2011-02-07

On-Orbit FPGA SEU Mitigation and Measurement Experiments on the Cibola Flight Experiment Satellite

William A. Howes
Brigham Young University - Provo

On-Orbit FPGA SEU Mitigation and Measurement Experiments

on the Cibola Flight Experiment Satellite

William Albert Howes

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Michael J. Wirthlin, Chair
Brent E. Nelson
David A. Penry

Department of Electrical and Computer Engineering

Brigham Young University

April 2011

ABSTRACT

On-Orbit FPGA SEU Mitigation and Measurement Experiments

on the Cibola Flight Experiment Satellite

William Albert Howes

Department of Electrical and Computer Engineering

Master of Science

This work presents on-orbit experiments conducted to validate SEU mitigation and detection techniques on FPGA devices and to measure SEU rates in FPGAs and SDRAM. These experiments were designed for the Cibola Flight Experiment Satellite (CFESat), which is an operational technology pathfinder satellite built around 9 Xilinx Virtex FPGAs and developed at Los Alamos National Laboratory. The on-orbit validation experiments described in this work have operated for over four thousand FPGA device days and have validated a variety of SEU mitigation and detection techniques including triple modular redundancy, duplication with compare, reduced precision redundancy, and SDRAM and FPGA block memory scrubbing. Regional SEU rates and the change in CFE's SEU rate over time show the measurable, expected effects of the South Atlantic Anomaly and the cycle of solar activity on CFE's SEU rates. The results of the on-orbit experiments developed for this work demonstrate that FPGA devices can be used to provide reliable, high-performance processing to space applications when proper SEU mitigation strategies are applied to the designs implemented on the FPGAs.

Keywords: FPGA, SDRAM, reliability, space-based computing, SEU mitigation, SEU rate prediction and measurement

ACKNOWLEDGMENTS

I am grateful for the opportunity to express appreciation to the many who have provided help and inspiration to me as I have completed this thesis. I am especially appreciative of the help of my advisor, Dr. Michael Wirthlin. This work would not be possible without his support, and my development as a writer and an engineer has been enhanced immeasurably by his influence. I am also grateful for the other members of my graduate committee, Dr. Brent Nelson and Dr. David Penry, who have been sources of support, knowledge, and positive influence as I have progressed in my education.

I am particularly grateful for the expertise and patience of those at Los Alamos National Laboratory who have made this work possible. I would particularly like to thank Michael Caffrey for his patience and mentorship, as well as Diane Roussel-Dupré, Tony Salazar, Keith Morgan, Joseph Palmer, Paul Graham, Heather Quinn, Tony Nelson, Aaron Morrison, and all of the members of the CFE team at LANL. The opportunity that I have had to work with an operational satellite as an undergraduate and graduate student has been a remarkable one, and it was made possible by the hard work and dedication of all those who have worked on the CFE project.

I am also grateful to the students in the BYU Configurable Computing Lab, particularly Daniel Richins, Jonathan Johnson, and Brian Pratt, who made significant contributions to this thesis by developing major portions of the FPGA designs tested in this work.

Finally, I thank my family for the inspiration and support that they have given me. My wife, Ashley, has been my greatest support and cheerleader as I have written this thesis, and I am especially grateful for her love, patience, and encouragement.

This work was supported by Los Alamos National Laboratory and Sandia National Laboratories with sponsorship by the DOE NNSA Office of Nonproliferation Research and Development (NA-22), as well as by the I/UCRC Program of the National Science Foundation under Grant No. 0801876.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

Satellites and other space-based systems are often used for complex applications, such as radar, imaging, and weather studies, which require the processing of large quantities of sensor data. In many currently operating space-based systems, sensor data is collected, stored, and then transmitted to the ground for processing. However, the data transmission links between space systems and ground stations often have very limited bandwidth, which limits the rate at which the data can be collected, stored, and processed. Much of the data transmission required for space applications can be eliminated if suitable processing hardware can be located in the space-based system itself. Many research efforts have focused on improving the ability of space-based systems to provide onboard high performance data processing capabilities to compute-intensive applications [1, 2, 3].

SRAM-based field-programmable gate arrays (FPGAs) are attractive candidates for use in these compute-intensive applications in space. The designer of an FPGA-based system has the ability to specify the configuration of the digital logic hardware within the FPGA, which can lead to increased performance over a microprocessor in many streaming signal processing or communications systems common to space applications. In some applications, a performance improvement of two orders of magnitude over a processor-based implementation can be achieved with an FPGA-based implementation [4]. SRAM FPGAs are also reconfigurable, meaning that a single FPGA device can be programmed to implement many different computing applications and can even be reconfigured in the field to provide new or improved functionality to the system. In addition, FPGAs are commercially available products that are much less expensive than application-specific alternatives.

Although FPGAs can be very useful in satellites and other space applications, the nature of the harsh environments of space makes using FPGAs in these environments more difficult. In particular, SRAM FPGAs are susceptible to errors caused by the radiation

often present in space. An FPGA's SRAM memory cells can be struck by high-energy particles which cause an unintended change in the state of the memory, a phenomenon known as a single event upset (SEU). SEUs in an FPGA's configuration memory can cause an unexpected change in the circuit's behavior since the FPGA's behavior is determined by the configuration bits. In addition, the memory used to store circuit state data, such as flip-flops and block memories, is also stored in the device's SRAM and is susceptible to SEUs, which can lead to unexpected changes in circuit state. If upsets to an FPGA's SRAM bits are not properly handled, the outputs of the application implemented on the FPGA may be incorrect or unreliable, or the application may be rendered inoperable.

Because of the risk of SEUs causing incorrect operation in space-based systems utilizing FPGAs, any space-based application which relies on SRAM FPGAs should have a well-validated strategy in place to mitigate against the effects of SEUs. A variety of techniques have been proposed to handle SEUs that occur in the FPGA configuration memory and user memory elements. These techniques include memory scrubbing, triple modular redundancy (TMR), duplication with compare (DWC), and reduced precision redundancy (RPR). These techniques rely on redundancy in the system to mask, detect and report, or correct any errors that occur within the circuit's digital logic or memories. SEU mitigation and detection techniques have been tested extensively with ground-based approaches such as fault simulation, fault injection, and particle accelerator testing, and the techniques under test have been shown to successfully handle SEUs that occur within FPGA-based designs [5, 6, 7, 8].

Several space-based systems have included FPGAs protected with SEU mitigation techniques; these systems demonstrate the advantages of using properly mitigated FPGA designs in space applications. The Australian science satellite FedSat, launched in 2002, was the first space mission to use a radiation-tolerant SRAM FPGA for reconfigurable computing [9, 10]. The NASA Mars Exploration Rovers, Spirit and Opportunity, landed on Mars in 2004 and used SRAM FPGAs to control pyrotechnic operations during descent and landing, as well as to oversee motors for the systems' wheels, steering, arms and cameras [11]. The successful use of FPGAs in these rovers led to the use of SRAM FPGAs in other NASA Mars missions such as the Mars Reconnaissance Orbiter, which reached Martian orbit in March

2006 [12], and Mars Science Lab, which is scheduled for launch in November 2011 [13]. The European Space Agency's Venus Express satellite uses a Xilinx Virtex SRAM FPGA in its Venus Express Monitoring Camera (VMC) to implement a microprocessor as well as peripheral logic and interfaces to various sensors and communication units [14].

Several SRAM FPGA-based applications have also been used on the Space Shuttle and on the International Space Station (ISS) in the Materials on the International Space Station Experiment (MISSE). The NASA SpaceCube computer uses SRAM FPGAs to implement a reconfigurable high-performance computer suitable for use in space applications, and it has been tested on a Hubble Space Telescope servicing mission of the Space Shuttle Atlantis [15, 16]. The FPGA-related applications used in the MISSE series of experiments are designed to validate the use of properly-mitigated FPGA designs in orbit. The seventh of these experiments, MISSE-7, included the FPGA-based SEUXSE experiment [17] as well a SpaceCube experiment. The latest iteration of the MISSE series of experiments, MISSE-8, includes updated versions of the FPGA-based MISSE experiments and is scheduled for future deployment to the ISS.

The Cibola Flight Experiment Satellite (CFESat), which was developed at Los Alamos National Laboratory and funded by the United States Department of Energy/NNSA/NA-22, was also among the earliest space-based systems to use SRAM-based FPGAs. An artist's depiction of CFESat in orbit is shown in Figure 1.1. CFE is a technology pathfinder mission, meaning that one of its major purposes is to validate a variety of new technologies as suitable for use in space. As part of its role as a technology pathfinder, a main objective of CFE is to validate SRAM FPGAs as suitable for high performance on-orbit processing [4]. CFE uses the reconfigurability of its payload FPGAs to provide a platform for on-orbit mitigation technique validation and SEU rate measurement studies. The reconfigurable nature of the CFE payload and its ability and availability to perform on-orbit SEU studies make it a suitable platform for measuring SEU rates and testing SEU mitigation and detection techniques. As such, since its launch in March 2007, CFE has been used to carry out a variety of different experiments relating to the effects of SEUs on its payload FPGAs.

The earliest SEU detection and correction experiments on CFE used the satellite's built-in, system level FPGA SEU scrubbing circuit to detect and report any SEUs in the

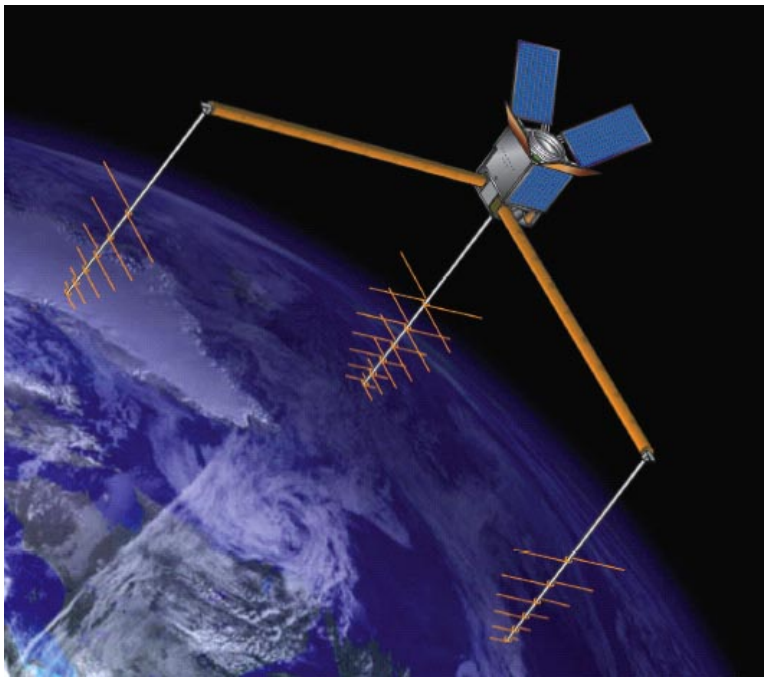

Figure 1.1: Artist's depiction of CFESat in orbit

FPGA configuration memory. These experiments allowed for a measurement of the satellite's FPGA configuration SEU rate, but they did not allow for the validation of in-circuit FPGA SEU mitigation techniques such as DWC, RPR, and FPGA block memory scrubbing. In addition, the early SEU experiments on CFE did not allow for the detection of SEUs within the satellite's payload SDRAM or for the validation of SDRAM SEU mitigation or detection techniques. This work uses the reconfigurable, in-orbit platform provided by CFE to expand the satellite's ability to perform SEU-related experiments.

1.1 Thesis Contributions

The main contribution of this work is the development and successful on-orbit operation of six CFE payload applications which validate in-circuit SEU mitigation and detection techniques and measure FPGA and SDRAM SEU rates. The experiments conducted in this work demonstrate that FPGA devices can be used to provide reliable, high-performance processing to space applications when proper SEU mitigation strategies are applied to the designs implemented on the FPGAs. The test results and analysis described in this work pro-

vide an important contribution to the overall effort of validating properly mitigated FPGA-based applications as suitable for use in space environments since they are based on the operations of a real, orbiting satellite.

The mitigation and detection validation applications created for this work have tested a variety of SEU mitigation and detection approaches, including TMR, RPR, DWC, and memory scrubbing techniques for FPGA block RAM (BRAM) and SDRAM. Several of the SEU mitigation strategies tested are designed to provide various levels of mitigation quality for corresponding levels of area cost. The SEU mitigation and detection validation experiments created for this work have operated on CFE for over four thousand FPGA device days, and all of the techniques tested have been observed to work correctly during their entire time of operation. Many occasions have been recorded during the experiments' deployment in which an SEU was detected and the mitigation or detection technique under test handled the SEU as expected, preventing the SEU from causing the circuitry implemented on the FPGA to produce incorrect results.

The SEU-related CFE applications created in this work also facilitate the detection of SEUs occurring in BRAM internal to the FPGAs and in SDRAM external to each payload FPGA. These applications, along with the CFE payload's built-in SEU detection capabilities, have allowed for measurement and analysis of the FPGA and SDRAM SEU rates seen on CFE. CFE's built-in, configuration scrubbing-based SEU detection and correction system has operated in orbit for over six thousand FPGA device days, enabling the collection of a significant amount of data that has allowed for detailed analysis of the configuration SEU rate on CFE. This work presents a comparison of SEU rate predictions made using the CREME96 orbit modeling tool with measured SEU rates, and the comparison shows that FPGA and SDRAM SEU rate predictions match reasonably well with measured rates when the limitations of the tools, models, and methodology used for creating the rate predictions are considered. In addition, analysis of regional SEU rates and the change in SEU rate over time shows the measurable, expected effects of the South Atlantic Anomaly and the cycle of solar activity on CFE's SEU rates.

1.2 Thesis Organization

The remainder of this thesis will provide background necessary to understanding the on-orbit SEU mitigation and rate measurement experiments created in this work, describe the hardware and software developed to carry out these experiments, and present the results of the experiments. The thesis is organized as follows: Chapter 2 gives a brief summary of background information relating to the space radiation environment, radiation effects on electronic devices, and the CFE satellite. Chapter 3 presents an overview of all of the SEU mitigation and detection technique experiments conducted on CFE along with their results. Chapter 4 presents and analyzes the SEU rate data collected by CFE's FPGA configuration scrubbing and by the BRAM and SDRAM scrubbing circuitry developed in this work. Chapter 5 concludes the thesis.

In addition, three appendices are included in this thesis to provide a more thorough treatment of background material as well as to present supplementary information about the CFE applications used to validate SEU mitigation techniques and to measure SEU rates. Appendix A describes space radiation effects on FPGAs and SDRAM, how those effects are estimated using orbit modeling tools and ground-based testing techniques, and how on-orbit testing can support and build upon SEU rate estimations and ground-based tests. Appendix B describes the details of CFE's architecture and operations that are relevant to the SEU mitigation and detection experiments developed in this work. Appendix C describes the design and operations of the seven different SEU-related applications that have operated on CFE. The six latest applications, SEU2-SEU7, were developed as part of this work.

CHAPTER 2. BACKGROUND

This chapter presents a short summary of background material relevant to the SEU mitigation and measurement applications and SEU rate analysis presented in this work. As the chapter provides only a brief introduction to a variety of topics, some readers may desire a more in-depth treatment of the material presented here. Those readers are directed to the first two appendices of this thesis for a more detailed discussion of the topics presented in this chapter.

The first section of this chapter will discuss the nature of the space radiation environment and its effects on spacecraft electronics. This discussion will highlight the effects of radiation on FPGAs and SDRAM since the experiments developed as part of this work are designed to detect and correct SEUs in these devices. The last section of this chapter will briefly describe details of the CFE payload that are necessary to understanding the architecture and on-orbit results of the experiments that will be discussed in Chapter 3.

2.1 Space Radiation Environment and Effects

One of the main hazards faced by any spacecraft is the effect of high energy radiation on its electronic components. Radiation can induce unwanted temporary or permanent effects in a spacecraft's electronic devices, and in many cases, these effects can cause the devices to operate incorrectly. Radiation that is capable of causing incorrect device operation or device damage can originate from several different sources, including belts of trapped radiation around the earth, cosmic rays emanating from the sun, or cosmic rays originating from outside the solar system. This radiation may consist of electrons, protons, neutrons, alpha particles, or heavy ions, and its composition and energy level is generally dependent on its place of origin.

The volume and intensity of solar radiation are roughly periodic, varying in an approximately eleven-year-long solar cycle. These cycles correspond roughly to the number of sunspots present on the sun and the latitude of the belt in which the sunspots appear [18]. During the portion of the cycle known as solar minimum, considered to be the first half of the cycle, the frequency and intensity of solar particle events are low, while during the second half of the cycle (solar maximum), the solar particle events are more intense and frequent.

One region of the near-earth space environment that is of particular interest in this work is the South Atlantic Anomaly (SAA), shown in Figure 2.1. The SAA is the area where the earth's inner radiation belt passes closest to the planet's surface. This radiation belt consists mainly of high-energy protons, which can induce damage or processing errors in electronic devices. Because the SAA is at a lower altitude than the rest of the inner radiation belt, it can be particularly troublesome to spacecraft like CFE that operate in low-earth orbits. The Hubble Space Telescope, for example, does not make observations when in the SAA [19]. Most upsets in electronic devices that occur in low-earth orbits occur in the SAA, and since the inner radiation belt consists mainly of protons, these upsets are mainly proton-induced [20].

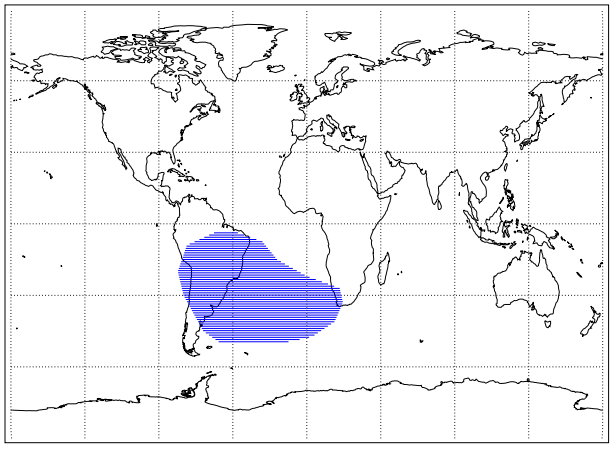

Figure 2.1: The South Atlantic Anomaly

The effects of radiation on electronic devices, including the FPGAs and SDRAM used on CFE, can be either permanent or repairable. Permanent device damage can be induced

by either the cumulative effects of radiation over time (total radiation dose) or the effect of a single particle event (such as single event latchup). The CFE experiments developed for this work, however, are mainly concerned with measuring and mitigating against the effects of SEUs, which are repairable events. SEUs arise when charge deposited by radiation causes a change of state in a circuit memory element [21]. Although SEUs do not cause permanent damage to FPGAs or SDRAM, they may cause the devices to have incorrect state.

In FPGAs, SEUs can lead to unreliable device operation by changing user state values in block memories and flip-flops or by changing values stored in the FPGA's configuration memory. Upsets to FPGA configuration memory require particular attention since the configuration memory controls the behavior of the configurable logic elements of the FPGA such as lookup tables (LUTs) and configurable routing resources. To ensure that incorrect state values caused by SEUs in FPGAs do not cause spacecraft electronics to output incorrect results, a strategy consisting of one or more SEU mitigation or detection techniques should be developed and implemented for any space-based system using SRAM FPGAs. Several different FPGA SEU mitigation and detection techniques were tested on CFE as part of this work; the techniques and their associated CFE experiments will be described in Chapter 3.

Architectural differences between FPGAs and SDRAM make the mechanisms and effects of SEUs in SDRAM somewhat different from those of SRAM FPGAs. SDRAM uses a capacitor to store its data value, which means that SDRAM memory cells need not suffer a complete "bit flip" to suffer from erroneous values in the memory; rather, the degradation of the stored charge to a level outside of the noise margin of support circuitry is sufficient to cause an error [22]. In addition, SDRAM cells are quite small, consisting of a single MOS transistor and a capacitor, as opposed to a traditional six-transistor SRAM cell used in typical FPGAs. This means that SDRAM can be more densely packed together, which leads to lower sensitivity per bit than might be expected [22], though this density also means that SDRAM can be more vulnerable to multi-bit upsets (MBUs) than an FPGA produced in a process of similar size [23]. Finally, SDRAM SEUs do not usually affect the behavior of the device itself since most of its SEU vulnerable area is dedicated to user data storage. A technique to detect and correct SEUs that occur in SDRAM user data was implemented

and tested on CFE as part of this work; the technique and its CFE test will be described in Chapter 3.

Some FPGA and SDRAM SEU mitigation techniques, including configuration and user memory scrubbing, rely on assumptions about the rate at which SEUs will occur to determine how quickly errors within the memory need to be corrected. For this reason, it is important that the anticipated SEU rate in the spacecraft's operating environment be taken into account during the development of a SEU management strategy. Software programs are available to help in estimating the SEU rate for a given electronic device in specific orbit environments. These programs use the results of particle accelerator tests on the devices bound for space and a specification of orbit parameters to provide a general estimate of the SEU rate that can be expected. On CFE, the CREME96 program [24] was used before launch to estimate the SEU rate of the device FPGAs in a variety of space weather conditions. These predictions will be presented and compared with CFE SEU rates actually measured in orbit in Chapter 4.

More information regarding the space radiation environment, radiation effects on FPGAs and SDRAM, and SEU rate prediction is presented in Appendix A.

2.2 The Cibola Flight Experiment

The Cibola Flight Experiment satellite (CFESat) was launched in March 2007 and has operated successfully from its launch until the time of writing. Nine space-qualified Xilinx SRAM FPGAs are used in the payload to provide high-performance processing capabilities. These FPGAs are easily reconfigured, and FPGA configuration files and software binaries for a new or updated payload application can be uploaded to the spacecraft and stored in the payload's non-volatile memories. Since its launch, CFE has received configuration data from the ground dozens of times, approximately once every 1-2 months on average [25].

The CFE payload is controlled by a radiation-hardened BAE RAD6000 microprocessor [26] which operates at 30 MHz and runs the VxWorks operating system. The bulk of the payload's data processing ability, however, is provided by three reconfigurable computing modules (RCCs). A block diagram of an RCC module is shown in Figure 2.2. Each RCC module contains three space-qualified Xilinx Virtex XQVR1000-CG560 FPGAs [27] with

SDRAM local to each device. A radiation-hardened Actel RT54SX32S antifuse FPGA [28] is also included in each RCC to perform FPGA configuration, correct any configuration SEUs that occur in the Xilinx devices, and provide the interface between the Xilinx devices and the microprocessor.

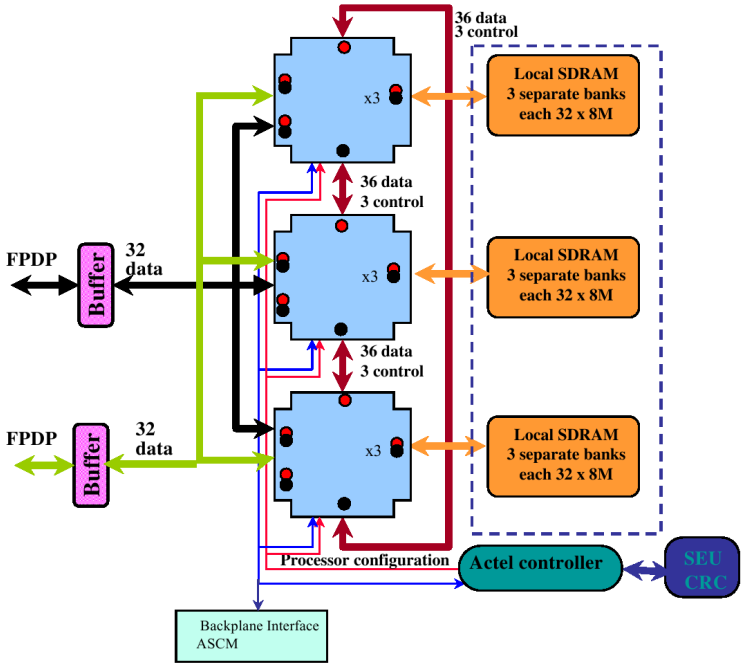

Figure 2.2: Block diagram of a CFE reconfigurable computer module (RCC)

The Xilinx FPGAs used in the payload RCC modules are radiation tolerant, which means that they are protected against total dose effects and latchup but still vulnerable to the effects of SEUs. In order to correct any SEUs that occur in those FPGAs, a configuration memory error detection and correction system using cyclic-redundancy checks (CRC) was built into the payload [29]. The antifuse Actel FPGA in each RCC unit uses configuration readback on the three Virtex devices to calculate the CRC of each frame, which is the smallest amount of configuration data that can be read back and reconfigured independently in a Virtex device. The calculated CRC value is then compared with a pre-calculated CRC stored in a codebook. A CRC mismatch indicates an upset in the configuration memory, and the Actel responds to this event by interrupting the RAD6000 microprocessor, which

then reconfigures the upset frame. The three Virtex FPGAs on a CFE RCC are scrubbed one at a time, and a scrubbing cycle through all of the FPGAs takes 180 milliseconds.

The CRC-based readback and reconfiguration technique for detecting and correcting SEUs is a major component of CFE's payload SEU management strategy. Since this strategy is enabled for a large percentage of the time that the payload is operational, it allows for a detailed and reliable measurement of FPGA configuration SEUs that occur in orbit. However, some errors in an FPGA circuit's state or outputs may affect the correct functionality of a design even after the SEU has been corrected by readback [30]. For this reason, many CFE applications use logic-level SEU mitigation techniques to allow for uninterrupted correct design operation. Several logic-level SEU mitigation techniques that were validated as part of this work will be described in Chapter 3.

Because of its reconfigurability, the CFE payload provides a powerful and flexible platform for a variety of applications, including software defined radios, decoders, demodulators, and FFT engines [29], as well as for all of the SEU measurement and mitigation experiments conducted in this work. The process of developing and deploying an application for CFE begins with the development, debugging, and integration of FPGA designs, software for the payload's RAD6000 processor, and ground station software. Once these components of the application are complete, the application's power consumption is measured and recorded. The application can then be uploaded to the spacecraft and scheduled to operate. A more thorough discussion of the application development and scheduling process can be found in Section B.3.5.

Appendix B contains a more detailed description of the CFE satellite and payload. In addition, several publications [4, 29, 31, 32] discuss the details of the satellite and its mission to date.

2.3 Conclusion

This chapter briefly described the nature of the near-earth space radiation environment, the effects of space radiation on FPGAs and SDRAM, and the key features of the CFE payload that enable the SEU measurement and mitigation experiments conducted in this work. Because the experiments presented in this work are implemented on an opera-

tional, orbiting satellite, they provide a real-world example of SEU mitigation and detection techniques preventing FPGA-based systems from experiencing radiation-induced failures. The next two chapters of this thesis will describe the architecture of these experiments, the SEU mitigation and techniques that they test, and the on-orbit results of the experiments.

CHAPTER 3. SEU DETECTION AND MITIGATION EXPERIMENTS ON CFE

Since SRAM-based FPGAs are sensitive to the effects of SEUs, several different techniques to detect or mitigate against SEUs in FPGAs have been proposed, including triple modular redundancy (TMR), duplication with compare (DWC), FPGA block memory scrubbing, and reduced precision redundancy (RPR). Each of these techniques has been used in the CFE payload in one or more custom applications developed as part of this work and used to conduct SEU mitigation and detection experiments. These experiments take advantage of the unique on-orbit, reconfigurable platform provided by the CFE payload. In addition, the payload FPGAs have also been configured to perform SEU detection and mitigation experiments on the SDRAM devices that provide additional data storage to the payload FPGAs.

This chapter will first describe the goals of the SEU detection and mitigation studies conducted on the CFE payload and discuss the general architecture of the CFE SEU mitigation and detection applications. This will be followed by by a discussion of each of the SEU mitigation and detection experiments conducted on CFE. Each technique under test will be described briefly, the specific architecture of the experiment will be discussed, and the on-orbit results of the experiment will be presented.

3.1 SEU Mitigation and Detection Applications on CFE

One of the main objectives of the SEU detection and mitigation studies on CFE is to validate the feasibility and correct operation of proposed FPGA SEU mitigation and detection strategies when used in an actual orbit environment. Many of these these techniques have been tested extensively with fault simulations [33], fault injection [6, 34], and radiation beam testing [7, 35, 36], but they have not been as often validated in a deployed and opera-

tional system in an actual orbit environment.[1] Another objective of the CFE detection and experiments is to determine the rate that SEUs occur in orbit in the payload FPGAs and SDRAM modules, and to compare these rates to those projected by theoretical means.

At times when the SEU detection and mitigation applications are scheduled to operate on CFE, all 9 of the Virtex FPGAs in the payload are configured with identical bitstreams. Each application's FPGA logic consists of test circuitry for one or more mitigation or detection techniques along with interrupt-forming logic and a register interface accessible to the payload RAD6000 microprocessor. When the SEU-related applications are operational, the microprocessor executes software which reads application status registers from the FPGAs every 30 seconds and reports them to the ground with a status packet; the flow of this software is shown in Figure 3.2. The periodic status packets provide a mechanism to verify correct operation of the experiment's hardware and software as well as a measurement of how long the experiment has been operating, which assists in SEU rate calculations. The processor also stands ready to service any interrupts triggered by an FPGA. The interrupt circuitry and register interface allow the test circuitry on any of the FPGAs to notify the processor of any noteworthy mitigation or detection event (such as a detected SEU) with an interrupt as well as to provide additional information about that event to the processor through status registers. All status and event packets are processed upon delivery to the ground station, and their information is combined into several experiment log files. The files can be further processed to obtain results specific to each of the various SEU detection and mitigation tests performed within the application.

For this work, we created and deployed six different SEU mitigation and measurement applications to the CFE payload over the course of two years. The first five of these applications, SEU2-SEU6, were developed in a staged manner, each either adding new mitigation or detection tests or repairing bugs in preceding applications. The last application developed as part of this work, SEU7, was developed separately from the previous applications and does not share functionality with these applications. The timeline of operation for each CFE SEU application is shown in Figure 3.1. Table 3.1 details the mitigation or detection tests included in each CFE SEU application. The remainder of this chapter focuses on the re-

[1] See Section A.5 for a detailed discussion of ground-based and on-orbit mitigation validation approaches.

sults of the mitigation and detection tests within SEU2-SEU6; for more detailed information about the runtime of each application, consult Appendix C.

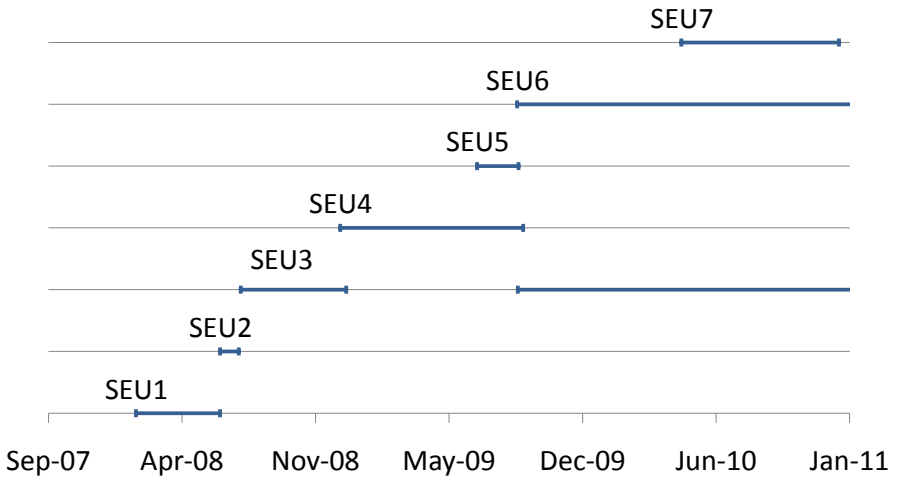

Figure 3.1: Timeline of operation for all CFE SEU applications.

Table 3.1: Description of which mitigation tests are present in each CFE SEU application

	SEU2	**SEU3**	**SEU4**	**SEU5**	**SEU6**	**SEU7**
DWC	X	X	X	X	X	
BRAM		X	X	X	X	
SDRAM			[a]	X	X	
RPR						X

[a]The SEU4 SDRAM test was determined to be faulty and was repaired in subsequent experiments.

3.2 Triple Modular Redundancy (TMR)

One of the most commonly used strategies to mitigate against system failures caused by SEUs in a digital hardware design is the insertion of redundancy into a design. The basic enabling principle of TMR is the creation of redundant hardware structures which allow

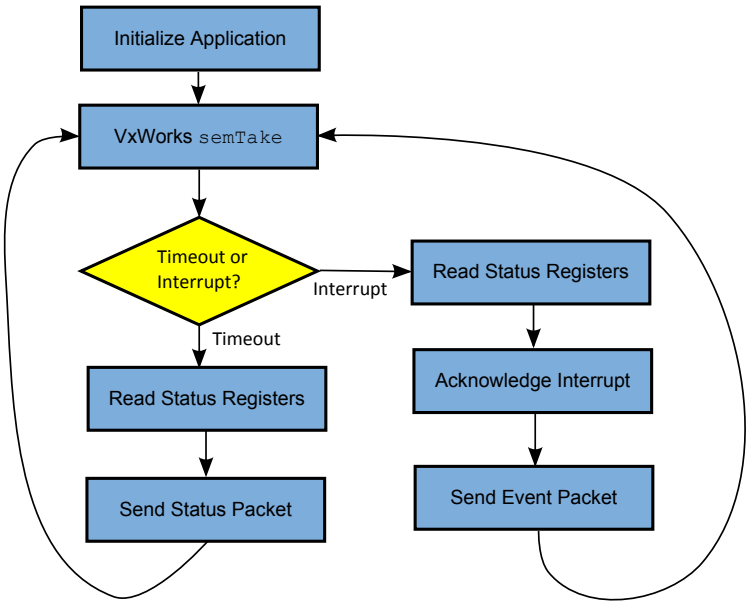

Figure 3.2: Flow of the CFE SEU application software

for the incorrect operation of a single structure to be masked by the correct operation of corresponding redundant structures. In a design employing TMR, three copies of a circuit structure are inserted into a design and their outputs voted upon by a majority voter or redundant voters [37], as shown in Figure 3.3. If at any time one of the circuit outputs is not in accord with its redundant counterparts, the correct result is still chosen as long as at least two of the redundant structures output the correct result.

One of the major drawbacks to the application of TMR to a circuit is the increase in circuit area required to triplicate the design and insert voters; in most cases, using TMR in an FPGA design requires a greater than 3X increase in design resource utilization [38]. One alternative to the complete application of TMR is partial TMR, which is the application of TMR to a subset of the design containing the circuitry that has been deemed most critical to the circuit's correct operation [36, 38].

TMR has emerged as the preeminent logic-level strategy for mitigation against SEUs in FPGAs, and no techniques have been found that can equal its effectiveness at a similar or lower hardware cost for all types of FPGA-based circuits [39]. Since TMR only masks SEUs and does not detect or correct them, TMR in FPGAs is often combined with configuration

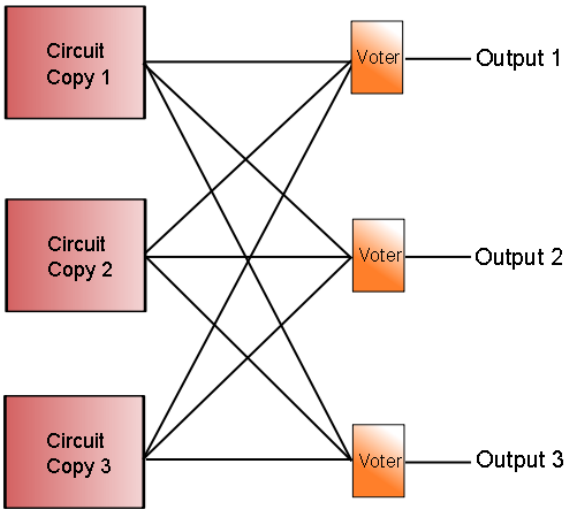

Figure 3.3: Triple modular redundancy (TMR) with triplicated voters

scrubbing in order to alleviate the problems caused by accumulating SEUs and to allow for the detection and reporting of SEUs that occur within the FPGA. Full and partial TMR used in have been tested extensively with ground-based testing, including fault simulation [33, 40], fault injection [6, 38, 41], and radiation testing [35, 36]. All of the ground-based tests have found TMR to be very effective at masking SEU-induced errors in an FPGA-based circuit's operation.

The application of TMR to payload FPGA designs is a major component of the CFE payload's upset mitigation strategy. Researchers at BYU and LANL developed a software tool, BL-TMR, before CFE's launch in order to facilitate rapid and automated application of TMR to the FPGA designs used on the CFE payload [36]. The tool has the ability to operate at the LUT level of the design, enabling the application of full or partial TMR at very fine increments in order to maximize the amount of the circuit to which TMR can be applied. Full and partial TMR as applied by BL-TMR have both been used regularly in CFE's catalog of applications.

In the applications developed for this work, we used full TMR to protect all of the test control circuitry from upsets, including finite state machines, the processor register interface,

and interrupt-generation circuitry. The mitigation and detection applications using TMR have operated for over four thousand FPGA device days, and no SEUs have been observed to cause functional errors in control circuitry throughout the time of these applications' operation. The BL-TMR tool has allowed for the quick, automated, and flexible application of TMR to application FPGA designs and has been invaluable to the design the SEU detection and mitigation experiments designed in this work.

3.3 Duplication With Compare (DWC)

One observation that enables a lower-cost strategy to manage SEUs is that some systems can tolerate errors and use system-level mechanisms to address them, provided that the errors can be detected quickly [7]. In this case, full mitigation of the errors on the logic level is not required, and circuitry to facilitate error detection can be added instead of more costly error-masking circuitry. A technique known as duplication with compare (DWC) is a commonly-used method for detecting circuit errors. Rather than triplicating all logic in the design, DWC operates with reduced hardware cost by duplicating the circuit and comparing the outputs at different points of the duplicate copies, as shown in Figure 3.4. If the outputs of the two copies do not match, an error in one of the copies is assumed, and an error signal is asserted. Self-checking, dual-rail comparators can be used in the error detection and reporting circuitry in order to facilitate the detection of errors within that circuitry as well as the duplicated circuit. The outputs of all of the comparators throughout the circuit are merged to form a system-level error code which denotes the presence or absence of errors throughout the entire circuit and is reported to the system [42].

DWC applied to FPGA-based designs has been tested on the ground with both fault injection [42] and particle accelerator testing [7]. In applications where adequate device resources are available to ensure complete duplication of the circuit, well over 99% of the SEU-induced output errors of the circuit were successfully detected by DWC in both methods of testing.

The goal of the DWC test on CFE is to validate in orbit the use of DWC as a technique appropriate for use in space. In the main CFE DWC test's circuitry, which was designed by Jonathan Johnson, DWC employing dual-rail comparators is applied to a long

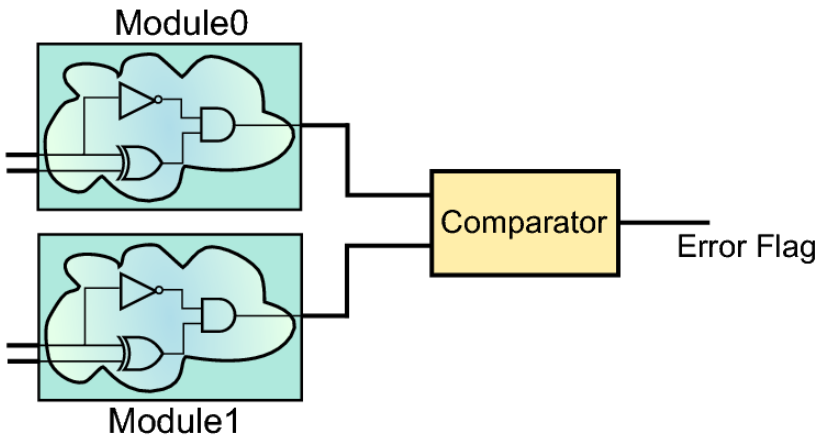

Figure 3.4: Basic duplication with compare (DWC)

32-bit wide shift register, shown in Figure 3.5. The shift register's length is parameterizable, allowing it to "fill the chip" after duplication and maximize the amount of the circuit that is sensitive to SEUs. The parameterization of this shift register allows the DWC portion of the circuit to grow or shrink depending on what other test circuitry is to be included in an application's FPGA design. In addition to the shift register circuit, DWC was applied to some of the control logic of the BRAM scrubbing test that will be described in Section 3.4 and is included with SEU3-6.

We used BL-DWC [42], a CAD tool developed at BYU, to automatically apply DWC using self-checking comparators to the test circuitry and to merge the comparator outputs into a system level error signal. This system-level signal is used by the DWC test's control circuitry to generate interrupts to the payload microprocessor whenever an FPGA's system level DWC error signal is asserted. When a DWC interrupt is triggered, the control circuitry also places the two-bit error code reported by DWC into a processor-readable status register. After reading this status register, the application software resets the FPGA in which the error was detected. As the DWC test's control circuitry is itself sensitive to SEUs, TMR

Table 3.2: CFE DWC-detected SEUs
(June 14, 2008 - January 27, 2011)

DWC Device Days	Configuration SEUs	DWC-Detected SEUs	Percent Sensitivity
4458.6	1300	105	8.1%

was applied to the control circuitry in order to avoid disruptive application errors caused by SEUs occurring within that circuitry.

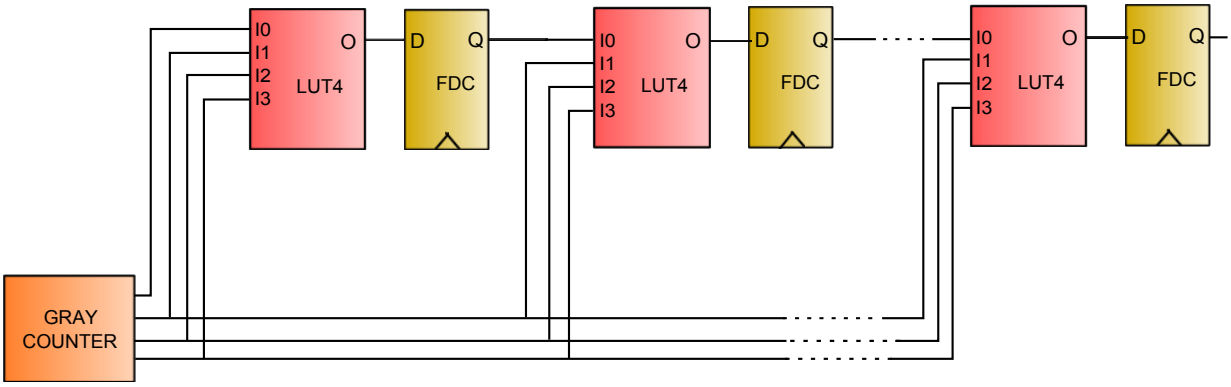

Figure 3.5: Gray code generator and shift register used in the DWC test

The CFE DWC test has been successful in demonstrating the ability of DWC to provide error detection in FPGA-based designs. The test was first developed with SEU2 and was also included in SEU3-6. It began regular operation on June 14, 2008 and has been scheduled to operate regularly since that date. Tables 3.2 and 3.3 summarize the operation of the test. Overall, the test has operated for 4458.6 FPGA device days, detecting a total of 105 SEUs that affected the outputs of the test circuitry. 4 of the DWC-detected SEUs occurred in the logic of the BRAM error detection and scrubbing test; none of these SEUs appeared to cause any unusual behavior in the operation of the BRAM test before the FPGA was reset.

Of the DWC-detected SEUs found on CFE, 95 corresponded to an SEU found by the configuration scrubbing performed by the Actel FPGA on each RCC. The remaining 10 (9.5%) of the DWC-detected SEUs did not correspond to an SEU found by the scrubber.

Table 3.3: Classification of CFE DWC-detected SEUs

Section of Design	Error Detections	Checker Errors	Total
Shift Register	93	8	101
BRAM Test Control	4	0	4
Total	97	8	105

Some of these events are possibly due to SEUs that changed user state (flip-flop values) which are not detectable by configuration scrubbing. However, since the sensitive cross section of FPGA flip-flops is about 0.3% of the cross section of configuration SEUs, it is likely that some other phenomenon accounts for some of the SEUs detected by DWC but not by the scrubber. Another possible explanation for these SEUs is that an erroneous logic value was induced by a single event transient and then latched into one of the DWC shift register's flip-flops. However, SETs are considered to be rare events in FPGAs [33].

As the DWC circuitry in the CFE SEU experiments utilizes dual-rail, self-checking comparators, the state of the DWC error codes reveals insight into whether the error detection circuitry is itself affected by SEUs. A checker error is manifest by a '1' on only one of the two DWC error signal bits and corresponds to the case where the error checking circuitry is itself in error. An example of how a DWC checker error might arise is shown in Figure 3.6.

On CFE, 8 checker errors have occurred, which is 7.6% of the total number of DWC events that occurred in the CFE DWC experiments. This figure is higher than checker error percentages found in various DWC designs tested in [7] and [42] with fault injection and radiation testing; however, the number of checker errors in a given design is very dependent on certain design characteristics including the number of comparators that are present in the circuit and the method in which comparator outputs are merged into a system-level error code. In addition, most of the CFE FPGA configurations containing DWC experiment circuitry contain both duplicated and unduplicated sections that result from the automated application of partial DWC. Partial DWC has been shown to increase the number of checker errors that occur in a design, since additional comparators are placed at points in the design where duplicated copies of design circuitry narrow down to an unduplicated section of the design [7].

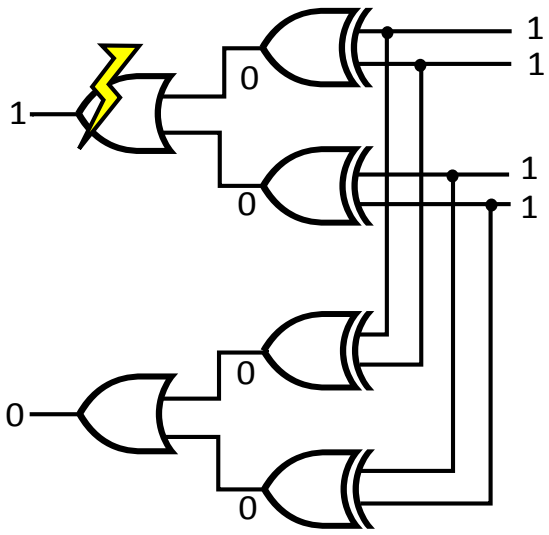

Figure 3.6: Example of a DWC checker error

3.4 BRAM SEU Detection and Scrubbing

Modern FPGAs usually contain dedicated block memories (BRAMs) to support applications that require a significant amount of data storage to meet their resource requirements. Unfortunately, the data stored within FPGA BRAM is sensitive to SEUs. If upsets in BRAM can be masked or detected and reported quickly, the system may be able to handle any errors that the upset may have caused. Unfortunately, SEUs in FPGA BRAM cannot be detected with configuration scrubbing as done for upsets in the FPGA configuration memory. Since the contents of FPGA block memories may be modified by the user application, a readback and comparison check utilizing a stored "golden" copy of the memory state or CRC values is not possible [43]. In order to detect upsets in BRAM, knowledge of the contents of the memories is required from some redundant source, such as duplication or triplication of the memory or redundancy embedded within the data such as error detection codes (EDC) or error correction codes (ECC). If adequate data redundancy is present, circuitry can be designed to detect, mask, or scrub out errors that occur within the BRAM elements.

The BRAM test on CFE serves mainly to report the number of errors found in the BRAM to aid in BRAM SEU rate calculations, but it also utilizes a scrubbing-based technique that could be combined with data redundancy to provide BRAM error detection

and correction. The BRAM SEU detection test circuitry was developed by Daniel Richins; a block diagram of the circuit is shown in Figure 3.7. All of the BRAMs in the FPGA are initially written with a predefined pattern of alternating 1s and 0s. A control circuit protected by DWC detects any SEUs in the BRAM by continuously scanning the entire contents of each BRAM and comparing the data read with the expected pattern. When the data read from the BRAM does not match the pattern, the circuitry records the error and continues scanning the BRAM. Once the end of scan of a single BRAM is reached, the circuit continues scanning the other BRAMs in the FPGA if no errors were found. If any errors were found in the scan, the control circuit interrupts the processor and places the number of errors found in the BRAM in a processor-readable status register along with the identifying address of that particular BRAM. Once the processor has acknowledged the interrupt, the circuit writes the correct data pattern to the BRAM to overwrite the error, and then continues to scan the rest of the BRAM in the circuit.

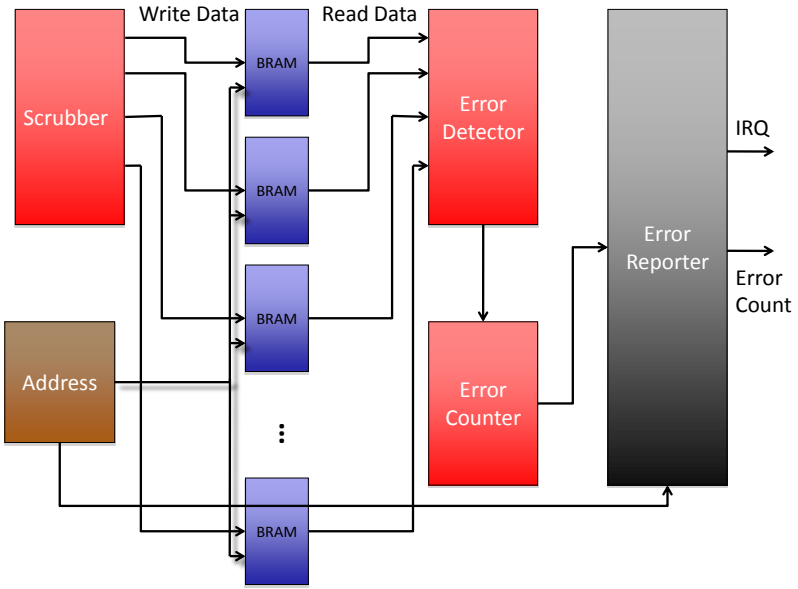

Figure 3.7: Block diagram of BRAM test circuitry

The BRAM error detection and correction test was first included with SEU3 and has also been included in SEU4-SEU6. The test began regular operation on July 15, 2008 and has been scheduled to operate regularly since that time. The BRAM error detection test

has operated in orbit for 4361.4 device days and has demonstrated the ability to detect and correct errors in FPGA block memories used in space through the proper design, implementation, and usage of a BRAM scrubbing circuit. The principles of BRAM error detection and correction validated in these experiments can be applied to the implementation of systems which enable reliable random access to FPGA block memories.

In addition to validating the use of BRAM scrubbing as a techniques to improve the reliability of of using FPGA BRAMs in space, the BRAM experiments on CFE have provided insight into the BRAM upset rates that can be expected in orbit. The experiments have detected 106 SEUs that occurred within the BRAM in orbit, resulting in a measured FPGA BRAM SEU rate of 0.026 upsets per device day. Two multiple bit upsets were also detected. A more detailed analysis of the BRAM upset rate measurement provided by this test will be presented with the rest of CFE's SEU rate data in Chapter 4.

3.5 SDRAM SEU Detection and Scrubbing

Although the block memory included within FPGAs is sufficient for many applications, some applications may require additional data storage beyond that provided within the FPGA. SDRAM is a commonly-used data storage solution for FPGA applications because of its high density and low cost, but like FPGA configuration memory and BRAM, SDRAM is sensitive to SEUs. Techniques similar to those used to detect and correct upsets in BRAM as described in Section 3.4 can be used to detect or mitigate against SEUs that occur in SDRAM by using the logic resources of an FPGA to implement the SEU detection or mitigation technique. Since SDRAM is a component external to the FPGA, however, implementation complexity for an SDRAM error detection and/or correction circuit is likely to be greater than for a similar BRAM circuit. For example, a memory controller will likely need to be implemented in the FPGA's configurable logic, and multiple clock domains may exist within the circuit if the memory requires a different clock rate than the FPGA circuitry. Since the FPGA circuitry used to implement the memory controller would be sensitive to SEUs, it should also employ SEU mitigation such as TMR, which requires special consideration when used in circuits employing multiple clock domains [44].

We designed the SDRAM error detection test on CFE to report the number of errors found in the SDRAM, enabling SDRAM SEU rate calculations and validating a scrubbing-based technique that could be expanded to perform SDRAM upset detection and correction. The FPGA circuitry for this test was designed by Daniel Richins. Figure 3.8 shows the test's system block diagram, and Figure 3.9 summarizes the operation of the system. As the FPGA circuitry responsible for controlling the SDRAM and detecting and correcting errors is itself susceptible to SEUs, TMR was applied to the FPGA circuitry in order to mitigate against SEUs occurring in that section of the FPGA. Each of the three banks of SDRAM associated with each FPGA is initially written with a different pattern: all ones, all zeroes, or alternating ones and zeros. Different data patterns are written to each SDRAM bank because the probability of an SEU causing an SDRAM bit with a value of 1 to transition to a 0 value is not equal to the probability of an SEU causing a 0 to 1 transition [23]. After writing data to the SDRAM banks, the control circuit implemented on the FPGA continually scans the SDRAM for errors. If any errors are present, the circuit records the error or errors and interrupts the processor, which sends information regarding the error to the ground in an event packet. Once the processor has acknowledged the interrupt, any errors in the SDRAM are corrected and a new scan commences.

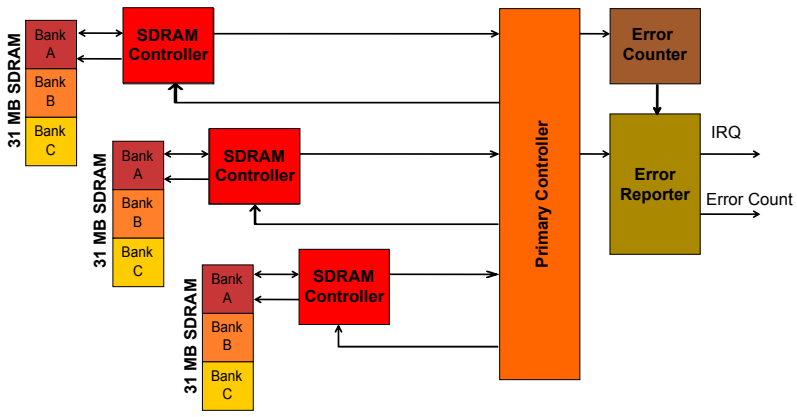

Figure 3.8: Block diagram of SDRAM test circuitry

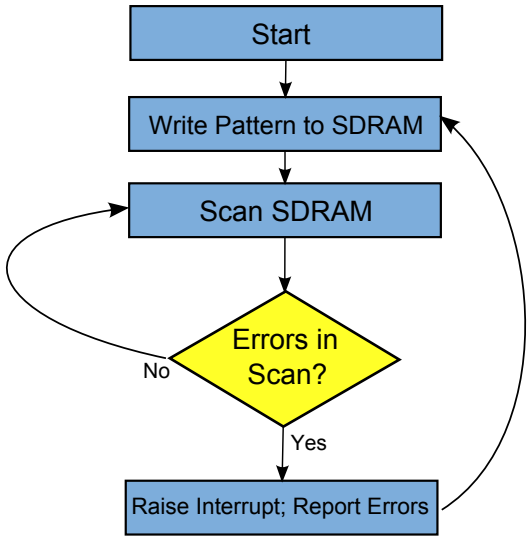

Figure 3.9: Flowchart of SDRAM test operation

The SDRAM error detection and scrubbing experiments on CFE were first included in SEU4; however, due to bugs in the SDRAM-related FPGA circuitry, this application yielded no SDRAM-related results. The bugs were fixed in SEU5 and SEU6, and the SDRAM test circuitry in these two applications has operated for a total of 17132.7 SDRAM device days.[2] The SDRAM test began in-orbit operation on July 4, 2009 and has been regularly scheduled to run on the payload since that time. The test has demonstrated the successful operation of an FPGA circuit to detect and repair SEU-induced errors in SDRAM external to the FPGA. This capability can allow for the development of an FPGA-based system enabling reliable random access from SDRAM with the added usage of techniques such as redundancy and error detection and correction codes. The successful implementation of such a system would allow for space-based systems requiring reliable volatile memories to use high density, relatively inexpensive SDRAM coupled with an off-the-shelf FPGA rather than more expensive technologies, provided that the parts themselves are qualified for usage in space.

[2]This figure is higher than for the other experiments described in this section since each FPGA has independent access to 12 SDRAM devices, each of which operates continuously during the application's runtime.

The SDRAM error detection and scrubbing experiments have also provided a means to measure the rate at which SEUs occur in CFE's SDRAMs. 2388 SDRAM SEUs have been detected by the experiments, yielding a SDRAM SEU rate of 0.14 SEUs per SDRAM device day. 142 of these upsets affected multiple SDRAM bits, including upsets of 2, 3, 4, 5, 7, and 11 bits. The SEU rate results from the SDRAM scrubbing experiments will be presented in greater detail in Chapter 4.

3.6 Reduced Precision Redundancy (RPR)

As one of the main drawbacks of using TMR to mitigate against SEUs in SRAM FPGA designs is the increase in device utilization required to apply the technique, lower-cost techniques to allow for correct circuit operation in the presence of upsets have been investigated. One observation that can facilitate lower-cost upset mitigation in many computational applications such as digital signal processing (DSP) is that the most significant bits of a computation are more critical to the correctness of the result than the lower-order bits. This observation is the basis behind reduced precision redundancy, or RPR. In general, RPR involves creating one or more smaller, reduced precision replicates of a computational module and using the outputs for a sanity check on the output of the full precision model [8, 45], as shown in Figure 3.10. When tested with fault injection, RPR has been shown to provide a significant increase in system reliability in some FPGA DSP applications with an implementation overhead of about one quarter of that required for TMR [8].

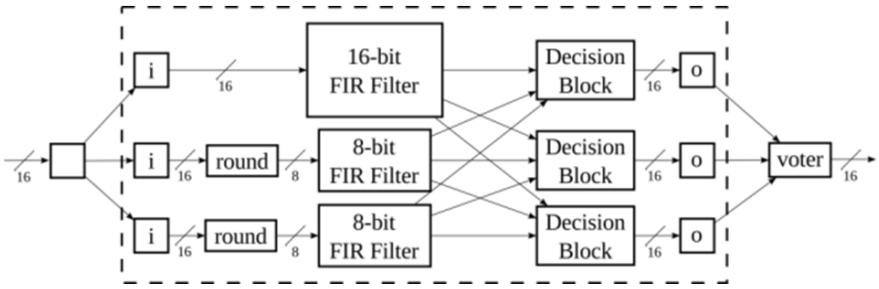

Figure 3.10: Application of reduced-precision redundancy (RPR) to a FIR filter

We designed the RPR test on CFE to verify the application of reduced precision redundancy in an FPGA-based digital communications system as a lower-cost mitigation alternative to TMR. The communications system to which RPR was applied was designed in Xilinx System Generator by Brian Pratt. In the test, which is diagrammed in Figure 3.11, a data generation circuit feeds data to several FIR filters which serve as matched filters in a BPSK receiver. One of these filters, the "golden" filter, employs TMR to mitigate against SEUs, while the rest of the filters are mitigated using RPR. All other circuitry in the experiment (with the exception of the data generation circuit) is triplicated. In the absence of SEUs, all filters should produce the same output, so if any of the RPR filter outputs differs from the golden filter output, an SEU is assumed to have caused the error. In this case, the squared difference between the two filters is accumulated over a set number of clock cycles in order to facilitate the calculation of the variance between the two filters. The test circuitry then interrupts the processor, which reads the variance and filter bit error rates from status registers, acknowledges the interrupt, and reports the status register values down to the ground in an event packet.

The results of the operation of the CFE RPR test are summarized in Table 3.4. The RPR test is included only in the SEU7 application, the most recent addition to CFE's catalog of SEU-related applications. SEU7 began in-orbit operation on May 6, 2010, and operated regularly until December 27 of that year. Since SEU7 is the newest of the applications and since it consumes significantly more power than the other applications, it did not operate in orbit for as long as the other applications. In general, the application operates in the SAA to maximize the number of SEUs to which the payload FPGAs are subject. The RPR test operated on CFE for 49.0 FPGA device days, during which 140 configuration SEUs were detected. One of these SEUs caused an error to occur in the output of one of the RPR filter outputs; however, the error was not destructive enough to the system to cause any bit errors in the BPSK system.

3.7 Conclusion

This chapter described the SEU detection and mitigation techniques developed in this work and scheduled to operate on the CFE payload. TMR is used to mitigate against

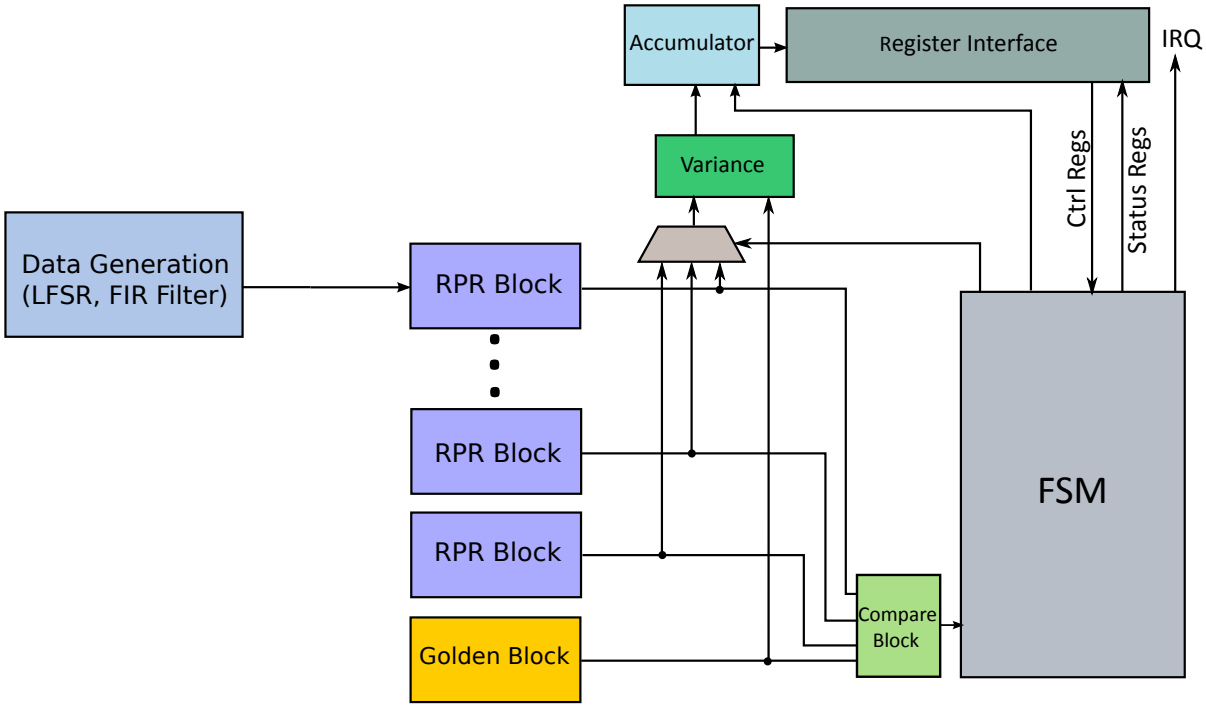

Figure 3.11: Block diagram of the RPR test on CFE

Table 3.4: Results of the CFE RPR test
(May 6, 2010 - December 27, 2010)

FPGA D.D.	Config SEUs	Total Events	Events With No Bit Errors	Events With TMR Bit Errors Only	Events With RPR Bit Errors Only	Events With TMR and RPR Bit Errors
49.0	140	1	1	0	0	0

SEUs in many of the payload applications that use the Virtex FPGAs, while DWC, RPR, BRAM error detection, and SDRAM error detection are implemented on CFE within scheduled applications designed to validate these techniques. These applications support the results of ground-based validation tests in demonstrating the correct in-orbit operation of the techniques.

CHAPTER 4. CFE SEU RATE MEASUREMENT

One of the major contributions of the SEU-related operations of the CFE payload and applications is the ability to calculate long-term upset rates for the SRAM-based FPGAs and SDRAM devices of the payload. As discussed in Chapter 2, the SEU rate in an orbit environment is an important factor in determining whether a given electronic device is suitable for use in that environment and whether a given upset mitigation strategy is appropriate for that environment.

This chapter will first discuss the SEU rate estimations and measurements for the CFE payload's Virtex FPGAs, followed by rate estimations and measurements for the payload's SDRAM devices. As there is some difference between the initial predictions and the measured upset rates, a discussion of the possible factors which may help to explain this variation follows. The chapter concludes with a discussion of four interesting phenomena associated with the SEUs detected in CFE payload electronics: single-event functional interrupts (SEFIs), multiple-bit upsets (MBUs), the effect of the South Atlantic Anomaly on on-orbit SEU rates, and the effect of the solar cycle on on-orbit SEU rates.

4.1 FPGA SEU Rate on CFE

Upset rates for the FPGAs used on CFE were estimated by Engel et al. before launch using radiation test data and the CREME96 orbit modeling software [24, 46]. The process of making these predictions with CREME96 is diagrammed in simplified form in Figure 4.1, and more detailed descriptions of the process of CREME96 rate prediction are given in Section A.4 and [46]. The main inputs that were required for CFE's rate predictions, including orbit and FPGA static cross section parameters, are summarized in Table 4.1. The device cross section parameters were obtained from radiation testing by members of the Xilinx Radiation Test Consortium (XRTC) [47, 48]. These parameters correspond to the SEU vul-

nerable area of the device and are calculated by fitting data points measured at different energy levels at a particle accelerator to the Weibull distribution, which has been proposed as an appropriate distribution for per-bit static cross section versus energy [49].

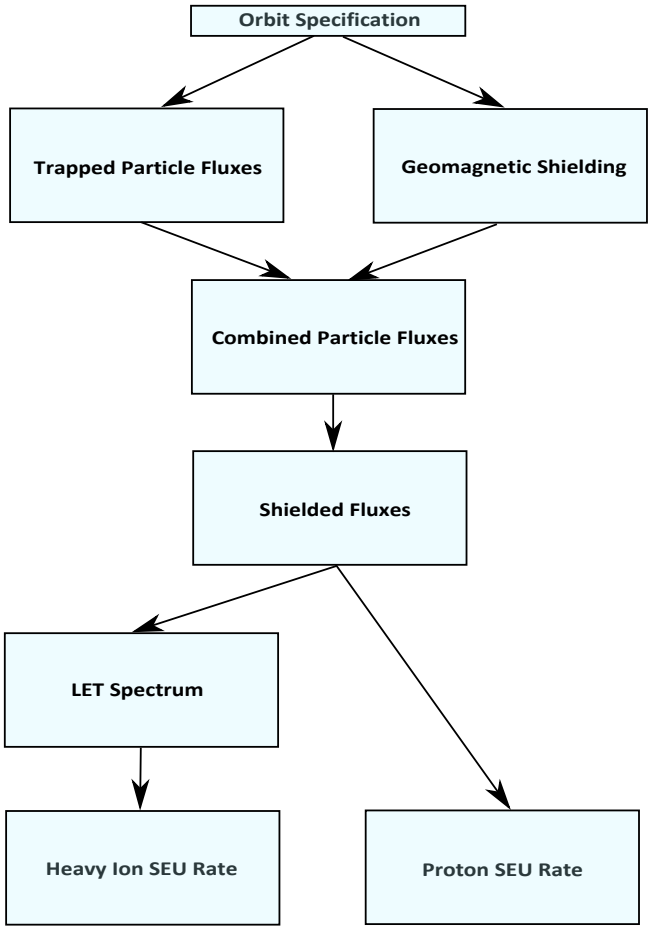

Figure 4.1: CREME96 Flow. Adapted from [46]

The predicted configuration and BRAM SEU rates for CFE's FPGAs were presented in [46]; these rate predictions are repeated here in Table 4.2. CREME96 allows for the calculation of several different SEU rates for different environment conditions. These rates include rates for solar minimum and solar maximum for both normal and worst-case trapped proton conditions, as well as rates for flare-enhanced solar conditions (worst week, worst day, and worst 5 minute peak). The output of CREME96 is divided into separate SEU rate

Table 4.1: Orbit and Weibull distribution cross-section parameters for the Xilinx Virtex FPGAs on CFE

Orbit Apogee	563 km	
Orbit Perigee	558 km	
Orbit Inclination	35.4 degrees	
Number of Configuration Bits	5810048	
Number of BRAM Bits	131072	
Proton Parameters	Onset	10 MeV
	Width	30
	Exponent	2
	Limit	$2.2 \times 10^{-14} cm^2$
Heavy Ion Parameters	X & Y	2.83 μ
	Z	1 μ
	Onset	1.2 $MeV/cm^2/mg$
	Width	30
	Exponent	2
	Limit	8 μ^2

predictions for protons and heavy ions for each of the environment conditions, and these rates can be easily added together to yield an overall rate prediction, as presented in Table 4.2.

Table 4.2: Predicted SEU Rate for CFE Virtex FPGAs (Upsets/Device Day, From [46])

	Config Best Estimate	**Config Worst Case**	**BRAM Best Estimate**	**BRAM Worst Case**
Sol Min	8.38E-1	8.62E-1	3.78E-2	3.89E-2
Sol Max	5.02E-1	5.21E-1	2.26E-2	2.35E-2
SolMin Trap Pro Peak	2.61E+1	2.61E+1	1.18E+0	1.18E+0
SolMax Trap Pro Peak	1.68E+1	1.68E+1	7.59E-1	7.59E-1
Worst Week	5.22E-1	5.52E-1	2.35E-2	2.49E-2
Worst Day	5.31E-1	5.56E-1	2.40E-2	2.51E-2
Peak	6.09E-1	6.50E-1	2.75E-2	2.93E-2

Data from the readback-based configuration scrubbing technique built into the CFE payload and described in Section B.3.3 is used to calculate CFE's FPGA configuration SEU rate. Configuration scrubbing is active during the execution of all CFE applications. The Actel antifuse FPGA in each RCC module detects any SEUs in the RCCs Virtex devices and

reports information about each SEU to the payload R6000 microprocessor, which packages SEU occurrence data into a packet to be sent to the ground. Periodic state-of-health packets are also sent, denoting the amount of time that the FPGA configuration scrubbing is enabled and the position of the satellite during that time. The information from these packets is stored in a database to enable further processing. Regional and overall SEU rates can then be calculated from the SEU occurrence data and the SEU scrubbing enable database.

Configuration scrubbing circuitry is not capable of detecting SEUs that occur in the FPGA block memories. Instead, data from the BRAM scrubbing circuit described in Section 3.4 is used to calculate BRAM SEU rates. Each event packet sent by the BRAM circuitry denotes the occurrence of an SEU, while status packets sent by each RCC module every 30 seconds allow for measurement of the amount of time that the BRAM error detection has been enabled. Each event and status packet includes also location information, which allows regional BRAM SEU rates to be calculated. Since the BRAM error detection circuitry is only included in the SEU3-SEU6 applications, the BRAM SEU rates presented here are only based on the periods of time that these applications were scheduled to operate. Although other BRAM upsets may have occurred within other applications, these upsets have not been detected and are not included in the BRAM upset rates presented here.

The overall FPGA SEU rates for the configuration memory and BRAM are presented in Table 4.3. These rates are lower than those predicted using CREME96; if compared to the solar minimum rates (which is appropriate since the solar cycle has been near minimum during CFE's orbit time to date), the configuration SEU rate is about a factor of 3 lower than the prediction, and the BRAM SEU rate is about a factor of 1.5 lower than the prediction. A discussion of what might cause this discrepancy between predicted and measured SEU rates will be presented in Section 4.3. Figure 4.2 shows the configuration SEU rate for 18 different regions around the earth. As expected, the measured SEU rate within the SAA is much higher than the rate outside of the SAA; this phenomenon will be discussed in detail in Section 4.6.

Table 4.3: CFE FPGA SEU rate

	Start/End Dates	FPGA Device Days	SEUs	SEUs/D.D.
Configuration	3/8/07 - 1/27/11	6254.4	1770	2.83E-1
BRAM	7/15/08 - 1/27/11	4361.4	114	2.61E-2

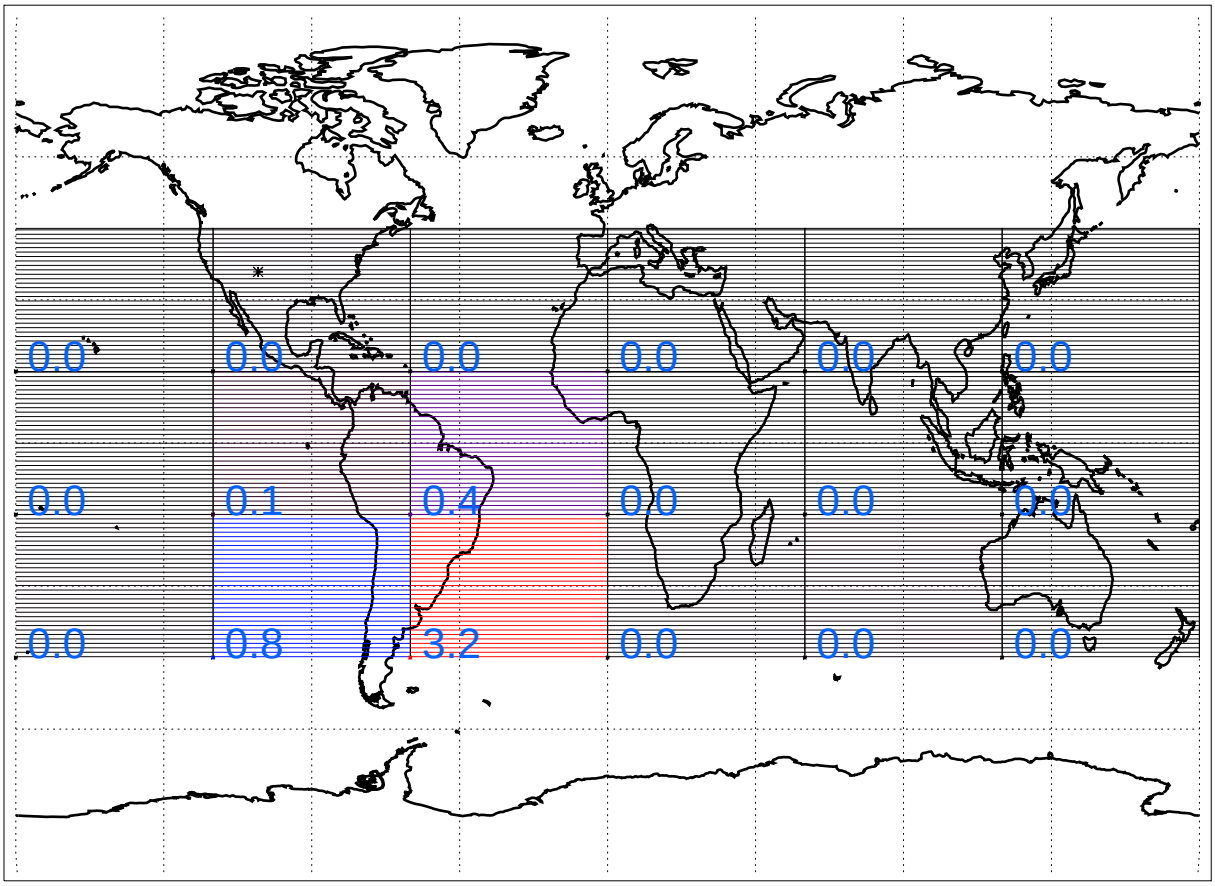

Figure 4.2: CFE FPGA SEU rate by region.

4.2 SDRAM SEU Rate on CFE

The process of predicting SEU rates for the CFE payload SDRAM is very similar to that of FPGA SEU rate prediction. The CREME96 flow is used with the same orbit specification as used in the FPGA SEU rate predictions, with the difference being in the device-specific parameters.

Table 4.4: Estimated Weibull distribution parameters for the CFE payload SDRAM

Number of Bits/Device	67108864	
Proton Parameters	Onset	33 MeV
	Width	11
	Exponent	1.2
	Limit	$1.13 \times 10^{-15} cm^2$

Since SDRAM SEU rate predictions were not made prior to CFE's launch, I computed post-launch rate predictions for these devices as part of this work. These predictions are presented in Table 4.5. Unfortunately, the specific device parameters obtained from radiation testing necessary for SEU rate prediction were not readily available at the time of writing. Proton testing for this part has been conducted and results presented in [50], and I estimated the best-fit Weibull distribution parameters to enable proton SDRAM rate predictions for the purposes of this thesis. Table 4.4 presents these estimated parameters. I did not make similar estimations for this device for heavy ions since the heavy ion SEU rate predictions are likely much lower than the proton SEU rate, as is the case in the FPGA SEU rate predictions.

Table 4.5: Predicted proton SEU rate for CFE payload SDRAM

	Upsets/Device Day
Sol Min	4.79E-1
Sol Max	2.94E-1

As described in Section 3.5, the SDRAM error correction and detection circuitry implemented on CFE's payload FPGAs allows for the collection of SDRAM SEU rate data. Similarly to the BRAM error detection and correction circuitry, periodic status packets are used to calculate the amount of time that a detection experiment has been in operation, and event packets denote any occasion where one or more SDRAM bits have been upset. Since both types of packets also contain location information, regional SEU rates can also be cal-

culated. As with the BRAM SEU rates, the SDRAM SEU rates are based only on the times when applications containing SDRAM error detection circuitry (SEU5-6) were scheduled to operate. Although more SDRAM upsets may have occurred during the execution of other applications, these upsets were not detected and are not included in the SDRAM upset rates presented here.

Table 4.6 summarizes the overall SEU rates calculated for the SDRAM in the CFE payload. Since the initial version of the SDRAM error detection and correction circuitry did not have a mechanism for counting the number of SDRAM bits that were upset by each upset event, its results are separated from those collected by subsequent versions of the design (see Appendix C for more information on the evolution of all of the CFE SEU-related applications, including the applications that include an SDRAM test.) As with the FPGA SEU rates, the observed rate is considerably lower than that predicted with CREME96. If solar minimum is assumed to be the closest match to the actual operating environment of CFE to date, the observed SEU rate is smaller than the predicted rate by a factor of about 3. This estimate is based on the rate of upset events rather than upset SDRAM bits, as CREME96 assumes that all upsets cause a single bit error.

Table 4.6: CFE SDRAM SEU rate

	Start/End Dates	**SDRAM D.D.**	**Events**	**Events/ D.D.**	**Bits Upset**	**Bits Upset/ D.D.**
No Error Counter	7/4/09 - 9/3/09	1204.1	223	1.85E-1	N/A	N/A
Error Counter	9/3/09 - 1/27/11	15928.6	2165	1.36E-1	2348	1.47E-1

4.3 Difference Between Estimated and Observed SEU Rates on CFE

As shown in the previous section, all of the CFE SEU rate predictions made by CREME96 overpredicted the rate at which SEUs have actually occurred. Although some difference in predicted and measured SEU rates is to be expected since the occurrence of SEUs is a random process, the degree of discrepancy is too large and the amount of data collected too great to be completely explained by random variation. However, such mismatches

in predicted and measured on-orbit upset rates are not uncommon. Peterson analyzed 126 comparisons of predicted and observed rates from 23 satellites in [20] and found several over-predictions and underpredictions of the SEU rate with differing magnitudes of disagreement and in a variety of devices and orbit environment.

Several hypotheses have been proposed by Peterson and others to explain the discrepancies between predicted and measured on-orbit SEU rates. Three of these possible factors may apply to the specific case of CFE and will be discussed in this section: the limitations of the AP-8 trapped proton environment model, the variation among different physical devices which implement a chip design, and the effect of shielding on SEU rate predictions.

4.3.1 AP-8 Trapped Proton Model Limitations

Geomagnetically trapped protons are the primary cause of single event effects in most spacecraft systems deployed in low earth orbits. The trapped proton module of CREME96 uses the NASA AP-8 models to model the effects of these trapped protons; these models were derived from measurements accumulated by satellites in the 1960s and 1970s [51] and consist of two different versions: AP8MIN for solar minimum conditions, and AP8MAX for solar maximum conditions.

The CREME96 documentation contains a discussion about the limitations of the AP-8 model and how they affect SEU rate predictions [52]. These limitations include the model's outdated geographic positioning, reduced accuracy at low altitude orbits, limited variability throughout the solar cycle, and lack of orbit generator precession terms. Because of these limitations, the documentation recommends that trapped proton rate predictions should be considered to be factor of two estimates. Peterson also describes these limitations and adds that although the AP-8 model may not provide an accurate description of the SAA, it is still adequate for making predictions of long-term SEU rate averages [20]. Since the CFE SEU rate calculations are long-term averages, it is not likely that the entire variation between predicted and measured SEU rates on CFE can be completely attributed to limitations of the AP-8 model.

4.3.2 Part Variation

A major factor that may lead to discrepancies between predicted and measured on-orbit SEU rates is the variation among different implementations of circuit designs. Different generations or versions of a circuit may have very similar features and functionality but still have very different low-level characteristics that can affect their response to SEUs. Even seemingly identical parts with the same part number may see variation, as electronic devices implemented in a CMOS process are subject to variations in film thickness, lateral dimensions, and doping concentrations, and these variations can occur from one wafer to another, between dice on the same wafer, or even across a single die [53]. These variations can have a significant impact on the effect of SEUs on both SRAM and SDRAM devices [23, 54].

Peterson notes that part variation is the single largest factor leading to mismatches between predicted and measured SEU rates on orbit, and is an especially large factor when generic part data is used for making predictions for a specific flight part [20], where generic test data is defined in [55] as data obtained from the parts of the same number but not necessarily the same mask set as the fight parts. The authors of [55] highlight the importance of conducting radiation testing on devices of the same lot as those that will actually be used in flight. This counsel is given as a result of the authors' experiences with the APEX Cosmic Ray Upset Experiment, in which they were unable to complete radiation testing on parts from the same lot as the flight part due to funding limitations, and thus based many upset rate predictions on generic data. The authors attributed the unexpected variation in upset rate predictions and measurements of different parts of the same part number to the inadequacy of the radiation testing.

Part variation is a likely explanation for some of the discrepancy between predicted and measured upset rates on CFE. The radiation test data used to make the rate predictions for the Virtex FPGAs was obtained from XRTC testing, and this data would likely be considered generic by the definition given in [55]. The device parameters used to make SDRAM predictions were estimated from published results and should also be considered to be generic. According to [20], predictions made with generic data often lead to large deviations between predictions and measured rates, and any designs based on those predictions

should account for at least a factor of ten underestimation of the SEU rate to allow for worst case conditions.

Some variation in the measured SEU rate has been seen among the nine Virtex FPGAs on CFE. Figure 4.3 shows the SEU rate measured on each payload Virtex FPGA; as shown, the SEU rate ranges from .390 down to .240 SEUs per device day. 95% confidence intervals are also included in the figure to account for the statistical variation in SEU rate that is expected since SEU occurrence is a random process. In general, the per-FPGA SEU rates on CFE are similar, and the rate variations are not statistically significant. The SEU rate of FPGA 3A, however, is considerably higher than the rates of the other FPGAs on CFE, and the difference is large enough to suggest that some other phenomenon besides random variation is responsible for its high SEU rate. Part variation or the location of the part within the satellite are two possible explanations for FPGA 3A's high SEU rate relative to the other payload FPGAs.

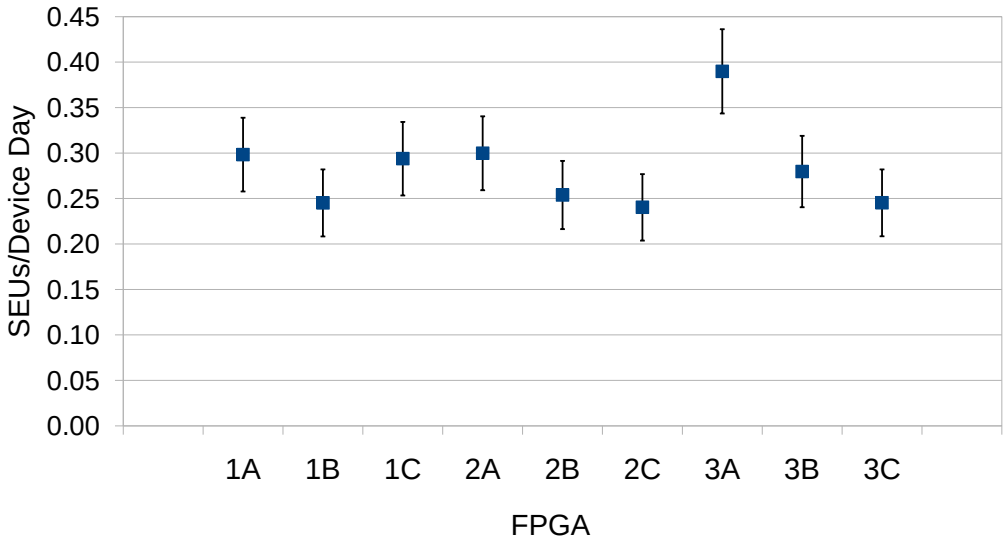

Figure 4.3: 95% confidence intervals for per-FPGA SEU rates

4.3.3 Shielding

Another possible cause in the disagreement between SEU rate predictions and measurements is the effect of shielding of the devices. Peterson states in [20] that the second most probable cause of differences between predicted and measured rates after part variation is the use of incorrect shielding distributions around separate parts. He suggests that shielding should be analyzed with sector analysis for the highest quality SEU rate predictions for a given part. The group responsible for studying single-event effects on the DRAM-based solid state recorders used on NASA's Orbview-2 spacecraft also found that the shielding parameters used had a major effect on the quality of rate predictions [56].

The SEU rate predictions for CFE's FPGAs and SDRAM do not take the specific shielding characteristics of the devices and the spacecraft into account. A shielding distribution from sector analysis as recommended by Peterson was not used in creating the predictions; instead, the CREME96 default value of 100 mils of aluminum shielding was used for all CFE SEU rate predictions. If the shielding of the CFE payload or of the spacecraft itself are more effective at shielding the parts from SEUs than would be expected from the 100 mils aluminum estimate, the predictions would tend to overpredict the SEU rate to some degree. Figure 4.4 shows configuration SEU rate predictions for the CFE payload FPGAs with different shielding thicknesses; as shown, an order of magnitude increase in shielding thickness would in this case lead to a decrease in the prediction of the configuration SEU rate by a factor of about 1.7.

It is likely that several of the factors mentioned above are major contributors to the significant disagreement between CFE's predicted and measured SEU rates. This disagreement highlights the imprecise nature of SEU rate prediction when generic parts and shielding distributions are used to make the predictions. It is thus very important to use such predictions as rough approximations of the environment that will actually be seen from a space-based system. Given the limitations of CFE's rate prediction and similar results seen from other spacecraft using generic data for their rate predictions [20, 55, 56], the factor of 3 SEU rate overprediction made for CFE is a reasonable result.

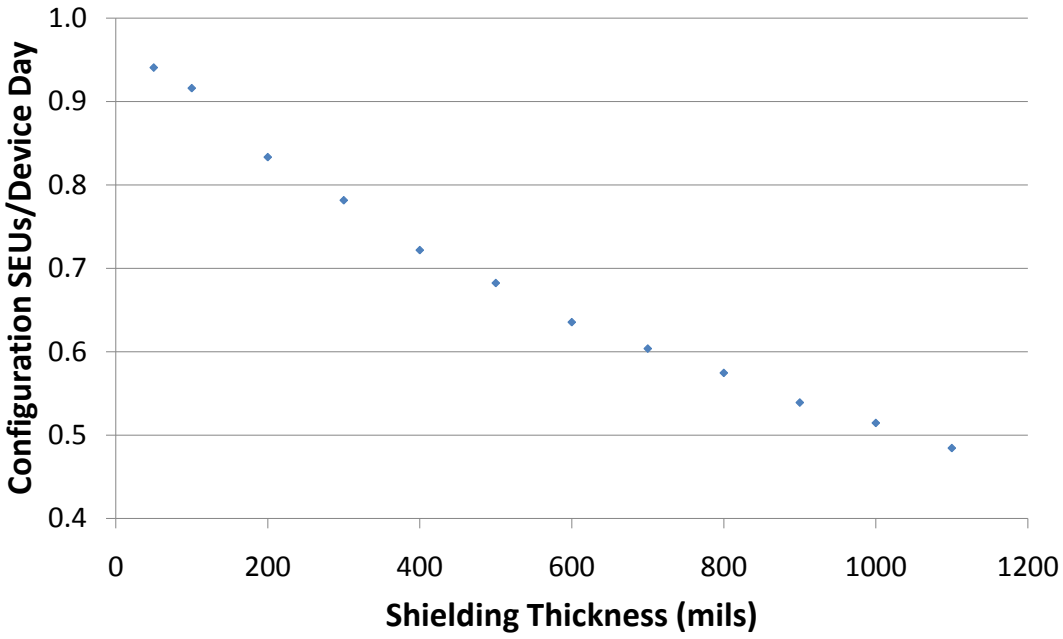

Figure 4.4: Effect of shielding thickness on FPGA SEU rate predictions

4.4 SEFIs In CFE FPGAs

Single event functional interrupts (SEFIs), discussed in detail in Section A.2.1, are SEUs which affect control structures of the device and have unusually dramatic effects. For the Xilinx Virtex FPGAs used in the CFE payload, radiation testing has been used to identify the SEFIs that may affect the devices as well as the rate at which the SEFIs are expected to occur. This radiation testing discovered three distinct types of SEFIs which have a combined cross section of less than $1e^{-5}cm^2$, which is about two one-thousandths of one percent or less of the sensitive cross section of the entire device [57]. This implies that SEFIs should occur very rarely on CFE, with one SEFI occurring for about every 47,600 SEUs that occur within the device, or at a rate of $1.76 \times 10^{-5} SEFIs/D.D.$ based on the CREME96 SEU rate prediction for solar minimum.

On CFE, a SEFI is assumed if any upset event causes a very large number of bits to appear to be upset simultaneously. To date, no SEFIs have been detected in any of CFE's payload FPGAs. This result is consistent with radiation test results, as fewer than 2000 configuration and BRAM SEUs have been detected within CFE FPGAs. As CFE continues

to operate, it is possible that actual SEFIs may be seen, but this is not likely given the very low SEFI rate prediction.

4.5 Multi-Bit Upsets In CFE FPGAs and SDRAM

Although SEUs which occur in electronic devices like FPGAs and SDRAM typically affect the value of only one bit, events do occur in which two or more bits are affected. These SEUs, commonly known as multi-bit upsets (MBUs), do not occur as often as single bit upsets but have been observed in radiation testing in both FPGAs and SDRAM devices. MBUs can be particularly troublesome for SEU mitigation efforts, as many common error correction or masking techniques are limited in their ability to handle multiple upsets at once. For example, two upset bits in a triplicated FPGA circuit can cause two incorrect copies of a circuit structure to erroneously outvote a single correct copy of that structure, allowing incorrect results to be propagated to the rest of the circuit [58]. In addition, some error correcting codes used to protect memory elements such as SDRAM and FPGA BRAM are not guaranteed to operate correctly if more than a single error occurs within a data word [59].

Directed radiation testing using protons and heavy ions has been conducted to estimate the frequency of MBUs in Virtex FPGAs [58]. In the proton testing, .04% of all SEUs detected were determined to be MBUs, and each MBU seen affected two bits. This estimate does not measure any of the SEUs which occurred in the BRAM, however. In each of the MBUs, the upset bits were in different frames of the device's configuration memory. In heavy ion testing, approximately 10%-15% of SEUs in most device resources were MBUs, with BRAM MBUs being more frequent (about 15%-20% of all BRAM SEUs.) No directed radiation testing has been conducted specifically to estimate the occurrence of MBUs in the SDRAM used on CFE; however, because of the small size and high density of SDRAM cells relative to SRAM cells, it would be expected that MBUs would make up a larger percentage of all SDRAM SEUs than of all FPGA SEUs, as discussed in Section 2.1.

Because of the potential problems that MBUs can cause to mitigation efforts, it is desirable to estimate the rate at which MBUs will occur within a space-bound system. Since CREME96 assumes that all upset events are single bit upsets, rate estimations alone cannot

provide for an estimate of how often MBUs are expected to occur. I used MBU-related radiation test data combined with general SEU rate estimations to obtain an MBU rate estimate for the payload FPGAs. These estimates, shown in Table 4.7 are based on the same rate predictions used for the overall SEU rate predictions in Table 4.2. They assume that 12.5% of configuration SEUs and 17.5% of BRAM SEUs caused by heavy ions will be MBUs, while .04% of all SEUs caused by protons will be MBUs.

Table 4.7: CFE FPGA MBU rate predictions

		MBUs/D.D.	
Type of Upset		**SolMin**	**SolMax**
Config	Heavy Ion	1.25E-3	1.02E-3
	Proton	3.31E-4	1.98E-4
	Total	**1.58E-3**	**1.21E-3**
BRAM	Heavy Ion	7.91E-5	6.44E-5
	Proton	1.50E-5	8.92E-6
	Total	**9.41E-5**	**7.33E-5**

4.5.1 Multi-Bit Upsets Observed on CFE

Multiple bit upsets have been observed in both the configuration memory and BRAM of the Virtex FPGAs used in the CFE payload, as well as in the payload SDRAM. Each of the classifications of MBUs have been detected by different circuitry: the configuration MBUs are measured by the CRC-based configuration scrubbing performed by the Actel FPGA on each payload RCC, the BRAM MBUs are measured by the BRAM error detection circuit described in Section 3.4, and the SDRAM SEUs are measured by the SDRAM error detection circuit described in Section 3.5. The MBU rates for FPGA configuration memory, BRAM, and SDRAM are presented in Table 4.8

One factor that limits the accuracy of any MBU measurement is that it is impossible to tell whether multiple upset bits occur due to a single ionizing particle or by the nearly simultaneous effects of multiple particles [58]. If the error detection circuit for the device being scanned operates slowly enough to allow for upsets to accumulate in the device while

Table 4.8: Measured MBU rates on CFE

Type of Upset	Start/End Dates	MBUs	Device Days	MBUs/D.D.
Config	3/8/07 - 1/27/11	6	6254.3	9.59E-4
BRAM	7/15/08 - 1/27/11	2	4361.4	4.59E-4
SDRAM	9/3/09 - 1/27/11	142	15928.6	8.91E-3

it is being scanned, some independent upsets may be mis-classified as being due to an MBU. However, the upset rate on CFE is low relative to the rate at which the FPGA configuration, BRAM, and SDRAM are scrubbed. The scrubbing period for these devices is on the order of milliseconds, while even the extreme worst case SEU rate predictions for CFE's devices expect around one SEU per hour. The SEU rates actually seen on orbit are much lower than this prediction. Because the scrub rate is so much higher than the device SEU rates, adjacency information of the bits upset in an event can in general reveal whether the event was caused by a single particle or by multiple particles, as it is very unlikely that multiple particles will cause simultaneous upsets in adjacent bits of the same device.

CFE's configuration scrubbing has allowed for measurement of the rate at which MBUs occur within the configuration memory of the payload FPGAs. Five events were detected by the configuration scrubbing system in which simultaneous SEUs were detected in adjacent frames. This is consistent with the MBUs observed in radiation testing; the architecture of the Virtex device is such that bits which configure the behavior of the lookup tables associated with adjacent frames share a well, which makes them more susceptible to MBUs. The configuration scrubbing system has been operational for 6254.3 FPGA device days, which corresponds to a configuration MBU rate of 9.59×10^{-4} MBUs per FPGA device day and is reasonably close to the predicted rate of $1.58 \times 10^{-3} MBUs/D.D.$ for solar minimum, especially considering that the the predicted rate is based on an FPGA SEU rate overprediction.

The BRAM error detection and correction circuitry used on CFE is capable of detecting any BRAM upset events which result in more than one upset bit. During this circuit's 4361.4 FPGA device days of operation, two MBUs events were detected. In one of the events, two BRAM bits were upset. In the other event, multiple upset bits were detected, but the

Table 4.9: Number of SDRAM bits upset
for SDRAM events on CFE

Bits Upset	1	2	3	4	5	6	7	8	>8
Events	2023	119	16	4	1	0	1	0	1

exact number of bits was not reported since that version of the BRAM circuitry did not include an error counter. The MBU rate measured during the BRAM test's time of operation on CFE is $4.59 \times 10^{-4} MBUs/D.D.$, which is considerably higher than the predicted rate of $9.41 \times 10^{-5} MBUs/D.D.$ Although this rate is high, it is not unreasonable compared to the prediction, especially since the measured rate is based on only two events.

The SDRAM error detection and correction circuitry is capable of counting the number of upset bits within an SDRAM device and can thus detect potential MBUs that occur within the SDRAM devices on CFE. In contrast with the MBUs found within the payload FPGAs, the MBUs are much more frequent, as would be expected, and the events are not limited to double bit upsets. Table 4.9 summarizes the SDRAM MBU events observed on CFE. There have been 142 SDRAM MBUs observed on CFE to date, and 22 of these upsets consisted of three or more upset bits. As the SDRAM error detection experiments capable of detecting MBUs have operated on CFE for a total of 15928.6 SDRAM device days, the SDRAM MBU rate measured on CFE is $8.91 \times 10^{-3} MBUs/D.D.$.

4.6 CFE SEU Rate and the South Atlantic Anomaly

A key observation that can be made from the SEU rate information measured on CFE is that the South Atlantic Anomaly has a dramatic effect on the SEU rate of both the payload FPGAs and SDRAM. As was discussed in Section 2.1, the SAA is the area where the earth's inner radiation belt comes closest to the surface of the earth due to irregularities in the geomagnetic field. Many spacecraft in low-earth orbit pass through the SAA during the orbit and are thus subject to the trapped protons and other particles that are abundant in the inner radiation belt. For this reason, proton-induced SEUs occur at a very high rate

in electronic devices operating in the SAA, and the SEU rate within the SAA generally dominates the rate seen outside of that region for low-earth orbits.

Because of the location information sent to the ground with CFE's packets, it is possible to keep track of the amount of time that the satellite spends detecting upsets in a certain geographical area as well as any SEUs that occur during that time. In order to measure the SEU rates for the SAA and outside of the SAA on CFE, it is also necessary to have an estimate of the geographic area considered to be part of the SAA. Because the SAA does not have the same characteristics throughout, changes over time, and varies with altitude, the accuracy of such an estimate is limited by the age of measured data used to develop the estimate and the orbit of the spacecraft used to measure the SAA. Figure 4.5 shows an estimate of the area of the SAA derived from the Compact Environment Anomaly Sensor (CEASE) on the Tri-Service Experiment-5 (TSX-5) satellite [60]. This estimate was created with data gathered 1-7 years before CFE's launch in a lower altitude than CFE's orbit (400 km, as opposed to CFESat's altitude of 560 km), but it still provides a reasonable estimate of the SAA for CFE SEU rate measurements. For the purposes of this work, the SAA is considered to be the area that falls within a polygon with 15 vertices which is based on the estimation of the SAA measured by CEASE. This area is presented graphically in Figure 4.6. However, the composition of the SAA is not identical throughout; this is reflected by the boundaries on Figure 4.5 which denote various levels of proton flux. These boundaries represent the contours (starting from center) of $\frac{1}{3}$ maximum, $\frac{1}{10}$ maximum, and 3 standard deviations above background level [60].

Figures 4.7 and 4.8 show the location of occurrence for all FPGA configuration SEUs on CFE and regional SEU rate for areas in the vicinity of the SAA, respectively. Figure 4.7 clearly shows that the vast majority of SEUs on CFE have occurred within the SAA and that the distribution of upsets is not equal even within the SAA estimate, as expected. This uneven distribution is further seen in Figure 4.8. At the core of the SAA, the SEU rate approaches 10 SEUs per FPGA device day in certain areas, and the rate gradually decreases at increasing distance from that core.

The SAA and non-SAA SEU rates for CFE's payload FPGAs (configuration memory and BRAM) and SDRAM are presented in Tables 4.10-4.12. It is clear that for each type of

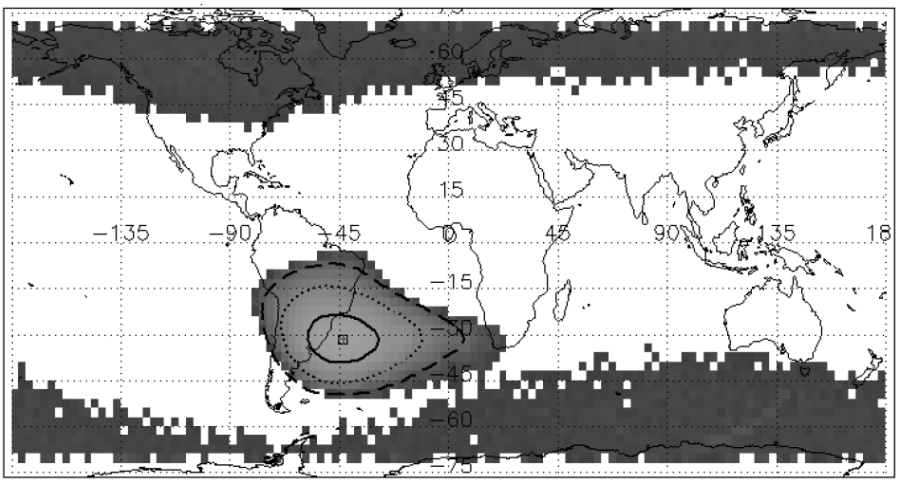

Figure 4.5: The South Atlantic Anomaly, as measured by CEASE on TSX-5 from 2000-2006. From [60]

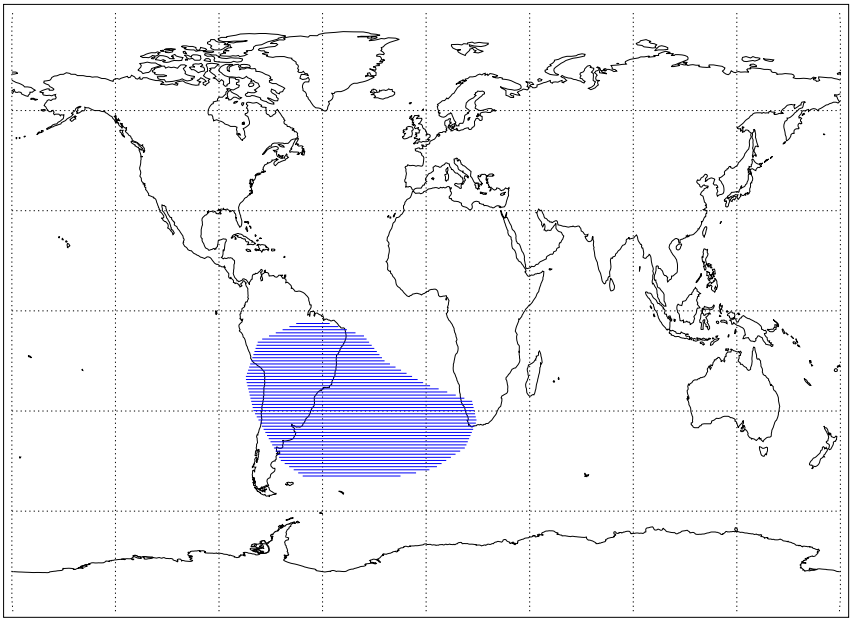

Figure 4.6: The estimate of the South Atlantic Anomaly used for SAA-related SEU rates presented in this work

SEU, the SEU rate is much greater inside the SAA, as each SAA rate is approximately two orders of magnitude larger than its corresponding outside-SAA rate. Even though the satellite only spends about 10% of its orbit time inside the SAA, about 93% of the

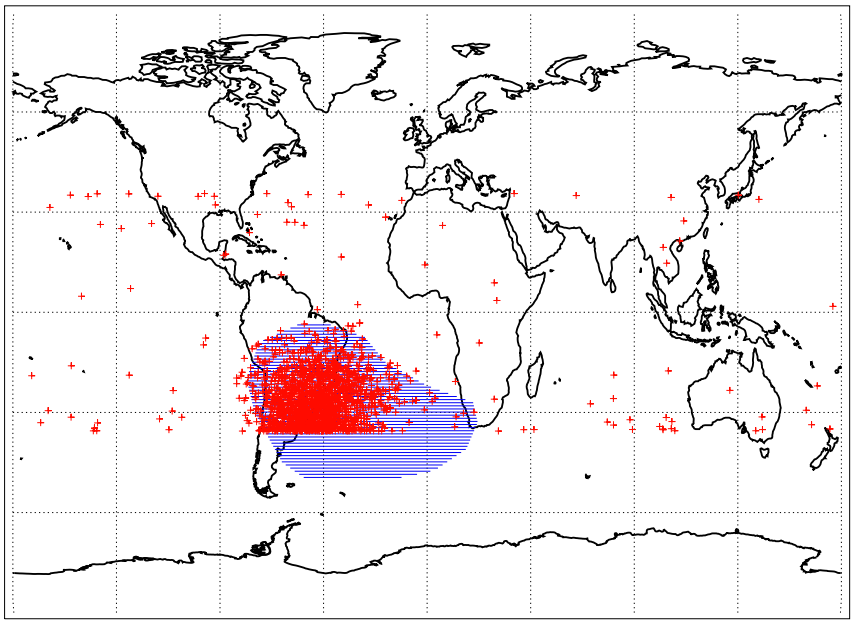

Figure 4.7: FPGA SEUs detected on CFE

configuration SEUs, 95% of the BRAM SEUs, and 95% of the SDRAM SEUs have occurred within the region.

Table 4.10: Effect of SAA on CFE FPGA config SEU rate
(March 8, 2007 - January 27, 2011)

	Device Days	**Config SEUs**	**SEUs/D.D.**
SAA	641.4	1638	2.55E0
Outside SAA	5612.9	132	2.35E-2

One interesting phenomenon that arises from the large difference in SEU rate inside and outside of the SAA is that a periodicity in the occurrence of SEUs is evident as the satellite passes through the SAA at regular intervals. Figure 4.9 is a histogram of the time elapsed between configuration SEUs in CFE's payload FPGAs (when fewer than 10^5 seconds, or nearly 28 hours), and Figure 4.10 is essentially a close-up of the first tenth of Figure 4.9 to more clearly show the first two peaks. The recurring peaks of the histograms correspond to the periodic occasions where the spacecraft passes through the SAA and is thus subject

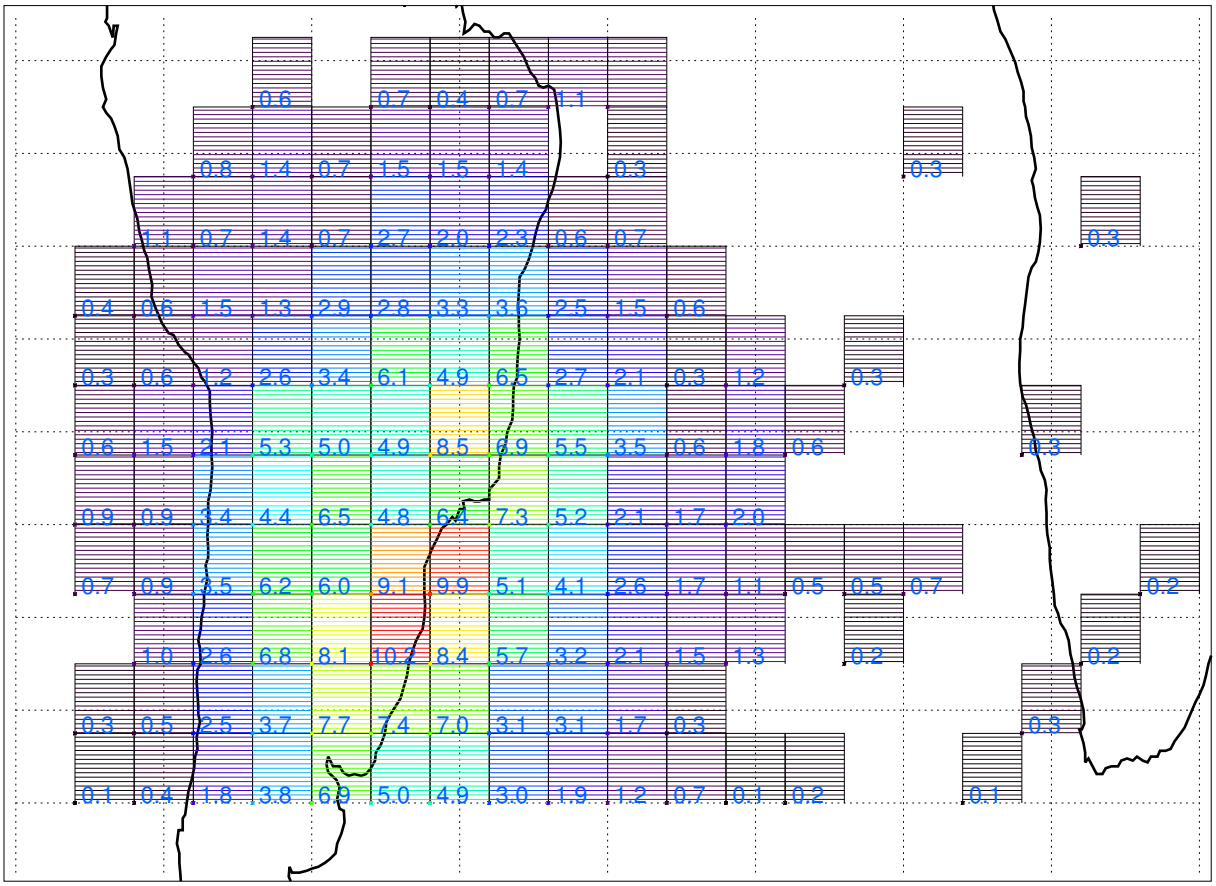

Figure 4.8: CFE FPGA SEU rate by region, in the vicinity of the SAA.

Table 4.11: Effect of SAA on CFE BRAM SEU rate
(July 15, 2008 - January 27, 2011)

	BRAM Device Days	**BRAM Upset Events**	**BRAM Events/D.D.**
Inside SAA	608.4	108	1.77E-1
Outside SAA	3752.8	6	1.60E-3

to a much higher SEU rate. The distance between the histogram peaks corresponds roughly to the 95.8 minute period of the CFE orbit, although the peaks are not all evenly spaced due to precession of the orbit [32].

Table 4.12: Effect of SAA on CFE SDRAM SEU rate
(September 3, 2009 - January 27, 2011)

	SDRAM Device Days	**SDRAM Upset Events**	**SDRAM Events/D.D.**
Inside SAA	2064.5	2054	9.95E-1
Outside SAA	13864.1	111	8.01E-3

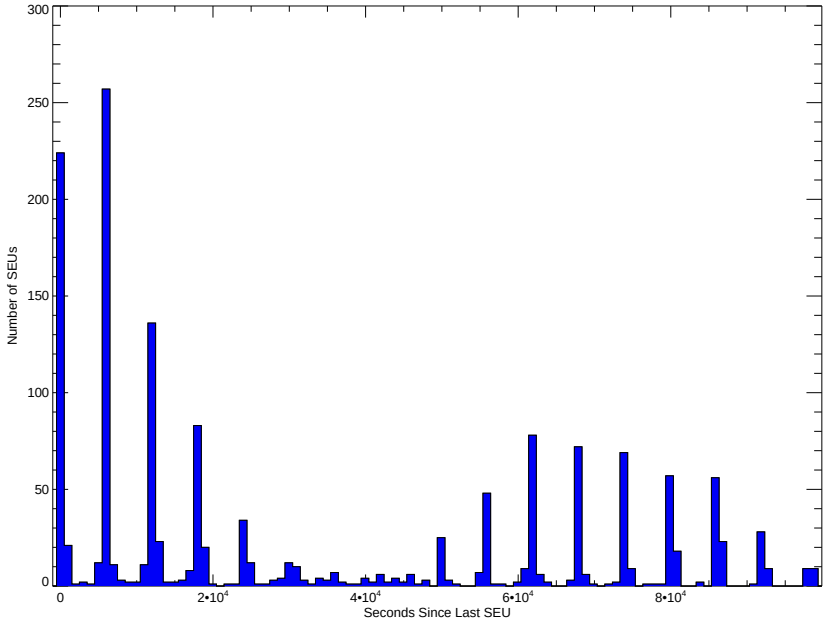

Figure 4.9: Histogram of time elapsed since last SEU (when less then 10^5 seconds)

4.7 Change in CFE SEU Rate With Solar Cycles

Another phenomenon that can be observed with analysis of the CFE SEU rate is the effect of the solar cycle on the rates in the near-earth space environment. The amount of solar activity varies over time in a periodic fashion, as discussed in Section 2.1. These solar cycles have a great influence on the concentrations and energies of both trapped particles and cosmic rays that can cause SEUs in electronic devices in space. In low-earth orbit environments like that in which CFE operates, trapped protons in the earth's inner radiation belt are the most common cause of SEUs. Since the trapped proton population in the inner radiation belt is highest when interactions with particles in the upper atmosphere are less frequent, the SEU rate in low-earth orbit environments tends to be higher during solar minimum than

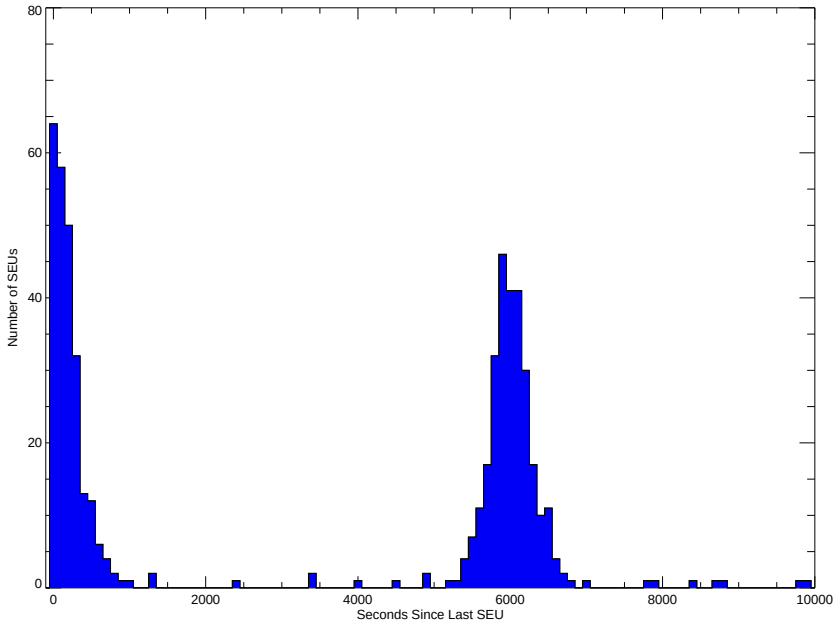

Figure 4.10: Histogram of time elapsed since last SEU (when less then 10^4 seconds)

during solar maximum. Recent work [61, 62] has found that the peak proton flux in the inner radiation belt follows solar minimum by about 1-2 years, which indicates that the low-earth orbit SEU rate should be highest at about this time.

CREME96 SEU rate predictions take into account to some degree the effect of the solar cycle on the SEU rate. As shown in Table 4.2, the SEU rate predictions are calculated for several different solar conditions. The solar minimum and solar maximum predictions are the best estimates of long-term, orbit-averaged SEU rates, and as expected, the predicted SEU rate during solar maximum is significantly lower than the rate predicted during solar maximum.

CFE's SEU detection and reporting strategy has facilitated the calculation of orbit-averaged SEU rates for specified periods of its lifetime. Figure 4.11 plots the FPGA configuration SEU rate for each three month period of CFE's mission lifetime along with 95% confidence intervals. The smoothed sunspot number over CFE's mission lifetime is also plotted.

As is evident from Figure 4.11, the CFE FPGA SEU rate has in general increased over CFE's mission lifetime. This is consistent with the observation that the peak trapped proton

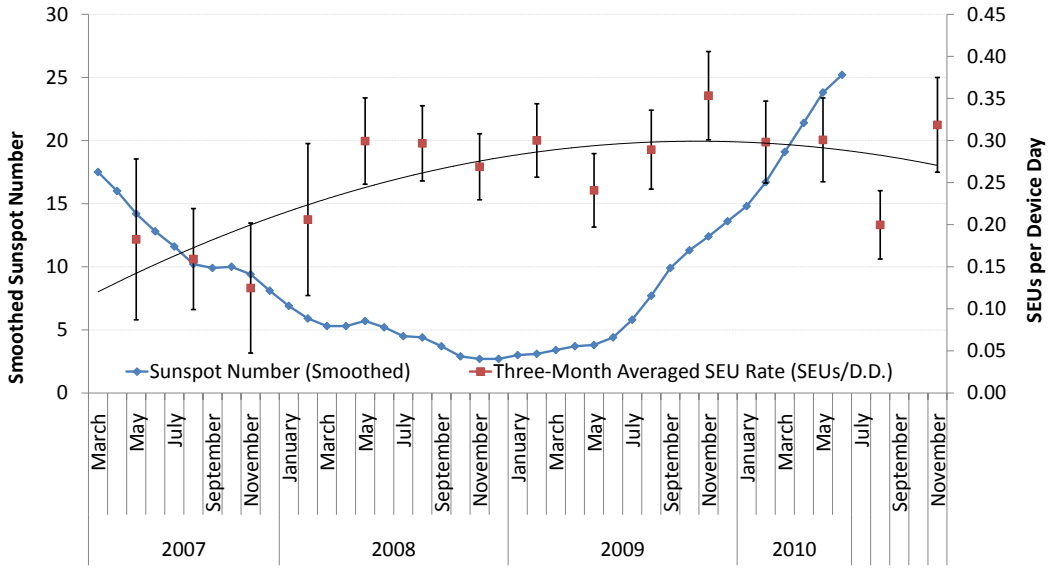

Figure 4.11: Three month FPGA configuration SEU rates

flux in the inner radiation belt occurs a year or two after solar minimum. Since the first solar minimum after CFE's launch occurred in December 2008 [63], it is expected that the SEU rate on CFE will reach a maximum sometime in 2010 or 2011 and then steadily decline until sometime after the next solar maximum, which at the time of writing is expected to occur in May 2013 [63].

4.8 Conclusion

CFE's reconfigurability and system-level FPGA SEU detection strategy have allowed for the calculation and analysis of a variety of SEU rates for CFE's payload FPGAs and SDRAM devices. The SEU rate measurements and analysis presented in this chapter provide snapshots of the near-earth space environment from an orbiting spacecraft; this is a valuable asset to the planning and deployment of future systems bound for orbit, particularly those employing FPGAs.

CHAPTER 5. CONCLUSION

The on-orbit SEU experiments developed in this work and conducted on CFE have contributed to the effort of validating TMR, RPR, DWC, and BRAM and SDRAM scrubbing as suitable for use in the near-earth space environment. The techniques under test have operated correctly for over four thousand FPGA device days and have provided additional confidence in the results of the extensive ground-based efforts to validate SEU mitigation and detection techniques. The proper use of these techniques can make it possible for many future space-based computing systems to reliably use FPGAs and SDRAM to carry out demanding processing tasks.

The SEU rate data calculated from CFE SEU measurement studies and analyzed in this thesis have provided a long-term, detailed insight into the radiation environment seen on CFE. The SEU rate on CFE is significantly lower than was predicted before flight, and this result highlights the imprecise nature of the SEU rate prediction process, especially when generic parts and shielding data are used. The SEU rate measurement on CFE and subsequent analysis presented in this thesis also confirm expectations about the effect of the solar cycle and the SAA on the SEU rate.

CFE's SEU rate data is an important contribution to the effort to understand the effects of space radiation on spacecraft electronics, and the additional knowledge of these effects provided by CFE SEU studies should be a valuable resource to designers of future electronic systems bound for space. In particular, the SEU rate data in this thesis will be publicly available and will be a valuable resource for those seeking to refine the models and methodology used to create SEU rate predictions. All of the SEU-related data measured on CFE and presented in this thesis is current as of January 27, 2011. It is anticipated that updates to the CFE SEU data, including updates to figures and tables presented in this thesis, will be posted on ScholarsArchive, BYU's institutional repository for the scholarly

and creative content produced by the University. ScholarsArchive may be accessed online at http://lib.byu.edu/sites/scholarsarchive/.

There are several avenues for future research relating to the work presented in this thesis. First, CFE's continued operation enables the continuation of both mitigation technique validation and SEU rate measurement studies. CFE's mission lifetime was expected at the time of launch to be three to five years [64]; however, past satellites designed and operated by LANL have worked successfully for longer than expected [65, 66]. The applications developed as part of this work continue to operate regularly on the CFE payload, and the data collected from their continued operation will provide additional confidence in the mitigation technique validation as well as provide a longer-term view into the SEU rate seen on CFE. In particular, as CFE continues to operate throughout the solar cycle, more evidence of the effect of the solar cycle on the SEU rate should become apparent. It may also be possible to observe the slight drift of the SAA as longer-term SEU rate data becomes available. Because of CFE's reconfigurable payload and ability to receive new configurations from the ground, additional applications to test new SEU mitigation or detection techniques for FPGAs or SDRAM could also be developed and deployed.

Another opportunity for future study relates to the use of very small satellites, such as nanosatellites and picosatellites, as platforms for on-orbit SEU studies. On-orbit tests require the use of a satellite for deployment and are thus often very expensive. Using very small satellites such as CubeSats [67] can provide a lower cost option for conducting on orbit tests, as they require much less design effort than larger satellites and can often take advantage of lower-cost launch opportunities. At least one on-orbit FPGA SEU study designed for a picosatellite has been proposed [68], and as CubeSats and other very small satellites become more common, SEU-related studies on these satellites will likely continue to be designed and deployed.

The continued success of CFE, as well as the success and results of the on-orbit SEU studies presented in Chapters 3 and 4, have demonstrated that it is possible to successfully and reliably use SRAM-based FPGAs in space-based high-performance systems if proper precautions are taken. CFE is only one example of an FPGA-based system that has operated successfully in orbit, and new FPGA-based systems bound for space continue to be

developed. More recent spacecraft have been designed to use newer, more powerful FPGAs than those used on CFE [13, 16]. These newer devices have been tested and qualified for use in space [69, 70, 71], allowing for new spacecraft to take advantage of these devices' higher computational performance and their new features such as dedicated microprocessors, digital signal processing blocks, and high-speed serial I/O circuitry [72]. The increasing use of FPGAs in space is improving the ability of spacecraft electronics to perform increasingly more complex processing tasks, and the SEU mitigation and detection techniques validated in this work will contribute to the effort of ensuring that these tasks are carried out in a dependable manner.

REFERENCES

[1] L. Alkalai, J. Klein, and M. Underwood, "The new millennium progam microelectronics systems advanced technology development," in *Proceedings of the 34th Aerospace Science Meeting and Exhibit*, Reno, NV, 1996.

[2] E. R. Prado, P. Prewitt, and E. Ille, "A standard product approach to spaceborne payload processing," in *Proceedings of the 2001 IEEE Aerospace Conference*, Big Sky, MT, March 2001.

[3] J. Ramos, J. Samson, D. Lupia, I. Troxel, J. Subramaniyan, A. Jacobs, J. Greco, G. Cieslewski, J. Curreri, M. Fischer, E. Grobelny, A. George, V. Aggarwal, M. Patel, and R. Some, "High-performance, dependable multiprocessor," in *Proceedings of the 2006 IEEE Aerospace Conference*, Big Sky, MT, March 2006.

[4] M. Caffrey, "A space-based reconfigurable radio," in *Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA)*, T. P. Plaks and P. M. Athanas, Eds. CSREA Press, June 2002, pp. 49–53.

[5] C. Carmichael, M. Caffrey, and A. Salazar, "Correcting single-event upsets through Virtex partial configuration," Xilinx Corporation, Tech. Rep., June 1 2000, XAPP216 (v1.0).

[6] F. Lima, C. Carmichael, J. Fabula, R. Padovani, and R. Reis, "A fault injection analysis of Virtex FPGA TMR design methodology," in *Proceedings of the 6th European Conference on Radiation and its Effects on Components and Sysemts (RADECS 2001)*, 2001.

[7] J. Johnson, W. Howes, M. Wirthlin, D. McMurtrey, M. Caffrey, P. Graham, and K. Morgan, "Using duplication with compare for on-line error detection in FPGA-based designs," in *Proceedings of the 2008 IEEE Aerospace Conference*, March 2008, pp. 1–11.

[8] B. Pratt, Ph.D. dissertation, Brigham Young University, to be published.

[9] A. S. Dawood, S. J. Visser, and J. A. Williams, "Reconfigurable FPGAs for Real Time Image Processing in Space," in *14th International Conference on Digital Signal Processing (DSP 2002)*, vol. 2, 2002, pp. 711–717.

[10] P. Bergsman, "Xilinx FPGA blasted into orbit," *Xilinx Xcell Journal*, Xilinx, Inc., 2003.

[11] M. Santarini, "Xilinx customer innovation: 85,000 to 2.5 billion transistors and beyond," *Xilinx Xcell Journal*, Xilinx, Inc., 2010.

[12] J. W. Bergstrom, W. Delamere, and A. McEwen, "MRO high resolution imaging science experiment (HiRISE) instrument test, calibration and operating constraints," in *Proceedings of the 55th International Astronautical Congress*, Vancouver, Canada, October 2004.

[13] "Mars exploration rovers celebrate 6 years on red planet," *Xilinx Xcell Journal*, Xilinx, Inc., 2010.

[14] B. Fiethe, H. Michalik, C. Dierker, B. Osterloh, and G. Zhou, "Reconfigurable system-on-chip data processing units for space imaging instruments," in *Proceedings of the 2007 Conference on Design, Automation, and Test in Europe (DATE)*, Nice, France, 2007.

[15] SpaceCube to debut in flight demonstration. NASA Goddard Space Flight Center. [Online]. Available: http://technology.gsfc.nasa.gov/SpaceCube.htm

[16] "Tiny FPGA-based computer accelerates space exploration," *Xilinx Xcell Journal*, Xilinx, Inc., 2010.

[17] "Breaking the logjam: Improving data download from outer space," *Scientific Computing*, April. [Online]. Available: http://www.scientificcomputing.com/news-HPC-Breaking-the-Logjam-Improving-data-download-from-outer-space-052510.aspx

[18] D. P. Stern and M. Peredo. (2004, September) The exploration of the earth's magnetosphere. NASA Goddard Space Flight Center. [Online]. Available: http://www-istp.gsfc.nasa.gov/Education/Intro.html

[19] "Hubble achieves milestone: 100,000th exposure," News Release, Space Telescope Science Institute, July 1996. [Online]. Available: http://hubblesite.org/newscenter/archive/releases/1996/25/text/

[20] E. Peterson, "Predictions and observations of SEU rates in space," *IEEE Transactions on Nuclear Science*, vol. 44, no. 6, pp. 2174–2187, 1997.

[21] D. E. Johnson, "Estimating the dynamic sensitive cross section of an FPGA design through fault injection," Master's thesis, Brigham Young University, August 2005.

[22] L. W. Massengill, "Cosmic and terrestrial single-event radiation effects in dynamic random access memories," *IEEE Transactions on Nuclear Science*, vol. 43, no. 2, pp. 576–593, April 1996.

[23] R. Ladbury, "SDRAM single-event error modes - characterization, rate calculation and mitigation," in *Proceedings of the 5th Annual International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, Laurel, MD, September 2002, Presentation.

[24] A. J. Tylka, J. H. Adams, P. R. Boberg, B. Brownstein, W. F. Dietrich, E. O. Flueckiger, E. L. Petersen, M. A. Shea, D. F. Smart, and E. C. Smith, "CREME96: A

revision of the cosmic ray effects on micro-electronics code," *IEEE Transactions on Nuclear Science*, vol. 44, no. 6, pp. 2150–2160, December 1997.

[25] D. Roussel-Dupré, 2010, personal correspondence.

[26] "RAD6000 space computers," BAE Systems, Manassas, VA, Datasheet PUBS-06-A49, 2006.

[27] "Radiation hardened Virtex 2.5V radiation-hardened FPGAs," Xilinx, Inc., San Jose, CA, Datasheet DS028, January 2010.

[28] "RTSX-S radtolerant FPGAs," Actel Corporation, Mountain View, CA, Datasheet 5172151-11/11.04, November 2004.

[29] M. Caffrey, K. Morgan, D. Roussel-Dupré, S. Robinson, A. Nelson, A. Salazar, M. Wirthlin, W. Howes, and D. Richins, "On-orbit flight results from the reconfigurable Cibola Flight Experiment satellite (CFESat)," in *Proceedings of the 17th IEEE Symposium on Field Programmable Custom Computing Machines (FCCM '09)*, April 2009.

[30] K. S. Morgan, M. Caffrey, P. Graham, E. Johnson, B. Pratt, and M. Wirthlin, "SEU-induced persistent error propagation in FPGAs," *IEEE Transactions on Nuclear Science*, vol. 52, no. 6, pp. 2438–2445, December 2005.

[31] P. Davies, J. Buckley, M. Sweeting, D. Roussel-Dupré, and M. Caffrey, "Cibola flight experiment satellite," in *Proceedings of the 4S Symposium: Small Satellites, Systems and Services*, September 2004.

[32] M. Caffrey, K. Katko, A. Nelson, J. Palmer, S. Robinson, D. Roussel-Dupré, A. Salazar, M. Wirthlin, W. Howes, and D. Richins, "The Cibola Flight Experiment," in *Proceedings of the 23rd Annual Small Satellite Conference*, August 2009.

[33] H. Quinn, P. Graham, and B. Pratt, "An automated approach to estimating hardness assurance issues in triple-modular redundancy circuits in xilinx FPGAs," *IEEE Transactions on Nuclear Science*, vol. 55, no. 6, pp. 3070–3076, 2008.

[34] E. Johnson, M. J. Wirthlin, and M. Caffrey, "Single-event upset simulation on an FPGA," in *Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA)*, T. P. Plaks and P. M. Athanas, Eds. CSREA Press, June 2002, pp. 68–73.

[35] C. Carmichael, E. Fuller, J. Fabula, and F. D. Lima, "Proton testing of SEU mitigation methods for the Virtex FPGA," in *Proceedings of the 4th Annual International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, 2001.

[36] B. Pratt, M. Caffrey, J. F. Carroll, P. Graham, K. Morgan, and M. Wirthlin, "Fine-grain SEU mitigation for FPGAs using partial TMR," *IEEE Transactions on Nuclear Science*, vol. 55, no. 4, pp. 2274–2280, August 2008.

[37] N. Rollins, M. Wirthlin, P. Graham, and M. Caffrey, "Evaluating TMR techniques in the presence of single event upsets," in *Proceedings of the 6th Annual International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, September 2003.

[38] B. Pratt, M. Caffrey, P. Graham, E. Johnson, K. Morgan, and M. Wirthlin, "Improving FPGA design robustness with partial TMR," in *Proceedings of the IRPS Conference*, March 2006.

[39] K. Morgan, D. McMurtrey, B. Pratt, and M. Wirthlin, "A comparison of TMR with alternative fault-tolerant design techniques for FPGAs," *IEEE Transactions on Nuclear Science*, vol. 54, no. 6, pp. 2065–2072, December 2007.

[40] L. Sterpone and M. Violante, "A new analytical approach to estimate the effects of SEUs in TMR architectures implemented through SRAM-based FPGAs," *IEEE Transactions on Nuclear Science*, vol. 52, no. 6, pp. 2217–2223, 2005.

[41] M. Alderighi, F. Casini, S. D'Angelo, M. Mancini, S. Pastore, and G. Sechi, "Evaluation of single event upset mitigation schemes for SRAM based FPGAs using the FLIPPER fault injection platform," in *Proceedings of the 2007 IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems*, Rome, Italy, September 2007, pp. 105–113.

[42] D. L. McMurtrey, "Using duplication with compare for on-line error detection in FPGA-based designs," Master's thesis, Brigham Young University, December 2006.

[43] N. Rollins, M. Fuller, and M. Wirthlin, "A comparison of fault-tolerant memories in SRAM-based FPGAs," in *Proceedings of the 2010 IEEE Aerospace Conference*, March 2010.

[44] Y. Li, B. Nelson, and M. Wirthlin, "Synchronization issues of TMR crossing multiple clock domains," in *Proceedings of the 12th Annual International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, Greenbelt, MD, September 2009.

[45] B. Shim, S. Sridhara, and N. Shanbhag, "Reliable low-power digital signal processing via reduced precision redundancy," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 5, 2004, pp. 497–510.

[46] J. D. Engel, M. J. Wirthlin, K. S. Morgan, and P. S. Graham, "Predicting on-orbit static single event upset rates in Xilinx Virtex FPGAs," Los Alamos National Laboratory and Brigham Young University, Tech. Rep., November 2006.

[47] E. Fuller, M. Caffrey, P. Blain, C. Carmichael, N. Khalsa, and A. Salazar, "Radiation test results of the Virtex FPGA and ZBT SRAM for space based reconfigurable computing," in *MAPLD Proceedings*, September 1999.

[48] Single-event effects consortium. Xilinx Inc. [Online]. Available: http://www.xilinx.com/esp/aero_def/see.htm

[49] E. Peterson, J. Pickel, J. Adams, and E. Smith, "Rate prediction for single event effects - a critique," *IEEE Transactions on Nuclear Science*, vol. 39, no. 6, pp. 1577–1599, 1992.

[50] H. K. Aage and P. B. Guldager, "Proton testing of micro advanced stellar compass TEC-QCA support activity to PROBA-II," in *Proceedings of the 8th ESA/ESTEC D/TEC-QCA Final Presentation Day*, January 2007.

[51] D. Sawyer and J. Vette, "AP-8 trapped proton environment for solar maximum and solar minimum," NASA Goddard Space Flight Center, Tech. Rep., December 1 1976.

[52] B. Sierawski. (2007) Important limitations of the trp trapped proton module. Vanderbilt University School of Engineering. [Online]. Available: https://creme-mc.isde.vanderbilt.edu/CREME-MC/help/important-limitations-of-the-trp-trapped-proton-module

[53] N. H. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 3rd ed. Pearson Education, September 2005.

[54] P. Dodd, F. Sexton, G. Hash, M. Shaneyfelt, B. Draper, A. Farino, and R. Flores, "Impact of technology trends on SEU in CMOS SRAMs," *IEEE Transactions on Nuclear Science*, vol. 43, no. 6, pp. 2797–2804, 1996.

[55] J. Adolphsen, J. Barth, E. Stassinopoulos, T. Gruner, M. Wennersten, K. LaBel, and C. Seidleck, "SEE data from the APEX cosmic ray upset experiment: predicting the performance of commercial devices in space," in *Proceedings of the 3rd European Conference on Radiation and its Effects on Components and Sysemts (RADECS 1995)*, 1995.

[56] C. Poivey, J. Barth, K. LaBel, G. Gee, and H. Safren, "In-flight observations of long-term single-event effect (SEE) performance on Orbview-2 solid state recorders (SSR)," in *Proceedings of the 2003 IEEE Radiation Effects Data Workshop*, July 2003, pp. 102–107.

[57] M. Caffrey, P. Graham, E. Johnson, M. Wirthlin, N. Rollins, and C. Carmichael, "Single-event upsets in SRAM FPGAs," in *Proceedings of the International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, Laurel, MD, September 2002.

[58] H. Quinn, P. Graham, J. Krone, M. Caffrey, S. Rezgui, and C. Carmichael, "Radiation-induced multi-bit upsets in Xilinx SRAM-based FPGAs," in *Proceedings of the International Conference on Military and Aerospace Programmable Logic Devices (MAPLD)*, Washington, D.C., September 2005.

[59] W. W. Peterson and E. Weldon, *Error-Correcting Codes*, 2nd ed. MIT Press, 1972.

[60] G. Ginet, D. Madden, B. Dichter, and D. Brautigam, "Energetic proton maps for the South Atlantic Anomaly," in *Radiation Effects Data Workshop, 2007 IEEE*, 2007, pp. 1 –8.

[61] S. Huston, G. Kuck, and K. Pfitzer, "Solar cycle variation of the low-altitude trapped proton flux," *Advances in Space Research*, vol. 21, no. 12, pp. 1625–1634, 1998.

[62] N. Kuznetsov, N. Nikolaeva, and M. Panayuk, "Variation of the trapped proton flux in the inner radiation belt of the earth as a function of solar activity," *Cosmic Research*, vol. 48, no. 1, pp. 80–85, 2010.

[63] (2010) Solar cycle progression. The NOAA/Space Weather Prediction Center. [Online]. Available: http://www.swpc.noaa.gov/SolarCycle/index.html

[64] "The Cibola satellite tests a reconfigurable supercomputer," *1663: Los Alamos Science and Technology Magazine*, Los Alamos National Laboratory, pp. 8–11, May 2007.

[65] D. Roussel-Dupré, P. Klingner, L. Carlson, R. Dingler, D. Esch-Mosher, and A. R. Jacobson, "Four years of operations and results with FORTE," in *Proceedings of the 2001 AIAA Space Conference and Exposition*, Albuquerque, NM, August 2001.

[66] D. Roussel-Dupré, J. Bloch, C. Little, R. Dingler, B. Dunne, S. Fletcher, M. Kennison, K. Ramsey, R. King, and J. Sutton, "ALEXIS, the little satellite that could - 4 years later," in *11th Annual AIAA Conference on Small Satellites*, Logan, UT, September 1997.

[67] H. Heidt, J. Puig-Suari, A. S. Moore, S. Nakasuka, and R. J. Twiggs, "CubeSat: A new generation of picosatellite for education and industry low-cost space experimentation," in *14th Annual USU Conference on Small Satellites*, Logan, UT, 2001.

[68] S. G. Ambat, "Single event upset detection in field programmable gate arrays," Master's thesis, University of Kentucky, February 2008.

[69] H. M. Quinn, P. S. Graham, M. J. Wirthlin, B. Pratt, K. S. Morgan, M. P. Caffrey, and J. B. Krone, "A test methodology for determining space readiness of Xilinx SRAM-based FPGA devices and designs," *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 10, pp. 3380–3395, 2009.

[70] Space-grade virtex-4qv fpgas. Xilinx. [Online]. Available: http://www.xilinx.com/products/v4qv/index.htm

[71] Space-grade virtex-5qv fpga. Xilinx. [Online]. Available: http://www.xilinx.com/products/virtex5qv/index.htm

[72] Xilinx, "Virtex-4 family overview," Xilinx, Inc., San Jose, CA, Product Specification DS112, September 2007.

[73] K. S. Morgan, "SEU-induced persistent error propagation in FPGAs," Master's thesis, Brigham Young University, August 2006.

[74] T. Bevill. (2008, August) What is space radiation? Space Radiation Analysis Group, NASA Johnson Space Center. [Online]. Available: http://srag-nt.jsc.nasa.gov/SpaceRadiation/What/What.cfm

[75] D. P. Stern. (2004, September) Birth of a radiation belt. NASA Goddard Space Flight Center. [Online]. Available: http://www-istp.gsfc.nasa.gov/Education/wbirthrb.html

[76] X. Li, D. Baker, M. Temerin, D. Larson, R. Lin, G. Reeves, M. Looper, S. Kanekal, and R. Mewaldt, "Are energetic electrons in the solar wind the source of the outer radiation belt?" *Geophysical Research Letters*, vol. 24, no. 8, pp. 923–926, 1997.

[77] X. Li and M. A. Temerin, "The electron radiation belt," *Space Science Reviews*, vol. 95, no. 1-2, pp. 569–580, January 2002.

[78] M. Sims, A. Sims, R. Bentley, P. Guttridge, and J. Gourlay, "Measured single event upset rates in low earth orbit for the ROSAT wide field camera," *Nuclear Instruments and Methods in Physics Research*, vol. 329, no. 1, pp. 329–336, 1993.

[79] ROSAT SAA. NASA Goddard Space Flight Center. [Online]. Available: http://heasarc.nasa.gov/docs/rosat/gallery/misc_saad.html

[80] J. Heirtzler, "The future of the South Atlantic anomaly and implications for radiation damage in space," *Journal of Atmospheric and Solar-Terrestrial Physics*, vol. 64, no. 16, pp. 1701–1708, 2002.

[81] N. Trivedi, B. Pathan, N. Schuch, M. Barreto, and L. Dutra, "Geomagnetic phenomena in the South Atlantic Anomaly region in Brazil," *Advances in Space Research*, vol. 36, no. 10, pp. 2021–2024, 2005.

[82] G. D. Badhwar, "Drift rate of the South Atlantic Anomaly," *Journal of Geophysical Research*, vol. 102, no. A2, pp. 2343–2349, 1997.

[83] F. Furst, J. Williams, R. E. Rothschild, K. Pottschmidt, D. M. Smith, and R. Lingenfelter, "Temporal variations of strength and location of the South Atlantic Anomaly as measured by RXTE," *Earth and Planetary Science Letters*, vol. 281, no. 3-4, pp. 125–133, May 2009.

[84] M. Wirthlin, E. Johnson, N. Rollins, M. Caffrey, and P. Graham, "The reliability of FPGA circuit designs in the presence of radiation induced configuration upsets," in *Proceedings of the 2003 IEEE Symposium on Field-Programmable Custom Computing Machines*, K. Pocek and J. Arnold, Eds., IEEE Computer Society. Napa, CA: IEEE Computer Society Press, April 2003, pp. 133–142.

[85] S. L. Clark, K. Avery, and R. Parker, "TID and SEE testing results of Altera Cyclone field programmable gate array," in *Proceedings of the 2004 IEEE Radiation Effects Data Workshop*, Atlanta, GA, July 2004, pp. 88–90.

[86] C. Yui, G. Swift, C. Carmichael, R. Koga, and J. George, "SEU mitigation testing of Xilinx Virtex II FPGAs," in *Proceedings of the 2003 IEEE Radiation Effects Data Workshop*, July 2003, pp. 92–97.

[87] M. W. Stettler, M. P. Caffrey, P. S. Graham, and J. B. Krone, "Radiation effects and mitigation strategies for modern FPGAs," in *Proceedings of the 10th Workshop on Electronics for LHC and Future Experments*, January 2004.

[88] "Actel's radiation-tolerant flash based FPGAs now qualified for spaceflight systems," News release, Actel Corporation, July 2010. [Online]. Available: http://www.actel.com/company/press/2010/7/19/4

[89] Xilinx, "Radiation hardened Virtex-II QPRO 1.5V platform FPGAs: Introduction and overview," Xilinx, Inc., San Jose, CA, Datasheet DS124-1, July 2003.

[90] Atmel, "ATF280F advance information, revision B," Atmel Corporation, San Jose, CA, Advance Information 7750B-AERO, December 2009.

[91] S. Guertin, J. Patterson, and D. Nguyen, "Dynamic SDRAM SEFI detection and recovery test results," in *Proceedings of the 2004 IEEE Radiation Effects Data Workshop*, Atlanta, GA, July 2004, pp. 62–67.

[92] L. Edmonds and L. Scheick, "Physical mechanisms of ion-induced stuck bits in the Hyundai 16M x 4 SDRAM," *IEEE Transactions on Nuclear Science*, vol. 55, no. 6, pp. 3265–3271, 2008.

[93] Maxwell, "D8SD1616 datasheet, revision 4," Maxwell Technologies, Inc., San Diego, CA, Datasheet 01.07.05REV4, January 2005.

[94] L. Edmonds, L. Scheick, D. Nguyen, and G. Swift, "Ion-induced stuck bits in 1 T/1 C SDRAM cells," *IEEE Transactions on Nuclear Science*, vol. 48, no. 6, pp. 1925–1930, 2001.

[95] D. Chenette, J. Chen, E. Clayton, T. Guzik, J. Wefel, M. Garcia-Munoz, C. Lopate, K. Pyle, K. Ray, E. Mullen, and D. Hardy, "The CRRES/SPACERAD heavy ion model of the environment (CHIME) for cosmic ray and solar particle effects on electronic and biological systems in space," *IEEE Transactions on Nuclear Science*, vol. 41, no. 6, pp. 2332–2339, 1994.

[96] J. Vette, "The AE-8 trapped electron model environment," NASA Goddard Space Flight Center, Tech. Rep., 1991.

[97] M. Ceschia, M. Violante, M. Sonza Reorda, A. Paccagnella, P. Bernardi, M. Rebaudengo, D. Bortolato, M. Bellato, P. Zambolin, and A. Candelori, "Identification and classification of single-event upsets in the configuration memory of SRAM-based FPGAs," *IEEE Transactions on Nuclear Science*, vol. 50, no. 6, pp. 2088–2094, 2003.

[98] R. Koga, "Single event effect ground test issues," *IEEE Transactions on Nuclear Science*, vol. 43, no. 2, pp. 661–670, 1996.

[99] M. Berg, C. Perez, and H. Kim, "Investigating mitigated and nonmitigated multiple clock domain circuitry in Xilinx Virtex-4 field programmable gate arrays," in *Proceedings of the Single-Event Effects Symposium*, 2008.

[100] H. Quinn, K. Morgan, P. Graham, J. Krone, and M. Caffrey, "Static proton and heavy ion testing of the Xilinx Virtex-5 device," in *Proceedings of the 2007 IEEE Radiation Effects Data Workshop*, Honolulu, HI, July 2007, pp. 177–184.

[101] L. Massengill, "SEU modeling and prediction techniques," *IEEE Nuclear and Space Radiation Effects Conference Short Course*, pp. 1–93, 1993.

[102] N. Ambrosiano, "Cibola Flight Experiment prepares for October launch," *Los Alamos Newsletter*, Los Alamos National Laboratory, vol. 7, no. 14, July 2006.

[103] C. Carmichael, "Triple module redundancy design techniques for Virtex FPGAs," Xilinx Corporation, Tech. Rep., November 1, 2001, XAPP197 (v1.0).

[104] P. Graham, M. Caffrey, D. Johnson, N. Rollins, and M. Wirthlin, "SEU mitigation for half-latches in Xilinx Virtex FPGAs," *IEEE Transactions on Nuclear Science*, vol. 50, no. 6, pp. 2139–2146, 2003.

[105] N. Ambrosiano, "Supercomputing satellite hits the road," News release, Los Alamos National Laboratory, August 2006. [Online]. Available: http://www.lanl.gov/news/index.php/fuseaction/home.story/story_id/8916

[106] J. Wisecup, "Historic launch puts six satellites into orbit at once," News release, Kirtland Air Force Base, March 2007. [Online]. Available: http://www.kirtland.af.mil/news/story.asp?id=123045485

[107] "RAD6000 radiation hardened 32-bit processor," Lockheed Martin, Manassas, VA, Product Brief 0897/Rev1/96000887/CDR35.

[108] "Software user's guide for the RAD6000 processor," Lockheed Martin, Manassas, VA, User's Guide 204A496, August 1998.

[109] *American National Standard for Front Panel Data Port Specifications*, VMEBus Interational Trade Association Std. ANSI/VITA 17-1998, 1999.

[110] "HY57V651620B 4 banks x 1M x 16Bit synchronous DRAM," Hyundai Electronics," Datasheet, April 2001.

APPENDIX A. SPACE RADIATION ENVIRONMENT, EFFECTS, AND ESTIMATION

In order to successfully use radiation-sensitive components in a space-based system, it is necessary to estimate the effects of radiation on the electronics used in the field and develop an appropriate upset mitigation strategy for that system. In addition, all mitigation techniques that are used as part of that mitigation strategy should be well-validated with accepted testing methods. Both the estimation and validation efforts are vital parts of the overall effort of developing a system that is capable of reliable processing in the radiation environments of space, and both have proven to be very important components to the success of CFE's reconfigurable payload.

This appendix first discusses the sources and effects of space radiation on SRAM-based FPGAs and SDRAM. A discussion of the methods used to predict SEU rates in electronic devices used in a specific space environment follows. The appendix concludes with a discussion of the testing methods used to determine the specific effects that SEUs may have on the operation of an FPGA design, including designs with SEU mitigation techniques applied. These testing methods, which include ground-based methods such as fault simulation, fault injection, and radiation testing, as well as on-orbit testing, provide a means for validating FPGA designs and SEU mitigation techniques as appropriate for use in space environments.

A.1 The Near-Earth Space Radiation Environment

The main sources of space radiation present in the vicinity of earth are cosmic rays and trapped radiation belts. Spacecraft electronic components, including those used on CFE, are often affected by both cosmic rays and trapped radiation, depending on their region of operation, and both are accounted for in SEU rate predictions for these components.

A.1.1 Galactic and Solar Cosmic Rays

Cosmic rays originating from the sun and from other sources throughout space often eject intense quantities of energized particles. Galactic cosmic rays (GCR) consist mainly of protons, although they also consist of smaller amounts of alpha particles and heavier nuclei [73]. These cosmic rays are of unknown origin; some physicists and astronomers hypothesize that GCRs may originate from supernovas [18].

Cosmic rays originating from the sun are injected into space during solar particle events (SPE) and consist of a wide variety of particles, including energized electrons, protons, alpha particles, and other, heavier particles [74]. The frequency and intensity of these events are roughly periodic, varying in an approximately eleven-year-long solar cycle. These cycles correspond roughly to the number of sunspots present on the sun and the latitude of the belt in which the sunspots appear [18]. During the portion of the cycle known as solar minimum, considered to be the first half of the cycle, the frequency and intensity of solar particle events are low, while during the second half of the cycle (solar maximum), the solar particle events are more intense and frequent. In general, ground-based systems as well as systems in orbits close to the earth are shielded from much of the solar and galactic cosmic ray activity by the earth's magnetosphere, but this shielding effect decreases with increasing altitude [73].

A.1.2 Trapped Radiation Belts

The radiation belts around earth, also known as the Van Allen belts, consist of trapped charged particles, including electrons, protons, and alpha particles. These particles are attracted by the earth's magnetic field and move throughout the earth's magnetosphere in a blend of several simultaneous, periodic motion patterns [18]. There are usually two distinct radiation belts around earth, an inner belt and an outer belt, although temporary radiation belts lasting several years and created by dramatic events (including the detonation of a hydrogen bomb above the atmosphere and a significant solar flare event) have been observed [75]. The radiation belts are not uniformly distributed around the earth, as the solar wind compresses the earth's magnetic field on the side toward the sun and stretches it into a long tail on the other side [74].

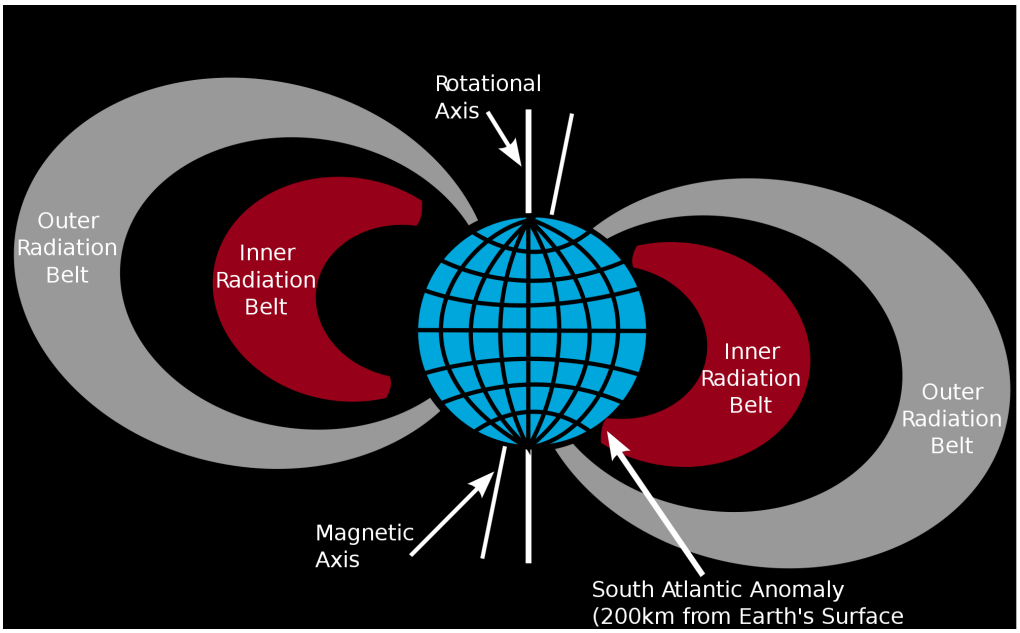

Figure A.1: The Van Allen Belts. From [74]

The outer radiation belt consists of high energy electrons and various ions which most likely originate from the solar wind and ionosphere and are energized by acceleration processes within the magnetosphere [76]. This radiation belt is quite unstable in comparison to the inner belt, as its composition is often affected by magnetic storms [18].

The inner radiation belt consists mainly of high energy protons, although electrons are also present in smaller quantities. The protons in this belt are believed to have been produced by the cosmic-ray albedo neutron decay (CRAND) process, in which neutrons from cosmic rays are broken up into other particles, including protons, due to interactions with earth's atmosphere [77]. The proton population within the inner radiation belt is somewhat dependent on the cycle of solar activity. The trapped particles within this radiation belt are subject to interactions with the upper atmosphere, and these interactions often cause the proton population of the radiation belt to drop [61]. At times when solar activity is greatest, these interactions occur more frequently; thus, the proton population is greater during solar minimum and smaller during solar maximum.

The altitude of the inner radiation belt is quite variable depending on its geographic position around the earth. The South Atlantic Anomaly (SAA) is the area where the inner radiation belt is closest to the earth's surface, down to an altitude of about 200-300 km.

This anomaly exists since the magnetic axis of earth is tilted about 11 degrees from the axis of rotation and the center of the earth's magnetic field is offset from its geographical center by about 280 miles [74]. A depiction of the geographic position of the SAA as measured by the ROSAT satellite [78] is shown in Figure A.2.

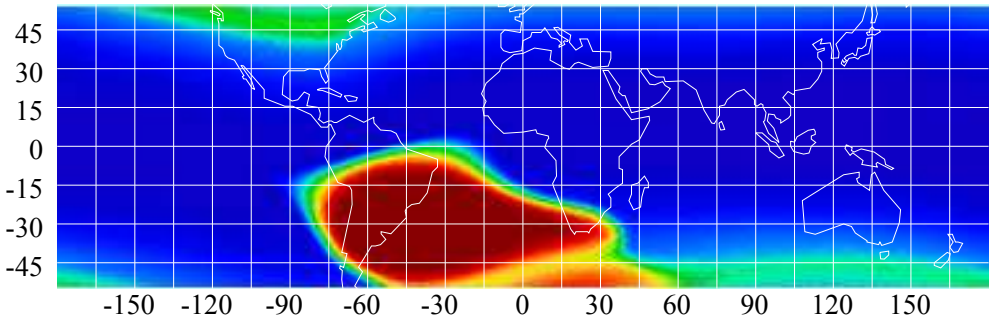

Figure A.2: The South Atlantic Anomaly, as measured by the ROSAT satellite in 1993. From [79].

The SAA does not have the same radiation characteristics throughout, and its boundaries change over time [80, 81]. Badhwar estimates that the SAA is drifting approximately .28 degrees to the west and .08 degrees to the north each year [82]. In addition to this drift rate, irregularities have been observed where the SAA suddenly moves eastward and the rate of drift changes [83].

Because of the low altitude of the inner radiation belt within the SAA, the SAA is a major concern for many spacecraft in low-earth orbits. The Hubble Space Telescope, for example, does not make observations when in the SAA [19]. Most upsets in electronic devices that occur in these orbits occur in the SAA, and since the inner radiation belt consists mainly of protons, these upsets are mainly proton-induced [20]. The effects of the SAA have been quite visible in the operation of CFESat, as the radiation present in that region has induced a significantly greater amount of upsets to CFE's payload FPGAs than have been manifest in other sections of the spacecraft's orbit.

A.2 Radiation Effects In FPGAs

The radiation present in space environments can have dramatic effects on the operation of FPGAs used in those environments. If the radiation to which an FPGA design will be exposed in its field of operation is not properly accounted for in a proper mitigation strategy, both temporary and permanent disruptions to the proper operation of the design may occur. These disruptions can be due to the total ionizing dose (TID) present in the device as well as to the specific effects of a single ionizing particle.

A.2.1 Effects

Total ionizing dose refers to the damage to semiconductor devices, including FPGAs, caused by long-term exposure to high-energy protons and electrons. A buildup of charge gradually increases within the oxide layer of the device which changes the device MOS transistor threshold voltage, increases leakage current, and modifies timing characteristics of device transistors [84]. These effects are cumulative, cause permanent device damage, and eventually lead to failures in the device's functionality.

In addition to permanent device damage from the cumulative charge buildup caused by radiation, individual ionizing particles can also induce permanent or temporary failures of semiconductor devices, including FPGAs. The effects on a device caused by a single ionizing particle are known collectively as single event effects (SEEs). The main type of SEE that can cause permanent device damage in an FPGA is single-event latchup (SEL). SEL occurs when parasitic transistors are activated by ionizing particles and as a consequence induces a very large flow of parasitic current, potentially enough to permanently damage the device [21]. A device's sensitivity to latchup may preclude it from being a suitable candidate for use in a space-based system [69, 85].

Two types of SEEs which do not cause permanent device damage are still of concern to the design of FPGA-based circuitry bound for space: single event upsets (SEUs) and single event transients (SETs). SEUs are changes in the state of a digital memory element caused by an ionizing particle. In FPGAs, SEUs can lead to unreliable device operation by changing user state values (in block memories and flip-flops) or by changing values stored in the

FPGA's configuration memory. Upsets to FPGA configuration memory require particular attention since the configuration memory controls the behavior of the configurable logic elements of the FPGA such as lookup tables (LUTs) and configurable routing resources. SEUs can be a frequent occurrence in many space applications using FPGAs. For example, nearly 1800 configuration SEUs have been detected in CFE's payload FPGAs during its time of operation (from March 8, 2007 onward), and these SEUs have occurred at a rate of .28 upsets per FPGA device day.

Occasionally, a single particle can induce a change in the value of more than one memory bit, an event known as a multiple bit upset (MBU). Although these events are generally infrequent, they can be problematic in some situations since many mitigation schemes can only handle the occurrence of one upset bit at a time [59, 58]. Eight multiple bit upsets have been observed so far in CFE's payload FPGAs since its launch.

Single event functional interrupts (SEFIs), a subset of SEUs, affect control structures of the device. These events can cause incorrect operations in configuration circuitry, device reset logic, or other control subsystems. Upsets to these subsystems can in many circumstances cause extensive erroneous behavior of the device. SEFIs usually require more extensive intervention to bring the FPGA design back into a state of correct operation than with conventional SEUs [69, 86]. SEFIs are usually low frequency events in orbit; for example, no SEFIs have been observed in the more than three years of CFE's on-orbit operation.

SETs arise when when an ionizing particle causes a short-lived current or voltage spike on a digital signal. In general, these events do not cause errors in digital systems unless they are sampled during the signal spike and an incorrect value is stored in a clocked storage element [21]. In FPGAs, latched-in transients appear identical to SEUs occurring in flip-flops, except that the rate at which transients are observed is dependent on the clock frequency. In general, SETs in FPGAs are possible but are considered to occur much less frequently than SEUs [69].

A.2.2 Avoidance and Mitigation

Fortunately, the permanent device damage caused by TID effects and latchup can be largely avoided in space applications using FPGAs if proper devices are used. Certain FPGA

devices using different types of configuration memory have been qualified for use in space applications. Antifuse FPGAs are largely immune to radiation effects and are more power efficient than SRAM FPGAs, but they are one-time programmable devices and have lower logic densities than SRAM FPGAs [87]. Recently, some FPGAs which use flash memory for their configuration memory have also been qualified for use in space [88]. Flash memory can be rewritten, meaning that FPGAs utilizing Flash for configuration memory can be reprogrammed. Radiation tolerant SRAM-based FPGAs are produced by several vendors and use process-level techniques to ensure that the TID and SEL performance of the devices is adequate to ensure the device's suitability for space operations [89, 90]. For example, Xilinx designed the QPro series of FPGAs to use a thin-epitaxial CMOS process in order to provide immunity to latchup as well as total dose tolerance which is acceptable for many space-bound missions [84]. Both antifuse and radiation-tolerant SRAM FPGAs are used in the CFE payload [4].

Although generally immune to latchup and tolerant of significant radiation dose, radiation tolerant SRAM FPGAs are still sensitive to SEUs, and appropriate system- and design-level techniques must be used to mitigate against the risk of these upsets causing incorrect design operation. Upsets in the configuration memory can be detected and repaired using system-level configuration readback and scrubbing techniques, while logic level, redundancy-based techniques such as TMR can mask SEUs that occur in the configuration memory and user flip-flops. Memory scrubbing techniques can be used to detect and correct SEU-induced errors that occur in user memories such as block RAM and LUT RAM. SEU mitigation and detection techniques, their use in the CFE payload, and the test strategies used on CFE to validate the techniques as suitable for use in space-bound FPGAs were described in greater detail in Chapter 3.1.

A.3 Radiation Effects In SDRAM

Synchronous dynamic random access memories (SDRAM) have become a popular solution for high-density, low-cost volatile memory storage in many applications, including many in space environments. These memories are, like FPGAs, sensitive to the effects of ionizing radiation. Radiation-induced effects in dynamic memories are similar to those

present in FPGAs in many respects, as both are MOS integrated circuits; however, differences do exist since dynamic memory cells are very different from the SRAM used in FPGAs in their principle and modes of operation, size, and structure.

A.3.1 Effects

Radiation-induced permanent damage to SDRAM is very similar in nature to that seen in FPGAs, as both latchup and total dose effects are possible in SDRAM. In addition, some SEFIs in SDRAM involve high current states that could cause permanent damage to the device [91]. Non-destructive SEUs, including MBUs and other types of SEFIs, are also possible in SDRAM and are a major obstacle to the reliable usage of SDRAM devices in space [23]. A semi-permanent effect sometimes observed in SDRAM is the stuck bit, or hard error, in which a certain memory cell is stuck at a 1 or 0 value. This cell may revert back to its normal operating state, or anneal, after some period of time [92].

There are several key characteristics of SDRAM which make its sensitivity to space radiation different than that of FPGAs. The first and most important characteristic that differentiates SDRAM radiation sensitivity from that of FPGAs is that dynamic memory is charge-based, where the presence or absence of charge on an isolated capacitive cell is the mechanism for storing binary data. As charge from a capacitor is subject to gradual leakage, a dynamic memory cell must be periodically refreshed to avoid data loss and is not a bistable circuit. Due to this method of information storage, dynamic memory cells, including those used in SDRAM, need not suffer a complete "bit flip" to suffer from erroneous values in the memory; rather, the degradation of the stored charge to a level outside of the noise margin of support circuitry is sufficient to cause an error [22]. This makes dynamic memory like SDRAM especially susceptible to errors caused by ionizing particles. In addition, this method of information storage causes the probability of a 0 erroneously transitioning to a 1 to be unequal to the probability of the opposite case [23].

The physical size and organization of SDRAM cells also cause their sensitivity to radiation to be different than that of FPGAs. SDRAM cells are quite small, consisting of a single MOS transistor and a capacitor, as opposed to a traditional six-transistor SRAM cell. This means that SDRAM can be more densely packed together, which leads to lower

sensitivity per bit than might be expected [22], though this density also means that SDRAM can be more vulnerable to MBUs than an FPGA produced in a process of similar size [23].

Another difference between radiation sensitivity of SDRAM and FPGAs is the extent to which the memory bits affect the behavior of the device. In an FPGA, upsets to the device's configuration memory can have a dramatic effect on the behavior of the device, and the SEU vulnerable section of the device is generally dominated by that of the configuration memory. In SDRAM, most of the device's SEU vulnerable area is for user data storage, and as such, upsets to this section of the device do not affect the behavior of the device beyond the potential of outputting errors in user data. However, since SDRAMs do include several modes of operation and an internal state machine, they are subject to SEFIs arising from upsetting control sections of the device, which can affect device functionality [91].

Single bit SEUs as well as MBUs have been observed in CFE's payload SDRAM during its time of operation. 2388 upset events have been detected by SDRAM scrubbing circuitry implemented on the payload FPGAs since SDRAM upset detection was deployed onto the CFE payload on July 4, 2009. 142 of these events resulted in errors in two or more SDRAM bits, with some events resulting in up to eleven upset bits.

A.3.2 Avoidance and Mitigation

Similar to FPGAs, permanent damage in SDRAM caused by TID and latchup effects can be largely avoided in some applications with the use of the proper device. The processes used to implement SDRAM devices can help provide some radiation tolerance; for example, Maxwell's RAD-PAK SDRAM packaging incorporates radiation shielding in the microcircuit package and provides adequate total dose and latchup performance for many space applications [93].

Several process and transistor-level technologies have been proposed to protect dynamic memory against SEUs, generally attempting either to protect the signal stored in DRAM capacitors or to reduce the noise to which the memory is subject [22]. On the system level, integrated error detection and correction (EDAC) hardware is present in some dynamic memories, using techniques such as error-correcting codes and parity bits [94], and such hardware may also be implemented off-chip if on-chip EDAC hardware is not avail-

able. The logical organization of SDRAM cells may be modified to improve the robustness of some EDAC techniques [22]. Finally, traditional redundancy-and-vote schemes like TMR can also be used for SDRAM, although they can to an extent cancel out some of the density advantages of using SDRAM [23].

A.4 Device SEU Rate Prediction

Since the radiation present in space can have such a dramatic affect on the operation of electronic devices such as FPGAs and SDRAM, an understanding of the radiation characteristics of a particular space environment is requisite to the proper use of electronics in that environment. In particular, knowing the rate at which SEUs will occur in electronic devices used in a given environment is an important step in the process of designing a system to operate in that environment.

There are several aspects of designing and operating a space-based digital system which require an understanding of the SEU rate that can be expected in the system's target operating environment. First, specific electronic devices used in the system must be qualified as suitable to be used in the system's operating environment, and the response of the device to single event effects including SEUs is an important component of that qualification. If the device is sensitive to SEUs, knowledge of the device's SEU rate is important to devising an appropriate SEU mitigation or detection strategy. For example, the rate at which an FPGA's configuration memory is read back and scrubbed is an important design parameter in a readback-based SEU detection and correction system, and this parameter can be optimized to account for the SEU rate in a given environment. Depending on the nature of the system being implemented and the expected SEU rate, reduced-cost mitigation or detection approaches can also be implemented. For example, if uninterrupted and error-free circuit uptime is not required for a given circuit design, an approach that detects and reports errors can be implemented to exchange the ability of the system to operate in an uninterrupted error-free state for a lower cost of mitigation. However, if the SEU rate for that circuit in its operating environment is high and the circuit reports errors continually, a mitigation strategy which allows for uninterrupted correct operation may be a more appropriate choice.

The first step in predicting the SEU rates for a certain electronic device in orbit is to determine the static cross section of that device. The static cross section is a quantity that corresponds to the sensitive (SEU vulnerable) area of the circuit at a particular level of particle energy. The cross section is obtained through radiation testing in a particle accelerator. In an FPGA, the cross section is calculated by dividing the number of errors by the fluence of the radiation, which is the number of particles per cm^2 [46]. Since devices in different orbits are subject to different particles at different energy levels, the cross section is often calculated at several different energy levels and then fit to a distribution such as the Weibull distribution, which has been proposed as an appropriate distribution for per-bit static cross section versus energy [49]. In addition, different cross sections are calculated for different types of radiation such as protons, heavy ions, and neutrons, since the mechanism of upset is different for different types of ionizing particles, and different orbit environments contain different compositions of these particles.

The next step in making an SEU rate prediction for a given device is to specify the orbit in which the device will operate. The orbit of a spacecraft is specified by several different parameters, including the orbit apogee and perigee (the elevation of the orbiting body at both it's furthest and closest point to earth, respectively), inclination (the angle between the satellite's orbit and the earth's orbital path), and parameters relating to the ascension of the satellite. These parameters are often supplied to a software tool to allow for the modeling of the particles that will be encountered by the spacecraft during the course of a set number of orbits. This modeling is based on reference models derived from data obtained from past satellite missions. Several different models for both trapped particles (both electrons and protons) and cosmic rays have been developed using data from different satellite missions [95, 51, 96]. The output of the orbit specification is an estimation of the particle flux that will be encountered for a spacecraft in that orbit. Different estimations are often produced to correspond to different space weather conditions, including the position in the solar cycle (solar maximum or solar minimum) and stormy conditions induced by solar flares.

Once the orbit and space weather conditions have been determined, the particle flux estimation and device-specific information are used to estimate the rate at which SEUs

will occur in the device in those conditions. The device-specific parameters which are used in this estimation may vary across different software tools, but often include cross-section related parameters such as Weibull distribution parameters, the material of which the device is composed, the number of bits in the device, and information about how the device is shielded [49]. These parameters are combined with the particle flux models calculated in the previous step to yield an SEU rate estimation. These rates can be calculated for a variety of space weather conditions as described above, and they are often separated into upset rates for different types of ionizing particles (heavy ions and protons).

SEU rate predictions were made before CFE's launch to approximate the environment in which the satellite's payload electronics would be expected to reliably operate [46]. These estimates predicted that during solar minimum, CFE's payload FPGAs would be subject to approximately .84 SEUs per device day. This prediction proved to be a conservative one, as the actual SEU rate seen on CFE is about .28 SEUs/device day. A more detailed presentation of CFE's measured SEU rate and a discussion of the difference between predicted and measured rates were presented in Chapter 4.

A.5 Validating FPGA SEU Mitigation and Detection Techniques

Since SEUs occurring in FPGA-based systems can cause those systems to operate incorrectly, techniques to mitigate against the effect of upsets should be well-validated as effective and appropriate for use in the system's field of operation. Validation of a mitigation technique involves the application of the technique to different FPGA designs and observing their behavior in the presence of real or simulated SEUs to see if the technique has adequately masked or reported incorrect circuit behavior or state. Typically, the effects of radiation-induced faults on FPGA designs are tested with ground-based techniques. These techniques allow for a simulation of the effects of SEUs on FPGAs in order to predict how a given circuit will behave in the presence of an upset. These approaches can be used to test circuits using a proposed mitigation technique in order to evaluate how well the technique improves the ability of the mitigated circuits to operate correctly in the presence of upsets. Several different on-the-ground testing techniques have been developed, including fault simulations [97], fault injection [21], and particle accelerator testing [98]. These techniques each

have specific advantages and disadvantages, and each technique is more suitable for use in some situations than in others.

In addition to ground-based validation techniques, on-orbit validation testing is an additional method of validating SEU mitigation and detection techniques for use in space. The CFE payload applications created for this work and discussed later in this thesis were designed to carry out on-orbit technique validation experiments, and this on-orbit validation provides an additional level of confidence in the declaration of the mitigation and detection techniques tested as suitable for use in space.

This section will first describe the principles of operation, strengths, and weaknesses of fault simulation, fault injection, particle accelerator testing, and on-orbit testing. The section concludes with a discussion how each method of testing might be properly used in the overall effort to validate an SEU mitigation or detection technique as appropriate for use in FPGAs in a given space environment.

A.5.1 Fault Simulation

In a fault simulation, a high level programming language is used to describe a model that simulates the behavior of a digital design under various conditions. This model can be designed at any level of abstraction, such as behavioral level, register transfer level (RTL), or transistor-level, depending on the desired degree of detail to be accurately modeled [21]. This fault simulation is typically executed in software, and as such can be time-consuming if the level of simulation detail is very high. One example of fault simulation is an RTL simulation model which was developed to accurately describe the behavior of Xilinx Virtex FPGAs, including the result of changing the value of any bit within the FPGA configuration memory [97]. Another simulation-based tool, STARC, allows designers to analyze a netlist-level design to quickly identify any problems with the design's application of TMR while also estimating the sensitive cross-section of unprotected sections of the design [33].

A main advantage of fault simulations is that they can be set up quickly and provide a quick and rough estimate for fast feedback. It can be done early in the design process since a full, completely implemented, hardware design is not necessary to perform many fault simulations. One of the key drawbacks of a fault simulation is that since it is conducted in

software, a fault simulation can either be fast but lack detail, or it can be detailed but very time consuming, requiring a large amount of computing resources. In addition, deriving an accurate and detailed fault simulation can be quite difficult, especially since many details that would be necessary to know in order to create such a simulation are often proprietary.

A.5.2 Fault Injection

Fault injection is another method of modeling the effects of radiation-induced faults on FPGA-based designs and in testing mitigation techniques applied to those designs. In fault injection, the reconfigurability of the FPGA being tested is exploited to actually modify the contents of the configuration memory while the circuit design on the FPGA is executing [21]. The behavior of the circuit can then be observed to determine the effects of the fault on the circuit's correct operation. Several different fault injection systems have been developed with various performance results; these results are heavily based on the configuration interface used to program the FPGA and whether full or partial device reconfiguration is used. Several different fault injection platforms have been developed for different FPGA devices [21, 41, 99].

Fault injection can provide a much faster test time than very highly detailed software simulations since the behavior of the circuit is observed from its actual execution in hardware instead of from a software simulation. In addition, the reaction of the FPGA to the "upset" of a given configuration bit in fault injection is very likely to be accurate to in-field behavior since it is actually executing on the device hardware. The fault injection environment can be considered to be a better match of operating conditions than the simulation environment since no modeling is necessary to determine the effect of an upset on a design's behavior. Disadvantages of fault injection include the fact that a fault injection test requires the entire FPGA configuration for the design under test to be designed and implemented before any testing can occur; this makes it less apt to early testing of mitigation techniques than fault simulations. In addition, fault injection cannot be used to test SEFIs that may occur in an FPGA or the effects of upsets in flip-flops used by circuit designs implemented on the FPGA.

A.5.3 Particle Accelerator Testing

The most accurate known method to produce an environment on the ground that approximates the effects of space radiation-induced faults on FPGA-based designs is to use a particle accelerator. In an accelerator test, the unit under test is bombarded with a stream of particles such as protons, neutrons, or heavy ions such as argon, neon, krypton, and xenon [69]. The specific particles that are used to test a specific device or design technique are dependent upon the characteristics of the environment in which the system under test will operate. For example, high energy protons are concentrated in the earth's radiation belts and other regions in the near earth space environment and often affect satellites operation in these regions, while neutrons often interact with circuitry at airplane altitudes [98].

A main strength of radiation testing for validating SEU mitigation techniques is that since actual radiation is used to induce SEUs in the FPGA device being tested, the testing environment provides a closer match to the actual field environment than either fault simulation or fault injection. However, this closer match also limits the amount of fine-grained control possible in the validation effort. Individual upsets can not be controlled in an accelerator test as they may in fault simulation and fault injection, and thus it is generally not possible to conduct tests directed towards measuring only one type of radiation effect that are not affected by other radiation effects. For example, SEU mitigation testing in an accelerator may be limited by the TID characteristics of the device under test or interrupted by SEFI events which require a specific course of action before SEU mitigation testing can resume. Also, in comparison with fault simulation and fault injection, accelerator testing for SEU mitigation technique validation is very time consuming and expensive [69].

Along with being used to validate SEU mitigation and detection techniques, accelerator testing is very often used to characterize electronic devices for their radiation sensitivity, including testing TID and latchup effects as well as the device's SEU cross-section [47, 100, 69]. These efforts are very important to the qualifying of a device as appropriate for orbit as well as for SEU rate predictions for usage of that device in a given space environment.

A.5.4 On-Orbit Testing

For space-based systems, any on-the-ground testing strategy for SEU mitigation testing attempts approximate to some degree the eventual operating environment of the system. In general, on-the-ground approximations of the operating environment can allow for mitigation technique testing to provide a high level of confidence in the suitability of that technique. However, the capability to additionally validate a technique in the field is very desirable, since the most accurate way to test how well a mitigated system or a given mitigation or detection technique will work in the field is to actually test it in the field. Since the test environment is the same as the deployment environment, the results of the test can be used to derive a very accurate projection of how the mitigation approach under test will perform in a real deployed system. This can provide a higher level of confidence in the evaluation of the quality of an SEU mitigation or detection technique.

A major advantage of on-orbit testing of SEU detection and mitigation is that data collected from in-field tests can be collected, analyzed, and then used to improve pre-field predictions, tools, and techniques. For example, SEU rate data from a given orbit acquired by an SEU detection test can be used to refine SEU rate prediction techniques or tools for that orbit. Another advantage of conducting an on-orbit validation test is that an on-orbit test of an SEU mitigation or detection technique can serve as a dry run for the actual application of the technique in a deployed system. The initial application of an SEU mitigation or detection technique to a system slated for orbit is likely to encounter implementation, integration, and other issues that can be avoided in subsequent missions utilizing that technique once the problems have been discovered and solutions identified, and thus it is beneficial for early applications of the technique to a space-bound system to be associated with an experimental or testing mission rather than with a mission where the risk of the technique failing would more greatly endanger the overall success of the mission.

On-orbit testing, however, is not without major disadvantages and limitations. One major limitation of on-orbit testing relative to ground-based tests is that the amount of data that can be collected in an on-orbit test is generally much smaller than the amount that can be collected in a test on the ground which induces upsets using artificial means. In an on-orbit test, the rate at which SEUs occurs is set by the environment in which the test is

operating, as opposed to ground based tests where the rate of SEUs can be controlled by, for example, changing a fault simulation parameter or increasing the energy of protons used in a radiation test beam. The ability to control the rate that SEUs occur during a test is a valuable way to collect adequate data to facilitate drawing conclusions about the part or mitigation technique under test without being bound by limitations of the field environment. Another major disadvantage of on-orbit testing is its potentially high cost relative to the cost of tests conducted on the ground. An on-orbit test requires for a suitable on-orbit testing platform to be developed, launched, and maintained for a length of time substantial enough to collect adequate data.

Because of the disadvantages and limitations of on-orbit testing, on-orbit tests of radiation effects on electronic devices have been considered to be impractical in many situations. Although several experimental systems have been either launched into orbit or carried "piggy-back" by other systems to gather SEU rate data and to validate and improve SEU mitigation techniques for a variety of electronic systems [101], few of these missions thus far have been designed specifically to test FPGAs.

The reconfigurable nature of FPGAs, however, suggests circumstances in which on-orbit testing of FPGAs can be made viable. The creation of reconfigurable, on-orbit platforms which can be reused for a wide variety of applications, including the validation of SEU mitigation techniques for FPGAs, can allow on-orbit tests to be conducted as one of many reconfigurable applications used. In this case, the cost of the platform can be considered to be amortized across all of the potentially very different mission tasks facilitated by the platform. In addition, since the validation of a single SEU mitigation or detection technique can provide a proven technique that can be used in many different applications, the cost of this validation can be considered further to be amortized across all of the future applications that will benefit from the validation of the technique. On-orbit testing which takes advantage of platform reconfigurability can be a more practical and less expensive way to further validate SEU mitigation and detection techniques beyond the validation provided by fault simulations, fault injection, and radiation testing.

The CFE payload applications designed and carried out in this work take advantage of CFE's reconfigurable platform in this way. The CFE technique validation experiments

have been operational on the CFE payload for over four thousand FPGA device days and have provided a valuable complement to the results of ground-based validation testing. More details about the mitigation technique validation experiments conducted on CFE were presented in Chapter 3.1.

A.5.5 Overall Technique Validation Methodology

It is clear that each of the ground-based testing approaches, as well as on-orbit testing, have specific advantages and disadvantages that make them more suitable for some goals than for others. To take advantage of this fact, Quinn et al. detail a three-tiered, ground-based methodology for the dynamic testing of FPGA-based circuit designs bound for space [69]. This methodology finds flaws in mitigation with simulation, uses fault injection to map the flaws to physical locations on the FPGA, and validates the results of the other techniques with accelerator testing. As the principles of testing a specific FPGA design are very similar to those of validating an SEU mitigation or detection technique (since validation consists of testing designs to which the mitigation technique under test has been applied), a similar methodology can be applied to validation testing of those techniques.

When a reconfigurable in-orbit platform like as CFE is available, the use of on-orbit testing can be of additional benefit to validating SEU mitigation and detection techniques. Because of the small amount of data that can be derived from an on-orbit test, on-orbit testing alone is not adequate for validating an SEU mitigation or detection technique as appropriate for a particular orbit. However, when combined with ground-based testing strategies, the accurate match of the field environment provided by an on-orbit test can provide an even greater level of confidence in the declaration of a mitigation or detection technique as suitable for a particular situation.

A.6 Conclusion

The radiation present in space can have a major effect on the correct operation of electronic devices used in space. In order to use SEU-sensitive devices reliably in space, the rate at which SEUs are expected to occur should be estimated and a well-validated mitigation

strategy implemented. This appendix discussed the nature of the radiation present in the space environment near earth as well as the effects of radiation on SRAM-based FPGAs and SDRAM. The procedures used to estimate the SEU rate for a particular device in orbit and to validate FPGA SEU mitigation and detection techniques were also described.

The on-orbit CFE experiments developed and carried out in this work provide a major contribution to the effort of reliably using FPGAs and SDRAM in space environments. These experiments have enabled the measurement of on-orbit SEU rates as well as the validation of several SEU mitigation and detection techniques. The results of these experiments allow for a more complete understanding of and more successful mitigation against the harsh radiation environments to which future spacecraft electronics will be subjected.

APPENDIX B. THE CIBOLA FLIGHT EXPERIMENT (CFE)

The six SEU rate measurement and mitigation technique validation applications created in this work were designed to operate on the Cibola Flight Experiment satellite, which is currently in orbit and is both available for and capable of performing on-orbit SEU mitigation and detection studies. The experiments take advantage of the CFE payload's microprocessor, FPGAs, and memories to collect SEU-related data, perform preliminary processing of the data, and format the processed data for transmission to the ground. Since the CFE payload is an integral part of the SEU-related applications' ability to operate, some background knowledge of CFE's architecture and operations is useful to understanding the organization and results of the SEU-related studies conducted on CFE. This appendix will give a brief overview of CFE's mission, present the details of aspects of the CFE's system architecture and operations which are relevant to understanding CFE's usage as a platform for on-orbit SEU mitigation and measurement studies, and then describe the process of creating payload applications that can be scheduled to operate in orbit.

B.1 Overview

CFE was funded by the United States Department of Energy's (DOE) National Nuclear Security Administration (NNSA) NA-22 Office of Research and Development, and it is the fourth DOE/NNSA/NA-22 satellite project [102]. A major aspect of CFE's mission is to improve the ability of the United States to detect and locate above-ground nuclear explosions [64]. These explosions emit electromagnetic pulses which can be detected by satellites with the necessary sensing capability. However, natural phenomena such as lightning can also emit electromagnetic noise, and complex processing is required to determine if an electromagnetic pulse is generated by a weapon or by natural phenomena. Past impulse detection and identification approaches, including those used by predecessor DOE/NNSA/NA-22

satellites [65], collected sensor data and then sent the data to the ground for processing. This approach proved to be less than ideal, as the satellite's memory was often quickly filled to capacity, preventing the satellite from making more observations until it could communicate with the ground station and offload stored data.

CFE was envisioned to implement an improvement to this approach, where a greater amount of processing could be performed on board, decreasing memory and data transmission requirements [64]. SRAM-based FPGAs were an attractive choice for performing this on-board processing because of their performance, cost, and reconfigurability. However, before CFE was designed, SRAM FPGAs were not well accepted as being suitable for use in space, and an extensive validation effort was required to first qualify the devices [47] and SEU mitigation strategies [5, 35, 103, 104] for use in space.

One of CFE's major objectives is to serve as a technology pathfinder, validating several new technologies as suitable for use in space applications. CFE was designed to demonstrate the successful in-orbit operation of a system using FPGAs and other commercial components to assist in in-orbit high-throughput data processing while tolerating or mitigating against the effects of SEUs on FPGA operation [4]. In addition to validating SRAM-based FPGAs, CFE is also validating the use of several additional technologies for space flight, including its power supply, battery pack, inflatable antennas, and launch-vehicle separation system [105].

The FPGAs in the CFE payload are used to implement and demonstrate the successful operation of various reconfigurable, high-throughput radio frequency (RF) signal processing systems such as software defined radios, demodulators, decoders, and FFT engines [32]. The reconfigurability of the payload allows for all of the signal processing applications to be executed with the same physical hardware by reconfiguring the FPGAs and executing different software on the payload's controlling microprocessor. In addition, CFE's reconfigurability allows for the execution of another class of applications: those designed specifically to collect data about the occurrence of SEUs on the payload as well as to demonstrate the effectiveness of SEU mitigation and detection techniques. One of the key aspects to demonstrating success in using of FPGAs in space is the validation of SEU mitigation techniques used for FPGA designs. As such, the SEU-related studies conducted on CFE, including the appli-

cations created as part of this work, provide a major contribution to the overall effort of validating FPGAs for use in space. The six SEU-related applications created for this work were described in detail in Chapter 3.

CFE was launched on March 8, 2007 into a circular low-earth orbit (560 km altitude, 35.4° inclination) [32]. As CFESat is a small satellite, measuring $60.9 \times 60.9 \times 96.5cm$ and weighing 160 kilograms [102], it was eligible for launch with the STP-1 mission, in which a single Atlas V rocket was used to launch, for the first time, six unique satellites with different orbits [106]. The launch was successful, communication with the ground and other payload operations commenced shortly after launch, and the operations of the satellite have been largely successful during the more than three years of flight time. CFE's mission lifetime was expected at the time of launch to be three to five years [64]; however, past satellites designed and operated by LANL have worked successfully for longer than expected [65, 66].

Figure B.1: Launch of Atlas-5 rocket carrying CFE

B.2 Satellite Organization

The components and subsystems of many satellites, including CFESat, can be divided into two broad groups: the satellite bus and payload. The satellite bus can be thought of as the satellite vehicle and provides the physical and electrical infrastructure necessary to support the payload, including power, telemetry, and stabilization subsystems. In order to support payload operations, the CFE satellite bus includes a power system which is capable of delivering 85 W to the payload, 3-axis stabilization, a thermal control system, solid state data recorders capable of storing 1 GB of data, and a telemetry subsystem [31].

The satellite payload contains the components that are directly tied to the specific missions of the satellite, such as sensors and processors used to carry out data processing experiments. The CFE payload consists of a chassis containing digital processing hardware, tuners, and power converters (shown in Figure B.2), as well as 4 log-periodic array (LPA) antennas [4, 32]. At the heart of the payload are 3 reconfigurable computing modules (RCC) utilizing SRAM-based FPGAs, which provide the bulk of the satellite's processing capability. The remainder of this section will describe the major structures within the payload which are relevant to the SEU detection and mitigation studies described later in this work.

B.2.1 Microprocessor

The digital modules of the CFE payload are controlled by a BAE RAD6000 microprocessor [26] running at 30 MHz. The processor runs the VxWorks operating system and executes several different tasks which interact with the payload FPGAs, monitor state of health (SOH) data, and manage all communications of the payload with the satellite bus [4]. The RAD6000 processor logic and its included SRAM were fabricated with a 0.5μm, QML-qualified CMOS process to harden it against radiation-induced processing errors [107]. However, the architecture and performance capability of the processor are primitive in comparison with modern commercial microprocessors. Radiation-hardened digital systems often lag in performance behind their commercial counterparts by a decade or more [4], and this is the case with the RAD6000, which is a feature-reduced implementation of IBM's POWER1 architecture, introduced in 1990 [108]. For this reason, the microprocessor on CFE is not

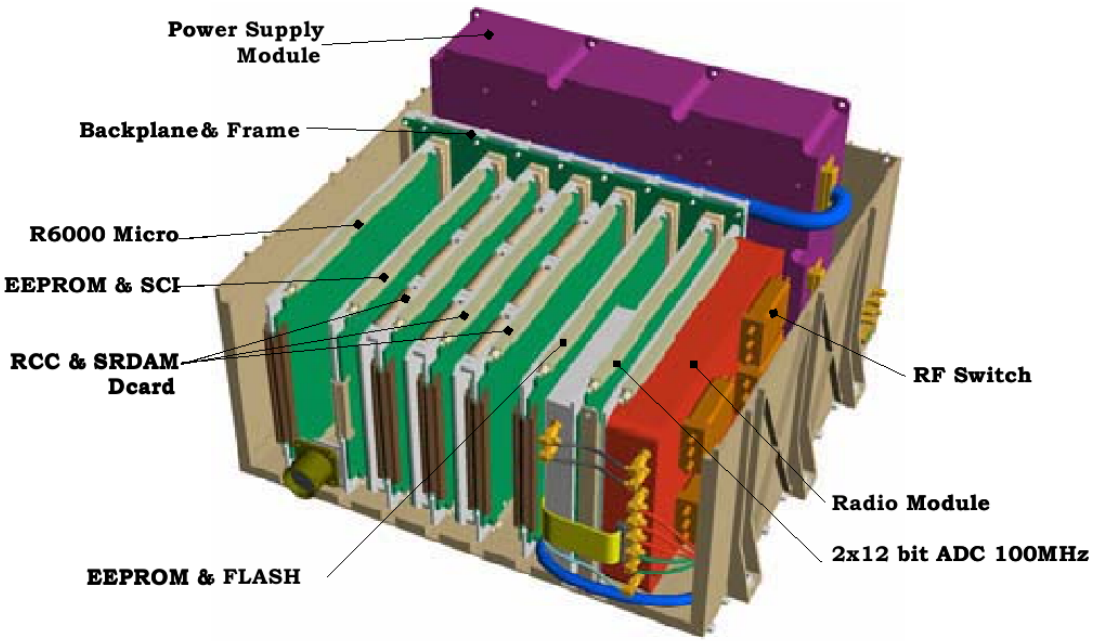

Figure B.2: Cutaway of the payload chassis

suitable for performing CFE's demanding real-time signal processing tasks in addition to its controller duties. The FPGAs in the reconfigurable computing modules of the payload are instead used for demanding signal processing tasks.

B.2.2 Reconfigurable Computer Modules

In order to provide the computational power necessary to perform high-throughput signal processing onboard, the CFE payload contains three reconfigurable computer modules utilizing SRAM FPGAs. Because the SRAM-based FPGAs used on CFE can allow for streaming signal processing tasks to be carried out in hardware instead of software and were implemented using a much newer process technology than the payload microprocessor, the payload FPGAs are capable of two to three orders of magnitude higher performance than could be expected from the payload microprocessor for certain applications [32]. The reconfigurability of the RCC module FPGAs allows for a variety of applications to take advantage of this performance advantage.

A functional diagram of an RCC module is shown in Figure B.3. Each RCC module contains three radiation tolerant Xilinx Virtex XQVR1000-CG560 FPGAs [27] with SDRAM local to each FPGA. A radiation-hardened Actel RT54SX32S antifuse FPGA [28] is also included in each RCC to perform watchdog monitoring, configure and scrub the Xilinx FPGAs, and provide the interface between the Xilinx FPGAs and the microprocessor. The RCC modules use two high-bandwidth TTL busses conforming to the FPDP specification [109] to move data on and off the card.

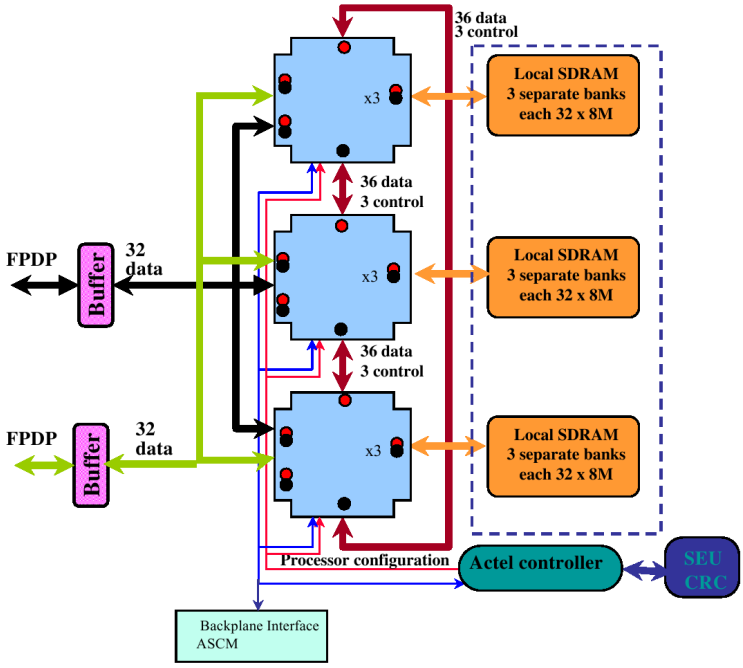

Figure B.3: Block diagram of a CFE reconfigurable computer module (RCC). Repeat of Figure 2.2

As shown in Figure B.3, the three Xilinx FPGAs are organized in a ring, with busses connecting each FPGA to the other two FPGAs in the RCC module in order to allow for data stream processing that is too complex to be contained in a single FPGA. In addition, the pinouts of all of the FPGAs are identical, which allows any of the FPGAs to be configured with the same configuration files.

As the Xilinx XQVR1000 FPGAs are at the heart of the payload and provide most of CFE's processing capability, these devices were subjected to extensive reliability qualification

for radiation environments [47]. The XQVR1000 uses a thin-epitaxial CMOS process and thus has acceptable latchup and total dose tolerance for use in many orbit environments [84], including CFE's, but it is still susceptible to SEUs in user flip-flops, memories, and configuration data. This requires the specific applications utilizing the FPGA to tolerate SEUs or to mitigate against their effects.

B.2.3 Memories

The CFE payload contains several different types of memory in order to support various FPGA-related tasks. Both volatile and non-volatile memories are used in the payload, and these memories facilitate the configuration and reconfiguration of the payload FPGAs, store the software binaries needed to control the payload and interact with the FPGAs, and provide data storage to the FPGAs in their processing tasks [29].

Nonvolatile memory is used to store the files required to perform FPGA configuration and the binaries for the operating system and user applications. The software binaries are stored in 3 MB of EEPROM, while the data files needed for FPGA configuration as well as for readback-based SEU mitigation are compressed and stored in 48 MB of flash memory. These nonvolatile memories are protected with error control coding (ECC) to mitigate against SEUs occurring during a memory read or write operation.

The SRAM FPGAs have access to both on-chip and off-chip memory sources to aid in their processing tasks. Each FPGA contains 16 KB of Block Select RAM which is available for application-specific data storage. In addition, each FPGA has access to three independent banks of Hyundai HY57V651620B SDRAM [110] which each provide 32 MB of storage. Each bank of SDRAM consists of four 64 MBit devices arranged into a 8 M word memory with a 32-bit word size. These memories are not protected against SEUs, so the user application is responsible for any necessary SEU mitigation.

B.3 Operations

As with any satellite, CFE's day-to-day operations and state of health must be carefully monitored and any problems quickly resolved in order to keep the satellite operating

properly. This section describes several of the efforts used on CFE to ensure its correct operation, including thermal and energy management, state of health (SOH) reporting, and SEU mitigation. In addition, CFE's reconfigurable payload allows for a variety of different applications to be scheduled and even for new applications to be developed and deployed. Sections B.3.4 and B.3.5 describe the processes used to reconfigure the payload and to develop new payload applications, respectively.

B.3.1 Thermal and Energy Management

Careful management of the payload temperature is extremely important due to the difficulty of temperature control in the vacuum of space. The FPGAs in the payload can consume widely varying amounts of power (and thus cause temperature fluctuations) since the power consumption of an FPGA design depends heavily on the specific application utilizing the FPGA. Due to the varying amounts of heat produced by the payload FPGAs as well as temperature fluctuations inherent to the orbit environment, the temperature within the spacecraft can cycle from high to low temperatures if not carefully controlled. These temperature cycles can lead to both suboptimal performance by the payload's FPGAs as well as physical damage to the spacecraft's components. Several techniques were used in the design of the RCC modules to minimize the negative effects of thermal cycling, including careful selection of the materials of the RCC printed circuit board and the development of a system of heat pipes capable of transporting more than 5 W of power with less than 1 degree C temperature drop across the pipe [32].

In addition, the amount of power available to the payload is limited by the capability of the spacecraft solar panels to generate power and of the spacecraft batteries' storage capability. Since the amount of power that can be generated depends heavily on orbit characteristics, the amount of power available at any one time is variable. To account for this reality, payload applications are carefully scheduled in order to comply with the spacecraft's energy budget and to prevent extreme battery charge/discharge cycles that can reduce battery life [32]. High performance signal processing experiments which consume large amounts of power are scheduled when there is adequate energy to support them, while lower-

power experiments such as those designed to collect SEU data are scheduled to operate when power constraints do not allow for the more power-demanding applications to be scheduled.

B.3.2 State of Health (SOH) Reporting

The CFE payload is monitored extensively and regularly reports data on the state of health of its instrumentation. There are four tiers of SOH information collected and reported; each tier has an associated microprocessor task to gather the appropriate information at specified intervals. In general, the rate of reporting decreases with increasing tier. Tier 0 information includes data rates, processor load, and information related to received commands. Tier 1 information includes certain temperatures, currents, and voltages. Tier 2 information includes the state of the registers in the payload digital modules, excepting SRAM FPGA registers which have varying values from application to application. Tier 3 information includes operating system and task statistics [32].

Some of the payload signals monitored have thresholds where, if the signal in question is determined to fall outside of set bounds, a panic signal will be reported to the satellite. The satellite can respond to panic signals in one of three ways: ignoring the signal, resetting the payload, or powering off the payload.

B.3.3 FPGA SEU Mitigation

Even though the Virtex FPGAs in the payload RCCs are radiation-tolerant, they are not immune to SEUs within user flip-flops, block memories, and configuration data [32]. The SEU mitigation scheme used for the Virtex FPGAs in the CFE payload consists of both system-level and application-level techniques.

The system-level technique used on CFE to both detect and correct SEUs in the Virtex FPGAs is based on configuration scrubbing. A scrubbing method using cyclic-redundancy checks (CRC) was developed in order to reduce the memory requirements of readback-based SEU detection and correction. The antifuse Actel FPGA in each payload RCC unit reads back the bitstream of each of the three Virtex devices and calculates the CRC of each frame, which is the smallest amount of configuration data that can be read back and

reconfigured independently in a Virtex device. The calculated CRC value is then compared with a pre-calculated CRC stored in a codebook. A CRC mismatch indicates an upset in the configuration memory, and the Actel responds to this event by interrupting the payload microprocessor, which then reconfigures the upset frame. Information about the SEU event including the time of the SEU occurrence and the location of the upset frame are then reported to the ground station and stored in a database which allows for overall SEU statistics to be calculated [32]. The three Virtex FPGAs on a CFE RCC are scrubbed one at a time, and a scrubbing cycle through all of the FPGAs takes 180 milliseconds.

The CRC-based readback and reconfiguration technique for detecting and correcting SEUs is a major component of CFE's payload SEU management strategy. Precomputed CRCs for each of the CFE applications utilizing the Virtex FPGAs are available on the payload flash memory in order to enable this SEU detection and correction strategy to operate for any FPGA configuration. This allows for a measure of SEU mitigation to be applied to all CFE applications using the payload FPGAs with little change in the FPGA design. In addition, since this strategy is enabled for a large percentage of the time that the payload is operational, it allows for a detailed and reliable measurement of SEUs in the FPGAs that occur in orbit and a calculation of the FPGA upset rate.

The application-level SEU mitigation techniques used on CFE also provide an important contribution to ensuring that the applications can operate reliably in the presence of SEUs. Most of the applications implemented on CFE use full or partial TMR to mask upsets that occur in the FPGA to allow for uninterrupted correct operation of the application hardware. The use of TMR on CFE was discussed in detail in Section 3.2. In addition, other logic-level techniques such as DWC, RPR, and user memory scrubbing are also tested in the CFE applications developed in this work. DWC and RPR can allow for the implementation lower-cost mitigation strategy than TMR, while the memory scrubbing techniques enable user memories to be used reliably in the presence of SEUs. These techniques and the applications designed to test them were described in detail in Chapter 3.

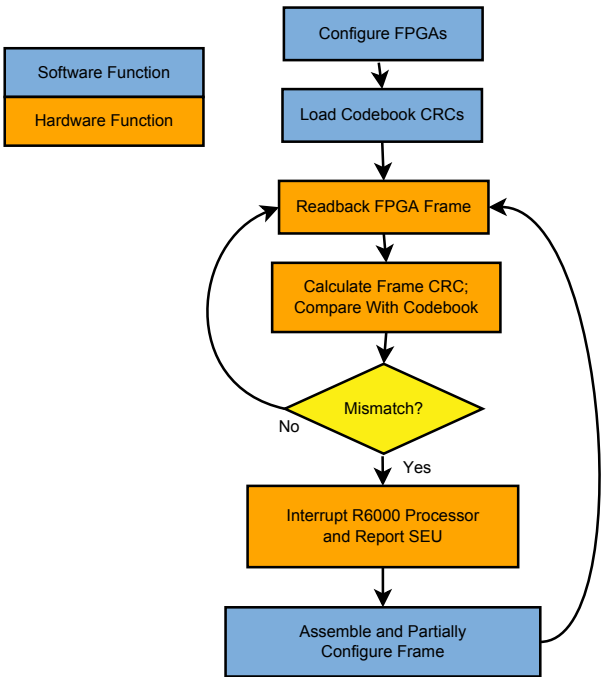

Figure B.4: Flow of CFE's CRC-based readback and reconfiguration SEU detection and correction

B.3.4 Reconfiguration

The CFE payload was designed with flexibility and reconfigurability in mind, and as such, it provides a variety of features which facilitate the conducting of different computing tasks. The reconfigurability of the Xilinx FPGAs within the payload provides the ability to utilize different computing hardware using the same silicon for varying applications. Configuration files and software binaries for a new or updated application can be uploaded to the spacecraft from the ground and stored in the payload flash and EEPROM, respectively.

The CFE software architecture also supports a dynamic command dictionary which defines 75 static commands and up to 1024 additional commands which can be created and inserted into the command table, or deleted when no longer needed. Many of these commands are associated with applications utilizing the FPGAs. In addition, the software architecture allows for the dynamic linking of object code while in orbit, which allows for new software to be uploaded without requiring software components already on the spacecraft to be re-uploaded [29].

Since its launch, CFE has received configuration data from the ground dozens of times, approximately once every 1-2 months on average [25]. The combination of the reconfigurable nature of the FPGAs, the capability to upload new FPGA configurations and software binaries, and the unique flexibility features of the software architecture allow for efficient and powerful payload reconfiguration capabilities. Application designers can update existing FPGA configurations and software or create completely new designs in order to repair application flaws, accomplish new mission tasks, or to improve the functionality or efficiency of existing applications.

B.3.5 Application Development and Scheduling

The process of developing applications to run on CFE's reconfigurable payload consists of several different tasks: FPGA configuration development, payload R6000 microprocessor software development, the development of an application command sequence, IDL data extraction and analysis software development, and the testing of the application hardware and software on an engineering model of the spacecraft. The CFE application design flow is summarized in Figure B.5. Each of the six CFE applications developed in this work was designed and debugged using this design flow.

First, the application's FPGA configuration or configurations must be developed. The algorithms which are targeted for the payload FPGAs are implemented using a combination of HDL code, Simulink models using blocks from the Xilinx System Generator blockset, and intellectual property (IP) cores such as those available in Xilinx Core Generator. Once these implementations perform correctly in simulation, the application is synthesized (and merged with other netlists, if necessary) into an EDIF netlist and prepared for SEU mitigation (including the removal of half latches [104] and LUT-based RAMs and shift registers). Mitigation techniques such as full and partial TMR and DWC are then applied; these techniques and the process used to apply them to the FPGA design were described in detail in Chapter 3. The resulting EDIF netlist is then implemented into an FPGA programming (.bit) file using the standard Xilinx toolflow. The CRCs for each frame of the FPGA configuration to be used in SEU configuration scrubbing are then calculated and saved in a .crc file which defines the CRC codebook to be used for that particular FPGA configuration.

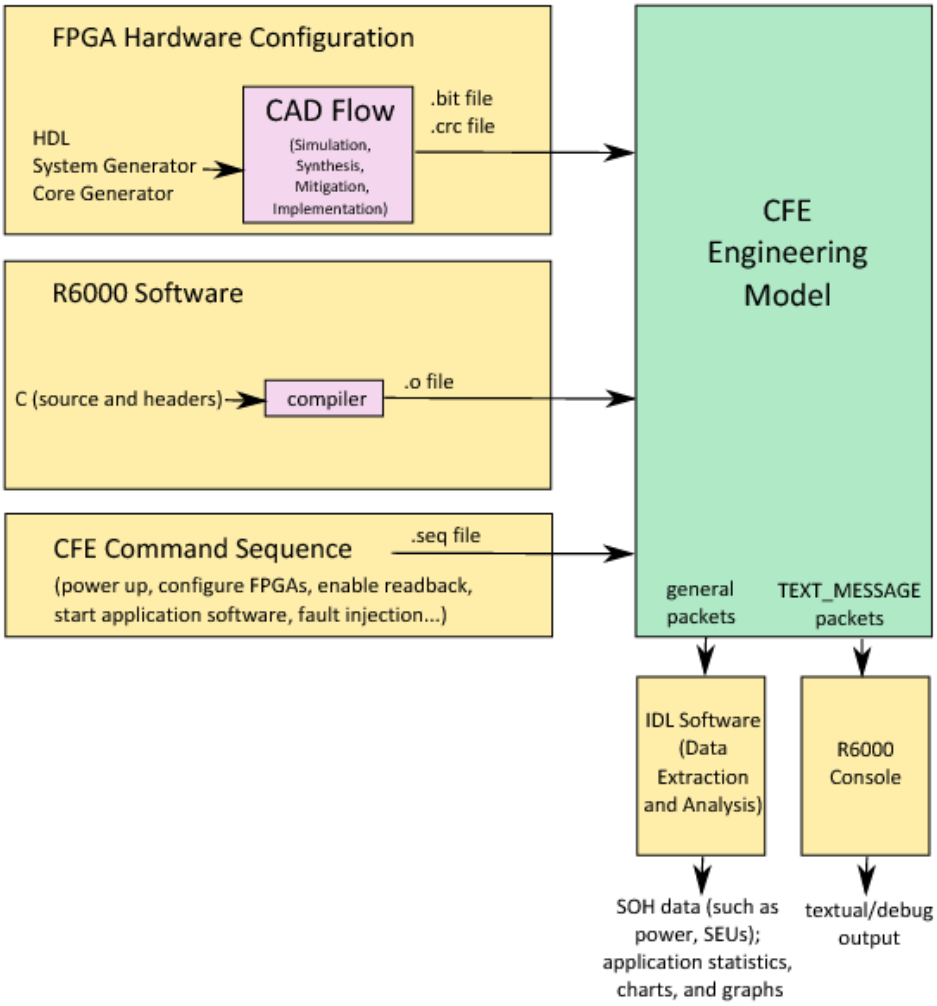

Figure B.5: Overview of application development on CFE

The application-specific software which executes on the payload microprocessor is written in C and is designed as a task for the VxWorks operating system. In general, a separate VxWorks task is created for each of the RCCs used in the application. These tasks are usually programmed to wait for an interrupt and then collect data from the RCC FPGAs, perform some amount of intermediate processing, format the data into application-defined data structures, and then packetize the data structures and hand them off to the VxWorks task responsible for the transmission of packets to the ground. In order to simplify the development of software for each application, a skeleton code generation script automates much of the process of setting up each application's code to run in the context of VxWorks

and to interact with RCC FPGAs. The application code is compiled into an object file that can then be dynamically linked with other object code in orbit, minimizing the amount of object code that must be sent to the spacecraft with each newly developed application.

Along with the software that executes on the payload processor, additional software must be written to integrate the new application with the ground station's data extraction and analysis software. The IDL programming language is used to write this software, which is responsible for extracting application data from packets as they are received from the satellite after a successful pass, as well as for processing the data received from the satellite and producing reports, charts, and tables from the data.

A new application's FPGA configurations and payload processor object files are debugged and tested together on one of two full-fidelity engineering units at LANL. These engineering units are controlled by a commanding interface on a host PC, which allows for the execution of many different commands including powering on and off or resetting specific parts of the payload, tuning the radio, configuring the FPGAs and enabling configuration scrubbing, or starting an application software task. Specific commands for FPGA fault injection are also available to enable the testing of SEU mitigation techniques or SEU-related experiments. The commanding interface can be used to send commands to the engineering unit interactively; however, most often a command sequence is created in order to automate the process and to simply the process of migrating an application from the engineering unit to the spacecraft once development and testing is complete. In a command sequence, the specific commands to send to the payload are specified in sequence along with the amount of time that should elapse before the next command is issued. The sequence is then loaded into a sequencer on the host, and commands are sent to the engineering units as dictated by the sequence.

In addition to providing the commanding interface, the host PC associated with each engineering unit is configured to receive all packets sent from the unit. The data in packets sent during engineering unit execution of applications can be extracted and processed using the IDL software mentioned above. In addition, a TEXT_MESSAGE packet can be sent with a simple C function call and allows for the printing of textual messages to a console accessible from the host, which facilitates printf-style debugging of applications.

Once an application appears to be functionally correct from engineering unit results, its power consumption is characterized in order to facilitate scheduling on the spacecraft. The necessary application files, including FPGA configurations, codebook CRCs, and software object files, can then be uploaded to the spacecraft. The FPGA configurations and codebook CRCs are stored in the payload's flash memory, while the software object files are stored in the payload's EEPROM. When all necessary files have been uploaded to the spacecraft and are stored in nonvolatile memory, the application can be scheduled to operate. The satellite operations team at LANL determines CFESat's application schedule, taking into account such factors as the power consumption of the candidate applications, the position and orientation of the satellite relative to the sun (which influences the amount of power available to the spacecraft), and at what times the satellite will be passing through the SAA (which influences the SEU rate that will be seen from the satellite).

B.4 Conclusion

Because of CFE's availability and capability for carrying out on-orbit SEU mitigation and measurement studies, it was used to carry out all of the SEU experiments presented in this work. The digital modules of the CFE payload, most notably the reconfigurable computer modules, provide a valuable platform for the validation of SEU mitigation and detection techniques, and the scrubbing-based FPGA SEU mitigation system has allowed for detailed FPGA SEU rate analysis to be conducted.

APPENDIX C. CFE SEU APPLICATIONS

This appendix presents descriptions and results for each of the seven SEU-related applications scheduled on the Cibola Flight Experiment (CFE) payload. All but the first of these experiments were developed collaboratively at BYU and LANL as part of this work. The first five applications developed in this work, SEU2-SEU6, were developed in a staged manner, each adding functionality to or repairing flaws in preceding applications. The sixth application created as part of this work, SEU7, was designed to validate the use of reduced precision redundancy (RPR) and was developed separately.

The early results of the first four SEU-related applications on CFE were published in [29], and this appendix presents an update of the results presented there as well as the results of applications developed after that paper's publication. The timeline of operation for each CFE SEU application is shown in Figure C.1, and Table C.1 shows which mitigation tests were included in each of the applications developed as part of this work.

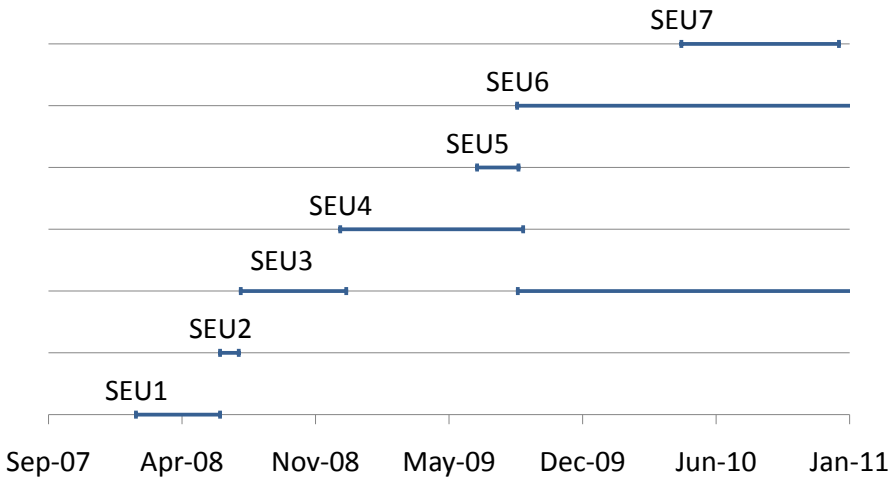

Figure C.1: Timeline of operation for all CFE SEU applications. Repeat of Figure 3.1.

Table C.1: Description of which mitigation tests are present in each CFE SEU application (repeat of Table 3.1)

	SEU2	**SEU3**	**SEU4**	**SEU5**	**SEU6**	**SEU7**
DWC	X	X	X	X	X	
BRAM		X	X	X	X	
SDRAM			[a]	X	X	
RPR						X

[a]The SEU4 SDRAM test was determined to be faulty and was repaired in subsequent experiments.

C.1 SEU1 - Configuration Upsets

The first SEU detection experiment, SEU1, was designed at LANL as a low-power simple circuit that does *not* perform in-circuit SEU detection. In this experiment, all 9 Xilinx FPGAs in the payload are configured with a simple circuit containing little logic and consuming minimal power. This simple experiment relied on the satellite's readback and configuration scrubbing technique for detecting and correcting SEUs in FPGA configuration memory. This experiment was created before the in-circuit detection techniques were available.

SEU1 began operation on February 9, 2008, and executed for 455.3 device days of operation (all 9 FPGAs operating for a total of 50.6 days). During this period, the readback process detected 216 SEUs indicating an upset rate of .47 upsets per day.

C.2 SEU2 - Online Detection

SEU2 was developed at LANL and BYU and is a more sophisticated test than SEU1 and the first experiment to implement the in-circuit detection using duplication with compare (DWC). The base circuit of SEU2 (i.e., the circuit before DWC is applied) includes a long 32-bit wide shift register driven by a gray code pattern generator. A gray code was used to minimize the dynamic power. LUTs are inserted between each shift register with a predetermined logic pattern. The use of LUTs between the registers provides more logic "area"

for SEUs to hit. The output of each LUT drives the input of a flip-flop and the LUT inputs are driven by upstream flip-flops and the gray code counter.

In order to accommodate future detection designs, the base circuit of SEU2 was designed to be entirely parameterizable in depth. Parameterization simplifies the process of creating a design that "fills" a device. This base circuit was used in subsequent SEU test experiments.

SEU2 replaced SEU1 on June 17, 2008 and operated for 101.6 device days. During this time, 46 SEUs were detected with 4 of the 46 SEUs detected by the DWC circuitry (8.7% sensitivity).

C.3 SEU3 - BRAM

The SEU3 experiment extended SEU2 by detecting and reporting SEUs that occur within the block memories (BRAM) in the Virtex FPGAs. For this test, a custom circuit was designed to detect BRAM SEUs by continuously scanning the entire BRAM memory, identifying SEUs, and reporting the total number to the processor. After receiving confirmation from the processor that the number has been recorded, the circuit proceeds to scrub (repair) the BRAM with predefined data.

The BRAM scrubber/detector is also sensitive to upsets. DWC is applied to this circuit as well to prevent erroneous data being reported due to SEUs in the detection circuitry. Should the DWC comparison circuitry detect an upset, an interrupt to the processor causes the FPGA to be reset and the configuration frame is fixed through conventional scrubbing. In addition to the BRAM scrubbing/detector circuit, SEU3 also includes the gray code shift register used in SEU2.

SEU3 replaced SEU2 on July 14, 2008 and has been operational for 1770.9 device days. Although SEU3 was replaced by SEU4, it resumed operation on CFE on September 3, 2009 because of the increasing power requirements of subsequent applications. Since it consumes significantly less power than SEU5-7, SEU3 is often scheduled to operate when it is necessary to conserve power on the spacecraft. During SEU3's runtime, 515 SEUs have been detected with readback, and 44 of these SEUs have been detected by the DWC detection

logic (8.5% sensitivity). In addition, 67 BRAM upsets have been detected by the scrubber. 66 of these upsets involved single bit upsets while one included two upsets within the BRAM.

C.4 SEU4, SEU5, SEU6 - SDRAM

The next detection test, SEU4, was designed to detect upsets within the SDRAM memory associated with each RCC FPGA. A basic SDRAM controller was designed to run at the SDRAM clock rate of 52 MHz. As there are three 32 MB SDRAM banks for each FPGA, three SDRAM controllers were required in each FPGA. An custom circuit was also designed to detect and correct any upsets found within the SDRAM. The SDRAM controller and scrubber/scanner is triplicated using the BL-TMR tool [36] in order to minimize the possibility of an upset occurring within the circuitry and causing erroneous data to be reported. The SEU4 test merges the SDRAM circuitry with the existing SEU3 detection test to provide detection for logic, BRAM, and SDRAM.

SEU4 replaced SEU3 on December 11, 2008 and was operational for 1162.8 device days. During this time, 326 SEUs were detected with readback and 29 of these SEUs were detected by the DWC detection logic (8.9% sensitivity). In addition to the configuration SEUs, 19 BRAM upsets were detected. No SEUs within the SDRAM were detected by the SEU4 experiment, which suggests that flaws existed in the SEU4 SDRAM detection or control circuitry.

Two subsequent applications were developed to repair flaws and add features to the SDRAM applications of the design. The SEU5 application involved a complete redesign of the SDRAM portion of SEU4, including the development of a new SDRAM controller and a new system for reporting multiple bit errors. SEU6 was developed to add two new features to the SEU5 SDRAM circuitry, including an error counter and the ability to disable the scanning of certain banks of SDRAM. These features were added after the observation of a flaw in SEU5's multiple-bit error reporting system and the manifestation of what appeared to be a stuck bit in a bank of SDRAM.

SEU5 operated for 100.3 FPGA device days, and during that time, 223 SDRAM upset events occurred (since no upset counter was present in the SEU5 circuitry, it is unknown how many of these events resulted in more than one upset bit.) In addition, 46 configuration

SEUs were detected by the configuration scrubber, 4 SEUs were detected by DWC, and no errors were found in the FPGA BRAM. SEU6 is still scheduled to operate on CFE when power constraints allow. So far, it has operated for 1327.4 FPGA device days, and during that time, 2054 SDRAM upset events occurred including 2218 upset bits (see Section 4.5 and Table 4.9). In addition, 372 configuration SEUs were detected by the configuration scrubber, 24 SEUs were detected by DWC, and 28 errors were found in the FPGA BRAM.

C.5 SEU7 - RPR/BPSK

SEU7 was developed separately from the rest of the SEU application sequence. This application contains the BPSK/RPR test, which compares the outputs of TMR and RPR matched filters in a BPSK system and determines the bit error rates for each system.

Since this application does not build upon previous applications, it consists solely of the RPR test circuitry described in Section 3.6. The results of this application are presented in that section.