RADIATION TOLERANT POWER CONVERTER DESIGN FOR SPACE APPLICATIONS

by

Solomon Mamo Banteywalu

Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Computer Engineering

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

July 2022

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

By: Solomon Mamo Banteywalu

This is to certify that Solomon Mamo Banteywalu's dissertation, titled ***Radiation Tolerant Power Converter Design for Space Applications,*** which was submitted in partial fulfillment of the degree of Doctor of Philosophy (PhD) in Computer Engineering, complies with University regulations and meets accepted standards in terms of originality and quality.

Approved and signed by the board of the Examining Committee

	Name	**Signature**	**Date**
Dean School of Electrical and Computer Engineering	Dr. Bisrat Derebssa		
Supervisor	Prof. Paul Leroux		25/04/2023
Supervisor	Dr. Getachew Bekele		26/04/2023
Supervisor	Prof. Valentijn De Smedt		
Internal Examiner	Dr. Getachew Alemu		
External Examiner	Prof. Jeffrey Prinzie		28/04/23

Keywords

DC-DC converter, satellite. analog to digital converter, sigma-delta modulator, digital controller, ionizing radiation, single event effects, space environment, total ionizing dose, spatial redundancy, temporal redundancy, radiation tolerant, FPGA, PID, DPWM, MTTF, RIF, fault tolerant, fault injection, reliability.

Abstract

Radiation and extreme temperature are the main inhibitors for the use of electronic devices in space applications. Radiation challenges the normal and stable operation of power converters, used as power supply for onboard systems in satellites and spacecrafts. In this circumstance, special design approaches known as radiation hardening or radiation tolerant designs are employed. FPGAs are beneficial for developing low-cost, high-speed embedded digital controllers for power converters, but their components are highly susceptible to radiation-induced faults. In safety and mission-critical systems, like space systems, radiation-induced faults are a major concern. Majority of commercial off-the-shelf (COTS) FPGAs are not developed to function in high radiation environments, with the exception of a handful of circuits that are radiation–hardened at the manufacturing process level at a very high cost overhead, making them less appealing from a performance and economic standpoint.

Design-based techniques are another option for reaching the necessary level of reliability in a system design. This work investigates and designs a novel FPGA-based radiation-tolerant digital controller for DC-DC converters, with applications in space. The controller's radiation-induced failure modes were analyzed in order to develop a mitigation strategy, which included identifying the error modes and determining how existing mitigation approaches could be improved. For FPGA implementation and optimization of the radiation tolerant digital controller, a model-based design approach is presented. To validate the recommended solution strategies, fault injection campaigns are employed.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

A/D	Analog/Digital
ADC	Analog to Digital Converter
ASIC	Application Specific Integrated circuit
BJT	Bipolar Junction Transistor
BPI	Byte Peripheral Interface
CDF	Cumulative Distribution Function
CIC	Cascaded Integrator- Combo
CLB	Configurable Logic Block
COTS	Commercial-of-the Shelf
CME	Coronal Mass Ejection
CMOS	Complementary Metallic Oxide Semiconductor
DAC	Digital to Analog Converter
DC	Direct Current
DD	Displacement Damage
DEC	Decimator
DPWM	Digital Pulse Width Modulator
DSET	Digital Single Event Transient
DSP	Digital Signal Processor
DUT	Design Under Test
ESA	European Space Agency
EEPROM	Erasable Electrically Programmable Read Only Memory
EMI	Electromagnetic Interference
FIR	Finite Impulse Response
FIS	Fault Injection System
FPGA	Field Programmable Gate Array
FMR	Five Modular Redundancy
GCR	Galactic Cosmic Rays
HDL	Hardware Description Language
HEO	High Earth Orbit
IC	Integrated Circuit

I/O	Input/output
JTAG	Joint Test Action Group
LASER	Light Amplification by Stimulated Emission of Radiation
LEO	Low Earth Orbit
LET	Linear Energy Transfer
LVDS	Low-Voltage-Differential-Signalling
LPF	Low Pass Filter
LUT	Lookup Table
MEO	Medium Earth Orbit
MIL	Model in the Loop
MOSFET	Metallic Oxide Semiconductor Field Effect Transistor
MeV	Mega electron Volt
MBU	Multi-Bit Upset
MTTF	Mean Time to Failure
MUX	Multiplexer
NASA	National Aeronautics and Space Administration
PDF	Probability Distribution Function
PID	Proportional Integral Derivative
PWM	Pulse Width Modulator
RB	Radiation Belt
RHBD	Radiation Hardening by Design
RIF\RII	Reliability Improvement Factor\Reliability Improvement Index
SAA	South Atlantic Anomaly
SEB	Single Event Burnout
SEE	Single Event Effect
SEGR	Single Event Gate Rupture
SEFI	Single Event Functional Interrupt
SEL	Single Event Latchup
SET	Single Event Transient
SEU	Single Event Upset
Si\SiO2	Silicon\Silicon dioxide
SP	Solar Particles
SPI	Serial Peripheral Interface

SRAM	Static Random-Access Memory
TID	Total Ionizing Dose
TMR	Triple Modular Redundancy
VCO	Voltage Controlled Oscillator
VHDL	Very High-Speed Hardware Description Language
VMC	Voltage Mode Controller

Declaration

I, the undersigned, attest that the work contained in this thesis has never been submitted for an award at this or any other higher education institution. Except where appropriate references are made, the thesis contains no content previously published or generated by another individual, to the best of my knowledge and belief.

Signature: 

Solomon Mamo Banteywalu

Date: 23/04/2023

Acknowledgments

In terms of professional experience and personal growth, the last five years have been incredibly intriguing. The PhD provided me with the opportunity to meet and work with a wide range of fascinating, highly skilled, and distinctive individuals. The study given here is the result of a lot of hard work and constructive discussions. I would want to thank everyone who took part in this study because the success of a PhD is dependent not only on personal drive and effort, but also on the direction of those who work with you.

First and foremost, I want to express my gratitude to Professor Paul Leroux and Professor Getachew Bekele for their assistance and guidance in the completion of this study. You both have a beautiful optimistic attitude and a high level of goodness, which is really beneficial to my studies as well as my personal development. Thank you once again for assisting me in determining my career path.

I would also like to express my gratitude to professor Valentijn De Smedt and Dr. Bassem Khan for their insightful comments and enthusiastic support of my research work.

I would like to thank the Ministry of Education and the GIZ GmbH-funded HGPP project for providing me with the opportunity to do research at KU Leuven in Belgium.

I would like to express my gratitude to Dr. Dereje Hailemariam and Professor Koen Eneman for their assistance during my time at KU Leuven.

Finally, I want to express my gratitude to my wonderful wife, children, extended family, and friends; your unwavering support was selfless and limitless, and I will always be grateful.

-

Chapter 1: Introduction

1.1 MOTIVATION

Man-made objects such as satellites and spacecrafts are launched into space to aid humanity in various ways. Satellites, for example, are becoming more prevalent in our everyday lives. They help us with media distribution, internet access, infrastructure monitoring, military applications, and weather forecasting, among other things. Satellites can also help developing countries, like Ethiopia, in attracting investment and accomplishing long-term economic goals [1]. To provide efficient services, these objects require complex electronic systems.

Power converters are vital components of today's electronic circuits. They are used as power supply for satellite and spacecraft onboard systems. They serve as power conditioning devices, transferring power to space system subcomponents at a variety of voltages and current levels. Figure 1.1 depicts the power distribution architecture of a typical satellite or spacecraft [2].

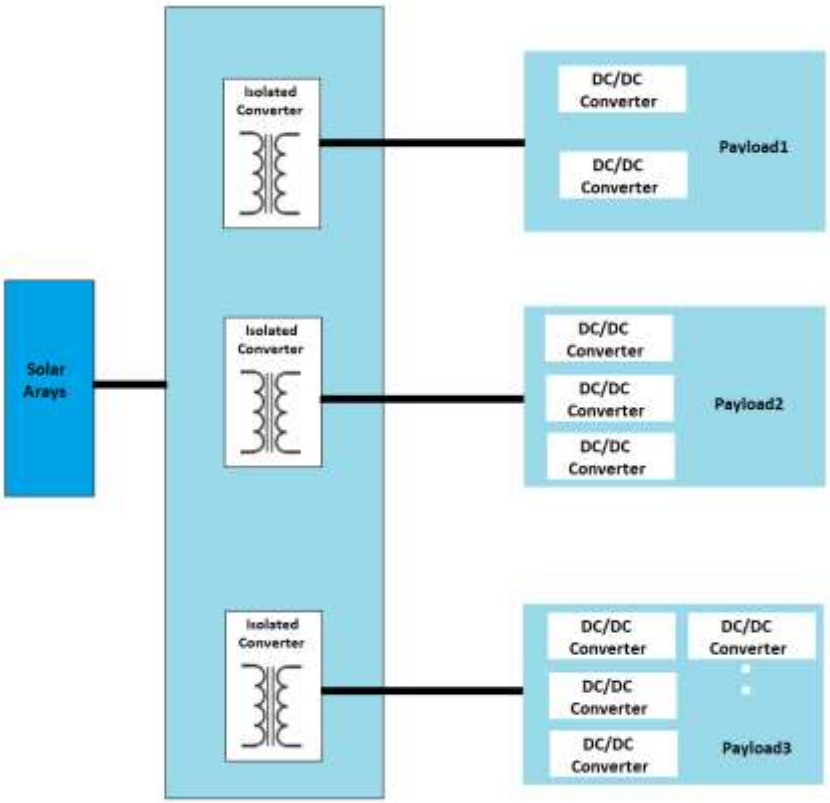


Figure 1.1. Typical space system power distribution architecture.

Consequently, they are crucial components that have a significant impact on the overall reliability of space applications. Space and military applications, unlike commercial uses, require circuits that can operate in a radiation environment [3].

In the space radiation environment, high-energy particles like heavy ions, protons, and electrons can interfere with the operation of electronic circuits causing them to malfunction. These particles have sufficient energy to ionize atoms and release electrons [4][5]. When an ionizing particle passes through an electronic circuit in space, several effects can happen. In semiconductor devices like transistors, an ionizing particle deposits charge in the form of electron-hole pairs in its path. The charges may recombine in an unharmful manner, but they may also build-up on circuit nodes, causing erroneous current and voltage anomalies.

Since solar arrays are often employed as a source of electrical energy in space and most space systems' microelectronic subcomponents use direct current, DC-DC converters are the most prominent power converter types used [6]. The power conditioning units of space systems use both isolated and non-isolated DC-DC converters [6], [7].

DC-DC converters used in space-based systems, in contrast to DC-DC converters used on ground, pose a significant reliability challenge due to possible component failures induced by radiation. Radiation damages converter components like power switches and pulse-width modulator (PWM) controllers, causing design parameters like efficiency, phase margin, and converter output voltage to deviate from their intended values, resulting in parts of the space system supplied from these converters to malfunction or, in the worst-case scenario, to completely fail [8]. This necessitates the development of radiation-tolerant DC-DC converters for usage in space and emphasizes the importance of the study topic.

The demand for increased capabilities at a lower cost has traditionally spurred the development of power converters [9]. As a result, analog control of power converters is usually the favoured method due to its lower cost as compared to digital control. Digital control of power converters, on the other hand, has a number of advantages over analog control, including lower sensitivity to noise and component parameter variations, as well as the ability to meet the implementation of complex algorithms [10]. A digital controller can also be hardened more easily against radiation-induced faults than its analog counterpart.

Recently, digital control of power converters has gained a lot of attraction. On the other hand, the majority of today's space power systems are created with antiquated technology and electrical components that are many generations behind current technological capabilities [11]. The demand for pioneering technology in space, such as Field Programmable Gate Arrays (FPGAs), has grown in tandem with the quest for higher performance and shorter design timelines. As a result, digital technologies are expected to play a significant role in the development of power converters for space applications in the future.

1.2 PROBLEM STATEMENT

The use of static random-access memory (SRAM) based field-programmable gate arrays (FPGAs) for the design of digital control algorithms for DC-DC converters intended for space applications has gained favour in recent years [12], [13]. SRAM-based FPGAs are well suited for space-based applications due to benefits such as flexibility, short turn-around time, and on-orbit reconfiguration capability. Furthermore, Commercial-Off-The-Shelf SRAM-based FPGAs (COTS-SRAM-based FPGAs) are products that have been widely used in a variety of applications where performance and cost-effectiveness are major considerations. Radiation-hardened SRAM-based FPGAs are also available, however, they can cost up to 100 times as much as conventional COTS-SRAM-based FPGAs, while often lagging 2-3 generations behind in terms of manufacturing technology. COTS-SRAM-based FPGAs, on the other hand, are not designed for operation in a radiation environment and are thus prone to radiation-induced errors produced by Single Event Effects (SEEs). High-energy particles passing across the device structure disturb the device charge equilibrium, resulting in voltage and current abnormalities at the device terminals, causing SEEs. Given the benefits they provide, COTS-SRAM-based FPGAs can be used for space-based applications if the risk of SEEs is minimized.

Effective mitigation approaches must be used to implement critical systems using COTS-SRAM-based FPGAs. To avert failures, fault tolerance techniques are applied. The most prevalent fault tolerance spatial redundancy technique is triple modular redundancy (TMR). Because it only operates by modifying the high-level design description, the TMR is ideal for COTS-SRAM-based FPGAs. It does not necessitate any changes to the device's hardware [14]. It however has some drawbacks and limitations [15],[16]:

- The design logic's size is multiplied by three, resulting in a >200 percent area overhead cost.
- Reliability concern for extended mission duration applications, i.e., TMR is equal to a system of two modules in series with a failure rate double that of a simplex (unmitigated) system in terms of reliability after the first failure.
- The system as a whole fails when two modules fail at the same time.

1.3 GOALS OF THE DISSERTATION

The primary purpose of this study is to develop a better SEE soft error mitigation technique for user logic implementation in SRAM-based FPGAs. The strategy is based on radiation hardening by design methodologies, notably the redundancy approach, and can be used to implement a radiation tolerant DC-DC converter PWM controller. With reasonable resource overhead, it is capable of masking multiple occurrences of flip-flops upsets and Single-Event-Functional-Interrupts (SEFIs) in the user logic.

One of the specific objectives is to use commercially available SRAM-based FPGAs for cost reduction. Another specific aim is to enhance reliability over existing methods in order to extend the mission time for which the technique can be used without functional failure. The approach is validated using the fault injection method.

1.4 DISSERTATION SCOPE

The following limitations are made to keep a consistent and straightforward approach.

- The mitigation methods proposed in this work are suitable for the design of radiation tolerant half-duty limited DC-DC converters, inverters, or similar circuits and/or applications.

1.5 PUBLICATIONS

The following research outputs were published in peer-reviewed publications as a result of this study, with some of the study findings included.

- Peer-reviewed journal

- Banteywalu SM, Bekele G, Khan B, De Smedt V, Leroux P. A High-Reliability Redundancy Scheme for Design of Radiation-Tolerant Half-Duty Limited DC-DC Converters. *Electronics.* 2021; 10(10):1146.
- Banteywalu SM, Khan B, De Smedt V, Leroux P. A Novel Modular Radiation Hardening Approach Applied to a Synchronous Buck Converter. *Electronics*.2019;8(5):513.

1.6 DISSERTATION OUTLINE

The remaining portions of the dissertation have been organized into the following chapters.

- Chapter 2: This chapter discusses the sources of radiation in space and how radiation interacts with matter, as well as how radiation can cause problems in electronics devices. Radiation impacts are categorised according to the mechanisms that cause them to manifest with emphases on single event effects (SEEs). A number of commonly used radiation mitigation techniques are also presented.
- Chapter 3: This chapter exhibits an overview of the methods used to analyze the reliability of systems implemented in SRAM-based FPGAs. The chapter also discusses currently used radiation testing methodologies focusing on fault injection methods.
- Chapter 4: This chapter provides an overview of the PWM controller IC architecture as well as a review of previous PWM controller radiation testing reports.
- Chapter 5: This chapter goes through the specifics of the suggested hybrid redundancy strategies. The recommended design flows are described in detail in order to obtain a user logic design that is protected by the approaches.
- Chapter 6: The details of the case studies used, as well as the fault injection method used and the procedure used for the FPGA implementation of the system, are discussed in this chapter.

- Chapter 7: In comparison to existing solutions, this chapter describes the characteristics of the proposed strategies in terms of area overhead, correction capability, and mean time to failure. The proposed methodologies' performance in terms of reliability are also discussed.
- Chapter 8: Finally, the conclusion remarks and the direction for possible future works are given in this chapter.

Chapter 2: Effects of Radiation on Electronics

All electronics are impacted when they are subjected to ionizing radiation. Ionizing radiation is a form of radiation with enough energy to remove electrons from chemical bonds. According to reports, radiation in space is to blame for 45 percent of satellite and spacecraft failures [17]. The operating environment in space is substantially different from that of regular ground-level applications. The lack of atmosphere in space poses a variety of problems. However, the presence of ionizing radiation and its effect on semiconductors generates an environment that has a substantial impact on electronic circuit reliability [18]. This is the parameter that will have the greatest impact on the DC-DC converters used in satellites, which are the focus of this research. As a result, in this chapter, we will discuss space radiation sources, the concept of radiation impacts on electronics, and some existing mitigation strategies.

2.1 SOURCES OF RADIATION IN SPACE

Observing the deflections of ionized tails from comets due to solar winds provided early signs of the presence of radiation, long before mankind launched satellites into space. In 1958, energetic particles were discovered in the Van Allen belts around Earth. After that, it became evident that for space travel missions, an exceedingly disruptive and demanding environment must be addressed, which affects electronic devices and destroys onboard equipment [19].

The Sun, which produces solar particles, the Van Allen belts, which trap protons and electrons within Earth's magnetic field lines, and Galactic Cosmic Rays (GCRs), which are high-energy protons or heavy-ions from beyond the solar system, are the three sources of ionizing radiation in space [20].

2.1.1 Galactic Cosmic Rays (GCRs)

Galactic Cosmic Rays (GCRs) are ions with a high energy that come from beyond our solar system. Protons account for about 85% of these particles, with alpha particles accounting for 14% and heavy ions contributing for 1% [21],[22]. The GCR

stream that reaches the solar system interacts with the solar wind and is partially attenuated. During the solar maximum, when the solar wind is strongest, this attenuation is greatest. The GCR flow, on the other hand, is greatest during solar minimum, when there is less attenuation due to less solar wind. Lower-energy particles are primarily suppressed by this action, while higher-energy particles are less affected [22],[23]. Incident particles ranging from protons to heavy ions make up the linear energy transfer (LET) spectra, which can be interpreted from the energy spectra shown in Figure 2.1 [22]. The LET is used to characterize the energy loss in a material of ionized particles per unit length, and it's significant for particle material interaction analysis, which is discussed in section 2.2.

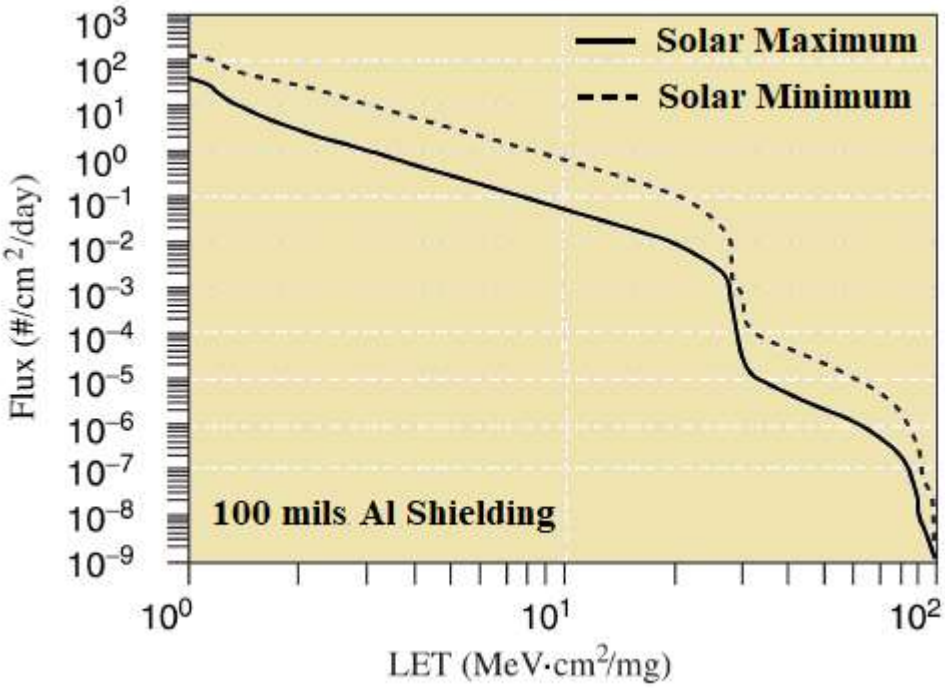


Figure 2.1. Galactic cosmic rays' spectrum [22].

The energy of ions in GCR spreads to hundreds of MeV range, and they travel at near the speed of light. As a result, when they penetrate any material, their in-material ranges are quite large, which causes secondary particle showers when they collide. Due to secondary particles, shielding is ineffective after the first few millimetres of aluminium shielding attenuates the lowest-energy component of the spectrum [24].

2.1.2 Solar Particles (SPs)

The sun’s activity generates these particles, which are similar to GCRs. Their energies, however, are lower. The three forms of radiation produced by the sun's activity that cause SPs are solar flares, Coronal Mass Ejections (CMEs), and solar wind. Because CMEs and solar flares accelerate particles at a far higher speed and energy than the solar wind, they have significant impact on electronics on board spacecraft [25].

During solar outbursts created by CMEs, large fluences are experienced. The solar material ejected by the CME also interacts with the Earth's magnetic field, significantly reducing natural shielding. X-rays, gamma rays, heavy ions, and subatomic particles such as electrons, protons, and neutrons are commonly found in SPs. Figure 2.2 shows what a typical solar eruption looks like.

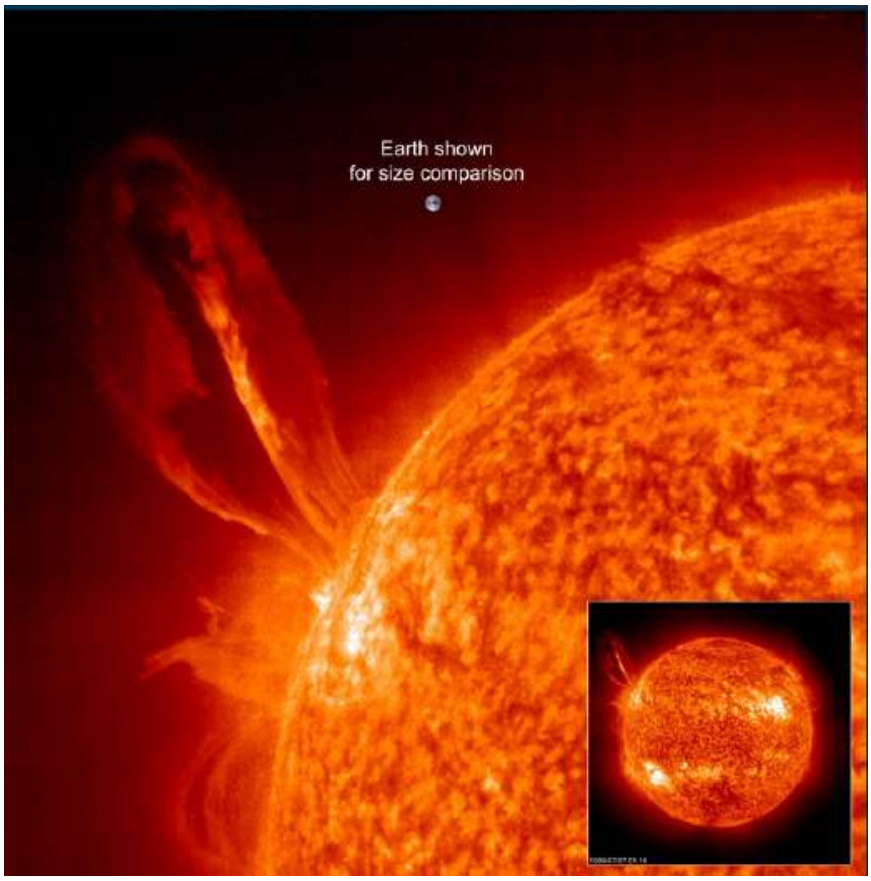


Figure 2.2. Typical solar eruption (courtesy of ESA).

2.1.3 Radiation Belts (RBs)

The planet's magnetic field traps solar and GCR particles, allowing radiation belts to form near planetary bodies in our solar system [26]. The Van Allen belts, which are close to our planet, were discovered in 1958 by James A Van Allen, an American scientist who designed the sensors on board the first US spacecraft (Explorer 1) [26],[27]. Electrons and protons make up the majority of the trapped particles. These particles are driven at nearly the speed of light back and forth along the magnetic field contours.

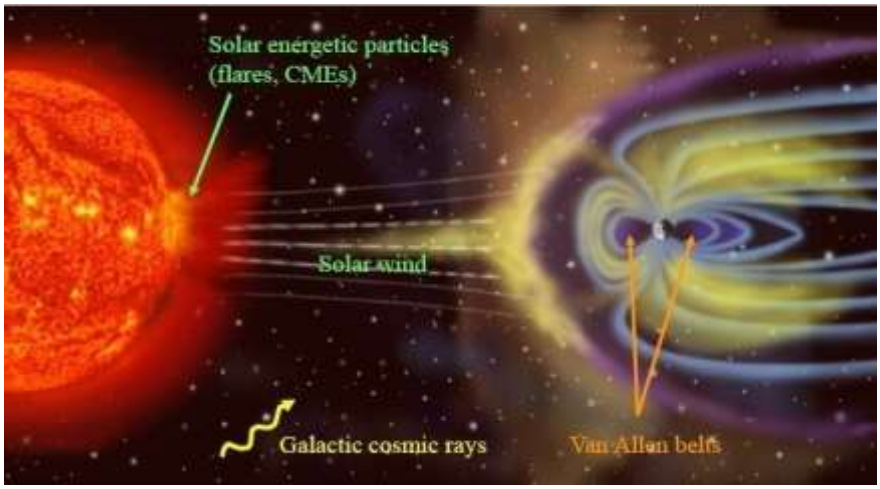


Figure 2.3. The effect of SPs such solar winds and CMEs as well as GCRs on the configuration of the Earth's magnetosphere (courtesy of NASA).

At distances ranging from 2000 km to 35,000 km, trapped protons with a wide variety of energy can have an influence on electronics. Protons of lower energy (~ 1MeV) dominate at 35,786 km and above. The South Atlantic Anomaly (SAA) is another region of large proton intensity. The magnetic poles of the Earth are 11 degrees apart from the rotational axis. Due to the magnetic poles tilting, radiation belts are closest to earth near Brazil, at the so-called SAA region [28],[29].

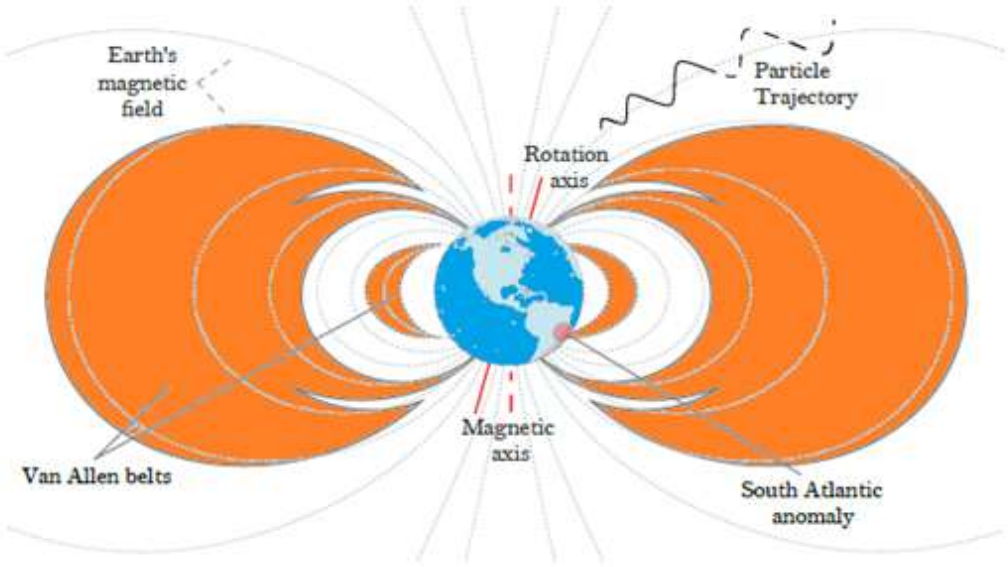


Figure 2.4. The Van Alen radiation belt and South Atlantic Anomaly (SAA) [28].

The SAA is located at significantly lower altitude and has an impact on satellites in low earth orbits (LEOs) ranging from 167 km to 2000 km.

2.2 RADIATION MATTER INTERACTIONS

Ionization occurs when a charged particle (for example, an ion) passes through the target material and creates electron-hole pairs along the way, ionizing the atoms. When a charged particle travels through matter, it loses kinetic energy and hence slows down, eventually coming to a stop in the target material. Nuclear interactions, interaction with the atomic nucleus, is also another way through which the incident particle loses its energy in materials [30]. The term integral linear energy transfer is used to describe the ionization induced by charged particles interacting with the substance they pass through. The transfer of energy from the charged particle to the target nucleus causes ionization, which results in the release of bound electrons and the formation of electron-hole pairs.

The energy loss per unit path length of a particle as it passes through a material is referred to as linear energy transfer (LET). It is measured in MeV-cm2/mg [31],[32].

$$LET = \frac{dE}{dx} \cdot \frac{1}{\rho} \qquad (2.1)$$

where *dE* is energy lost by the incident particle, *dx* the unit length and ρ the material density. If LET is known, it is possible to estimate the amount of generated charge (Q_{gen}) using the following expression.

$$Q_{gen} = \frac{q \cdot LET \cdot \rho \cdot x}{E_{feh}} \qquad (2.2)$$

where q denotes the unit charge, E_{feh} denotes the average energy used to create an electron-hole pair (in Si this is about 3.6 eV), and x denotes the length of the path.

2.3 RADIATION EFFECTS

Radiation has two significant effects on electronic circuits.

1. The passage of a single particle through a semiconductor material causes random, immediate interruptions known as single event effects (SEEs). For any given radiation incident, an SEE could cause failures in multiple device parts.
2. Dose effects are defined as long-term operational or parametric shifts associated with prolonged radiation exposure, which eventually cause the semiconductor device to drift out of tolerance and fail. Displacement Damage (DD) and Total Ionizing Dose (TID) are the two major effects of long-term operation in a radiation environment.

2.3.1 Displacement Damage (DD)

Atoms in the crystal lattice may be displaced by energetic particles as a result of continuous exposure to radiation, through nuclear interactions or scattering, which eventually leads to crystal lattice defects. A vacancy and an interstitial defect, known a Frenkel pair [32],]33], can be created inside the device. Due to the creation of recombination spots in the crystal structure, displacement damage usually leads to a decrease in the quantity of minority carriers. The DD has a significant impact on Bipolar Junction Transistors (BJTs) because BJTs' basic operation is based on the concentration levels of majority and minority carriers in the device.

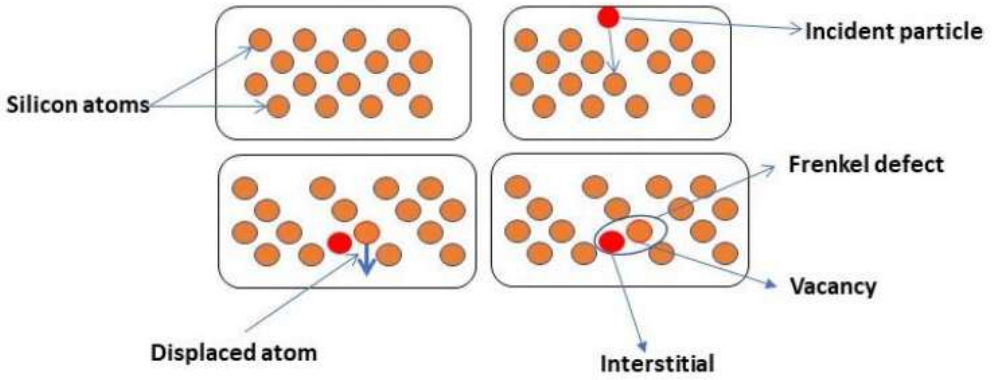


Figure 2.5. Crystal defects as a result of displacement damage.

2.3.2 Total Ionization Dose (TID)

TID stands for the total radiation dose accumulated by ionization effects on electronics over time, resulting in long-term device parameter changes. TID phenomena are driven by the formation, transit, and trapping of holes in insulating layers or at the silicon/ silicon-dioxide (Si/SiO2) interface. The accumulated charge will eventually lead to a radiation-induced failure, if the device dose limit is exceeded [34].

Gray (Gy) is a unit of TID that is defined as incident absorbed energy per kilogram: 1Gy = 1J/kg. The rad, which is defined as 1rad = 0.01Gy, is another often used unit for TID [35], [36].

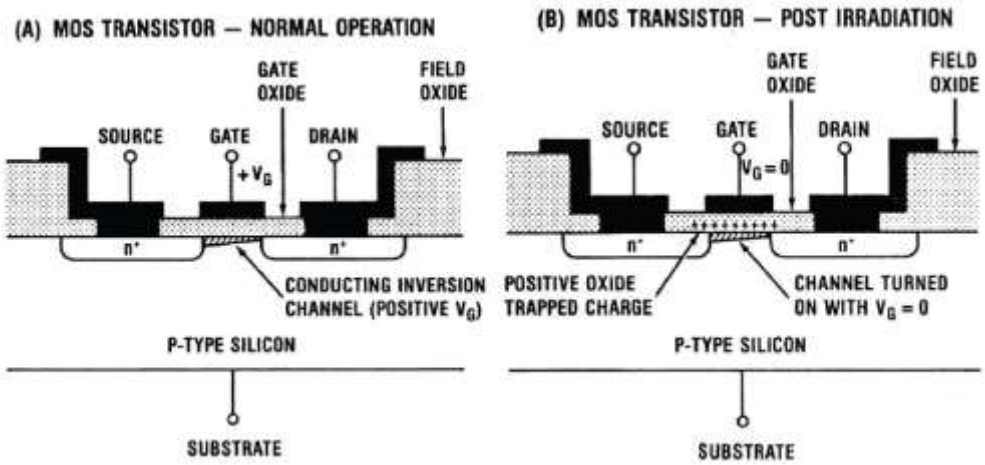


Figure 2.6. Radiation-induced charging in n-channel MOSFETs gate oxide: (a) normal operation (b) after-irradiation [36].

TID has a range of effects on transistors, such as a shift in the threshold voltage, device leakage, effect on switching speed, loss or reduced functionality, and so on.

TID and DD effects develop gradually, after days, weeks, or even years of device operation, depending on the radiation intensity, before full failure, whereas SEEs are sporadic events that frequently affect the functionality of electronic circuits as soon as they occur. The focus of this dissertation is to reduce the effects of SEEs on electronic circuits, specifically on DC-DC converters used in space applications. As such, the next section concentrates on SEEs and their numerous subdivisions.

2.3.3 Single Event Effects (SEEs)

In an electronic device, an energetic particle traveling at high speeds across the device might cause transitory behaviour or an abrupt behavioural change. Such effects are classified as Single Event Effects (SEEs) [37].

A charged particle deposits charge as it travels through a transistor, as shown in Figure 2.7.

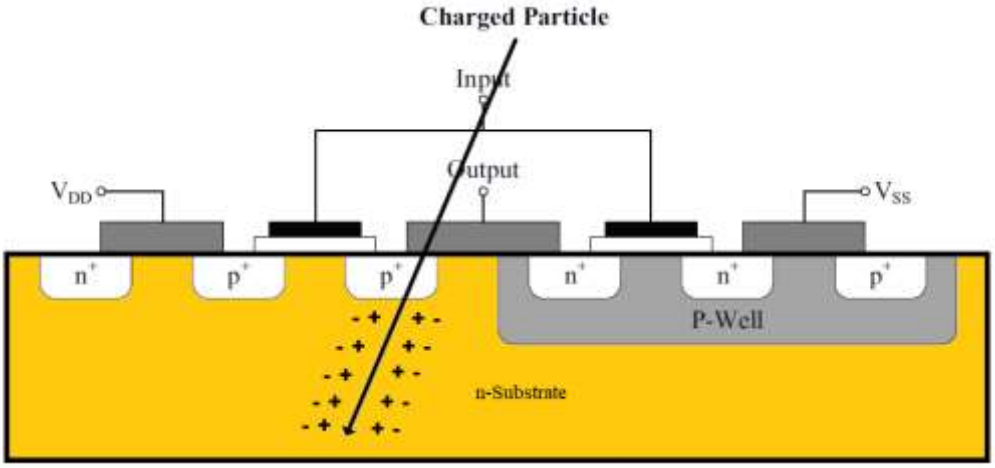


Figure 2.7. Charge deposited on a transistor's substrate by a charged particle.

To alter the operation of a circuit, a charged particle needs to transfer enough charge to a transistor node. The smallest quantity of charge necessary to affect a transistor's operation is known as Q_{crit}, as indicated in the equation below [38],[39].

$$Q_{crit} = C_{node} \cdot V_{node} \qquad (2.3)$$

The capacitance between transistor nodes and ground is C_{node}, while the transistor gate voltage is V_{node}. As transistor process sizes reduce, the node capacitance

and transistor operational voltage also reduce resulting in lower Q_{crit} [39], in effect significantly lowering the charged particle energy required for causing SEEs to occur.

There are two broad categories of SEEs: destructive and non-destructive SEEs. Non-destructive SEEs cause a visible disturbance or corruption in a data state or an output without inflicting damage or destruction to the circuit element itself [40].

The charge disturbance generated by the incident particle might modify the data state of the impacted node if SEEs occur in sequential digital circuits or memory elements. Subsequent writes to the device will correct the erroneous state, but the data will remain faulty and persistent in the system until this happens. If the erroneous data state is read and used in subsequent circuits, such faults might induce failures. The SEE has not harmed the equipment in any way in non-destructive SEEs; only the data has been altered. As a result, non-destructive SEEs are frequently called as "soft errors." [41].

Non-destructive SEEs include single-event transients (SETs), single-event upsets (SEUs), and single-event functional interrupts (SEFIs). Destructive SEEs cause a data state or output to become corrupted, as well as damage or destruction of the circuit element. The physical consequences of a destructive SEE are similar to those of a non-destructive SEE, but the device is permanently damaged or destroyed. "Hard errors" are a term used to describe destructive SEEs. Single-event latchups (SELs), single-event gate rupture (SEGR), and single-event burnout (SEB) are categorised under destructive SEEs.

2.3.3.1 Non-destructive Single Event Effects

2.3.3.1.1 Single Event Transient (SET)

When a single charged particle generates a momentary voltage or current spike, it is called a single event transient (SET). An SET will always occur unless the energetic particle does not have enough energy to reach the semiconductor substrate where the active device portions are located. The spike formed by SET can be latched in a flip-flop and propagate across the circuit if the pulse width is sufficiently wide and happens at the right moment [42]. In general, SETs from larger LET events are more likely to produce bigger voltage spikes and last longer Furthermore, as the operational clock frequency rises, the likelihood of the glitch getting latched increases as well [43].

The term "digital single-event transient (DSET)" refers to an SET that is generated and propagated through digital logic [28], [44], [45]. If the DSETs are below the digital voltage threshold, they will quickly dissipate and have no influence on the system. Larger DSETs, on the other hand, will produce erroneous digital signals, that could cause downstream systems to malfunction. DSETs can also arise and propagate in the clock tree, but only with very high LET events, as clock trees frequently have considerably larger capacitance because of the many distributed nodes [28].

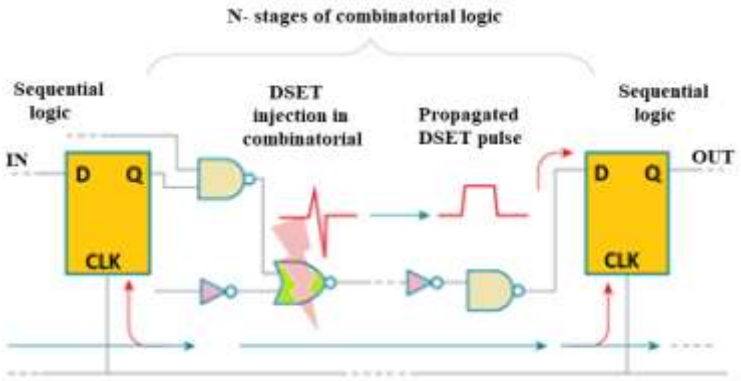


Figure 2.8. Occurrence of DSETs in combinational logic [28].

2.3.3.1.2 Single Event Upset (SEU)

A sustained error known as a single event upset (SEU) occurs when radiation incidents happen inside the node of a data storage element, such as in a static random-access memory (SRAM) bit, a user logic flip-flop, or a latch [46].

The system impact of an SEU varies depending on the type of error and its location, but because the erroneous state is sustained until it is overwritten with new data, SEUs pose a risk to digital system reliability because the erroneous data can be used in downstream processes without the system realizing it is bad. Figure 2.8 shows a change in the state of an SRAM bit-cell as a result of an SEU [47], [48].

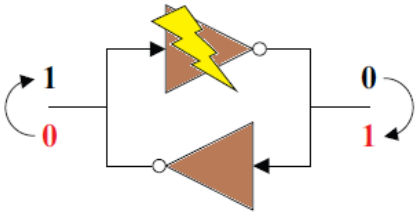


Figure 2.9. SEU Occurrence in SRAM bit-cell.

If the SEU is not masked or corrected, it will likely cause a single event functional interrupt (SEFI). SEUs are divided into two categories. Single Bit Upset (SBU) refers to a change in the state of only one bit, whereas Multiple Bits Upset (MBU) refers to a change in the state of two or more bits [49].

2.3.3.1.3 Single Event Functional Interrupt (SEFI)

When the bit that is flipped (by an SEU) is in a vital system register, such as those that regulate operations, or when an SET is caught by a user logic flip-flop, Single Event Functional Interrupts (SEFIs) can occur in digital devices. Such occurrences wreak havoc on the overall system's operation [50].

If the SEFI effect is not masked, an FPGA-based system must be reset and configurations reloaded to recover from a SEFI, which requires a minimum downtime of tens or hundreds of milliseconds [51].

2.3.3.2 Destructive Single Event Effects

2.3.3.2.1 Single Event Latchup (SEL)

Latchup is a possibly dangerous phenomenon in which a low-resistance path forms between power and ground and persists after the triggering event has passed. When a high-energy particle collides with CMOS devices, parasitic transistors are activated in a positive feedback loop forming a thyristor [52]. The device is short-circuited as a result of the thyristor being triggered. The device can be damaged by a short circuit caused by a SEL event due to the significant quantity of heat produced [53].

2.3.3.2.2 Single Event Burnout (SEB)

Single Event Burnout (SEB) happens when a very energetic ion collides with a transistor source, creating a high current conduction. These occurrences mostly affect power MOSFETs, but they can also cause IGBTs, diodes, and other circuits to fail. SEBs will occur in MOSFETS, when an energetic ion impacts the substrate exactly under the source, causing forward-biasing, and a voltage greater than the breakdown is supplied to the drain-source connection. Because of the significant thermal effects in the area, the device is destroyed [54].

2.3.3.2.3 Single Event Gate Rupture (SEGR)

Single Event Gare Rupture (SEGR) refers to the rupturing of the gate-oxide insulation caused by a high-energy ion impact. The rupturing of gate-oxide insulation in MOSFETs damages the current routes, rendering the device useless [55].

2.4 RADIATION EFFECT ON SRAM-BASED FPGAS

This section delves into the structure of current SRAM-based FPGAs, as well as the sub-components that are affected by radiation.

2.4.1 Overview of the Architecture

As depicted in Figure. 2.10, the FPGA is a two-layered device. All application-level elements, such as Block RAMs, I/O blocks, Configurable Logic Blocks (CLB), and so on, are found at the logic layer. The second layer is the configuration layer, which contains the configuration memory and access ports. The configuration bits of an FPGA are kept in configuration memory and used to build a circuit. This collection of bits is called a "bitstream." SRAM-based FPGAs are supplied among other by Altera and Xilinx, two of the most well-known companies in the industry. Both of them provide comparable architectures [56], [57],[58].

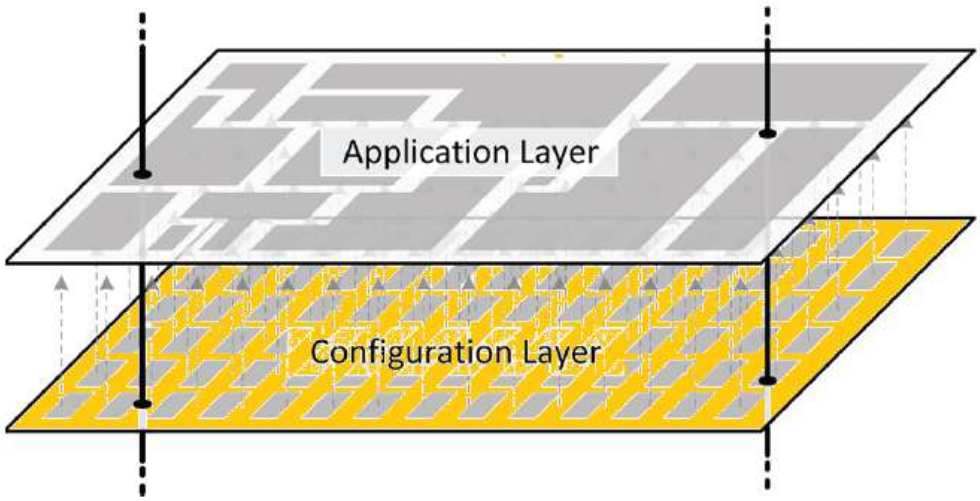


Figure 2.10. The two FPGA layers [58].

Figure 2.11 depicts a general structure of the application resources available, for a user in a typical FPGA, in the logic layer. A set of programmable links connects these resources in a matrix formation, resulting in an arrangement of programmable

blocks of logic of various types such as multipliers, memory, general logic or other specialized circuits. Programmable input/output blocks (I/O) surround the arrangement, which connect the FPGA to other systems [58],[59].

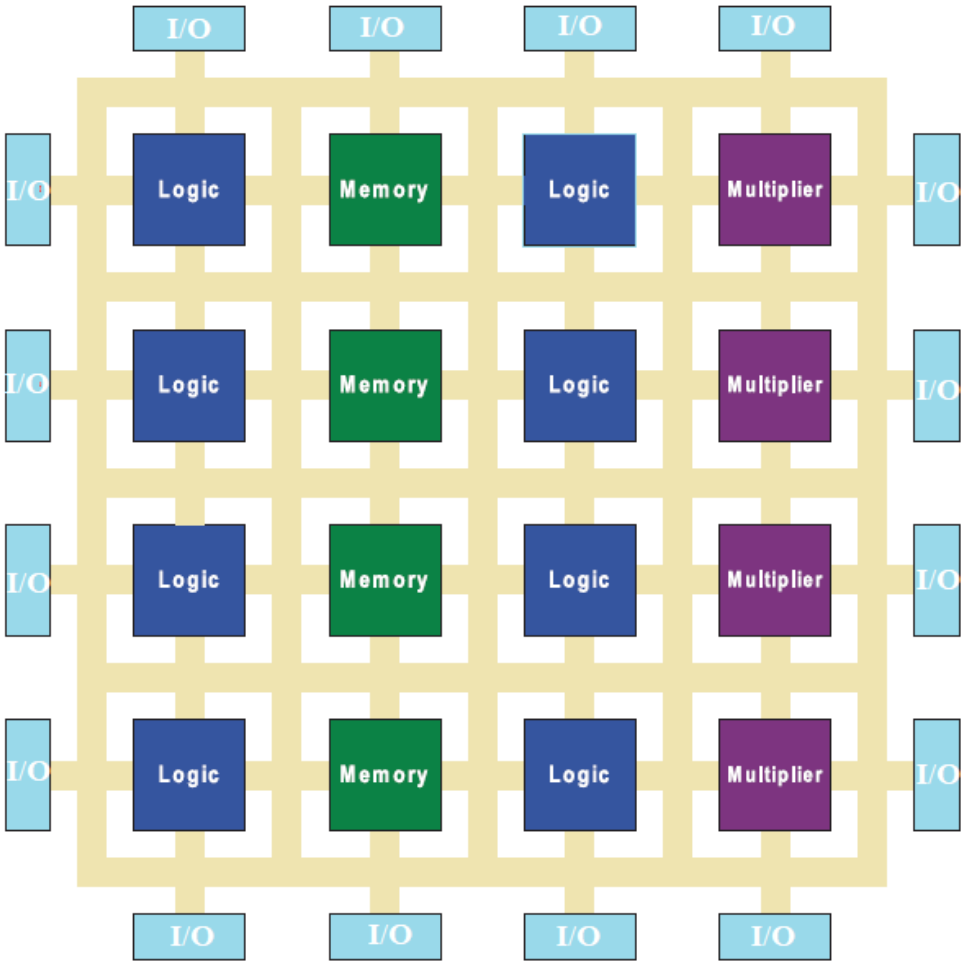


Figure 2.11. FPGA structure in its basic form [57].

The fundamental distinction between a traditional CMOS-based digital design and an SRAM-based FPGA is its ability for reconfiguration. The programmability of configurable blocks provides this customization freedom. After the manufacture of the FPGA, this arrangement allows multiple applications to be realized in the FPGA. Look-up tables (LUTs) are used in newer FPGAs to maintain a good balance between versatility and circuit performance characteristics including power and area overheads. A set of LUTs is required for implementing any logical function. It is a multiplexor consisting of n selectors and 2^n inputs. SRAM-cells in the bitstream are connected to these inputs. As a result, this architecture can be used

to create any combinational circuit containing n inputs. Flip-flops, carry propagation parts and multiplexers are frequent components of configurable blocks, in addition to LUTs [57],[60].

FPGAs have embedded memory blocks in addition to configurable logic units. These blocks are reserved to the user circuit and are based on SRAM-cells. There are also specialized arithmetic blocks known as DSP blocks. DSPs contain adders and multipliers which are used to build digital signal processing functions like digital filters [61].

The bits in the configuration layers' bitstream serve a variety of purposes. The configuration layer contains bits that govern LUT functions, as well as bits that control the configuration of resources including DSP blocks, memory, and I/O blocks, and bits that control the connectivity of configurable blocks. To program SRAM-based FPGAs, a binary bit-stream is generally stored off-chip [62]. A radiation-hardened EEPROM or Flash is one of the most used methods for off-chip storage of the configuration bits. Because SRAM-based configuration memory is volatile, reprogramming the FPGA at start-up and during power cycling is required. The programming logic is in charge of writing configuration bits to the FPGA via one of the configuration interfaces [63].

In Xilinx architectures, several configuration interfaces are available for accessing the configuration memory. The configuration memory of the device can be accessed from outside the device using Byte Peripheral Interface (BPI), JTAG, and Serial Peripheral Interface (SPI) [64].

2.4.2 Radiation Effects on SRAM-based FPGAs

TID degradation is less of a worry with today's integrated circuits due to technology scaling. Because the oxide thickness is becoming very thin, it is highly unlikely that a large amount of charge will be trapped. TID tolerance levels of 300krad or higher can be achieved using the 65nm manufacturing node, and some can even survive TID tolerance levels of up to Grad [65]. Furthermore, newer technologies that use the 22nm process node can tolerate a dose of 600krad or more [66].

Nevertheless, because an incident radiation particle can carry sufficient energy to disrupt a device state, the shorter diffusion areas in modern devices raise SEE

vulnerability [67]. As a result, previously inconsequential particles are now accountable for SEEs in FPGAs.

In the case of SRAM-based FPGAs, the concern is with non-destructive SEEs. Because destructive SEEs are relatively easy to asses as they result in complete device failure or destruction. Non-destructive SEEs will usually show their effects as a glitch on the device output corrupting its output state or interrupting its function.

Any section of the FPGA, whether it is a user logic or a configuration memory, can be affected by non-destructive SEEs, resulting in the failure of the corresponding logic unit [68]. Bit flips and other data alterations can happen. SEEs can also affect the connectivity of logic blocks. Figure 2.12 shows how these faults are visualized.

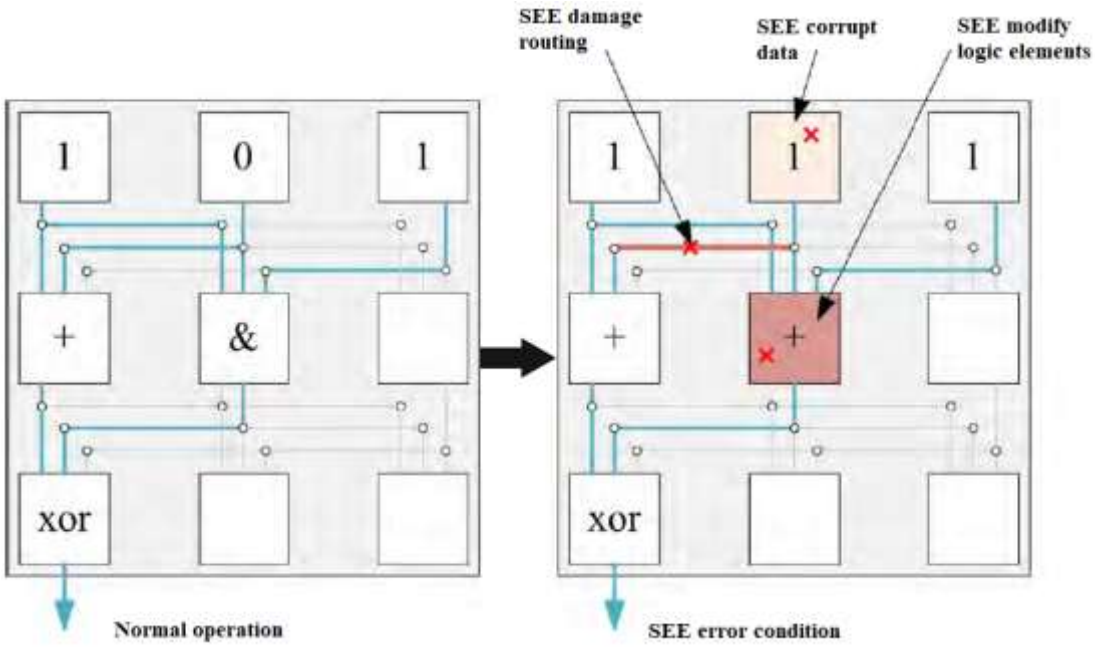


Figure 2.12. SEE effects on FPGA operation.

This research focuses on the radiation effects that occur in the user logic. The user logic, unlike the configuration memory bitstream, contains components that are not easily testable for SEEs, according to [69]. Because most of these elements' contents are subject to change as a result of normal logic activity. Unless the user logic design can detect the occurrence of the event and take appropriate action, observability is limited. As a result, the user's logic design must be mitigated against soft-errors in order to avoid operational disruptions. Logic-block flip-flops, block memory, and I/O flip-flops are all parts of the user logic.

2.5 CURRENT MITIGATION TECHNIQUES

Critical systems need reliable components to function in severe environments. In FPGA-based applications, reliability can be achieved by implementing the design as a:

1) radiation hardened, or
2) radiation tolerant

The term "radiation-hardened" refers to a device's ability to withstand the effects of radiation up to a specific dose limit. The term "radiation tolerant" refers to those devices that are made to function normally in a given radiation environment despite being susceptible to radiation. To put it another way, radiation hardening refers to modifications in the manufacturing process that minimize radiation effects, while radiation-tolerant refers to adjustments in the logic design that reduce consequences of radiation effects [70],[71]. A technique of designing a radiation-tolerant system using SRAM-based COTS-FPGA is explored in this study.

Redundancy is usually considered when designing fault-tolerant systems. The four categories of redundancy are hardware, software, information, and time-based.

Hardware redundancy refers to the presence of additional hardware or data processing components. The addition of more data to an existing system is referred to as "information redundancy" (e.g., checksum, parity bits etc.). Software redundancy refers to the presence of multiple functionalities in a program. Temporal redundancy involves the use of additional time to provide service to the system.

Hardware faults are frequently solved via hardware, information, or time redundancy, whereas software faults (bugs) are typically addressed by software redundancy.

When designing and implementing in any COTS-FPGA device, radiation tolerant design incorporates design-based fault-tolerant solutions ranging from temporal redundancy to hardware-based redundancy approaches. This is due to the fact that the vast majority of COTS-FPGA systems lack or are built with just minimal reliability support.

2.5.1 Shielding

Many approaches for reducing the effects of various types of radiation have been developed, tested, and implemented. Shielding is usually the first thing that comes to mind when it comes to radiation protection. The usage of a barrier between the radiation environment and the electronic device is required for radiation shielding.

We can use any shielding material for ground-based applications, regardless of its weight, size and material type. However, given current space technology, the cost of significant shielding in space applications is prohibitive. Furthermore, some GCRs are powerful enough to penetrate whatever shielding a space system may use [72].

Shielding can actually amplify the influence of a single incoming particle on electronics by creating a shower of secondary particles due to the interaction between a GCR and the shielding material [73].

2.5.2 Configuration Memory Scrubbing

Memory scrubbing ensures the integrity of memory contents, in order to give radiation hardness to a system, the contents of memory sections are regularly updated with known good data in this operation. This decreases the chances of erroneous data values being used in processes and prevents the accumulation of memory errors. Scrubbing can be done naively by overwriting the memory regardless of its validity on a regular basis, or by a readback technique in which memory data is compared to known good data (Golden copy) and only updated if a mismatch is discovered. Figure 2.13 depicts the memory readback arrangement [74].

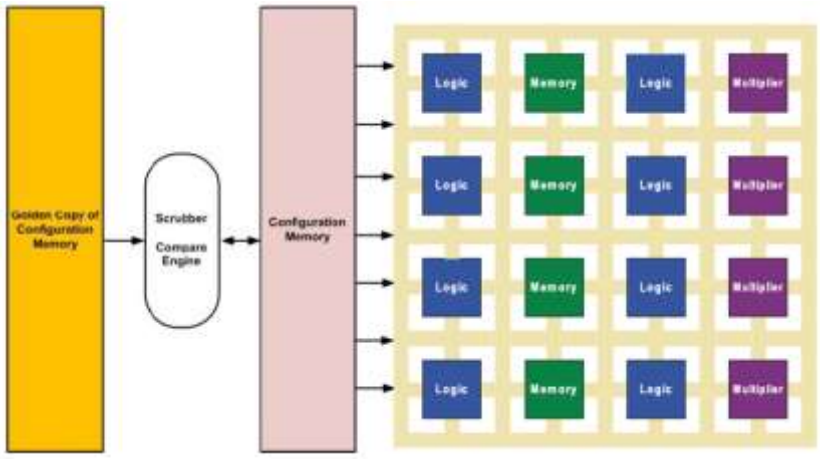


Figure 2.13. Configuration Memory scrubbing technique [74].

Memory scrubbing is used in FPGA systems to keep the configuration memory contents up to date. The existence of a scrubber significantly improves a system's overall reliability.

2.5.3 Protection of the User Logic Design

User logic protection is necessary for important applications that require a greater level of reliability, or simply where any service disruption is unacceptable, such as power conditioning units on satellites and spacecrafts [75],[76]. In order to safeguard user logic, soft-errors mitigation solutions should be able to filter out the effects of upsets in the user logic components, as well as the consequences of transient effects or other functional interruptions. In the following sections, we'll look at some of the most common mitigation strategies for user logic protection.

2.5.3.1 Hardware based Redundancy

2.5.3.1.1 Module Level Mitigation

In order to implement soft-error mitigation in a user's FPGA design, redundant instances of a complete module are replicated and the modules' final outputs are determined. A module can represent the overall design of a device or a sub-component of that design. This is a powerful soft-error mitigation technique that can be carried out fully on a single device.

Triple Module Redundancy (TMR) with voting is a well-known mechanism for mitigating soft-errors in the user logic. Figure 2.14 depicts the basic architecture. The modules are triplicated to perform the same computation in parallel. The correct outcome will be determined by a majority voter. If one of the modules fails, the majority voter will mask the faulty module's output by recognizing one of the two remaining fault-free modules' output as correct, [77],[78].

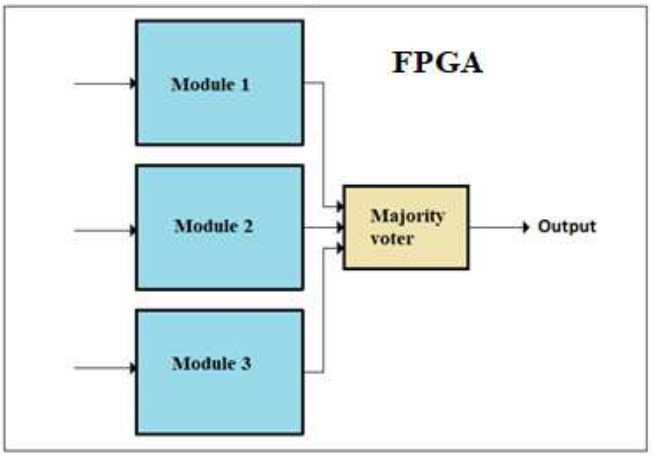


Figure 2.14. Triple modular redundancy.

One out of every three module faults can be masked by a TMR system. A double fault (faults in two distinct units at the same time) would result in a faulty output from the voter [79]. Figure 2.14 depicts a basic design with a flaw in that an error in the voter circuit could result in a voted signal that is incorrect. As a result of this problem, the voter circuitry is frequently triplicated as well, as shown in Figure 2.15.

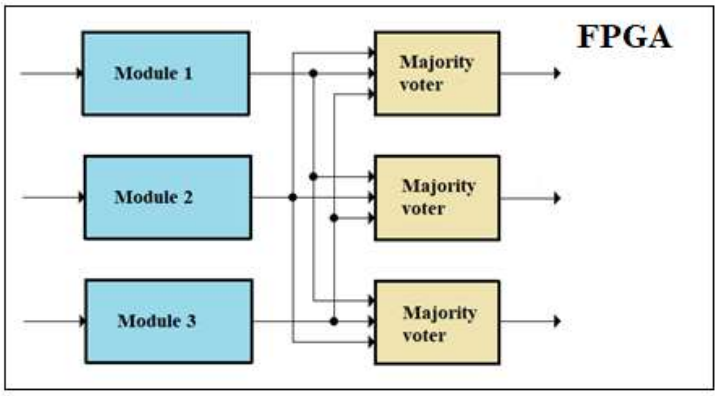


Figure 2.15. TMR with triplicated voters.

It is worth mentioning that the TMR system loses its reliability after the first module failure, even when compared to the unmitigated (simplex) system. This is because the remaining two modules act as though they are connected in series, and if one of them fails, the entire system would fail. As a result, TMR-based systems are only suited for short-duration missions, such as in airplanes, and are not suitable for long-duration missions, such as in space systems.

TMR-simplex is a strategy that is meant as a substitute for the TMR scheme. It combines the advantages of TMR and simplex systems in one system. It is a masked, reconfigurable redundancy strategy that identifies discrepancies in unit outputs and reconfigures the TMR system [80]. When an error is identified, one of the good modules as well as the failed module are discarded, effectively reducing the TMR system to a simplex system. As a result, effective radiation-sensitive areas are minimized, leading to greater reliability than TMR with a failed module.

However, this method has the drawback of discarding a working module together with a failed module. Furthermore, TMR's reliability benefits are also unavailable after the first failure, and incorrect detection (false alarm) may result in modules being removed, considerably lowering the reliability further. Because of these disadvantages, TMR-simplex is rarely used in fault-tolerant systems.

2.5.3.1.2 Multiple Device Level Mitigation

Applying configuration management and reproducing the design on several FPGAs with a voting mechanism on the FPGA outputs is another effective mitigating technique for a user logic [81],[82]. There are a variety of implementations available, extending from two to three or more FPGAs.

Figure 2.16 depicts a two FPGA implementation with two copies of the same design on each FPGA. A voter on a radiation-hardened device can then vote on the results. If one output deviates from the remaining three, the voter should ignore all the outputs from the faulty FPGA until it synchronizes with the remaining FPGA. If the remaining FPGA's outputs are mismatched, all outputs should be ignored and both FPGAs should be reset [81],[82].

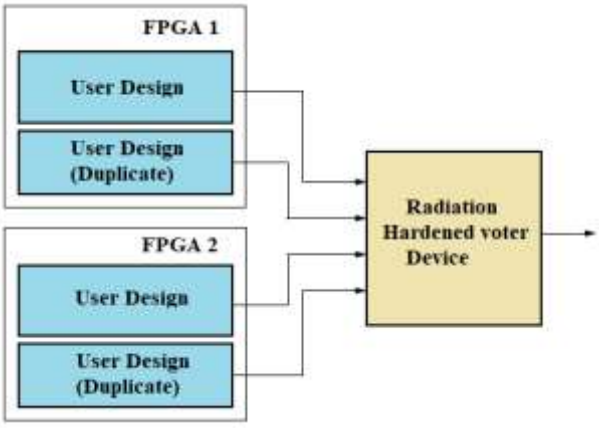


Figure 2.16. Two FPGA scheme [81].

Figure 2.17 shows a solution with three or more FPGAs, each FPGA has the same implemented design and the outputs are voted on a hardened device. For more than three FPGA implementations, voting can be executed on three of the FPGAs while the other FPGAs are kept in reserve. If one of the three primary FPGAs fails, the reserve FPGA takes over until the failing FPGA is restored and in sync with the other FPGAs. As long as there are two matching FPGA outputs, this approach can work [81].

Nevertheless, it can be difficult to design applications with redundant-device mitigation. If one of the FPGAs becomes temporarily unresponsive, putting it back into sync with the other FPGAs may necessitate some complex design considerations. Furthermore, as compared to single device solutions, multiple device level mitigation techniques are the most expensive, often with just a slight advantage over the other options.

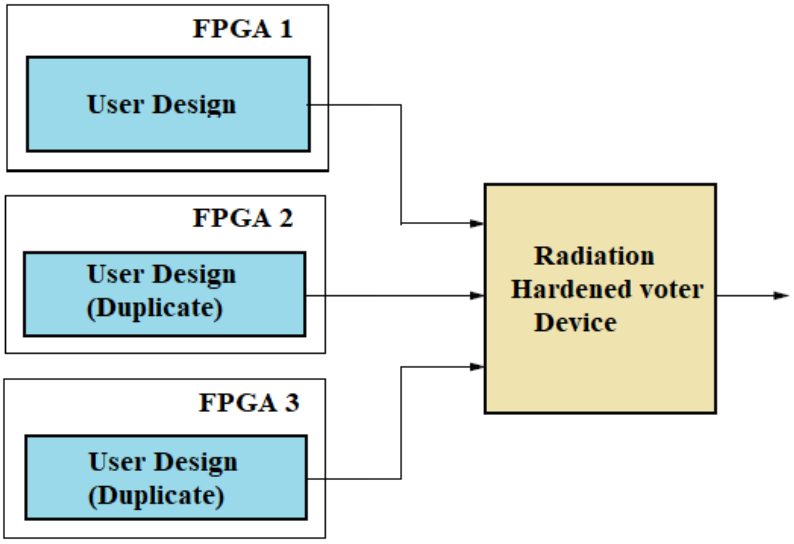


Figure 2.17. Three FPGA scheme [81].

2.5.3.2 Temporal Redundancy

Temporal redundancy techniques, which exploit the transient pulse characteristic to inspect the same signal at different times, are commonly used to identify SETs occurrences in a user logic. Hardware-based redundancy systems need a substantial amount of extra hardware. In situations where time is less important than hardware, temporal redundancy is a strategy to reduce the amount of extra hardware

at the expense of additional time. Because of their nature, transient errors can be identified by repeating computations at different times and comparing the obtained results [83],[84]. Depending on the actual implementation and how a system manages transient errors, temporal redundancy schemes can be characterized as:

1) Simple temporal redundancy or
2) Full temporal redundancy

Simple temporal redundancy focuses on comparing output signals at two separate times and takes advantage of the transient nature of the erroneous pulse (SET) created by the particle impact.

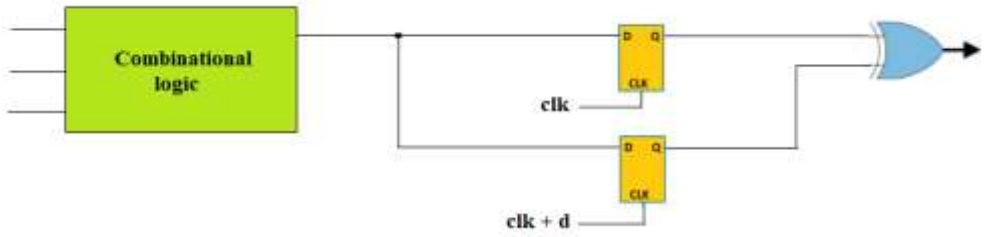


Figure 2.18. Simple temporal redundancy.

The signal from the combinational logic is latched twice, with the second latch's clock edge offset by time d, which is considered to be longer than the SET period. A comparator would identify the presence of a transient pulse since the two inputs do not arrive at the same time. Figure 2.18 shows a single bit comparator, which is nothing more than a two-input XOR gate. With this approach, SETs can only be detected, not masked or corrected, and fault restoration can be performed by re-executing the previous operation [84], [85].

Figure 2.19 shows a full temporal redundancy scheme. Full temporal redundancy ensures the right output value in the presence SET. The method is similar to the TMR scheme in that it uses three different values captured at three different times. The combinational logic output is latched three times in this configuration, with the second latch's clock edge delayed by time delay d and the third latch's clock edge delayed by time delay 2d. The majority voter decides on the final proper output [85].

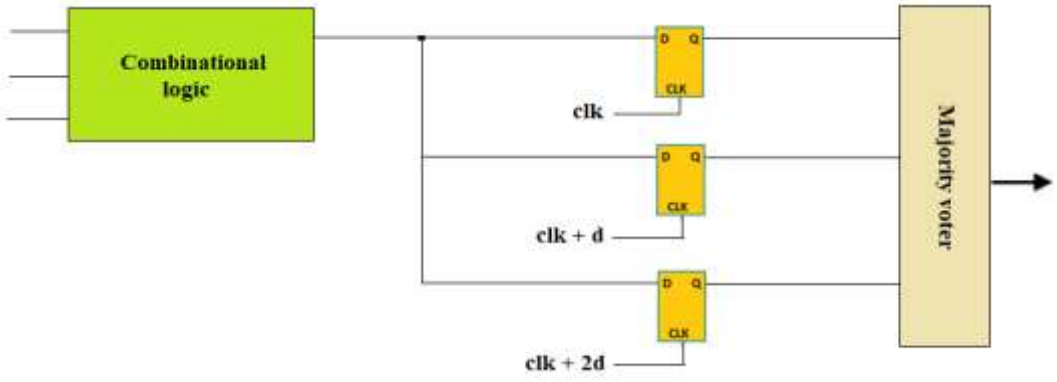


Figure 2.19. Full temporal redundancy.

Chapter 3: Radiation Testing and Reliability Measurement

Before considering any proposed radiation mitigation technique, unmitigated systems are usually subjected to radiation testing to establish the level of reliability and failure modes. The radiation testing of the unmitigated design establishes a benchmark against which any form of mitigation strategy can be measured. To determine the reliability of circuits utilized in high-radiation conditions, a variety of testing approaches are used. These approaches can be used to determine circuits' radiation sensitivity as well as, in the case of mitigated system, verify that a circuit has a good chance of surviving the unfavourable conditions in the intended radiation environment.

Physical accelerated radiation testing, simulated radiation fault injection, and emulated radiation fault injections are the most prevalent methods utilized in the verification of radiation mitigated systems [86],[87]. In this study, the latter techniques are utilized to assess the effectiveness of the proposed mitigation strategies. This chapter provides an overview of these testing methods and the concept of reliability measurement metrics.

3.1 PHYSICAL ACCELERATED RADIATION TESTING

One method for determining a circuit's response to a radiation environment is to subject it to physical accelerated radiation testing, or exposing it to an actual radiation source. Particle accelerators, for example, produce massive fluxes of various particles utilized in accelerated experiments, such as heavy ions, protons, and alpha radiation. These radiation sources won't be able to create particles with the same energy as those found in space. However, because the LET for heavy ions and the energy for protons are crucial properties in defining the interaction between a particle and matter, particle accelerators can be made to create particles with the needed LETs and energies [87],[88].

Accelerated radiation testing has two major benefits: it simulates real-world effects in the intended environment and it is accelerated. The first is the most important. Exposing a circuit to the similar environment in which it will be utilized

reveals potential radiation consequences and helps in determining how well the circuit can withstand them. However, in order to properly forecast how the circuit would perform once deployed, it must be tested for a long enough period of time or with a high enough frequency to collect meaningful data. Furthermore, because the entire device is irradiated, SEE characterization utilizing particle beams is a comprehensive method. Such a test generates a series of events for a specific fluence of particles, but without any detail about the observed faults' locations. As alternatives, focused or narrow laser or X-ray of heavy ions beams can be employed to determine the sensitivity of complex electronic components exposed to radiation and distinguish between different impacts. These tests make it simple to identify the circuit parts into which faults are injected [89],[90].

The accelerated radiation testing facilities are costly, demanding and somewhat inaccessible, which is the major downside of accelerated radiation testing. Despite this, accelerated radiation testing remains the greatest method for validating electronics in a radiation environment.

3.2 SIMULATED FAULT INJECTION METHOD

Fault injection is a system reliability assessment technique in which one or more faults are injected into a system in a predictable rate and their effects analysed. By introducing artificial faults into the device, it aims to mimic the behaviour of radiation-induced faults on the design under test (DUT) [91]. It can be conducted in a variety of ways.

A Hardware Description Language like VHDL or Verilog can be utilized in conjunction with fault injection via software in the case of simulation-based fault injection. This allows the developer to initiate injecting faults at the beginning of the design and see if the expected performance is achieved.

For FPGA designs, these tests are valid. Software techniques can insert soft-errors, that are supposed to be induced by radiation conditions, into the design. Thus, the behaviour of a design subjected to radiation-induced soft-errors can be thoroughly examined without the use of physical accelerated radiation experiments.

This can be performed with the help of saboteurs and mutants [92]. The goal of using the first is to connect saboteurs in series or in parallel with the required signal that can change the signal value as needed.

Mutants are designed to replace a functioning component with an equivalent component that has new qualities, and are thus referred to as an original component in its mutated form. An OR-gate, for example, can be configured to always output a HIGH when the mutation is triggered using extra signals controlled by the test system [92],[93].

The alternative option is to utilize the simulator's built-in capabilities to change signal values. This doesn't really necessitate any source code changes, however the performance provided is dependent upon whatever simulator is utilized. The primary benefit of this approach is that the injection of the faults can be conducted on a model at the design phase, which helps to uncover vulnerable points in the system.

Because the simulation must be stopped and started for each fault injected, the simulation time overhead imposed by simulation-based fault injection is mostly related to fault injection management. To circumvent this, a series of fault injection experiments are commonly used; these are based on the concept of designing only one design that includes all required faults and then activating them one by one; however, this may increase simulation time. As a result, the simulation and compilation times are the overhead trade-offs.

The major goal of employing fault injection in this dissertation is to verify the mitigation capabilities of the proposed strategies. As a result, a fault injection campaign in this study entails exhaustive and progressive module-by-module fault injection at the required locations in order to identify those that cause functional failures or to ensure that the proposed mitigation method will filter the faults without causing any functional interruptions.

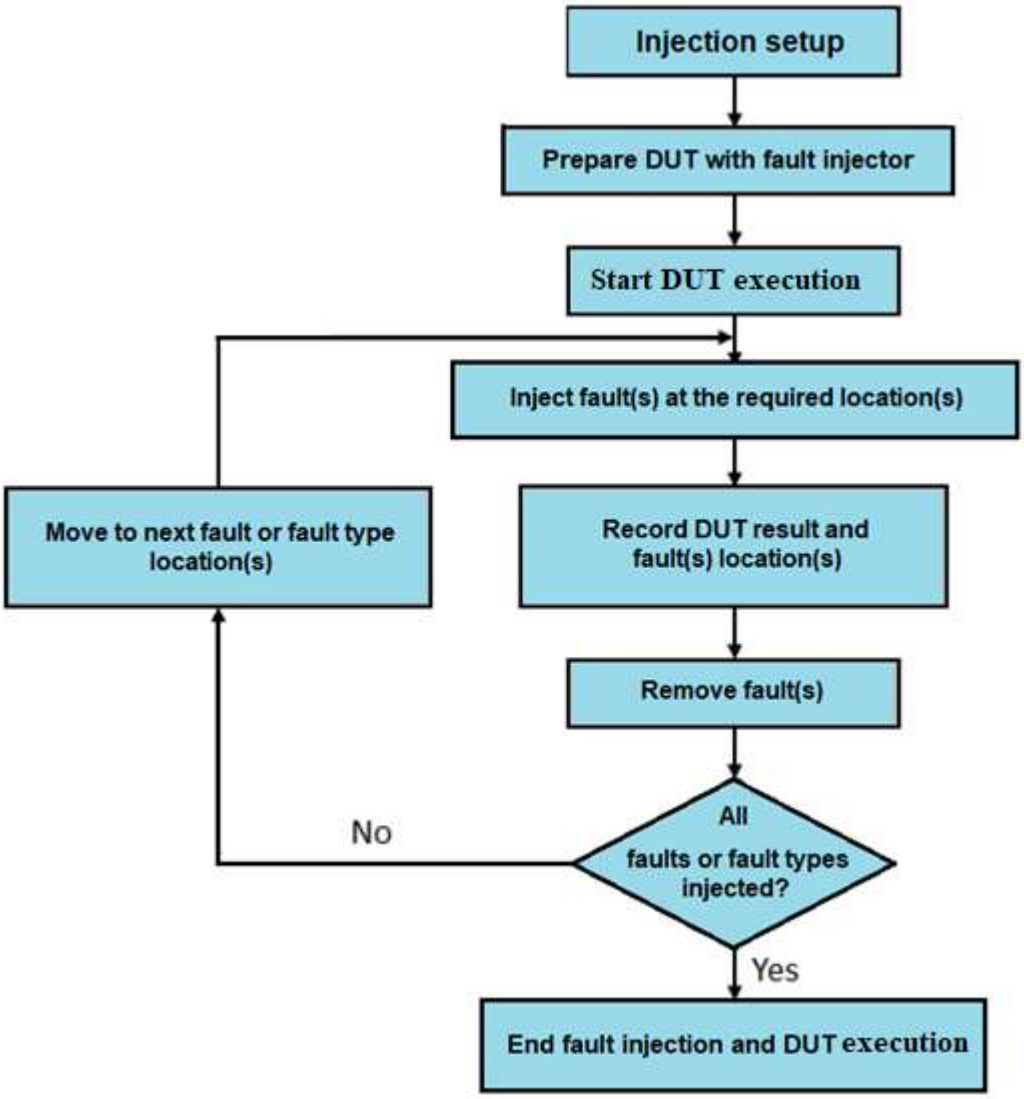


Figure 3.1. Simulation-based fault injection procedure.

3.3 EMULATED FAULT INJECTION METHOD

Emulation-based fault injection employing hardware prototyping on FPGA-based logic emulation systems has been proposed to deal with the time constraints imposed by simulation-based fault injection while also taking into account the effects of the circuit environment in the application [94]. Starting with the high-level circuit description, the circuit is built onto the FPGA utilizing a traditional synthesis, placement, and routing design method. The development board is connected to a host computer, which is used to specify the fault injection campaign, control the injection trials, and view the results. In order to do this, changes to the circuit description must

typically be made, keeping in mind that the description must still be synthesizable and fulfil a set of hardware requirements. It may be difficult to make changes to the circuit descriptions, and it is frequently necessary to create numerous updated descriptions, each of which enabling the injection of a specific set of faults.

In a number of applications, FPGAs are already being employed to speed up fault injection [95]. Generally, the aim is to use the high running speed of a hardware prototype to minimize the fault injection testing time in comparison to a simulation-based approach.

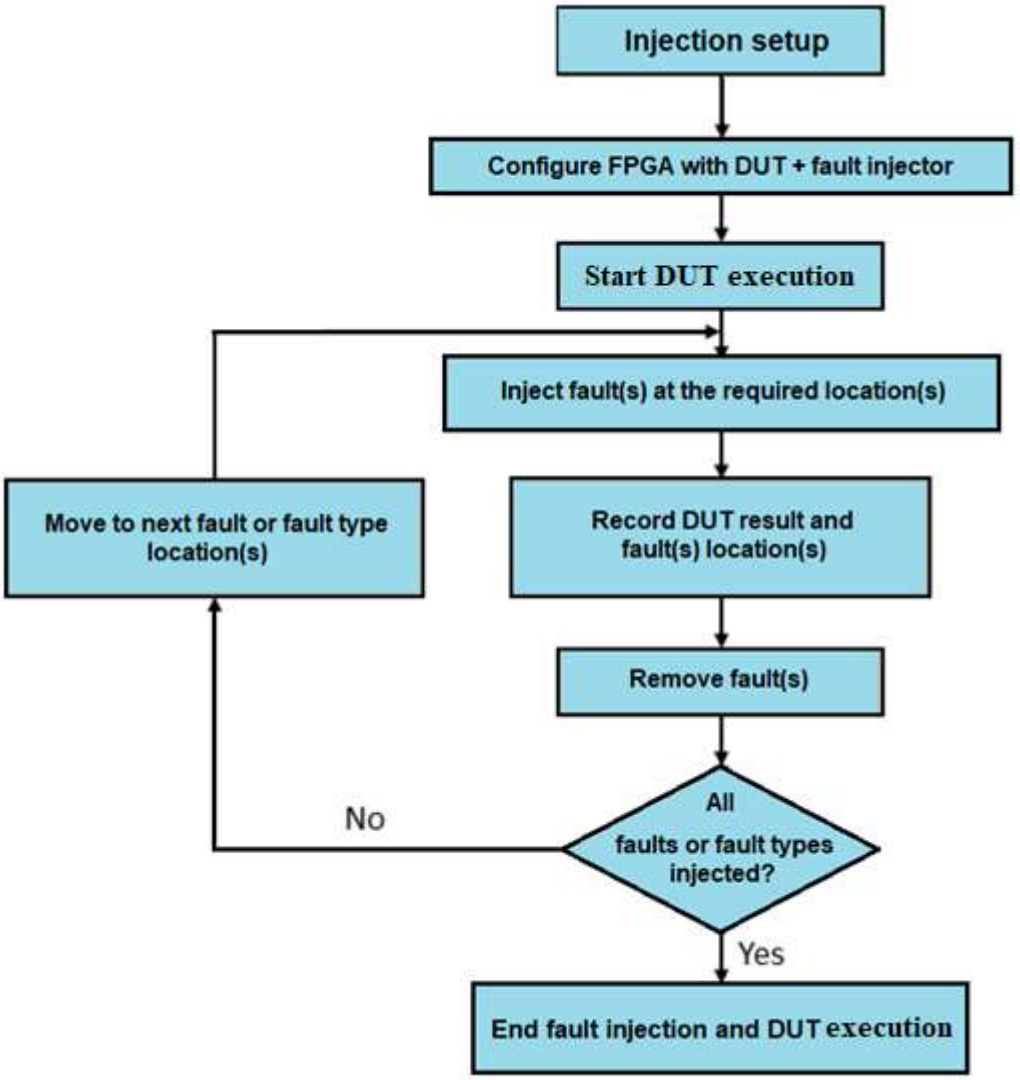


Figure 3.2. Emulation-based fault injection procedure.

3.4 RELIABILITY MEASUREMENT

The reliability of a fault-tolerant system is an important quality metric. It is defined as the probability of not failing in a certain environment over the duration of the mission [96]. Assume that a system contains N identical components. Let S(t) represent the number of components that have survived until time t, and Q(t) represent the number of components that have failed until time t. Then the reliability R(t), which is defined as the chance of the components surviving, is given by:

$$R(t) = \frac{S(t)}{N} \tag{3.1}$$

A measure of failure, often known as the unreliability or failure time distribution, is defined as F(t):

$$F(t) = \frac{Q(t)}{N} \tag{3.2}$$

Since S(t) + Q(t) = N, then,

$$R(t) + F(t) = 1, \quad or \quad F(t) = 1 - R(t) \tag{3.3}$$

Because F(t) represents a probability, its derivative is a probability distribution function, which is given by:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{3.4}$$

where f(t) is the failure probability per unit time.

The failure-rate λ is now given as the number of failures per unit time divided by the number of components that survive.

$$Failure\ rate = \frac{number\ of\ failure\ per\ unit\ time}{number\ of\ survivors\ at\ the\ given\ time} \tag{3.5}$$

$$\lambda = \frac{1}{R(t)} \cdot \frac{dF(t)}{dt} = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{3.7}$$

By considering R(t) = 1 at time t = 0, and the reliability at time t equals R(t), the expression can be integrated from 0 to time t as follows:

$$\int_0^t \lambda\, dt = -\int_1^{R(t)} \frac{dR(t)}{R(t)} \tag{3.8}$$

During the useful life of the system, λ is frequently assumed to be constant. Thus,

$$\lambda\, t = -\ln R(t), \quad or \quad -\lambda\, t = \ln R(t) \tag{3.9}$$

This gives,

$$R(t) = e^{-\lambda t} \tag{3.10}$$

The system's mean time to failure (MTTF) is another tool for measuring system's dependability and is calculated as follows:

$$MTTF = \int_0^\infty R(t)\, dt = \frac{1}{\lambda} \tag{3.11}$$

When calculating the reliability of independent systems, the binomial formula is frequently utilized. Using the binomial theorem, assume independent and identical modules with R_m reliability and a constant failure rate of $\lambda = 1 - R_m$. The reliability of an k-out-of-n system is the probability that at least k of the n components will work. The following is the cumulative binomial probability:

$$\sum_{x=k}^{n} \frac{n!}{x!\,(n-x)!} R_m^x (\lambda)^{n-x} \tag{3.12}$$

3.4.1 Reliability Improvement Factor (RIF)

The Reliability Improvement Factor (RIF), also known as the Reliability Improvement Index (RII), has been shown to be effective in evaluating resilient systems as a radiation hardness indicator [80], [97]. It is defined as the ratio of the failure probability of the non-redundant system to the failure probability of the redundant system. For a particular mission length and radiation level, if R_N and R_R are the non-redundant and redundant systems' reliabilities, respectively, then,

$$RIF = \frac{1 - R_N}{1 - R_R} \tag{3.13}$$

These reliability measures give the necessary criteria for comparing the designs and implemented SEE mitigation strategies explored in this dissertation work. Each of the previously listed metrics has benefits and limitations. The basis for validating and proving SEE mitigation approaches to boost FPGA design reliability will be laid by collecting and evaluating fault injection using these reliability measures.

3.4.2 Reliability of TMR Method

TMR is more reliable than Simplex (unmitigated system) only until one of the three modules fails, as mentioned in Chapter 2. As a result, it is usually used in applications with short mission times relative to component life. If R_m is the reliability

of one of the modules (simplex system), the reliability equation of the TMR system if an ideal voter is assumed is given by, [80].

$$R_{TMR} = 3R_m^2 - 2R_m^3 \qquad (3.14)$$

Despite the fact that the TMR-simplex isn't generally used because of its multiple shortcomings (described in Chapter 2), we'll use it as a reference here. If an ideal voter is assumed, [80] gives the TMR-Simplex system's reliability.

$$R_{TMR/Simplex} = 1.5R_m - 0.5R_m^3 \qquad (3.15)$$

The reliability of simplex, TMR, and TMR-simplex systems is compared to the normalized mission time (time/MTTFsimplex) in Figure 3.3. TMR is better than simplex until 0.7 MTTFsimplex, as seen in Figure 3.3, but TMR-simplex is always better than either TMR or simplex alone.

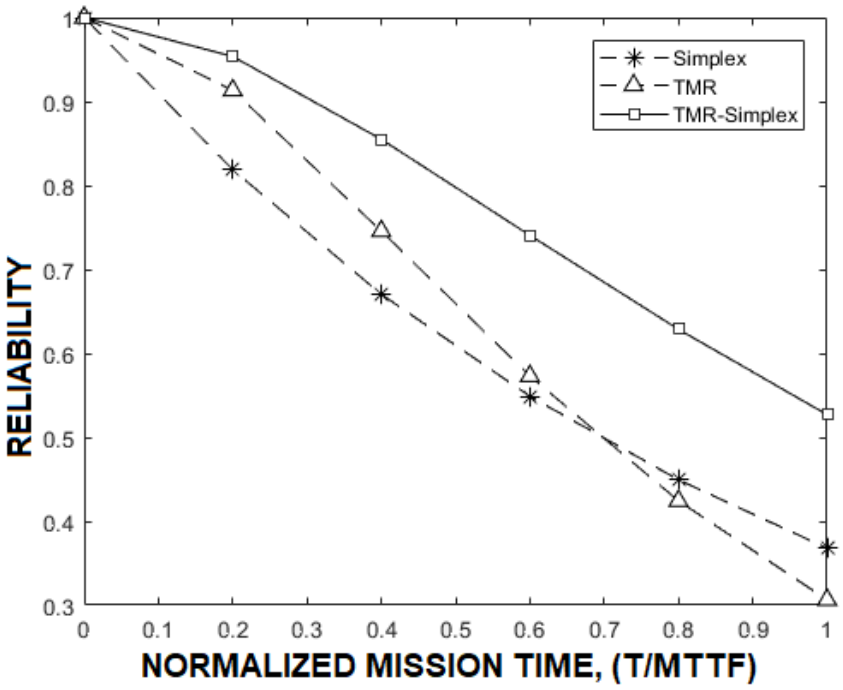


Figure 3.3. Reliability vs. normalized mission time for simplex, TMR, and TMR-simplex systems.

Chapter 4: Single Event Effects in PWM Controllers

PWM (pulse-width modulation) controllers are the primary controller types for power converters used in space because they provide low output ripple and good efficiency during medium to high load conditions. Furthermore, they operate at a constant frequency which makes developing circuitry to prevent electromagnetic interference (EMI) a straightforward task. This chapter gives background on structure and previous radiation testing of PWM controllers.

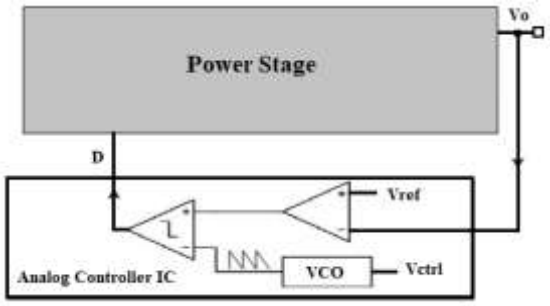
4.1 PWM CONTROLLER ARCHITECTURE

PWM is a method of regulating the average power of an electrical signal by dividing it into discrete segments. The average value of voltage and current given to the load can be controlled by rapidly switching the switch between supply and load on and off. The overall average power given to the load is determined by how long the switch is on relative to its off-state [98]. This section describes the analog and digital system architectures of PWM controllers for switching voltage converters.

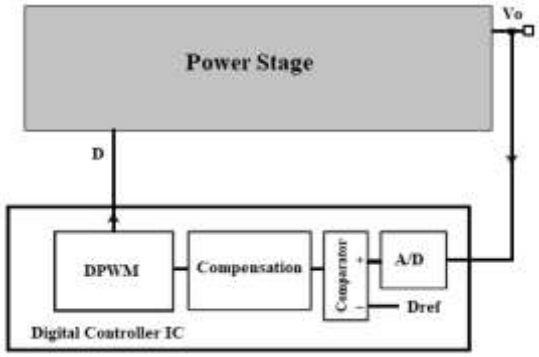
4.1.1 Analog and Digital PWM Controllers Structures

A voltage-controlled oscillator (VCO), an error amplifier, and a comparator are commonly found in an analog PWM controller IC. It could also contain a soft-start circuit, among other things. An analog-to-digital converter (ADC), a compensator, and a digital pulse-width-modulator (DPWM) make up the digital PWM controller IC. Because they are all made of transistors and diodes, all of these subcomponents are susceptible to single event impacts. The impacts usually appear as a glitch on the controllers' outputs.

In an analog PWM controller IC, the output voltage (V_o) is compared to the reference voltage (V_{ref}), and in a digital controller IC, the reference signal is a digital reference voltage (D_{ref}). To regulate the output voltage (V_o), the duty ratio D governs the on-time and off-time lengths of the power stage transistors [98]. Figures 4.1_a and 4.1_b depict the basic analog PWM controller and basic digital PWM controller structures, respectively.



a) An analog PWM controller IC structure



b) A digital PWM controller IC structure.

Figure 4.1. PWM architecture.

By adjusting the voltage level with an appropriate duty cycle, the controller drives the power stage to deliver an output voltage that approximates a given reference voltage in both analog and digital scenarios.

4.2 PREVIOUS SEE TESTING OF PWM CONTROLLERS

4.2.1 Heavy Ion Testing

A nucleus of an element heavier than the proton is known as a heavy ion. The LETs of heavy ions are related to their ion types and energies. Heavy ion radiation exists all throughout space, despite the fact that there is no significant heavy ion radiation on the ground. As a result, heavy ion tests are useful for determining the susceptibility of an electronic circuit to SEEs.

Over the last two decades, several radiation tests on PWM controllers have been conducted. PWM controllers were tested for their response to SEEs in some of the studies [99],[100],[101],[102],[103]. The heavy ion test reported in [99] resulted in

missing or very long pulses at the PWM controller's output, causing voltage transients at the DC-DC converter's output. The researchers have conducted their studies using both a physical heavy-ion experiment and simulation analysis utilizing a pulse-generator to inject pulses of various durations that matched the voltage swings and durations seen in the real heavy-ion experiments [99].

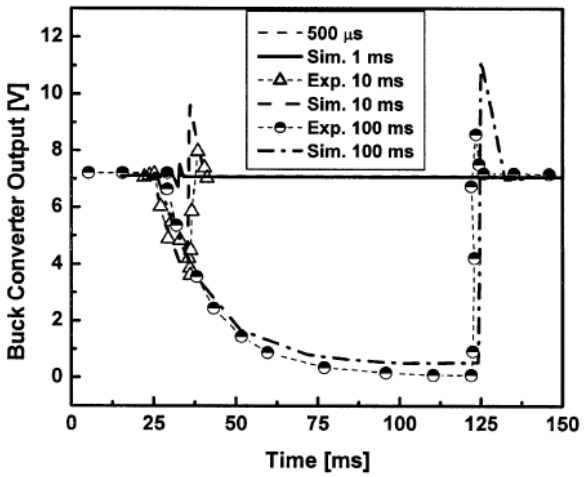


Figure 4.2. Experimental and simulated buck converter output waveforms for various lengths of missing PWM pulses [99].

As illustrated in Figure 4.2, notable transient effects began to develop at the buck converter's output for pulses suppressed for longer than 1 ms, with a significant reduction in output voltage evident for 10 ms or longer pulses.

A heavy-ion test on Texas's PWM5032 controller IC revealed soft-error signs, such as missing pulses and extra-long pulses, at the device output, according to a publication in [102]. When the controller IC was bombarded with ions of different LETs. The output of the DC-DC converter used in the experiment plummeted to zero, as observed on the power-good pin as shown in Figure 4.3.

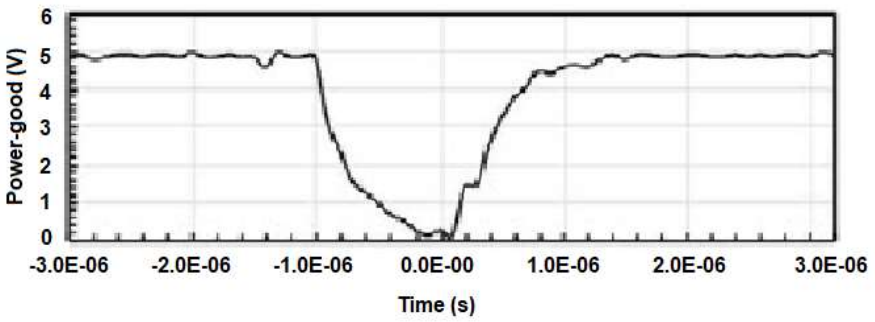


Figure 4.3. Transient on power-good line [102].

4.2.2 Pulsed Laser and Pulsed X-ray Testing

Passing light via a resonator, gain medium, and an optical cavity, pumped by an electric field produces light amplification by stimulated emission of radiation (LASER). The gain medium amplifies light as it goes through the resonator, and there are a pair of mirrors at the end of an optical cavity that reflect light back and forth, causing it to be amplified repeatedly. Only the wavelength of light that matches the cavity's distance is amplified. Because of its well-controlled irradiation location and timing, pulsed laser techniques have lately become popular for SEEs measurements [100]. The beam size, location and the irradiation interval between each pulse are highly controllable parameters of the pulsed laser tests. There are a lot of devices tested for SEEs response using the pulsed laser testing technique [99], [100].

X-rays are a type of radiation that is produced by an atomic transition between higher and lower discrete energy levels. They have been used for a long time as a source of radiation. Pulsed X-rays have lately been described as having the ability to test SEEs in microelectronic circuits [99]. Pulsed X-ray testing is more intriguing than pulsed laser testing because of its shorter wavelength and ability to penetrate metal casings.

The findings of the pulsed X-ray test published in [100] were obtained using a COTS PWM controller to perform SET measurements. Initially, the experiment was carried out using a lower energy monochromatic X-ray pulse, with no discernible SET at the output. Transients are noticed at the PWM controller's output when a higher energy pink (polychromatic) X-ray is employed, resulting in a drop in voltage on the power-good pin, as illustrated in Figure 4.4. The pulsed X-ray result is shown in comparison to the pulsed laser test result they previously acquired.

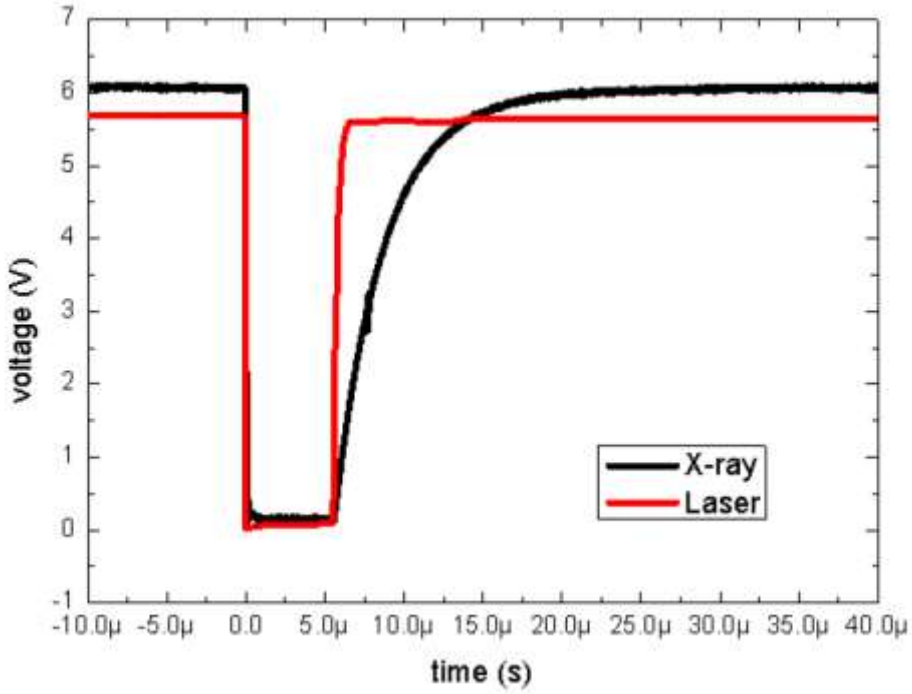


Figure 4.4. X-ray and laser induced SET at the output [100].

Both X-ray and laser test runs, as shown in Figure 4.4, exhibited a drop in converter output voltage for the duration of the SET presence.

4.3 SUMMARY

In summary, soft-errors in PWM controllers cause a glitch in the controller's output, which is commonly seen as:

1) Pulse duration(s) of the PWM controller output change (increase above or decrease below the correct pulse-width).
2) Complete pulse loss due to a PWM controller failure or inability to recover from a previous malfunction (mostly assumed to be due to the output changing to logic-low permanently or until power recycling).
3) Missing pulses that occur when the PWM controller's output remains at logic-high or logic-low for one or more PWM cycles.

As a result, there is a huge transient voltage anomaly at the converter output, which might disrupt the operation of powered systems.

Chapter 5: Our Approach

This chapter describes the design strategies proposed in this study for radiation mitigation of a DC-DC converter's PWM controller, which is implemented in a COTS SRAM-based FPGA. Current mitigation approaches for space applications, as described in Chapter 2, have a wide range of cost, performance, and reliability characteristics. The suggested design strategies will combine the benefits of current state-of-the-art mitigation strategies while trying to reduce the disadvantages and limitations. The major goal is to develop a system that is both cost-effective and capable of withstanding dangerous radiation in space while maintaining a good reliability level.

5.1 THE FIRST APPROACH

The first proposed method is based on the triplex–duplex redundancy architecture [104]. In a triplex-duplex setup, there are three main pairs, each with two duplicate modules. As a result, six identical modules are organized in three pairs and run in parallel. A comparator is used to compare the computational results of each pair. The output of the comparator is included in the vote if the results are in agreement. If this isn't the case, the switch deems the pair of modules to be defective and removes them from the system. Triplex-duplex architecture is similar to the TMR method, with each pair matched to each module in the TMR case, and thus suffers from the same operational limitations. When compared to an unmitigated system, the hardware resource usage is 500% more, while the technique consumes twice as much resources as the TMR approach. Also, if the two duplicate modules in each pair are put in each FPGA, the triplex-duplex architecture is comparable to the three FPGAs architecture described in chapter 2, and hence a very resource-intensive approach.

5.1.1 Modified Triplex-Duplex Architecture

The triplex–duplex architecture has the disadvantage of requiring two times the amount of hardware as the TMR approach and having one more module than the Five Modular Redundancy (FMR) method. As soon as one of the two modules in the duplex fails, both units are withdrawn from the voting. If no repair is used, the overall system

mean time to failure (MTTF) is reduced. As a result, with the exception of defective duplex detection, it operates similarly to TMR.

In the effort of modifying this architecture and making it suitable for a radiation tolerant DC-DC converter controller design with improved reliability, the comparator and switch parts of the triplex-duplex structure were combined and modified in such a way that all duplexes are connected to all disagreement detectors and switch blocks, allowing any module in the three duplex systems to act as an active spare for any other module in the three duplex systems as shown in Figure 5.1. As a result, even if one module in each of the three duplexes fails, the overall system will continue to function, whether there is just one duplex left, or two duplexes with one good module each. This considerably improves the entire system's MTTF and, if any repair or reconfiguration is required, helps to reduce the frequency of such repair or reconfiguration when compared to TMR or FMR alone. This is done by running the output of each module through a static-detect block, which, using the comparison between each module's output and its max-duty delayed counterpart as shown in figure 5.1, looks for incidents of extra-long high (stuck-at high) or extra-long low (stuck-at low or missing) faults and replaces them with low-duration (outside converter operation range) pulses. The replacement low-duration pulses are voted out with the use of max-duty PWM pulse as the agreement between fault-free PWM pulse(s) and max-duty PWM pulse overrides the low-duration pulses as shown in figure 5.1. The detail of static-detect block is explained in section 5.1.3.

This method, on the other hand, is resource intensive, requiring 500% more hardware than a simplex system and twice as much as the TMR method. However, it provides a huge boost in reliability. The algorithm for the modified triplex-duplex method is provided in the Appendix B.

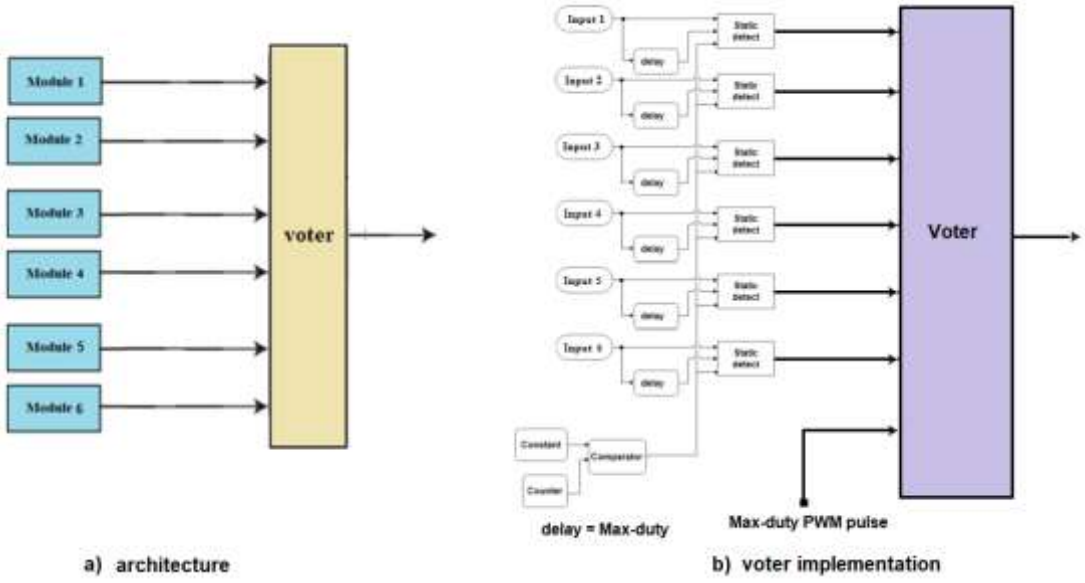


Figure 5.1. Modified triplex–duplex redundancy.

If R_m is the reliability of one of the modules (simplex system), the reliability equation of the modified triplex–duplex approach using equation (3.12) and assuming an ideal voter is given by:

$$R_{(triplex\_duplex)mod} = \quad 5R_m^6 - 24R_m^5 + 45R_m^4 - 40R_m^3 + 15R_m^2 \qquad (5.1)$$

The reliabilities of simplex, TMR, TMR-simplex, and the modified triplex-duplex systems are compared to the normalized mission time (time/MTTFsimplex) in Figure 5.2. In terms of reliability, the modified triplex-duplex strategy outperforms both TMR and TMR-Simplex systems, as demonstrated in Figure 5.2.

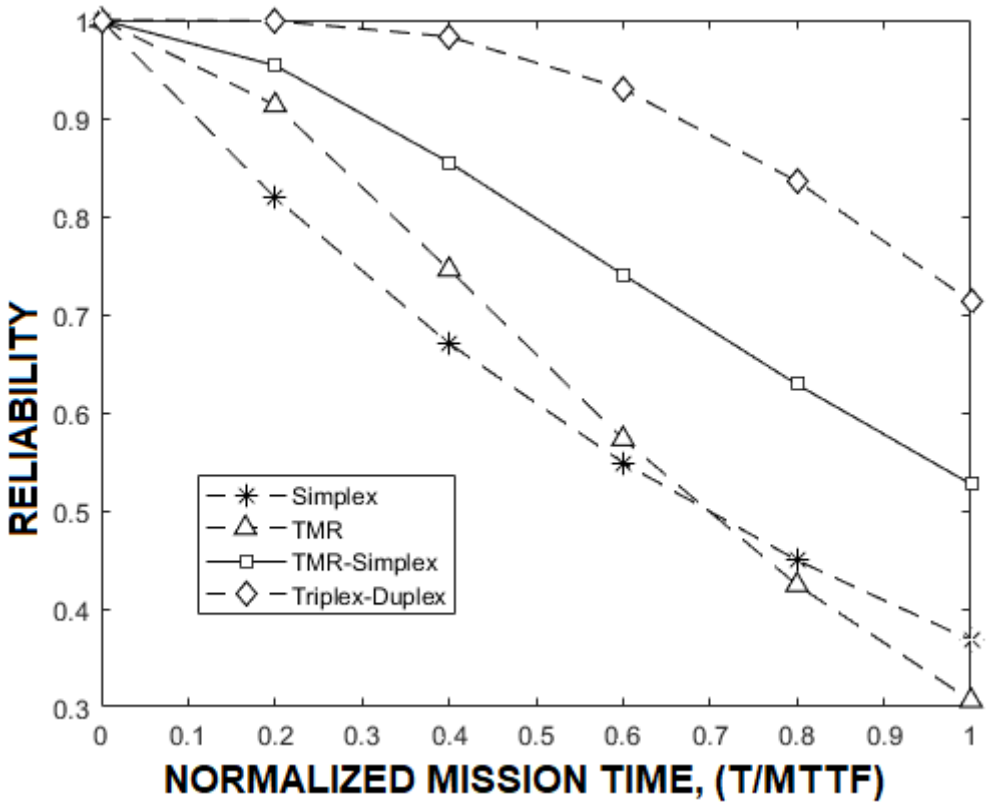


Figure 5.2. Reliability vs. normalized mission time for simplex, TMR, TMR-simplex and modified triplex-duplex systems.

5.1.2 Four Modules Architecture

In order to achieve high reliability while reducing resource requirements, a four-module architecture was devised, which has higher reliability than the TMR method and lower hardware resource requirements than the Five modular Redundancy (FMR) [105], and the modified triplex–duplex methods. The method has two variants. The first variant is comparable to the modified triplex-duplex technique described before, but instead of duplicating the design into six modules, it does it in four, which greatly reduces the amount of hardware resources needed, shown in figure 5.3.

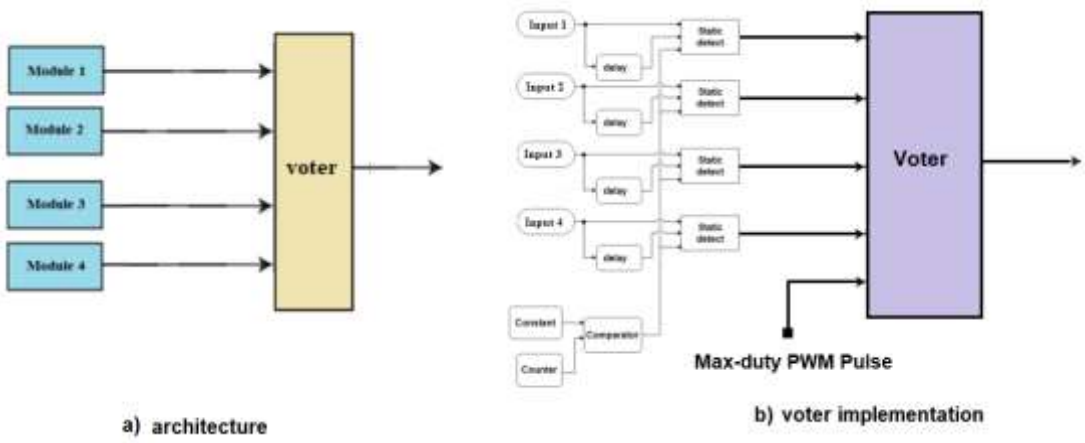


Figure 5.3. Proposed four modules redundancy (first variant).

The second variant is shown in figure 5.4 below.

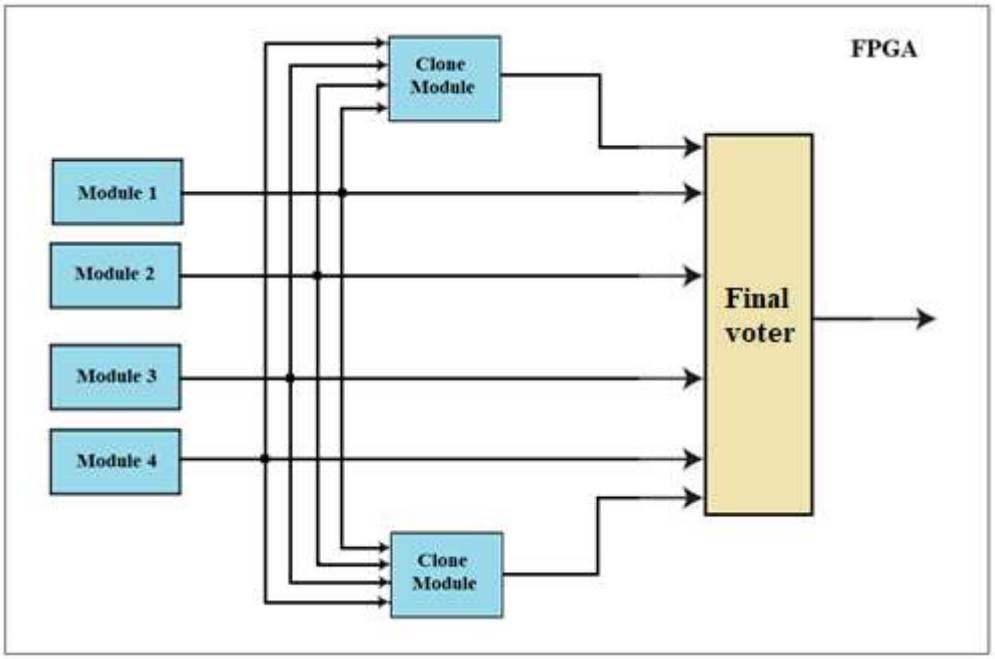


Figure 5.4. Proposed four modules redundancy (second variant).

Each module in Figure 5.4 represents an implementation of a digital controller. The architecture is similar to the modified triplex–duplex architecture described above, with the exception that there are four physical modules and two clone modules, resulting in a total of four duplicated modules rather than six. The clone modules are formed as long as at least two of the physical modules remained fault free, resulting in a considerable reduction in hardware resource use. Additionally, because the clone

module circuit is significantly simpler than the entire digital controller implementation, both clone modules can be integrated into the final voter. When applied to a radiation tolerant DC-DC converter controller design, the scheme shown in Figure 5.4 can mask stuck-at 0 and stuck-at 1 faults of any duration in any two of the modules, as well as any functional interruptions that may occur due to bit-flips in the user logic design of any two modules and/or transient glitches on any two modules' outputs. The final voter is a simple circuit in itself, but if there is a need to avoid a single point of failure, the final voter can be triplicated and a TMR voter added at the end. As a result, failures of any two of the four modules, including physical and cloned modules, are masked by the architecture.

5.1.3 Operation of the Four-Modules Approach (second variant)

As shown in Figure 5.5, there are four static output detector blocks, a counter, a comparator, and a clone voter in each of the clone module blocks. Each clone module block receives PWM pulse outputs from the four physical modules. If in any of the four inputs (outputs from the four physical modules) a stuck-at 0 or stuck-at 1 fault is detected, that pulse is replaced with a short-duration pulse of the same frequency by the static detect block. The following signals are fed into the static-detect block in Figure 5.4:

1. The PWM pulse output of each module, (PWM_PULSE).
2. Each module’s PWM pulse output delayed by ½ PWM period, (PWM_PULSE_DELAYED).
3. A low-duration PWM pulse of the same frequency, (LOW_DURATION_PWM_PULSE).

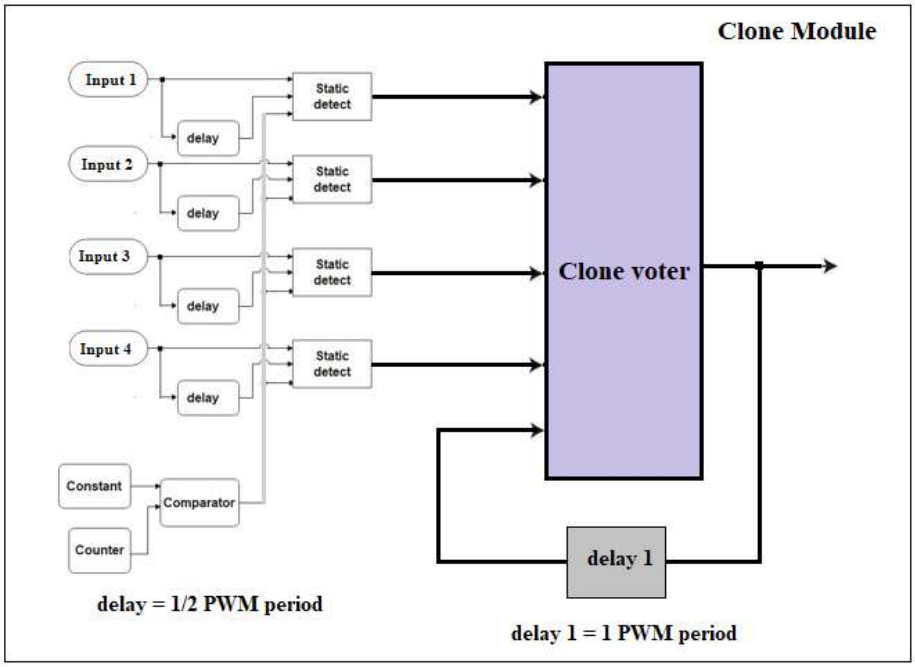


Figure 5.5. Clone module.

Comparing each of the four PWM input pulses to their 1/2 duty delayed counterparts should provide a difference if each pulse is free of the stuck-at 0 and stuck-at 1 fault. If this is the case, that pulse is propagated to the clone voter by the static detect block. The algorithm for the static-detect block is given below.

Algorithm 1 Static-detect block pseudocode

1: **Input:** PWM_PULSE, PWM_PULSE_DELAYED, LOW_DURATION_PWM_PULSE

2: **If** (PWM_PULSE ≠ PWM_PULSE_DELAYED)

3: **Output:** PWM_PULSE

4: **Else Output:** LOW_DURATION_PWM_PULSE

5: **End if**

Then, the clone voter generates an output representing a cloned module output and propagates it for the final voting. The algorithm for the clone voter is shown below.

Algorithm 2 Clone voter pseudocode

1: **Input:** STATIC_DETECT_OUT1, STATIC_DETECT_OUT2, STATIC_DETECT_OUT3, STATIC_DETECT_OUT4, PREVIOUS_PWM_PULSE

2: **If** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT2) && (STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT3) && (STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT4))

3: **Output:** STATIC_DETECT_OUT1

4: **Else if:** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT2) && (STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT3)

5: **Output:** STATIC_DETECT_OUT1

6: **Else if:** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT2) && (STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT4)

7: **Output:** STATIC_DETECT_OUT1

8: **Else if:** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT3) && (STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT4)

9: **Output:** STATIC_DETECT_OUT1

10: **Else if:** ((STATIC_DETECT_OUT2 = = STATIC_DETECT_OUT3) && (STATIC_DETECT_OUT2 = = STATIC_DETECT_OUT4)

11: **Output:** STATIC_DETECT_OUT2

12: **Else if** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT2) && (STATIC_DETECT_OUT1 = = PREVIOUS_PWM_PULSE))

13: **Output:** STATIC_DETECT_OUT1

14: **Else if** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT3) && (STATIC_DETECT_OUT1 = = PREVIOUS_PWM_PULSE))

15: **Output:** STATIC_DETECT_OUT1

16: **Else if** ((STATIC_DETECT_OUT1 = = STATIC_DETECT_OUT4) && (STATIC_DETECT_OUT1 = = PREVIOUS_PWM_PULSE))

17: **Output:** STATIC_DETECT_OUT1

18: **Else if** ((STATIC_DETECT_OUT2 = = STATIC_DETECT_OUT3) && (STATIC_DETECT_OUT2 = = PREVIOUS_PWM_PULSE))

19: **Output:** STATIC_DETECT_OUT2

20: **Else if** ((STATIC_DETECT_OUT2 = = STATIC_DETECT_OUT4) && (STATIC_DETECT_OUT2 = = PREVIOUS_PWM_PULSE))

21: **Output:** STATIC_DETECT_OUT2

22: **Else if** ((STATIC_DETECT_OUT3 = = STATIC_DETECT_OUT4) && (STATIC_DETECT_OUT3 = = PREVIOUS_PWM_PULSE))

23: **Output:** STATIC_DETECT_OUT3

24: **Else**

25: **Output:** 0

26: **End if**

By receiving six signals, the PWM outputs of the four physical redundant modules, and the outputs of the two clone modules, the final voter decides the final radiation fault free correct actual PWM pulse. A four out of six-majority voting procedure is used by the final voter to select the correct output.

5.2 THE SECOND APPROACH

The TMR-Simplex scheme, as explained in chapter 2, can be a good alternative for the TMR scheme and provides more reliability than either the TMR or Simplex system alone, allowing the scheme to be utilized for longer missions.

However, it abandons a working resource and has other operational limitations as described in chapter 2; consequently, another technique is sought that does not discard a working resource.

A new redundancy architecture is developed in order to meet the aforementioned research problem, as depicted in Figure 5.6. In this architecture, a hybrid redundancy system that blends Spatial/hardware and Temporal redundancies is employed to construct a high-reliability redundancy scheme that alleviates the issues affecting the traditional TMR or TMR-Simplex approaches. SEEs have one or more of the

following consequences on the DC-DC converter PWM controller output as described in chapter 4:

1. A change in the PWM controller output pulse duration(s) (for one or more cycles).
2. Pulse loss (due to complete failure of the PWM controller; most likely caused by a permanent change in output to logic-low or zero).
3. Missing pulses (due to the PWM controller's output being stuck at logic-high or logic-low for one or more cycles).

If any of these errors occur at a PWM controller's output, the voltage output of the converter controlled by the PWM controller will collapse or increase, interrupting the function or damaging the components supplied by the converter. However, for a particular input voltage, the operating duty cycle and, as a result, the logic-high length of the pulse generated by the PWM controller can be determined. This pulse duration can be used to identify and mask the three forms of radiation-induced errors listed above, ensuring that their effect does not alter the correct output state of the converter.

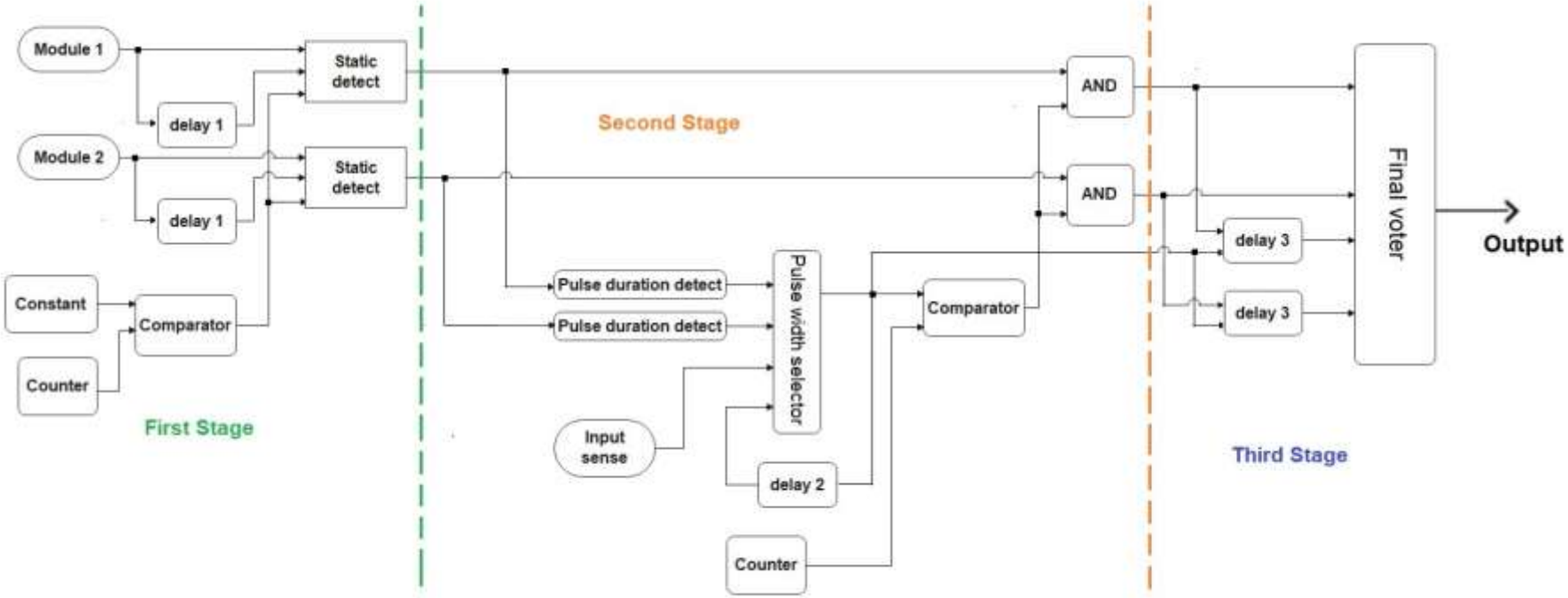


Figure 5.6. The proposed technique implementation for the two modules case

Figure 5.6 shows a two-module implementation of the proposed technique to demonstrate the concept. Note that the actual number of possible parallelable redundant modules is limited only by other design constraints, such as space and power requirements; otherwise, 2, 3, 4, 5, 6, 7, and so on, redundant modules can be paralleled to achieve the required level of reliability, regardless of whether they are an odd or even number of modules. This is one of the major advantages of the proposed technique.

As a result, the suggested technique's reliability outperforms conventional modular redundancy solutions for radiation hardening half-duty limited DC-DC converters. Figure 5.6 depicts the proposed voter in three stages. The following is how each stage works:

5.2.1 First Stage

A counter, a comparator, a constant block, two delay blocks, and two first-stage sub-voters make up this stage. The following faults are detected at this stage:

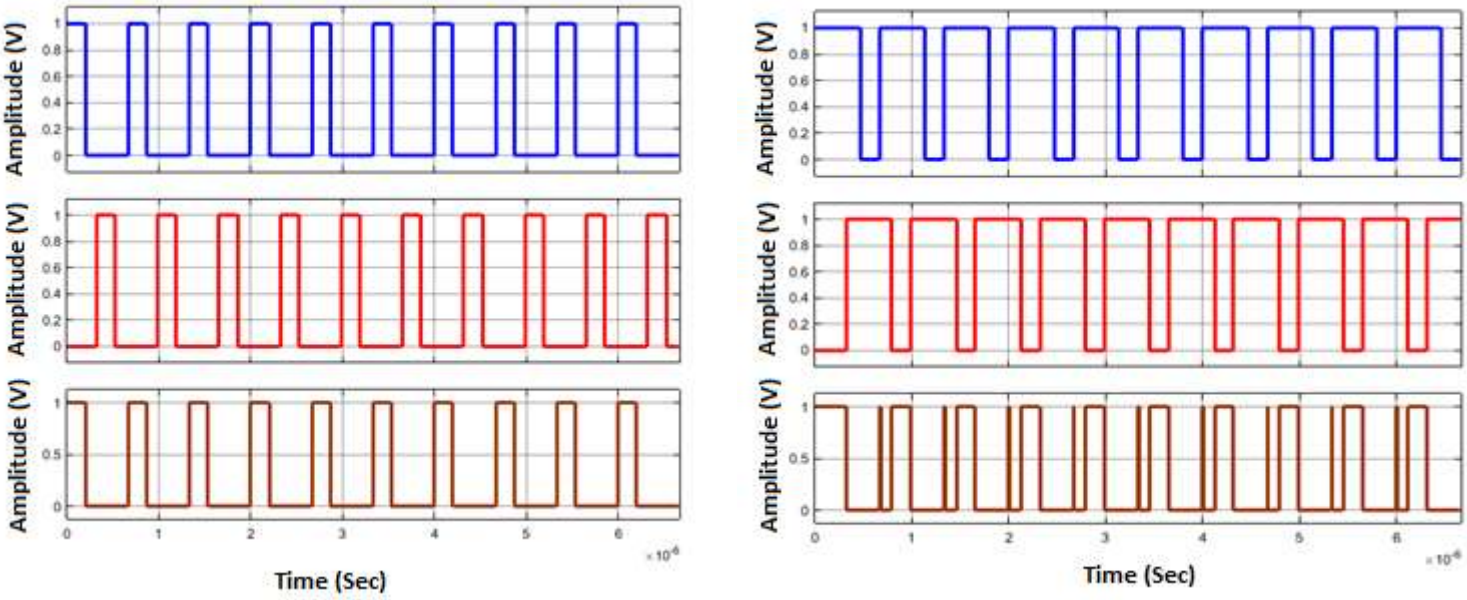
1. Faults that cause a change in PWM pulse duration that exceeds the maximum duty limit (max-duty value ≤ 50%).
2. Faults that cause one or more PWM cycles to be stuck at logic-high or logic-low.

Similar to the static-detect block discussed in the first approach, the controllers' outputs are replaced with a low-duration pulse of the same frequency if the above two fault categories are identified. The final stage is responsible for the actual masking of these replacement pulses.

If each module’s PWM output pulse is free of the faults listed above, or if radiation causes a pulse-duration change smaller than the fixed maximum duty-limit used, then comparing that module's PWM output pulse to its fixed maximum duty-limit delayed counterpart should yield a difference, as shown in Figure 5.7 a (upper-blue and middle-red). If this is the case, as shown in Figure 5.7 a, the first-stage sub-voter propagates the pulse to the next stage (lower-brown). If radiation causes a pulse-duration change greater than the maximum duty-limit used, the first-stage sub-voter passes that pulse only for the duration of time that that pulse and its maximum duty delayed counterpart are dissimilar; otherwise, the low-duration pulse is passed as indicated in Figure 5.7 b. Furthermore, if radiation produces a fault that causes a

module's output to be permanently or temporarily stuck at logic-low or logic-high, there will be no difference when this output is compared to its fixed maximum duty-limit delayed equivalent. As demonstrated in Figure 5.7 c, d, the first-stage sub-voter will substitute that module's output with a low-duration pulse of the same frequency.

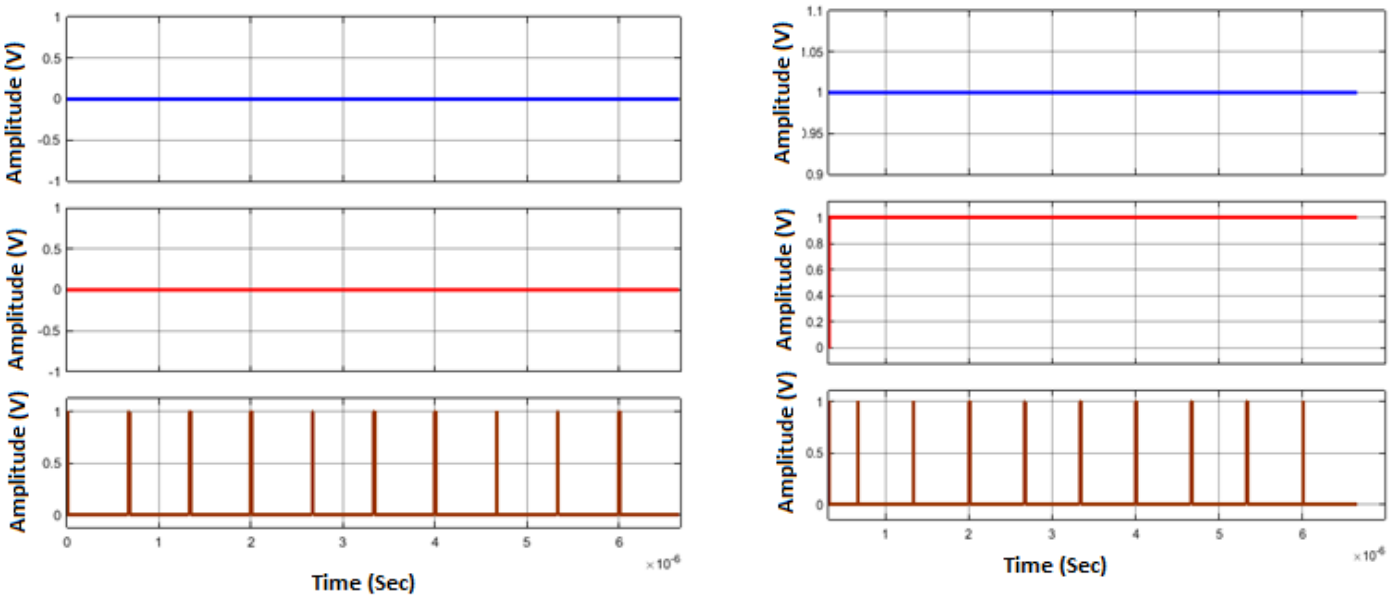
This stage involves identifying faults that result in a change in PWM pulse duration that is greater than the maximum duty-limit employed, including faults that are either permanent or temporary stuck at logic-low or stuck at logic-high for one or more PWM cycles. However, radiation-induced faults that result in a change in PWM pulse duration less than the maximum duty-limit are not detected at this stage. First-stage's sub-voter pseudocode is similar to the static-detect block discussed in the first approach.



(a) **(b)**

a) A 1.5 MHz 30% Actual duty PWM Pulse (upper-blue), its 48% Pulse-duration Delayed Counterpart (middle-red) and resultant first stage sub-voter output PWM pulse (lower-brown).

b) A Faulty 1.5 MHz 70% duty, (larger than the maximum duty, max-duty=48%), PWM Pulse (upper-blue), its 48% Pulse-duration Delayed Counterpart (middle-red) and resultant first stage sub-voter output PWM pulse (lower-brown).



(c) **(d)**

c) A Faulty 1.5 MHz 0% duty, (stuck at logic-low fault), PWM Pulse (upper-blue), its 48% Pulse-duration Delayed Counterpart (middle-red) and resultant first stage sub-voter output PWM pulse (lower-brown).

d) A Faulty 1.5 MHz 100% duty, (stuck at logic-high fault, PWM Pulse (upper-blue), its 48% Pulse-duration Delayed Counterpart (middle-red) and resultant first stage sub-voter output PWM pulse (lower-brown).

Figure 5.7. First stage detection process.

5.2.2 Second Stage

A counter, a comparator, a delay block, two pulse-duration detection algorithm blocks, and two two-inputs AND blocks make up this stage. The following functions are carried out by this stage:

1. Determines the current actual pulse duration by detecting the pulse durations of each incoming pulse.
2. Faults that cause a PWM pulse length change smaller than the maximum duty-limit but larger than the actual PWM pulse duration are detected and rejected (or corrected).

The pulse durations of each input pulse are detected in this stage, and the actual pulse duration is selected and used to generate a pulse that will be ANDED with the

outputs of the first stage. After the ANDING operation, only PWM pulses, with equal or smaller pulse lengths than the designated actual pulse duration, are allowed to advance to the third stage.

Note that, the previous correct PWM cycle's duty-value as well as the current input voltage value, (that is, the fact that the product of the input voltage and primary turn-on time is almost a constant value, no matter how fast the input voltage changes), is used to select the correct pulse-duration in the second stage sub-voter (Pulse width selector block in Figure 5.6). Therefore, the only faults that can pass through this stage are those that result in smaller pulse-durations than that of the actual pulse-duration.

The second stage works by inputting:

1. The outputs from the pulse-duration detectors, (PULSE_DURATION_1 and PULSE_DURATION_2).
2. The previous PWM cycle's duty value, (PREVIOUS_DUTY).
3. The current input voltage-output voltage relation, that is, current duty value calculated using the equation, (DUTY):

$$DUTY = \frac{N \cdot \ Output\ voltage}{Current\ input\ voltage} \cdot \text{NPWM} \qquad (5.2)$$

For an 8-bit DPWM utilized in the study, N is the turn-ratio, and NPWM = 2^8 =256. Because N, NPWM, and output voltage are all constants, the input detecting circuit just senses the current input voltage value.

The algorithm for the second stage pulse-width-selector block in Figure 5.5 is:

Algorithm 3 Second stage pulse-width selector block pseudocode

1: **Input:** PULSE_DURATION_1, PULSE_DURATION_2, PREVIOUS_DUTY, DUTY

2: **If** (PULSE_DURATION_1 = PULSE_DURATION_2)

3: **Output:** PULSE_DURATION_1

4: **Else If (**(PREVIOUS_DUTY ≤ PULSE_DURATION_1 + TOLERANCE) && (PREVIOUS_DUTY ≥ PULSE_DURATION_1 - TOLERANCE))

5: **Output:** PULSE_DURATION_1

6: **Else If (**(PREVIOUS_DUTY ≤ PULSE_DURATION_2 + TOLERANCE) && (PREVIOUS_DUTY ≥ PULSE_DURATION_2 - TOLERANCE))

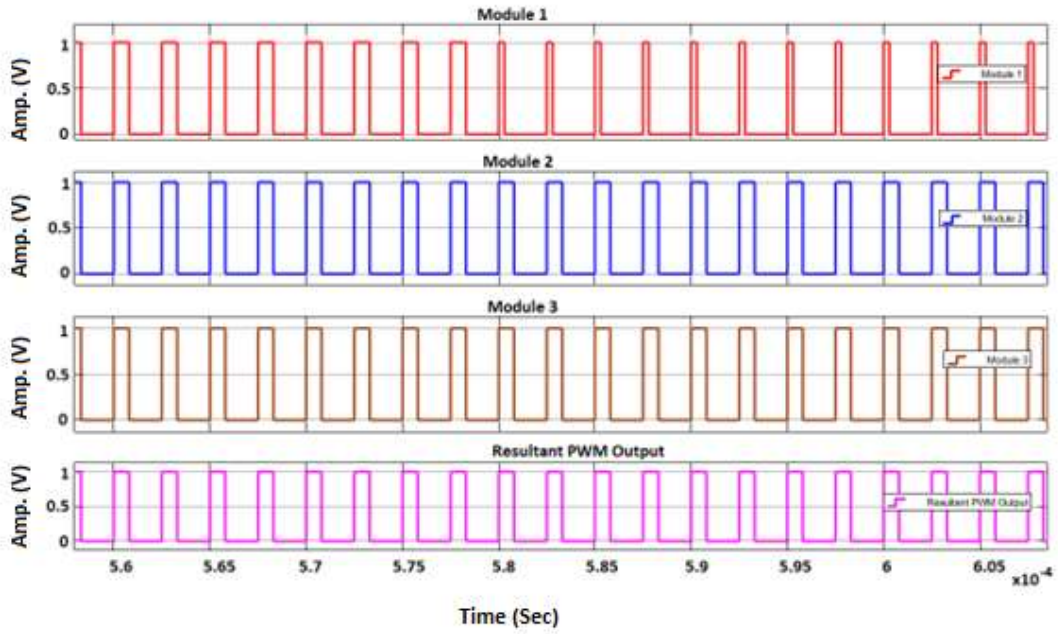
7: **Output:** PULSE_DURATION_2

8: **Else Output:** DUTY

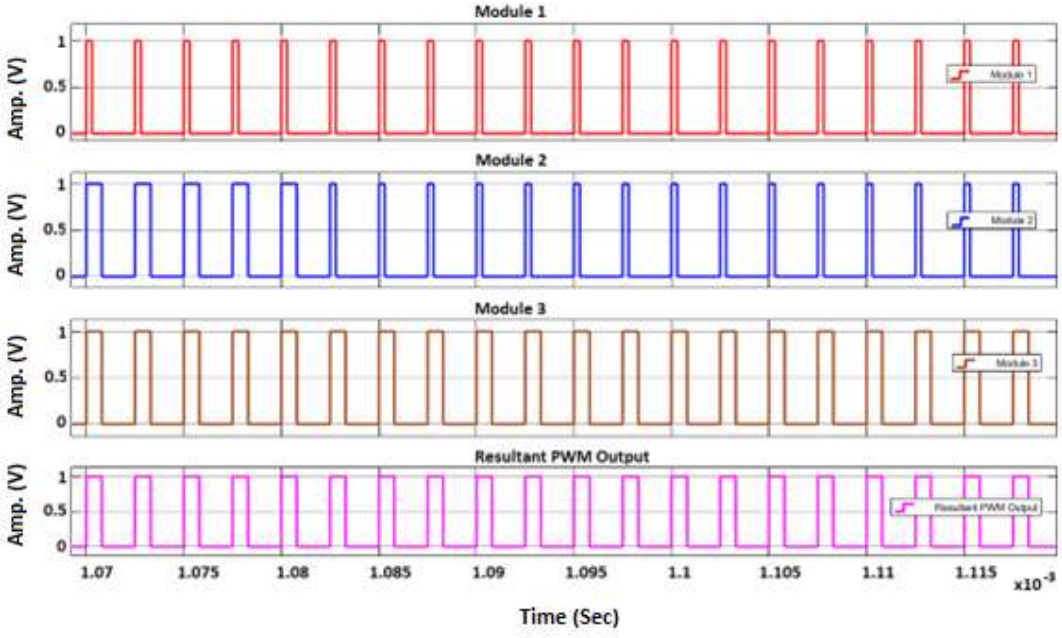
9: **End if**

The maximum output voltage variation/tolerance that can be tolerated determines the TOLERANCE value. The TOLERANCE value employed in this study is 2 clock-durations, which translates to a maximum duty value fluctuation of 2/256 = 0.0078125 or a 140mV output voltage variation above or below the nominal 4V value (maximum of 140mV variation occurs at the largest input voltage). The TOLERANCE value can be tightened if necessary.

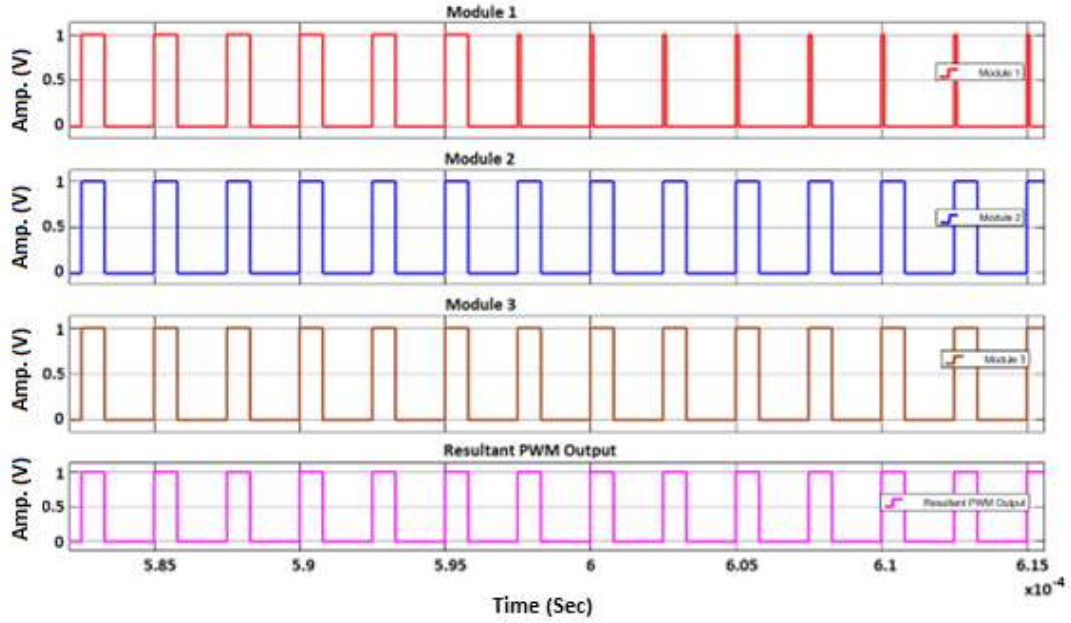
Figures 5.8 shows the simulation runs of the three-modules implementation of the proposed technique. In the figures, initially the three-modules system is running with the actual duty-value of 30%. Then after an approximately 0.58 milli-second, the first module is switched to a duty-value of 10% to emulate a radiation induced fault (figure (5.8 a)), then after an approximately 1.0825 milli-second the second module is switched to a duty-value of 10%, to emulate double fault, (figure (5.8 b)). Figure (5.8 c) shows the outputs after the AND blocks with the first module switched to a duty-value of 80% after approximately 0.5975 milli-second of the simulation run and figure (5.8 d) shows the outputs with the second module switched to a duty-value of 80% after approximately 1.03 milli-second of the simulation run. In Figures (5.8 c) and (5.8 d), since faulty pulses that have larger pulse-durations than the maximum duty-value are masked by the first stage, the outputs after the AND blocks are a low duration substitute pulses which can easily be masked by the third stage voter. In all the figures, the bottom pulse-graph is the resultant actual PWM pulse output after the third stage during the simulation runs. This shows that the failure(s) of one or two module(s) is masked by the two or single fault free remaining module(s) respectively.



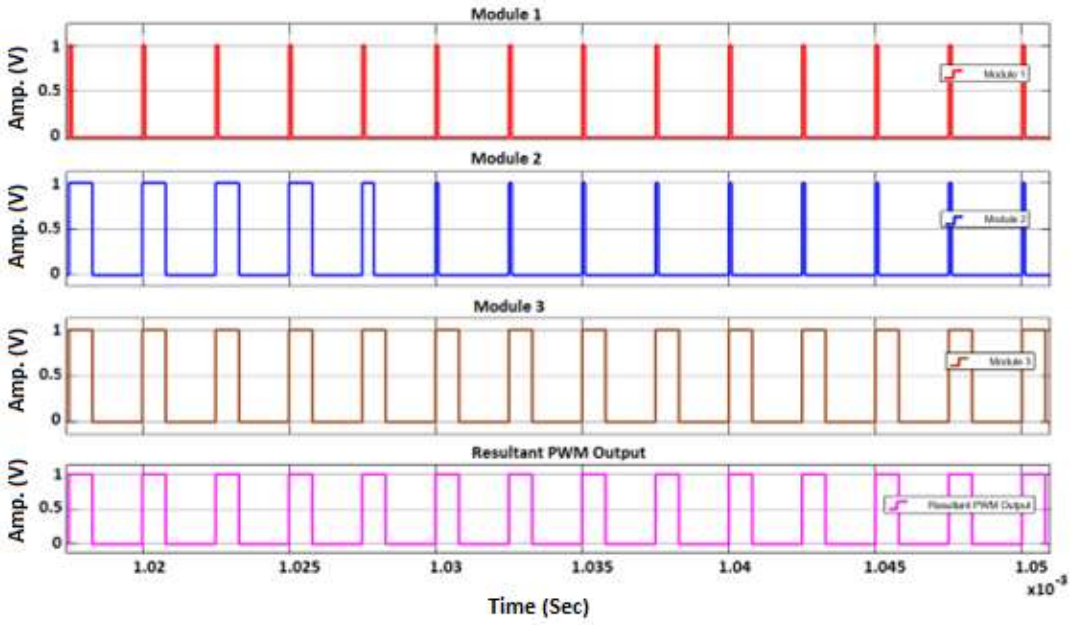
a) Outputs after AND blocks and the final voter when module 1 is forced to output 10% duty to emulate a sudden change in pulse-duration.



b) Outputs after AND blocks and the final voter when module 2 is also forced to output 10% duty to emulate a sudden change in pulse-duration.



c) Outputs after AND blocks and the final voter when module 1 is forced to output 80% duty to emulate a sudden change in pulse-duration.



d) Outputs after AND blocks and the final voter when module 2 is also forced to output 80% duty to emulate a sudden change in pulse-duration.

Figure 5.8. Second stage's detection and rejection process.

5.2.3 Third Stage

Two run-time delay blocks and the final sub-voter, (final voter in figure 5.6), make up this stage. A dynamically generated run-time delay is employed in this stage to detect and reject lower pulse-duration faulty pulses that have passed through the second stage.

The pseudocode for the third stage is similar to that for the first stage, with the exception that no low-duration-pulse is required as a replacement for the faulty pulses in this stage, and the delay duration is dynamically determined in the second stage so it is not constant. By inputting the two redundant modules' PWM outputs and their actual duty-value delayed counter-parts, the final sub-voter in this stage determines the final accurate actual PWM pulse. The algorithm for this stage's sub-voter is:

Algorithm 4 Third stage sub-voter pseudocode

1: **Input:** PULSE_OF_MODULE_1, PULSE_OF_MODULE_2, ACTUAL_PWM_DELAYED_PULSE_1, ACTUAL_PWM_DELAYED_PULSE_2

2: **If** (PULSE_OF_MODULE_1 ≠ ACTUAL_PWM_DELAYED_PULSE_1)

3: **Output:** PULSE_OF_MODULE_1

4: **Else If** (PULSE_OF_MODULE_2 ≠ ACTUAL_PWM_DELAYED_PULSE_2)

5: **Output:** PULSE_OF_MODULE_2

6: **Else Output:** 0

7: **End if**

As can be observed from Figure 5.9, while the actual pulse-duration delayed pulse (Figure 5.9 d) gives dissimilarity to the actual PWM pulse (Figure 5.9 b), at each clock cycle in the PWM cycle the smaller pulse-duration faulty pulse (Figure 5.9 a) is not different from its actual pulse-duration delayed equivalent (Figure 5.9 c), which can easily be detected and rejected by the final voter. This is because any low duration

pulse sent over from the second stage is overridden by the actual PWM pulse at this stage.

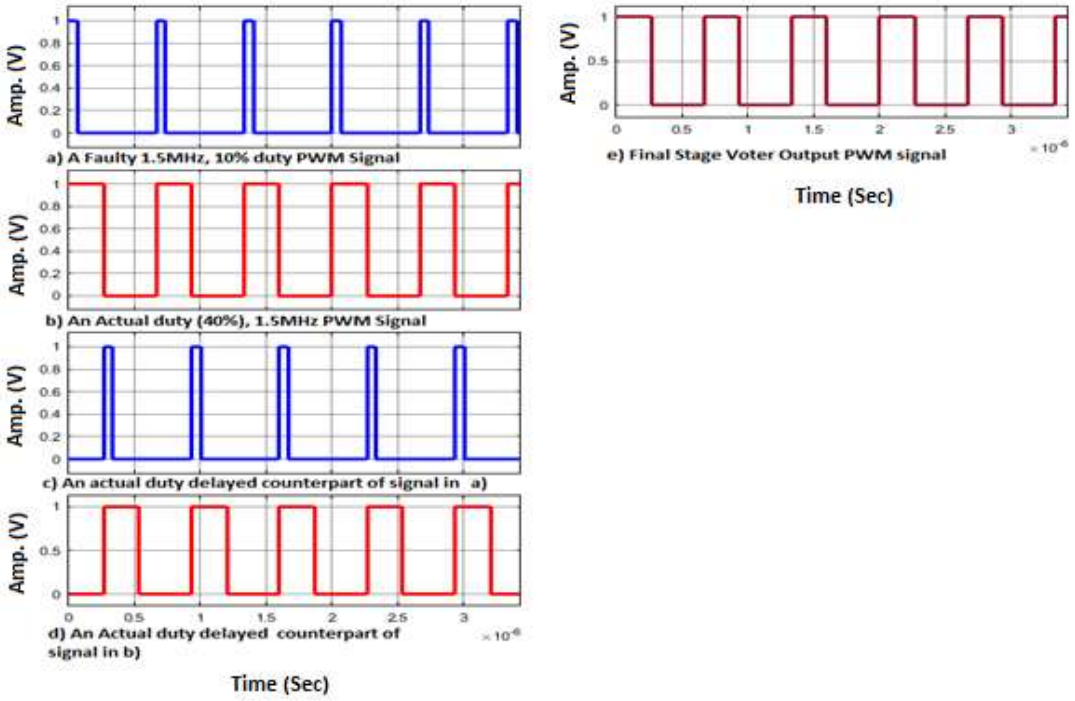


Figure 5.9. Third stage detection and rejection process illustrations.

Chapter 6: Case Study and Implementation

As a case study, two equivalent converters are designed, a synchronous buck converter and an isolated dual-switch forward converter. The designs and design parameters used in the case studies, as well as the fault injection method and technique used for the system's FPGA implementation, are described in the following subsections.

6.1 SYNCHRONOUS BUCK CONVERTER CONTROLLER DESIGN

6.1.1 Closed-loop Control System

A synchronous buck converter with digital control feedback is shown in Figure 6.1. The four functional units are an Analog-to-Digital Converter (ADC), a compensator (error compensation), a Digital Pulse-Width Modulator (DPWM), and a synchronous buck converter power stage.

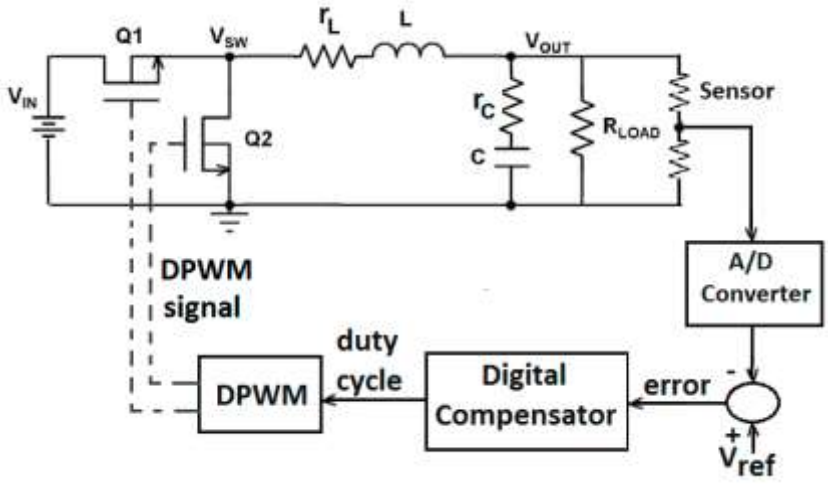


Figure 6.1. Digital closed-loop control of synchronous buck converter.

The purpose of this circuit is to keep the difference between V_{ref} and V_{out} as little as possible. As a result, we need to design a digital PID compensator to track the error and reduce it as much as practical.

6.1.2 Digital PID Compensator Design

Figure 6.2 shows a block diagram of the buck converter structure utilized for control system design purposes in this study.

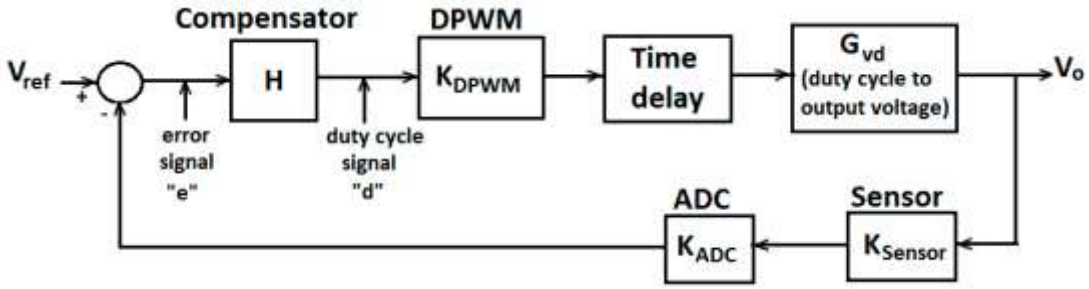


Figure 6.2. Buck converter from control system point of view.

The main blocks are the power stage or plant's duty cycle-to-output transfer function (G_{vd}), the compensator (H), the control loop's total time delay (T_d), the DPWM gain (K_{dpwm}), the ADC gain (K_{adc}), and the output voltage sensor gain (K_{sensor}). For a buck converter, the small signal control to output transfer function is given in [106] as.

$$G_{vd}(s) = \frac{V_i(sr_cC + 1)}{s^2LC\left(\frac{R + r_c}{R}\right) + s\left(r_cC\left(\frac{R + r_L}{R}\right) + \frac{L}{R} + r_LC\right) + \left(\frac{R + r_L}{R}\right)} \tag{6.1}$$

Table 6.1 lists the design parameters that were used.

Table 6.1

Design Parameters of the Converter

Parameter	Rating Value
Input Voltage (Vi)	12V, (11–16V)
Output Voltage (Vo)	5V
Output Current (Io)	2.5A, (1.25–5A)
Inductor (L), ESR	4.75µH, 10mΩ
Capacitor (C), ESR	2.466µF, 5mΩ
Load (R)	2Ω, (1–4 Ω)
Switching Frequency (Fsw)	1.5MHz

G_{vd} (s) is calculated using the above design parameters:

$$G_{vd}(s) = \frac{1.48e^{-07}s + 12}{1.131e^{-11}s^2 + 2.325e^{-06}s + 1.005} \tag{6.2}$$

The plant transfer function, including the impacts of the ADC, DPWM, and sensor, is:

$$G_{vdsys}(s) = K_{sensor}K_{ADC}K_{DPWM}G_{vd}e^{-s(t_{adc}+dT_s+t_{dpwm})} \quad (6.3)$$

where t_{adc} is the ADC conversion time and t_{dpwm} is the DPWM delay time.

The exponent term in Equation (6.3) reflects the entire time delay, which is commonly regarded to be equal to the switching period. That is, $T_s = (t_{adc} + dT_s + t_{dpwm})$. Then, the plant transfer function is given by:

$$G_{vdsys}(s) = K_{sensor}K_{ADC}K_{DPWM}G_{vd}e^{-sT_s} \quad (6.4)$$

In the MATLAB control system toolbox, the transfer function presented in Equation (6.4) is used to design the analog domain compensator. The gain margin of the designed compensator is 12.9dB, and the phase margin is 66.7 degrees.

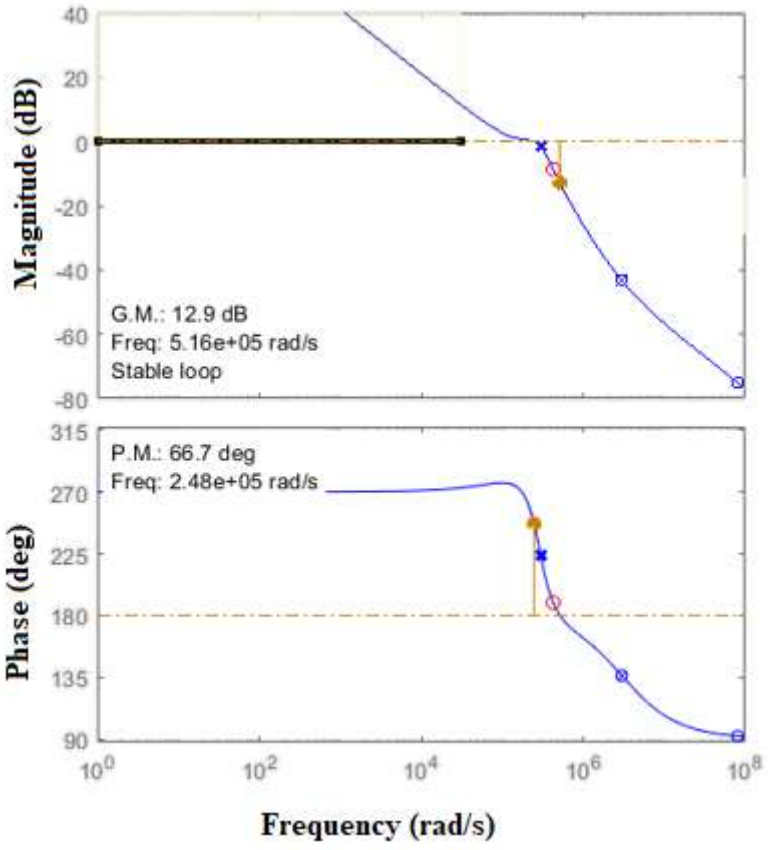


Figure 6.3. Bode plot of the designed compensator.

It's worth noting that the phase margin has been purposely increased to compensate for the loss of phase margin when converting to digital form. Using the bilinear transformation, the compensator is then converted to its equivalent digital form. The following is the final digital PID compensator transfer function:

$$G_c(z) = \frac{1.304e^{-02} - 2.032e^{-02}z^{-1} + 7.916e^{-03}z^{-2}}{1 - z^{-1}} \qquad (6.5)$$

6.2 DUAL-SWITCH FORWARD CONVERTER CONTROLLER DESIGN

Dual-Switch Forward converter, like the typical Single-Switch Forward converter, is derived from the buck converter topology. The main difference between a forward converter and a buck converter is that the forward converter uses a transformer. The transformer separates the input and output parts, and the turn ratio allows the duty cycle to be adjusted for the application's specific input and output voltage needs. The Dual-Switch Forward converter topology is shown in Figure 6.4. An input capacitor C_{IN}, two switches Q_H and Q_L, clamp diodes D_H and D_L, a power transformer T_1, rectifier diodes D_1 and D_2, an inductor Lo, and a capacitor C_o are all parts of the circuit. To enhance efficiency in applications with low output voltage, the rectifier diodes D_1 and D_2 on the secondary side of the power transformer can be replaced with synchronous rectifier switches at a somewhat higher cost.

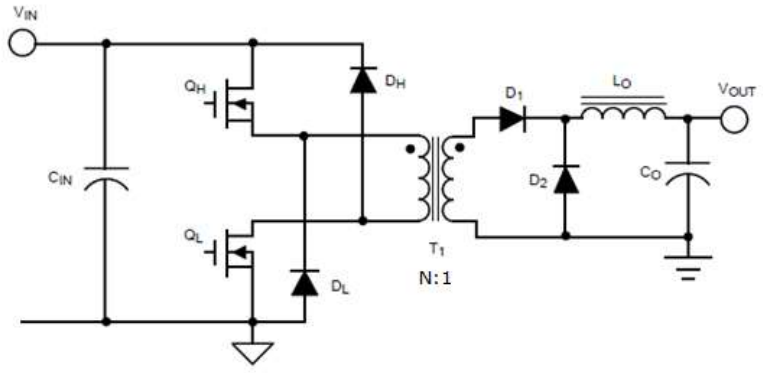


Figure 6.4. Dual-switch forward converter topology.

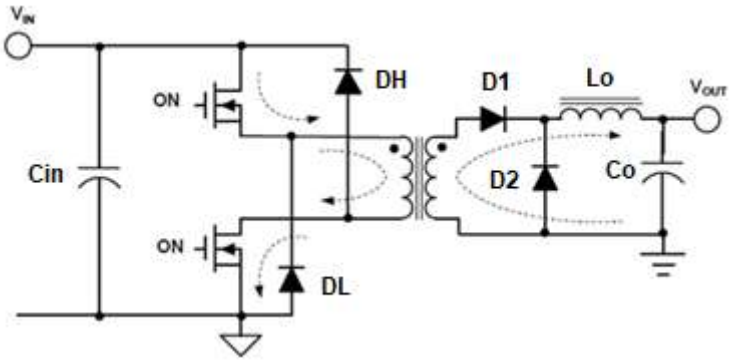
6.2.1 Operation Modes

The Dual-Switch Forward converter has two operational modes, as shown in Figure 6.5. The two switches are turned on and off at the same time during operations. The duty cycle of the switches is modulated to manage the output voltage. The

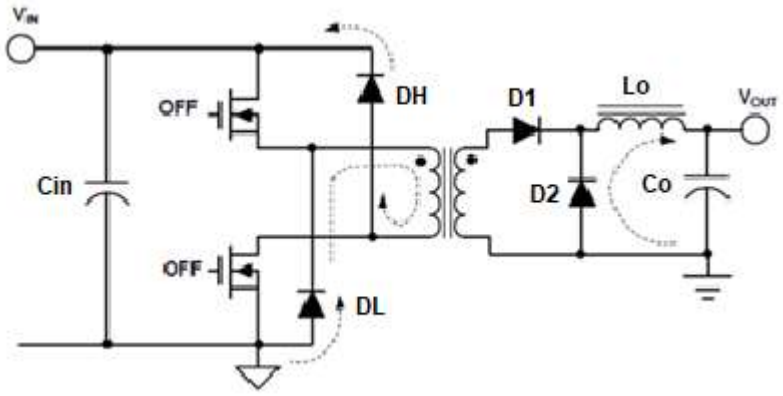
following equation describes the relationship between the input voltage V_{IN}, output voltage V_{OUT}, duty cycle D, rectifier diode forward-drop V_F, and transformer turns ratio N.

$$D = \frac{N \cdot (V_{OUT} + V_F)}{V_{IN}} \tag{6.6}$$

When the two switches are turned on, the input voltage is applied to the power transformer primary, as shown in Figure 6.5a. As a result, the transformer core becomes magnetized, and power is transferred to the secondary side circuit via the transformer coupling. When both switches are turned off, the power to the primary is cut off, as shown in Figure 6.5b. The voltage across the primary winding is reversed due to the transformer's residual magnetizing inductance, forcing the two clamp diodes DH and DL to conduct. By providing the input voltage in reversed polarity to the primary winding of the power transformer, the switch voltage is successfully clamped to the input voltage, and the transformer is demagnetized and reset.



a) Current paths during switches are on



b) Current paths during switches are off

Figure 6.5. Operating modes of dual-switch forward converter

During the ON and OFF periods of the power switches, the primary of the transformer gets voltages of almost similar magnitude but opposite polarities. To establish a volt-second balance between the magnetizing and demagnetizing periods, the maximum duty cycle should be kept below 50%. This will ensure that the Dual-Switch Forward converter completes a full reset of the power transformer during every switching cycle.

6.2.2 Digital PID Compensator Design

The Dual-Switch Forward Converter's design specifications are listed in Table 6.2 below.

Table 6.2

Design Parameters of the Dual-Switch Forward Converter

Parameter	Rating Value
DC Input Voltage (Vin) range	80 - 144V
Turn ratio, N	8
Output Voltage (Vout)	4V
Output Current (Io) range	2 -- 20A
Inductor (L), ESL	1μH, 8mΩ
Capacitor (C), ESR	13μF, 15mΩ
Load (R) range	0.2 - 2Ω
Switching Frequency (Fsw)	1.5MHz
Output Power (Po)	80 Watts
Maximum duty cycle (Dmax)	0.48
Efficiency (η)	> 90%

Because a forward converter is based on the buck converter topology, with the exception of the use of a transformer for isolation, the controller is designed by adopting a similar procedure as in the case of buck converter previously discussed. The MATLAB control system toolbox was used to design a voltage mode PWM controller (VMC) for the dual-switch forward converter in the analog domain. The designed PID compensator has a gain margin of 11.2dB and a phase margin of 54.2 degrees.

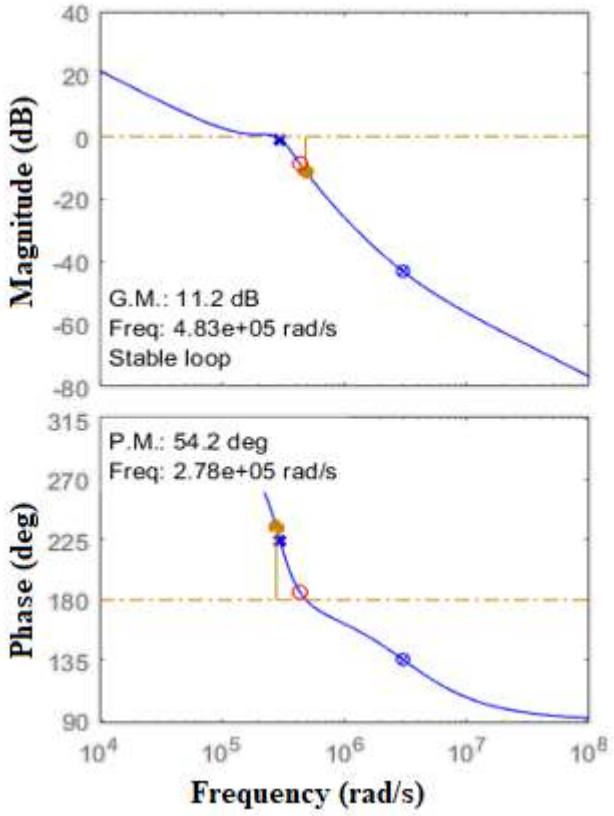


Figure 6.6. Bode plot of the designed compensator.

$$G_{Comp}(s) = \frac{7.7128\, e^{-08}\left(s + 4.332e^{05}\right)^2}{s} \qquad (6.7)$$

The bilinear transformation is then used to convert the designed analog compensator to its digital equivalent. The following is the final digital PID compensator transfer function:

$$G_c(z) = \frac{2.412e^{-02} - 3.743e^{-02}z^{-1} + 1.452e^{-02}z^{-2}}{1 - z^{-1}} \qquad (6.8)$$

6.3 SIGMA-DELTA ADC DESIGN

ADCs with sigma-delta modulation are common building parts in DC-DC converter digital controllers design [107]. The sigma-delta ADC has very few analog components and is primarily digitally processed on the FPGA. The first-order sigma-delta modulator will be employed in this work, as shown in Figure 6.7. It consists of a single-bit DAC, an integrator, and a comparator. The modulator disperses quantization noise away from the frequency range of interest by using feedback around the comparator, which acts as a single-bit quantizer. The modulator uses a closed loop system that samples and compares incoming analog input signal with the integrator voltage on the comparator's positive side.

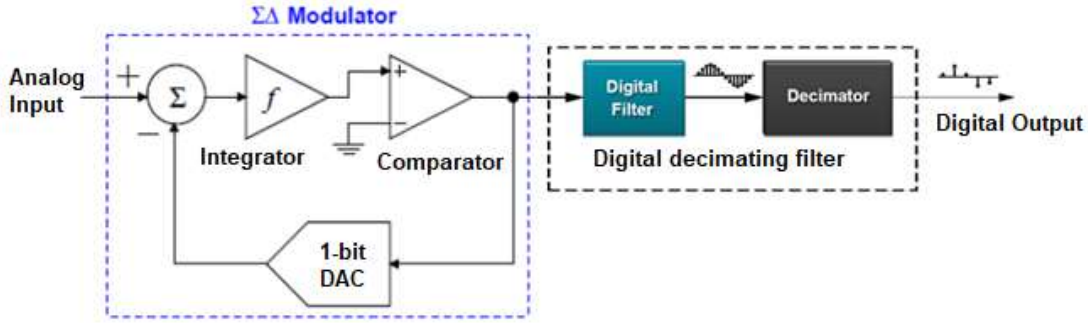


Figure 6.7. First-order sigma-delta ADC.

As a result, an oversampled bit stream of digital output represents the sampled analog input signal. To produce a good digital output conversion, the resulting bit stream of data should be filtered and decimated. The sampling rate of the input bit stream will be reduced using a cascaded integrator comb filter (CIC), with the results decimated and filtered further using a low pass filter (LPF).

Splitting the first order sigma-delta converter into analog and digital components allows for FPGA implementation of the converter. Basic analog integrated circuits can thus be used to build the analog half of the converter, while the digital half is implemented using FPGA [108],[109],[110],[111]. The functional block diagram shown in Figure 6.8 describes an FPGA based sigma-delta analog-to-digital implementation.

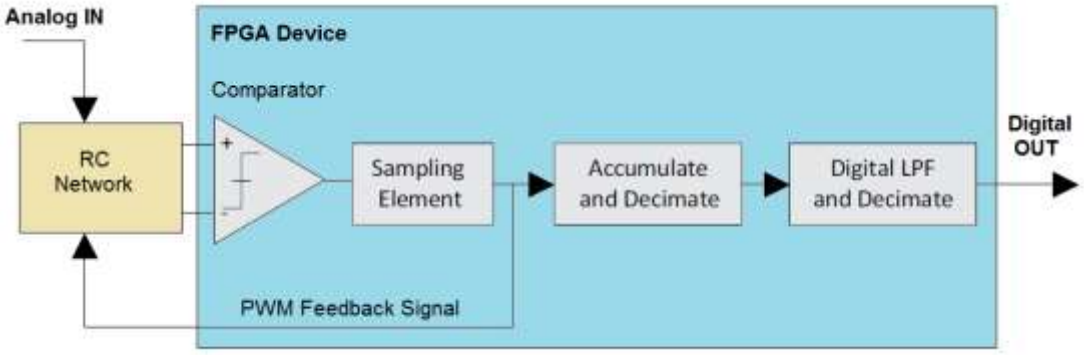
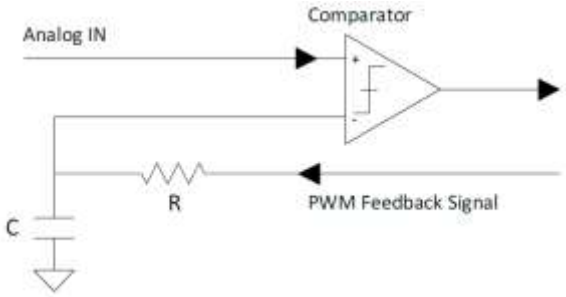


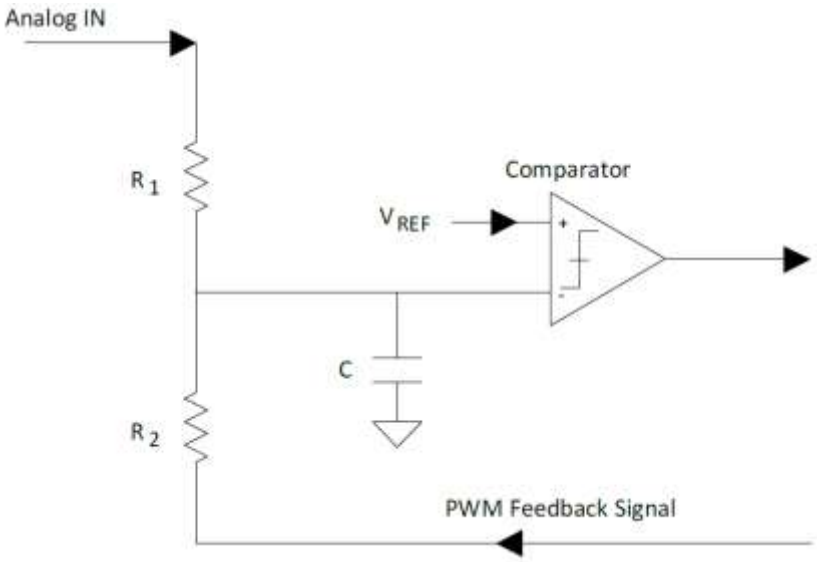
Figure 6.8. FPGA based sigma-delta ADC functional block diagram [111].

6.3.1 RC Network

The RC network output perfectly tracks the input-voltage at the comparator terminals by using the average value of the digital pulse over a given time period. Figure 6.9 shows two different methods to arrange the RC network stages [110],[111]. A topology with a small number of components is shown in Figure 6.9 (a). The disadvantage is that the analog signal is limited to the input voltage range of the comparator.



a)



b)

Figure 6.9. RC network topologies [111].

Figure 6.9 (b) depicts a more complex and flexible network with an acceptable component count increase and a flexible input voltage range while keeping the comparator terminals' input voltage fixed. In this work, the second topology is used with an external comparator setup.

6.3.2 Comparator

The comparator is used as a single-bit analog-to-digital converter (quantizer). Any low-voltage differential signalling (LVDS) capable comparator, including FPGA's on-board input buffers, can be used [111]. For maximum flexibility, an external LVDS capable comparator is used in this study.

6.3.3 Sampling Element

To capture the comparator output, a flip-flop running at the over sampling clock-rate is usually utilized as a sampling element [111]. The flip-flop’s output is a pulse-width modulated (PWM) version of the analog-input.

6.3.4 Digital Filter

Figure 6.8 shows the use of two-stage digital filters. These filters also integrate the PWM signal and give some anti-aliasing functionality. The digital filter's accumulator transforms the pulse-width-modulated stream from a single-bit, high-

frequency signal to a multi-bit, intermediate-frequency signal. This filter is commonly implemented as a comb filter (CIC).

The second filter uses an arithmetic average function on the accumulator data to reduce the frequency of the analog-to-digital converter output and provide anti-aliasing. This filter is usually implemented as a FIR filter.

For the designs in this study, a CIC filter performs all integration and decimation functions in the first stage, and a FIR filter performs low pass filtering in the second stage. Bitstreams from the modulator are fed into a decimation filter, which converts them to 8-bit resolution digital output in addition to the sign bit. We used three levels of CIC filters instead of a single large filter because multistage architecture allows much of the filter circuitry to operate at a lower frequency than a single stage decimator. The implemented sigma-delta ADC's block diagram is shown in Figure 6.10.

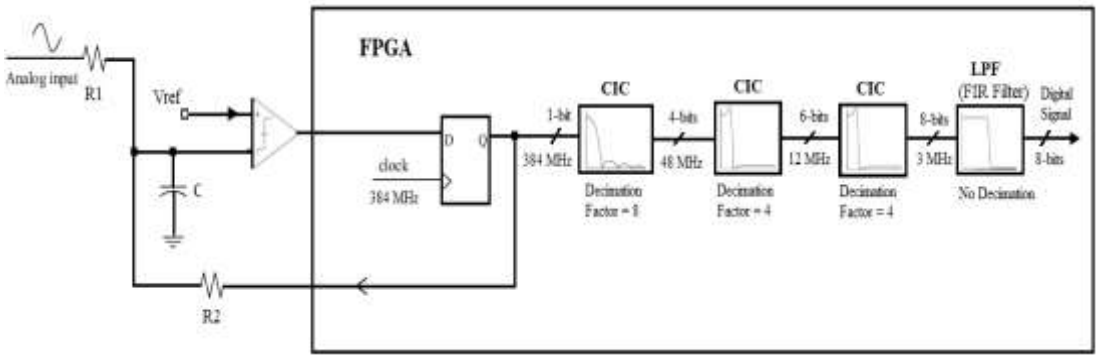


Figure 6.10. The implemented sigma-delta ADC.

The prototype ADC was chosen to operate in the switching frequency range (up to 1.5 MHz). For one of the designs, the values chosen for R1, R2, and C were 1k, 1k, and 2.7nF, respectively.

The first CIC filter stage takes one-bit samples at 384 MHz and outputs 4-bit samples at 48 MHz It consists of a single-stage CIC filter with a decimation factor of 8. The previous CIC filter's output samples are passed into the second CIC stage, which produces 6-bit samples at 12 MHz with a rate change factor of 4, this filter is also a single-stage CIC filter. The third CIC filter stage accepts the output samples from the second CIC filter and outputs 8-bit samples at 3 MHz This is also a 4-rate change factor single-stage CIC filter. The low-pass FIR filter stage is designed to attenuate

signals outside the region of interest, with a sharp cut-off frequency of 3 MHz as shown in Figure 6.11.

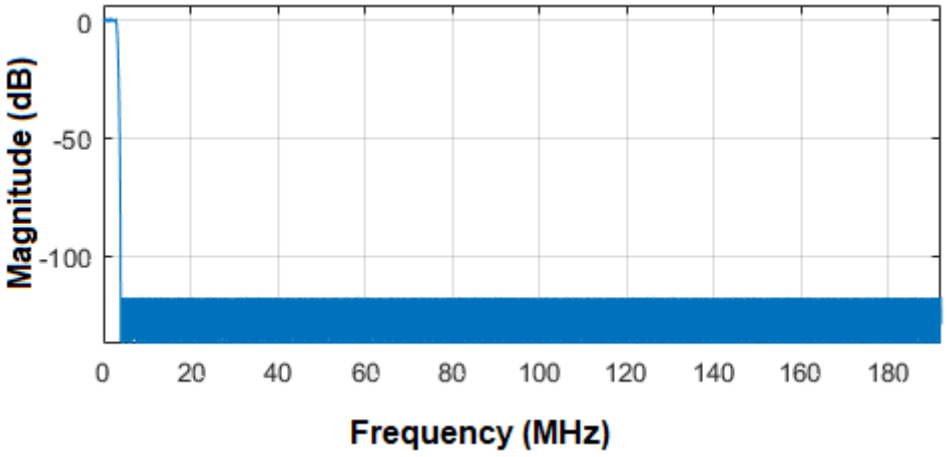


Figure 6.11. Magnitude response of the designed filter.

6.4 DIGITAL PWM GENERATOR

One of the most important components of a DC-DC converter's digital controller is the digital pulse-width modulator (DPWM). The DPWM receives the duty-cycle information from the compensator's output and delivers suitable switching signals, to the power stage, to provide the appropriate output voltage.

To achieve high-bandwidth, precision voltage regulation in digitally controlled DC-DC converters, high-frequency, high-resolution DPWMs are required. Even though sigma-delta or dithering techniques can improve effective DPWM resolution to some extent, achieving high-hardware resolution with as few hardware resources as practical is far better. As a result, we have used a counter-based DPWM [112], which is a digital-domain equivalent of analog PWM.

Each input clock cycle advances an n-bit counter. The input-clock frequency, F_{clk}, of a counter-based DPWM is proportional to the number of bits used in the counter, N_{DPWM}, and the switching frequency, F_{sw}, required. Counter-based DPWM has the advantages of simplicity and linearity.

$$F_{clk} = 2^{N_{DPWM}} F_{sw} \tag{6.9}$$

6.5 FAULT INJECTION MECHANISM

Fault injection methods employed in this study are based on simulation and emulation approaches, as mentioned in Chapter 3. While simulation-based fault injection methods have a high level of observability and controllability, they can take a long time to complete. One alternative is to adopt an emulation-based fault injection method that makes use of the high running speed of a prototype implemented on an FPGA, but only if the entire design, including the fault models, is synthesizable. Synthesizable fault models from [113] are used to test the proposed methods in both simulation and emulation approaches in this work.

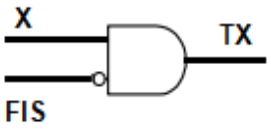
The synthesizable fault models described in [113] can be employed to inject the following fault categories into the HDL design at the appropriate locations.

1) Permanent faults (extra-long pulses or missing pulses or permanent failure).
2) Transient faults (single event transient).
3) Bit-upset faults (single event upset(s)).

These are the types of faults that cause the PWM controller output to be corrupted resulting in an anomaly at the power converter's output as described in chapter 4. This is because these faults occur at one or more locations inside the controller's logic design. Modifying the system's target VHDL model and adding new gates and wires to the design description can be used to inject these faults during simulation or emulation.

6.5.1 Permanent fault models

The following logic-gates arrangements are used in VHDL design to support permanent faults (stuck-at 0 or stuck-at 1 faults), with a wire called Fault Injection System (FIS) managing the activation and deactivation of the faults as needed. The permanent fault into the selected wire will be injected by setting the FIS signal high during fault injection time as shown in Figure 6.12 [113].



Synthesizable fault model for stuck-at-0

Synthesizable fault model for stuck-at-1

Figure 6.12. Synthesizable permanent fault models [113].

The truth tables for the stuck-at-0 and stuck-at-1 fault categories are provided in Tables 6.3 and 6.4, respectively.

Table 6.3

Truth Table for Stuck-at-0 Synthesizable Fault Model

X	FIS	TX
0	0	0
1	0	1
0	1	0
1	1	0

Table 6.4

Truth Table for Stuck-at-1 Synthesizable Fault Model

X	FIS	TX
0	0	0
1	0	1
0	1	1
1	1	1

When injecting either stuck-at 0 or stuck-at 1 permanent faults by setting FIS input high, the original signal (say X) will be replaced with a modified signal TX wherever, in the design, the fault models are applied.

6.5.2 Transient fault model

Figure 6.13 depicts the circuit for a transient fault injection. Similar to permanent faults, a fault emulating a transient fault can be injected at the relevant locations in the design by keeping the FIS signal high for the required duration of time [113].

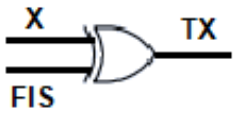


Figure 6.13. Synthesizable transient fault model [113].

Table 6.5 shows the truth table for the transient synthesizable fault model while Figure 6.14 shows the simulation waveforms.

Table 6.5

Truth Table for Transient Synthesizable Fault Model

X	FIS	TX
0	0	0
1	0	1
0	1	1
1	1	0

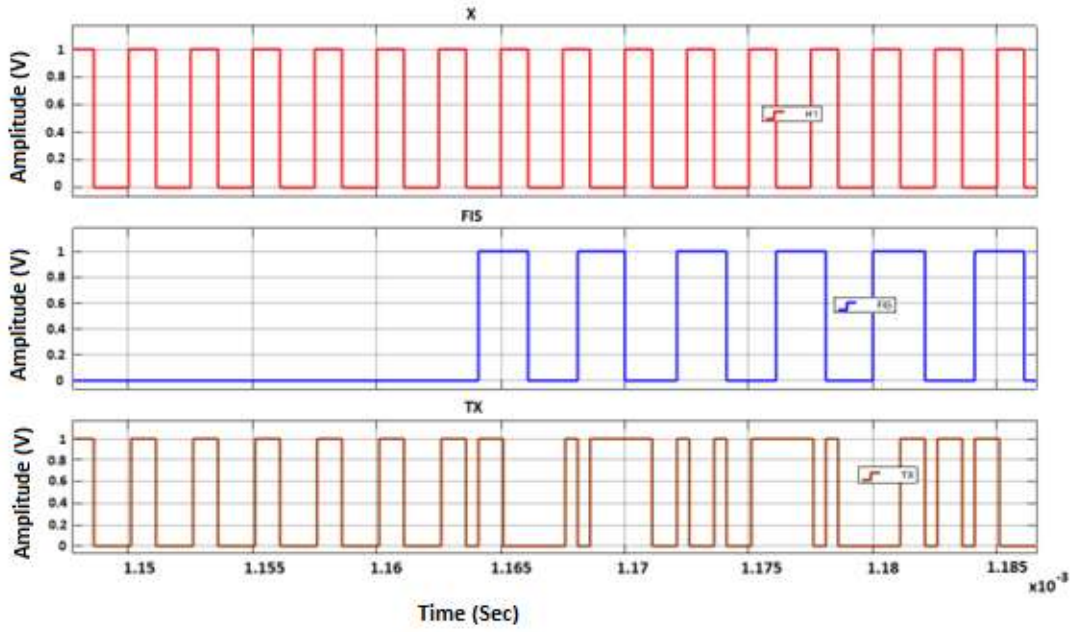


Figure 6.14. **S**ynthesizable transient fault model simulation.

6.5.3 Bit-flip or single event upset fault model

A circuit for emulating a bit-flip at the required place in the design description is shown in Figure 6.15 [113].

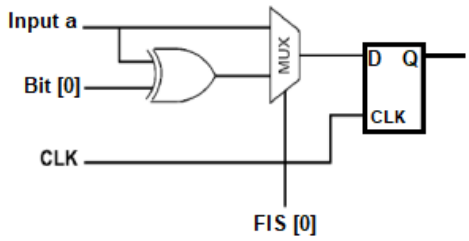


Figure 6.15. Synthesizable single event upset fault model [113].

To simulate a bit-flip fault, the signals Bit and FIS, a multiplexer, and a flip-flop are used in addition to the XOR gate. When both the FIS and Bit signals are high, the inverted input is passed to the flip-flop for the next clock, and any input received after the Bit and FIS signals are high, is flipped. The truth table and simulation waveforms of a bit-flip synthesizable fault model are shown in Table 6.6 and Figure 6.16 respectively.

Table 6.6

Truth Table for a Bit-flip Synthesizable Fault Model

Input a	FIS & Bit	Output
0	0	0
1	0	1
0	1	1
1	1	0

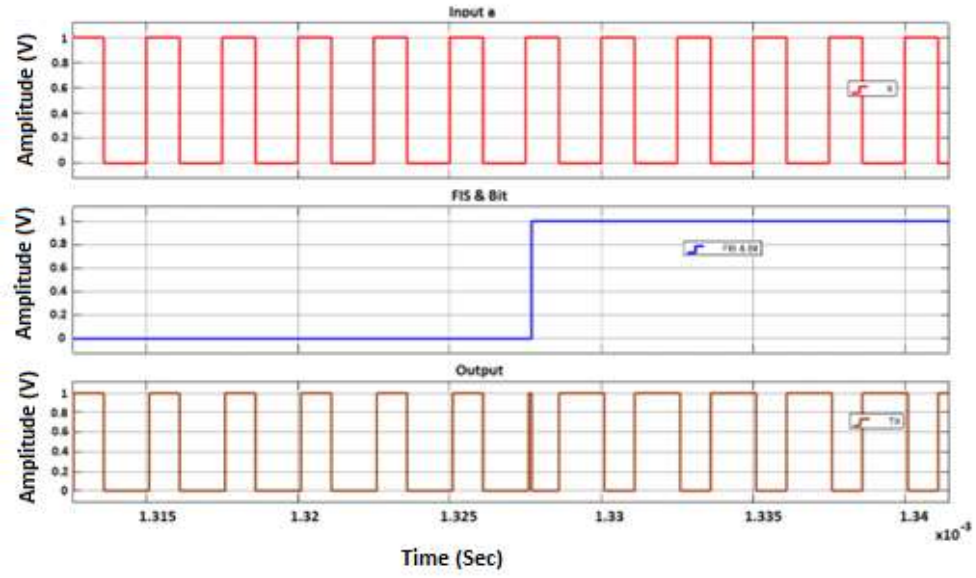


Figure 6.16. **S**ynthesizable bit-flip fault model simulation.

6.6 IMPELEMENTATION

In this study, a model-based design approach is used to design, implement, and test the proposed methods. There are nowadays more intelligent systems in the world than humans. As technology advances, these systems become more sophisticated and their capabilities expand. To perform well in navigation, propulsion, and security, a self-driving electric automobile, for example, requires around 1 billion lines of code [114]. To build and test such complex software, a model-based design methodology is required. In general, as projects become more complex, the ability to break down a system's components and model its functionality with the associated controls becomes increasingly important. A model-based design approach is usually used to accomplish this.

Model-based design has a number of advantages, including the capability to make the design process more efficient, consistent, highly reliable, adaptive, and less expensive. The capability to build modular systems is a critical component of model-based design because the entire system is built using foundational blocks. It is possible to design a hierarchical architecture that depicts the system model's many layers of abstraction using the subsystem notion. These techniques enable designers to encapsulate the operation of their subsystems, making the system easier to comprehend and test.

MATLAB's FPGA-based design framework is quite well integrated. MATLAB can be used for design, simulation, co-simulation, and verification [115]. Because of this tight integration, a single HDL design description may be produced and refined both architecturally and algorithmically in a single design environment.

Figure 6.17 shows a typical model-based design flow for planning, designing and implementing different applications in the MATLAB and Simulink environment [116].

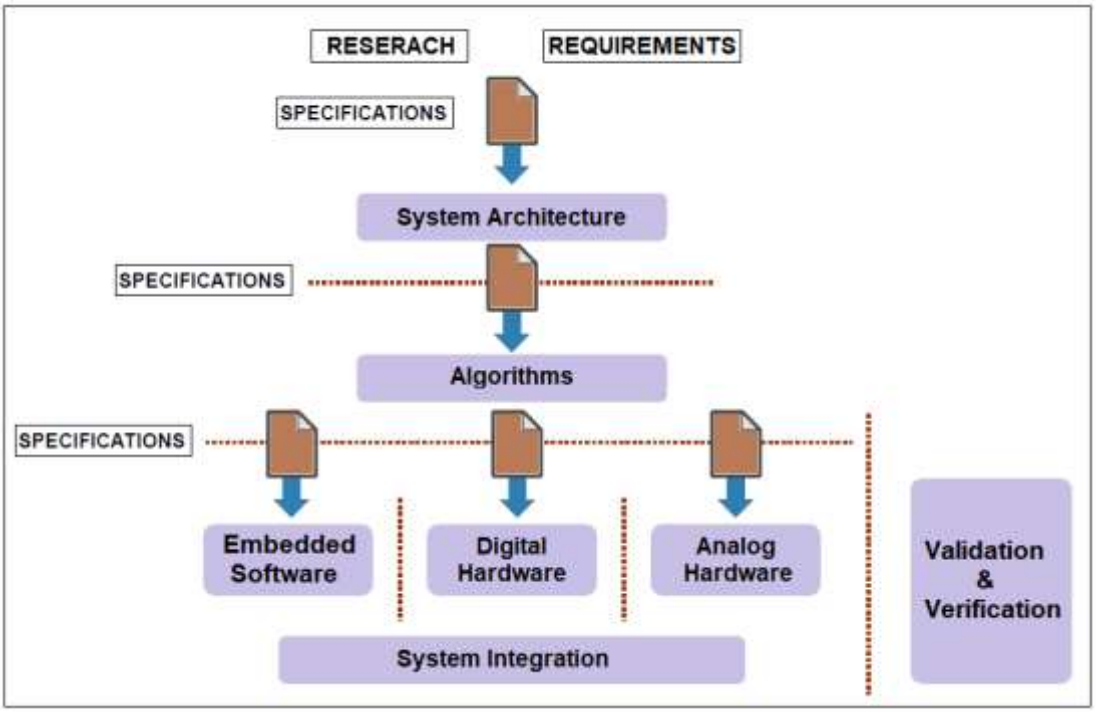


Figure 6.17. Model-based design flow for various applications in MATLAB/Simulink [116].

Model-in-the-Loop (MIL) can be used to test design criteria directly in the simulation environment, as well as to create source code for further analysis and verification on a real system using the Hardware Co-simulation platform.

Nowadays, the technique is used to tackle engineering problems by visualizing the system's building parts and their interactions using a fundamental mathematical framework. It is utilized in signal processing, communication, control systems, process control, automobiles, power systems, aerospace, and space, to name a few engineering domains. Many tools and approaches are now available that allow this paradigm to be used to the design of efficient and cost-effective embedded systems.

Figure 6.18 portrays the model-based design flow used in this study to realize and test the proposed system.

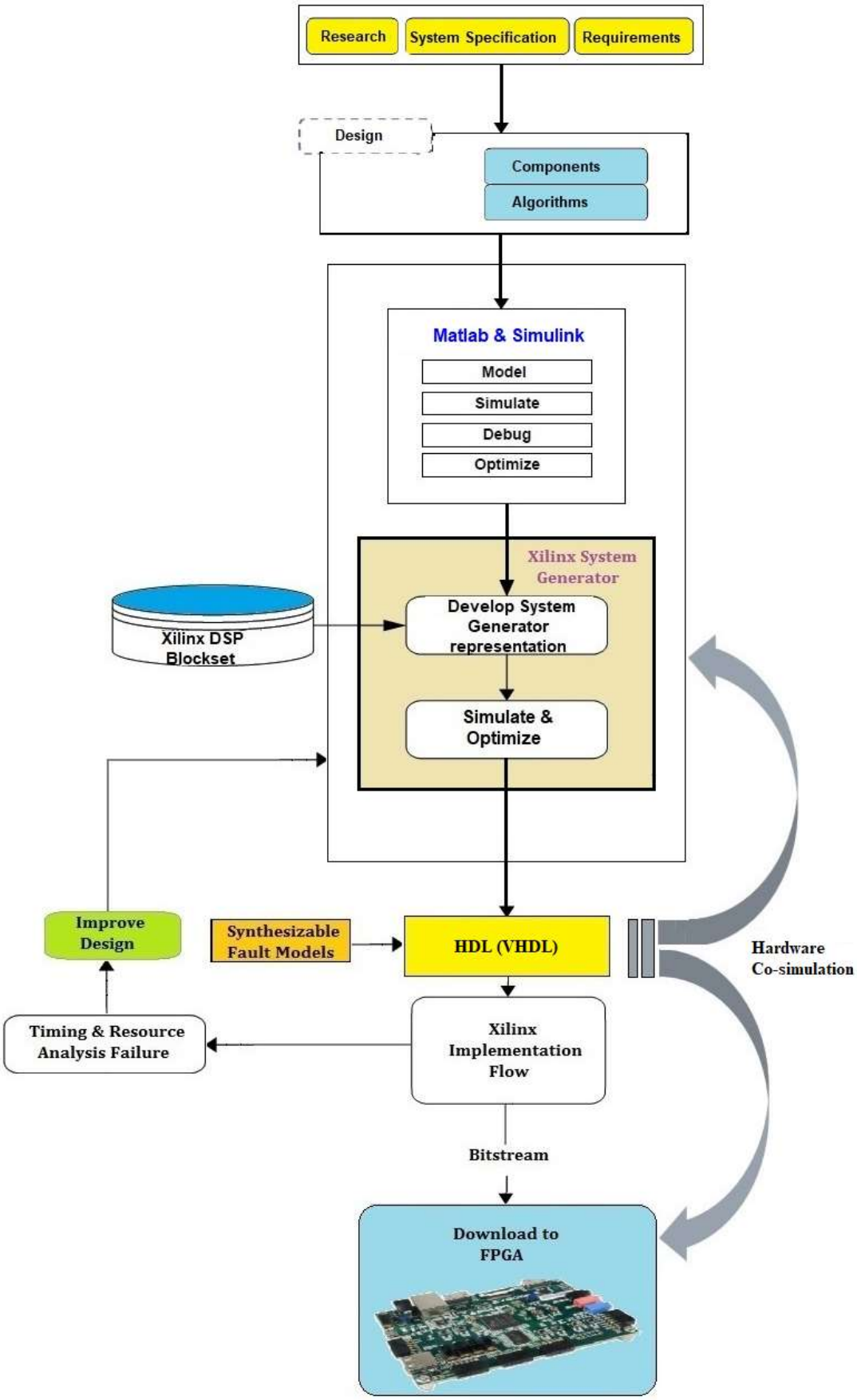


Figure 6.18. Model-based design flow employed.

Chapter 7: Tests and Results

7.1 PERFORMANCE RESULTS

We have validated the proposed techniques by implementing the prototype on the zynq-7000 (zybo) board, which has a non-radiation hardened Artix 7 SRAM-based FPGA, using a Xilinx system generator and MATLAB/Simulink. The digital controllers were used to test the suggested approaches' functionality and radiation fault mitigation capabilities. The first approach is tested using a buck converter controller implementation, whereas the second technique is tested using a dual-switch forward converter implementation.

7.1.1 FPGA Resource Utilization Results

Tables 7.1 and 7.2 demonstrate the FPGA resource utilization overheads of the two proposed strategies in comparison to the commonly used methods. While the first proposed four-modules method, as shown in Table 7.1, requires fewer resources than FMR and the proposed modified triplex–duplex redundancy, it does require more resources than the TMR method due to the full implementation of an additional digital controller. Its advantage over the TMR technique is higher reliability, as explained in the next section.

Table 7.1

Comparison of the first Strategy with Regularly used Methods in terms of Hardware Resource Utilization

Methods	DSP (80)	LUT (17600)	Registers (35200)
TMR	3	1934	874
Proposed Technique (Four Modules)	4	2710	1189
FMR (Five Modules)	5	3195	1446
Proposed Modified Triplex-Duplex (Six Modules)	6	4053	1729

The resource utilization of the second technique with two and three module implementations is shown in Table 7.2. The two-module version of the approach uses fewer resources (LUT) than the TMR implementation. Except for the DSP usage, the three-module version only required 2% more of the FPGA resource. Each redundant

module's ADC implementation requires one DSP; thus, TMR uses three DSPs, whereas the proposed method's two-module and three-module implementations use three and four DSPs, respectively. One more DSP is required for the implementation of the ADC in the input voltage sensing circuit.

Table 7.2

Comparison of the Second Strategy with TMR Method in terms of Hardware Resource Utilization

Methods	**DSP (80)**	**LUT (17600)**	**Registers (35200)**
TMR	3	1500	1467
Proposed Technique (Two Modules)	3	1317	1536
Proposed Technique (Three Modules)	4	1793	2094

7.1.2 Reliability, RIF and MTTF Evaluations

In terms of mean-time-to-failure (MTTF), reliability-improvement factor (RIF), and reliability, this section compares the proposed methods to commonly used redundancy approaches. Equation (3.11) gives an expression for the MTTF, which indicates an average life span before the first failure, whereas equation (3.14) establishes reliability expression for TMR technique. The reliability expression for the first proposed four-module technique, assuming Rm as the reliability of a simplex module, can be determined as follows using equation (3.12).

$$R_{Four\_mod} = B(4:4) + B(3:4) + B(2:4) \quad (7.1)$$

$$R_{Four\_mod} = \binom{4}{4}R_m^4(1-R_m)^0 + \binom{4}{3}R_m^3(1-R_m)^1 + \binom{4}{2}R_m^2(1-R_m)^2 \quad (7.1.i)$$

$$R_{Four\_mod} = 3R_m^4 - 8R_m^3 + 6R_m^2 = 3e^{-4\lambda t} - 8e^{-3\lambda t} + 6e^{-2\lambda t} \quad (7.1.ii)$$

Following similar procedure, the reliability of Five-Modular-Redundancy (FMR) method is given by:

$$R_{5MR} = 10R_m^3 - 15R_m^4 + 6R_m^5 = 10e^{-3\lambda t} - 15e^{-4\lambda t} + 6e^{-5\lambda t} \quad (7.2)$$

Similarly, reliability formulas for the two-module and three-module implementations of the second technique are given as follows:

$$R_{two\_modules} = 2R_m - R_m^2 = 2e^{-\lambda t} - e^{-2\lambda t} \quad (7.3)$$

$$R_{three\_modules} = R_m^3 - 3R_m^2 + 3R_m = e^{-3\lambda t} - 3e^{-2\lambda t} + 3e^{-\lambda t} \quad (7.4)$$

Figure 7.1 shows the reliability of simplex, TMR, FMR and the proposed four-modules implementation of the first approach vs the normalized mission time (time/MTTFsimplex). The proposed technique clearly outperforms both TMR and FMR techniques.

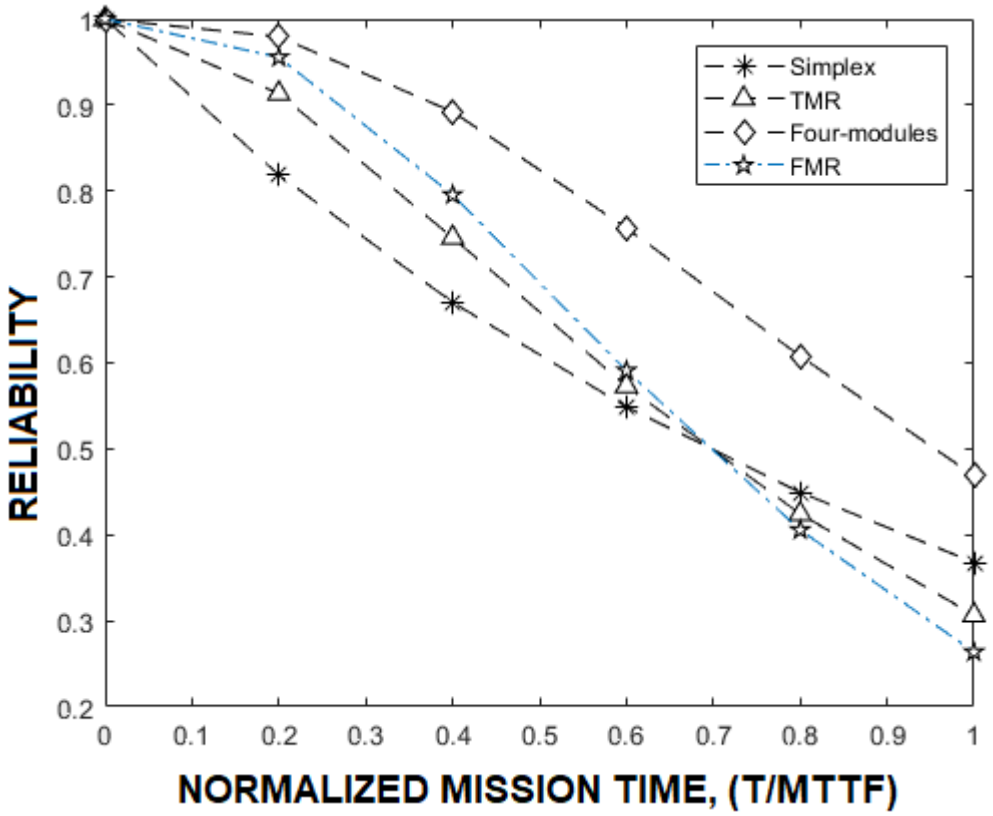


Figure 7.1. Reliability versus normalized mission time for simplex, TMR, FMR and the proposed four modules method.

Figure 7.2 depicts the reliability of simplex, TMR, TMR-Simplex and the proposed two-module and three-module implementations of the second approach vs. normalized mission time (time/MTTFsimplex).

As shown in Figure 7.2, when compared to both TMR and TMR-Simplex approaches, the proposed method provides the best reliability for all t> 0, making it suitable for comparatively longer mission time applications. The graph further emphasizes the idea that the suggested second technique's dependability grows as the number of paralleled redundant elements increase.

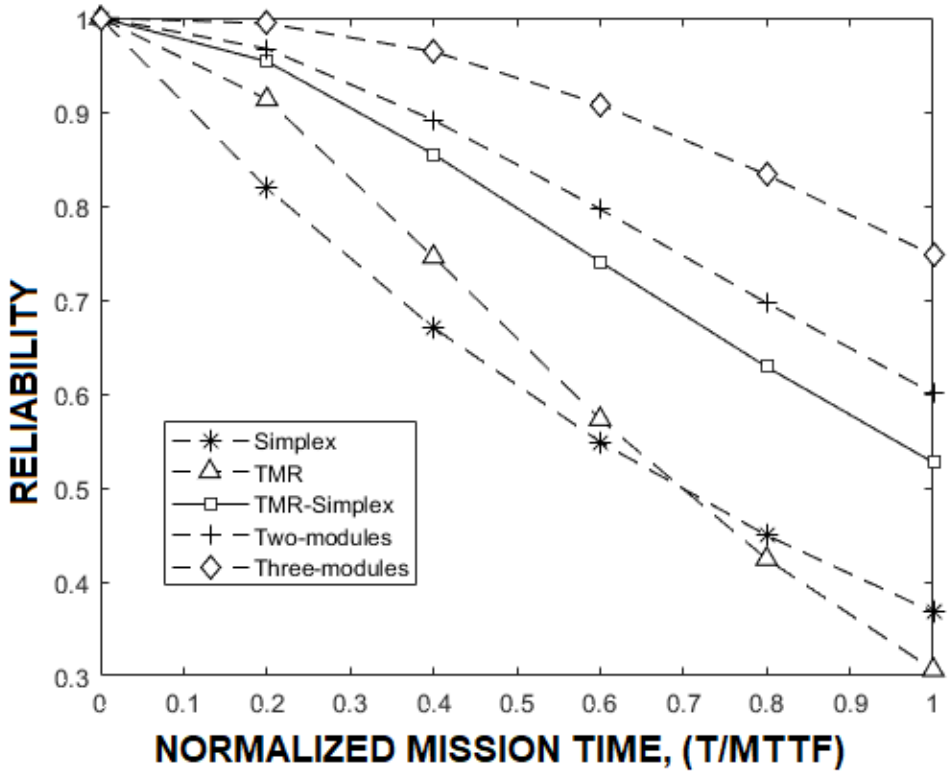


Figure 7.2. Reliability versus normalized mission time for simplex, TMR, TMR-Simplex and the proposed method for two and three modules implementation.

Tables 7.3 and 7.4 show that, as indicated by these reliability measurement metrices, both suggested strategies outperform TMR and TMR-Simplex techniques for the stated domain of applications, and so are more suitable for comparatively longer mission time applications.

Table 7.3

Comparisons of the First Approach to Commonly used Methods in terms of Reliability, MTTF, and RIF

Methods	**Reliability, RIF, & MTTF (λ = 10%)**		
	MTTF (In years)	**Reliability for Mission Time t**	
		t =1 year	**RIF**
Simplex	10	0.9	1
TMR	39	0.9746	3.94
TMR-Simplex	71	0.9860	7.14
Proposed Technique (four Modules)	312	0.9968	31.25
FMR (Five Modules)	135	0.9926	13.5
Modified Triplex-Duplex (Six Modules)	18,182	0.999945	1818.2

Table 7.4

Comparisons of the Second Approach to Commonly used Methods in terms of Reliability, MTTF, and RIF

Methods	Reliability, RIF, & MTTF (λ = 5%)		
	MTTF (In years)	Reliability for Mission Time t	
		t =1 year	RIF
Simplex	20	0.95	1
TMR	145	0.9931	7.25
TMR-Simplex	286	0.9965	14.30
Proposed Technique (Two Modules)	417	0.9976	20.83
Proposed Technique (Three Modules)	10,000	0.9999	500

7.2 FAULT INJECTION TESTS AND RESULTS

A Hardware co-simulation setup was used to test mitigation capabilities of the proposed techniques. There were two experiments designed. In experiment 1, we looked at the effects of injecting the three types of emulated radiation-induced faults (permanent, transient, and bit-flips) in the presence of input disturbances, and in experiment 2, we looked at the effects of injecting the three types of emulated faults in the presence of output (load) disturbances.

To inject emulated radiation-induced faults, synthesizable fault models were placed into the desired places in the VHDL design in both experiments. Appendix A presents schematics for the three-module implementation of the second approach, as well as the four-module version of the first approach with bit-flip fault models added at each controller's outputs.

7.2.1 First Approach Fault Injection Test

In experiment 1, we have initiated an emulated fault injection test on the four-module redundancy technique, injecting a bit-flip fault at each module's outputs to imitate the controller's outputs flipping due to single event effect soft errors.

The simulation interval was set to 6.66 milliseconds, and the input DC-Bus voltage was set to swing between 14 and 14.5 V, with a 2-Ohm output load. Then the following series of events took place:

1) Bit-flip fault at the output of the controller (single event upset fault on the route) for multiple PWM cycles.

    a. At t = 0 ms the simulation is started with the four controller modules outputting the same actual PWM pulse.
    b. At t = 1ms, a bit-flip fault is activated at the first controller module's output.
    c. Starting from t = 1.5ms, the periodic input disturbance is injected and repeated at 1ms intervals of switching between 14V and 14.5V until the simulation ends.
    d. At t = 1.8ms, the bit-flip fault is activated at the second controller module's output, (this brings the number of concurrently failing modules to two).
    e. At t = 2.2 ms, the second module bit-flip fault is deactivated, restoring the module's output.
    f. At t = 2.8ms, the bit-flip fault is activated at the third controller module's output, (this again brings the number of concurrently failing modules to two).
    g. At t = 3.2 ms, the third module bit-flip fault is deactivated, restoring the module's output.
    h. At t = 3.8ms, the bit-flip fault is activated at the fourth controller module's output, (this again brings the number of concurrently failing modules to two).
    i. At t = 4.2 ms, the fourth module bit-flip fault is deactivated, restoring the module's output.
    j. At t = 4.8ms, the bit-flip fault is activated at one of the clone voter's outputs, (this again brings the number of concurrently failing components to two = 1 physical module + clone voter).
    k. At t = 5.2 ms, the first module bit-flip fault is deactivated, restoring the module's output.
    l. At t = 5.8ms, the bit-flip fault is activated at the second clone voter's output, (this again brings the number of concurrently failing components to two = clone voter + clone voter).

m. Starting at t = 6.2 ms, both clone voters are cleared sequentially of bit-flip faults, restoring their correct outputs.

The simulation is repeated for all three types of synthesizable fault models to imitate various fault types.

In experiment 2, the input DC-Bus voltage is fixed at 12V and the output load fixed part is set to 2-Ohms, while the cyclic load current demand switches between 0 and 1A, causing the total load current demand to switch between 2.5A and 3.5A at 1-milisecond intervals beginning 1.5-mili-seconds after the simulation began.

The converter output response for experiment 1 is shown in Figure 7.3, while the converter output response for experiment 2 is shown in Figure 7.4. In the presence of input or output disturbances, the converter tolerates the three radiation-induced fault categories previously discussed, as shown in the Figures. Similar converter responses are seen for various fault models.

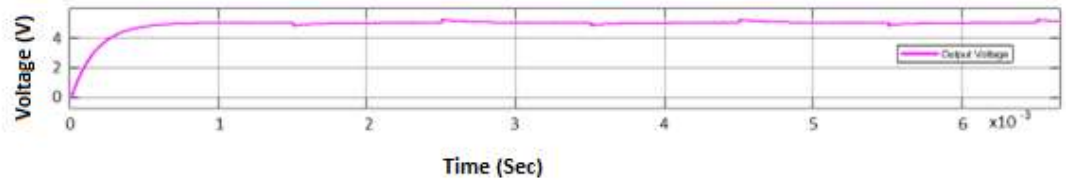


Figure 7.3. Converter output voltage response when input DC-Bus voltage switches between 14V and 14.5V with radiation induced faults sequentially injected (experiment 1).

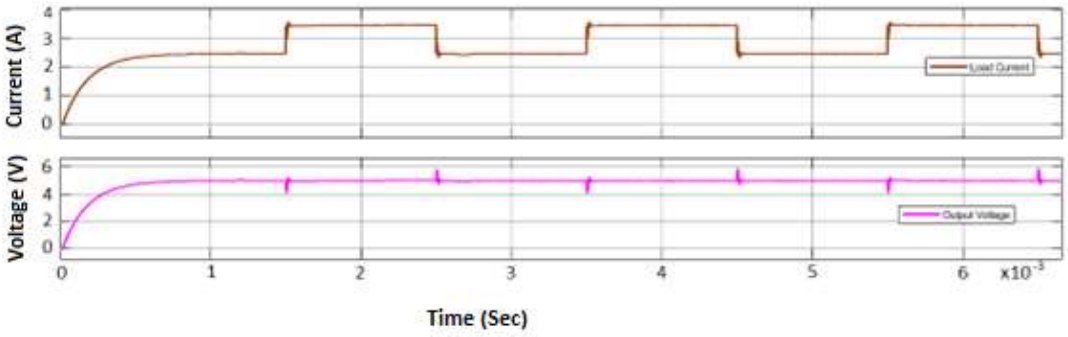


Figure 7.4. Converter output response when output load current switches between 2.5A and 3.5A with radiation induced faults sequentially injected (experiment 2).

7.2.2 Second Approach Fault Injection Tests

In this case, we evaluated the two-modules and three-modules variants of the second approach, and both yielded similar results.

7.2.2.1 Single Fault Masking Potential of the two-modules case

To verify the proposed two-module redundancy approach's single fault masking capability, we set the simulation interval to 2-miliseconds, the input DC-Bus voltage to swing between 144V and 128V at 0.3-milisecond intervals, and the output load to 0.2 ohms. The following series of events is then carried out:

1) Permanent fault (stuck-at 0) for multiple PWM cycles.
    a. At t = 0 ms, the simulation is started with the two controller modules outputting the same actual PWM pulse.
    b. At t = 0.2ms, the stuck-at 0 permanent fault is activated at the first controller module's output.
    c. Starting from t = 0.3ms, the periodic input disturbance is injected and repeated at 0.3ms intervals of switching between 144V and 128V until the simulation ends.
    d. At t = 0.5ms, the first module stuck-at 0 fault is deactivated, restoring the module's output.
    e. At t = 0.7ms, the stuck-at 0 permanent fault is activated at the second controller module's output.
    f. At t = 1ms, the second module stuck-at 0 fault is deactivated, restoring the module's output.

Permanent in this context refers to faulty output from the corresponding modules that persists throughout several PWM cycles. To emulate other fault types, the simulation is repeated for all the three types of synthesizable fault models.

7.2.2.2 Double Fault Masking Potential of the three-modules case

The proposed three-modules redundancy approach's double fault masking capability was verified using the same procedure as the two-modules scenario, with the exception that we tested for stuck-at 1 fault instead of stuck-at 0 for variation. Then the following series of events are executed:

1) Permanent fault (stuck-at 1) for multiple PWM cycles.

1: At t = 0 ms, the simulation is started with the three controller modules outputting the same actual PWM pulse.
2: At t = 0.2ms, the stuck-at 1 permanent fault is activated at the first controller module's output.
3: Starting from t = 0.3ms, the periodic input disturbance is injected and repeated at 0.3ms intervals of switching between 144V and 128V until the simulation ends.
4: At t = 0.5ms, the stuck-at 1 permanent fault is activated at the second controller module's output, (this brings the number of concurrently failing modules to two).
5: At t = 0.7ms, the second module stuck-at 1 fault is deactivated, restoring the module's output.
6: At t = 1ms, the stuck-at 1 permanent fault is activated at the third controller module's output, (this again brings the number of concurrently failing modules to two).
7: At t = 1.3ms, the first module stuck-at 1 fault is deactivated, restoring the module's output.
8: At t = 1.6ms, the stuck-at 1 permanent fault is activated at the second controller module's output, (this again brings the number of concurrently failing modules to two).
9: Finally, both stuck-at 1 fault at the outputs of the second and third modules are deactivated, restoring the modules' outputs.
10: End of simulation.

In experiment 2, the same procedure and simulation interval are used as in experiment 1 above, but the input DC-Bus voltage is fixed at 144V and the output load fixed part is set to 0.8-Ohms, while the cyclic load current demand switches between 0 and 2.5A, causing the total load current demand to switch between 5A and 7.5A at 0.3-mili-second intervals beginning 0.3-mili-seconds after the simulation began.

Figure 7.5 depicts the converter output response for experiment 1 and Figure 7.6 depicts the converter output responses for experiment 2. The converter tolerates the three radiation-induced fault categories previously discussed in the presence of input or output disturbances, as shown in the Figures. For the various fault models, similar converter responses are observed.

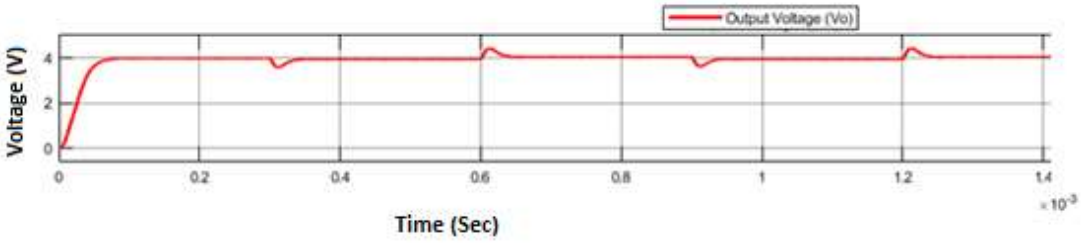


Figure 7.5. Converter output voltage response when input DC-Bus voltage switches between 128V and 144V with radiation induced faults sequentially injected (experiment 1).

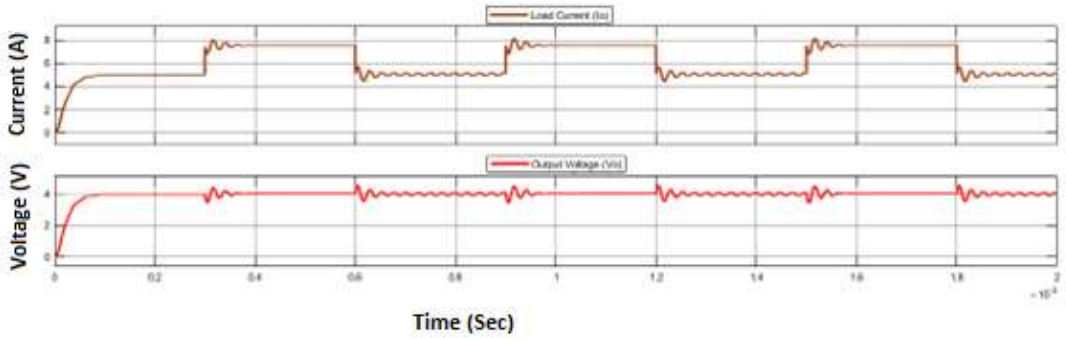


Figure 7.6. Converter output response when output load current switches between 5A and 7.5A with radiation induced faults sequentially injected (experiment 2).

Chapter 8: Conclusions

Radiation-tolerant, low-cost power converters are in significant demand in high-energy physics, in nuclear facilities, and in space applications, due to the rising complexity, functionality, and high reliability requirements of these systems. COTS SRAM-based FPGAs are well-suited for implementing a low-cost digital controller for DC-DC converters used in these applications, but their components are particularly vulnerable to soft errors induced by radiation.

The reliability properties of SRAM-based FPGAs, with a focus on SEE soft errors, were explored in this dissertation. Means of analyzing the dependability of systems implemented on SRAM-based FPGAs were then presented, with an emphasis on fault injection using emulation methodology.

Finally, with an emphasis on the implementation of the digital controller, mitigation methods for user designs implemented in SRAM-based FPGAs are given and validated in fault injection sessions.

8.1 MAIN CONTRIBUTIONS

Single event soft errors can be mitigated using the proposed methods in half-duty limited DC-DC converters and inverters, or similar circuits and/or applications; examples include isolated dual-switch forward and flyback DC-DC Converters.

In the first approach, we have proposed a highly reliable redundancy technique called modified triplex–duplex redundancy, which has a longer expected life than TMR and FMR approaches, though it has the highest hardware resource requirement of the three. It has the capacity to mask concurrent faults in up to four out of six modules. It is a useful solution for implementing radiation-tolerant digital controllers in applications where reliability is critical, such as satellites and spacecraft.

To address the modified triplex–duplex approach's hardware utilization issue, we proposed a unique four-module redundancy methodology derived from the modified triplex–duplex method, which has the following advantages:

- It has higher RIF and MTTF than FMR while requiring less hardware resources.

- It provides higher RIF and MTTF than the TMR technique.
- It has the potential to mask double-faults (two out of four).

We have also presented a very high reliability redundancy technique for radiation tolerant digital controller design in the second approach. The technique's key benefit is that it may be used to parallel any number of redundant modules, whether even or odd, with a significant gain in reliability as the number of paralleled redundant modules increases. Furthermore, even if only one module is free of radiation-induced faults, the technique continues to work. The concept is also an excellent solution for multiple device implementation if the voter and input voltage sensing circuits are placed in a radiation-hardened device, provided that the extra hardware resource is tolerated.

The two-module version of the system utilized slightly fewer LUTs than the TMR method, while the three-module version used slightly more resources but provided much superior reliability, as well as the capacity to mask multiple concurrently occurring faults.

If memory scrubbing techniques are utilized in conjunction with the proposed methods, the potential of the proposed solutions to mask multiple concurrently occurring faults will help to reduce the frequency of such processes. The soft error mitigation capability of the combined system will be very high.

8.2 FUTURE WORK

The fundamental issue for radiation-induced fault protection of user designs implemented in FPGA, is new technology scaling. This allows for more frequent and longer-than-circuit-cycle-time transient pulses to occur, affecting many parts and producing multiple faults in various design modules, rendering most current mitigation measures obsolete.

As a result of this work, strategies for mitigating multiple faults in the FPGA implementation of a digital PWM controller were developed and validated. The recommended solutions, on the other hand, are limited to half-duty limited PWM controllers or DC-DC converters. As a result, one future endeavor could be to broaden the application domain of the techniques by expanding the existing work to encompass the entire duty-value range, from 0 to 100% duty.

Clock trees are less impacted by transient pulses generated by low to moderate energy particles striking because they have numerous distributed nodes and hence a bigger capacitance. However, as technology scaling continues and clock speeds increase, the possibility of a transient fault on the clock path cannot be discounted. As a result, another topic of future research could be the protection of the clock tree from radiation-induced failures. With some modifications, both the first and second recommended solutions can be utilized to protect the distributed clock tree.

Bibliography

[1] Leloglu, U. M., & Kocaoglan, E. (2008). Establishing space industry in developing countries: Opportunities and difficulties. *Advances in Space Research*, 42(11), 1879-1886.

[2] Patel, M. R. (2004). *Spacecraft power systems*. CRC press.

[3] Turriate, V., Witcher, B., Boroyevich, D., & Burgos, R. (2018). Design considerations for a gallium nitride-based phase shifted full bridge DC-DC converter for space applications. In *2018 IEEE 6th Workshop on Wide Bandgap Power Devices and Applications (WiPDA)* (pp. 303-310). IEEE.

[4] Snyder, N. (Ed.). (2012). *Energy conversion for space power* (Vol. 3). Elsevier.

[5] Ray, B. (2002, July). High-reliability space power converters: design and analysis issues. In *IECEC'02. 2002 37th Intersociety Energy Conversion Engineering Conference*, 2002. (pp. 242-247). IEEE.

[6] De Luca, A. (2011). Architectural design criteria for spacecraft solar arrays. In *Solar Cells-Thin-Film Technologies*. IntechOpen.

[7] Barbi, I., & Gules, R. (2003). Isolated DC-DC converters with high-output voltage for TWTA telecommunication satellite applications. *IEEE Transactions on Power Electronics*, 18(4), 975-984.

[8] Zhu, H., Zhang, D., Zhang, B., & Zhou, Z. (2015). A nonisolated three-port DC–DC converter and three-domain control method for PV-battery power systems. *IEEE Transactions on Industrial Electronics*, 62(8), 4937-4947.

[9] LaBel, K. A., Barry, R. K., Castell, K., Kim, H. S., & Seidleck, C. M. (1995). Implications of single event effect characterization of hybrid DC-DC converters and a solid-state power controller. *IEEE Transactions on Nuclear Science*, 42(6), 1957-1963.

[10] Wong, L. K., Leung, F. H. F., Tam, P. K. S., & Chan, K. W. (1997, November). Design of an analog fuzzy logic controller for a PWM boost converter. In *Proceedings of the IECON'97 23rd International Conference on Industrial Electronics, Control, and Instrumentation* (Cat. No. 97CH36066) (Vol. 1, pp. 360-363). IEEE.

[11] Murphy, P., Xie, M., Li, Y., Ferdowsi, M., Patel, N., Fatehi, F., ... & Lee, F. (2002). Study of digital vs analog control. In *Power Electronics Seminar Proceedings (CPES Center for Power Electronics Systems)* (pp. 203-206).

[12] Adell, P. C., Witulski, A. F., Schrimpf, R. D., Baronti, F., Holman, W. T., & Galloway, K. F. (2010). Digital control for radiation-hardened switching converters in space. *IEEE Transactions on Aerospace and Electronic Systems*, 46(2), 761-770.

[13] Skup, K. R., Grudziński, P., Orleański, P., & Nowosielski, W. (2013, August). A digital controller for satellite medium power DC/DC converters. *In 2013 18th International Conference on Methods & Models in Automation & Robotics (MMAR)* (pp. 566-571). IEEE.

[14] Kastensmidt, F. L., Neuberger, G., Carro, L., & Reis, R. (2004, April). Designing and testing fault-tolerant techniques for sram-based fpgas. In *Proceedings of the 1st conference on Computing frontiers* (pp. 419-432).

[15] Lisboa, C. A. L., Schuler, E., & Carro, L. (2005, September). Going beyond TMR for protection against multiple faults. In *2005 18th Symposium on Integrated Circuits and Systems Design* (pp. 80-85). IEEE.

[16] JAYADEVAPPA, D. *Over Coming of Errors in TMR System Utilizing Scanchain Methods*.

[17] Tafazoli, M. (2009). A study of on-orbit spacecraft failures. *Acta Astronautica,* 64(2-3), 195-205.

[18] James, B. F. (1994). *The natural space environment: Effects on spacecraft* (Vol. 1350). National Aeronautics and Space Administration, Marshall Space Flight Center.

[19] Stassinopoulos, E. G., & Raymond, J. P. (1988). The space radiation environment for electronics. *Proceedings of the IEEE*, 76(11), 1423-1442.

[20] Boudenot, J. C. (2007). Radiation space environment. *In Radiation Effects on Embedded Systems* (pp. 1-9). Springer, Dordrecht.

[21] Saganti, P. B., Cucinotta, F. A., Wilson, J. W., Cleghorn, T. F., & Zeitlin, C. J. (2006). Model calculations of the particle spectrum of the galactic cosmic ray (GCR) environment: Assessment with ACE/CRIS and MARIE measurements. *Radiation measurements*, 41(9-10), 1152-1157.

[22] Bourdarie, S., & Xapsos, M. (2008). The near-earth space radiation environment. *IEEE transactions on nuclear science*, 55(4), 1810-1832.

[23] Slaba, T. C., Bahadori, A. A., Reddell, B. D., Singleterry, R. C., Clowdsley, M. S., & Blattnig, S. R. (2017). Optimal shielding thickness for galactic cosmic ray environments. *Life Sciences in space research*, 12, 1-15.

[24] Ryan, J. M., Lockwood, J. A., & Debrunner, H. (2000). Solar energetic particles. *Space Science Reviews*, 93(1), 35-53.

[25] Gusev, A. A., Pugacheva, G. I., Jayanthi, U. B., & Schuch, N. (2003). Modeling of low-altitude quasi-trapped proton fluxes at the equatorial inner magnetosphere. *Brazilian Journal of Physics*, 33(4), 767-774.

[26] Van Allen, J. A. (1958). *Scientific uses of earth satellites*. Рипол Классик.

[27] Gledhill, J. A. (1976). Aeronomic effects of the South Atlantic anomaly. *Reviews of Geophysics*, 14(2), 173-187.

[28] Baumann, R., & Kruckmeyer, K. (2019). *Radiation* handbook for electronics. *Texas Instruments*: Dallas, TX, USA, 117.

[29] Leroy, C., & Rancoita, P. G. (2011). *Principles of radiation interaction in matter and detection*. World Scientific.

[30] Katti, R. R. (2019, July). Radiation-induced errors at elevated linear energy transfer levels and magnetic error rate interactions in magnetic tunnel junctions. In 2019 *IEEE Radiation Effects Data Workshop* (pp. 1-4). IEEE.

[31] Reier, M. (1988). An experimental measurement of the energy loss of californium fission fragments in air—a comparison with calculations. *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms*, 30(4), 503-506.

[32] Gao, D. Z., El-Sayed, A. M., & Shluger, A. L. (2016). A mechanism for Frenkel defect creation in amorphous SiO2 facilitated by electron injection. *Nanotechnology*, 27(50), 505207.

[33] Srour, J. A., & Palko, J. W. (2013). Displacement damage effects in irradiated semiconductor devices. *IEEE Transactions on Nuclear Science*, 60(3), 1740-1766.

[34] Barnaby, H. J. (2006). Total-ionizing-dose effects in modern CMOS technologies. *IEEE Transactions on Nuclear Science*, 53(6), 3103-3121.

[35] Ashton, C. (2016). *Total dose radiation test methodologies for advanced spacecraft electronics experiencing enhanced low dose rate sensitivity*. University of Surrey (United Kingdom).

[36] Oldham, T. R., & McLean, F. B. (2003). Total ionizing dose effects in MOS oxides and devices. *IEEE transactions on nuclear science*, 50(3), 483-499.

[37] Petersen, E. (2011). *Single event effects in aerospace*. John Wiley & Sons.

[38] Melinger, J. S., McMorrow, D., Buchner, S., Knudson, A. R., Tran, L. H., & Campbell, A. B. (1998). Investigations of single-event upsets and charge collection in micro-electronics using variable-length laser-generated charge tracks. *IEEE Transactions on Nuclear Science*, 45(3), 1487-1493.

[39] Faccio, F., Kloukinas, K., Marchioro, A., Calin, T., Cosculluela, J., Nicolaidis, M., & Velazco, R. (1999). Single event effects in static and dynamic registers in a 0.25/spl mu/m CMOS technology. *IEEE Transactions on Nuclear Science*, 46(6), 1434-1439.

[40] Gaillard, R. (2011). Single event effects: Mechanisms and classification. In *Soft errors in modern electronic systems* (pp. 27-54). Springer, Boston, MA.

[41] Schrimpf, R. D., & Fleetwood, D. M. (Eds.). (2004). Radiation effects and soft errors in integrated circuits and electronic devices (Vol. 34). *World Scientific*.

[42] Ferlet-Cavrois, V., Massengill, L. W., & Gouker, P. (2013). Single event transients in digital CMOS—A review. *IEEE Transactions on Nuclear Science*, 60(3), 1767-1790.

[43] Dodd, P. E., Shaneyfelt, M. R., Felix, J. A., & Schwank, J. R. (2004). Production and propagation of single-event transients in high-speed digital logic ICs. *IEEE Transactions on Nuclear Science*, 51(6), 3278-3284.

[44] Benedetto, J. M., Eaton, P. H., Mavis, D. G., Gadlage, M., & Turflinger, T. (2006). Digital single event transient trends with technology node scaling. *IEEE Transactions on Nuclear Science*, 53(6), 3462-3465.

[45] Ferlet-Cavrois, V., Massengill, L. W., & Gouker, P. (2013). Single event transients in digital CMOS—A review. *IEEE Transactions on Nuclear Science*, 60(3), 1767-1790.

[46] Dodd, P. E., & Massengill, L. W. (2003). Basic mechanisms and modelling of single-event upset in digital microelectronics. IEEE Transactions on nuclear Science, 50(3), 583-602.

[47] Campbell, A., McDonald, P., & Ray, K. (1992). Single event upset rates in space. *IEEE Transactions on Nuclear Science*, 39(6), 1828-1835.

[48] Ohlsson, M., Dyreklev, P., Johansson, K., & Alfke, P. (1998, July). Neutron single event upsets in SRAM-based FPGAs. In *1998 IEEE Radiation Effects Data Workshop. NSREC 98. Workshop Record. Held in conjunction with IEEE Nuclear and Space Radiation Effects Conference (Cat. No. 98TH8385)* (pp. 177-180). IEEE.

[49] Radaelli, D., Puchner, H., Wong, S., & Daniel, S. (2005). Investigation of multi-bit upsets in a 150 nm technology SRAM device. *IEEE Transactions on Nuclear Science*, 52(6), 2433-2437.

[50] Maqbool, S. (2006). *A system-level supervisory approach to mitigate single event functional interrupts in data handling architectures*. University of Surrey (United Kingdom).

[51] Smith, G. L., & de la Torre, L. (2006, March). Techniques to enable FPGA based reconfigurable fault tolerant space computing. In *2006 IEEE Aerospace Conference* (pp. 11-pp). IEEE.

[52] Schwank, J. R., Shaneyfelt, M. R., Baggio, J., Dodd, P. E., Felix, J. A., Ferlet-Cavrois, V., ... & Blackmore, E. (2005). Effects of particle energy on proton-induced single-event latchup. *IEEE Transactions on Nuclear Science, 52(6)*, 2622-2629.

[53] Becker, H. N., Miyahira, T. F., & Johnston, A. H. (2002). Latent damage in CMOS devices from single-event latchup. *IEEE transactions on nuclear science, 49(6)*, 3009-3015.

[54] Hohl, J. H., & Galloway, K. F. (1987). Analytical model for single event burnout of power MOSFETs. *IEEE Transactions on Nuclear Science, 34(6)*, 1275-1280.

[55] Sexton, F. W., Fleetwood, D. M., Shaneyfelt, M. R., Dodd, P. E., & Hash, G. L. (1997). Single event gate rupture in thin gate oxides. *IEEE Transactions on Nuclear Science*, *44(6)*, 2345-2352.

[56] Babu, P., & Parthasarathy, E. (2021). Reconfigurable FPGA architectures: a survey and applications. *Journal of The Institution of Engineers (India): Series B*, *102(1)*, 143-156.

[57] Kuon, I., Tessier, R., & Rose, J. (2008). FPGA architecture: Survey and challenges. *Foundations and Trends® in Electronic Design Automation, 2*(2), 135-253.

[58] Herrera-Alzu, I., & Lopez-Vallejo, M. (2014). System design framework and methodology for Xilinx Virtex FPGA configuration scrubbers. *IEEE Transactions on Nuclear Science, 61*(1), 619-629.

[59] Churiwala, S., & Hyderabad, I. (2017). Designing with Xilinx® FPGAs. In *Circuits &Systems. Springer*.

[60] Farooq, U., Marrakchi, Z., & Mehrez, H. (2012). FPGA architectures: An overview. *Tree-based heterogeneous FPGA architectures*, 7-48.

[61] Hwang, J., Milne, B., Shirazi, N., & Stroomer, J. D. (2001, August). System level tools for DSP in FPGAs. In *International Conference on Field Programmable Logic and Applications* (pp. 534-543). Springer, Berlin, Heidelberg.

[62] Adell, P., Allen, G., Swift, G., & McClure, S. (2008, September). Assessing and mitigating radiation effects in Xilinx SRAM FPGAs. In *2008 European Conference on Radiation and Its Effects on Components and Systems* (pp. 418-424). IEEE.

[63] Circuit, A. S. I., Array, F. P. G., Interface, S. P., & Circuit, I. I. Node Architecture.

[64] Wang, Y., Xie, J., Lai, J., & Tong, J. (2008). Design and implementation of the configuration circuit for FDP FPGA. In *APCCAS 2008-2008 IEEE Asia Pacific Conference on Circuits and Systems* (pp. 696-700). IEEE.

[65] Menouni, M., Barbero, M., Bompard, F., Bonacini, S., Fougeron, D., Gaglione, R., ... & Wang, A. (2015). 1-Grad total dose evaluation of 65 nm CMOS technology for the HL-LHC upgrades. *Journal of Instrumentation, 10*(05), C05009.

[66] LaMeres, B. J., Harkness, S., Handley, M., Moholt, P., Julien, C., Kaiser, T., ... & Crum, G. A. (2015). RadSat-Radiation Tolerant SmallSat Computer System.

[67] Amusan, O. A., Witulski, A. F., Massengill, L. W., Bhuva, B. L., Fleming, P. R., Alles, M. L., ... & Schrimpf, R. D. (2006). Charge collection and charge sharing in a 130 nm CMOS technology. *IEEE Transactions on nuclear science, 53(6)*, 3253-3258.

[68] Sterpone, L., & Violante, M. (2005). A new analytical approach to estimate the effects of SEUs in TMR architectures implemented through SRAM-based FPGAs. *IEEE Transactions on Nuclear Science*, 52(6), 2217-2223.

[69] Alfke, P. (2000). Recent progress in field programmable logic.

[70] Sinclair, D., & Dyer, J. (2013). Radiation effects and COTS parts in SmallSats.

[71] Todd, B., & Uznanski, S. (2016). Radiation risks and mitigation in electronic systems. *arXiv preprint arXiv:1607.01573*.

[72] Smith, E. C. (1994). Effects of realistic satellite shielding on SEE rates. *IEEE transactions on nuclear science*, 41(6), 2396-2399.

[73] Dachev, T. P., Tomov, B. T., Matviichuk, Y. N., Dimitrov, P. G., Semkova, J. V., Koleva, R. T., ... & Benghin, V. V. (2020). Solar modulation of the GCR flux and dose rate, observed in space between 1991 and 2019. *Life Sciences in Space Research*, 26, 114-124.

[74] LaMeres, B. J. (2012). FPGA-based radiation tolerant computing. In *Embry-Riddle Aeronautical University Research Colloquium*.

[75] Battezzati, N., Gerardin, S., Manuzzato, A., Merodio, D., Paccagnella, A., Poivey, C., ... & Violante, M. (2009). Methodologies to study frequency-dependent single event effects sensitivity in flash-based FPGAs. *IEEE Transactions on Nuclear Science*, 56(6), 3534-3541.

[76] Munteanu, D., & Autran, J. L. (2008). Modeling and simulation of single-event effects in digital devices and ICs. *IEEE Transactions on Nuclear science*, 55(4), 1854-1878.

[77] Cassano, L., Bosio, A., & Di Natale, G. (2014, May). A novel adaptive fault tolerant flip-flop architecture based on TMR. In *2014 19th IEEE European Test Symposium (ETS)* (pp. 1-2). IEEE.

[78] Lima, F., Carro, L., & Reis, R. (2003, June). Designing fault tolerant systems into SRAM-based FPGAs. In *Proceedings of the 40th annual Design Automation Conference* (pp. 650-655).

[79] Mukherjee, A., & Dhar, A. S. (2014). Double-fault tolerant architecture design for digital adder. In *Proceedings of the 2014 IEEE Students' Technology Symposium* (pp. 154-158). IEEE.

[80] DeVries, R. C. (1979). Fault-Tolerant Techniques for Radiation Environments. *IEEE Transactions on Nuclear Science*, 26(3), 4320-4326.

[81] Bridgford, B., Carmichael, C., & Tseng, C. W. (2008). Single-event upset mitigation selection guide. *Xilinx Application Note, XAPP987 (v1. 0)*, 69.

[82] Adell, P. C., Witulski, A. F., Schrimpf, R. D., Baronti, F., Holman, W. T., & Galloway, K. F. (2010). Digital control for radiation-hardened switching converters in space. *IEEE Transactions on Aerospace and Electronic Systems*, 46(2), 761-770.

[83] Dodd, P. E., Shaneyfelt, M. R., Felix, J. A., & Schwank, J. R. (2004). Production and propagation of single-event transients in high-speed digital logic ICs. *IEEE Transactions on Nuclear Science, 51*(6), 3278-3284.

[84] Sengupta, A., & Kachave, D. (2017). Spatial and temporal redundancy for transient fault-tolerant datapath. *IEEE Transactions on Aerospace and Electronic Systems*, 54(3), 1168-1183.

[85] Garcia, P., Gomes, T., Salgado, F., Cabral, J., Cardoso, P., Ekpanyapong, M., & Tavares, A. (2012). A fault tolerant design methodology for a FPGA-based softcore processor. *IFAC Proceedings Volumes*, 45(4), 145-150.

[86] Frost, C. D., Ansell, S., & Gorini, G. (2009, April). A new dedicated neutron facility for accelerated SEE testing at the ISIS facility. *In 2009 IEEE international reliability physics symposium* (pp. 952-955). IEEE.

[87] Vanát, T., Pospiil, J., Kriek, F., Ferencei, J., & Kubátová, H. (2015, August). A system for radiation testing and physical fault injection into the FPGAs and other electronics. In *2015 Euromicro Conference on Digital System Design* (pp. 205-210). IEEE.

[88] Suhir, E. (2002). Accelerated life testing (ALT) in microelectronics and photonics: its role, attributes, challenges, pitfalls, and interaction with qualification tests. *J. Electron. Packag.*, 124(3), 281-291.

[89] Winokur, P. S., Shaneyfelt, M. R., Heidenheimer, T. L., & Fleetwood, D. M. (1994). Advanced qualification techniques [microelectronics]. *IEEE transactions on nuclear science*, 41(3), 538-548.

[90] Winokur, P. S., Fleetwood, D. M., & Sexton, F. W. (1994). Radiation-hardened microelectronics for space applications. *Radiation Physics and Chemistry*, 43(1-2), 175-190.

[91] Weller, R. A., Mendenhall, M. H., Reed, R. A., Schrimpf, R. D., Warren, K. M., Sierawski, B. D., & Massengill, L. W. (2010). Monte Carlo simulation of single event effects. *IEEE Transactions on Nuclear Science*, 57(4), 1726-1746.

[92] Leveugle, R. (2000, October). Fault injection in VHDL descriptions and emulation. In *Proceedings IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems* (pp. 414-419). IEEE.

[93] Tonfat, J., Kastensmidt, F., & Reis, R. Frame-Level Redundancy Scrubbing Technique for SRAM-Based FPGAs.

[94] Grinschgl, J., Krieg, A., Steger, C., Weiss, R., Bock, H., & Haid, J. (2011, June). Automatic saboteur placement for emulation-based multi-bit fault injection. In *6th International Workshop on Reconfigurable Communication-Centric Systems-on-Chip (ReCoSoC)* (pp. 1-8). IEEE.

[95] Sterpone, L., & Du, B. (2014, May). Analysis and mitigation of single event effects on flash-based FPGAs. In *2014 19th IEEE European Test Symposium (ETS)* (pp. 1-6). IEEE.

[96] Geist, R., & Trivedi, K. S. (1990). Reliability estimation of fault-tolerant systems: Tools and techniques. *Computer*, 23(7), 52-61.

[97] Na, J., & Lee, D. (2013, September). A study on the reliability improvement factor of fault tolerant mechanisms. In *Safecomp 2013 FastAbstract* (p. NC).

[98] Liu, L. J., Kuo, Y. C., & Cheng, W. C. (2009, December). Analog PWM and Digital PWM Controller IC for DC/DC Converters. In *2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC)* (pp. 904-907). IEEE.

[99] Adell, P. C., Schrimpf, R. D., Choi, B. K., Holman, W. T., Attwood, J. P., Cirba, C. R., & Galloway, K. F. (2002). Total-dose and single-event effects in switching DC/DC power converters. *IEEE Transactions on Nuclear Science*, 49(6), 3217-3221.

[100] Ren, Y., Chen, L., Shi, S. T., Guo, G., Feng, R. F., Wen, S. J., ... & Bhuva, B. L. (2013, April). Single-event transient measurement on a DC/DC PWM controller using Pulsed X-ray technique. In *2013 IEEE International Reliability Physics Symposium (IRPS)* (pp. SE-3). IEEE.

[101] Schwank, J. R., Shaneyfelt, M. R., & Dodd, P. E. (2013). Radiation hardness assurance testing of microelectronic devices and integrated circuits: Test guideline for proton and heavy ion single-event effects. *IEEE Transactions on Nuclear Science*, 60(3), 2101-2118.

[102] Likar, J. J., Katz, S. L., & Sulyma, R. M. (2019, July). Heavy ion Single Event Effects (SEE) results for PWM5032 Pulse Width Modulator Controller. In *2019 IEEE Radiation Effects Data Workshop* (pp. 1-7). IEEE.

[103] Howard, J. W., Carts, M. A., LaBel, K. A., Forney, J. D., & Irwin, T. L. (2003, July). Single event effects testing of the Linfinity SG1525A pulse width modulator controller. In *2003 IEEE Radiation Effects Data Workshop* (pp. 133-140). IEEE.

[104] Jain, M., & Gupta, R. (2011). Redundancy issues in software and hardware systems: an overview. *International Journal of Reliability, Quality and Safety Engineering*, 18(01), 61-98.

[105] Soltani, H., Dolatshahi, M., & Sadeghi, M. (2016, December). Comparing the reliability in systems with triple and five modular redundancy. In *2016 5th International Conference on Computer Science and Network Technology (ICCSNT)* (pp. 437-442). IEEE.

[106] Choudhury, S. (2007). Designing the digital compensator for a UCD91XX-based Digital power supply. *Texas Instruments*, 184, 5-2.

[107] Cai, S., Pi, C., Yan, W., & Li, W. (2011). A low noise high efficiency buck DC-DC converter with sigma—delta modulation. *Journal of semiconductors*, 32(7), 075004.

[108] Uchagaonkar, P. A., Shinde, S. A., Patil, V. V., & Kamat, R. K. (2012). FPGA based sigma–Delta analogue to digital converter design. *International Journal of Electronics and Computer Science Engineering*, 1(2), 508-513.

[109] Ghasemi Shahabi, A., & Lotfivand, N. (2016). Design and FPGA Implementation of Sigma Delta ADC on Spartan 6.

[110] Uchagaonkar, P. A., Shinde, S. A., Patil, V. V., & Kamat, R. K. (2012). FPGA based sigma–Delta analogue to digital converter design. International Journal of Electronics and Computer Science Engineering, 1(2), 508-513.

[111] URL: http://www.latticesemi.com/~/media/LatticeSemi/Documents/ReferenceDesigns/SZ/SimpleSigmaDeltaADCDocumentation.pdf?document_id=35762

[112] Wei, G. Y., & Horowitz, M. (1996, August). A low power switching power supply for self-clocked systems. In *Proceedings of 1996 International Symposium on Low Power Electronics and Design* (pp. 313-317). IEEE.

[113] Rudrakshi, S., Midasala, V., & Bhavanam, S. N. (2012). Implementation of FPGA based fault injection Tool (FITO) for testing fault tolerant designs. International Journal of Engineering and Technology, 4(5), 522.

[114] URL: https://www.sunnewsonline.com/jaguar-l-rover-teaches-teenagers-to-write-code-for-a-self-driving-future/. accessed on Nov. 26 2022.

[115] Paiz, C., Kettelhoit, B., & Porrmann, M. (2007, May). A design framework for FPGA-based dynamically reconfigurable digital controllers. In *2007 IEEE International Symposium on Circuits and Systems* (pp. 3708-3711). IEEE.

[116] URL: https://au.mathworks.com/videos/adopting-model-based-design-for-fpga-asic-and-soc-development-1559811099219.html. accessed on Sep. 5 2022.

Appendices

Appendix A

After-synthesis schematics.

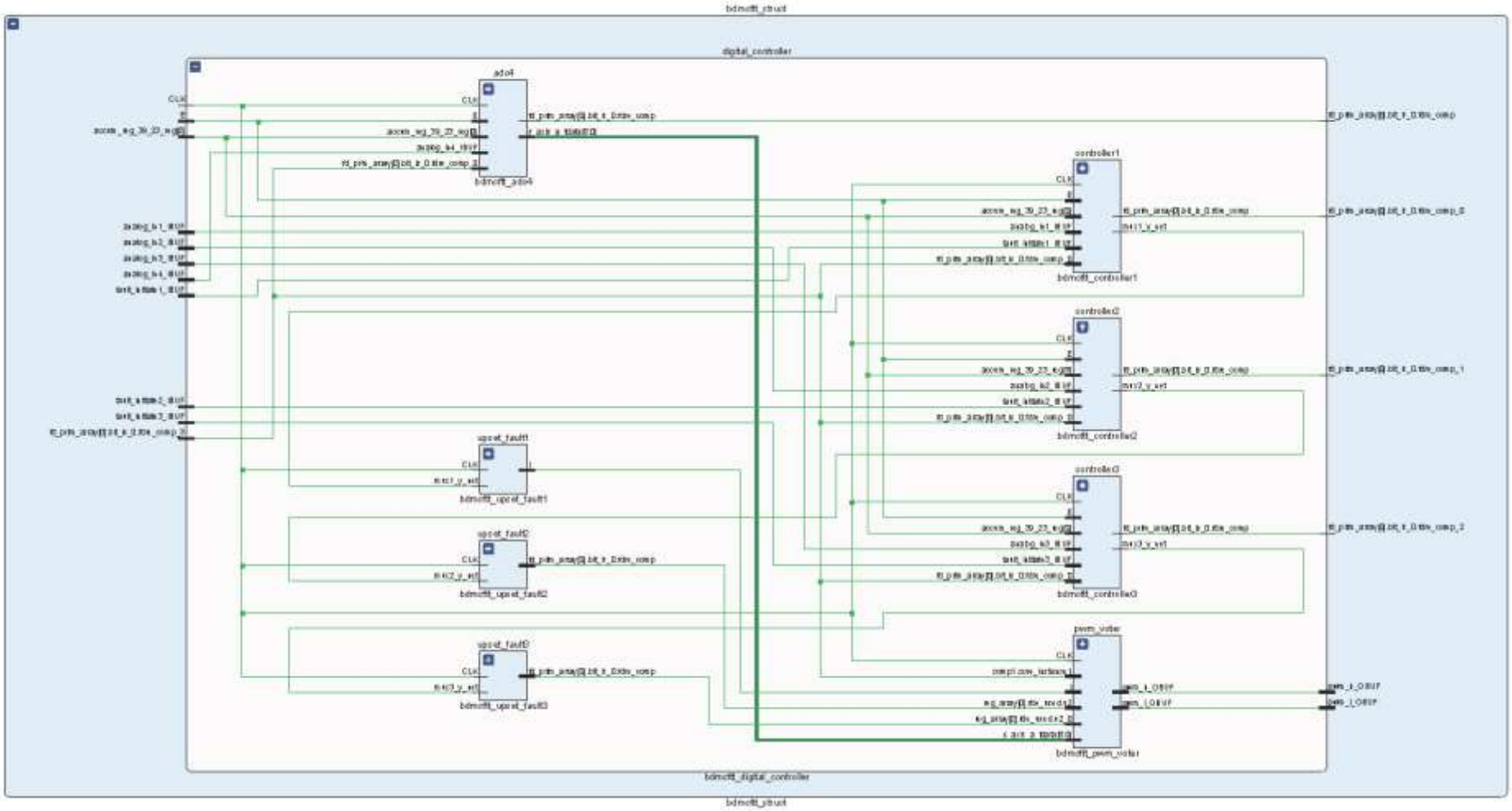


Figure A.1. Bit-flip synthesizable fault model insertion sites in a three-module second approach implementation.

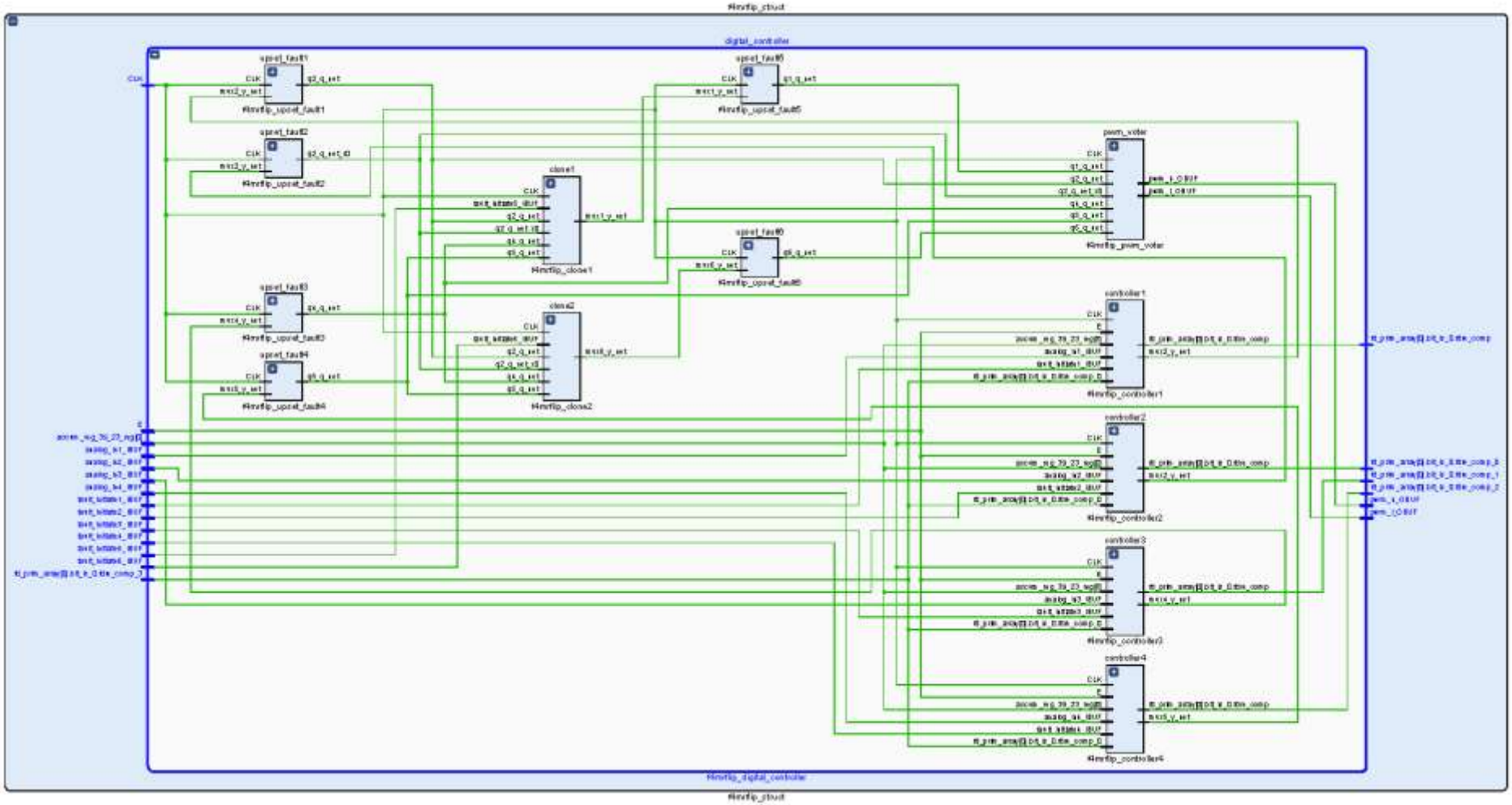


Figure A.2. Bit-flip synthesizable fault model insertion sites in a four-module first approach implementation.

Appendix B

Modified triplex-duplex redundancy algorithm

STATIC_DETECT_OUT1 = w , STATIC_DETECT_OUT2 = x,
STATIC_DETECT_OUT3 = y , STATIC_DETECT_OUT4 = r,
STATIC_DETECT_OUT5 = t , STATIC_DETECT_OUT6 = m ,
MAX_DUTY_PWM_PULSE = q;

1: **Input:** w, x, y, r, t, m, q

2: **If** $\left({}^{6}C_{6}\right)$ (w, x, y, r, t, m) ➔ 1 combination)

3: Output: any one of (w, x, y, r, t, m)

4: **Else If** $\left({}^{6}C_{5}\right)$ (w, x, y, r, t, m) ➔ 6 combinations)

5: **Output:** any one of the majorities of 5

6: **Else If** $\left({}^{6}C_{4}\right)$ (w, x, y, r, t, m) with each equal to 1 and q = 1 ➔ 15 combinations)

7: **Output:** any one of the majorities of 4

8: **Else If** $\left({}^{6}C_{3}\right)$ (w, x, y, r, t, m) with each equal to 1 and q = 1 ➔ 20 combinations)

9: **Output:** any one of the combinations of 3

10: **Else If** $\left({}^{6}C_{2}\right)$ (w, x, y, r, t, m) with each equal to 1 and q = 1 ➔ 15 combinations)

11: **Output:** any one of the combinations of 2

12: Else

13: Output: 0

14: **End If**

Where:

$$ {}_nC_r = \frac{n!}{r!(n-r)!} $$

${}_nC_r$ = number of possible combinations

n = total number of duplicated modules

r = number of choosing modules from total modules

Appendix C

VHDL codes

Included in the accompanying Compact Disc (CD-ROM).