many modern CMOS technologies [1].

Soft errors are typically measured in terms of either Soft Error Rate (SER) or Mean Time between Failure (MTBF). The SER is the rate at which soft errors occurs in a device for a given environment. When the particular environment is known then SER can be given in failure in time (FIT). In semiconductor memory, FIT is often given in FIT/Mb or in FIT/device, where one FIT represents a failure in 109 hours. MTBF defines the time between any two consecutive errors and is normally expressed in years. A MTBF of one year is approximately equivalent to 114 077 FIT.

CHAPTER 3

RADIATION HARDNESS IN FPGA DEVICES

As the general structure of FPGA devices includes regular arrays of programmable memory, logic blocks, interconnect structures, and I/O blocks, they exhibit potential vulnerabilities in all of these areas. Any upset in the configuration memory can be catastrophic as it may change the operation of the look up tables, routing, I/O, and other resources, thereby permanently changing device functionality.

Techniques used to harden an overall design against soft errors are known as mitigation techniques. There are two basic mitigation techniques available: minimizing the amount of charge that can be collected by a node at a single event and/or increasing the critical charge necessary to produce an error [2].

3.1 Scrubbing:

The technique of scrubbing [5] involves checking the memory, detecting an error, and rewriting the correct data in the right memory location. The process increases the reliability of memory within radiation environments. In practice, error detection methods require additional hardware and are mostly applied to RAM-based structures, especially SRAM. At present, three scrubbing techniques are in common use is as follows:

- Read-back with correction upon error detection;
- Internal configuration access port (ICAP) and FRAME ECC cores;
- Blind writes (also called blind scrubbing).

A “read-back” scrubber detects configuration SEUs when comparing configuration data from the FPGA with its reference, or “golden” configuration data. The scrubber will correct the configuration SEU by re-writing the reference data when

an error has been detected. Using read-back to correct SEU requires additional hardware and memory space. The read-back and comparison processes can triple the necessary amount of system memory making it untenable for many highly constrained applications.

The proprietary ICAP provides access to the configuration memory from within the FPGA core and is available only in Xilinx VIRTEX-4 and VIRTEX-5 FPGAS. This technique is also known as internal scrubbing. The Frame ECC function is performed each time a frame is read via the ICAP and the location and type of the error can be detected. A single bit error is corrected (i.e., inverted) in the frame data stored in the block RAM. The repaired frame is then written back into the configuration memory at the same frame address from which it was read. Read back resumes with the first frame of configuration memory in the configuration column containing the newly repaired frame. When a configuration column has been completely read and repaired, the SEU controller advances to the next configuration column in the array. One limitation with this technique is its inability to repair multiple bits upsets (MBUs). As a result MBUs accumulate, creating potentially serious interconnect errors. Further, the internal scrubber circuitry may cause improper function or may be stopped completely if it is hit. This method has been used in conjunction with TMR, which is also unable to detect MBUs.

Blind scrubbing is the simplest method to implement. In this case, valid configuration frame data is continuously written at a chosen interval over existing data into the device without checking whether there is an upset or not. Thus, any error resulting from a SEU will be over-written with a copy of the original data. However, the limitation with blind scrubbing is the need for the configuration logic to be continuously in “write mode.” The chosen scrubbing frequency must be based on the expected static upset rate, which may vary widely at different times and in different operating environments. The technique obviously requires additional hardware, including an external configuration memory to hold the original copy of the bit stream and an additional interface controller. These external hardware components must be protected from SEUs, using either mitigation techniques or via radiation hard design techniques.

The limitations of blind scrubbing, i.e., the need to continuously operate the configuration interface can be avoided by using partial reconfiguration (PR). This self-scrubbing technique allows a portion of the design to be reconfigured while the remaining FPGA can be performing its normal function. Partial reconfiguration can also serve to reduce FPGA circuit resources as instantiated components can be swapped in and out of the design. Thus, the same mechanism can be used to scrub configuration errors and to modify or upgrade the design at run time. One limitation of this method is that PR is not possible while scrubbing is taking place as both cannot access the configuration memory simultaneously.

3.2 Triple Modular Redundancy:

The TMR concept is often used in SRAM-based FPGAs to mitigate SEUs. TMR involves triplicating the circuit and voting to choose the correct result. Thus, the circuit has two redundant copies of the original circuit (referred to as a domain) plus the majority voter that selects the final output. A single fault in any domain will not produce an error at the output as the voter circuit will select the correct result from two other domains [1].

Although TMR is very easy to implement, it has a number of drawbacks. First, it has to be associated with some form of scrubbing as TMR will provide a faulty result in the event that two of the three domains are faulty. This situation may arise when a burst of SEUs accumulates without correction (scrubbing), eventually creating errors in multiple domains and breaking the protection offered by redundancy. Second, circuits with feedback will require voters to be inserted somewhere within a feedback loop as well in positions to restore the state of a corrupted domain. In addition, if the voter circuit itself is not protected using a radiation hard technology or some other mitigation technique, it is also prone to SEUs.

Despite the relative ease of implementation of full TMR, it involves a significant hardware overhead with two redundant copies of the circuit plus the voter circuit. Voting after each look-up table (LUT) within a design can require up to six times the area of the original circuit. In the case where full TMR is not needed, partial mitigation is an attractive alternative to reduce the extra hardware required. While partial mitigation can increase the reliability of a design at a lower cost, it is not as

reliable as full TMR. A partial mitigation should, therefore, be applied to the parts of a system that will increase the reliability the most. This reduces the area overhead with a minimum loss in reliability.

3.3 SOI Radiation Hard Technology:

CMOS SOI technology is intrinsically more radiation resistant than bulk CMOS due to the separation of its active area from the substrate by an insulating layer that can be silicon dioxide, silicon oxi-nitride, or sapphire. In this last case, the fabrication technology is called SOS [2].

SOS is a hetero-epitaxial process that consists of a thin layer (typically thinner than 0.6 μm) of silicon grown on a sapphire (Al2O3) wafer. A film of single crystalline silicon film is grown over the substrate, then etched into islands and is doped to make a bipolar or FET transistor. As the inter-device silicon is etched away in this technology, and the crystalline silicon sits on the sapphire insulator, complete electrical isolation is created between active devices, and between the devices and the substrate. Therefore, the guard rings that are normally used to limit leakage current between transistors are unnecessary. Further, there are no deep well diffusions, removing the need for the additional separation and overlap rules associated with this feature. Clearly therefore, neither well nor substrate contacts are necessary. The overall result is higher packing density of the active devices, which can be equivalent to the density gain from shrinking one full technology node.

Further, there are no parasitic transistors to cause latch up and the interconnection capacitances are greatly reduced compared to bulk CMOS. Finally, SOI supports a number of circuit techniques that are simply not possible in bulk CMOS. One such technique, an unconventional EEPROM cell has been developed for use in the commercial SOS process. Put simply, the EEPROM cell comprises a pair of cross coupled nMOS and pMOS transistor sharing a common floating gate. The floating gate can be charged positive or negative with respect to ground via the injection of either holes or electrons through the gate oxide. Unlike more traditional floating gate EEPROM cells, this SOS cell requires no special process layers and is, therefore, relatively easy to fabricate [1], [2].

CHAPTER 4

SOS EEPROM-BASED CONFIGURATION CELL

Each EEPROM memory cell contains a built in Schmitt sense amplifier that offers two useful features. First, the hysteresis of the Schmitt increases its Qcrit, reducing the likelihood that a particle strike will result in a transient error. Second, a strike on the EEPROM that causes its value to decay to zero will increase the static current of the Schmitt by up to five orders of magnitude, which is very easily detectable using conventional methods [1], [2].

4.1 Silicon on Sapphire EEPROM:

The basic organization of the silicon-on sapphire EEPROM cell, shown in Fig 4.1, comprises two crossed intrinsic P and N transistors which share a common channel that forms a small ‘island’ of intrinsic (un-doped) silicon [1], [2].

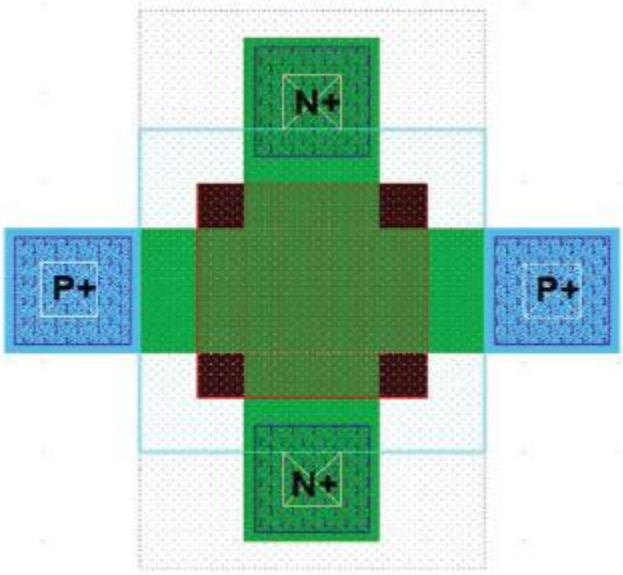

Fig 4.1: Basic Silicon-on-Sapphire EEPROM Cell

As both transistor types are available, charge of either polarity can be injected from the channel through the gate oxide and onto the floating gate and, since both the substrate and body are floating, a cell can be both written and erased with positive voltages. The gate is charged (negatively) using avalanche injection of hot electrons from the P-channel device, whereas injecting holes via the N-channel erases the cell. As a result, there can be no over-erasure problem and it impossible for any decay in the cell charge resulting either from conventional oxide leakage or from a charged particle strike to completely flip the logic value (Fig. 4.2).

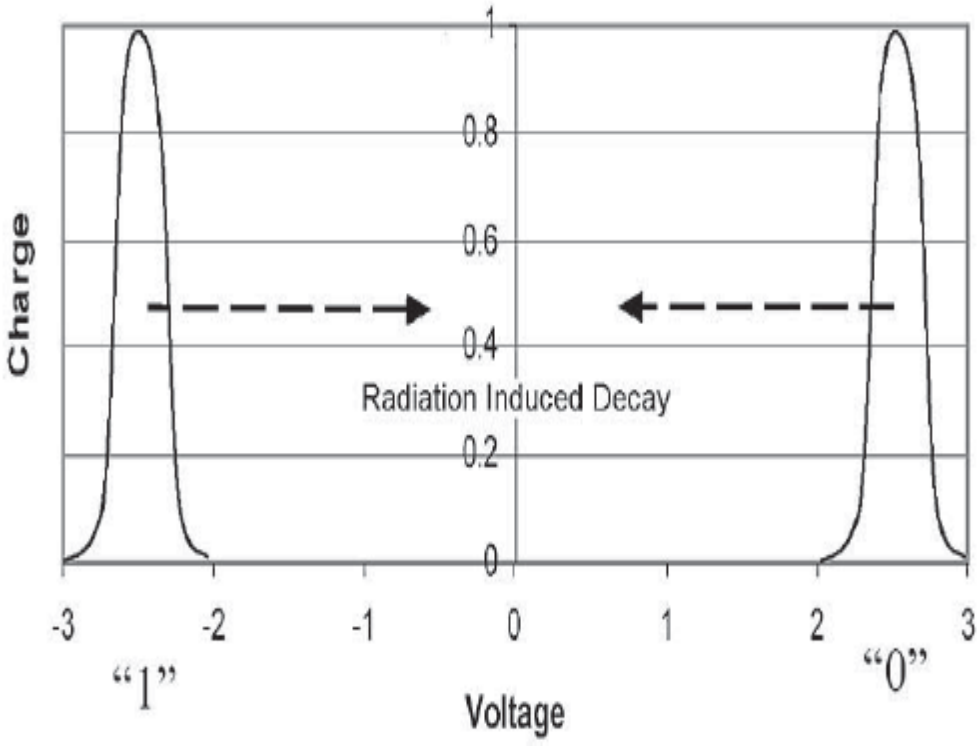

Fig 4.2: EEPROM charge storage characteristics.

This also represents a key difference between the operation of these SOI cells and conventional EEPROM or Flash. Rather than just the presence or absence of charge on the gate indicating the programmed logic value, in the case of the SOI cell both logic levels are established by specifically charging the floating gate to an appropriate level. Constant current programming is most often employed here as it improves the cell endurance.

4.2 SOS EEPROM-Based Configuration Cell:

In a typical configuration, the floating EEPROM gate is integrated with a simple inverter structure that forms a built-in sense amplifier. The configuration cell extends this basic idea by using a Schmitt sense amplifier with thresholds set at ±VDD/2 (Fig. 4.3), thus providing complete immunity from configuration errors.

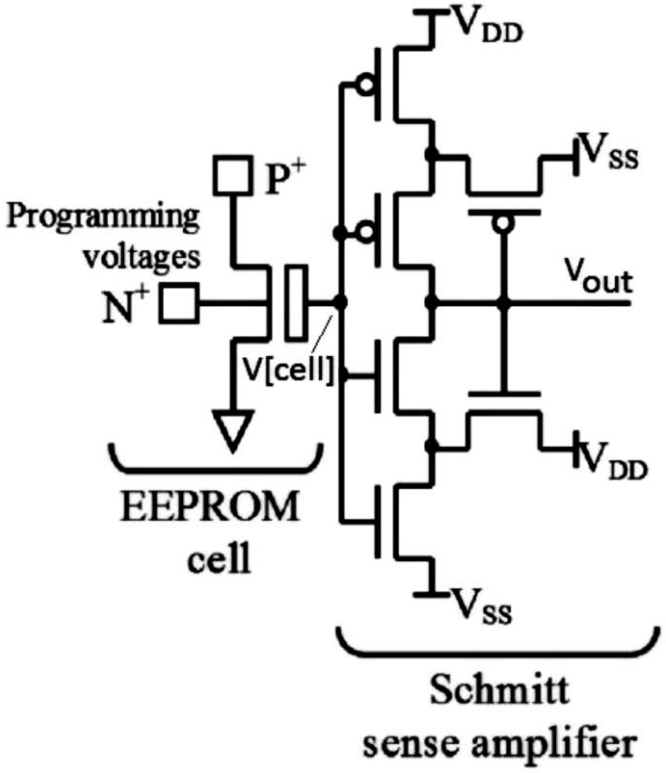

Fig. 4.3: EEPROM Cell with Schmitt Sense Amplifier

The Schmitt sense amplifier offers two main advantages. First, while a particle strike on the interface may result in a transient upset, there is no direct mechanism by which the logic value of the configuration memory cell can be permanently flipped. In the event that a strike is sufficient to bring the charge (and therefore the voltage) of the EEPROM cell down to zero, the hysteresis of the Schmitt will ensure the correct output logic value is still maintained (Fig. 4.4). The use of a Schmitt sense amplifier circuit has the further benefit of increasing the critical charge (QCRIT), i.e. the minimum charge resulting from a particle strike at which the sense circuit will be disturbed.

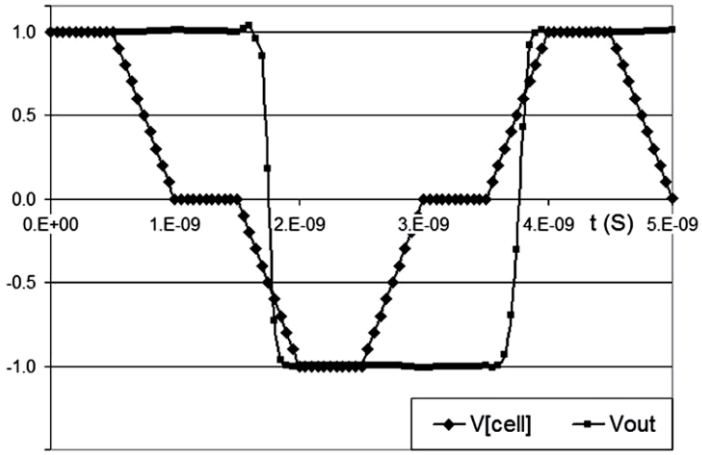

Fig. 4.4: DC characteristics of the configuration cell

Even if the gate charge reduces completely to zero, the Schmitt threshold ensures that the correct output is maintained. It can be seen that switching can only occur when the floating gate voltage reaches V+ or V- (depending on the direction of charge/discharge), something that cannot actually occur in the memory cell [2].

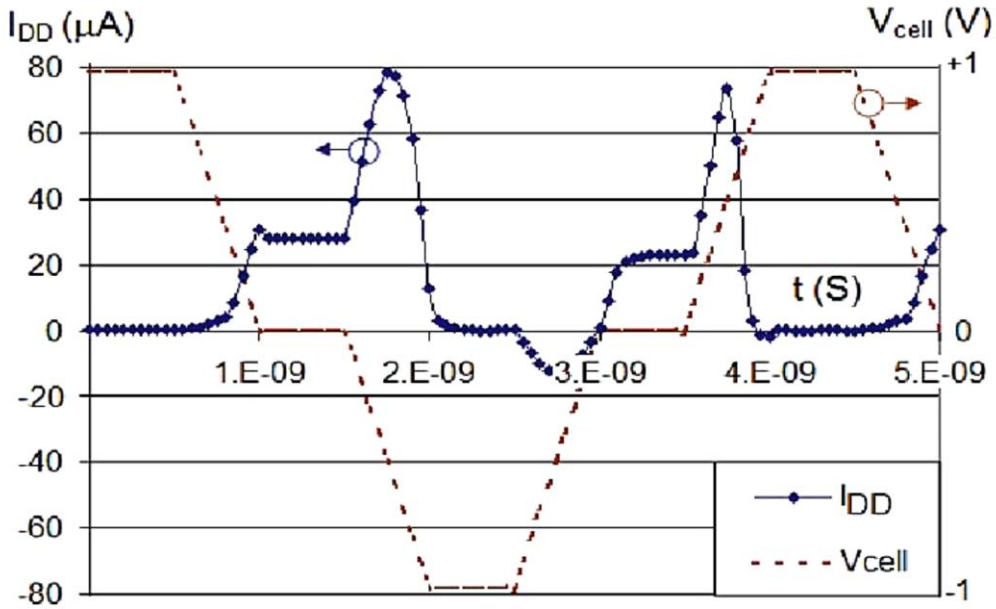

Fig. 4.5: Sense Amplifier Static Current Behaviour

Fig. 4.5 shows the simulated static (DC) current vs. cell voltage for the Schmitt circuit. High threshold transistors ($V_{TH} \approx \pm 0.7$ V) were used throughout that resulted in very small static current values in normal operation, in the pA range when

$|V_{CELL}| > 0.7$ V. It can be seen that the static current increases $3x10^6\times$ from <10 pA to more than 28 μA at V*cell*=0. This behaviour offers an opportunity to easily detect the occurrence of an upset event in the memory cell. Any partial charge/discharge due to a particle strike will be reflected in a significant increase in the static current drain of the sense amplifier. For example, even at a partially discharged cell voltage of 0.5V, the static current has increased well over $10^3\times$, which are easily detectable using standard techniques [1].

Fig. 4.6 shows a trial layout for the memory cell using models for a commercial SOS process supplied by the foundry.

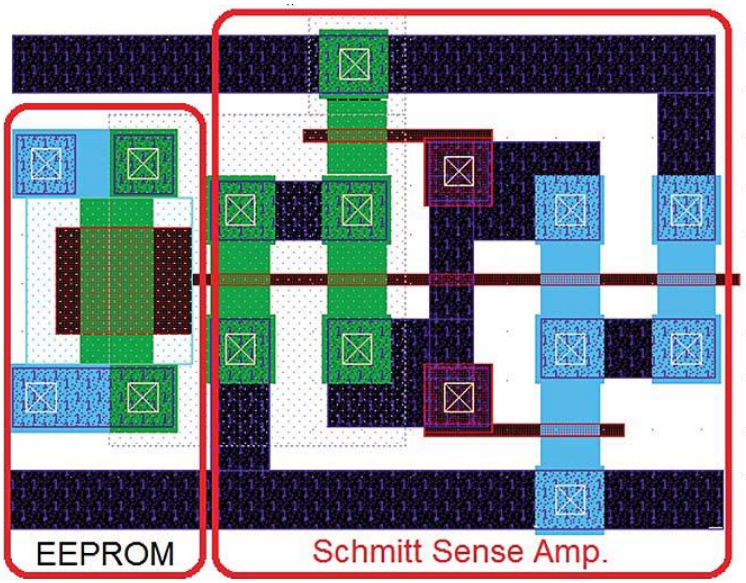

Fig 4.6: Layout of EEPROM cell with Schmitt sense amplifier.

Here, the SOS EEPROM layout has been folded in a way to match the height of the sense amplifier. It can be seen that the memory circuit is larger than a conventional EEPROM. The area of the Schmitt is similar to that of a standard 6T SRAM in the same technology while the PlusCell adds approximately the area of two additional transistors. The result is a memory cell that is similar in size to radiation tolerant SRAMs, but smaller than recent radiation tolerant SRAM circuits that may comprise as many as 11 transistors. In terms of both area and power, the design compares favourably with conventional mitigation techniques, such as TMR or scrubbing that require complex additional hardware. In addition, the system is both reprogrammable and non-volatile. Fig also shows how the lack of both well and substrate contacts in SOS can result in very compact circuit layouts.

4.3 Current Sensing Mechanism:

The scrubbing process is triggered by the large ($> 10^3\times$) increase in current that arises in the Schmitt when the SOS EEPROM cell suffers an upset event that moves its floating gate voltage toward zero. A conventional cross-coupled current sensor can be set up to compare the supply current with a reference current that may be set at design time according to the number of blocks covered and their expected static current. The large difference between the currents to be sensed means that an error in either a single cell or a large group of blocks could still is readily detected, even allowing for a wide spread in individual static current values, as might be caused by manufacturing variability [1], [2].

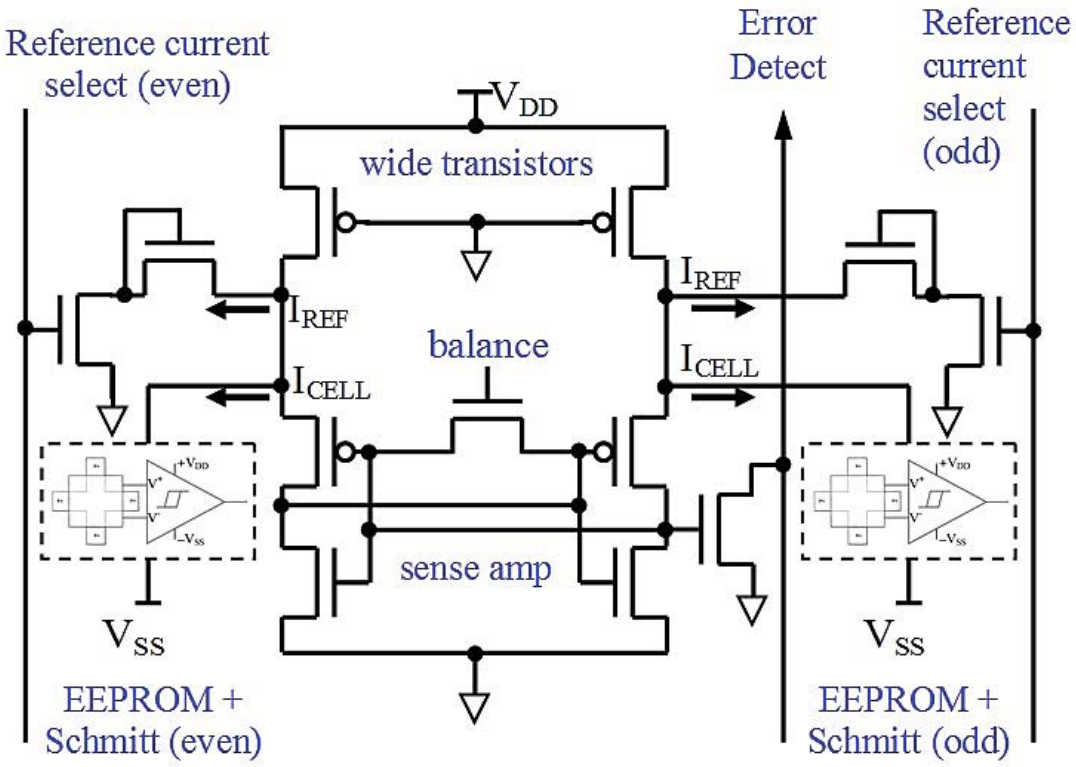

Fig 4.7: Current detection for odd and even memory bank.

A conventional cross-coupled current sense of the type shown in Fig. 4.7 can be used to compare the composite supply current with a reference that is set at design time by the number of blocks and their expected static current. The large difference between the currents to be sensed means that an error in a single cell in a group of more than 10^5 blocks could still is readily detected, even allowing for a wide spread in

individual static current values, as might be caused by manufacturing variability. In this case, a pair of configuration cells shares a single current detection circuit that allows it to be merged into the configuration cell layout. This type of conventional cross-coupled inverter organization is common to SRAM or similar circuits. While this organization limits the average time between a failure onset and its detection within the scrubbing system, it probably represents a worse case in terms of its area overhead. In the example layout, it can be seen that the single current detection circuit that is shared between two adjacent EEPROM/Schmitt cells more than doubles the area of the composite circuit. However, the area overhead still compares favourably with TMR, which would require three copies of the EEPROM/Schmitt block plus a voter circuit, and with read-back scrubbing which requires external memory and control hardware.

The current sensing operates in a simple sequence of steps that can be derived from a small state machine controller of the sort shown in Fig 4.8.

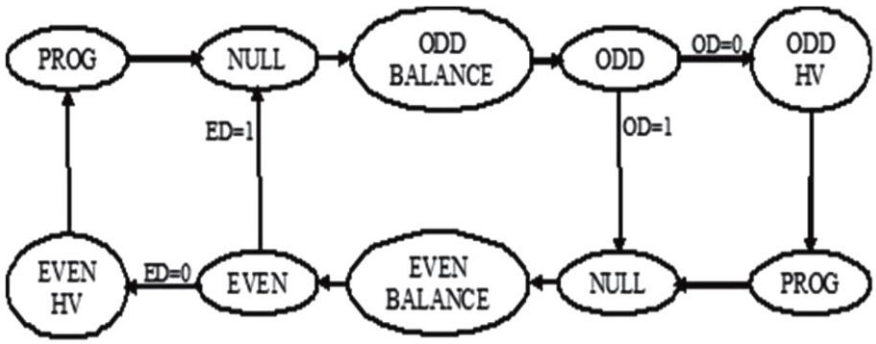

Fig. 4.8: scrubbing state machine diagram.

In the first state, the balance signal (BALANCE) drives the sense amplifier into its metastable region while a reference current for either the ODD or EVEN bank is enabled. The corresponding error detect line is also pre-charged. In the next state, the balance signal is deactivated and the sense amplifier allowed relaxing to one of its stable states, depending on the relationship between the reference and memory cell currents. The detect line from the current sense is used to trigger a reconfiguration event within a column of memory cells. In particular, the current detection might be used to start a read back and comparison process to detect and correct the specific

faulty cell. Equally, blind scrubbing could be used, either on all cells in an individual column or on the entire memory.

In case of an event in the odd or even bank, the programming sequence is entered, otherwise the state machine simply moves on to check the next odd/even mode.

CHAPTER 5

AUTO-SCRUBBING BEHAVIOUR

The Auto-Scrubbing [1] behaviour allows individual configuration memory cells to be monitored and scrubbed when a SEU is detected. This behaviour is called auto-scrubbing. Although the SOI EEPROM and the Schmitt exhibit high intrinsic resistance to radiation-induced errors, it is still possible for a sequence of two particle strikes to permanently upset the configuration value.

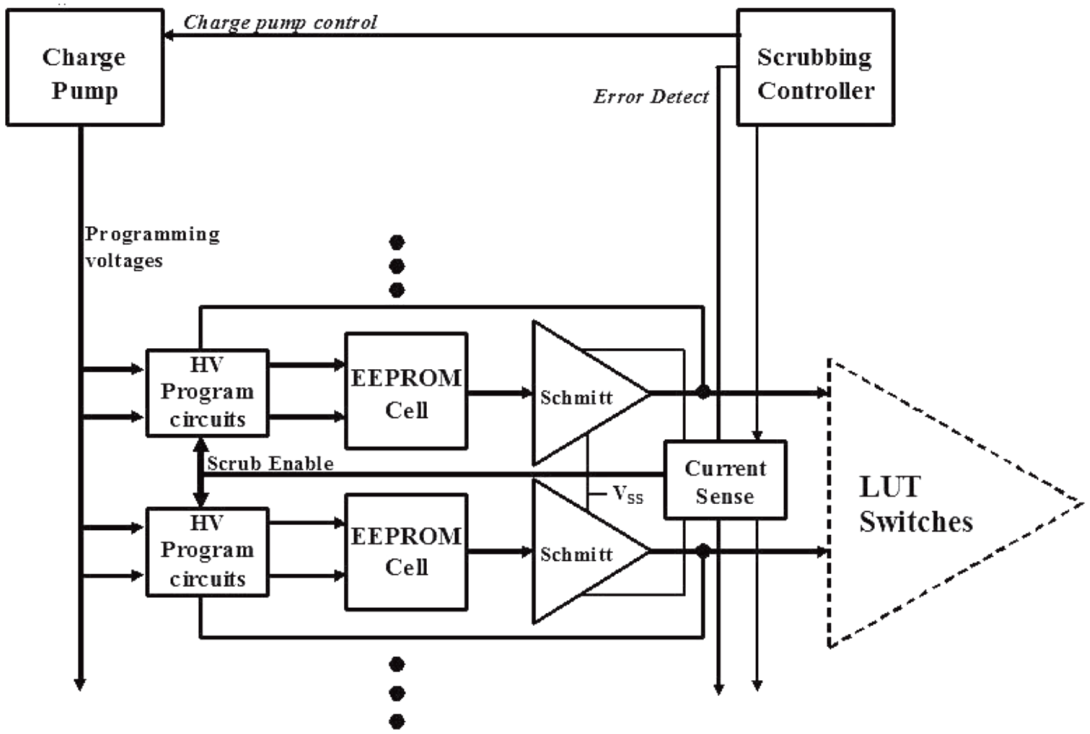

Fig 5.1: Auto-scrubbing system configuration.

The basic auto-scrubbing concept is illustrated in Fig. 5.1. To write values into the memory, the high voltage (HV) programming circuits are activated by enabling a charge pump. Keeping it disabled until required saves power and greatly reduces the

likelihood that the charge pump itself will be degraded or damaged by repeated particle strikes. Any reduction in the EEPROM cell voltage can be detected by comparing the supply current of its sense amplifier against a reference that is set somewhere between the normal operating supply current (<10 nA) and that induced by an error (>10 μA). A reprogramming sequence is then initiated on the compromised cell using the value from the Schmitt as its reference.

The worse-case effect of a particle strike on the EEPROM cell will be a reduction in its stored charge, possibly to zero but never to the opposite charge. As long as the cell voltage (V_{CELL}) is outside the band: $V- \leq V_{CELL} \leq V+$, then the Schmitt behaves as a purely combinatorial circuit. A strike on one of its internal nodes will cause only a transient error and the output will return to correct value following the event. Thus, under these circumstances, the output value of the Schmitt represents a stable reference that can be used to reinstate the EEPROM value, removing the need to store it externally. However, when V_{CELL} is inside that range, the partial feedback that produces the hysteresis effect results in state behaviour and a radiation event can flip the sense amplifier to its opposite state, losing the configuration value. A sequence of two events is required. The first would “deprogram” the EEPROM, reducing VCELL to within the critical band followed closely (i.e., within the re-configuration time) by a second event that flips the sense amplifier.

5.1 Soft Error Analysis:

SOI technology is intrinsically more resistant to radiation events, at least in part due to its smaller collection depth resulting from the underlying insulating substrate. The silicon thickness (around 110 nm in the UltraCMOS process) defines the lower limit of the collection volume [1].

To gain an approximate understanding of the effect of simultaneous particle strikes on the combined EEPROM/Schmitt circuit, the generalized MTBF model of Fig. can be used. In this paper, a particle strike on the EEPROM represents the onset of the failure state for an individual cell. At this point, there will be a period of time before the detection of the error that is determined by the clock period of the state machine controlling the current detection circuit. This is the mean time to detection (MTTD). Once the error condition is detected, there will be a further period of time to

repair the error, the mean time to repair (MTTR), which will include the worst case time to activate the charge pump circuit, followed by the cell programming time.

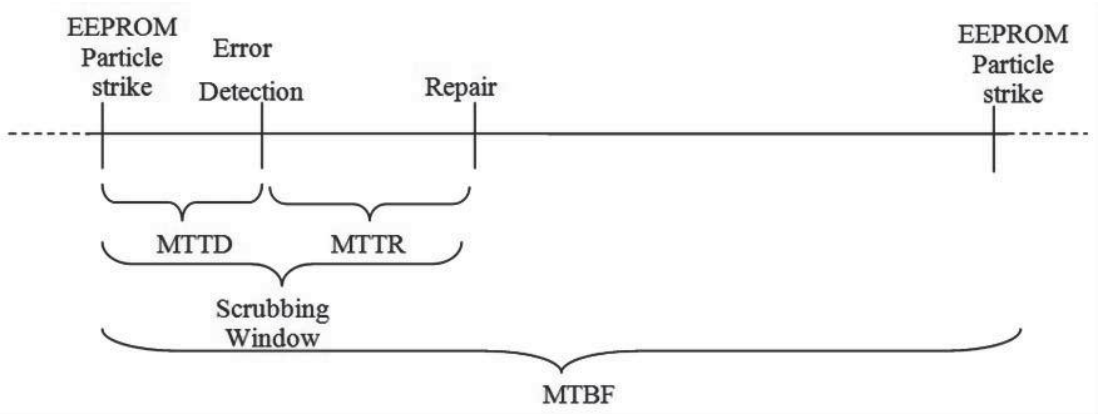

Fig 5.2: MTBF Failure Mode

In the standard model, the time MTTD + MTTR defines the availability of the system, i.e., the proportion of the time it is functioning correctly, given by

$$\text{Availability} = \frac{\text{MTBF} - (\text{MTTD} + \text{MTTR})}{\text{MTBF}}.$$

In our case, the time (MTTD + MTTR) represents a scrubbing window within which the configuration memory is vulnerable to a second strike on the Schmitt. A permanent, non-correctable failure in the memory block will require two failure events in the correct order (EEPROM then Schmitt) and for the second event to occur within the scrubbing window.

The most pessimistic value of SER, therefore, assumes that the two events on the EEPROM and Schmitt are exactly coincident (e.g., as a result of a dense burst of radiation) and using a simple statistical analysis, the SER of the entire cell will be the multiplication of the individual SER values for the two. This results in a value in the order of 3.7×10^{-29}, equivalent to a MTBF of 1034 years for a single memory cell.

CHAPTER 6

CONCLUTION

The seminar describes a method of building radiation hardened field programmable gate array components based on silicon-on-sapphire technology, a subclass of SOI technology in which sapphire is used as the insulator. SOS technology was applied here due to its inherent radiation tolerance and because of the unique circuit opportunities it offers.

The programmable, non-volatile silicon-on-sapphire based EEPROM that forms the basis of this paper can be manufactured using a standard single Polysilicon process with no special layers. This organization is only possible because of the lack of reverse-biased P-N junction from the transistor active regions to the substrate. Further, as the cell operates by charging its single floating gate to positive or negative potentials, using hot-electron or hot-hole avalanche injection through the gate oxide, it is not possible for a radiation induced event to permanently flip the EEPROM state as this would require the floating gate charge to be completely discharged to zero, then reversed.

In the configuration memory proposed here, a Schmitt sense amplifier was attached to each EEPROM, which not only enhances the radiation resistance of the overall cell but also works to maintain the logic value of the cell in the face of any event that causes a partial de-programming of the EEPROM and therefore a reduction in the magnitude of its effective storage voltage. On such events, the thresholds of the Schmitt act to maintain the correct logic value on to the output. Any reduction in the magnitude of the cell voltage will cause a large increase in the static current of the cell. Such a large increase in current was easily detected using a conventional sense amplifier and this simple property can be used to set the cell set up to be self-correcting, exhibiting so-called “auto scrubbing” behaviour.

While the memory is resistant to permanent changes from isolated particle strikes, it is still possible for a sequence of two events to permanently upset the configuration value. An error will occur only when two particles with charge above the critical charge hit the EEPROM and the Schmitt within the same write window (i.e., the scrubbing window).

REFERENCES

[1] K. Haque and P. Beckett, "Radiation-Hard Field-Programmable Gate Arrays Configuration Technique Using Silicon on Sapphire," in *IEEE transactions on VLSI systems*, vol. 22, no. 2, february 2014, pp. 232–241

[2] K. Haque and P. Beckett, "A SOI EEPROM based configuration cell with simple scrubbing detection," in *Proc. 24th Int. Conf. VLSI Design*, Jan. 2011, pp. 24–29

[3] H. L. Hughes and J. M. Benedetto, "Radiation effects and hardening of MOS technology: Aevices and circuits," IEEE Trans. Nucl. Sci., vol. 50, no. 3, pp. 500–521, Jun. 2003.

[4] F. L. Kastensmidt, L. Carro, and R. Reis, "Fault-Tolerance Techniques for SRAM-Based FPGAs", *(Frontiers in Electronic Testing)*, vol. 32. New York, USA: Springer-Verlag, 2006.

[5] A. M. Saleh, J. J. Serrano, and J. H. Patel, "Reliability of scrubbing recovery-techniques for memory systems," *IEEE Trans. Rel*., vol. 39, no. 1, pp. 114–122, Apr. 1990.