# STUDY OF RADIATION EFFECTS IN SRAM-BASED FPGAs for NPP I&C SYSTEM DESIGN

*By*

**NIDHIN T. S**

**ENGG02201304014**

**INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH, KALPAKKAM**

*A thesis submitted to the*

*Board of Studies in Engineering Sciences*

*In partial fulfillment of requirements*

*for the Degree of*

**DOCTOR OF PHILOSOPHY**

*of*

**HOMI BHABHA NATIONAL INSTITUTE**

**NOVEMBER, 2020**

# Homi Bhabha National Institute

## Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by **Nidhin T. S** entitled "**Study of Radiation Effects in SRAM-based FPGAs for NPP I&C System Design**" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

| | | |
|---|---|---|
| Chairman : | **Dr. B. P. C. Rao** | Date: 02/11/2020 |
| Guide / Convener : | **Dr. K. Velusamy** | Date: 2.11.2020 |
| Examiner : | **Prof. Anindya Sundar Dhar** | Date: |
| Member 1 : | **Dr. K. Devan** | Date: 2/11/2020 |
| Member 2 : | **Dr. T.S. Lakshmi Narasimhan** | Date: 02/04/20 |
| Member 3 : | **Prof. Rupesh Nasre** | Date: *Nov. 02, 2020* |
| Technology Advisor : | **Smt. T. Jayanthi** | Date: 2/11/2020 |

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I/We hereby certify that I/we have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

**Date:** 02/11/2020
**Place:** Indira Gandhi Centre for Atomic Research, Kalpakkam

02/11/2020
**Dr. K. Velusamy**
**(Guide)**

# STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

**Date:** 02/11/2020

**Place: Kalpakkam**

**(NIDHIN T. S)**

# DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

**Date:** 02/11/2020

**Place: Kalpakkam**

**(NIDHIN T. S)**

# List of Publications arising from the thesis

Publications in Refereed Journals:

1. **T. S. Nidhin**, Anindya Bhattacharyya, Aditya Gour, R. P. Behera, T. Jayanthi, K. Velusamy, "Measurement of radiation absorbed dose effects in SRAM based FPGAs", **IETE Journal of Research, Taylor and Francis**, DOI: 10.1080/03772063.2020.1768159, May 2020.

2. **T. S. Nidhin,** Anindya Bhattacharyya, R.P. Behera, T. Jayanthi, K. Velusamy "Understanding radiation effects in SRAM-based field programmable gate arrays for implementing instrumentation and control systems of nuclear power plants" **Nuclear Engineering and Technology (NET), Elsevier**, Vol. 49, No. 8 (December 2017) pp. 1589-1599.

3. **T. S. Nidhin,** Anindya Bhattacharyya, R. P. Behera, and T. Jayanthi," A Review on SEU Mitigation Techniques for FPGA Configuration Memory", **IETE Technical Review**, doi:10.1080/02564602.2016.1265905, Jan. 2017.

Other Publications:

a. Conference/Symposium

1. T. S. Nidhin, Anindya Bhattacharyya, R. P. Behera, T. Jayanthi, K. Velusamy, "Dependable System Design with Soft Error Mitigation Techniques in SRAM Based FPGAs," IEEE International Conference on Innovations in Power and Advanced Computing Technologies", i-PACT-2017, VIT University, Vellore, April 21-22, 2017. DOI: 10.1109/IPACT.2017.8244907

2. T. S. Nidhin, Anindya Bhattacharyya, R. P. Behera, T. Jayanthi, K. Velusamy," SEU Mitigation by Golay Code in the Configuration Memory of SRAM based FPGAs", IEEE International Conf. ICCICCT-16, Dec. 16-17, 2016, pages 49-53, DOI: 10.1109/ICCICCT.2016.7987918 (received best paper award).

3. T. S. Nidhin, Anindya Bhattacharyya, R. P. Behera, T. Jayanthi, K. Velusamy," Verification of Fault Tolerant Techniques in Finite State Machines using Simulation Based Fault Injection Targeted at FPGAs for SEU Mitigation", IEEE International conference on electronics and communication systems (ICECS), 24-25 Feb. 2017, pp.153-157, Coimbatore, India, DOI: 10.1109/ECS.2017.8067859

4. R. P. Behera, T. S. Nidhin, M. Sakthivel, T. Jayanthi, K. Madhusoodanan "Total Ionizing Dose Effects in GaAs-Si Based Electronic Components", IEEE International Conference on Innovations in Power and Advanced Computing Technologies", i-PACT-2017, VIT University, Vellore, April 21-22, 2017, DOI: 10.1109/IPACT.2017.8245063.

5. T. S. Nidhin, Anindya Bhattacharyya, R. P. Behera, T. Jayanthi, K. Velusamy, "Study of Radiation Effects in SRAM based FPGAs for Safety Critical System Design", RSM-MSENM 2018, IGCAR, Kalpakkam, May 7-9, 2018.

6. T. S. Nidhin, Anindya Bhattacharyya, Aditya Gour, R. P. Behera, T. Jayanthi, "Study of Total Ionization Dose Effects in Electronic Devices", IARPIC'18, BARC, Mumbai, Jan 16-20, 2018.

02/11/2020

**(NIDHIN T. S)**

**"TO MY PARENTS"**

# ACKNOWLEDGEMENTS


- To my guide Dr. K. Velusamy (Associate Director, NSAG, Indira Gandhi Centre for Atomic Research (Retd.)) for being my source of guidance.
- To my other doctoral committee members: Dr. B. P. C. Rao, Dr. K. Devan, Dr. T. S. Lakshmi Narasimhan and Dr. Rupesh Nasre for their guidance and mentoring.
- To Smt. T. Jayanthi (Director, EIG, IGCAR) for being my supportive technology advisor.
- To Shri. R. P. Behera (Head, RTSD/EIG, IGCAR) for all the encouragement, discussions and assistance.
- To Shri. Anindya Bhattacharyya (Scientific Officer/E, RTSD/EIG, IGCAR) for being my collaborator. I am lucky to have worked with him, and I cannot thank him enough for his valuable suggestions and reviews.
- To Mr. Aditya Gour for his valuable suggestions especially in the hardware debugging part, Prashant Sharma for being my support in all good and bad moments in the lab. Also, to K. Sujith, M. Chandramouli Sharma, and Mahesh Patankar for being good lab mates.
- To Dr. Arun Kumar Bhaduri, Director, IGCAR and Dr. S. A. V. Satya Murty and Dr. P. R. Vasudeva Rao, former Directors, IGCAR for providing an excellent environment to carry out research work.
- To former EIG Directors Dr. B. K. Panigrahi and Shri K. Madhusoodanan, for their motivation and support.
- To the reviewers and editors of journals, and conferences for reviewing my work.
- To Shri N. Murali, former Associate Director, ICG, EIRSG.
- To Shri. M. Sakthivel, and all Engineers and staff at EIG for all their encouragement and help.

- To Mr. K. Praveen, EIG for all the suggestions and encouragement.
- To Dr. Puspalata Rajesh, WSCD, BARC facilities and Mr. H. Krishnan, RSD, IGCAR for their support during the experiments at Gamma Chamber-5000
- Special thanks to Dr. Sunil Kumar, RDG for his support for modelling of shielding.
- To my dear friend Dr. Shivang Tripathi for his selfless support.
- To my dear friends: Dr. Vikas Kumar Jha, Dr. Manoj Kumar Parida, Dr. Chandan Kumar Bhagat and Dr. Sumathi Gopi for all the good moments we had and the encouragement and the positive energy you showered on me.
- To all my cricket team members, both inter-lab and enclave cricket league for all the fun times we had.
- To the administrative staff of HBNI/IGCAR for timely assistance.
- To the Department of Atomic Energy (DAE) for providing me with the research fellowship.
- To my dear parents, brother and other family members for just being there for me in all up and downs.
- To my soulmate Dr. Meghana for her love and patience during my struggling period.

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF EQUATIONS

# LIST OF ACRONYMS

| | |
|---|---|
| AMUSE | Autonomous Multilevel emulation-based fault injection for Soft Error Evaluation |
| ASIC | Application Specific Integrated Circuits |
| ASRAM | Asymmetric Static Random Access Memory |
| BJT | Bipolar Junction Transistor |
| BRAM | Block Random Access Memory |
| BWR | Boiling Water Reactor |
| CMOS | Complementary Metal-Oxide Semiconductor |
| COTS | Commercial Off-The-Shelf |
| CPLD | Complex Programmable Logic Devices |
| CRC | Cyclic Redundancy Check |
| CTR | Current Transfer Ratio |
| DDD | Displacement Damage Dose |
| DIP | Dual In-line Package |
| DORT | Discrete Ordinates Transport Code |
| DSO | Digital Storage Oscilloscope |
| DUT | Device Under Test |
| DWC | Duplication With Compare |
| ECC | Error Correction Codes |
| ECR | Error Correction with Remap |
| EDR | Error Detection with Remap |
| FF | Flip-flop |
| FIT | Failure In Time |

| | |
|---|---|
| FPGA | Field Programmable Gate Array |
| FSM | Finite State Machine |
| GA | Genetic Algorithm |
| GF | Galois Field |
| HCS | Heterogeneous CRAM Scrubbing |
| HPD | Hardware Description Language Programmed Devices |
| I&C | Instrumentation and Control |
| IAEA | International Atomic Energy Agency |
| ICAP | Internal Configuration Access Port |
| IPD | In-Place Decomposition |
| IPF | In-Place X-filling |
| IPR | In-Place Reconfiguration |
| JTAG | Joint Test Action Group |
| LED | Light Emitting Diodes |
| LET | Linear Energy Transfer |
| LUT | Lookup Tables |
| MBU | Multiple Bit Upset |
| MOSFET | Metal-Oxide-Semiconductor Field-Effect Transistor |
| MTBFF | Mean Time Between Functional Failures |
| NETFI | NETlist Fault Injection |
| NMOS | N-type Metal-Oxide-Semiconductor |
| NPP | Nuclear Power Plant |
| PFBR | Prototype Fast Breeder Reactor |
| PLC | Programmable Logic Controller |
| PMOS | P-type Metal-Oxide-Semiconductor |

| | |
|---|---|
| PMT | Photomultiplier Tube |
| PR | Partial Reconfiguration |
| PSO | Particle Swarm Optimisation |
| PWR | Pressurized Water Reactor |
| RCB | Reactor Containment Building |
| RHBD | Radiation Hardened By Design |
| RoRA | Reliability-Oriented Place and Route Algorithm |
| RTC | Real Time Computer |
| RTL | Register Transfer Level |
| SA | Severe Accident |
| SC | Safety Critical |
| SEE | Single Event Effects |
| SEFI | Single Event Functional Interrupt |
| SEL | Single Event Latchup |
| SET | Single Event Transients |
| SEU | Single Event Upset |
| SR | Safety Related |
| SRAM | Static Random Access Memory |
| TCL | Tool Command Language |
| TID | Total Ionization Dose |
| TL | Thermo-luminescence |
| TLD | Thermoluminescent Dosimeters |
| TMR | Triple Modular Redundancy |
| VERIFY | VHDL-based Evaluation of Reliability by Injecting Faults efficiently |
| VHDL | VHSIC Hardware Description Language |

# 6

# CONCLUSIONS AND SCOPE FOR FUTURE WORK

*The present chapter summarizes the conclusions derived from various research activities carried out in the study of radiation effects in SRAM based FPGAs for the design of nuclear power plant instrumentation and control systems. It also provides the scope for future work in this area.*

## 6.1. SUMMARY OF THE THESIS

The aim of the present dissertation was to study the radiation effects in SRAM based FPGAs targeted for NPP I & C system design. As there is no history of data available for commercial grade SRAM based FPGAs used in nuclear applications this study has its significant importance. From the literature it is found that TID effects and SEUs are the common cause of failures in the systems implemented using SRAM based FPGAs and deployed in a radiation environment. It is also found that during various operating conditions of the reactor, gamma rays are the major sources of radiation in the reactor environment. So, this study has given focus to cumulative absorbed dose effects due to gamma radiation. As gamma radiation can cause TID effects as well as SEUs in the MOS based devices, an experimental study has been conducted to measure the tolerance level of the system in such an environment. As there is a possibility of SEUs in the system either due to gamma or due to other reasons, a detailed investigation has been conducted on SEU mitigation techniques. By

controlling the SEUs and delaying the cumulative effects, the time duration for which the device can perform its intended function can be extended. Keeping these targets, the objectives of the research were set and the achieved results are summarized.

1) A detailed investigation in to various SEU mitigation techniques has been carried out and their efficiencies are quantified based on area overhead, complexity of implementation to assist designers/researchers to choose the appropriate technique based on specific requirement. Further a hybrid hardware/software scrubber with selective hardening either by giving frame level redundancy or implementing improved error correction codes for sensitive frames, is proposed.

2) An error recovery mechanism based on extended Golay code is proposed to detect up to four errors and to correct up to three errors in a block of 24 bits. This can improve the period between partial reconfigurations required to keep the system soft error free.

3) An efficient fault injection technique has been developed for easy implementation to support automatic detection of sensitive nodes and fault injection at RTL and netlist levels.

4) Based on controlled irradiation experiments employing Gamma chamber -5000, it is found that the device under test, Spartan 6 FPGA, can withstand upto 322 krad of accumulated dose without any functional failure. This form an input data for deciding the shielding essential to protect SRAM based FPGAs functioning in radiation environment of nuclear reactor.

5) In an environment where the neutron energy is less than 10 MeV, the device under test can efficiently work with error correction codes with selective redundancy. However, in environments having neutron energies higher than 10 MeV, partial reconfiguration or periodic scrubbing is required.

6) The possible reduction in dose rate experienced by the device under test, Spartan 6 FPGA, by providing stainless steel shielding has been measured in the gamma-chamber 5000. The measurements have also been validated by computational modelling using a two-dimensional transport code DORT and IGC-S3 cross-section set. It is found that the duration of functional time can be extended almost two times by appropriate shielding.

## 6.2. SCOPE FOR FUTURE WORK

The findings of the present experiments/analysis can be implemented in the safety Core Temperature Monitoring System (CTMS). It is classified as safety-critical system and has two main failure modes: (i) failure to initiate SCRAM signal when parameters exceed their threshold values; which places demand on the hardware based CTMS and other diversified shutdown systems, (ii) generation of spurious SCRAM signals, which affects the plant availability. The implementation of CTMS in SRAM based FPGA provides diversity in the existing RTC based triple modular system. As per the present experimental results, the system can be deployed inside the RCB, so multiple penetrations in the RCB can also be avoided. Golay code-based error recovery mechanism and other fault tolerant techniques discussed in the thesis can be implemented to provide additional tolerance. Also, a detailed study on hardware accelerator combined with dynamic partial reconfiguration for isolating the affected

area and reconfigure the affected functional block in the non-affected area can be performed. A diversified Hardware CTMS combining all the three constituent systems of CTMS together augmenting it with radiation tolerant features can be developed which can be located inside the reactor containment building.

# ABSTRACT

SRAM based Field Programmable Gate Arrays (FPGA) can provide the most advanced technology solutions for the applications in the instrumentation and control systems (I&C) of nuclear power plant (NPP). Traditionally, NPP system designers adopt proven and reliable technologies rather than using the latest technologies. Even though SRAM based FPGAs are not used in nuclear applications, it is a well-known technology in other critical applications such as aerospace, medical, automotive, etc. As the International Atomic Energy Agency (IAEA) recommends the use of FPGAs in future and existing nuclear I&C systems the advanced features of SRAM-based FPGAs make it a better choice. Even though SRAM based FPGAs have numerous advantages, they are vulnerable to radiation effects either due to transient or cumulative radiation exposure. Therefore, a comprehensive study of radiation effects in SRAM based FPGAs is needed before its implementation in the I&C system of the NPPs. The present research work would further aid in improving the reliability of the designs implemented in FPGAs.

In this research work, we are considering the application in the I&C systems of sodium-cooled fast breeder reactors. At present most of the I&C systems are not being installed in the radiation environment. Even though the radiation level in the active areas of the sodium-pooled fast reactors such as the Reactor Containment Building (RCB), fuel building, steam generator building and radiation waste building (RWB) is maintained at 25 μSv/h, I&C systems are not deployed in such areas expecting the radioactivity increase due to the scenarios like fuel pin failures in the core and other anomalies. As most of the I&C systems are kept outside the RCB there is a need for multiple penetration assemblies and which in turn reduces the integrity of

the RCB. Also, the current I&C systems are real-time computer-based systems implemented with triple modular redundancy technique, so common cause failures are probable. Hence, it is required to develop diversified hardware based I&C system with radiation tolerant features to be kept inside the RCB. SRAM based FPGAs makes a better choice for this requirement.

It is found that gamma radiation is the major source of radioactivity in the reactor environment, so this study has given focus on radiation effects due to gamma radiation. Even though the presence of neutron which can cause upsets in electronic devices is negligible in such areas, to ensure the reliability of the system, this study has given importance to the upset mitigation techniques. TID effects and SEUs are the common cause of failures in the systems implemented using SRAM based FPGAs and deployed in a radiation environment. The objectives of the thesis are set based on the intensive literature review. The research objectives mainly have two divisions, the first one is the study and analysis of SEU mitigation techniques in the configuration memory of SRAM based FPGAs. Secondly the Measurement of TID tolerance level of SRAM based FPGAs by irradiation experiments

The first one discusses the mitigation techniques for SEUs in the configuration memory of SRAM-based FPGAs as the configuration memory is highly susceptible to SEUs. Various reconfiguration methods are studied; mainly, the partial reconfiguration with error correction codes and scrubbing. It also covers the algorithmic and architectural changes which prevent or mitigate SEUs in the configuration memory bits dedicated for routing resources and logic resources. The major techniques are compared and quantified for their efficiencies, based on their SEU mitigation capabilities, area overheads, and delays. From the analysis, it is

proposed that the error correction codes which are presently used in the communication channels can be utilized for error mitigation in the configuration memory. An error recovery mechanism based on extended Golay code (24, 12, 8) with a minimum distance of 8, which can detect a maximum of 4 errors and can correct up to 3 errors has been designed. This chapter also discusses the development of a simple tool command language (TCL) script-based automated fault injection methodology built around the target simulator which can take designs in both RTL and netlist level of abstractions. The proposed methodology parses a design in a guided or automated manner selecting sensitive nodes where the fault is to be injected and generating a TCL script for the same. By using the developed fault injection method, analysis of the efficiency of error mitigation techniques like triple modular redundancy (TMR) and duplication with compare (DWC) is performed. These methods are also validated with emulation techniques. The design is implemented with fault tolerant techniques, both coded in VHDL and the fault injection for analysis is done by HDL code modifications. The performance is analyzed using ChipScope analyzer.

The second and the major objective of the thesis discuss the design of the irradiation experiment at gamma chamber and the measurement setup. The design of experiment comprises of shielding box attenuation calculation, dose estimation using CaSO4: Dy powder with thermo-luminescence (TL) phenomenon and the design of test circuits. The device under test is Xilinx Spartan 6 FPGA of 45 nm CMOS process technology.

The power supply current variation and the functionality failure of the device are monitored both in the power-on and power-off conditions. In the power-on test, the

device is configured with particular functionalities and the parameters are measured continuously but, in the power-off test, the performance variations of the device are captured after configuring the device at particular time intervals during the experiment. Along with the power supply current variation, an indirect method of measuring the propagation delay based on ring oscillator implementation has been adopted. The device has been irradiated up to a dose level of 2.5 Mrad in power-on test and up to 50 Mrad in the power-off test. The major parameter shift observed in this experiment is the increase in power supply current. Here the device under test was irradiated at a high dose rate of 5.753 krad/minute (3.452 kGy/h). So, annealing at the time of irradiation was not possible and due to the cumulative dose, the characteristic changes will be more than that in an identical device absorbing the same total dose at lower dose rate. In this experiment, it is observed that the device is functionally tolerant up to a radiation dose level of 322 krad. So if the system is implemented with SEU mitigation techniques, the device can withstand up to 322 krad of accumulated dose without any failure. For further improvement in the life of the system, shielding should be provided. Two-dimensional transport code, DORT and IGC-S3 cross-section set are used for the modelling and prediction of the attenuation of gamma radiation inside the fabricated shielding box at the gamma chamber facility. Also, predicted the reduction in dose rate inside the shielding under core disruptive accident (CDA) conditions in the reactor containment building. It is found that the designed shielding box could able to extend the life of the system almost two times. By considering the worst-case condition inside the RCB i.e., during the CDA the average neutron energy is 1.8 MeV and the probability of causing an upset is very less. So, when we are deploying the device inside the RCB where the neutron energy is less than 10 MeV the device can efficiently work with error

correction codes with selective redundancy. Based on the criticality of the system, partial reconfiguration or periodic scrubbing can be used to improve efficiency.

The indirect way of propagation delay measurement method used here, which is based on ring oscillator can be very well suitable for measuring the TID effects in flash-based FPGAs, as the propagation delay is the major parameter change due to TID in flash based FPGAs. The future scope is to implement the identified safety systems of NPP I&C using SRAM based FPGAs based on the results of the study, analysis and experiments performed.

# 1

# INTRODUCTION

*This work involves the study of radiation effects, analysis of upset mitigation techniques and experiments to measure the upset sensitivity in SRAM based FPGAs, primarily targeted for nuclear power plant instrumentation and control system design. The study covers the advantages of SRAM based FPGAs over other FPGA technologies and microprocessor-based systems, various types of radiation effects on FPGAs, sources of radiation, upset sensitivity and analysis of available irradiation experimental results. Based on the study and analysis, various objectives of the thesis are set. This chapter includes the introduction of the thesis, the motivation behind the objectives and how the thesis is organized. The successive chapters illustrate how the objectives of the thesis are achieved.*

Field programmable gate array (FPGA) is already a well-known technology in applications such as aerospace, automotive, medical, high-performance computing and data storage. FPGAs are also used in the Instrumentation and Control (I&C) systems of nuclear power plants (NPP) but rarely. However, the International Atomic Energy Agency (IAEA) recommends the usage of FPGAs or other hardware description language programmed devices (HPDs) instead of analog and microprocessor-based systems in future and existing nuclear I&C systems to improve reliability and also to overcome fast obsolescence [1]. At present, there are only a few nuclear reactors in the

world that employ FPGA-based systems for their I&C. Among those, most of the systems are implemented using antifuse FPGAs [2]. EPROM/EEPROM based FPGAs are called flash-based FPGAs. Flash based FPGAs need additional fabrication process compared to the advanced CMOS process technology. As these devices are non-volatile it is not required to have an in-system SPI flash memory to configure the FPGA. The device can be configured and reconfigured out of circuit (off board). If required these FPGAs can be reconfigured from a host device through JTAG or SPI [3]. When compared with flash or antifuse FPGAs, SRAM-based FPGAs have the benefit of the most up-to-date fabrication process on par with complementary metal oxide semiconductor (CMOS) process technology; since they offer much higher integration and logic capacity. Further, SRAM-based FPGAs can be reconfigured many times without any degradation in their performance [4, 5]. The above discussed features make SRAM based FPGAs a better option for implementing complex designs.

As a result of the implementation of defence in depth concept [4] in I & C architecture, the use of HPD based designs are varied in their applications and importance. For example, the HPD based designs used to develop instrumentation for shutdown systems and data acquisition systems come under design assurance levels ‘high’ and ‘moderate to low’ respectively. SRAM-based FPGAs are primarily targeted for designs in which the assurance level required is ‘moderate to low’. The typical cross-section data [5] for SRAM FPGAs suggest that the failure rate in failure in time (FIT) due to irradiation in the current installed locations of I&C systems are much less than the overall target failure rate of the system i.e., if the selected device is not the weakest link in the structure and can be safely used. SRAM FPGAs supports reading back its

configuration memory and reconfigure the FPGA in case of any error, this feature is missing in antifuse and flash based FPGAs. Antifuse based FPGAs are mostly used in safety applications where they are made as simple as possible to enhance reliability. The capability of SRAM based FPGAs for complex computations and features like dynamic partial reconfiguration [6] are not much required for these systems. However, the safety critical systems like core temperature monitoring system (CTMS) in fast reactors which is tasked with the responsibility for core supervision for early detection of core anomalies such as plugging of fuel sub-assemblies and error in core loading is a notable exception [7]. It requires substantial I/O handling capability, processing power and is usually implemented using a microprocessor based system. Compared to microprocessor-based designs, FPGA based solutions can generally be made simpler, more testable, less reliant on complex software and easier to qualify for safety and safety-related applications [8]. SRAM based FPGAs with their large logic processing capacities are ideal candidates for hardware implementation of this system and hence require a detailed study.

Even though SRAM based FPGAs have numerous advantages, they are vulnerable to radiation effects either due to transient or cumulative radiation exposure [9]. FPGAs can be affected by gamma photons, neutrons and also heavy charged particles like protons, alpha particles etc. Radiation effects in FPGAs can be categorized as total ionization dose (TID) effects, single event effects (SEE) and displacement damage dose effects (DDD). Therefore, an intensive study of radiation effects in SRAM based FPGAs is extremely essential before they are used in I&C systems of nuclear

power plant (NPP). This study would further aid in improving the reliability of the designs implemented in FPGAs.

In the next section the research motivations are given, followed by the objectives of the thesis and how the thesis is organized based on the objectives.

## 1.1. MOTIVATION

From the literature survey, it appears that such data for SRAM based FPGAs used in NPP I & C systems are not reported in the open literature. Also, the only existing standard IEC-62566, which is specific for the standards and guidelines for FPGA based safety-critical system design, is not adopted by most regulatory bodies as the reliability aspects related to operating under harsh environments, aging and physical degradation are not handled in this standard. As the system error is unacceptable in NPP applications, a detailed study on radiation effects is required before deploying a system implemented in SRAM based FPGAs. It is observed from the literature that low energy neutron, i.e., energy less than 10 MeV also can cause SEUs in the modern FPGAs. Moreover, the accumulated dose enhances the soft error rate in the FPGAs. So, when the device is used in an environment having both gamma and neutron sources, SEUs and TID effects need to be taken care. In a nuclear reactor environment, gamma radiation is the major source of radiation effects hence the present study has given focus on radiation effects by gamma rays. In addition, it is necessary to study the feasibility, understanding and outlining the challenges involved in the design of I & C systems for NPP applications.

The I&C systems of NPP are classified as safety critical (SC), safety related (SR) and non-nuclear safety systems. The I&C systems of a sodium cooled fast reactor includes the systems for reactor startup, operation, fuel handling, shutdown and maintenance [10, 11]. Most of the I&C systems are real time computer (RTC) based systems with triple modular redundancy (TMR) or dual hot standby architecture. The currently used triplicated RTC though reliable has the following pitfalls which are outlined as follows: a) triplicated system is identical and hence is a potential source of common cause failure, b) the use of software in the RTC lends an element of uncertainty in the current design, and c) the use of multiple penetration assemblies in Reactor Containment Building (RCB) lowers the integrity of the RCB. Hence, it is required to develop a diversified hardware based I&C system with radiation tolerant features which can be kept inside the RCB.

As identical RTC based blocks are used in the triplicated system it is advisable to use diversified systems in the triplicated system to avoid common cause failures. A mix of hardwired and RTC based systems can be used to make the diversity. Hardwired implementation can be either by application specific integrated circuits (ASIC) or FPGA based. SRAM based FPGAs make a better choice for this particular requirement but with following challenges involved:

- There is a need for diversified modular redundant techniques in most of the I & C systems of NPPs.
- The use of software in the real time computer lends an element of uncertainty.
- System error is unacceptable in safety critical applications.

- No history of data available for SRAM based FPGAs used in NPP I & C systems.
- There is only one specific document for standards and guidelines for FPGA based safety critical system design, that also not adopted by most regulatory boards.
- It is identified that Gamma radiation is the major source of radiation effects in NPP applications.
- It is also found that TID effects and SEUs are the common causes of failure in SRAM based FPGAs.
- The accumulated dose enhances the soft error rate in the FPGAs.

## 1.2. OBJECTIVES OF THE THESIS

The main objectives of the thesis are set based on the literature review and they are as follows:

### 1.2.1. Investigation into SEU Mitigation Techniques in the Configuration Memory

As there are several SEU mitigation techniques reported in the literature, it is necessary to have a classification based on the advantages, drawbacks, the level of complexity of implementation and efficiency, to adopt those techniques based on specific requirements.

### 1.2.2. Design of Improved Error Recovery Mechanism for Configuration Memory

It is identified that the Golay code and the extended Golay code exhibit better error detection and correction capability than the other error correction codes available

for SEU mitigation in the configuration memory of FPGAs. So, the design and development of an error recovery mechanism based on Golay code will improve the efficiency of the system.

### 1.2.3. Analysis of verification solutions for the design used in reactor applications

To evaluate the sensitivity of a design to SEUs, the design has to be verified thoroughly either at simulation level or validated at the FPGA level on the test board. This entails the use of fault injection methodology. There are techniques reported in the literature but most of the techniques are not commercially available and such solutions may not be suitable for reactor applications. So, it's necessary to have a robust technique to inject fault at the RTL and netlist level of abstraction suitable for verification of the designs used in reactor applications.

### 1.2.4. Measurement of TID Tolerance Level by Irradiation Experiments

Measuring the total absorbed dose effects in SRAM based FPGAs is one of the major objectives of this thesis. As the accumulated dose increases the upset rate in FPGAs, it is required to know how the accumulated dose alone affects the characteristics of the device. Towards this, an irradiation experiment has been designed to suit the Gamma-5000 facility available at this centre. Experiments have been conducted by keeping the device both in power-on and power-off states. It may be highlighted that in some applications, the device is deployed in the radiation environments and remains in power-off condition for a substantial period before it is put into service. From this consideration, the irradiation experiment at power-off state is assumed importance.

## 1.3. STRUCTURE OF THE THESIS

**Chapter 1** (**Introduction, motivation and objectives**):- This chapter provides an introduction to SRAM based FPGAs and their advantages over other technologies, the need for FPGAs or other hardware description language programmed devices (HPDs) in nuclear power plant I&C systems. It also, covers the motivation and objectives of the thesis.

**Chapter 2** (**Literature review**):- In this chapter, a detailed review of radiation effects in SRAM based FPGAs, which includes the sources of radiation effects, different types of soft errors/hard errors and analysis of irradiation experimental results is presented. It also, discusses the guidelines and standards to follow for FPGA based safety critical system design.

**Chapter 3 (Investigation into Various Aspects of SEU Resistant Design)**:- This chapter deals with analysis of SEU mitigation techniques and design of error recovery mechanism based on Golay code. This chapter also provides a comparison on commercially available radiation hardened FPGAs and the non-radiation hardened FPGAs hardened by the design aspects implemented by the user.

**Chapter 4 (Analysis of Verification Solutions for the Design used in Reactor Applications):-** This chapter investigates the non-suitability of the design and verification techniques available in the literature as well as commercially available solutions and their shortcomings for reactor applications. This chapter also discusses the development of script-based error recovery mechanism, verification of the efficiency of fault tolerant techniques based on simulation and emulation.

**Chapter 5 (Measurement of Total Ionization Dose effects in SRAM based FPGAs)**:- This chapter discusses the design of irradiation experiment at gamma chamber and the measurement setup. The design of experiment comprises of (i) shielding box attenuation calculation, (ii) dose estimation using CaSO4:Dy powder with thermo-luminescence (TL) phenomenon, (iii) design of test circuits and (iv) analysis of the experimental results.

**Chapter 6 (Conclusion and Scope for Future Work):-** This chapter summarizes the major findings and elaborates scope for future work.

# 2

# LITERATURE REVIEW

*The current chapter presents a detailed study on radiation effects in SRAM based FPGAs which includes the sources of radiation effects, different types of soft/hard errors and analysis of irradiation experimental results. It also discusses the possible guidelines and standards to be followed in SRAM FPGA based safety-critical system design.*

## 2.1. BASICS OF SRAM BASED FPGA

The design that needs to be implemented in FPGA is converted into binary, i.e., bitstreams, downloaded into the device. The bitstreams are stored in the configuration memory, which holds the functionality and the routing of the design mapped into the FPGAs. The configuration memory, which constitutes an array of SRAM memory cells, along with the configuration access ports and control logic, forms the configuration layer. The user logic, user memory, and I/O resources form the application layer. The current state of the functionality is stored in the user memory [13, 14]. The configuration memory is organized as an array of frames; each bit is stored in the static RAM (SRAM) cells. Each SRAM cell is formed by two CMOS inverters connecting back to back with two access transistors as shown in Fig. 2.1. These configuration memory cells implement the lookup tables (LUTs), control multiplexers, and other control elements. A LUT stores its truth table in the configuration memory cells, which

implements the combinational logic function. The interconnection structure includes a programmable interconnection point, mostly a pass transistor that is controlled by the value stored in the configuration memory cell [14]. The selection line values of the multiplexers and other programmable elements are also stored in the configuration memory cells. The registers [flip-flops (FFs) and latches] and on-chip memory (Block RAM (BRAM)) bits hold the current state of the circuit [15]. Among the elements of the SRAM-FPGAs, the configuration memory bits are very prone to radiation effects; the bits dedicated to routing resources are more vulnerable than the bits dedicated to logic resources [16]. In the application layer, BRAM is highly susceptible while registers and I/O resources are moderately susceptible to radiation effects [17]. The logic resources structure and routing architecture are shown in Figs. 2.2 and 2.3 respectively.

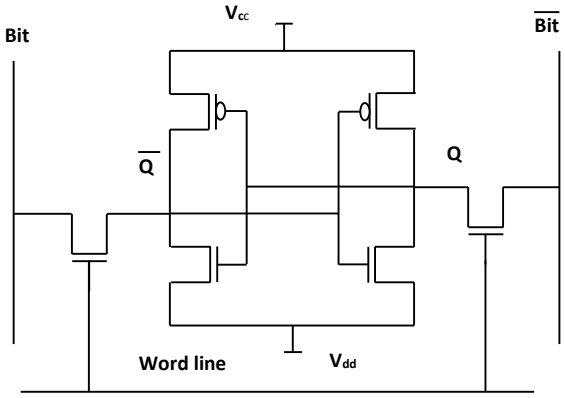



**Figure 2.1. Basic SRAM cell**

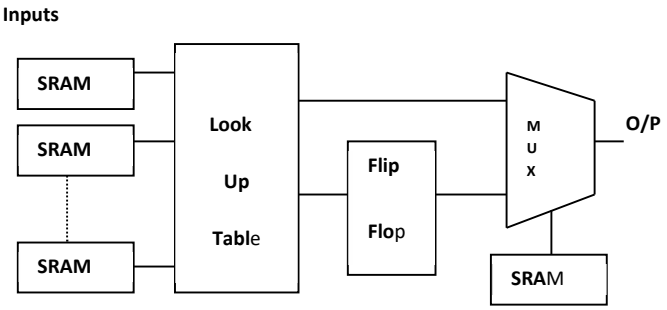



**Figure 2.2. Logic resources**

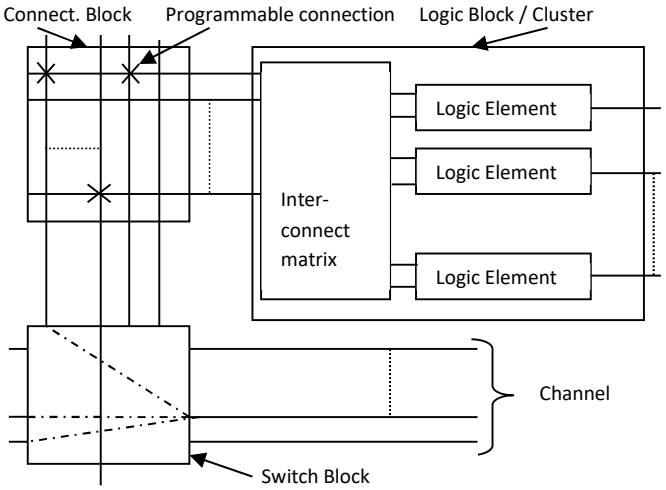



**Figure 2.3. Routing Architecture**

## 2.2. UNDERSTANDING RADIATION EFFECTS IN SRAM BASED FPGAs

### 2.2.1. Sources of Radiation Effects

FPGAs can be affected by gamma photons, neutrons and also heavy charged particles like protons, alpha particles etc. When electronic devices are exposed to gamma ray photons, the energy of the photons gets deposited in the devices, mainly by ionization process. The energy required to form an electron-hole pair is called the ionization dose. However, the cumulative energy absorbed by the circuit during the whole exposure is determined as total ionization dose (TID) [18]. The ionization process can take place directly by gamma photons themselves or indirectly by secondary recoil particles. The major damaging effects due to gamma photons are basically single event effects (SEEs) and TID effects caused by increased conductivity and trapped charges in the electronic devices. Neutron interaction with matter is dominated by collisions, with nuclei leading to either scattering or absorption. In elastic scattering, a neutron collides with a nucleus and scatters in different directions. The

energy lost by the neutron is gained by the target nucleus. In inelastic scattering, the neutron strikes a nucleus, forming a compound nucleus, and the de-excitation process of the nucleus produces gamma radiation. The neutron absorption reaction includes radiative capture and nuclear fission. A neutron can be captured by nuclei through one of the following nuclear reactions: (n, p), (n, α), or (n, γ). Elastic scattering is more probable for high-energy neutrons and the capture effect is more likely for low-energy ones. The secondary particles generated by the neutron interaction can cause ionization in the targeted material. For example, an alpha particle generated in such a way has very high linear energy and it can transfer/deposit its whole energy, ionizing the material. Neutrons generally cause displacement damage dose (DDD) and SEEs in targeted devices. The types of particle interactions and the primary as well as secondary effects they cause are illustrated in Table 2.1 [19-22].

**Table 2.1. Types of particle interaction**

| Rad. Type | Energy Range | Type of interaction | Primary effects | Secondary effects |
|---|---|---|---|---|
| Photons | < 0.1 MeV | Photoelectric effect | Ionizing phenomena | Displacement Damage |
| | 0.3-3MeV | Compton effect | | |
| | >1.024MeV | Pair production | | |
| Neutrons | ~ 0.025eV | Slow diffusion and Capture by nuclei | Displacement damage | Ionizing phenomena |
| | < 10MeV | Elastic scattering, capture, nuclear excitation | | |
| | >10MeV | Elastic, inelastic scattering, various nuclear reactions, secondary charged reaction products | | |
| Alpha Particles | 4-8 MeV | Coulomb attraction | Ionization phenomena | -- |

### 2.2.2. Radiation Effects in SRAM Based FPGAs

#### 2.2.2.1. TID effects

TID effects are reliant on the dose rate, the type of radiation applied, and the internal electric field including space charge effects [23], device geometry [24, 25], operating temperature, time after irradiation [26, 27] and so on. The ionization radiation effects cause the accumulation of charge in the SiO2 and Si/SiO2 interface. These trapped charges affect the electronic parameters of the MOS transistor, with the threshold voltage ($V_{th}$ ) being the most important parameter [28]. The other effects are a reduction in transconductance, an increase in leakage current, reduction in drain-source breakdown voltage, deterioration in noise parameters, and reduction in surface mobility [29-31]. The n-type metal-oxide-semiconductor (NMOS) transistors are more vulnerable to radiation and undergo threshold voltage shift more easily than p-type metal-oxide-semiconductor (PMOS) transistors. The positive threshold voltage can either decrease or increase in NMOS transistors, as shown in Fig. 2.4 [32]. Initially, the charge sheet moves toward the interface due to positive gate bias voltage and a decrease in threshold voltage happens when the oxide trapped charge ($Q_{ot}$) effect dominates. The threshold value can move to a positive side when the charge deposition increases. The threshold voltage shift in the PMOS transistor is as shown in Fig. 2.5 [32]. PMOS transistors, due to the presence of holes as charge carriers, are slower and carry less current than NMOS transistors, which has electrons as carriers [33]. Given a constant area of influence of a radiation event, the percentage of area affected in the NMOS is two to three times that in PMOS, and hence, PMOS is more tolerant. In modern processes, short channel effects, such as saturation velocity, reduce this ratio to a much

lower value [34]. In this context, an isolated NMOS will be more vulnerable than a PMOS. In another perspective, the change in threshold voltage of MOS devices depends on the electric field in the silicon dioxide [35].

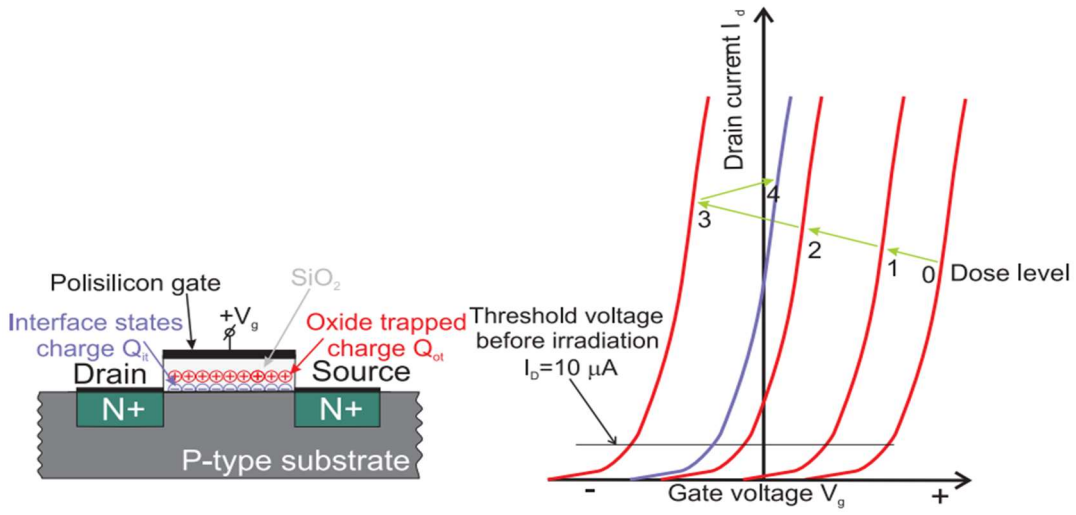



**Figure 2.4. Oxide and oxide-silicon trapped charge in NMOS transistor together with ID-VG curves reflecting shifts in threshold voltage [32]**

Therefore, the biasing voltage has serious impact on charge generation and deposit. The threshold voltage shift can be expressed as the sum of two voltage changes caused by the increase of the charge in silica ($Q_{ot}$) and two interface trapped charges ($Q_{it}$) [36]. The effect of the trapped charge and the interface state formation are additive in PMOS devices, but for the source of the differential in NMOS devices lies in the difference in worst case logic bias conditions for PMOS and NMOS transistors [37]. Biasing voltage is the major component that decides the position of charge built-up in MOS devices. Due to negative biasing, the distance between the gate terminal and the charge sheet is larger in PMOS devices while it is smaller in NMOS devices due to the positive biasing. For this reason, PMOS transistors are considered to be more tolerant

to radiation effects [38]. Charges trapped in MOS oxide will shift the threshold voltage negatively in NMOS, leading to unacceptable drain-source leakage current. In PMOS, the opposite occurs, increasing the threshold and reducing the leakage [38].

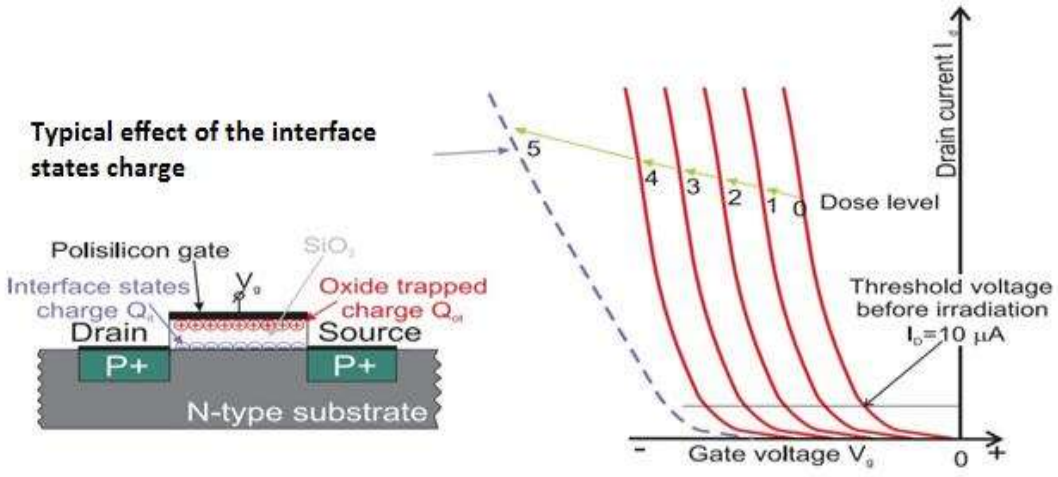



**Figure 2.5. Oxide and oxide-silicon trapped charge in PMOS transistor together with ID-VG curves reflecting shifts in the threshold voltage [32]**

### 2.2.2.2. DDD effects

The DDD quantizes the displacement damage to the semi-conductor lattice due to the impact of energetic particles. If the transferred energy is higher than the displacement energy, a lattice atom will be removed from its original position in the lattice and a defect will be created [23]. A cascade of disruptions in the silicon lattice is possible with higher energy particle exposure. The main types of displacement defects are vacancy, divacancy, interstitial, Schottky and Frenkel as shown in Fig. 2.6 [21]. The displacement damage mainly causes permanent damage by altering the placement of atoms in the crystal lattice. DDD also changes the electronic properties of the device.

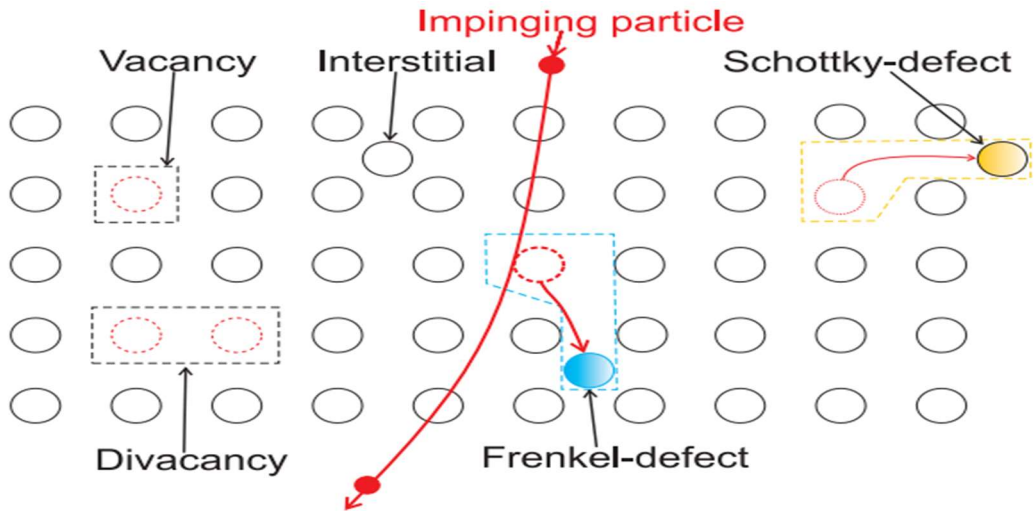



**Figure 2.6. Displacement damage defects [21]**

### 2.2.2.3. Single event effects

A SEE is caused by a single energetic particle, which generates an electrical charge in a material depending on the amount of energy the ionizing particle transfers to the material. This process is also known as linear energy transfer (LET) [39]. LET is expressed in $MeV\mu m^{-1}$ and it can also be measured in $MeVcm^2\ g^{-1}$ when it is normalized to the specific mass of the absorbing material [40]. Critical LET, or the LET threshold ($LET_{th}$), is the maximum LET value deposited by a high-energy particle travelling through a semi-conductor device for which failure is not yet observed. When the created electron hole pairs are expressed as a charge, the minimum charge necessary to create SEE is called the critical charge [41]. The SEEs can be classified as soft errors and hard errors [42], as illustrated in Fig. 2.7. Hard errors, being not recoverable, can permanently damage the hardware in the same way as in the case of a burnout resulting from a short circuit. A soft error is a change in the signal or a data bit flip and it can occur in logic modules, I/Os, routing resources, and block random access memory

(RAMs) virtually any part of the FPGA. When a soft error occurs, the device may still function correctly or may exhibit partial functionality [43]. Different from hard errors, soft errors can be found out and recovered without performing any power reset to the device.

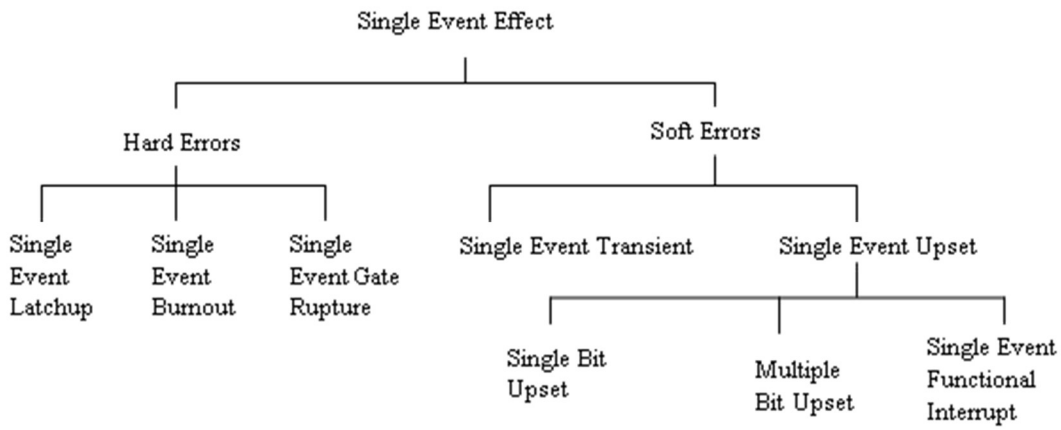



**Figure 2.7. Classification of single event effects**

- ***Soft errors***

The capacitance and voltage levels of logic circuits have a significant role in the generation of soft errors; the higher these parameter values are, the less probability there is of a soft error generation. The critical charge value varies for each node in the FPGAs. The capacitance of the internal nodes of SRAM cells is very low compared to that of FFs. Therefore, it requires less charge deposition to alter the value stored in the SRAM cells. Soft errors are mainly classified into two types: they are single event transients (SETs) or SEUs.

The basic mechanism of soft error generation is illustrated in Fig. 2.8 [44]. When the charged particles pass through the device material, they generate electron-hole pairs. The most susceptible parts are generally reverse-biased p-n junctions. The

charge carriers are collected by the electric field and drift to the nearby node, where a current/voltage transient is created. The majority of the charge is collected by rapid drift process, and this is followed by a diffusion process, as shown in Fig. 2.9 [44]. A funnel-shaped extension of the depletion region enhances the drift collection; therefore, more charges can be effectively collected at the node [45, 46].

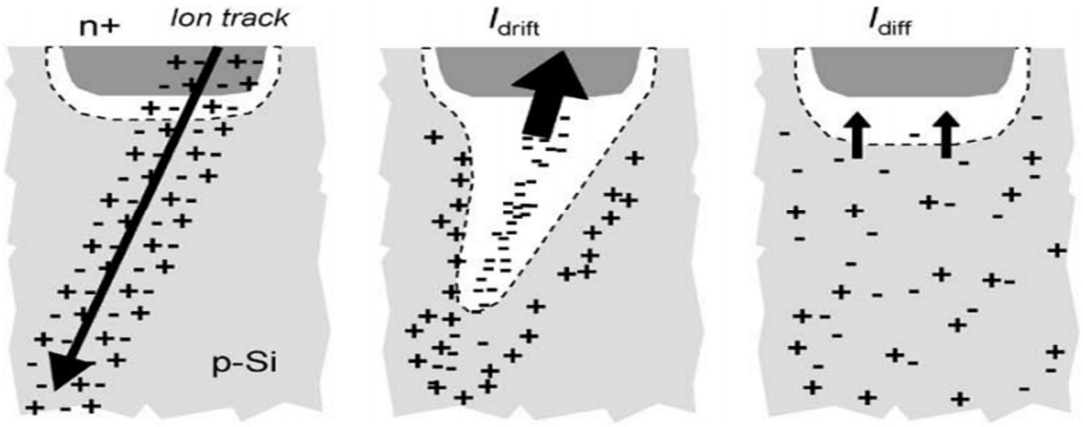



**Figure 2.8. Charge generation and collection phase in a reverse-biased junction [44]**

- ***Single event transient***

A SET is a current or voltage spike generated due to particle strikes. SET could be a glitch in the circuit or it may get captured in FFs or other memory elements and can cause a functional error in the operation of the device [47]. SETs are not always harmful to the device and may be transitory in nature. The probability of transient pulse capture is increased by high clock Speeds [48]. As SET captures are asynchronous, it is impossible to predict them by static timing analysis. The generation of a transient pulse and its capture are shown in Fig. 2.10.

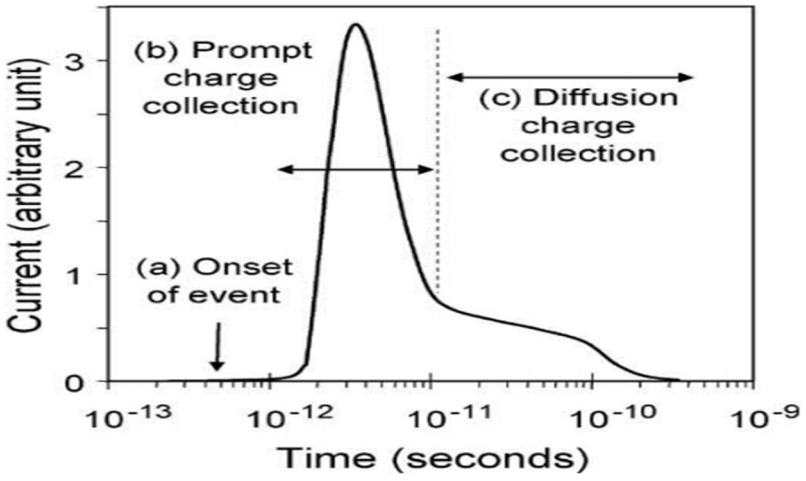



**Figure 2.9. Current pulse generated due to radiation effect [34]**

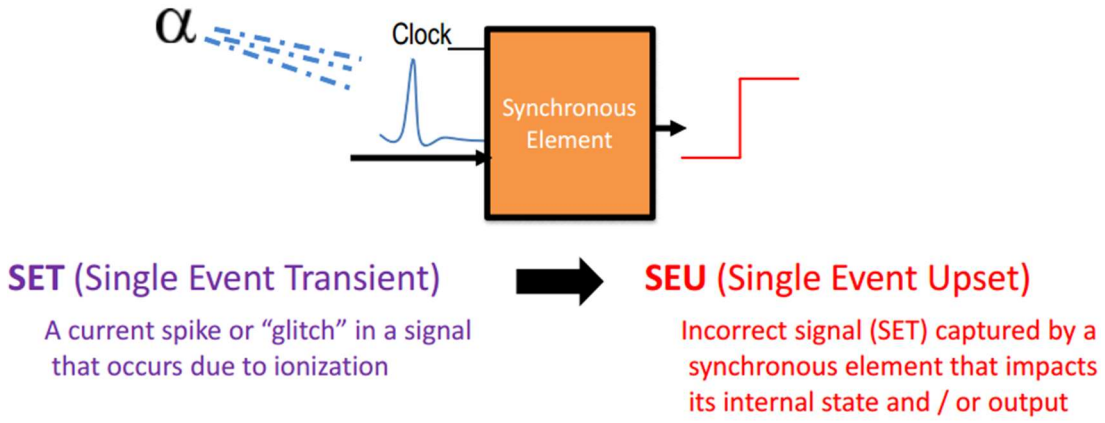



**Figure 2.10. SET captured in a synchronous element [15]**

- ***Single event upset***

SEU is a soft error caused by a transient signal induced by a single energetic particle strike when the collected charge is greater than the critical charge required to cause a change in state of a memory cell, register, latch, or FF. For 0.5mm technology, the critical charge required to cause an SEU is roughly in the range of femto coulombs. The SEU sensitivity is measured by cross-section and is expressed in $cm^2$/bits or $cm^2$/device. The most sensitive regions in SRAM cells are the reverse-biased drain

junctions of a transistor biased in the off state [49, 50]. SEU generation is dependent on lots of factors such as the LET, particle strike location, charge collection, recovery process, etc. From a technology standpoint, it depends on the restoring transistor current drive and minority carrier lifetimes in the substrate [51-54]. A bit flip in an SRAM cell is illustrated in Fig. 2.11 [55].

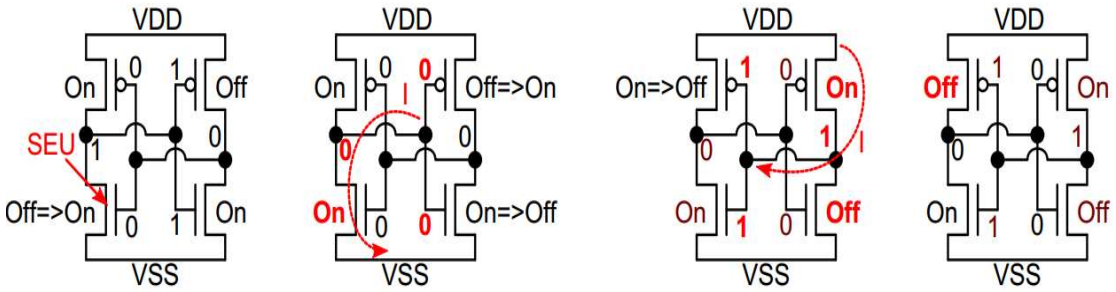



**Figure 2.11. A bit flip in an SRAM cell (a) Particle hits a transistor in off state, (b) charge is collected by the collector of the left NMOS and creates current I, which discharges gate of the right transistor, (c) right transistor toggles and enables current to charge gates of left transistors, and (d) left PMOS switches off and the circuit reaches a stable condition [55]**

- ***Single bit and multiple bit upsets***

A single particle strike can affect either single or multiple memory cells based on whether it is a single bit upset or multiple bits upset, respectively. A single particle strike can pass through multiple adjacent cells and can cause multiple bit upsets. There are three major principles for multiple bit upset origination: (a) a particle impact angle that allows the particle to pass through more cells; (b) a diameter of the cylinder in which the charge is deposited, that crosses more memory cells such that SEUs may occur there; (c) memory cells that are upset by the products of spallation reactions from the primary particle in the chip [56].

- ***Single event functional interrupt***

Single event functional interrupt (SEFI) causes the interruption of normal operation of the affected device [57]. SEFI is a special case of SEU in which SEU either occurs in control logic or control over the logic, and the device functionality are lost. SEFI in SRAM-based FPGAs is due to upsets in particular circuits that involve power-on-reset, failures in the joint test action group (JTAG) or select-map communications port, loss of configuration capability, or others [58, 59].

- ***Hard errors***

- ***Single event latchup***

Single event latchup (SEL) occurs when the energy released by a particle strike can activate the parasitic thyristor (PNPN structure) embedded in the CMOS architecture [60, 61]. When activated, this structure presents positive feedback, causing the involved transistor to start to drain high current [62]. Depending on the resistance, the latchup can be a) fatal when the current density exceeds safe current limits or b) temporal (soft) when a latchup generates heat that further increases current consumption. However, after the power cycle, the device recovers [54]. The SEL typically requires power cycling of the device (when the latchup occurs between the supply voltage and ground) but can also occur within signals where the latchup can be stopped by the change of values.

- ***Single event burnout***

Even when there is no P-N-P-N structure, an ion strike can turn on a real bipolar junction transistor (BJT) or a parasitic BJT structure in a (usually) n-channel metal-

oxide-semiconductor field-effect transistor (MOSFET). The resulting second breakdown causes a high-current state and can cause thermal failure of the device. Due to particle strike, the substrate right under the source region gets forward biased, and the drain-source voltage is higher than the breakdown voltage of the parasitic structures. The resulting high current and overheating may then destroy the device. MOSFETs, BJTs, and some CMOS structures are very susceptible to single event burnouts [63, 64].

- ***Single event gate rupture.***

A local breakdown happens in the insulating layer of SiO2, causing local overheating and destruction of the gate region [65]. Single event gate rupture only affects transistors when they are in their non-conducting states (VGS≤0V for n-channel devices or VGS≥0V for p channel devices). In the case of single event gate rupture, holes from the ion strike pileup under the gate, thus increasing the electric field across the MOSFET gate oxide to its dielectric breakdown point. The resulting flow of the current causes thermal failure of the gate oxide. These events represent localized breakdowns in the oxide and also can result in latent damage [66].

As hard errors are non-recoverable errors it is required to apply preventive mechanisms against hard errors. Such techniques are related to fabrication and shielding. These techniques include thinning the oxide thickness, removal of impurities during the oxide preparation, modification of technology parameters, etc. One of the widely accepted fabrication related methods is Silicon on Insulator technology [36].

Fault location determination and performance enhancement via runtime hardware accelerators are discussed in [67]. If there is an occurrence of hard error that area in the device can be isolated and the logic which performs that function can be reconfigured using dynamic partial reconfiguration [68]. Reconfiguration techniques are discussed in detail in section 3.1.1. A research area currently being explored is runtime instantiation of custom hardware accelerators as peripheral devices to the processors. This method allows to offload computationally intensive operations performed by the software to hardware resources [67]. In this thesis we are focusing mainly on recoverable errors.

## 2.3. MEASUREMENT OF RADIATION UPSET SENSITIVITY

Before deploying FPGA-based systems in NPP I&C systems, the sensitivity of the device to radiation needs to be measured. For this purpose, the device has to be exposed to radiation sources and the consequences have to be analyzed. While doing irradiation experiments the objectives can be set as listed in [69], they are: a) measure SEU sensitivity of configuration memory and block RAM cells (with and without mitigation techniques), b) measure SEU sensitivity of input/output blocks (IOBs) and c) measure the TID effects. SEE evaluation can be mainly classified into three areas, viz (i) static: during irradiation the FPGA design is tested in unclocked state, and configuration memory upsets and SEFI failure modes are measured [70], (ii) dynamic: the FPGA design is tested in clocked state and this mainly helps to measure the SETs and also measure SEFIs and IOB upsets; process requires observation to measure the upsets during transient signal propagation [70] and (iii) mitigation: after implementing the error mitigation techniques, the FPGA design is evaluated for upsets. Worst case

execution time is an important parameter while considering the mitigation techniques for SEUs. Worst case execution time (WCET) in case of single event upset is the sum of maximum time interval between the occurrence of SEU and detection and the time required to repair the SEU [71].

The radiation test needs to be conducted mainly to determine faults in the configuration memory that covers the logic resources (LUT error, multiplexer (MUX) error, and FF error) [72] and routing resources (short error, open error, open/short error) [73].

In the static test, the configuration memory is initialized with a known pattern. Then, during radiation exposure, the FPGA memory is periodically readback and compared with the expected pattern. The main parameter to determine is the probability that the particle flips a single bit, which is known as a cross-section (s) and is measured in $cm^2$/bit or $cm^2$/device. The device cross-section is defined as the ratio between the number of SEUs ($N_{SEU}$ ) and the fluence of the hitting particles (ø) given in Eqn. (2.1). Fluence is the total number of particles that impinge upon a unit surface area for a given time interval expressed in particles/$cm^2$. Based on the cross-section value, the sensitivity of the FPGAs to a specific radiation source can be quantified.

$$Cross\ section, \sigma = \frac{Nseu}{ø} \quad \text{(Eqn. 2.1)}$$

The expected failure rate of FPGAs can be expressed as FIT. One FIT equal one failure per billion ($10^9$) hours and is statistically projected from the results of the accelerated test procedures, given by Eqn. (2.2) The mean time between functional failures (MTBFF) can be calculated as per Eqn. (2.3) [74].

$$FIT = Cross\ section \times Particle\ flux \times 10^6 \times 10^9 \quad \text{(Eqn. 2.2)}$$

$$MTBFF = SEUPI \times [1/(Bits \times Cross\ section \times Particle\ flux)] \quad \text{(Eqn. 2.3)}$$

The estimation of the single event upset probability impact (SEUPI) factor is explained in [75] wherein the particle flux is defined as the rate at which particles impinge upon a unit surface area and is expressed in particles/cm$^2$/s. Dynamic tests are conducted when the device is performing its functionality in a clocked state while the results of static tests can be taken as a reference for these tests [70].

TID effects can be measured by finding the change in propagation delay of each paths in a circuit implemented in FPGA, before and after irradiation. TID effects can also cause variations in duty cycle response, power supply current, and temperature [76]. There are two main kinds of experiments available. The first is to measure the propagation delay between the input and output where the measurement path includes the I/O logic and the internal logic. The inputs are given from a function generator and delay is measured by comparing the outputs using an oscilloscope or a logic analyzer [76, 77]. The second method measures the delay between internal elements, which provides more accuracy [78].

The total ionization limit for the majority of space applications is 300 krad (Si) and the LET limit for SEU in both configuration memory and user FF and registers is 37 MeV-cm$^2$/mg [79]. There have been many experiments conducted at various facilities to measure the sensitivity of radiation upsets in SRAM-FPGAs, mainly for space applications. The results are analyzed mainly based on the source, cross-section, and upsets generated. The overall results are illustrated in Table 2.2. At IEAv and ISIS facilities the device showed a mean bitstream upset rate of 0.38 upsets/hour and 16.45 upsets/hour respectively [80, 81]. In another experiment at IEAv facility, the same

device was irradiated with Co-60 source with a dose rate of 1.749krad (Si) per hour at room temperature. Later the device was irradiated with neutron source and it was observed that the soft error rate had increased from 0.49 errors/hour to 0.622 errors/hour after the device had an accumulated ionization dose of 15 krad (Si) and 0.640 errors/hour after 30 krad (Si).

**Table 2.2. Analysis of irradiation experimental results**

| Facility | Source | Neutron CS ($cm^2$) | Time (h) | Mean Flux ( n. $cm^{-2}$. $s^{-1}$ ) | Energy (MeV) | Upsets |
|---|---|---|---|---|---|---|
| IEAv facility [80] | $^{241}$Am-Be | $1.45 \times 10^{-15}$ | 261 | $7.87 \times 10^{3}$ | Up to 10.5 | 0.38 upsets/ h |
| ISIS [81] | (spallation process) | $1.37 \times 10^{-14}$ | 2 | $3.43 \times 10^{4}$ | 10 and above | 16.45 upsets/ h |
| LANSCE [82] | | $1.00 \times 10^{-14}$ | -- | -- | -- | -- |

## 2.4. RADIATION DOSE LEVEL AT SEVERE ACCIDENT CONDITIONS.

Performance of I&C systems during severe accident (SA) conditions also needs to be taken care of while designing a system for safety applications in NPP. As per the available information the dose level in boiling water reactor (BWR) and pressurized water reactor (PWR) during a SA condition is well reported. Severe accident conditions in boiling water reactors and pressurized water reactors are classified into the following: (i) SA1 is the condition in which the reactor core is damaged, but the core fuel remains inside, (ii) SA2 is the condition in which reactor pressure vessel/reactor vessel failure has occurred, and the core has relocated to outside the reactor pressure vessel/reactor vessel, (iii) SA3a is the condition in which a primary containment vessel/containment vessel failure has occurred, but water has been successfully injected within 24 h after

the safety control rod actuation mechanism (SCRAM), and (iv) SA3b: is the condition in which a primary containment vessel/containment vessel failure has occurred and efforts to inject water before 24h after the scram have failed, but after 24 h successful injection of water occurs [83]. The possible radiation dose levels during accidental conditions in boiling water reactors and pressurized water reactors are given in Table 2.3. [83].

**Table 2.3. Radiation levels in BWR and PWR at severe accident conditions**

| Plant/Environment Condition | SA1 | SA2 | SA3a | SA3b |
|---|---|---|---|---|
| BWR (Radiation dose) | 500 MRad/6 months (plant) 30 MRad/6 months (environment outside containment vessel (CV)) | 500 MRad/6 months (Plant) 30 Mrad /6 months (environment outside CV) | 500 MRad/6 months (plant) 200 Mrad/6 months (environment outside CV) | 500 Mrad/6 months (plant) 200 Mrad/6 months (environment outside CV) |
| PWR (Radiation dose) | Below the conventional PAM's environmental conditions | 200 MRd/year (an annular space is 500 MRad/year) | 200 MRad/year (an annular space is 500 MRad/year) | 200 MRad/year (an annular space is 500 MRad/year) |

## 2.5. GUIDELINES AND STANDARDS FOR SRAM FPGA BASED SAFETY CRITICAL SYSTEM DESIGN

I&C systems of NPPs are classified as systems important to safety and non-nuclear safety systems. The safety classification of these systems based on IEC, IEEE

and IAEA is given in Table 2.4 [84-86]. Considering Indian establishments, the I&C systems of Indian prototype sodium cooled fast reactor is classified based on Atomic Energy Regulatory Board (AERB) and IAEA guidelines. I&C for safety critical systems are covered in the safety guide AERB/SG/D-10 on safety critical systems [87] and guide on computer-based systems are as per AERB/SG/D-25 [88].

When considering SRAM based FPGAs for safety critical applications, the study and analysis of radiation effects play a major role. Along with this, there are few guidelines and standards to be followed while considering SRAM based FPGAs in safety critical applications. From the available literature it is found that there is only one guidance and requirements (IEC-62566) specific for FPGA based solutions for nuclear power industry and it is not being adopted by most of the regulatory bodies [89]. IEC 62566 provides guidance to use available commercial off the shelf items to use in an I&C development with HDLs and related tools. Since the existing regulatory documents are not specific about FPGA design practices, is considered prudent to follow the standards and regulatory approaches by different international standards and guidelines on computer-based or electronic/programmable devices as discussed in Table 2.5.

**Table 2.4. Safety classification of I&C systems in NPPs**

| Standard | Systems important to safety | | | Non-nuclear safety systems |
|---|---|---|---|---|
| IEC 61513 [84] | Class 1 | Class 2 | Class 3 | unclassified |
| IAEA Safety Guide NS-G-1.3 [85] | Safety | Safety related | | Systems not important to safety |
| IEEE standard (Std) 323-2003 [86] | Class 1E | | | Non-class 1E |

IEC 61513 provides requirements & guidelines for overall I&C architecture which may contain conventional hardwired equipment, computer-based equipment or by using both [84]. Reliability aspects related to environmental qualification and failures due to ageing or physical degradation are not handled in IEC 62566 standard. Most of the FPGA based designs prefer the standards which are used in other critical applications. Among the existing standards DO-254 is more preferable. This standard provides design assurance guidelines for FPGAs and application specific integrated circuits (ASIC) [90]. This standard is concerned with the entire hardware design life cycle. There are mainly two categories of information required for FPGA based safety critical design, they are (i) design assurance guidance applicable to FPGA based systems, and (ii) acceptable FPGA design practices. Design assurance guidelines can be adopted from available documents like DO-254, IEEE 1012 [91], IEEE 603, IEEE 7-4.3.2, and IEC 61508 [92], etc. while the FPGA design practices are covered in detail in many articles [93].

**Table 2.5. Comprehensive view of existing standards/guidelines for safety systems**

| Standard/guideline | Features and guidelines covered | Draw backs considering FPGA based design |
|---|---|---|
| IEC 62566-2:2020 [89] | Dedicated HPD life-cycle addressing each phase of the development of HPDs, planning and complementary activities such as modification and production, selection of pre-developed components, tools used to design, implement and verify HPDs. | Reliability aspects like radiation, aging, and other physical degradation are not considered. |
| IAEA NS-G 1.3 [85] | Includes classification of safety systems, general I&C design guidelines, quality assurance and documentation. | Not specifically gives any guidelines for FPGA based I&C system design |
| DO-254 [90] | Defines five levels of safety criticality as below catastrophic, hazardous/severe, major, minor, no effect. DO-254 covers | Considers FPGAs as purely hardware devices. |

| | | |
|---|---|---|
| | the whole process of hardware design from planning till certification. | |
| IEC 61508 [92] | This standard covers the design life cycle of programmable electronic devices and its safety assessment. Also, provided safety integrity requirements that covers only three levels of design assurance i.e., low, medium, and high. | FPGA-specific areas that are not sufficiently addressed. |
| NUREG/ GR-0020 [94] | Dependability analysis of embedded digital systems as well as metrics that characterises the dependability, reliability, availability and safety. | Not specific to FPGA based systems or digital systems. |
| IEEE 1012-2004 [91] | The tools used in FPGA design, verification and implementation involves software; as defined in IEEE 1012-2004, software does not require to be verified separately and can be considered as a final product and run on hardware platforms. | Covered generic V&V processes i.e., not specific to FPGAs. |
| IEEE 7-4.3.2 [95] | Design assurance guidance applicable to FPGA-based systems. Provides guidance for design tool verification. Addresses the V&V process for safety systems in nuclear plant and includes the requirements for independent V&V. | Not specifically gives any guidelines for FPGA based I&C system design |
| IEC 61513 [84] | This standard provides guidelines for hardwired equipment and computer-based equipment for the systems important to safety. | Recommends the use of complex electronic components such as ASICs or FPGA. But it recommends to use these devises following the guidance for conventional electronic equipment, or similar to computer-based equipment. |
| IEC/IEEE 60780-323 [96] | Nuclear facilities electrical equipment important to safety qualification. Some equipment needs to be qualified for conditions that are beyond design basis of the plant. Especially in the conditions like extended station backout, extreme natural hazards and severe accident. | Not specifically gives any guidelines for FPGA based I&C system design |
| IEC 60987 [97] | This covers the standards for computer-system hardware i.e., part of safety systems of NPPs. | Not specific to FPGAs |
| IEC 62342 [98] | NPPs I&C systems important to safety - Management of ageing. | Not Specific to FPGAs |

Most of these standards can be used by safety critical applications like space, nuclear, automotive, etc., Compared to the safety critical NPP I&C systems the major difference with space systems is it can be considered as mission critical systems. Mission-critical systems must be able to handle peak loads, scale on demand and always maintain sufficient functionality to complete the mission. Most of the NPP I&C systems are not required to handle peak loads and harsh environments at normal operating conditions. Another major difference is the NPP systems life is normally 40 years even though there is a possibility of hot swap, but the life of space systems is comparatively less.

## 2.6. SUMMARY

From the literature review, it is concluded that the common cause of failures in most of the SRAM based FPGAs are due to TIDs and single event upsets (SEU). Hence, this thesis is primarily focused towards the study of SEUs and TID effects on SRAM based FPGAs. From the literature, it is found that there is no history of data available for SRAM based FPGAs used in NPP I & C systems. Also, the only existing standard, which is specific for the standards and guidelines for FPGA based safety critical system design, is not adopted by most regulatory bodies. As the system error is unacceptable in NPP applications, an intensive study on radiation effects is required before deploying a system implemented in SRAM based FPGAs. It is observed from the literature that low energy neutron i.e., energy less than 10 MeV also can cause SEUs in the modern FPGAs. Moreover, the accumulated dose enhances the soft error rate in the FPGAs. So, when the device is used in an environment having gamma and neutron sources both the effects, i.e., SEUs and TID effects need to be taken care of. In addition, it is necessary

to study the feasibility, understanding and outlining the challenges involved in the design of I & C systems for the applications in the NPPs.

# 3

# INVESTIGATION IN TO VARIOUS ASPECTS OF SEU RESISTANT DESIGN

*As the single event upset (SEU) is one of the major causes of failures in the systems implemented in SRAM based FPGAs, the mitigation of SEUs has significant importance when such devices are used in NPP I&C system design. This chapter is organized mainly in three sections; the first section covers the analysis of SEU mitigation techniques, the second section discusses on the proposed error mitigation technique and the third section discusses on the comparison of radiation hardened FPGAs with non-radiation hardened FPGAs.*

## 3.1. ANALYSIS OF CONFIGURATION MEMORY ERROR MITIGATION TECHNIQUES

As the configuration memory of SRAM based FPGA is highly susceptible to SEUs, various mitigation techniques are critically analyzed. The mitigation techniques include various reconfiguration methods; mainly, the partial reconfiguration with error correction codes and scrubbing. The analysis covers the algorithmic and architectural changes which prevent or mitigate SEUs in the configuration memory bits dedicated for routing resources and logic resources. Important techniques are quantitatively compared for their efficiency, based on their SEU mitigation capability, area overhead, and delay. Further, new techniques to improve the efficiency of the mitigation techniques are proposed.

It is known that the configuration bits are dedicated to logic resources and routing resources. Irradiation testing on SRAM-based FPGAs shows that the configuration memory bits are highly susceptible to heavy ion induced SEUs [99]. The meaning of every configuration bit according to the affected resource allows classifying the critical bits which are responsible for the failure [100]. The SRAM memory cells which is part of interconnection is more susceptible to SEUs. The SEUs in the configuration memory adversely affect the functionality of the system, and hence the use of fault-tolerant techniques plays an important role to keep the system more dependable against SEUs [101]. Three categories of upsets experienced by the SRAM-based FPGAs are (i) static configuration bitstream upset, (ii) dynamic upset (either transient or upset of a user memory cell), and (iii) functional upset (e.g. upset on configuration circuit or JTAG tap controller). The following section gives an idea about reconfiguration and explains how SEUs can be mitigated by partial reconfiguration (PR) with error correction codes (ECC) and scrubbing methods. An overview of the techniques for mitigating SEUs in the configuration bits of routing resources and logic resources is presented latter. Each section is concluded with a comparison of the major techniques available with a recommendation for efficient mitigation techniques.

### 3.1.1. Reconfiguration

Reconfiguration is the process of post configuration memory write, which is the most efficient way to mitigate the configuration memory, upsets. Reconfiguration can be either partial or full. Full reconfiguration will completely replace the configuration bitstream or partial reconfiguration modifies a fraction of the resources. Partial reconfiguration can be categorised as static and dynamic. The static Partial

reconfiguration modifies a portion of the FPGA while the entire FPGA remains inactive and non-operational. However, the dynamic Partial reconfiguration occurs while the device is active and operational. Compared to full system reconfiguration partial reconfiguration requires less memory space and time [102, 103].

#### 3.1.1.1. Partial Reconfiguration with ECCs

Static memory bit upsets can be detected by reading back and comparison of the bitstream after the initial configuration. This process supports reading back the configuration memory bits and current state of the flip-flops without any interruptions. Most of the modern FPGAs uses a cyclic redundancy check (CRC) register which utilises a standard 32-bit CRC checksum algorithm to verify bitstream integrity during configuration [104, 105]. Dynamic Partial reconfiguration enables mission specific adaptability on demand, which provides the ability to reconfigure the FPGA device while other processes continue in the rest of the device. Current SRAM-based space suitable FPGAs provide a platform for these advanced enhancements [106]. Dynamic Partial reconfiguration coupled with TMR-based techniques can detect, locate and mask the SEUs in the configuration memory [107, 108]. Forward error correction (FEC) techniques like hamming codes is the widely used error correction code for SEU mitigation. Other FECs also can be utilized for SEU mitigation. The comparison of ECCs for SEU mitigation is illustrated in Table 3.1.

### 3.1.1.2. Scrubbing

Scrubbing is a method used to restore the initial state by a post configuration write in the configuration memory [109]. It is an effective error mitigation technique for configuration memory in SRAM-based FPGAs, to avoid the accumulation of errors in the configuration memory.

**Table 3.1.Comparison of ECCs for SEU mitigation**

| **Error Correction Technique** | **Error Detection and Correction Capability** | **Drawbacks** |
|---|---|---|
| SEC-DED using Hamming code, ($d_{min}$= 4) | Single error correction<br>Double error detection | Cannot correct Multiple Cell Upsets and miscorrection |
| SEC-DAED using Hamming Code | Single error correction<br>Double adjacent error detection | Miscorrection of triple adjacent errors |
| SEC-DED-TAED using extended Hamming code | Single error correction, double error detection and triple adjacent error detection | Cannot correct more than single bit error |

The circuitry which performs such task is known as the scrubber. In some situations, it is required to stop the application for a particular time period and fully rewrite the configuration layer. At the same time, a read back is performed in the background and it does not disrupt the performance. The scrubber has an optional detection phase which makes it more complex but provides a powerful mitigation. But, if the size of the configuration memory is large the detection methodology required will be very complex.

There are different scrubbing methodologies and architectures. Choosing a right methodology and architecture among them is more important based on the requirement. The methodologies can be categorised as preventive or blind versus corrective, device versus frame oriented and fixed versus adaptive. The architectures available are external versus internal, hardware versus software, and one versus N-way [110]. Figures 3.1 and 3.2 illustrate the external and internal scrubbing methodologies. Table 3.2 depicts the benefits and draw-backs of the major scrubbing methods available [110-119]. It is categorised based on the complexity of implementation and the error mitigation efficiency and quantified as low, medium, and high.

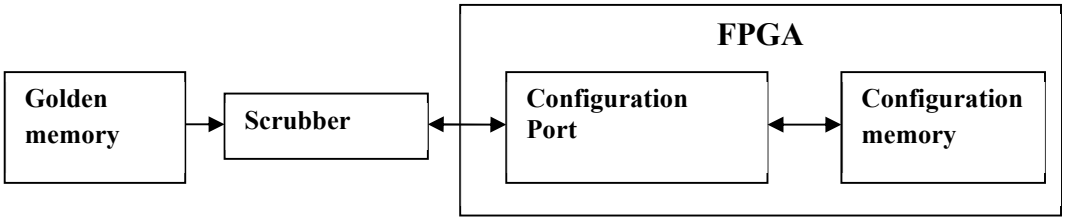



**Figure 3.1. External scrubbing**

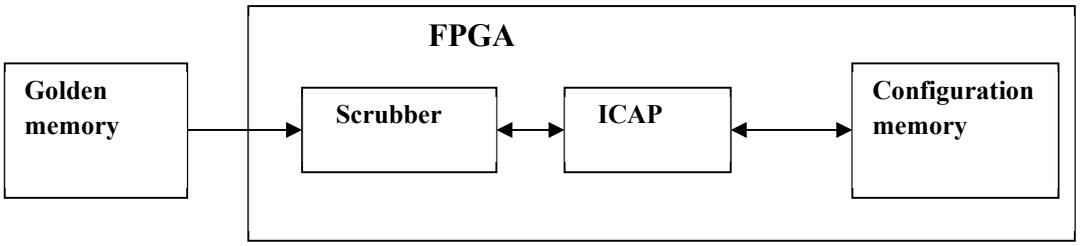



**Figure 3.2. Internal scrubbing**

### 3.1.1.3. Mitigation in routing resources

Routing fabric becomes more important in the FPGA architectures even after the advancement in the technologies [120]. The programmable routing in an FPGA can be categorised as routing within each logic block and routing between the logic blocks. Interconnect matrix connects between the logic blocks and it is the routing within the logic blocks and switch blocks. The interconnections are carried out through

programmable switches; it consists of a pass transistor controlled by a SRAM cell [121].

**Table 3.2. Comparison of scrubbing methodologies**

| Scrubbing Architecture/ Methodology | Benefits | Drawbacks | Complexity of Implementation | Mitigation efficiency |
|---|---|---|---|---|
| External Scrubbing | Scrubbing logic is protected from SEU, highly dependable | Radiation hardened auxiliary devices are required | low | High |
| Internal Scrubbing | No auxiliary devices are required | SEU can affect the scrubber logic itself | Medium | Medium |
| Hardware based | Very fast in error detection and correction | Difficult to implement complex scrubbing strategies | Complex | High |
| Software based | Flexibility and capability to implement complex algorithms | Slow | Medium | Medium |
| Scrubber coupled with TMR | Mask the soft errors during the reconfiguration | Area overhead is high (Selective hardening based on sensitivity can reduce it) | Complex | High |
| Heterogeneous CRAM Scrubbing (HCS) | Better reliability, No area, performance and power overhead | As CRAM granularity increases the improvement by HCS decreases | Complex | High |
| Fault Tolerant ICAP scrubber | Better reliability | Area overhead | Medium | Medium |

The routing resource structure is illustrated in Fig. 2.3, chapter 2. Almost 90% of the configuration bits are for routing resources. This section overviews the mitigation techniques based on different place and route algorithms and modified architectures. Table 3.3 gives the analysis of mitigation techniques for the errors affecting the routing resources [122-131]. Along with the benefits and drawbacks of the techniques, it is compared with area overhead and the mitigation efficiency.

**Table 3.3. Comparison of mitigation in routing resources**

| Methodology | Benefits | Drawbacks | Area Overhead | Mitigation efficiency |
|---|---|---|---|---|
| Reliability-Oriented Place and Route Algorithm (RoRA) | Multiple errors affecting two different connections are not possible, better SEU tolerance than TMR | Performance penalty of 22% on an average compared to TMR | High | Medium |
| Interconnection architecture with self-map property | Less area, delay and power compared to parity applied architecture | Applied only for single faults | High | High |
| By using unused programmable switches in the switch module for open errors | Reliability of the connections increased about 30% | Increases critical path delay and power consumption | Low | Medium |
| Programmable and hardwired | Increases the reliability, | Channel width and area of the | Medium | Medium |

| Methodology | Benefits | Drawbacks | Area Overhead | Mitigation efficiency |
|---|---|---|---|---|
| switch module structure for short errors | reduces the power consumption and circuit delay | circuit implemented are increased | | |
| Switch box Architecture | Decreases the probability of bridging and short errors | Increases the delay and channel width | Low | High |
| Decoder-based switch box architecture | Probability of SEU is reduced to two-third of the traditional switch box architecture | Delay overhead of 1.5% and area overhead of 3% in comparison with traditional switch architecture | High | High |
| Asymmetric SRAM cell (ASRAM) | Reduces the Failure In Time | Only suitable for bridging errors | Low | Medium |
| Asymmetric SRAM cell (Refreshing SRAM) | Completely hardened for 0 to 1 flip and very less FIT for 1 to 0 flip | Area overhead | High | High |
| Evolutionary method based on Genetic Algorithm (GA) and Particle Swarm | More than 35% reduction on Soft Error Rate compared to the versatile Place and Route Counter parts | Critical path delay and total wire length increased | Medium | Medium |

| Methodology | Benefits | Drawbacks | Area Overhead | Mitigation efficiency |
|---|---|---|---|---|
| Optimisation (PSO) | | | | |

### 3.1.1.4 Mitigation in logic resources

The popular techniques for error detection in the logic resources are dual modular redundancy (DMR) and triple modular redundancy. DMR technique uses two replicated logic blocks or two diverse blocks which perform the same functionality with a comparator logic at the output which detects any anomaly. This technique is mainly preferred for error detection. DMR technique can be used with partial reconfiguration to achieve error detection and correction [71]. A k-input look-up-table (LUT) can implement any function with k inputs and it acts as a function generator. The truth table of LUT and selection line values of multiplexers is stored in the configuration memory. The logic resources structure is illustrated in Fig 2.2, chapter 2. A logic error can lead to flip in one of the entries of the LUTs, which alters the functionality of the mapped logical function. Table 3.4 gives the comparison of the mitigation techniques in logic resources [132-138]. The techniques are rated based on the area overhead and error mitigation efficiency.

### 3.1.1.5. User memory SEU mitigation techniques

The current state values of the application implemented in FPGAs will be in flip flops and on-chip memories. The combinational logics will be implemented in LUTs, Multiplexers and carry logics. The sequential logics will be in latches and

flip-flops. The control parts of most FPGA-based designs are built by Finite State Machines (FSM) which are implemented mostly in LUTs and flip-flops. Any bit-flips due to Single Event Effects (SEE) in FSMs can adversely affect the performance and reliability of the overall system. The techniques used for mitigating SEUs in combinational and sequential circuits implemented in FPGAs are illustrated in Table 3.5.

**Table 3.4. Comparison of mitigation in logic resources**

| Methodology | Benefits | Drawbacks | Area overhead | Mitigation efficiency |
|---|---|---|---|---|
| Error Detection with Remap (EDR) and Error Correction with Remap (ECR) | Capable of detection and correction of 96 % of errors, less area than DWC and TMR | TMR with single voter gives better percentage of error detection and correction | High | Medium |
| In-Place Decomposition (IPD) | Robust against SEU without any area and timing overhead | Does not tolerate faults on interconnect configuration bits | Low | Medium |
| In-Place X-filling (IPF) | Mask the errors in LUT and interconnect configuration bits | Finding correlation between errors is the difficult part to extend it to multiple errors | Medium | High |
| In-Place Reconfiguration (IPR) | Reduces the fault rate and area with preserving the function and topology of the logic network | Algorithm works mainly for single fault, pre-layout ROSE and post-layout IPR gives better reliability | Low | Medium |

**Table 3.5. Comparison of mitigation in the user memory**

| Mitigation Techniques | Mitigation efficiency |
|---|---|
| Mapping of FSM into Synchronous Embedded Memory Block (SEMB): it enhances the runtime reliability [139, 140]. | Medium |
| Duplication with self-checking and Triple Modular Redundancy [141]. | High |
| Duplication with comparison (DWC) and concurrent error detection (CED [142]. | Medium |
| Automatic recovery of Single bit errors using Hamming Code [143]. | Medium |
| SEC with Single Independent Decoder block (architecture SID), Distributed Error Correction (architecture DEC), UPset oriented SID (UPS) and Upset-oriented DEC (UPD) [144]. | Medium |
| CED for finite state machines implemented using embedded memory blocks of FPGAs [145]. | Medium |
| Increase the sequential circuit reliability by adding redundant equivalent states to the states with a high probability of occurrence [146]. | High |
| TMR architecture, Duplex architecture, Explicit Error Correction architecture, Modified EEC and Implicit Error Correction [147]. | High |
| A design methodology for realizing Total Self-Checking VLSI systems derived from a VHDL description. Algorithm based on heuristic; state encoding is explained in [148]. | High |
| Temporal Data Sampling: this stage helps to store data samples at different time intervals, these samples are compared with each other to decide whether the data is error free or not [149]. | Medium |
| Redundancy Addition and Removal (RAR) [150]. | Medium |
| Selective Voltage Scaling (SVS): the same amount of charge disturbance produces a smaller (less harmful) SET at gates with high supply voltage than at gates with low supply voltage [151]. | Medium |

| Mitigation Techniques | Mitigation efficiency |
|---|---|
| Clock Skew Scheduling: adjusts the arrival times of clock signals to memory elements to reduce the probability of capturing transient pulses [152]. | Medium |
| Synthesis of sequential circuits based on decomposing the embedded memory in to two; a combinational address modifier and a smaller memory block [153]. | Low |
| Built-in self-test (BIST) design technique supports self-test of a circuit and BIST controller coordinates the operations of different blocks of the BIST [154]. | Medium |
| Error Correction Code (ECC) and Triple Module Redundancy (TMR) [155]. | High |
| Non-concurring error detection, identification and correction by choosing the proper encoding technique and redundant dynamics [156]. | Low |

### 3.1.2. Summary

Dependable system design in SRAM based FPGAs for terrestrial applications face more challenges from radiation-induced soft errors than hard errors. Due to the susceptibility of SRAM based FPGA resources to radiation effects, it is necessary to implement the designs with fault-tolerant techniques to achieve the dependability. The ECCs like Hamming codes are mainly used for SEU mitigation in the configuration memory. So, it is proposed to use other coding techniques which are used for protecting the memories and in the communication, field could also be utilised for SEU mitigation by coupling with PR for better error detection and correction. Scrubbing is one of the efficient techniques for SEUs in the configuration memory. Among the scrubbing methodologies, external-hardware scrubber gives better error mitigation efficiency but

it is difficult to implement complex error correction algorithms in hardware. Therefore, it is proposed to have a hybrid hardware/software scrubber with selective masking of configuration bits by frame level redundancy or block level redundancy. Using ASRAM cells can harden the configuration memory against SEUs. In the ASRAM cell, the design is asymmetric with respect to the transistor threshold voltage ($V_t$). But in RSRAM, once the data are written in the cell, the pass transistor which is connected in the feedback line is turned off using a refreshing signal and turned on only for a very short time to maintain the charge stored at the cell nodes. Even though the ASRAM cells give better reliability for bridging errors, it is not suitable for open errors in the routing. The switch module architecture which utilises the unused switches to provide alternative paths between switch terminals works efficiently against the open errors in the routing.

The replacement of some of the switches in the switch module with hardwired nets is suitable for short error mitigation. The programmable switches in the switch box are the main cause of errors; the architecture which eliminated some of the programmable switches increasing the reliability by mitigating bridging and short errors. A place and route algorithm based on GA and PSO reduces the number of used programmable switches as well as configuration avoidance, and thus reduces the soft error rate. By decoding the configuration bits in the switch boxes, the number of bits required for programming the switch box is reduced by 67% without any impact on the routing capability of the switch box. The architecture does not require any modifications of the existing place and route algorithms. Resynthesis algorithm (ROSE) changes the topology of the LUT-based logic network which limits the applicability in the overall system design flow. However, in IPR the function and

topology are preserved. Both techniques use logic masking/redundancy to minimise the effect of SEU. IPD does the decomposition within the logic block itself, therefore and there is no overhead on area and timing in the logic block level. Even though ROSE, IPD, and IPR give better mitigation capability in LUTs, IPF improves overall system reliability by mitigating SEUs in the LUTs and interconnect resources.

The complete knowledge of structure (transistor level) and the bitstream of modern SRAM-based FPGAs makes it easy for implementing design techniques for dependable application development in FPGAs. The prediction of SEU sensitivity of each bit in the bitstream to the place and route algorithm can improve the dependability of the system design. This section of the chapter discussed the SEU mitigation techniques only for the configuration memory. To achieve the overall system reliability, it's necessary to consider the usage of techniques like redundancy, parity coding etc., for user memory too.

## 3.2. DEVELOPMENT OF GOLAY CODE BASED ERROR RECOVERY MECHANISM

From the literature review, it is found that single error corrections codes are mostly used for configuration memory error mitigation. If an error correction code which can correct more than a single error can extend the time duration between two partial/full reconfigurations. In terms of error detection and correction capability, the Golay code and the extended Golay code are better than other error correction codes available for SEU mitigation in the configuration memory of FPGAs. So, an error recovery mechanism for configuration memory based on extended Golay code has been proposed.

### 3.2.1. Golay Code for SEU Mitigation

Linear block codes are generally defined in terms of generator and parity check matrices. It is represented as (n, k, d) codes, where n is the codeword length, k is the information bits and d is the minimum distance. The information bits are divided into blocks of message bits with a fixed length. Message blocks are indicated as m, which contains k information bits. Golay code (23, 12, 7) is the only nontrivial binary block code other than hamming code. There is a metric called Hamming distance for comparing two binary strings of equal lengths, it is the number of bit positions in which the two bits are different. Among a set of strings with equal lengths, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of strings in that set [157]. Error correction involves detection and correction of errors. Golay code (23,12,7) code has a minimum distance of 7 and it can correct any combination of three errors or fewer random errors in a block of 23 digits. The Golay code can be extended by placing an overall parity check bit to each codeword. The extension results in Golay code (24, 12, 8) with a minimum distance of 8, this code is capable of correcting three or fewer errors and detecting all error patterns of four errors [158-159].

The binary codes are constructed by using a Galois field (GF) and it is denoted as GF (2) for a binary field [160]. The possible generator polynomials over GF (2) for Golay code (23, 12, 7) are x11 + x10 + x6 + x5 + x4 + x2 + x1 and x11 + x9 + x7 + x6. The generator matrix in its systematic form can be written as, G = [ P I12], where I12 is the identity matrix of dimension 12 and P matrix is as given below:

$$\begin{vmatrix} 1&0&0&0&1&1&1&0&1&1&0&1 \\ 0&0&0&1&1&1&0&1&1&0&1&1 \\ 0&0&1&1&1&0&1&1&0&1&0&1 \\ 0&1&1&1&0&1&1&0&1&0&0&1 \\ 1&1&1&0&1&1&0&1&0&0&0&1 \\ 1&1&0&1&1&0&1&0&0&0&1&1 \\ 1&0&1&1&0&1&0&0&0&1&1&1 \\ 0&1&1&0&1&0&0&0&1&1&1&1 \\ 1&1&0&1&0&0&0&1&1&1&0&1 \\ 1&0&1&0&0&0&1&1&1&0&1&1 \\ 0&1&0&0&0&1&1&1&0&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{vmatrix}$$

The P matrix is symmetrical with respect to its diagonal, the ith column is the transpose of ith row and the sub-matrix obtained by deleting the last row and column is formed by circularly left shifting the first row 11 times. If we form a 23-bit codeword and cyclically shift it any number of bits the result is also a valid Golay code. This feature is known as cyclic invariance. Similarly, if we invert the codeword the result is also a codeword [161].

The parity check matrix, $H= [I_{12}\ P^T]$

The codeword is computed by performing multiplication of generator matrix and message bits.

$V = m * G$

Where V = 24 bits codeword

m = 12 bits message

G = generator matrix

Correctable error pattern for Golay code (24, 12, 8) can be expressed in terms of P, pi, u(i) and S,where pi indicates the $i^{th}$ row of P and u(i) is the 12 tuple in which the $i^{th}$ component is non-zero. Let e = (x, y) be an error vector, where x and y are binary 12-tuples. Suppose a codeword v is transmitted and correctable error pattern e = (x, y) occurs, then the received vector is r = v + e.

Any correctable error pattern with weight w (e) ≤ 3 will have the following four possibilities [160],

(i) w (x) ≤ 3 and w(y) = 0,

(ii) w (x) ≤ 2 and w(y) = 1,

(iii) w (x) ≤ 1 and w(y) = 2,

(iv) w (x) ≤ 0 and w(y) = 3.

A decoding algorithm which can detect and correct up to 3 errors is explained below [158]:

Step 1 Compute the syndrome S of the received bits r

Step 2 If w (S) ≤ 3, then set e = (S, 0) and go to step 8

Step 3. If w (S + pi) ≤ 2 for some row pi in P, then set e = (s + pi, u(i)) and go to step 8

Step 4. Compute S. P.

Step 5. If w (S. P) = 2 or 3, then set e = (0, S. P) and go to step 8

Step 6. If w (S. P + pi) = 2 for some row pi in P, then set e = (u (i), S. P + pi) and go to step 8

Step 7. If the syndrome is not matching with any of the correctable error pattern, halt the decoding process, or request for retransmission.

Step 8. Set the decoded codeword v* = r + e and stop.

The error trapping ability of the code refers to the ability to prediction, finding and fixing of errors. If error correction is not considered, the error-detection-only properties, per 24-bit extended Golay codeword includes i) 100% of one- to six-bit errors detected, ii) 100% of odd bit-errors detected and iii) 99.988 %of other errors detected [161]. The error correction facilities of the code explained above have the data reliability rates of i) 100% of one- to three-bit errors corrected, any pattern, ii) 100% of four-bit errors detected, any pattern, iii) 100% of odd numbers of bit errors detected, any pattern and iv) 0.24% of other errors corrected (1/4096) [161].

### 3.2.2. Implementation of Error Recovery Mechanism

Golay code has not been used for SEU mitigation so far. However, the extended Golay code can detect four errors and can correct up to three errors which can be utilized for SEU mitigation in the configuration memory of FPGAs. Internal configuration memory readback and error correction technique have to be used for implementing this recovery mechanism. A basic block diagram of Golay implementation is depicted in Fig 3.3 The configuration bitstream is stored in external memory and this is also called as a golden memory. While configuring, the frame bits are split into blocks of 12 bits and the Golay code encoder generates its equivalent codeword. The parity bits in the code words are stored in the BRAM memory.
The configuration memory frames can be readback and rewritten by Internal Configuration Access Port (ICAP). Golay decoder does the error detection and

correction process and the overall mechanism is controlled by the control logic, which is based on a finite state machine. The advantage of using this technique is up to three errors in any of the 12 bits of each frame in the configuration memory. If the number of errors exceeds three it has to undergo partial reconfiguration or full reconfiguration from the external golden memory. The disadvantage of this technique is the error recovery mechanism implemented can also be affected by the radiation and can cause SEUs within the recovery mechanism.

### 3.2.2.1. Control logic for error recovery mechanism

The proposed control logic state diagram is shown in Fig 3.4. Whenever the device is configured or reconfigured,the encoder will generate the parity bits and store in the memory. Once the encoding process is ompleted, the control logic will initiate the readback process. After every readback, the error detection process will be executed. If there is at least one error it will be corrected and written back to the memory. If the number of errors are more than three, partial reconfiguration will be initiated.

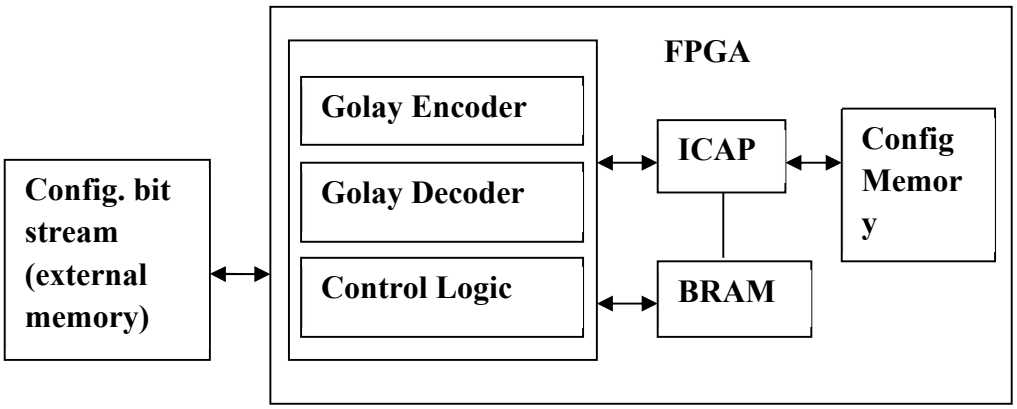



**Figure 3.3. Error recovery mechanism using Golay code**

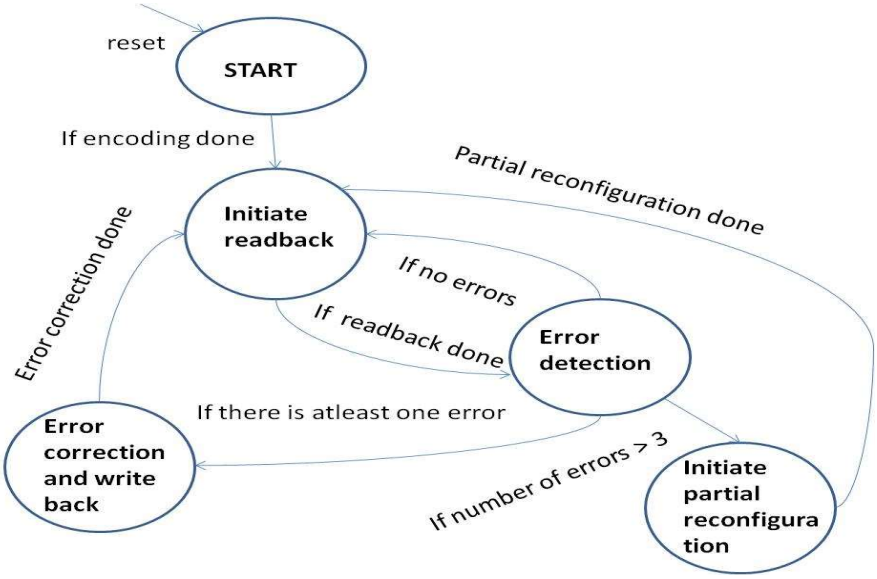



**Figure 3.4. Control logic state diagram**

### *3.2.2.2. Golay encoder and decoder implementation*

The proposed encoding procedure is described as follows

1. The input bits are multiplied with the generator matrix to find out the codeword.
2. All the rows of P matrix are combined to form a 144 bits array as the $i^{th}$ row and $i^{th}$ column of the generator matrix are same.
3. The inputs are bitwise AND with first 12 bits of the array and XOR all the bits to find the first parity bit.
4. Likewise repeat the process with next 12 bits of the array and so on.
5. Codeword is generated by appending the parity bits with the message bits.

The basic architecture of the implemented extended Golay code encoder is depicted in Fig 3.5.

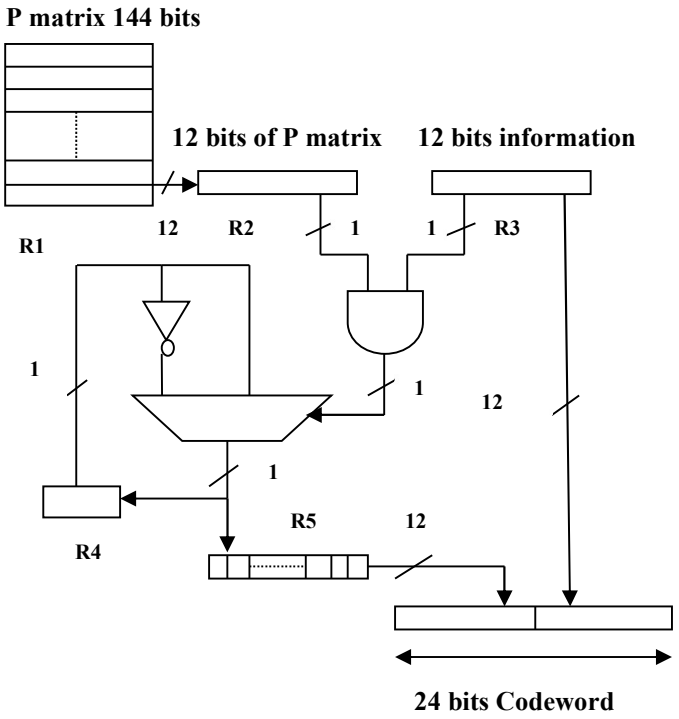



**Figure 3.5. Golay encoder architecture**

The iteration steps are not included in the architecture. The design has a latency of 12 clock cycles and having a throughput of output at every clock cycle. The decoder architectute is adopted from [158] and the proposed arhiteture has a latency of 27 clock cycles with a better throughput which generate outputs at every clock cycles.

### 3.2.3. Summary

Golay codes are mostly used for data transmission in digital communication. We brought this technique in to the application of mitigating SEUs in the configuration memory of FPGAs. The proposed extended Golay code based error recovery mechanism can correct up to three errors. So, this method can extend the time between partial reconfiguration. As the area overhead is high, this technique shall be used only for the critical or sensitive memory bits.

## 3.3. COMPARISON OF RHBD FPGAs WITH NON RADIATION HARDENED COTS FPGAs

There are many hurdles for using the radiation-hardened by design (RHBD) FPGAs in NPP applications. Considering the Indian scenario, there are also legal issues to use RHBD devices and the required toolsets in NPP applications. Along with that such devices are highly expensive. So we are forced to harden the devices that need to be deployed in the radiation environments. In this section, a comparison on commercially available RHBD FPGAs and the non-radiation hardened commercial off-the-shelf (COTS) FPGAs hardened by the design aspects implemented by the user is provided. For the analysis purpose, we have considered Xilinx Virtex 5QV FPGA and Xilinx Spartan 6 FPGA. The available space grade FPGAs from Xilinx are Virtex 4QV of 90 nm and Virtex 5QV of 65 nm process technology. This thesis does not attempt a quantitative comparison of the SEU susceptibilities of Xilinx Virtex 5QV and Xilinx Spartan 6 FPGAs. The comparisons aimed to give an insight that even though the majority of the building blocks of RHBD FPGAs are tolerant to radiation effects, a few blocks are still susceptible to radiation effects irrespective of the process technology.

Even though Virtex 5QV is fabricated with dual node configuration cells, 12 transistor flip flops and epitaxial CMOS process technology [162], many other components in this FPGA require mitigation by user design aspects. BRAM cells in Virtex 5QV are susceptible to radiation effects as in Spartan 6 FPGAs [163]. Also, the dynamic reconfiguration port (DRP) bits such as DCM, PLL and GTX bits in Virtex 5QV are as susceptible to radiation as in Spartan 6 [163, 164]. Table 3.6 gives a comparison of the radiation susceptibility of the blocks in Virtex 5QV and Spartan 6 FPGAs. The

mitigation techniques discussed in this chapter for the configuration memory cells can provide a better hardening for the unhardened blocks in Spartan 6 FPGA. The advantages and disadvantages of external and internal scrubbing techniques used for mitigation in COTS FPGAs are applicable for Virtex 5QV FPGAs also. We can very well use the commercial off the shelf (COTS) SRAM based FPGAs for NPP applications by taking a few measures in the design aspects.

**Table 3.6. Comparison of Susceptibility to Radiation Effects on Virtex 5QV and Spartan 6 FPGAs**

| | Xilinx Spartan 6 FPGA | Xilinx Virtex 5QV |
|---|---|---|
| Logic Cells | Susceptible to radiation | Radiation hardened |
| LUTs and FFs | Susceptible to radiation | Radiation hardened |
| BRAMs | Susceptible to radiation | Susceptible to radiation |
| Dynamic Reconfiguration bits in PLL, DCM, GTX, etc | Susceptible to radiation | Susceptible to radiation |

# 4

# ANALYSIS OF VERIFICATION SOLUTIONS FOR THE DESIGNS USED IN REACTOR APPLICATIONS

*This chapter investigates the non-suitability of the design and verification techniques available in the literature as well as commercially available solutions and their shortcomings for reactor applications. Subsequent sections explain the verification of the efficiency of fault-tolerant techniques and the development of simulation-based fault injection technique.*

## 4.1. VERIFICATION APPROACHES FOR THE DESIGN

In general, system designers prefer proven and reliable device technologies as well as design and verification methodologies for reactor applications. Verification of a design, is to check whether the system meets a set of design specification or not [91]. Verification proves the design meets the specification. Verification can be achieved by simulation or emulation techniques. While, validation of a design is, to check whether the system meets the operational needs of the user or not. Validation proves the design and specification meet the purpose. FPGA based prototyping and virtual prototyping are validation techniques [91, 165].

Widely preferred hardware description languages in industries are VHDL (IEEE 1076-2008 std.) and Verilog (IEEE 1364-2005). Both the languages support

design and verification of FPGA/ASIC based digital systems. VHDL is mostly preferred in this thesis since it is a strongly typed and deterministic language. As a result, the codes written in VHDL are considered as self-documenting and helps to catch errors in the initial stages of the design [166]. The designers and verification engineers can choose any of the available languages among Verilog, VHDL, System Verilog, Blue-spec System Verilog, System C, etc., as per the convenience and applications. Verilog is a C like syntax language and it is deterministic as well. In recent times System Verilog (IEEE 1800-2012 std.) is preferred over Verilog and VHDL as this combines the features of both and it is becoming the best hardware description and verification language [166]. Blue-spec is a rule-based language where hardware is described as object-oriented modules. Usage of Blue-spec requires expertise because the complexity of hardware clock-cycles, data movement and concurrency are exposed to the designer [167]. System C (IEEE 1666-2011) is not preferred in hardware design but it is one of the best languages for verification and high-level modelling.

As we don't have much history of failure information of FPGA based systems in nuclear reactor applications, we are considering the failures reported in space applications. Most of those failures reported were due to inadequate development and verification approaches [168-170].

For reactor application, two things are necessary: a) verification in a simulator and b) in target validation on hardware. ECSS-Q-ST-60-02C standard recommends the additional requirements related to the faults generated due to radiation. Handling of errors and testing of devices in the radiation environment to verify and validate the radiation hardening mechanism are also important.

The available tools are lacking for error injection and the error injection ports are the responsibility of intellectual property (IP) designer. Most of the third-party IPs is developed for general purpose and hence, so there will be many hidden unwanted functionalities. These cause difficulty in predicting the reliability of the system. So, it is necessary to custom design each IP according to the specific requirements of reactor applications giving provision for testing. The same for design solutions are applicable for verification solutions. A general solution to test error scenarios is missing in the readily available solutions.

Single event upset is one of the major challenges being faced by the designers and developers while implementing dependable systems in SRAM based FPGAs. Soft errors can affect almost all the resources of these FPGAs. Error mitigation techniques are necessary to ensure the reliability of the implemented design functionality. Assessing the efficiency of those implemented mitigation techniques is also important. To evaluate the sensitivity of the design to SEUs, the design has to be verified thoroughly either at simulation level or validated at the FPGA level on the test board. This entails the use of fault injection methodology. There are techniques reported in the literature. However, most of the techniques are not commercially available. So, it's necessary to have a simple technique to inject fault at the RTL and netlist levels of abstraction.

In the following section verification solutions for the design and fault-tolerant techniques are explained.

### 4.1.1. An Overview of Fault Injection Techniques

Fault injection is well documented in the literature as a verification/validation technique for characterizing the reliability of HPDs. VHDL-based Evaluation of Reliability by Injecting Faults efficiently (VERIFY) introduces a new way for defining the behavior of hardware components in case of faults by extending the VHDL language with fault injection signals together with their rates of occurrence [171]. Autonomous Multilevel emulation-based fault injection for Soft Error Evaluation (AMUSE) is a method that can inject SET faults by integrating both Register Transfer Level (RTL) and netlist level [172]. An easy to develop and flexible FPGA fault injection technique which utilizes the debugging facilities of Altera FPGA in order to inject SEU and MBU fault models in flip-flops and other memory units is presented in [173]. Another technique based on simulator commands, saboteurs and mutants are presented in [174]. There are many other simulation/emulation or hybrid fault-injection tools and methods available which include a method/tool called NETFI (NETlist Fault Injection). It can inject fault in any HDL model, VHDL, Verilog etc. [175].

### 4.1.2. Design and Development of Fault Injection Method

The major challenge in any fault tolerant design technique is the methodology used for verification or validation for quality assurance of the final product. The methodology used is often too complex and customized to be used across a substantially big project with multiple designs with different specifications. We propose a simple fault injection technique that is developed based on the TCL script can verify the designs in the design entry-level and synthesized netlist level. The proposed methodology parses a design in a guided or automated manner selecting sensitive nodes

where the fault is to be injected and generating a TCL script for the same. The "force –freeze" command is used to change the value of any signal/wire. The value can be made stuck or frozen at either '1' or '0' for any particular period of time. For example; "force -freeze sim:/test_prep3/I1/CURRENT_STATE(7) 1 {200 ns} -cancel {250 ns}" stuck the value of 7th bit of register CURRENT_STATE as '1' for a duration of 50 nanoseconds.

The process of generating the TCL file containing the fault injection is automated and can be coded in Perl/Python/.net or any other suitable language. The algorithm proposed here parses and finds the nodes with maximum fan-out, so a single injected fault caused maximum damage to the functionality of the design.

As shown in the Fig. 4.1, the verification setup consists of a self-checking assertion based test bench which is used for generating the stimulus and counting the number of errors. If there is any mismatch in the values than the expected, fault counter counts an error.

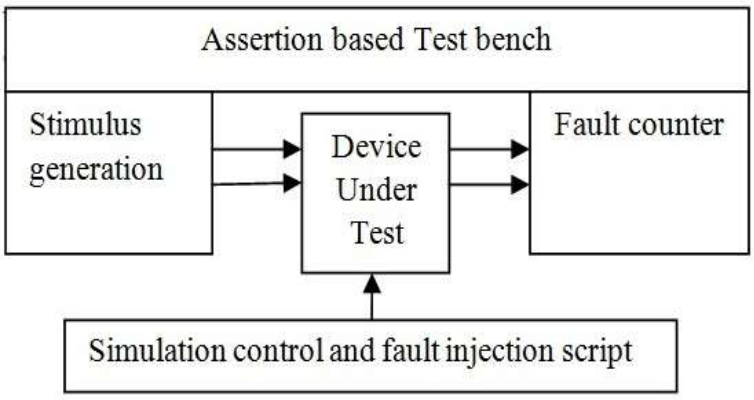



**Figure 4.1. Verification setup block diagram**

For indication purposes only, the fault is injected at the netlist level, particularly focused on state registers of the FSM as the target FPGA is only sensitive to SEUs at

the register level. The methodology developed is flexible to inject faults at any technology FPGAs. Simple designs have been taken up for proving the effectiveness of the methodology.

### 4.1.3. Verification of Fault Tolerant Techniques using Simulation Based Fault Injection

Once the single event upset is generated it will be propagated through the registers (i.e., flip flops) to affect the functionality of the system implemented. In this section, the way the propagated SEUs affect the system is studied using the developed fault injection method. Also, assessed it's the improvement in the efficiency of the system after implementing fault-tolerant techniques.

#### 4.1.3.1. Synthesis and simulation results

The control parts of most FPGA based designs are built by FSMs and any bit-flips due to SEEs in FSMs can adversely affect the performance and reliability of the overall system [176]. PREP3 benchmark was taken up as a primary benchmark for initial analysis followed by PREP4 and two other general designs. The PREP3 is a mealy state machine with eight inputs and eight outputs, which has eight states and twelve transitions. PREP4 is a large mealy FSM with 16 states and 43 transitions. The parameters such as increase in the percentage of resource utilization and the decrease in timing performance are compared to the parameters of normal design are shown in the Fig. 4.2 and Fig. 4.3 respectively. The increased area for Hamming code, when compared to TMR is attributed to the fact that TMR is implemented for the state registers only, not the entire combinational logic part of the design. Safe FSMs also

show a marked increase in resource utilization and is a major reason why synthesizing tools remove the excess logic associated unless the 'safe' attribute for FSM is used. The reduction in frequency is maximum for Hamming-3 implementation. So, it is noted that TMR method is superior when compared to the other two in terms of resource utilization and timing while Hamming will have an advantage of indicating and correcting single bit error in state registers which can be used to take the FSM to a safe state.

The value of the state register is changed from '1' to '0' or '0' to '1' for particular time periods and the number of errors generated due to the injected fault is measured by the self-checking assertion based test bench simulating the netlist file. This is repeated for all the netlist files which are generated after implementing the fault tolerant techniques and the results are analyzed. The technique developed can be suitably modified to parse the netlist files and pick up random signals/nets for fault injection and checking.

Fig. 4.4 shows the simulation waveform of PREP3 FSM after injecting fault in the state and output registers randomly. Total of 24 faults injected into the signals CURRENT_STATE(7) to CURRENT_STATE(0) and OUTT_I_C(7) to OUTT_I_C(0) in random time intervals and which generated 20 errors.

Fig. 4.5 shows the waveform for TMR. Faults are injected to the state and output registers of one of the TMR logic blocks. It uses 2 out of 3 voting logic and so it has corrected all the faults injected in one TMR block. The fault injected in more than one TMR logic block and voting logic cannot be corrected by TMR method. This was analysed and verified by injecting fault in these blocks.

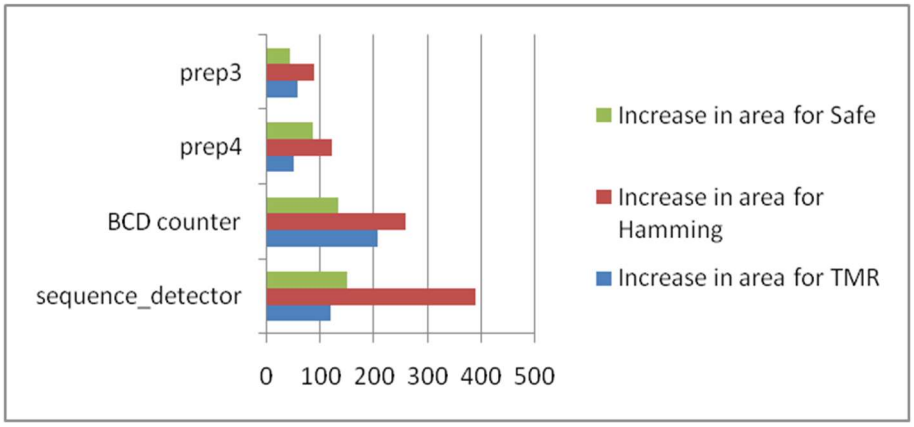



**Figure 4.2. Resource utilization increase in percentage.**

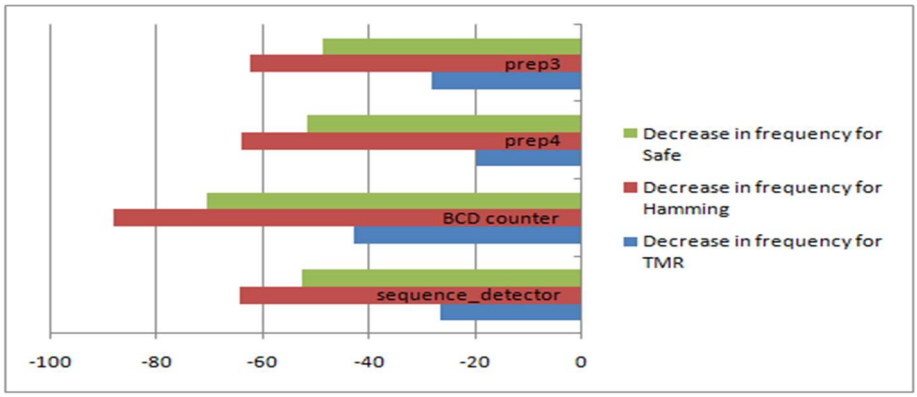



**Figure 4.3. Maximum frequency reduction in percentage.**

As shown in Fig. 4.6. a fault is injected in one of the state registers i.e., CURRENT_STATE_DUP(7), by forcing the value of the register to high from 100 ns to 150 ns which leads the FSM to an unreachable state. The safe FSM implementation forced the state machine into a reset state.

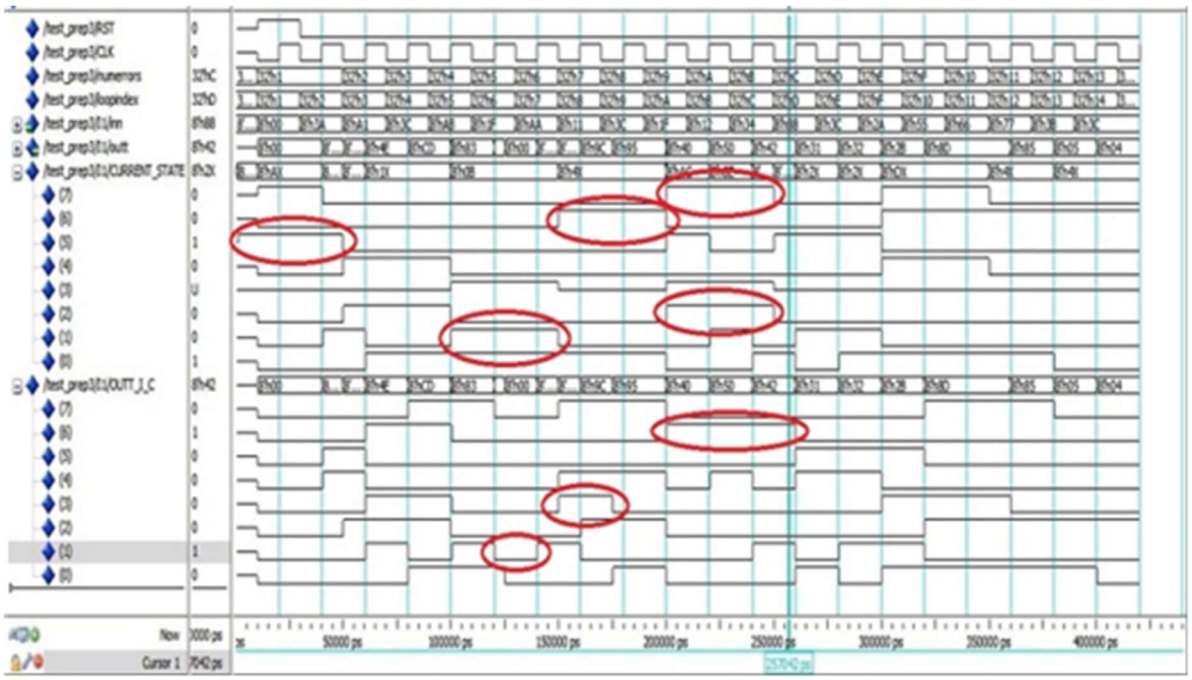


**Figure 4.4. The Waveform of fault injection without using any fault tolerant methods**

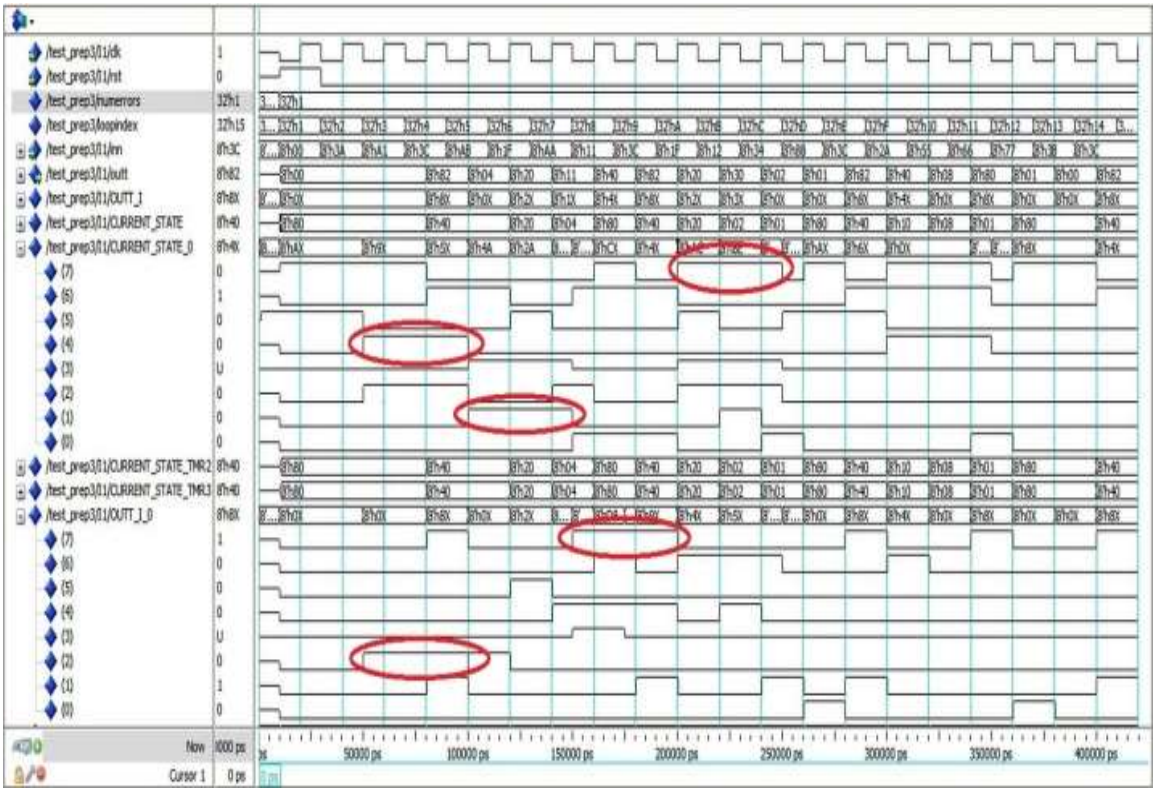


**Figure 4.5. The Waveform of fault injection in one of the TMR logic**

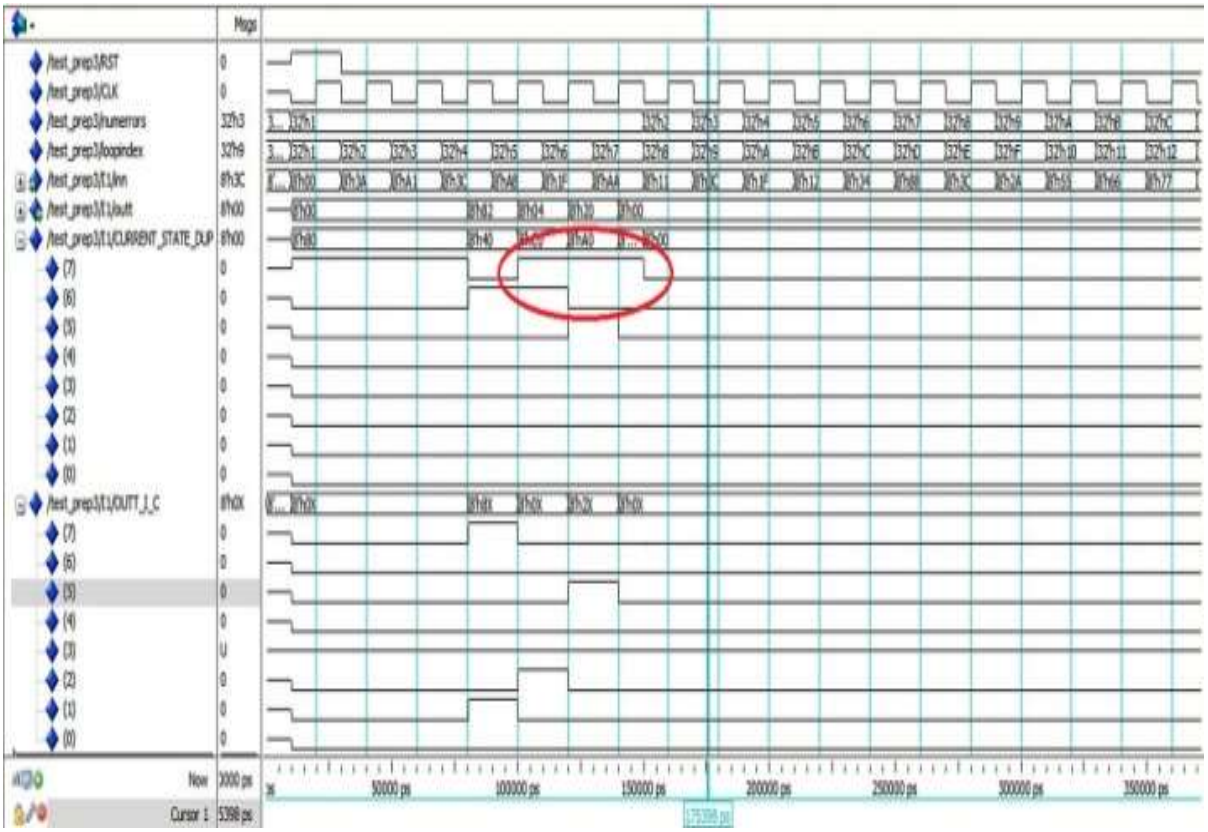


**Figure 4.6. The Waveform of fault injection after implementing safe FSM**

It is found that the TCL scripting based fault injection tool could able to inject any number of faults at netlist level efficiently. From the data it is concluded that TMR gives the best performance in terms of area and timing. Hamming-3 encoding shall only be used when the probability of single bit upset exists and safe FSM implementation takes the FSM to a fail-safe state when an invalid state occurs.

### 4.1.4. Emulation Based Verification of Fault Tolerant Techniques

#### 4.1.4.1. Fault injection by VHDL code modification

This section explains the analysis of error mitigation techniques like triple modular redundancy and duplication with compare (DWC). These methods are verified with simulation and validated with emulation techniques. The design is implemented

with fault tolerant techniques, both coded in VHDL and the fault injection for analysis is done by HDL code modifications. The bitstream generated is loaded into an FPGA evaluation board. The fault injection is controlled by a DIP switch and the performance is analyzed using ChipScope analyzer.

The design used for the analysis purpose is a 4-bit counter circuit and the techniques like TMR and DWC are applied in the design. A flag force_in is introduced in the design coding itself for controlling the fault injection. When the fault injection flag has triggered, the fault in the form of stuck at ‘1' or ‘0' will be activated in the design. For verification by simulation, the force_in signal is activated in the test bench for a particular time period and the changes in the design are analyzed. In Fig. 4.7, the waveform of fault injected in one of the DWC logic is shown. The error flag monitors the error and counter gives the erroneous output.

If the fault is injected only in one of the TMR logics, it will not affect the functionality of the circuit. As shown in Fig. 4.8, force_in signals are made zero for a particular time period between 100 ns and 200 ns, there is no error generated and also no effect on the counter output.

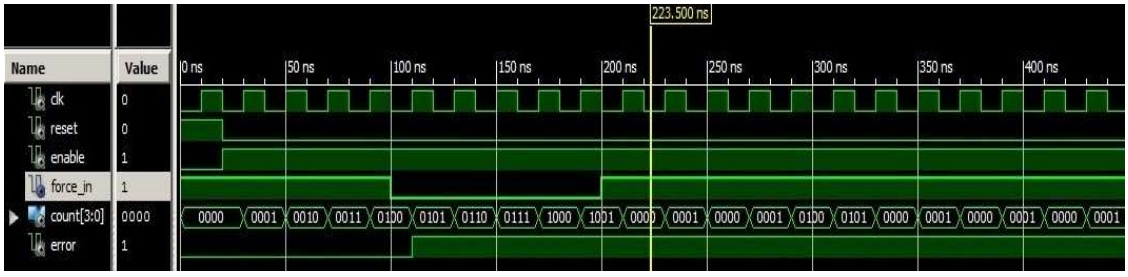



**Figure 4.7. The waveform of fault injected in one of the DWC logic**

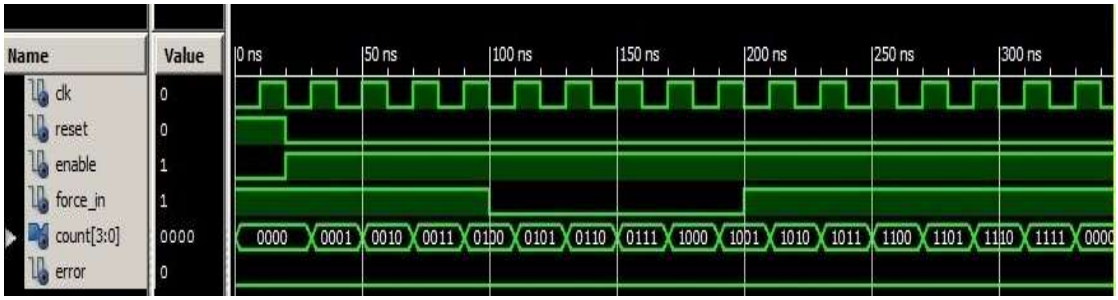



**Figure 4.8. The waveform of fault injected in one of the TMR logics**

The fault injection in either two or more than two TMR logics affects the functionality of the circuit. The waveform shown in Fig. 3.14 generates error flag and the changes in the desired counter output values can be seen.

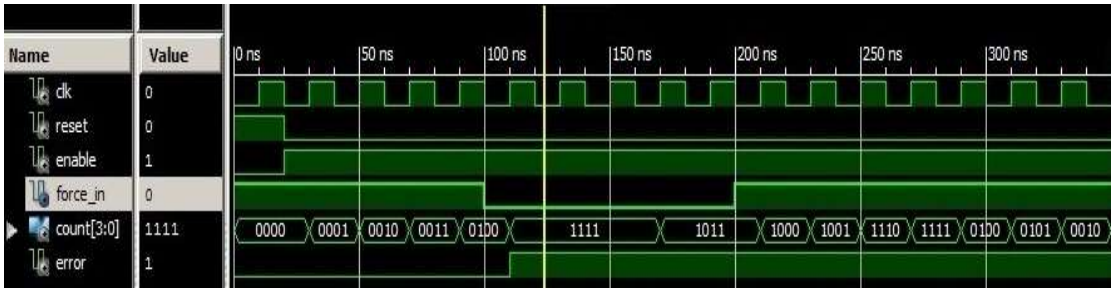



**Figure 4.9. The waveform of fault injected in two of the TMR logics**

### 4.1.4.2. Evaluation of SEU mitigation technique by emulation

It is important to validate the soft error mitigation techniques which are verified by fault injection-based simulation. The bitstream generated is loaded into the Xilinx Spartan 6 FPGA residing in SP605 evaluation board. In post-synthesis, I/O pin planning, the fault injection control flag force_in is assigned to a DIP switch. This enables us to inject faults while the design is running in the FPGA. The test setup is shown in Fig. 4.10 which includes a computer with Xilinx ISE design suite having ChipScope Pro analyzer and SP605 evaluation board.

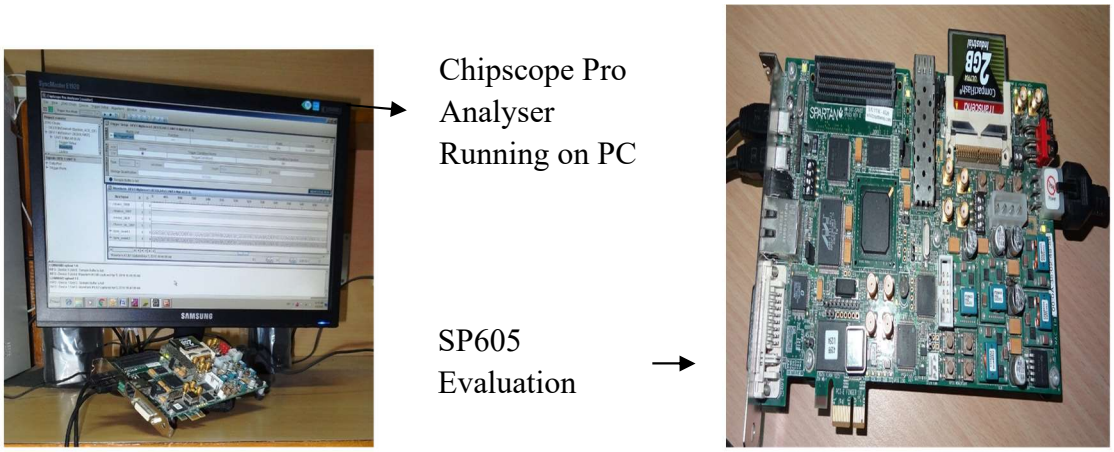



**Figure 4.10. Emulation test setup**

The communication between the computer and the evaluation board is through the JTAG interface. After the bitstream is loaded into the FPGA, the fault is introduced by DIP switch and the variations in the circuit are analyzed using ChipScope analyzer. The error flag is assigned to a LED residing on the evaluation board. Whenever there is an error, the LED glows. In Fig. 4.11, the operation of the counter circuit implemented with DWC (with no fault introduction) is shown.

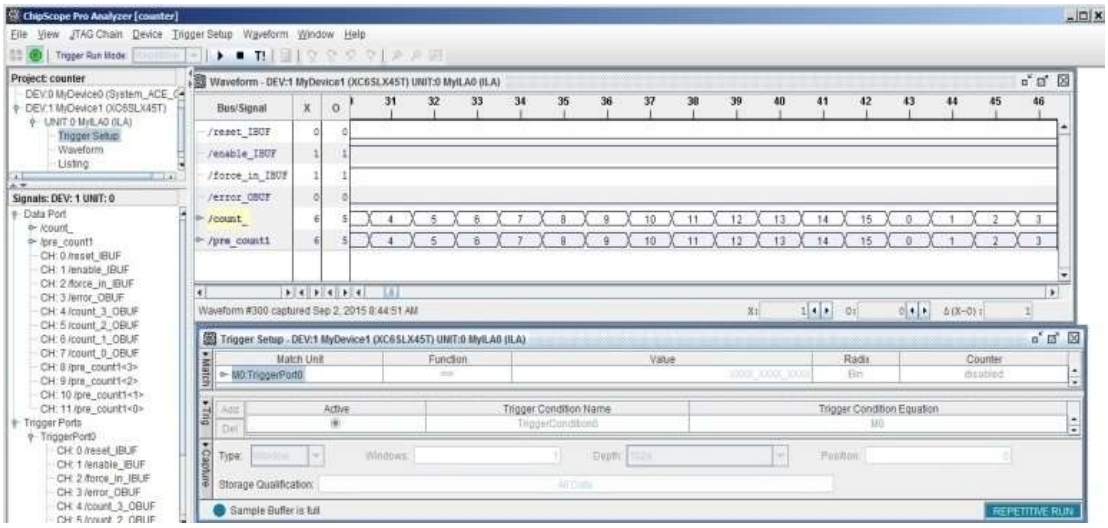



**Figure 4.11. Waveform of DWC implemented without any fault injected**

When we enabled the fault injection through the DIP switch, an error is generated in the design and error monitor LED glows. TMR masks the error if there is a fault in any one of the three TMR logic blocks. If there is an error in more than one TMR logic block or in the voting logic then the functionality of the system will be affected. In Fig. 4.12, fault injection into two of the TMR logic blocks is shown.

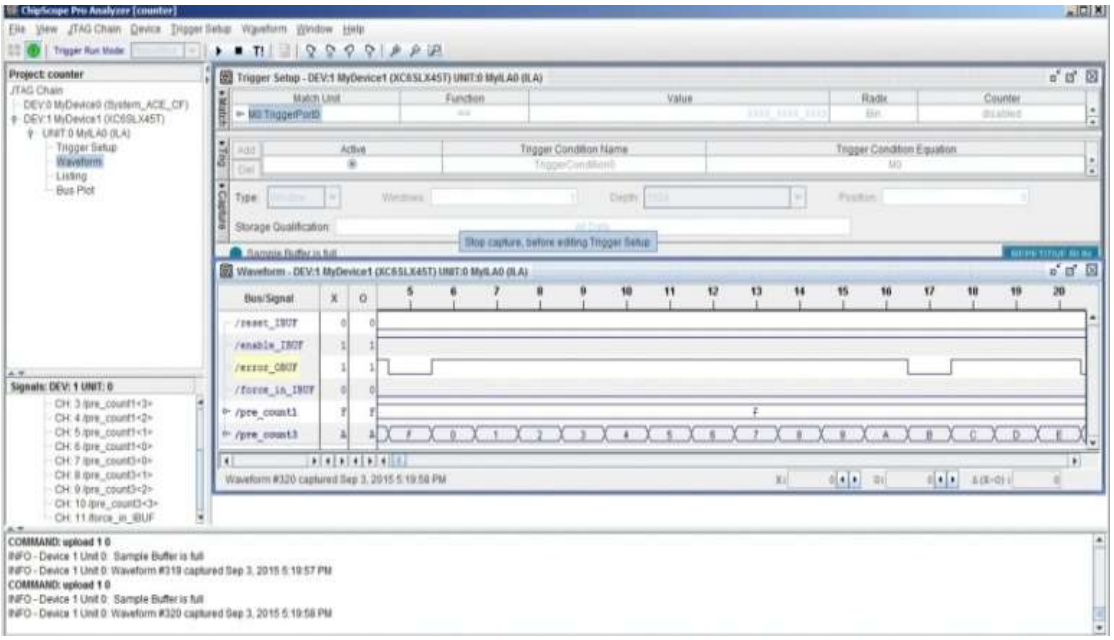



**Figure 4.12. The waveform of fault injected in two TMR logic blocks**

### 4.1.5. Summary

It is found that the TCL scripting based fault injection tool is able to inject any number of faults at netlist level efficiently. It can automatically/manually choose the sensitive nodes and inject faults. Most of the techniques reported in the literature are not commercially available and this one can be developed and used easily.

# 5

# MEASUREMENT OF RADIATION ABSORBED DOSE EFFECTS IN SRAM BASED FPGAs

*Measuring the effects of total absorbed dose effects in SRAM based FPGAs is one of the major objectives of this thesis. As the accumulated dose increases the upset rate in FPGAs, it is required to know how the accumulated dose alone affects the characteristics of the device. Towards this, an irradiation experiment has been designed to suit the Gamma-5000 facility available at this centre. Experiments have been conducted by keeping the device both in power-on and power-off states. It may be highlighted that in some applications, the device is deployed in the radiation environments and remains in power-off condition for a substantial period before it is put into service. From this consideration, the irradiation experiment at the power-off state is assumed important. This chapter also includes the modelling of shielding to extend the life of the device deployed in the radiation environment.*

## 5.1. IRRADIATION EXPERIMENTS ON SRAM-FPGAs

The experiments in gamma chamber aim to measure the tolerance level of SRAM based FPGAs due to the cumulative absorbed dose. Along with the functionality failure, the major parameter to be measured is the power supply current variation. In

the power-on test, the device was configured with particular functions and the parameters were measured continuously. But in the power-off test, the performance variations of the device were captured after configuring the device at particular time intervals during the experiment. Along with the power supply current variation, an indirect method of measuring the propagation delay based on ring oscillator implementation was adopted. The device was irradiated up to a dose level of 2.5 Mrad in the power-on test and up to 50 Mrad in the power-off test. There are many studies carried out on the radiation effects in SRAM based FPGAs, especially on SEEs [177-180]. As already mentioned, there is not much-published literature on cumulative radiation absorbed dose effects in commercial-grade SRAM based FPGAs, both in power-on and power-off states.

Other than the parameters discussed above, TID effects are evaluated based on the propagation delay of different paths in the implemented circuits after a chain of dose steps especially in flash-based and antifuse based FPGAs. Other parameters which are the indicators of TID effects are the duty-cycle response, and temperature [181]. The test paths included an FPGA input, FPGA internal circuitry, an FPGA output, and an external measurement device (e.g., an oscilloscope). The propagation delay from input to output of each dose step is measured. But there are two primary issues; first is the mix of technologies between the propagation paths for example, internal logic and input/output (I/O) logic, makes it more complex and the second is the incapability of capturing sub-nanosecond TID degradation with sufficient resolution because measurements are performed external to the device [180, 181]. Another technique that addresses these issues, by measuring the delay from one internal element to another

internal element, which avoids the convoluted propagation delay contribution and the degradation in propagation delay, is measured internally for every path in the design. This gives a better granularity and observation of degradation on the order of picoseconds [182]. A built-in runtime test approach for measurement of TID degradation in SRAM based FPGAs based on changes in propagation delay is proposed in [183]. These changes are measured by ring oscillators (OSC) and a counter built-in FPGA [184].

In the present experiments, an indirect way of propagation delay measurement based on a ring oscillator implementation is adapted. Compared to the available experimental results, here experiments at high dose rates of 315 krad/h for power-off test and 345.2 krad/h for power-on test have been carried out. Along with the device's functional failure, the increase in power supply current is also measured, which affects the performance of the system.

### 5.1.1. Measurement Methods

We are measuring the propagation delay degradation by two different methods, the conventional and the indirect method. In the conventional method, the measurement path includes the internal logic and the I/O logic, i.e., from the input buffer to the output buffer. To measure the propagation delay low to high at 50% of the slope, the output needs to be captured by an oscilloscope and compared to the input signal [181]. The input signal can be applied using a function generator. The measurements need to be conducted before and after irradiation. By comparing both the values, the propagation delay degradation can be calculated.

For the direct measurement, circuits chosen are NAND inverter chains and the inputs are given from a function generator and also from the FPGA clock. The NAND chain implemented in FPGA is shown in Fig. 5.1.

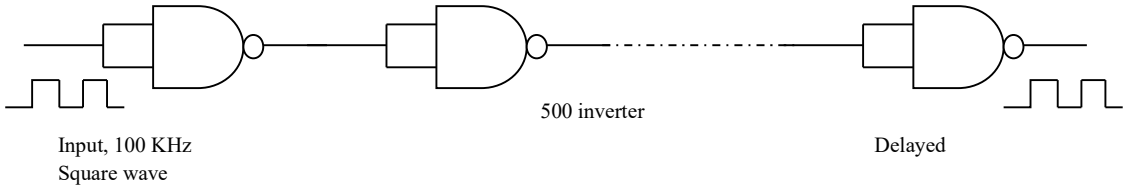



**Figure 5.1. NAND inverter chain**

The circuit chosen for indirect measurement of propagation delay is a Ring Oscillator circuit, which generates a particular frequency. The change in frequency is measured during and after irradiation and compared with the original frequency it generated before irradiation. The frequency variation is due to the delay it generates in the inverter chain due to radiation effects. The ring oscillator circuit, which is implemented in FPGA, is depicted in Fig. 5.2.

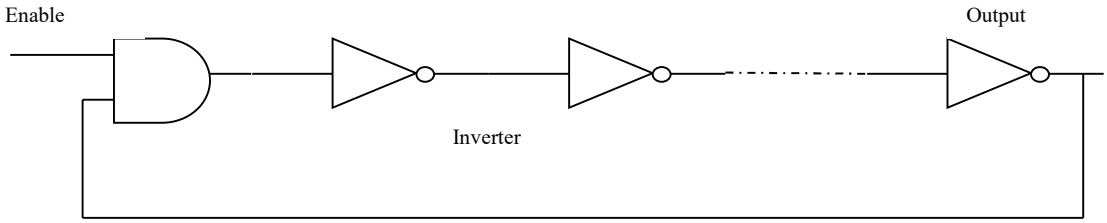



**Figure 5.2. Ring oscillator**

The block diagram of the test board with the device under test (DUT) of Xilinx-Spartan 6 FPGA is shown in Fig. 5.3 and the coding is done using VHDL language. While implementing the inverter chains to avoid the optimization by simplifying the listed nodes, we have used “keep” attribute, its specification must include the names of the signals that must be preserved. A portion of the usage of keep attribute is as mentioned below

```
signal nand_signal : std_logic_vector (499 downto 0);

attribute keep: Boolean;

attribute keep of nand_signal : signal is true;
```

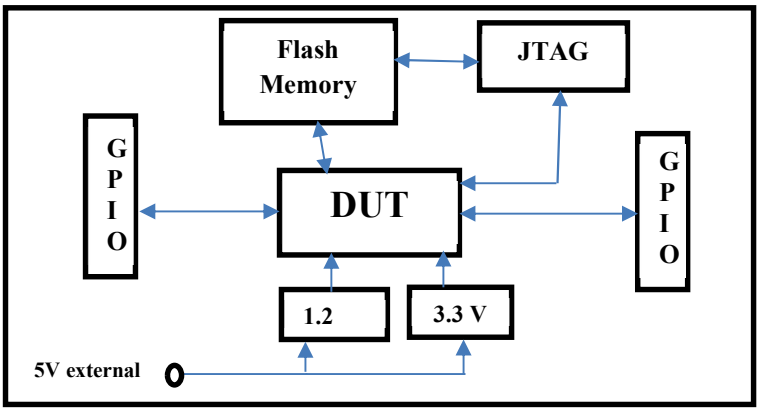



**Figure 5.3. Block diagram of test board**

### 5.1.2. Experimental Setup

In this section, the experimental facility used for the experiment is discussed. The gamma spectrum of Co-60 source has two significant peaks, one at 1173.2 keV and another at 1332.5 keV. The radiation field is provided by a set of stationary cobalt-60 sources placed in a cylindrical cage. It is having a PLC based control system and can be operated both on auto and manual modes. The main features are safe and self-shielded, automatic control of irradiation time, manual control of irradiation temperature, remote operation and dose uniformity [181]. The experimental setup at gamma chamber 5000 is shown in Fig. 5.4.

**Figure 5.4. Irradiation experimental setup at gamma chamber -5000**

The measurement instrumentation mainly consists of digital storage oscilloscope (DSO), function generator, power supply and a multimeter. A square wave of 100 kHz is applied as input to the inverter chains using a function generator in power-off test and power on test. The FPGA clock frequency is divided into 100 kHz and 400 kHz and given as input to each inverter chains. The propagation delay between input and output is captured in a DSO along with the frequency variation in the ring oscillator. The power supply current variation is measured using a digital multimeter.

### 5.1.3. Results and Discussion

#### 5.1.3.1. Power-off test

As already indicated, there is no open literature available on the behaviour of the device when it is exposed to radiation in the power-off state. The focus of the present study is the permanent failure of the device or degradation of the performance of the device. So, the test is performed by irradiating the device in the power-off state. The measurements are taken by configuring the device at particular intervals of time. The

device under test is configured through embedded SPI flash memory. The configuration bit file is stored in the flash memory through JTAG interface. Alternatively, it can be programmed directly by JTAG interface. But each time the device is powered up, it has to be configured separately. Two identical devices are exposed to gamma radiation and the power supply current and propagation delay variations are measured. The increase in power supply current against total dose absorbed in DUT1 and DUT2 are depicted in Fig. 5.5.

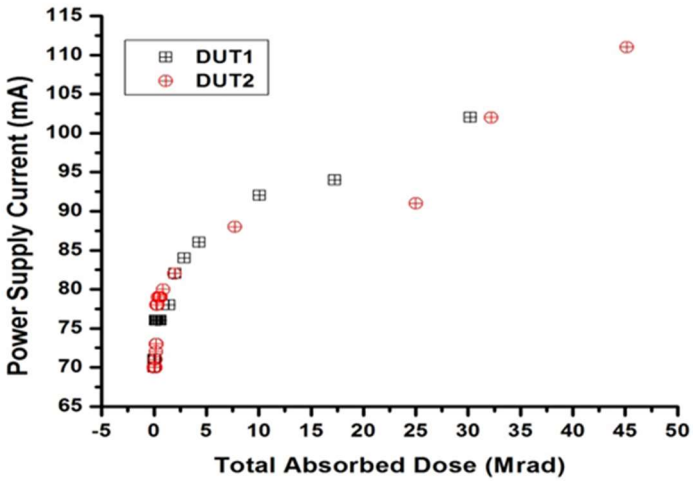



**Figure 5.5. Power supply current variations in DUT1 and DUT2**

The propagation delay was gradually increasing up to a dose level of 4 Mrad and after that it's found that there is a drastic drop in the propagation delay. The propagation delay variation against total absorbed dose is shown in Fig. 5.6.

Even if the device is in the power-off state, the absorbed dose generates electron-hole pairs in the device. The number of electron-hole pairs generated is proportional to the amount of energy deposited in the device by radiation. Once the device is powered on some of the electron-hole pairs will recombine, migrate and drift

under the action of an electric field and differences in the diffusion. But some of the charge carriers can trap in the oxide layer and interface layer and can cause electrically active defects. The rearrangement of atomic bonds at the oxide-silica interface, production of new interface states and border traps or slow interface states also cause the change in electrical properties of the device.

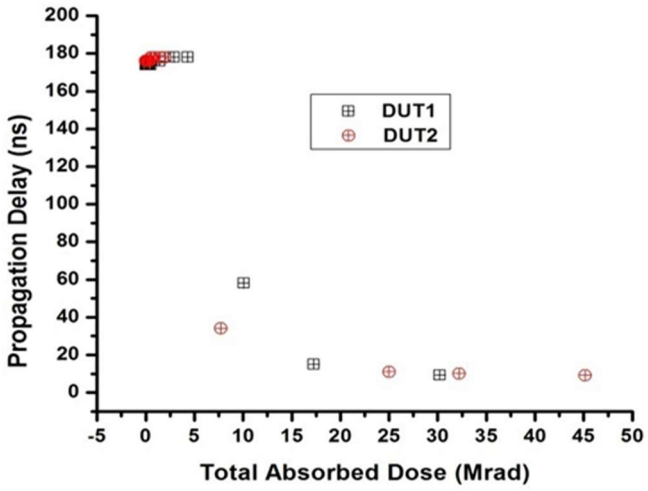



**Figure 5.6. Propagation delay variation in DUT1 and DUT2**

Generally, the threshold voltages of an n-channel and p-channel shifted in the negative direction under irradiation, as reported in the literature and the same caused the initial propagation delay degradation up to a dose level of 5 Mrad. The propagation delay has reduced drastically when there is a permanent failure of the device. Even after reconfiguring the device, several times the signal output captured was the same degraded output. When the radiation dose levels were beyond 10 Mrad there were only higher frequency components available in the signal and it was considered a permanent failure of the device.

The response to radiation of an integrated circuit made up of thousands of logic gates is difficult to predict without extensive simulations and irradiation experiments.

### 5.1.3.2. Power-on test

Three-ring oscillator circuits, each having 500 inverter chains and two NAND inverter chains of 500 inverter stages, are implemented in FPGA for the testing purpose. The input to the NAND inverter chains is given from a 32-bit counter circuit. The circuit divides the 100 MHz clock frequency available from the on-board clock oscillator into various frequencies and among those frequencies 96 kHz and 390 kHz are given as input to the NAND inverter chains.

The frequency (propagation delay) generated by the ring oscillators before irradiation and the variation in the frequency during irradiation are monitored. Initially, the propagation delay increased marginally without significantly affecting the performance. However, later at a dose level of 805 krad, the propagation delay dropped down drastically which contained only the higher frequency components. The behaviour was almost in the same manner as observed in the power-off test. The waveform generated by the ring oscillator is captured in a DSO and depicted in Fig. 5.7.

The counter output which is given as input to the NAND inverter chain and the inverter chain output are captured in a DSO and the delay between both the signals are measured.

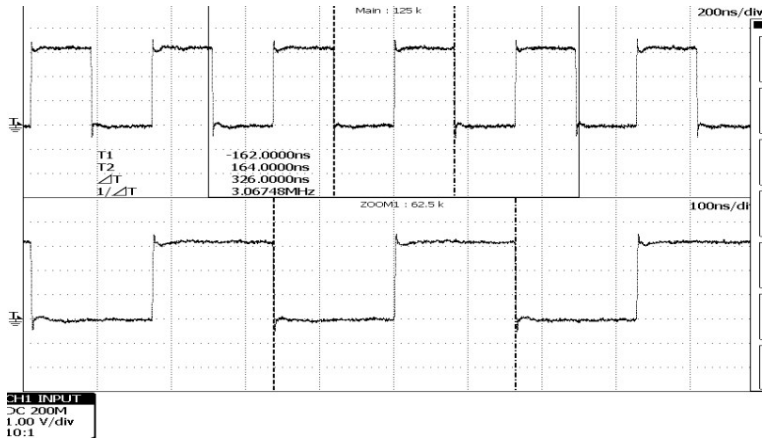



**Figure 5.7. Ring oscillator output**

The power supply current variation during irradiation was continuously monitored and the first functional failure was observed at a dose level of 512 krad in DUT1 and 322 krad in DUT2. The power supply current variations due to absorbed dose in DUT1 and DUT2 are illustrated in Fig. 5.8 and Fig. 5.9 respectively. The current reaches up to a value of 325 mA in DUT1 and 384 mA in DUT2 from an initial current of 64 mA and 62 mA respectively. During the irradiation periods, mild increase and reduction in the current are observed. It is also observed that even after reconfiguration and the power cycle the current remained almost the same. This suggests the presence of electrically active defects due to trapped charges.

In the case of DUT1, the ring oscillator output drastically drops at a dose level of 805 krad. This can be considered as a permanent failure, because even after power-on reset and reconfiguration it was unable to give the correct behaviour. Unlike the ring oscillator, counter circuit restarted its functionality at a dose level of 1.49 Mrad in DUT1. A sudden increase in power supply current is observed at that particular time. This was followed by failure of DUT1. The behaviour observed in both the devices are

nearly identical, viz, (i) an increase in the power supply current when the counter circuit performs its functionality, and (ii) a drop in current once the device fails.

The major parameter shift observed in this experiment is the increase in power supply current. This occurs due to the leakage current or toggling of transistors between on and off states due to the shifts in threshold voltage. Spartan 6 FPGAs use middle or medium thickness oxide transistors in the configuration memory and interconnect pass transistors, combined with a mix of channel lengths and voltage thresholds. During normal operating conditions, this approach significantly reduces the leakage current. But irradiation with high dose rate changes the behaviour of nmos and pmos devices drastically. The large negative threshold voltage shift in nmos devices due to the trapped charges makes the device partially ON even in the non-biased condition. N-channel devices biased during irradiation shows significantly larger leakage current than that of the grounded devices [185]. In p-channel, the leakage current formation during irradiation is identical when in biased as well as in non-biased conditions. Thus, even when the device is in power-off state shows significant degradation and potential failure due to the cumulative absorbed dose take place.

The irradiation was continued up to a radiation level of 1.783 Mrad in DUT1 and 2.358 Mrad in DUT2. Subsequently, the devices were removed from the irradiation chamber and allowed to anneal for a period of five hours without giving power-on reset. A decrement in the power supply current was observed during the annealing process. Even after the annealing process, the device could not come back to its original functionality.

Even after the irradiation stops, the characteristics of SRAM based FPGAs may still change due to post-irradiation effects. The threshold voltage of transistors which shifted in a negative direction under irradiation, will start to shift in the positive direction till their original values (or in some cases beyond the original) are reached. The negative shift in $V_t$ is due to the trapped holes in the oxide or at the interface traps. During the annealing process at room temperature, the electrons from the continuous structures of CMOS, tunnel into the oxide layer and recombine with the trapped holes. The rate of this process increases at higher temperatures [186]. In this experiment, the annealing is performed at room temperature. Thus, it is concluded that the trapped charges are not fully recombined even after five hours of annealing.

As per the literature, if the device is irradiated at a lower dose rate, the device may be able to anneal some of the damages due to absorbed dose while they are still under irradiation. Here the device under test was irradiated at a high dose rate of 5.753 krad/min (3.452 kgy/h). So, annealing at the time of irradiation was not possible and due to the cumulative dose, the characteristic changes may be more than that in an identical device absorbing the same total dose at lower dose rate. The radiation-induced shifts in threshold voltage ($V_t$) in CMOS devices vary approximately with the cube of the oxide thickness. When the oxide thickness is small, the recombination of electrons and holes are more complete. So, nanometer-size CMOS process technologies are less prone to TID effects due to their smaller oxide thickness.

Simulation-based static power analysis is performed in the implemented design after performing synthesis and implementation. The importance of this analysis is to

know the change in power consumption according to the variation in temperature. The total on-chip power according to various junction temperatures is given in Table 5.1.

The temperature inside the chamber is measured using a K-type thermocouple to analyse the variation in the device behaviour due to temperature. The maximum temperature measured is 50.4 degree Celsius. As per the simulation data, the total power at room temperature has shown almost 35% of increment when it reached the maximum value of measured temperature. The increase in power supply current and variation in temperature inside the chamber according to the total absorbed dose are plotted in Fig. 5.10. It is observed that there is no significant variation in the power supply current contributed by the increase in temperature inside the chamber.

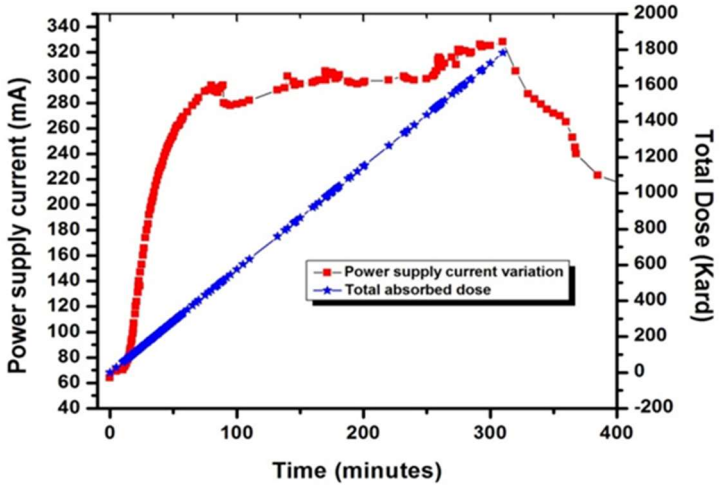



**Figure 5.8. Power supply current variation due to total radiation absorbed dose-DUT1**

### 5.1.4. Design of Shielding Box to Extend Device Life

It is essential to protect the device from radiations with high dose rate and extend the life of the system. Towards this, fabrication of a stainless steel box was envisaged. The geometry of the shielding box is decided based on the space available in the gamma chamber test facility.

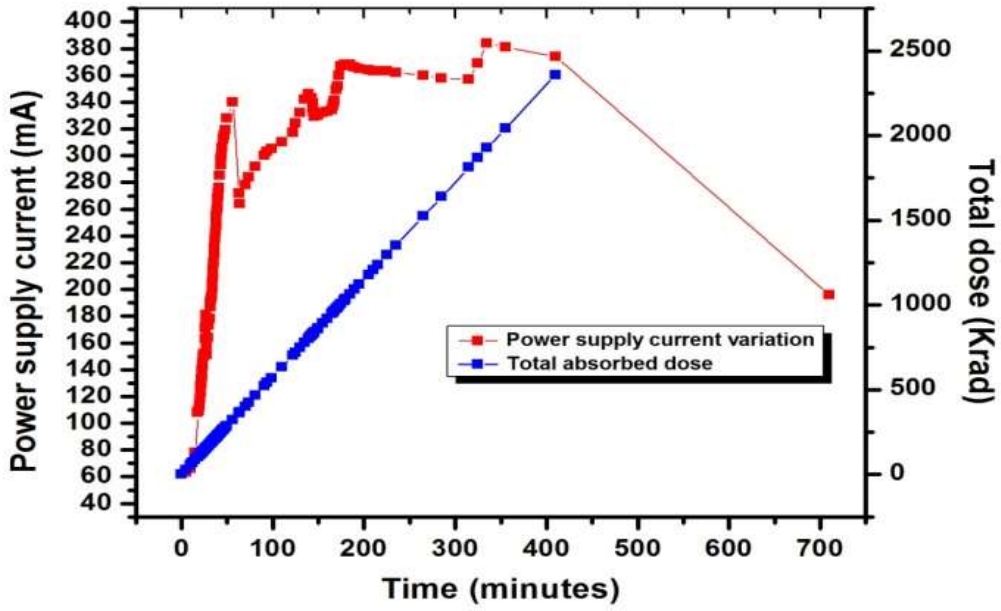



**Figure 5.9. Power supply current variation due to total radiation absorbed dose- DUT2**

**Table 5.1. Power analysis based on temperature variation**

| Junction temperature (Degree Celsius) | Total Power (on-chip) in watts |
|---|---|
| 25.5 | 0.014 |
| 35 | 0.017 |
| 45 | 0.021 |
| 50 | 0.023 |
| 55 | 0.026 |

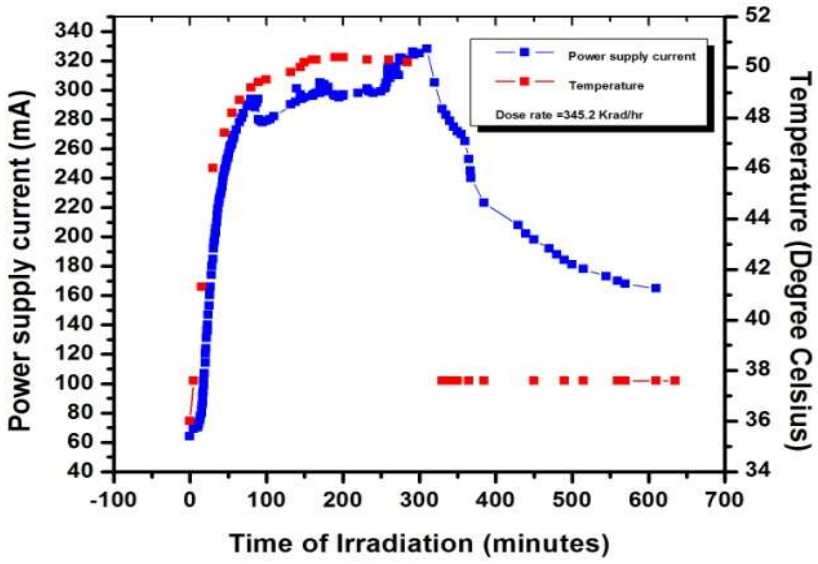



**Figure 5.10. Total dose Vs temperature and power supply current**

Hence a computational modelling is done for calculating the dose rate inside the box. The dose rate inside the box is also measured by using the thermoluminescence (TL) method. The dose rate of the gamma chamber-5000 facility is 3.15 kGy/h. As the present experiments are meant for applications in the nuclear power plant I&C system design, modelling of radiation attenuation is also performed by considering the active areas of the nuclear reactor.

### 5.1.4.1. Radiation levels in the active areas of reactor

The active areas in a pool type sodium-cooled fast reactor are the Reactor Containment Building (RCB), fuel building, steam generator building and radiation waste building. The multiple barriers for activity release in a fast reactor are shown in Fig. 5.11. During normal operating condition**,** the dose rate in these areas is maintained below 25 µSv/h. It is proposed to locate the SRAM-FPGA based system inside the RCB. Hence the focus of this section is to understand the variations in radiation activity

inside the RCB. The radiation on the top shield is generally higher than the radiation level elsewhere in the RCB. The reactor is designed for continuous operation with four or less than four failed fuel pins in the core. With failed pins inside the core, the maximum limit of 25 μSv/h is reached. However, in the unlikely event of multiple fuel pin failures inside the core, the activity inside the RCB can rise beyond 25 μSv/h. So, while designing a system to be kept inside the RCB, we need to consider the worst-case scenario that can occur in a nuclear reactor, i.e., core disruptive accident (CDA) condition.

During a hypothetical CDA condition almost 350 kg of radioactive sodium can enter into the RCB and the dose rate can go up to 8000 Gy/h, i.e., 800 krad/h. The major isotopes which contribute to the radioactivity inside the RCB are presented in Table 4.2. Once CDA happens continuous chain reaction will be stopped and neutron production will be negligible inside the RCB. But there is a possibility of spontaneous fission reaction caused mainly by an isotope of a fuel material Pu-240 and fission product Curium (Cm). The average energy of neuron generated is estimated to be 1.8 MeV. Hence it is clear that Gamma is the major source of radiation effects in the reactor containment building after a hypothetical CDA.

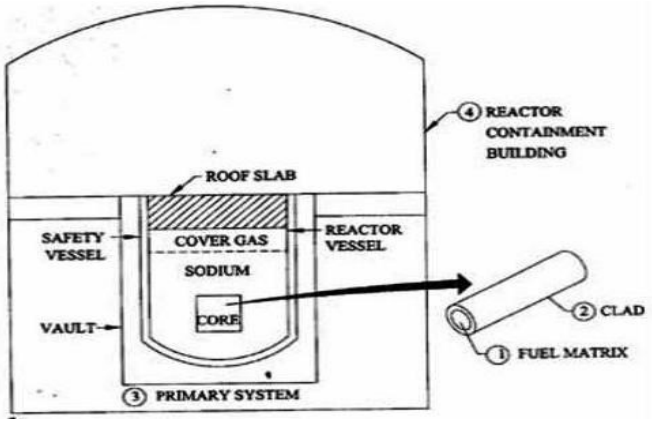



**Figure 5.11. Multiple barriers of radioactivity containment [187]**

**Table 5.2. RCB source term after a CDA in a 500 MWe pool type fast reactor normalised w.r.t. that of Xe-135**

| ISOTOPE | Strength normalised w.r.t. that of Xe-135 |
|---|---|
| Iodine-132 (I-132) | -0.15964 |
| Iodine-133 (I-133) | -0.04533 |
| Iodine-134 (I-134) | -0.00788 |
| Iodine-135 (I-135) | -0.06504 |
| Caesium-134 (Cs-134) | -0.48838 |
| Caesium-136 (Cs-136) | -0.49173 |
| Rubidium-88 (Rb-88) | -0.41171 |
| Ruthenium-103 (Ru-103) | -0.03548 |
| Cerium-141 (Ce-141) | -0.15373 |
| Cerium-144 (Ce-144) | -0.30351 |
| Tellurium-131m (Te-131m) | -0.43989 |
| Tellurium-132 (Te-132) | -0.16555 |
| Barium-141 (Ba-140) | -0.1419 |
| Zirconium-95 (Zr-95) | -0.1892 |
| Lanthanum-140 (La-140) | -0.13599 |
| Argon-41 (Ar-41) | -0.50454 |
| Krypton-83m (Kr-83m) | -0.48443 |
| Krypton-85 (Kr-85) | -0.50354 |
| Krypton-85m (Kr-85m) | -0.4663 |
| Krypton-87 (Kr-87) | -0.43477 |
| Krypton-88 (Kr-88) | -0.41526 |
| Krypton-89 (Kr-89) | -0.39949 |
| Xenon-131m (Xe-131m) | -0.50237 |

| ISOTOPE | Strength normalised w.r.t. that of Xe-135 |
|---|---|
| Xenon-133m (Xe-133m) | -0.48946 |
| Xenon-135 (Xe-135) | 0 |
| Xenon-135m (Xe-135m) | -0.39042 |
| Xenon-137 (Xe-137) | -0.10051 |
| Xenon-138 (Xe-138) | -0.15176 |
| Uranium-239 (U-239) | -0.47872 |
| Uranium-238 (U-238) | 4.126952 |
| Neptunium-239 (Np-239) | 4.107244 |
| Curium-243 (Cm-243) | -0.50453 |
| Sodium-22 (Na-22) | -0.50454 |
| Sodium-24 (Na-24) | -0.50449 |
| Manganese-54 (Mn-54) | -0.48877 |
| Iron-59 (Fe-59) | -0.50281 |
| Cobalt-58 (Co-58) | -0.43595 |
| Cobalt-60 (Co-60) | -0.5042 |
| Molybdenum-99 (Mo-99) | -0.48518 |
| Chromium-51 (Cr-51) | -0.49551 |

#### 5.1.4.2. Shielding box attenuation calculation

The sidewall thickness of the shielding box is taken as 2 cm and bottom and top thickness are fixed as 2.5 cm each. The space inside the box is 9 cm diameter and 3 cm in height. A hole of 1.5 cm diameter is given to expose the DUT to radiation if needed during the tests otherwise it will be kept closed with the same stainless steel material. A provision for taking out the cables is provided through a 0.8 cm diameter hole. The

fabricated stainless steel box is shown in Fig. 5.12. A Two-dimensional transport code DORT and IGC-S3 cross-section set are used for the modelling of the shielding box inside the gamma chamber for dose rate prediction. The calculations are performed in RZ geometry and the schematic model is shown in Fig. 5.13a. The results of the modelling with variations of dose rate (Gy/h) with a radial distance of the model are shown in Fig. 5.13b.

It is found that the radiation distribution in the gamma chamber is not uniform due to the fact that source pencils are located along the sides, where the space provided to keep the samples to be irradiated. The dose rate calculated is 0.877 kGy/h at the centre of the box. The peak is found outside the shielding box within the chamber. If the box is kept horizontally, the radiation dose rate is predicted to be 1.00 kGy/h at the centre. For this calculation, the uncertainties related to cross-section, modelling and changes in geometry are not considered. But, after considering an uncertainty factor of 2, the dose rate inside the shielding box is 175.4 krad/h when the box is kept vertically and 200 krad/h when the box is kept horizontally. The reduction in dose rates is 1.8 times and 1.6 times from the actual value.

The expected attenuation during CDA is estimated by distributing the sources surrounding the model. The dose rate estimated inside the box is 1000 Gy/h i.e. 100 krad/h. By considering an uncertainty factor of 2, the dose inside the shielding box will be 200 krad/h. Here, reduction is more compared to that in the gamma chamber-5000, because even lower energy gammas are also contributing to CDA whereas, in Co-60 source used in Gamma chamber-5000, higher energy gammas of 1.33 and 1.17 MeV are used whose attenuation is less compared to lower energy gammas. It is computed

that during the CDA condition, the device can operate for 96 minutes without any functional failure. This input will form important input towards safety assessment of the reactor including signals for containment isolation, post accident monitoring of RCB etc.

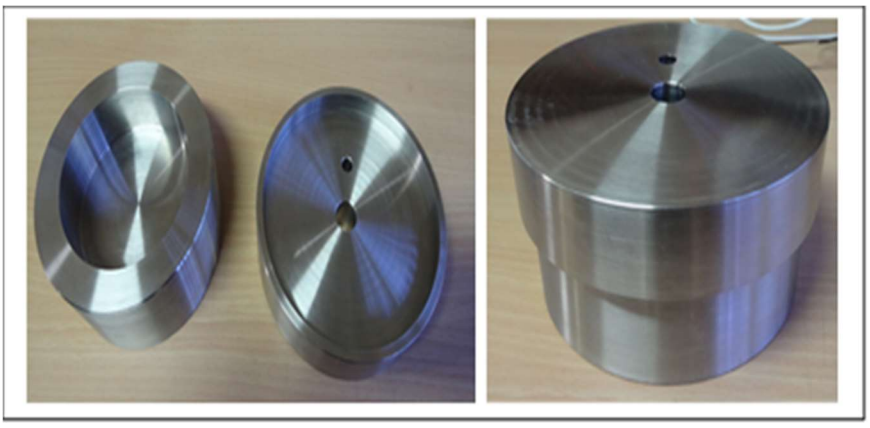


**Figure 5.12. Stainless steel shielding box**

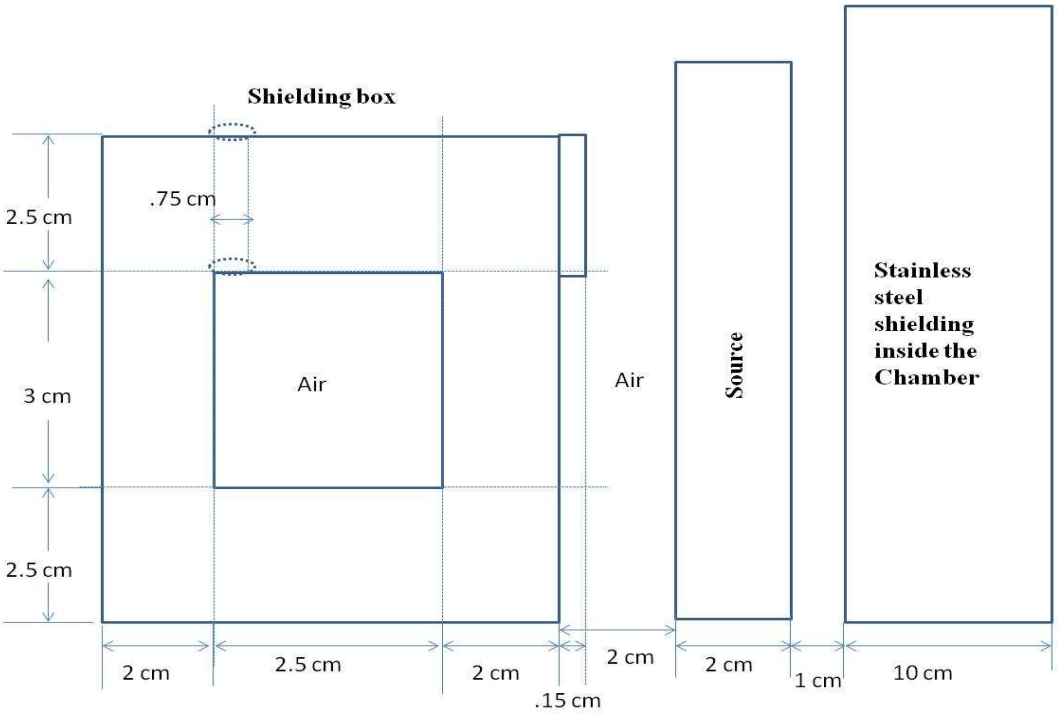



**Figure 5.13a. Schematic model for shielding calculation**

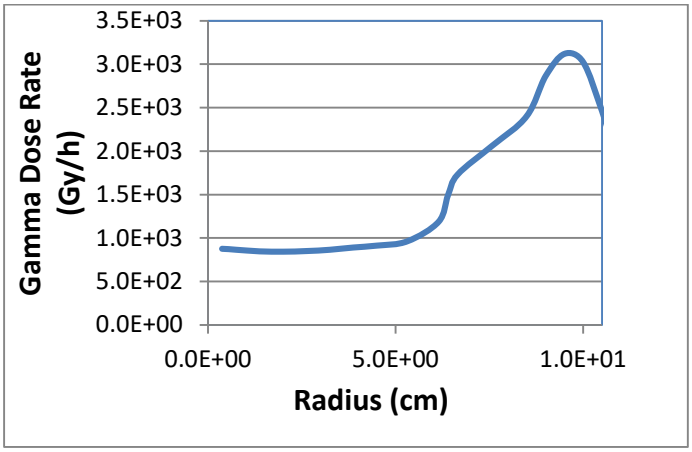
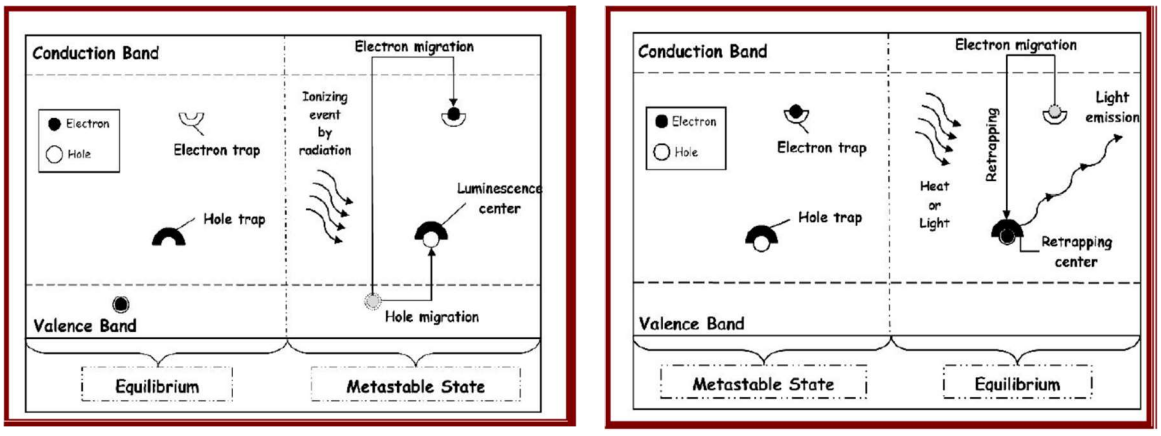



**Figure 5.13b. Variations of dose rate (Gy/h) with radial distance of the model**

### 5.1.4.3. Dose estimation using $CaSO_4$:Dy powder with thermo-luminescence (TL) phenomenon

Thermoluminescence (TL) is the thermally stimulated emission of light following the previous absorption of energy from radiation and the process is shown in Fig. 5.14.




**(a) Before irradiation | upon irradiation** **(b) after irradiation | upon heating**

**Figure 5.14. Thermoluminescence process**

Thermoluminescent Dosimeters (TLDs) are available in various forms like powder, chips, etc. TLDs are measured using a TLD reader. A basic TLD reader consists of a planchet for placing and heating the TLD, a photomultiplier tube (PMT) to detect the thermoluminescence light emission and convert it into an electrical signal proportional to the absorbed radiation dose on TLD. The TL emission intensity can be recorded as a function of temperature (T). The resulting curve (spectra) is called the TL glow curve and it is shown in Fig. 5.15. Area under the curve is directly proportional to the absorbed dose on the TLD material. So, the total TL signal can be correlated to dose through proper calibration.

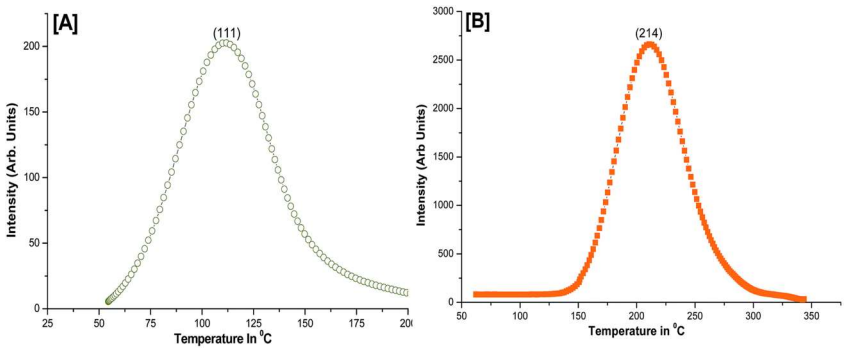



**Figure 5.15. Schematic diagram for TL glow curve**

In the present experiments four pellets of *$CaSO_4$:Dy* (two of them kept freely inside the chamber and other two kept inside the shielding box) are used. The pellets are irradiated for one-minute duration and the absorbed dose on the pellets is measured. The dose rate in the chamber is found to be 48 Gy/minute and inside the shielding box it is 28 Gy/minute. The reduction in dose rate calculated from the measurement is 1.7 times the dose rate measured outside the box.

### 5.1.4.4. Results and discussion

From the irradiation experiments, it is found that the device is functionally tolerant up to a cumulative absorbed dose of 322 krad. The time duration for which the device worked satisfactorily can be calculated by dividing the tolerance level of the device by the dose rate, i.e., (322 krad) / (5.7533 krad/ min) = 56 minutes. The system functional time can be extended by using proper shielding. Based on the shielding box that was designed, the possible time extension is presented in Table 5.3.

**Table 5.3 Extended system functioning time by using shielding box**

| | Functional time |
|---|---|
| Actual value without shielding | 56 minutes (measured) |
| With shielding: Based on the prediction of the Two-dimensional transport code DORT and IGC-S3 cross-section set | 101 minutes (computed) |
| With shielding: Based on Thermoluminescent Dosimeters (TLD) measurement | 95 minutes (measured) |

## 5.2. SUMMARY

When the oxide thickness is small, the recombination of electrons and holes are more complete. Hence, nanometer-size CMOS process technologies are less prone to TID effects due to their smaller oxide thickness. Based on the radiation experiments carried out using Gamma-chamber 5000, it is observed that the device under test (Spartan 6 FPGA) is functionally tolerant up to a radiation dose level of 322 krad,

suggesting that if the system is implemented with SEU mitigation techniques, the device can withstand up to 322 krad of accumulated dose without any failure. In an environment where the neutron energy is less than 10 MeV, the device can efficiently work with error correction codes with selective redundancy. However, in the environment having neutron energies higher than 10 MeV, partial reconfiguration or periodic scrubbing is required. For further improvement in efficiency, appropriate shielding can be provided. The shielding requirement can be determined using the 2D transport code DORT and IGC-S3 cross-section data set.

Based on the computational modelling of shielding box and TLD based dose rate measurement in the Gamma chamber, it is found that the duration of functional time can be extended almost two times by using shielding.

The indirect way of propagation delay measurement adopted here, which is based on ring oscillator, can be used for measuring the TID effects in flash-based FPGAs, as the propagation delay is the major parameter change due to TID in flash based FPGAs.

# 6

# CONCLUSIONS AND SCOPE FOR FUTURE WORK

*The present chapter summarizes the conclusions derived from various research activities carried out in the study of radiation effects in SRAM based FPGAs for the design of nuclear power plant instrumentation and control systems. It also provides the scope for future work in this area.*

## 6.1. SUMMARY OF THE THESIS

The aim of the present dissertation was to study the radiation effects in SRAM based FPGAs targeted for NPP I & C system design. As there is no history of data available for commercial grade SRAM based FPGAs used in nuclear applications this study has its significant importance. From the literature it is found that TID effects and SEUs are the common cause of failures in the systems implemented using SRAM based FPGAs and deployed in a radiation environment. It is also found that during various operating conditions of the reactor, gamma rays are the major sources of radiation in the reactor environment. So, this study has given focus to cumulative absorbed dose effects due to gamma radiation. As gamma radiation can cause TID effects as well as SEUs in the MOS based devices, an experimental study has been conducted to measure the tolerance level of the system in such an environment. As there is a possibility of SEUs in the system either due to gamma or due to other reasons, a detailed investigation has been conducted on SEU mitigation techniques. By

controlling the SEUs and delaying the cumulative effects, the time duration for which the device can perform its intended function can be extended. Keeping these targets, the objectives of the research were set and the achieved results are summarized.

1) A detailed investigation in to various SEU mitigation techniques has been carried out and their efficiencies are quantified based on area overhead, complexity of implementation to assist designers/researchers to choose the appropriate technique based on specific requirement. Further a hybrid hardware/software scrubber with selective hardening either by giving frame level redundancy or implementing improved error correction codes for sensitive frames, is proposed.

2) An error recovery mechanism based on extended Golay code is proposed to detect up to four errors and to correct up to three errors in a block of 24 bits. This can improve the period between partial reconfigurations required to keep the system soft error free.

3) An efficient fault injection technique has been developed for easy implementation to support automatic detection of sensitive nodes and fault injection at RTL and netlist levels.

4) Based on controlled irradiation experiments employing Gamma chamber -5000, it is found that the device under test, Spartan 6 FPGA, can withstand upto 322 krad of accumulated dose without any functional failure. This form an input data for deciding the shielding essential to protect SRAM based FPGAs functioning in radiation environment of nuclear reactor.

5) In an environment where the neutron energy is less than 10 MeV, the device under test can efficiently work with error correction codes with selective redundancy. However, in environments having neutron energies higher than 10 MeV, partial reconfiguration or periodic scrubbing is required.

6) The possible reduction in dose rate experienced by the device under test, Spartan 6 FPGA, by providing stainless steel shielding has been measured in the gamma-chamber 5000. The measurements have also been validated by computational modelling using a two-dimensional transport code DORT and IGC-S3 cross-section set. It is found that the duration of functional time can be extended almost two times by appropriate shielding.

## 6.2. SCOPE FOR FUTURE WORK

The findings of the present experiments/analysis can be implemented in the safety Core Temperature Monitoring System (CTMS). It is classified as safety-critical system and has two main failure modes: (i) failure to initiate SCRAM signal when parameters exceed their threshold values; which places demand on the hardware based CTMS and other diversified shutdown systems, (ii) generation of spurious SCRAM signals, which affects the plant availability. The implementation of CTMS in SRAM based FPGA provides diversity in the existing RTC based triple modular system. As per the present experimental results, the system can be deployed inside the RCB, so multiple penetrations in the RCB can also be avoided. Golay code-based error recovery mechanism and other fault tolerant techniques discussed in the thesis can be implemented to provide additional tolerance. Also, a detailed study on hardware accelerator combined with dynamic partial reconfiguration for isolating the affected

area and reconfigure the affected functional block in the non-affected area can be performed. A diversified Hardware CTMS combining all the three constituent systems of CTMS together augmenting it with radiation tolerant features can be developed which can be located inside the reactor containment building.

# REFERENCES


1. IAEA Nuclear Energy Series No. NP-T-3.17, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, International Atomic Energy Agency Vienna, 2016. Available: http://www-pub.iaea.org/MTCD/ Publications/ PDF/Pub1701_ web.pdf.

2. Catherine Menon and Sofia, Field programmable gate arrays in safety-related instrumentation and control applications, Report 112 (2015). ADELARD LLP, 2015.

3. https://www.microsemi.com/product-directory/dev-tools/4970-programming#programming-info

4. Defence in depth in nuclear safety –INSAG-10, a report by the international nuclear safety advisory group, IAEA, Vienna, 1996. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1013e_web.pdf

5. Xilinx Device Reliability Report, UG116 (v10.6.1), July 11, 2017.https://www. xilinx.com/support/documentation/user_guides/ug116.pdf.

6. C. Bernardeschi, L. Cassano, A. Domenici, SRAM-based FPGA systems for safety-critical applications: A survey on design standards and proposed methodologies, J. Comput. Sci. Technol. 30 (2) (Mar. 2015) 373-390, https://doi.org/10.1007/s11390-015-1530-5.

7. Saritha P. Menon, N. Sridhar, D. Thirugnana Murthy, Computer based Core Temperature Monitoring System for Prototype Fast Breeder Reactor, Bhabha Atomic Research Centre, India, 2013.

8. Fink, R.T., Killian, C.D., Nguyen, T., Druilhe, A., Daumas, F., Naser, J.A. 2010. Guidelines and a primer on application of field-programmable gate arrays in nuclear plant I&C systems. In: NPIC&HMIT 2010, 7–11 November, Las Vegas, Nevada, pp. 1305–1315.

9. B. Todd, S. Uznanski, Radiation Risks and Mitigation in electronic Systems, in: the proceedings of CAS-CERN Accelerator School: Power Converters, Baden, Switzerland, May 2014, pp. 245e263.https://doi.org/10.5170/CERN-2015-003.245 (Accessed 21 Oct. 2016).

10. S. Chetal, V. Balasubramaniyan, P. Chellapandi, P. Mohanakrishnan, P. Puthiyavinayagam, C.Pillai, S. Raghupathy, T. Shanmugham and C. S. Pillai, The design of the Prototype Fast Breeder Reactor, Nuclear Engineering and Design, vol. 236, no 7-8, pp.852-860, 2006.

11. P. Swaminathan, Modeling of instrumentation and control system of prototype fast breeder reactor. PhD thesis, Sathyabama University, December 2008.

12. M. Herrera-Alzu, L opez-Vallejo, Design techniques for Xilinx Virtex FPGA ConfigurationMemory Scrubbers, IEEE Trans. Nucl. Sci. 60 (1) (February2013).

13. Xilinx, Spartan-6 FPGA Configuration User Guide, UG380 (v2.9), August 11, 2016. https://www.xilinx.com/support/documentation/user_guides/ug380.pdf (Accessed January 03, 2017).

14. Xilinx, 7Series FPGAsConfigurationUserGuide, UG470 (v1.11), September 27, 2016. https://www.xilinx.com / support / documentation / user_ guides /ug470_7Series_Config.pdf.

15. Particle Radiation effect Mitigation Techniques in FPGAs: Synopsys application note, April 2013. Available: https://www.synopsys.com/Tools/Implementation/FPGAImplementation/Pages/fpga-application-notes.aspx.

16. Paul Graham, Michael Caffrey, Jason Zimmerman, Prasanna Sundararajan, Eric Johnson, and Cameron Patterson, Consequences and Categories of SRAM FPGA Configuration SEUs, Military and Aerospace Programmable Logic Devices International Conference, Washington DC 9/9-9/11/2003.

17. RamindaUdayaMadurawe, Three-dimensional Integrated Circuits, U.S Patent 7,538,575. B. 26 May 2009.

18. G. Messenger, M. Ash, The Effects of Radiation on Electronic Systems, seconded., Van Nostrand Reinhold, New York, 1992.

19. F. Wrobel, Fundamentals of particle matter interaction, New challenges for radiation tolerance assemblies, in: Proceedings of the 8th European Conference on Radiation and its Effects on Components and Systems (RADECS), France, September 19e23, 2005, pp. 5-31.

20. J.A. Dennis, Neutron flux and energy measurements, Phys. Med. Biol. 11 (1) (1966) 1-14.

21. G. Barbottin, A. Vapaille, Instabilities in Silicon Devices, New Insulators De-vices and Radiation Effects, vol. 3, Elsevier, 1999, pp. 2-938.

22. James E. Turner, Atoms, Radiation and Radiation Protection, Wiley, New York, 1995.

23. J.S. Browning, M.P. Connors, C.L. Freshman, Total dose characterization of a CMOS technology at high dose rates and temperatures, IEEE Trans. Nucl. Sci.35 (6) (Dec. 1988).

24. D.M. Fleetwood, L.C. Riewe, J.R. Schwank, Radiation effects at low electric fields in thermal, SIMOX, and bipolar-base oxides, IEEE Trans. Nucl. Sci. 43 (No. 6) (December 1996) 2537-2546.

25. B. Djezzar, A. Smatti, A. Amouche, M. Kechouane, Channel-length Impact on Radiation-Induced threshold-voltage shift in N-MOSFET's devices at low Gamma Rays Radiation doses, IEEE Trans. Nucl. Sci. 47 (6) (December 2000).

26. M.R. Shaneyfelt, D.M. Fleetwood, P.S. Winokur, J.R. Schwank, T.L. Meisenheimer, Effects of device scaling and geometry on MOS radiation hardness assurance, IEEE trans. Nucl. Sci. 40 (6) (Dec. 1993).

27. M. Simons, Rapid annealing in irradiated CMOS transistors, IEEE Trans. Nucl. Sci. 21 (6) (1974) 172-178.

28. H.J. Barnaby, Total-ionizing-dose effects in modern CMOS technologies, IEEE Trans. Nucl. Sci. 53 (6) (Dec. 2006) 3103-3121.

29. Daniel Montgomery MacQueen, Total Ionizing Dose Effects on Xilinx Field-Programmable Gate Arrays, A Master of Science Thesis submitted to the Faculty of Graduate Studies and Research, Department of Physics Edmonton, Alberta, 2000.

30. P.S. Winokur, K.G. Kerris, L. Harper, Predicting CMOS inverter response in nuclear and space environments, IEEE Trans. Nucl. Sci. 30 (Issue 6) (1983) 4326-4332.

31. S.S. Rathod, A.K. Saxena, S. Dasgupta, Radiation effects in MOS-based devices and Circuits: A Review, IETE Tech. Rev. 28 (6) (Dec. 2011) 451-469.

32. P.E. Dodd, L.W. Massengill, Basic mechanisms and modeling of single-event upset in digital microelectronics, IEEE Trans. Nucl. Sci. 50 (3) (Jun. 2003) 583-602.

33. R.C. Hughes, Charge carrier transport phenomena in amorphous SiO2: direct measurement of mobility and carrier lifetime, Phys. Rev. Lett. 30 (1973) 1333.

34. Kiran Agarwal Gupta, Dinesh K. Anvekar, V. Venkateswarlu, Modeling of short channel MOSFET devices and analysis of design aspects for power optimisation, Int. J. Model. Optimization 3 (No. 3) (June 2013).

35. C.E. Barnes, D.M. Fleetwood, D.C. Shaw, P.S. Winokar, Post-Irradiation Effects (PIE) in integrated circuits, IEEE trans. Nucl. Sci. 39 (3) (1992) 324-341.

36. Dariusz Markowski, The impact of radiation on electronic devices with the special consideration of neutron and gamma radiation monitoring, PhD dissertation submitted to technical University of Lodz, dept. of microelectronics & computer science, 2006.

37. R. C. Lacoe, J. V. Osborn, D. C. Mayer, S. Brown, J. Gambles, Total-dose tolerance of the Commercial Taiwan Semiconductor Manufacturing Company (TSMC) 0.35-pm CMOS Process, 2001 IEEE Radiation effects data Workshop, NSREC 2001, Workshop Record. Held in conjunction with IEEE Nuclear and Space Radiation Effects Conference, Pages 72-76.

38. T.P. Ma, Paul. V. Dressendorfer, Ionizing Radiation effects in MOS Devices and Circuits, A Wiley-Interscience publication, John wiley & Sons, 1989.

39. L. Adams, A. Holmes-Siedle, handbook of radiation effects, Oxford University press, 2004.

40. J.S. Browning, M.P. Connors, C.L. Freshman, G.A. Finney, Total dose characterization of a CMOS technology at high dose rates and temperatures, IEEE Trans. Nucl. Sci. 35 (Issue 6) (1988) 1557-1562.

41. Heather M. Quinn, Paul S. Graham, Michael J. Wirthlin, Brian Pratt, Keith S. Morgan, Michael P. Caffrey, James B. Krone, A test methodology for determining space readiness of Xilinx SRAM-based FPGA devices and designs, IEEE Trans. Instrumentation measurement 58 (No. 10) (Oct. 2009).

42. C. Detcheverry, C. Dachs, E. Lorfevre, C. Sudre, G. Bruguier, J.M. Palau, J. Gasiot, R. Ecoffet, SEU critical charge and sensitive area in a submicron CMOS technology, IEEE Trans. Nucl. Sci. 44 (No. 6) (1997) 2266-2273.

43. M. Nicolaidis, Soft Errors in Modern Electronic Systems, vol. 41, Springer, New York, 2011.

44. Robert C. Baumann, Radiationinduced soft errors in advanced semiconductor technologies, Device and Materials Reliability, IEEE Trans. Vol. 5 (no. 3) (2005) 305-316.

45. F.B. McLean, T.R. Oldham, Charge funneling in n and p-type Si substrates, IEEE Trans. Nucl. Sci. 29 (Dec. 1982) 2018-2023.

46. L.D. Edmonds, A simple estimate of funneling-assisted charge collection, IEEE Trans. Nucl. Sci. 38 (Feb. 1991) 828-833.

47. M.J. Gadlage, R.D. Schrimpf, J.M. Benedetto, P.H. Eaton, D.G. Mavis, M. Sibley, Single event transient pulse widths in digital microcircuits, IEEE Trans. Nucl. Sci. 51 (6) (2004) 3285-3290.

48. B. Narasimham, B.L. Bhuva, R.D. Schrimpf, L.W. Massengill, M.J. Gadlage, O.A. Amusan, Characterization of digital single event transient pulsewidths in 130nm and 90nm CMOS technologies, Nucl. Sci. IEEE Trans. 54 (6) (2007) 2506-2511.

49. P.E. Dodd, F.W. Sexton, G.L. Hash, M.R. Shaneyfelt, B.L. Draper, A.J. Farino, R.S. Flores, Impact of technology trends on SEU in CMOS SRAMs, IEEE Trans. Nucl. Sci. 43 (Dec.1996) 2797-2804.

50. H.T. Weaver, Soft error stability of p-well versus n-well CMOS latches derived from 2D, transient simulations, in: IEDM Tech. Dig, 1988, pp. 512-515.

51. P.E. Dodd, F.W. Sexton, Critical charge concepts for CMOS SRAMs, IEEE Trans. Nucl. Sci. 42 (Dec. 1995) 1764-1771.

52. C.L. Axness, H.T. Weaver, J.S. Fu, Mechanisms leading to single event upset, IEEE Trans. Nucl. Sci. NS-33 (6) (1986) 1577-1580.

53. H.T. Weaver, C.L. Axness, J.S. Fu, J.S. Binkley, J. Mansfield, RAM cell recovery mechanisms following high-energy ion strikes, IEEE Electron. Device Lett. 8 (Jan. 1987) 7-9.

54. Jiri Kvasnicka, Reliability Analysis of SRAM-based Field Programmable Gate Arrays, PhD Thesis submitted to Chech technical University in Prague, August 2013.

55. J.A. Zoutendyk, L.D. Edmonds, L.S. Smith, Characterization of multiple-bit errors from single ion tracks in integrated circuits, IEEE Trans. Nucl. Sci. 36 (6) (1989) 2267-2274.

56. R. Koga, S.H. Penzin, K.B. Crawford, W.R. Crain, Single event functional interrupt (SEFI) Sensitivity in Microcircuits, in: RADECS 97, Fourth European Conference on Components and Systems, 1997, pp. 311-318.

57. G. Allen, G. Swift, C. Carmichael, Virtex-4QV static SEU characterization summary, NASA Jet Propulsion Laboratory, Xilinx, JPL Publication, 2008,08-16 4/08.

58. Felix siegle, Fault detection, isolation and recovery schemes for space borne reconfigurable FPGA-based systems, PhD Thesis Submitted to Department of Engineering University of Leicester, Oct. 2015.

59. S. Duzellier, Radiation effects on electronic devices in space, Aerospace Sci. Technol. 9 (1) (2005) 93-99.

60. Gregory R. Allen, Farokh Irom, Leif Scheick, Sergeh Vartanian, Michael O'Connor, Heavy Ion Induced Single-Event Latchup Screening of Integrated Circuits Using Commercial Off-the-Shelf Evaluation Boards, IEEE Radiation Effects Data Workshop (REDW), 2016, pp. 1-7.

61. ECSS, Methods for the calculation of radiation received and its effects, and a policy for design margins, ESA-ESTEC, Standard ECSS-E-ST-10-12C, 2008.

62. Nathaniel Anson Dodds, Single event latchup: Hardening strategies, Triggering mechanisms, and Testing considerations, Doctoral Thesis submitted at Graduate School of Vanderbilt University, Nashville, Tennessee, USA, Dec.2012.

63. J.H. Hohl, K.F. Galloway, Analytical model for single event burnout of power MOSFETs, IEEE Trans. Nucl. Sci. 34 (6) (1987) 1275-1280.

64. D.C. Mayer, R. Koga, J.M. Womack, The impact of radiation induced failure mechanisms in electronic components on system reliability, IEEE Trans. Nucl. Sci. 54 (6) (2007) 2120-2124.

65. J.R. Brews, M. Allenspach, R.D. Schrimpf, K.F. Galloway, J.L. Titus, C.F. Wheatley, A conceptual model of a single event gate rupture in power MOSFETs, IEEE Trans. Nucl. Sci. 40 (no. 6) (1993) 1959-1966.

66. Gary Swift, Richard Katz, An experimental Survey of heavy ion induced dielectric rupture in actel Field Programmable Gate Arrays (FPGAs), IEEE Trans. Nucl. Sci. 43 (3) (1996) 967-972.

67. J. A. Hogan, R. J. Weber and B. J. LaMeres, 'A network-on-chip for radation tolerant multi-core FPGA systems', IEEE Aerospace conference, Big Sky, MT, pp. 1-7, 2014.

68. R. J. Weber, Reconfigurable hardware accelerators for high performance radiation tolerant computers, PhD thesis submitted to Montana state University, Bozeman, Montana, 2014.

69. J. George, S. Rezgui, G. Swift, C. Carmichael, Initial Single-event effects testing and mitigation in the Xilinx Virtex II-Pro FPGA, The north American Xilinx Test Consortium, MAPLD 2005/P211.

70. C.C. Yui, G.M. Swift, C. Carmichael, R. Koga, J.S. George, SEU Mitigation testing of Xilinx Virtex-II FPGAs, in: IEEE proc. Radiat. effects data workshop, 25 July, 2003, pp. 92-97.

71. Michail Vavouras, Single Event Upset Mitigation Techniques in Reconfigurable Hardware, Submitted in part fulfilment of the requirements for the degree of Doctor of Philosophy of Imperial College London September 2017.

72. N. Jing, J.-Y. Lee, Z. Feng, W. He, Z. Mao, L. He, SEU fault evaluation and characteristics for SRAM-based FPGA architectures and synthesis algorithms, Article 13, ACM Trans. Des. Automation Electron. Syst. 18 (1) (Dec. 2012), https://doi.org/10.1145/2390191.2390204, 18 pages.

73. E.S.S. Reddy, V. Chandrasekhar, M. Sashikanth, V. Kamakoti, Detecting SEU-caused routing errors in SRAM-based FPGAs, in: Proc. 18th Int. Conf. On VLSI Design, 2005, pp. 736-741.

74. SOOS, Csaba (European Organization for nuclear Research (CERN)), SEU effects in FPGA, how to deal with them? in: 1st Combined R2E Workshop & School-Days, 2 June 2009.

75. Prasanna Sundararajan, Scott McMillan, Brandon Blodget, Carl Carmichael,Cameron Patterson, Estimation of Single event upset Probability Impact of FPGA designs, MAPLD, 2003.

76. Fernanda Lima Kastensmidt, Evaldo Carlos Pereira Fonseca, Rafael Galhardo Vaz, OdairLelis Gonçalez, Raul Chipana, Gilson In acio Wirth, TID in flash-based FPGA: Power Supply-Current Rise and logic function Mapping effects in Propagation-delay degradation, IEEE Trans. Nucl. Sci. 58 (NO. 4) (Aug. 2011).

77. Stephen L. Clark, TID and SEE Testing Results of Altera Cyclone Field Programmable Gate Array, Mathematics and Statistics Faculty Research&Cre-ative Works, Missouri University of Science and Technology, 2004.

78. Edward Wilcox, Melanie Berg, Mark Friendlich, Joseph Lakeman, Hak Kim, Jonathan Pellish and Kenneth LaBel. A Robust Strategy for Total Ionizing Dose Testing of Field Programmable Gate Arrays. Available:https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120009206.pdf.

79. RaminRoosta, A comparison of radiation hardened and radiation tolerant FPGAs for space applications, JPLD-31228, NASA electron. parts packaging program, Dec. 30, 2004.

80. Lucas A. Tambara, Jorge L. Tonfat, Ricardo Reis, Fernanda L. Kastensmidt, Evaldo CF. Pereira, Rafael G. Vaz, Odair L. Goncalez, Soft error rate in SRAM-based FPGAs under neutron-induced and TID effects, in: Test Workshop-latw, 2014 15th Latin American, IEEE, 2014, pp. 1-6.

81. M. Violante, et al., A New Hardware/Software Platform and a new 1/E neutron source for soft error studies: testing FPGAs at the ISIS facility, IEEE trans. Nucl. Sci. 54 (4) (Aug 2007) 1184-1189.

82. Xilinx, Device Reliability Report, UG116 (v10.5.1), December 19, 2016.

83. IAEA TECDOC Series. Assessment of equipment capability to perform reliability under severe accident conditions. IAEA-TECDOC-1818. Available: http://www-pub.iaea.org/MTCD/Publications/PDF/TE-1818_web.pdf.

84. IEC 61513:2013, Nuclear power plants–Instrumentation and control important to safety – General requirements for systems, International Electrotechnical Commission, 2013-03.

85. International Atomic Energy Agency, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA NS-G-1.3, Vienna, Austria, 2002.

86. Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std. 323-2003, Piscataway, New Jersey, 2003.

87. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Safety Critical Systems', AERB/SG/D-10, Mumbai, India, October 2005.

88. ATOMIC ENERGY REGULATORY BOARD, Computer Based Systems of Pressurized Heavy Water Reactors, AERB/NPP-PHWR/SG/D-25, January 2010.

89. IEC, 2012, Nuclear Power Plants Instrumentation and Control Important to Safety Development of HDL programmed Integrated Circuits for Systems Performing Category A. International Electrotechnical Commission 62566.

90. Advisory Circular, RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, June 2005.

91. Institute of Electrical and Electronics Engineers, Inc., IEEE STD 1012–2004, IEEE Standard for Software Verification and Validation, sponsored by Software Engineering Standards Committee, June 2005.

92. International Standard, IEC 61508-2, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems—Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems.

93. M. Bobrek, D. Bouldin, D.E. Holcomb, S.M. Killough, S.F. Smith, C. Ward, and R.T. Wood, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, U.S.NRC document, NUREG/CR-7006 ORNL/TM-2009/020, Jan 2010. https://www.nrc. gov/ docs/ML1005/ML 100541301.pdf

94. Embedded Digital System Reliability and Safety Analyses, NUREG/GR-0020, February 2001.

95. Institute of Electrical and Electronics Engineers, Inc., IEEE STD 7-4.3.2–2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2003.

96. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Facilities – Electrical Equipment Important to Safety – Qualification, IEC/IEEE 60780-323 std. (Edition 1.0), Geneva, 2016.

97. Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems, IEC 60987:2007, August 2007.

98. Nuclear power plants - Instrumentation and control systems important to safety - Management of ageing, IEC 62342:2007**,** August 2007.

99. M. Ceschia, M. Violante, M. S. Reorda, A. Paccagnella, P. Bernardi, M. Rebaudengo, D. Bortolato, M. Bellato, P. Zambolin, and A. Candelori, Identification and classifica-tion of single-event upsets in the configuration memory of SRAM-based FPGAs, IEEE Trans. Nucl. Sci., Vol. 50, no. 6, pp. 2088–94, Dec. 2003.

100. M. Bellato, P. Bernardi, D. Bortolato, A. Candelori, M. Ceschia, A. Paccagnella, M. Rebaudengo, M. Sonza Reorda, M. Violante, and P. Zambolin, Evaluating the effects of SEUs affecting the configuration memory of an SRAM based FPGA, in Proceeding of the IEEE, DATE'04, Paris, Feb. 16–20, 2004, pp. 584–9.

101. F. H. Schmidt, Jr., Fault tolerant design implementation on radiation hardened by design SRAM-based FPGAs," Ph.D. dissertation, Dept. Aeronautics and Astronautics, Massachusetts Inst. Technol., USA, 2013.

102. M. G. Parris, Optimizing dynamic logic realizations for PR of field programmable gate arrays, MS dissertation, Dept. Electrical Engineering and Computer Science, University of Central Florida, USA, 2008.

103. W. Lie and W. Fengyan, Dynamic PR in FPGAs, in Third International Symposium on Intelligent Information Technology Application, NanChang, Nov. 21–22, 2009, pp. 445-8.

104. Xilinx PR user guide, UG702 (v14.1). April 2012.

105. P. Brinkley, Avnet, and C. Carmichael, SEU mitigation design techniques for the XQR4000, Xilinx appl. note, XAPP181 (v1.0). March 2000.

106. B. Osterloh, H. Michalik, S. Alexander Habinc, and B. Fiethe1, Dynamic PR in space applications, NASA/ESA Conference on Adaptive Hardware and Syst. 978-0-7695-3714-6/09, IEEE. doi:10.1109/AHS.2009.

107. C. Bolchini, A. Miele, and M. Santambrogio, TMR and partial dynamic reconfiguration to mitigate SEU faults in FPGAs, in Proceeding of the IEEE International Symposium of Defect and Fault-Tolerance in Very Large-Scale Integration Systems, Rome, Sept.26–28, 2007, pp. 87–95.

108. C. Bolchini, D. Quarta, and M. Santambrogio, SEU mitigation for SRAM-based FPGAs through dynamic PR, in Proceeding of the ACM/IEEE Great Lake Symposium VLSI, Lago Maggiore, Mar. 11–13,2007, pp. 55–60.

109. I. Herrera-Alzu and M. Lopez-Vallejo, Design techniques for Xilinx Virtex FPGA configuration memory scrubbers, IEEE Trans. Nucl. Sci., Vol. 60, no. 1, pp. 376–85, Feb. 2013.

110. M. Berg, C. Poivey, D. Petrick, D. Espinosa, A. Lesea, K. LaBel, M. Friendlich, H. Kim, and A. Phan, Effectiveness of internal vs. external SEU scrubbing mitigation

strategies in a Xilinx FPGA: Design, test, and analysis, in Proceeding of the IEEE RADECS07, France, Sept. 10–14,2007, pp. 1–8.

111. J. Heiner, B. Sellers, M. Wirthlin, and J. Kalb, FPGA PR via configuration scrubbing," in Proceeding of the IEEE International Conference on Field Programmable Logic and Applications, Czech Republic, Aug. 31–Sept. 2,2009, pp. 99–104.

112. I. Herrera-Alzu and M. Lopez-Vallejo, System design framework and methodology for Xilinx Virtex FPGA con-figuration scrubbers, IEEE Trans. Nucl. Sci., Vol. 61, no.1, pp. 619-29, Feb. 2014.

113. D. K. Pradhan, Fault-Tolerant Computing: Theory and Techniques. Upper Saddle River, NJ: Prentice-Hall, Inc., 1986.

114. N. Rollins, M. Wirthlin, M. Caffrey, and P. Graham, Evaluating TMR techniques in the presence of single event upsets, in Proceeding of the International Conference on Military and Aerospace Programming and Logic Devices, Washington, D.C. Sept. 26–28,2006, p. 63.

115. P. K. Samudrala, J. Ramos, and S. Katkoori, Selective tri-ple modular redundancy (STMR) based single-event upset (SEU) tolerant synthesis for FPGAs, IEEE Trans. Nucl. Sci., Vol. 51, no. 5, pp. 2957–69, Oct. 2004.

116. A. Sari and M. Psarakis, Scrubbing-based SEU mitigation approach for systems-on-programmable-chips, in Proceeding of the IEEE Field-Programmable Technology, New Delhi, Dec. 12–14, 2011, pp. 1–8.

117. C. Carmichael, E. Fuller, P. Blain, and M. Caffrey, SEU mitigation techniques for Virtex FPGAs in space applications, MAPLD99 Poster Paper, p. 24.

118. J.-Y. Lee, C.-R. Chang, N. Jing, J. Su, S. Wen, R. Wong, and L. He, Heterogeneous configuration memory scrubbing for soft error mitigation in FPGAs, in Proceeding of the IEEE International Conference on FPT, Seoul, Dec. 10–12, 2012, pp. 23–8.

119. J. Heiner, N. Collins, and M. Wirthlin, Fault tolerant ICAP controller for high-reliable internal scrubbing, in Proceeding of the IEEE Aerospace, Big Sky, MT, Mar. 1–8, 2008, pp. 1–10.

120. J. Rose and D. Hill, Architectural and physical design challenges for one-million gate FPGAs and beyond, in Proceeding of the ACM/SIGDA International Symposium on FPGAs, Monterey, CA, Feb. 9–11,1997, pp. 129–32.

121. M. I. Masud, FPGA routing structures: A novel switch block and depopulated interconnect matrix architectures, Ph.D. dissertation, Dept. Elect. Computer Eng., Univ. British Columbia, Canada,1999.

122. S. R. Matteo, S. Luca, and V. Massimo, Multiple errors produced by single upsets in FPGA configuration memory: a possible solution, in proceeding of the IEEE, European Test Symposium, Tallinn, May 22–25, 2005, pp. 136–41.

123. H. Ebrahimi, M. S. Zamani, and H. R. Zarandi, Mitigating soft errors in SRAM-based FPGAs by decoding configuration bits in switch boxes, Elsevier Microelectronics. J., Vol. 42, no. 1, pp. 12-20, Jan. 2011.

124. E. S. S. Reddy, V. Chandrasekhar, M. Sashikanth, and V. Kamakoti, Detecting SEU-caused routing errors in SRAM-based FPGAs, in Proceeding of the 18th International Conference on VLSI Design, Kolkata, Jan. 3–7,2005, pp. 736–41.

125. H. R. Zarandi, S. G. Miremadi, D. K. Pradhan, and J. Mathew, Soft error mitigation in switch modules of SRAM-based FPGAs, in Proceeding of the IEEE International Symposium on Circuits and Systems, New Orleans, LA, May 27–30,2007, pp. 141–4.

126. S. Srinivasan, A. Gayasen, N. Vijaykrishnan, and M. Kandemir, Improving soft error tolerance of FPGA configuration bits, in Proceeding of the IEEE/ACM International Conference, San Jose, CA, Nov. 7–11, 2004, pp. 107–10. Prentice-Hall, Inc., 1986.

127. B. S. Gill, C. Papachristou, and F. G. Wolff, A new asymmetric SRAM cell to reduce soft errors and leakage power in FPGA, in IEEE Conference on Design,

Automation & Test in Europe Conference & Exhibition, Nice Acropolis, Apr. 16–20, 2007, pp. 1–6.

128. H. Ebrahimi, M. S. Zamani, and A. Razavi, A switch box architecture to mitigate bridging and short faults in SRAM-based FPGAs, in Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Kyoto, Oct. 6–8,2010, pp. 128–34.

129. A Rohani and H. R. Zarandi, Two effective methods to mitigate soft error effects in SRAM-based FPGAs, Elsevier Microelectronics. Reliab., Vol. 50, no. 1, pp. 1171–80, May 2010.

130. H. Jahanirad and K. Mohammadi, Reliable implementation on SRAM-based FPGA using evolutionary methods, IETE J. Res., Vol. 59, no. 5, pp. 597–603, Sep.– Oct. 2013.

131. E. S. S Reddy, V. Chandrasekhar, M. Sashikanth, V. Kamakoti, and N. Vijaykrishnan, Efficient methodology for detection and correction of SEU-based interconnect errors in FPGAs using partial reconfiguration (extended abstract), in Proceeding of the 13th ACM International Symposium on FPGAs, Monterey, CA, Feb. 22–24,2005, pp. 265.

132. E. S. S. Reddy, V. Chandrasekhar, M. Sashikanth, and V. Kamakoti, Novel CLB architecture to detect and correct SEU in LUTs of SRAM-based FPGAs, in Transactions of IEEE International Conference on Field-Programmable Technology, Brisbane, Dec. 6–8,2004, pp. 121–8.

133. J. Y. Lee, Z. Feng, and L. He, In-place decomposition for robustness in FPGA, in Proceeding of the IEEE/ACM International Conference on Computer Aided Design, San Jose, CA, Nov. 7–11,2010, pp. 143–8.

134. Z. F. Hu, L. He, and R. Majumdar, Robust FPGA resynthesis based on fault-tolerant Boolean matching, in Proceeding of the IEEE/ACM, ICCAD, San Jose, CA, Nov. 10–13,2008, pp. 706–13.

135. Z. Feng, N. Jing, G. S. Chen, Y. Hu, and L. He, IPF: In-place X-filling to mitigate soft errors in SRAM-based FPGAs, in Proceeding of the IEEE International Conference on Field Programmable Logic and Applications, Chania, Sep. 5–7,2011, pp. 482–5.

136. Z. Feng, Y. Hu, L. He, and R. Majumdar, IPR: In-place reconfiguration for FPGA fault tolerance, in Proceeding of the IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, Nov. 2–5, 2009, pp. 105–8.

137. N. Jing, J.Y. Lee, W. He, and Z. Mao, Mitigating FPGA interconnect soft errors by in-place LUT inversion, in Proceeding of the IEEE/ACM, ICCAD, San Jose, CA, Nov. 7–10,2011, pp. 582–6.

138. J. Su, J.-Y. Lee, C. Wu, and L. He, In-place LUT polarity inversion to mitigate soft errors for FPGAs, in IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, Storrs, CT, Sep.19–20,2016, pp.81–6.

139. Anurag Tiwari, Karen A. Tomko, Enhanced Reliability of Finite-State Machines in FPGA Through Efficient Fault Detection and Correction, IEEE Transactions on reliability, Vol. 54, No. 3, Sept. 2005.

140. Anurag Tiwari, Karen A. Tomko, Saving Power by Mapping Finite State Machine into Embedded Memory Blocks in FPGAs, IEEE Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 16-20 Feb. 2004, Vol. 2, pp. 916-921.

141. Maico Cassel, Fernanda Lima Kastensmidt, Evaluating One-Hot Encoding Finite State Machines for SEU Reliability in SRAM-based FPGAs, Proceedings of the 12th IEEE International On-Line Testing Symposium (IOLTS'06), Como, Italy, 10-12 July 2006.

142. Fernanda Lima, Luigi Carro, Ricardo Reis, Designing Fault-Tolerant Systems into SRAM-based FPGAs, DAC'03, Anaheim, California, USA, 2-6 June, 2003.

143. Kumar, Nand, Darren Zacher, Automated FSM error correction for single event upsets, Military and Aerospace Programmable Logic Device (MAPLD) International Conference, Washington, DC, USA. Sep. 2004.

144. R. Rochet, R. Leveugle, G. Saucier, Analysis and Comparison of Fault Tolerant FSM architectures based on SEC codes, The IEEE International Workshop on Defect and Fault Tolerance in VLSI Systems, Venice, Italy, 27-29 Oct. 1993.

145. Andrzej Krasniewski, Concurrent Error Detection for FSMs Designed for Implementation with Embedded Memory Blocks of FPGAs, 10th Euromicro Conference on Digital System Design Architectures, Lubeck, Germany, 29-31 Aug 2007.

146. Aiman H. El-Maleh, Ayed S. Al-Qahtani, A finite state machine based fault tolerance technique for sequential Circuits, Microelectronics Reliability, Elsevier , Vol. 54, Issue 3, March 2014, pp. 654-661.

147. Shailesh Niranjan, James F. Frenzel, A Simplified Approach to Fault Tolerant State Machine Design for Single Event Upsets, IEEE Transactions on Reliability, Vol. 45. No. 1, March 1996.

148. C. Bolchini, R. Montandon, F. Salice, D. Sciuto, Design of VHDL-Based Totally Self-Checking Finite State Machine and Data-Path Descriptions, IEEE Trans. Very Large-Scale Integration Systems, Vol. 8, No. 1, Feb. 2000.

149. S. Baloch, T. Arslan, A. Stoica, Design of a Single Event Upset (SEU) Mitigation Technique for Programmable Devices, Proceedings of the 7th International Symposium on Quality Electronic Design (ISQED'06), San Jose, CA, USA, 27-29 March 2006.

150. Kai-Chiang Wu, Marculescu. D, Soft error rate reduction using redundancy addition and removal, Design Automation Conference, Anaheim, CA, USA, 8-13 June 2008.

151. Kai-Chiang Wu, Marculescu. D, Power-aware soft error hardening via selective voltage scaling, IEEE International Conference on Computer Design (ICCD 2008), Lake Tahoe, CA, USA, 12-15 Oct. 2008.

152. K.-C. Wu, D. Marculescu, Clock skew scheduling for soft-error-tolerant sequential circuits, Automation & Test in Europe Conference & Exhibition (DATE 2010), 8-12 Mar. 2010, Dresden, Germany.

153. Henry Selvaraj, Mariusz Rawski, Tadeusz Łuba, FSM Implementation in embedded memory blocks of programmable logic devices using functional decomposition, Proc. Int. Conf. on Information Technology: Coding and Computing, Las Vegas, NV, USA, 5-7 April 2002, pp. 355-360.

154. Jamuna. S, Agrawal.V.K, Implementation of bistcontroller for fault detection in CLB of FPGA, International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 15-16 March 2012, pp. 99-104.

155. Fernanda Gusmao de Lima, Designing single event upset mitigation techniques for large SRAM-based FPGA devices, PhD Thesis, Porto Alegre, 11 February 2002.

156. Christoforos N. Hadjicostis, Finite-State Machine Embeddings for Non-concurrent Error Detection and Identification, Journal of Latex class files, Vol. 1, No. 11, Nov. 2002.

157. https://www.tutorialspoint.com/what-is-hamming-distance

158. Satyabrata Sarangi and Swapna Banerjee, Efficient Hardware Implementation of Encoder and Decoder for Golay Code, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., Vol. 23, No. 9, Sept. 2015.

159. Scott A. Vanstone, Paul C. van Oorshot, An introduction to error correcting codes with applications, Springer, 1989.

160. Ankita Pramanik, Implementing fast and simple FEC for ultra high frequency ratio, Nat. Conf. Communication (NCC), 02/2012.

161. http://aqdi.com/articles/using-the-golay-error-detection-and-correction-code-3/

162. G. Swift and G. Allen. Virtex-5QV Static SEU Characterization Summary. Technical report, Xilinx Radiation Test Consortium, July 2012. 35, 42, 44, 62, 64, 66, 112.

163. Ken Chapman. XAPP 864 SEU Strategies for Virtex-5 Devices. Xilinx, v2.0 edition, April 2010. 41, 53, 56, 70, 71, 72, 76, 79, 80, 82, 83, 86, 128.

164. Sandi Habinc. Lessons Learned from FPGA Developments, September 2002. Technical Report. Gaisler Research.

165. https://blogs.synopsys.com/breakingthethreelaws/2012/02/%E2%80%9Cverification-or-validation-what-do-you-think%E2%80%9D/

166. Rob Dekker, What's the Difference Between VHDL, Verilog, and SystemVerilog? SEP 17, 2014.
Available: https://www.electronicdesign.com/resources/whats-the-difference-between/article/21800239/whats-the-difference-between-vhdl-verilog-and-systemverilog

167. Arcas Abella O., Sonmez N, Blue Spec System Verilog, In: Koch D., Hanning F., Ziener D. (eds) FPGAs for software programmers, Springer, cham., 2016.

168. W. Gibbons and H. Ames. Use of FPGAs in Critical Space Flight Applications - A Hard Lesson. In Proceedings of the Military and Aerospace Applications of the Programmable Devices and Technologies Conference. National Aeronautics and Space Administration (NASA), 1999.

169. A. Fern´andez-Le´on. Field programmable gate arrays in space. IEEE Instrumentation Measurement Magazine, 6(4):42–48, 2003.

170. M. Spachmann, Automatic generation of parallel CRC circuits, IEEE Des. Test. Comput., vol. 18, no. 3, pp. 108-114, May/Jun. 2001.

171. V. Sieh, O et al., VERIFY: evaluation of reliability using VHDL models with embedded fault description, Proc. of the International Symposium on Fault-Tolerant Computing, Jun. 1997, pp. 32-36.

172. L. Entrena et al., Soft Error Sensitivity Evaluation of Microprocessors by Multilevel Emulation-Based Fault Injection, Trans. On Computers, pp.313-322, 2012.

173. Mojtaba Ebrahimia, Abbas Mohammadi, Alireza Ejlali, Seyed Ghassem Miremadi, A fast, flexible, and easy-to-develop FPGA-based fault injection technique, Microelectronics Reliability 54 (2014) 1000–1008, Elsevier.

174. D. Gil, J. Gracia, J.C. Baraza, P.J. Gi, Study, comparison and application of different VHDL-based fault injection techniques for the experimental validation of a fault-tolerant system, Microelectronics Journal 34 (2003) 41–51, Elsevier.

175. Wassim Mansour, Raoul Velazco, An automated SEU fault-injection method and tool for HDL-based design, J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

176. Chu, pong P, RTL hardware design using VHDL, A Wiley InterScience Publication, USA, ISBN: 978-0-471-72092-8, pp.313-373, 2006.

177. Tambara, Lucas A., Jorge L. Tonfat, Ricardo Reis, Fernanda L. Kastensmidt, Evaldo CF Pereira, Rafael G. Vaz, and Odair L. Goncalez, Soft error rate in SRAM-based FPGAs under neutron-induced and TID effects, In Test Workshop-LATW, 2014 15th Latin American, pp. 1-6. IEEE, 2014.

178. M. Violante et al, A New Hardware/Software Platform and a new 1/E neutron source for soft error studies: Testing FPGAs at the ISIS facility, IEEE trans. Nuclear Science, Vol. 54, no. 4, Aug 2007, pp. 1184-1189.

179. José Rodrigo Azambuja, Gabriel Nazar, Member, Paolo Rech, Member, Luigi Carro, Fernanda Lima Kastensmidt, Thomas Fairbanks, and Heather Quinn, Evaluating Neutron Induced SEE in SRAM-Based FPGA Protected by Hardware- and Software-Based Fault Tolerant Techniques, IEEE Trans. Nuclear Science, Vol. 60, No. 6, Dec. 2013.

180. Mattias Ohlsson, Peter Dyreklev, Karin Johansson, Peter Alfke, Neutron Single Event Upsets in SRAM based FPGAs.Xilinx Application note. Available: https://www.xilinx.com/appnotes/FPGA_NSREC98.pdf

181. Fernanda Lima Kastensmidt, Evaldo Carlos Pereira Fonseca, Rafael Galhardo Vaz, Odair Lelis Gonçalez, Raul Chipana, and Gilson Inácio Wirth, TID in Flash-Based FPGA: Power Supply-Current Rise and Logic Function Mapping Effects in Propagation-Delay Degradation, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 58, NO. 4, AUGUST 2011

182. Stephen L. Clark, TID and SEE Testing Results of Altera Cyclone Field Programmable Gate Array, Mathematics and Statistics Faculty Research & Creative Works, Missouri University of Science and Technology.

183. Edward Wilcox, Melanie Berg, Mark Friendlich, Joseph Lakeman, Hak Kim, Jonathan Pellish and Kenneth LaBel, A Robust Strategy for Total Ionizing Dose Testing of Field Programmable Gate Arrays, available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120009206.pdf

184. Ning Ma, Shaojun Wang, Datong Liu, Yu Peng, A run-time built-in approach of TID test in SRAM based FPGAs, Microelectronics Reliability 64 (2016) 42–47.

185. J. A. Felix, M. R. Shaneyfelt, P. E. Dodd, B. L. Draper, J. R. Schwank and S. M. Dalton, Radiation-induced off-state leakage current in commercial power MOSFETs, in IEEE Transactions on Nuclear Science, vol. 52, no. 6, pp. 2378-2386, Dec. 2005. doi: 10.1109/TNS.2005.860724.

186. T.D. Ma & P.V. Dressendorfer, editor, Ionizing radiation effects in MOS devices and circuits, John Wiley & Sons, 1989.

187. S. M. Lee, A Perspective on Fast Breeder Reactor Safety, IGCAR. Available : https://dae.nic.in/?q=node/173

# Thesis Highlight

**Name of the Student:** Nidhin T. S
**Name of the CI/OCC:** IGCAR, Kalpakkam **Enrolment No.:** ENGG02201304014
**Thesis Title:** Study of radiation effects in SRAM based FPGAs for NPP I&C system design
**Discipline:** Engineering Sciences; **Sub-Area of Discipline:** Electronics & Communication Engg.
**Date of viva voce:** 02/November/2020

The aim of the present dissertation was to study the radiation effects in SRAM based FPGAs targeted for NPP I & C system design. As there is no history of data available for commercial grade SRAM based FPGAs used in nuclear applications this study has its significant importance. This study has given focus to cumulative absorbed dose effects due to gamma radiation. As gamma radiation can cause TID effects as well as SEUs in the MOS based devices, an experimental study has been conducted to measure the tolerance level of the system in such environment.

Based on the radiation experiments carried out using Gamma-chamber 5000, it is observed that the device under test (Spartan 6 FPGA) is functionally tolerant up to a radiation dose level of 322 krad, suggesting that if the system is implemented with SEU mitigation techniques, the device can withstand up to 322 krad of accumulated dose without any failure. The major parameter changes have been measured during irradiation. The power supply current variation due to absorbed dose is illustrated in fig.1. For further improvement in efficiency, appropriate shielding can be provided. The efficiency of shielding has been determined using the 2D transport code DORT and IGC-S3 cross-section data set. Based on the computational modelling of shielding box and TLD based dose rate measurement in the Gamma chamber, it is found that the duration of functional time of the device under test can be extended almost two times by using shielding.

A detailed investigation in to various SEU mitigation techniques has been carried out and their efficiencies are quantified based on area overhead, complexity of implementation. Also, a Golay code-based error recovery mechanism has been proposed which can detect and correct up to 3 errors in a block of 24 bits, the state diagram is given in fig.2. SRAM based FPGAs provides a diversity in safety related applications and if deploy inside the RCB it can avoid the extra penetrations for taking out the cables.

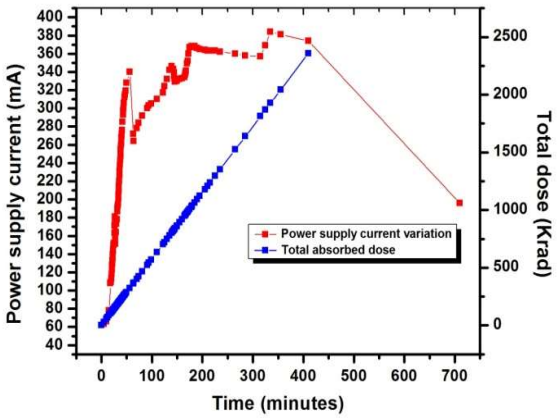



*Figure 1. Power supply current variation due to total radiation absorbed dose-DUT*

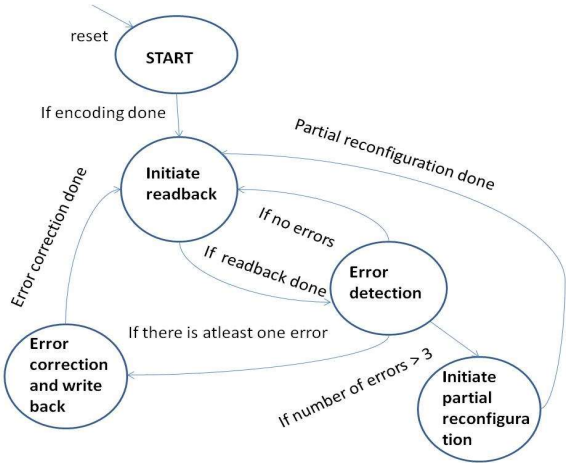



*Figure 2. Control logic state diagram of error recovery mechanism*