Gaisler Research

Suitability of reprogrammable FPGAs in space applications

Feasibility Report

FPGA-002-01
Version 0.4
September 2002

Prepared by Sandi Habinc, compilation from various sources

Table of contents

1   INTRODUCTION

1.1   Scope

The dominating reprogrammable Field Programmable Gate Array (FPGA) devices currently on the space market are from Xilinx Inc. San Jose, California, USA. The devices have a relatively good total dose resistance, but the on-chip configuration memory is soft with respect to Single Event Upsets (SEUs).

Xilinx has in several publications stated that they have developed mitigation techniques that would cancel out the effects of Single Event Upsets in their FPGAs. During the last couple of years these techniques have been updated and improved. The techniques are received with scepticism in the European space market and there has been a need for a thorough analysis of the techniques to assess their feasibility. The scope of this report is to compile and review all publications available concerning the use of Xilinx FPGAs in harsh environments.

Although Xilinx has two families of FPGAs that are targeted towards the space segment, the XQR4000XL and the XQVR-Virtex series, this report will concentrate on the newer Virtex technology. The older XQR4000XL technology will be discussed to a lesser extent.

1.2   Acknowledgements

This document is a compilation of information retrieved from the documents and papers referenced hereafter. Instead of rewording the findings of others, the relevant passages in the referenced documents have been copied directly into this document. In some cases the imported text has been edited to promote clarity and place it in its right context. A reference to the original work has been provided where feasible. There is no claim from the author on the originality of this document, since based in its entire on the works of others.

The author wishes to thank all referenced authors for their work in the field of programmable logic for aerospace applications. A large part of the information presented and referenced in this document has been retrieved from Mr. Richard Katz's (NASA) web site at *www.klabs.org*.

1.3   Acronyms and abbreviations

ASIC	Application Specific Integrated Circuit
BIST	Built-In Self Test
ESA	European Space Agency
FPGA	Field Programmable Gate Array
NASA	National Aeronautics and Space Administration
SEE	Single Event Effects
SEFI	Single Event Functional Interrupt
SEU	Single Event Upset
SRAM	Static Random Access Memory
TMR	Triple Modular Redundancy
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuits

1.4   Reference data sheets

RD1   Virtex 2.5 V Field Programmable Gate Arrays, Introduction and Ordering Information, Product Specification, DS003-1 (v2.5) April 2001, Xilinx Inc.

RD2   Virtex 2.5 V Field Programmable Gate Arrays, Functional Description, Product Specification, DS003-2 (v2.6) July 2001, Xilinx Inc.

RD3   Virtex 2.5 V Field Programmable Gate Arrays, DC and Switching Characteristics, Product Specification, DS003-3 (v3.0) February 2002, Xilinx Inc.

RD4   Virtex 2.5 V Field Programmable Gate Arrays, Pinout Tables, Product Specification, DS003-4 (v2.7) July 2001, Xilinx Inc.

RD5   QPRO Virtex 2.5V Radiation Hardened FPGAs, Preliminary Product Specification, DS028 (v1.2) November 2001, Xilinx Inc.

RD6   QPRO Virtex 2.5V QML High-Reliability FPGAs, Preliminary Product Specification, DS002 (v1.5) December 2001, Xilinx Inc.

RD7   QPRO XQR4000XL Radiation Hardened FPGAs, Product Specification, DS071 (v1.1) June 2000, Xilinx Inc.

RD8   QPRO XQ4000XL Series QML High-Reliability FPGAs, Product Specification, DS029 (v1.3) June 2000, Xilinx Inc.

RD9   QPRO XQ4000E/EX QML High-Reliability FPGAs, Product Specification, DS021 (v2.2) June 2000, Xilinx Inc.

RD10   QPRO Series Configuration PROMs (XQ) including Radiation-Hardened Series (XQR), Preliminary Product Specification, DS062 (v3.1) November 2001, Xilinx Inc.

RD11   QPRO Family of XC1700D QML Configuration PROMs, Product Specification, DS070 (v2.1) June 2000, Xilinx Inc.

RD12   QPRO XQ18V04 (XQR18V04) QML In-System Programmable Configuration PROMs, Preliminary Product Specification, DS082 (v1.2) November 2001, Xilinx Inc.

RD13   XC18V00 Series of In-System Programmable Configuration PROMs, Product Specification, DS026 (v3.2) February 2002, Xilinx Inc.

RD14   Packages and Thermal Characteristics: High-Reliability Products, PK100 (v1.0) June 2000, Xilinx Inc.

1.5   Reference application notes

RD15   Virtex FPGA Series Configuration and readback, Application Note: Virtex Series, XAPP138 (v2.5) November 2001, Xilinx Inc.

RD16   Virtex Series Configuration Architecture User Guide, Application Note: Virtex Series, XAPP151 (v1.5) September 2000, Xilinx Inc.

RD17   SEU Mitigation Design Techniques for the XQR4000XL, Application Note: FPGAs, XAPP181 (v1.0) March 2000, Xilinx Inc.

RD18   Triple Module Redundancy Design Techniques for Virtex FPGAs, Application Note: Virtex Series, XAPP197 (v1.0) November 2001, Xilinx Inc.

RD19   Correcting Single-Event Upsets Through Virtex Partial Configuration, Application Note: FPGAs, XAPP216 (v1.0) June, 2000, Xilinx Inc.

RD20   QPRO High-Reliability QML Products Quality and Reliability Program, June 2000 (v1.0), Xilinx Inc.

1.6 Reference reports

RD21 Radiation Evaluation of Power-up Behaviour of Xilinx FPGA XQVR300, D-P-REP-1092-SE, January 2002, Saab Ericsson Space

RD22 Radiation Pre-Evaluation of Xilinx FPGA XQVR300, D-P-REP-1091-SE, August 2001, Saab Ericsson Space

1.7 Reference publications

RD23 Programmable Logic Application Notes, July 2001, R. Katz, EEE Links, NASA

RD24 Programmable Logic Application Notes, November 2000, R. Katz, EEE Links, NASA

RD25 Programmable Logic Application Notes, May 2000, R. Katz, EEE Links, NASA

1.8 Reference papers

RD26 A CCSDS-Based Communication System for a Single CHip On-Board Computer, D. Zheng et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD27 A Design Technique for High-Performance Self-Checking Combinational Circuits, T. Bengtsson, IEEE European Test Workshop, Stockholm, Sweden, June 2001

RD28 A Low Complexity Methond for Detecting Configuration Upset In SRAM Based FPGAs, R. J. Andraka et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD29 A Low Cost Approach for Detecting, Locating, and Avoiding Interconnect Faults in FPGA-Based Reconfigurable Systems, D. Das et al., IEEE International Conference on VLSI Design, Goa, India, January 1999

RD30 A Memory Coherence Technique for Online Transient Error Recovery of FPGA Configurations, W.-J. Huang et al., 9th ACM International Symposium on Field-Programmable Gate Arrays, Monterey, California, February 2001

RD31 A New Approach to Detect-Mitigate-Correct Radiation-Induced Faults for SRAM based FPGAs in Aerospace Application, Y. Li et al., Proceedings of IEEE 51st National Aerospace and Electronics Conference (NAECON), Dayton, USA, October 2000

RD32 A Portable and Fault-Tolerant Microprocessor Based on the SPARC V8 Architecture, J. Gaisler, The International Conference on Dependable Systems and Networks, Washington D.C., USA, June 2002

RD33 A Reconfigurable, Nonvolatile, Radiation Hardened Field Programmable Gate Array (FPGA) For Space Applications, D. Mavis et al., 1998 Military and Aerospace Applications of Programmable Devices and Technologies Conference (MAPLD), Johns Hopkins University, Laurel, Maryland, USA, September 1998

RD34 A Space Based Reconfigurable Radio, M. Caffrey, 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD35 A VHDL Implementation of an On-board ACF Application Targeting FPGAs, E. A. Bezerra et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD36 Adaptive Instrument Module - A Reconfigurable Processor for Spacecraft Applications, R. F. Conde et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD37 An Immune System Paradigm for the Design of Dependable Systems, A. Avizienis et al., First Workshop on Evaluating and Architecting System Dependability (EASY), Göteborg, Sweden, July 2001

RD38 Column-Based Precompiled Configuration Techniques for FPGA Fault Tolerance, W.-J. Huang et al., 2001 IEEE Symposium on Field-Programmable Custom Computing Machines, Rohnert Park, California, April 2001

RD39 Combinational Logic Synthesis for Diversity in Duplex Systems, S. Mitra et al., 2000 International Test Conference, Atlantic City, New Jersey, October 2000

RD40 Construction Analysis of the XQVR300 FPGA and the XQR18V04 PROM, F. Felt, 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD41 COTS for the LHC radiation environment: the rules of the game, F. Faccio, 6th Workshop on Electronics for LHC Experiments, Kraków, Poland, September 2000

RD42 Current Radiation Issues for Programmable Elements and Devices, R. Katz et al., IEEE Transactions on Nuclear Science, Vol. 45, December 1998

RD43 Design for Signal and Power Integrity in FPGA Designs, M. Alexander, 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD44 Design of a Radiation-Tolerant Low-Power Transceiver, D. Weigand et al., 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD45 Embedded Computer System with Soft Core CPU for Space Applications, T. Takahara et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, Sept. 2002

RD46 Experiences Designing a System-on-a-Chip for Small Satellite Data Processing and Control, H. Tiggeler et al., 15th Annual AIAA/USU Conference on Small Satellites, Logan, Utah, USA, August 2001

RD47 Fault Location in FPGA-Based Reconfigurable Systems, S. Mitra et al., IEEE International High Level Design Validation and Test Workshop, La Jolla, California, November 1998

RD48 Fault-Tolerance Projects at Stanford CRC, P.P. Shirvani et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, September 1999

RD49 Fault-Tolerant FPGA-Based Switch Fabric for SpaceWire: Minimal loss of ports and throughput per chip lost, P. Walker, 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD50 Fault-Tolerant Voting Mechanism and Recovery Scheme for TMR FPGA-based Systems, S. D'Angelo et al., 1998 International Symposium on Defect and Fault Tolerance in VLSI Systems, Austin, Texas, USA, November 1998

RD51 Finite State Machine Synthesis with Concurrent Error Detection, C. Zeng et al., 1999 International Test Conference, Atlantic City, New Jersey, September 1999

RD52 Heavy Ion Characterization of SEU Mitigation Methods for the Virtex FPGA, F. Sturesson et al., 2001 RADECS, Grenoble, France, September 2001

RD53 Heavy Ion Irradiation of SRAM based FPGAs, M. Ceschia et al., 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD54 Improving Reconfigurable Systems Reliability by Combining Periodical Test and Redundancy Techniques: A Case Study, E. Bezerra et al., Journal of Electronic Testing: Theory And Applications - JETTA, Norwell, Ma, Usa, Vol. 17, No. 3, 2001

RD55 Irradiation of an FPGA in Submicron CMOS Process, D. MacQueen et al., Aug. 1999

RD56 LEON-1 Processor - First Evaluation Results, J. Gaisler, European Space Components Conference, ESCCON 2000, Noordwijk, The Netherlands, March 2000

RD57 Logic Design Pathology and Space Flight Electronics, R. Katz et al., ESCCON 2000, Noordwijk, The Netherlands, May 2000, and at 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD58 Merging BIST and Configurable Computing Technology to Improve Availability in Space Applications, E. Bezerra et al., LATW00 - 1st IEEE Latin-American Test Workshop, Rio de Janeiro, 2000

RD59   Mitigating Single Event Upsets From Combinational Logic, K. J. Hass et al., 7th NASA Symposium on VLSI design, 1998

RD60   Mitigation of Single Event Upset by Virtual Redundancy in Design, K. Wu et al., 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD61   Neutron Single Event Upsets In SRAM-Based FPGAs, M. Ohlsson et al., 1998 IEEE NSREC Data Workshop, 1998

RD62   Proton Induced Radiation Effects on a Xilinx FPGA and Estimates of SEE in the ATLAS Environment, N. J. Buchanan et al., ATLAS-LARG internal note ATL-LARG-2001-011, 2001

RD63   Proton Induced Single-Event Upset Cross-Section of an SRAM-Based FPGA, N.J. Buchanan et al., American Institute of Aeronautics and Astronautics Journal of Spacecraft and Rockets, 2000

RD64   Proton Single Event Upsets in a Xilinx FPGA, N. Buchanan, UofA-Atlas-99-02, 1999

RD65   Proton Testing of SEU Mitigation Methods for the Virtex FPGA, C. Carmichael et al., 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD66   Radiation Characterization, and SEU Mitigation, of the Virtex FPGA for Space-Based Reconfigurable Computing, E. Fuller et al., 2000 IEEE NSREC, October 2000

RD67   Radiation Effects on Current Field Programmable Technologies, R. Katz et al., IEEE Transactions on Nuclear Science, Vol. 44, No. 6, December 1997

RD68   Radiation Effects on FLASH MEMORY Based FPGA, J. J. Wang et al., 1998 MAPLD, NASA Goddard Space Flight Center, Greenbelt, Md, USA, September 1998

RD69   Radiation Hard Reconfigurable Field Programmable Array, J. McCabe, 1998 MAPLD, NASA Goddard Space Flight Center, Greenbelt, Md, USA, September 1998

RD70   Radiation Test and Application of Application of FPGAs in the Atlas Level 1 Trigger, V. Bocci, 7th Workshop on Electronics for LHC Experiments, Stockholm, Sweden, September 2001

RD71   Radiation Test Results of the Virtex FPGA and ZBT SRAM for Space Based Reconfigurable Computing, E. Fuller et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD72   Radiation Testing Update, SEU Mitigation, and Availability Analysis of the Virtex FPGA for Space Reconfigurable Computing, E. Fuller et al., 2000 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2000

RD73   Radiation Tolerance of High-Density FPGAs, P. Alfke, 1998 MAPLD, NASA Goddard Space Flight Center, Greenbelt, Md, USA, September 1998

RD74   Recent Improvements on the Specification of Transient-Fault Tolerant VHDL Descriptions: A Case-Study for Area Overhead Analysis, R. Vargas et al., 13th Symposium on Integrated Circuits and Systems Design, Manaus, Brazil, September 2000

RD75   Recent Progress in Field Programmable Logic, P. Alfke, 6th Workshop on Electronics for LHC Experiments, Krakow, Poland, September 2000

RD76   Recent Total Dose Radiation Test Results for Programmable Devices, I. Kleyner, 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD77   Reconfigurable Single-Chip On-Board Computer for a Small Satellite, T. Vladimirova et al., 52nd International Astronautical Congress, Toulouse, France, October 2001

RD78   Reliability of Programmable Input/Ouput Pins in the Presences of Configuration Upsets, N. Rollins et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD79   Results of Radiation Test of the Cathode Front-end Board for CMS Endcap Muon Chambers, B. Bylsma, 6th Workshop on Electronics for LHC Experiments, Krakow, Poland, September 2000

RD80   SEE and TID Extension Testing of the Xilinx XQR18V04 4Mbit Radiation Hardened Configuration PROM, C. Carmichael et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD81   SEU and SET Mitigation Techniques for FPGA Circuit and Configuration Bit Storage Design, D. G. Mavis et al., 2000 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2000

RD82   SEU Hardening of Field Programmable Gate Arrays (FPGAs) For Space Applications and Device Characterization, R. Katz et al., 31st Annual Nuclear and Space Radiation Effects Conference, 1994 NSREC, Tucson, USA, July 1994

RD83   SEU Mitigation Techniques for Virtex FPGAs in Space Applications, C. Carmichael et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD84   Single-Event-Effect Mitigation from a System Perspective, K. A. LaBel et al., IEEE Transactions on Nuclear Science, Vol. 43, April 1996

RD85   Single Event Effects Testing of Xilinx FPGAs, G. Lum et al., 1998 MAPLD, NASA Goddard Space Flight Center, Greenbelt, Md, USA, September 1999

RD86   Single-Event Upset Susceptibility Testing of the Xilinx Virtex II FPGA, G. Swift et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD87   Single Event Upset Test Results for the Xilinx R1701L PROM, S. M Guertin, Jet Propulsion Laboratory, August 2000

RD88   Single Event Upset Test Results for the Xilinx XQ1701L PROM, S. M Guertin, 36th Annual Nuclear and Space Radiation Effects Conference, 1999 NSREC, Norfolk, Virginia, USA, July 1999

RD89   Single-Event Upsets in SRAM FPGAs, M. Caffrey et al., 2002 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2002

RD90   SRAM Based Re-programmable FPGA for Space Applications, J.J. Wang et al., IEEE Transactions on Nuclear Science3, Vol. 46, No. 6, December 1999

RD91   The Impact of Software and CAE Tools on SEU in Field Programmable Gate Arrays, R. Katz et al., 1999 IEEE Nuclear Space Radiation Effects Conference, Norfolk, Virginia, USA, July 1999

RD92   The Multiversion Design Technology of an Onboard Fault-Tolerant FPGA Devices, V. S. Kharchenko et al., 2001 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2001

RD93   Transient and Permanent Fault Diagnosis for FPGA-Based TMR Systems, S. D'Angelo et al., 1999 International Symposium on Defect and Fault Tolerance in VLSI Systems, Albuquerque, New Mexico, USA, November 1999

RD94   Total Ionizing Dose Effects in a SRAM based FPGA, D. M. McQueen et al., 1999 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 1999

RD95   Total Ionizing Dose Effects in a Xilinx FPGA, N. J. Buchanan et al., ATLAS-LARG internal note ATL-LARG-99-003, 1999

RD96   Total Ionizing Dose Performance of SRAM based FPGAs and supporting PROMs, J. Fabula et al., 2000 MAPLD, Johns Hopkins University, Laurel, Maryland, USA, September 2000

RD97   Ultra-Low Power, Radiation Tolerant, Reconfigurable Field Programmable Gate Array (FPGA) Technology Development, E. Fuller et al., Advanced Information Systems Technology (AIST) Program's NASA Research Announcement for 1999

RD98   Word-Voter: A New Voter Design for Triple Modular Redundant Systems, S. Mitra et al., 18th IEEE VLSI Test Symposium, Montreal, Canada, April 2000

2   BACKGROUND

Field Programmable Gate Array (FPGA) devices have been used in space for more than a decade with a mixed level of success. Until now, few reprogrammable devices have been used on European spacecraft due to their sensitivity to involuntary reconfiguration due to Single Event Upsets (SEU) induced by radiation. But with the advent of reprogrammable devices featuring a million system gates or more, it is not longer feasible to disregard these technologies. The FPGA vendors have already begun to develop SEU mitigation techniques in order to make their devices usable in space applications.

2.1   Re-programmable FPGAs and their potential

The capacity and performance of FPGAs suitable for space flight have been increasing steadily for more than a decade. For reprogrammable devices the increase has been from tens of thousands to millions system gates. The application of FPGAs has moved from simple glue logic to complete subsystem platforms that combine several real time system functions on a single chip, even including microprocessors and memories [RD46] and [RD36]. The potential for FPGA use in space is steadily increasing, continuously opening up new application areas. The FPGAs are more commonly being used in critical applications and are replacing ASICs on a regular basis.

Until recently only two major FPGA vendors have supplied devices for the space market: Actel and Xilinx. New vendors are planning to offer flight FPGAs: UTMC and Atmel. This report will concentrate on the reprogrammable devices from Xilinx.

In [RD75], Xilinx provides an analysis of recent progress in field programmable logic, high lightning the following areas:
- The FPGAs have become bigger, comprising several million gates and up to a million bits of on-chip memory, all contained in packages with up to 1517 leads;
- The FPGAs have become faster, allowing system clock rates up to 200 MHz and I/O speed of up to 800 Mbits/second;
- The FPGAs have become more versatile, featuring dedicated carry structures to support adders, accumulators and counters; featuring on-chip digital delay locked loops to solve the problem of clock distribution; featuring multi-standard input/output to support LVDS, etc.
- The FPGAs have also become cheaper, measuring cost per logic gate.

The potential of reprogrammable FPGAs has been presented in [RD77] and [RD26] and is repeated hereafter. Reconfigurable computing technology is still a relatively new field of study for space applications. Space environment is different from terrestrial systems in that incident radiation can cause bit flips in memory elements and ionisation failure in semiconductors. This kind of hardware faults cannot be debugged and repaired, requiring high-reliability manufacture, assembly and operating techniques. Nowadays driving force and technological base of reconfigurable computing are reprogrammable logic chips with gate densities exceeding millions of gates and capable of supporting run-time-reconfiguration. The use of run-time-reconfiguration in space will allow to modify on-board hardware by replacing faulty/outdated designs at different stages of a mission. Some example applications are: rectification of design faults, improvement of processing algorithms, alteration of system functionality in response to changed mission requirements, change of hardware configurations to reduce weight and power characteristics, etc. The authors even mention the possibility of debugging the FPGA in orbit.

With the large re-programmable devices, digital designers can use an FPGA to perform not only familiar logic functions, but also tasks that were formerly handled at the board level by separate, dedicated parts. Large re-programmable devices eliminate the need for components such as phase lock loops, voltage translation buffers, and memory when on-chip memory is sufficient. This high level of integration allows designers to reduce overall system power requirements, cut costs, and save board space.

2.2 Single event effect mitigation techniques

Current reprogrammable FPGAs are susceptible to Single Event Upsets (SEU) as will be discussed in detail in this document. There are several different approaches to cope with SEUs in digital logic that will not be discussed here at any length. In conventional digital devices, the SEUs have affected the registers and memory elements. For reconfigurable FPGAs, the SEUs also affect the functionality of the combinatorial logic. Mitigation techniques for such FPGA devices will be discussed in detail in section 5. Here follows an overview of other mitigation approaches. A general discussion on SEU mitigation is provided in [RD84] and [RD57].

A straight forward approach to SEU protection is to use Triple Modular Redundancy (TMR) for all registers. TMR refers to triple voting, a register implementation technique in which each register is implemented by three flip-flops or latches such that their vote determine the state of the register. Note that TMR can also be applied to complete designs or part of circuits, not only flip-flops as discussed here. The inclusion of TMR can be done directly in the VHDL source code, which does not necessarily require a too great an effort. An example of this is the LEON SPARC microprocessor in which flip-flops are protected with TMR directly in the VHDL source code [RD32]. There are also synthesis tools, such as Synplify from Synplicity Inc., that can replace any flip-flop with a TMR based flip-flop, without the need for rewriting the VHDL source code. A thorough discussion on TMR for FPGAs is provided in [RD82].

The problem with the above approach is that it only covers the registers and does not protect on-chip memory, neither does it handle the effects of multiple upsets. For real-time systems it is not sufficient to detect and correct SEUs, the effects should also be completely masked not to propagate to the operating system or applications software. One example of a design capable of doing this is the LEON SPARC microprocessor [RD56], which employs several different protection techniques. The effects of SEUs are not confined to the registers in digital designs, but are also present in the combinatorial logic for which there are several protection schemes proposed as in [RD59] and [RD81].

As will be later discussed, current Static Random Access Memory (SRAM) based FPGAs are not only susceptible to SEUs in user registers but also in the configuration memory. The effect of an SEU is in this case much more difficult to predict since it can effect the logical function of a design. There have been several different approaches presented to handle this problem.

One proposed approach is to triplicate the design into three identical FPGAs and to vote the outputs external to the devices, e.g. [RD31]. After a fault is detected, the faulty FPGA is programmed to remove the upset in the configuration memory and the internal state is restored by copying the user flip-flop contents of one of the other two FPGAs by means of scan chains. The fault FPGA is reconfigured to the same state as the other two devices, and the whole system can resume its operation. The disadvantages of this method are that it requires hardware

overhead for performing the voting and the scan chains, and that it will incur a down time of the system during the fault correction. A similar approach is discussed in [RD45].

An elaborate scheme for hardware diagnosis of faults that can affect TMR based systems has been presented in [RD93]. In particular the scheme allows to identify whether a detected error is due to a transient or permanent fault affecting a replicated module, or the used voter, or the proposed scheme itself. The availability of such a diagnosis scheme can be exploited to activate a suitable recovery technique for the identified fault. The proposed scheme has been designed to feature self-checking ability with respect to a wide set of possible internal faults, and has been implemented using Xilinx XC4000 FPGAs. Similar issues are discussed in [RD50].

Another novel approach to redundancy is presented in [RD60], where idle cycles in the design are used for concurrent error detection. This has been prototyped using a Xilinx Virtex device. A similar approach is discussed in [RD28] and [RD34].

In another approach described in [RD74], a tool has been developed to insert SEU protection mechanisms for registers and memory automatically in the VHDL code description, the mechanisms being based on Hamming coding and two dimensional parity arrays. The obtained reliability of the produced result is also estimated by the tool. The approach has been demonstrated using Altera EPF10K and Xilinx XC4000 FPGAs.

In [RD58], the use of a Built-In Self Test (BIST) technique and traditional fault-tolerance strategies together with configurable computing technology are introduced, in order to improve the availability of on-board computers used in space applications. The paper discusses the use of cyclic refresh of the configuration memory, TMR using multiple FPGAs, signature analysis driven refresh, etc. During the case study implementation using Xilinx FPGAs, a series of problems related to the development arose. For instance, the synthesis tools available for high-level languages (e.g. VHDL) were considered inefficient, and one has to follow strict rules to obtain good results. An FPGA design generated from a high-level language consumes more gates and represents a less preforming circuit when compared to one generated from schematic diagrams or low level structural description in VHDL. The same authors discuss similar issues in [RD54].

In [RD35], a Xilinx based application was implemented without taking into consideration any fault tolerant strategies. The main reason for that was the short mission duration, which was about 20 minutes long. The FPGA based version of the application was designed with three main goals: increased performance, increased portability, and a reduction in the number of hardware components. This illustrates potential future usage of reprogrammable FPGAs and their advantages, as well as the fact that SEU protection is not always considered to be required in all applications.

Other interesting fault-tolerance papers in which reprogrammable FPGA have been used for proof of concept are [RD27], [RD37] and [RD92].

Although there may be uncertainties about the reliability of SRAM based FPGAs in space, it is interesting to see that in [RD49] this is considered based on the fact that any amount of fault-tolerance is achievable for the target application. The application is considered possibly one of the most appropriate for trial use of SRAM based FPGAs in space due to its inherent requirement for fault-tolerance.

2.3   Other technologies

A general discussion on the use of commercial off the shelf components in harsh environments is presented in [RD41], providing an overview of Single Event Effect (SEE) problems related to FPGAs. It provides a discussion on what the benefits are of testing devices on the board-level.

Honeywell has announced that they will develop a CMOS silicon on insulator (SOI) version of the 30 000 gate, 6 400 register, AT6010 FPGA to meet the radiation hardness levels required for commercial and military space and missile systems. The radiation hardened reconfigurable FPGA will be fully compatible with Atmel Corporation's commercial FPGA, allowing users to take advantage of Atmel Corporation's FPGA design system by interchanging the commercial and radiation hardened FPGA products. The radiation hardened FPGA development effort is being funded and managed by the NASA Goddard Space Flight Center (GSFC). The status of the development was reported in [RD24]. Stating that the goals for the programme include a total dose hardness of 200 krads (Si), no SEL, and an SEU $LET_{TH} > 30$ MeV-cm^2/mg for both user storage and configuration elements.

Actel Corporation has evaluated their ProASIC FLASH based reprogrammable FPGA family. The results were presented in [RD68], concluding that SEL occurred at an LET of 37.4 MeV-cm^2/mg. Total ionizing dose measurements results of about 60 krad (Si) were presented in [RD25] and in [RD76]. A further discussion is provided in [RD69].

As presented in [RD33], a new FPGA has been designed specifically for total dose tolerance and SEU immunity in space environments. The device uses Northorp Grumman CMOS/ SONOS circuits for nonvolatile, reconfigurable programming. A new tierable and nestable directional routing architecture enables the use of good radiation hard circuit design practices and specifically avoids the use of pass gates. The FPGA contains ~4k equivalent gates, is hardened to >200krad (Si) total dose, uses SEU immune programmation storage and SEU immune logic latches, and has control lines hardened to an LET > 100 MeV-cm^2/mg for transient glitches.

A more drastic approach is presented in [RD97], where an FPGA is developed in a completely new technology which is insensitive to SEUs. The architecture is not developed from scratch, but is cloned from the Xilinx XC6200 device. The disadvantage is that the proposed FPGA is of a comparably low complexity, only 64 thousand system gates. This should be compared with current anti-fuse based FPGAs that feature 108 000 system gates.

An SRAM based FPGA processed in 0,25 μm CMOS technology by a commercial foundry, for which the manufacturer is not mentioned, is discussed in [RD90]. In addition to the already discussed SEU sensitivity in the configuration memory, several other problems such as potential micro-latchup is discussed.

Heavy ion tests have also been performed on the Altera EPF10K100 devices as reported in [RD53]. The results showed that SEFI errors were vastly dominant, because of the high SEU sensibility of the configuration memory and the JTAG controller; in this sense, the choice of the design to implement in the DUT is irrelevant. The results found are in good accordance to what is found in the literature for similar devices. A better comparison of the results and a thorough characterization of the device to heavy ions would imply the possibility of re-reading the configuration memory that, unfortunately, is not supported for these Altera devices.

2.4   Customers

To illustrate that Xilinx FPGAs are being used in different critical applications, both for avionics and space flight, three press releases from Xilinx Inc. have been summarised hereafter.

2.4.1   Avionics

Xilinx announced in 1998 the results of tests that show that Xilinx SRAM based field programmable gate arrays (FPGAs) demonstrate a low susceptibility to atmospheric radiation. The results of the tests, conducted by Ericsson Saab Avionics AB in Sweden in conjunction with Xilinx, indicate that the devices can be used without limitation in high altitude aviation environments. The tests were carried out to determine the sensitivity of SRAM based FPGAs to Single Event Upset (SEU) induced by high-energy neutrons. Xilinx FPGAs exhibited virtually no upsets due to neutron interaction, said Mattias Ohlsson of Ericsson Saab Avionics. Parts tested were from the Xilinx QPRO family of high reliability QML products, which are derived from specific foundries and mask sets. Both 5,0 Volt and 3,3 Volt Xilinx QPRO FPGA devices were irradiated by neutrons with energy of 100 MeV using the cyclotron at The Svedberg Laboratory (TSL) in Sweden. The SEU frequency for the 5,0 volt devices, containing 178 096 RAM-bits, averaged 1 bit error per 1,3 million flight hours at an altitude of 10 kilometers, or about 33 000 feet. The SEU frequency for the 3,3 volt devices, containing 283 376 RAM-bits, averaged one bit error per 275 000 flight hours at the same altitude.

2.4.2   High performance reconfigurable data processor

Xilinx and Los Alamos National Laboratory announced in year 2000 a cooperative program aimed at the development of high performance reconfigurable data processors for space-based systems. The program calls for Xilinx to provide specially processed Virtex field programmable gate arrays (FPGAs) and for Los Alamos National Laboratory to perform radiation testing of the Xilinx devices. Both parties are cooperating on applications development in high speed digital image and signal processing. Engineers at Los Alamos National Laboratory are building a reconfigurable data processing module for space-based remote-sensing applications. Heavy ion testing was conducted at the Texas A&M University Cyclotron Institute in College Station, Texas, to measure the sensitivity in the Xilinx Virtex devices to both single event latch-up (SEL) and single event upset (SEU) caused by cosmic rays in space. Extensive SEU characterization indicates that the frequency of single event upset is 4×10^{-6} upsets/bit-day in a typical geosynchronous orbit. The bit upsets that may occur can be tolerated through a combination of rapid detection and recovery and logic redundancy.

2.4.3   2003 Mars Exploration Rover

Xilinx announced in year 2001 that it has begun shipment of the one-million system-gate radiation hardened Virtex FPGAs, the XQVR1000TM device, to the Jet Propulsion Laboratory and other customers for deployment in space systems. NASA's Jet Propulsion Laboratory has one such programme that has selected Virtex devices for the 2003 Mars Exploration Rover mission. The Raytheon OPTUS space program is also using these devices. Designers of space systems are choosing Xilinx QPRO Virtex as the platform for their programmes because of density, flexibility, and cost-effectiveness. Doing costly custom ASICs or smaller one-time programmable devices is no longer practical for the increasing complexity of space missions. Additionally, the Xilinx QPRO Virtex devices, with many available IP cores, allow customers to meet aggressive development schedules since they are available off-the-shelf.

3   XILINX VIRTEX ARCHITECTURE

This section is entirely based on the descriptions found in the Xilinx Virtex data sheets [RD1], through [RD5]. A detailed description of the architecture is also provided in [RD83].

The Virtex FPGAs feature a regular architecture that comprises an array of configurable logic blocks (CLBs) surrounded by programmable input/output blocks (IOBs), all interconnected by a hierarchy routing resources. The routing resources permits the Virtex family to accommodate complex designs. Virtex FPGAs are SRAM based and are customized by loading configuration data into internal memory cells. In some modes, the FPGA reads its own configuration data from an external PROM. Otherwise, the configuration data is written into the FPGA.

Virtex devices provide better performance than previous generations of Xilinx FPGAs. Designs can achieve synchronous system clock rates up to 200 MHz including I/O. Virtex inputs and outputs comply fully with PCI specifications, and interfaces can be implemented that operate at 33 MHz or 66 MHz. Virtex supports the hot-swapping requirements of Compact PCI.

The standard Xilinx Foundation and Alliance Series Development systems deliver design support for Virtex, covering from behavioural and schematic entry, through simulation, automatic design translation and implementation, to the creation, downloading, and readback of a configuration bit stream.

3.1   Virtex FPGA features

- Densities from 50 000 to 1 000 000 system gates
- Multi-standard interfaces
  - 16 high-performance interface standards
  - Connects directly to ZBTRAM devices
- Built-in clock-management circuitry
  - Four dedicated delay-locked loops (DLLs) for advanced clock control
  - Four primary low-skew global clock distribution nets, plus 24 secondary local clock nets
- Hierarchical memory system
  - Look-up-Tables (LUTs) configurable as 16-bit RAM, 32-bit RAM, 16-bit dual-ported RAM (all named LUTRAMs), or 16-bit shift-register
  - Configurable synchronous dual-ported 4k-bit block RAMs (BRAMs)
  - Fast interfaces to external high-performance memories
- Flexible architecture that balances speed and density
  - Dedicated carry logic for high-speed arithmetic
  - Dedicated multiplier support
  - Cascade chain for wide-input functions
  - Abundant registers/latches with clock enable, dual synchronous/asynchronous set/reset
  - Internal tri-state busing
  - IEEE 1149.1 boundary-scan logic

3.2   QPro Virtex 2.5V Radiation Hardened FPGAs

As stated in [RD83], the Xilinx XQVR product line is a radiation-tolerant version of the of the commercial Virtex series FPGA. Virtex has become a common ASIC replacement in commercial markets due to its density, performance, and wide range of capabilities. The XQVR utilizes a 0,22 µm, 5-layer epitaxial process that renders it latch-up immune to an LET of 125 MeV-cm^2/mg. Although the XQVR is latch-up immune, the configuration memory SRAM cells do have susceptibility to Single Event Upsets (SEU). As stated in [RD5], the devices are guaranteed over the full military temperature range and are QML certified. The guaranteed total ionizing dose is up to 100 krad (Si). The possible packages are CB228, 228-pin Ceramic Quad Flat Package, and CG560, 560-column Ceramic Column Grid Package. The possible ordering grades are M-grade (Military Ceramic), V-grade (QPro Plus) and Class-Q (MIL-PRF-38535). Quality classes are further described in [RD20].

Device	SMD	System gates	CLB array	Logic cells	I/O	BRAM bits	LUTRAM bits
XQVR300	5962-99572	322 970	32x48	6 912	316	65 536	98 304
XQVR600	5962-99573	661 111	48x72	15 552	316	98 304	221 184
XQVR1000	5962-99574	1 124 022	64x96	27 648	404	131 072	393 216

Table 1:   *QPro Virtex Radiation Hardened Field-Programmable Gate Array family*

Symbol	Description	Min.	Max.	Units
TID	Total Ionizing Dose, Method 1019, Dose Rate ~9.0 rad(Si)/sec	100	-	krad(Si)
SEL	Single Event Latch-up Immunity Heavy Ion Saturation Cross Section, LET > 125 MeV-cm^2/mg	-	0	cm^2/device
SEU$_{FH}$	Single Event Upset CLB Flip-flop, Heavy Ion Saturation Cross Section	-	6,5E-8	cm^2/bit
SEU$_{CH}$	Single Event Upset Configuration Latch, Heavy Ion Saturation Cross Section	-	8,0E-8	cm^2/bit
SEU$_{CP}$	Single Event Upset Configuration Latch Proton (63 MeV) Saturation Cross Section	-	2,2E-14	cm^2/bit
SEU$_{BH}$	Single Event Upset BRAM Bit, Heavy Ion Saturation Cross Section	-	1,6E-7	cm^2/bit

Table 2:   *Radiation specifications*

3.3   Other QPro members

According to [RD96], the Virtex-E family, 0,18 µm and 6 metal layers, is available in the QPro product line. According to Xilinx representatives, the Virtex-II family, 0,15 µm and 8 metal layers, is being evaluated, see [RD86]. No further information is available at the Xilinx web site.

3.4   Virtex Array

The Virtex user programmable gate array comprises two major configurable elements: configurable logic blocks (CLBs) and input/output blocks (IOBs). CLBs provide the functional elements for constructing logic. IOBs provide the interface between the package pins and the CLBs. CLBs interconnect through a general routing matrix. The architecture also includes the following circuits that connect to the general routing matrix:

• Dedicated block RAM memories (BRAM) of 4096 bits each;
• Clock Delay Locked Loops (DLLs) for clock distribution and clock domain control;
• Tri-state buffers (BUFTs) in each CLB that drive dedicated routing resources.

Values stored in static memory cells control the configurable logic elements and interconnect resources. These values load into the memory cells on power-up, and can reload if necessary to change the function of the device.
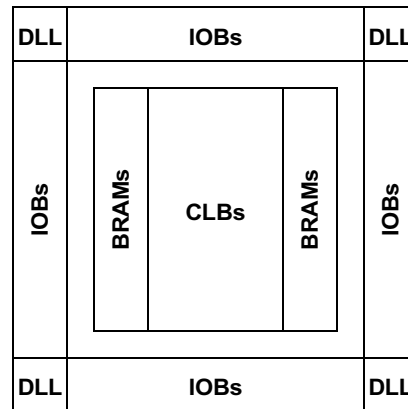
Figure 1:   *Virtex architecture overview*

3.4.1   Input/Output Block (IOB)

The Virtex IOB, features inputs and outputs that support a wide variety of I/O signalling standards. Three IOB storage elements function either as edge-triggered D-type flip-flops or as level sensitive latches. Each IOB has a clock signal shared by the three flip-flops and independent clock enable signals for each flip-flop. In addition to the clock and clock enable control signals, the three flip-flops share a common set/reset. For each flip-flop, this signal can be independently configured as a synchronous set, a synchronous reset, an asynchronous preset, or an asynchronous clear.

3.4.2   Configurable Logic Block (CLB)

The basic building block of the CLB is the logic cell (LC). An LC includes a 4-input *function generator*, *carry logic*, and a *storage element*. The output from the function generator in each LC drives both the CLB output and the D input of the flip-flop. Each Virtex CLB contains four LCs, organized in two similar slices. In addition to the four basic LCs, the CLB contains logic that combines function generators to provide functions of five or six inputs. Consequently, when estimating the number of system gates provided by a given device, each CLB counts as 4.5 LCs.

Figure 2:   *2-slice Virtex CLB*

3.4.2.1 Look-Up Tables (LUT)

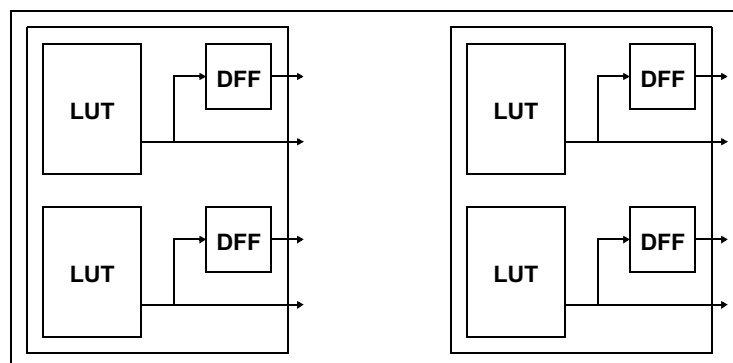Virtex function generators are implemented as 4-input look-up tables (LUTs). In addition to operating as a function generator, each LUT can provide a 16 x 1-bit synchronous RAM. Furthermore, the two LUTs within a slice can be combined to create a 16 x 2-bit or 32 x 1-bit synchronous RAM, or a 16x1-bit dual-port synchronous RAM. All these distributed memories are called LUTRAMs hereafter. The Virtex LUT can also provide a 16-bit shift register that is ideal for capturing high-speed or burst-mode data. This mode can also be used to store data in applications.

3.4.2.2 Storage elements

The storage elements in the Virtex slice can be configured either as edge-triggered D-type flip-flops or as level-sensitive latches. The D inputs can be driven either by the function generators within the slice or directly from slice inputs, bypassing the function generators. In addition to clock and clock enable signals, each slice has synchronous set and reset signals. Synchronous set forces a storage element into the initialization state specified for it in the configuration. Synchronous reset forces it into the opposite state. Alternatively, these signals can be configured to operate asynchronously. All of the control signals are independently invertible, and are shared by the two flip-flops within the slice.

3.4.2.3 Additional logic

The multiplexer in each slice combines the function generator outputs. This combination provides either a function generator that can implement any 5-input function, a 4:1 multiplexer, or selected functions of up to nine inputs. Similarly, another multiplexer combines the outputs of all four function generators in the CLB by selecting one of the preceding multiplexer outputs. This permits the implementation of any 6-input function, an 8:1 multiplexer, or selected functions of up to 19 inputs. Each CLB has four direct feed through paths, one per LC. These paths provide extra data input lines or additional local routing that does not consume logic resources.

3.4.2.4 Arithmetic logic

Dedicated carry logic provides fast arithmetic carry capability for high-speed arithmetic functions. The CLB supports two separate carry chains, one per slice. The height of the carry chains is two bits per CLB. The arithmetic logic includes an XOR gate that allows a 1-bit full adder to be implemented within an LC. In addition, a dedicated AND gate improves the efficiency of multiplier implementation. The dedicated carry path can also be used to cascade function generators for implementing wide logic functions.

3.4.2.5 BUFTs

Each CLB contains two tri-state drivers (BUFTs) that can drive on-chip buses. Each BUFT has an independent tri-state control pin and an independent input pin.

3.4.3   Block RAM memories (BRAM)

Virtex FPGAs incorporate several large block RAM memories (BRAM). These complement the distributed LUTRAMs that provide shallow RAM structures implemented in CLBs. Block RAM memory blocks are organized in columns. All Virtex devices contain two such columns, one along each vertical edge. These columns extend the full height of the chip. Each memory block is four CLBs high, and consequently, a Virtex device 64 CLBs high contains 16 memory blocks per column, and a total of 32 blocks.

Each block RAM cell is a fully synchronous dual-ported 4096-bit RAM with independent control signals for each port. The data widths of the two ports can be configured independently, providing built-in bus-width conversion. The Virtex block RAM also includes dedicated routing to provide an efficient interface with both CLBs and other block RAMs.

3.4.4   Programmable routing matrix

It is the longest delay path that limits the speed of any worst-case design. Consequently, the Virtex routing architecture and its place-and-route software were defined in a single optimization process. This joint optimization minimizes long path delays, and consequently, yields system performance. The joint optimization also reduces design compilation times because the architecture is software-friendly. Design cycles are correspondingly reduced due to shorter design iteration times.

3.4.4.1 Delay-Locked Loop (DLL)

Associated with each global clock input buffer is a digital Delay-Locked Loop (DLL) that can eliminate skew between the clock input pad and internal clock-input pins throughout the device. Each DLL can drive two global clock networks. The DLL monitors the input clock and the distributed clock, and automatically adjusts a clock delay element. Clock edges reach internal flip-flops one to four clock periods after they arrive at the input. This closed-loop system eliminates clock-distribution delay by ensuring that clock edges arrive at internal flip-flops in synchronism with clock edges arriving at the input. In addition to eliminating clock-distribution delay, the DLL provides control of multiple clock domains. The DLL provides four quadrature phases of the source clock, can double the clock, or divide the clock.

3.4.4.2 Boundary Scan

Virtex devices support all the mandatory boundary-scan instructions specified in the IEEE standard 1149.1. A Test Access Port (TAP) and registers are provided that implement the EXTEST, INTEST, SAMPLE/PRELOAD, BYPASS, IDCODE, USERCODE, and HIGHZ instructions. The TAP also supports two internal scan chains and configuration / readback of the device. The TAP uses dedicated package pins.

3.5   Configuration

Virtex devices are configured by loading configuration data into the internal configuration memory. Values stored in static memory cells control the configurable logic elements and interconnect resources. These values load into the memory cells on power-up, and can reload if necessary to change the function of the device.

Some of the pins used for the configuration control are dedicated configuration pins, while others can be re-used as general purpose inputs and outputs once configuration is complete.

The following are dedicated pins:
• Configuration mode pins
• Configuration clock pin
• Program and Done pins
• Boundary-scan pins

Depending on the configuration mode chosen, the configuration clock can be an output generated by the FPGA, or it can be generated externally and provided to the FPGA as an input. Note that some configuration pins can act as outputs.

3.5.1   Configuration modes

Virtex supports the following four configuration modes
• Slave-serial mode
• Master-serial mode
• SelectMAP mode
• Boundary-scan mode

The configuration mode pins select among these configuration modes with the option in each case of having the corresponding IOB pins either pulled up or left floating prior to configuration. Configuration through the boundary-scan port is always available, independent of the mode selection. Selecting the boundary-scan mode simply turns off the other modes. The three configuration mode pins have internal pull-up resistors, and default to a logic high if left unconnected.

3.5.1.1   Slave-serial mode

In slave-serial mode, the FPGA receives configuration data in bit-serial form from a serial PROM or other source of serial configuration data. The serial configuration bitstream is fed synchronously to the FPGA. Multiple FPGAs can be daisy-chained for configuration from a single source.

3.5.1.2   Master-serial mode

In master-serial mode, a clock output on the FPGA drives a Xilinx serial PROM that feeds bit-serial data to the FPGA. After the FPGA has been loaded, the data for the next device in a daisy-chain is presented synchronously on an output from the FPGA: The interface is identical to slave-serial except that an internal oscillator is used to generate the configuration clock. A wide range of frequencies can be selected for this clock which always starts at a slow default frequency. Configuration bits then switch configuration clock to a higher frequency for the remainder of the configuration. Switching to a lower frequency is prohibited.

3.5.1.3   SelectMAP mode

The SelectMAP mode is the fastest configuration option. Byte-wide data is written into the FPGA with a busy flag controlling the flow of data. An external data source provides a byte stream. Data can also be read using the SelectMAP mode. Configuration data can be read out of the FPGA as part of a readback operation. In the SelectMAP mode, multiple Virtex devices can be chained in parallel

3.5.1.4   Boundary-scan mode

In the boundary-scan mode, no non-dedicated pins are required, configuration being done entirely through the IEEE 1149.1 Test Access Port (TAP). Configuration through the TAP uses the CFG_IN instruction. This instruction allows data input to be converted into data packets for the internal configuration bus.

3.5.2   Configuration sequence

The configuration of Virtex devices is a three-phase process. First, the configuration memory is cleared. Next, configuration data is loaded into the memory, and finally, the logic is activated by a start-up process. Configuration is automatically initiated on power-up unless it is delayed by the user. The configuration process can also be initiated by the user.

3.5.3   Readback

The configuration data stored in the Virtex configuration memory can be readback for verification. Along with the configuration data it is possible to readback the contents all flip-flops/latches, LUTRAMs, and BRAMs. This capability is used for real-time debugging etc.

4   SINGLE EVENT UPSET SUCEPTIBILITY

The Virtex FPGAs are susceptible to SEUs in different parts of the FPGA architecture. To understand the discussion on mitigation techniques one needs to understand the susceptibility of the architecture and how testing has been performed to determine the corresponding effects. Single Event Latchup (SEL) and Total Ionizing Dose (TID) will be discussed in section 6.

4.1   Upsets categories

According to [RD75], Single Event Effect (SEE) induced upsets in the Xilinx SRAM based FPGAs can be grouped into three categories: configuration upsets, functional upsets in user logic, and architectural upsets. The physics are the same for all, but the observability and consequences vary. Upset categories are also discussed in detail in [RD66] and in [RD65], using the same vocabulary. In [RD52], a slightly altered vocabulary is used, but the same partition between categories is kept.

According to [RD75], there are two main objectives behind understanding the upset rate and the contribution of these different upset categories. Firstly, one wants to understand all the possible mechanisms that introduce functional errors. Secondly, to assess the severity of the upset problem, one needs to understand the frequency and its consequences. These factors determine the cost of mitigation measures and where they are most effectively directed.

4.1.1   Configuration upsets

According to [RD75], configuration upsets occur in the configuration memory and can be detected by readback of the programmed configuration memory. The likelihood of failure depends on which bit is upset, and the specific design utilization of the device resources. Most static bits in the device are accessible via readback. There are normally more than a million configuration bits stored and the cross-section per bit for heavy ions and protons is low. Accordingly the static bit cross-section for the part is equal to the product of the number of bits and the cross-section per bit. The actual cross-section will be less because not every bit upset will be significant in a given design. In[RD17], a similar definition is used for the XQR4000XL series devices, where the configuration memory is also referred to as the *basement*.

According to [RD83], the readback function is an efficient means for SEU detection. If a particle penetrates the susceptible portion of a configuration memory cell and thus alters its state, a readback and verification of the configuration data will detect the upset. To perform a verification (SEU detection), the configuration data is readback from the device and compared to the configuration memory bitstream.

In [RD65], it is concluded that the reprogrammable nature of the FPGA presents a new sensitivity due to the configuration memory bitstream. The function is determined when the bitstream is downloaded to the device. Changing this data changes the design's function. While this provides the benefits of adaptability, it also makes the device vulnerable to inadvertent SEU reconfiguration upset. A device configuration upset may result in a functional upset.

The term Single Event Reprogramming (SER) is discussed in [RD67], describing the effects of SEUs in configuration memory of a re-programmable FPGA. As concluded in [RD41], the consequence of an SEU in a configuration bit varies from no effect to destruction of the device.

4.1.2   User logic upsets

According to [RD75], the user logic contains elements that are not directly testable for upset through the configuration memory bitstream. Although most of these elements are accessible through readback of the configuration memory, their contents are subject to change due to normal logic operation. These elements include block memory, logic-block flip-flops and I/O flip-flops. Operational upsets can only be mitigated with redundancy in the user's logic design. Observability is limited unless the user design can capture an event. In[RD17], a similar definition is used for the XQR4000XL series devices. Where the user logic is also referred to as the *first floor*.

4.1.3   Architectural upsets

According to [RD75], architectural upsets occur in the control elements of the FPGA (e.g. configuration circuits, JTAG TAP controller, reset control, etc.). SEUs in these elements are often only detectable indirectly by observing an upset signature and associating it with a control element function. This type of upsets are also referenced as Single Event Functional Interrupts (SEFI), as in [RD83].

4.2   Testing approaches

According to [RD71], there are two approaches to SEU testing, static and dynamic, when to measure the upset characteristic of each of the storage latches present in an FPGA. For the Virtex FPGA it is easy to measure the static characteristic since a serial scan capability exists for each configuration routing bit and for the BRAM, CLB, and other functional blocks of the part. The XQVR300 tested included the accessible static bits listed in table 3.

Latch type	Function	Number of bits
CLB	Configuration Logic Blocks	6 144
IOB	Programmable IO Blocks	948
LUT	Look Up Tables	98 304
BRAM	Block RAM	65 536
	Routing & other Bits	1 579 860

Table 3:   *Latch types in the Virtex XQVR300 FPGA*

Dynamic SEU testing is needed to test what static testing misses. Even though it is possible to interrogate more than 1,7Mbits on the XQVR300, there is much more circuitry that is not tested which the authors generally refer to as combinatorial logic; that is, the circuitry that connects the latches together. Moreover, in dynamic operation, transient signal propagation can be upset if an ion strike occurs along such a path, and the sensitivity can vary with operating frequency. These additional sensitivities can add to the total cross-section of the device.

To summarise, static SEU testing only determines the sensitivity of each memory element, without observing the effects on the functionality of the application. Dynamic SEU testing takes the functionality of the application into account.

4.3   Sensitive structures

In [RD18], mitigation techniques are discussed from the architectural view point for the Xilinx Virtex technology. The document provides a division between different types of problems that can occur due to SEUs and provides ways of mitigating them. In this section only the different problem areas will be presented, leaving the mitigation techniques for a later discussion.

4.3.1   General logic

General logic should be seen as all user logic not using any of the special features of the architecture.

4.3.1.1   Sequential logic

Sequential logic comprises all storage elements that are not implemented with BRAMs, LUTRAMs and shift-registers in LUTs. Finite State Machines (FSMs) are normally built with sequential logic.

4.3.1.2   Combinatorial logic

Combinatorial logic does not comprise any storage elements.

4.3.1.3   Half-latch structures

In [RD89], it is reported that so called half latches, which generate many of the constant "0" and "1" values used by Xilinx designs, are susceptible to SEUs. When upset, the output values of these circuits will remain inverted until the device is fully reprogrammed. Further, this inversion is not directly observable, making it hard to know whether or not a design is functioning normally based on tests that validate the FPGA devices' programming bit streams. Approaches that modify designs earlier in the process are less likely to eliminate all half latches since synthesis, technology mapping, and, possibly, placement and routing may introduce half latches into the design implementation. Careful design may insure that half latches are never used in the design in the first place, but this will require fairly involved design practices, such as requiring that the explicitly generated constant values be connected throughout the design so that half latches are not introduced. As an additional complication to these approaches, design practices which worked for older synthesis and technology-mapping tools may not work for new tools as synthesis and technology mapping techniques evolve.

4.3.2   Special architectural features

While the majority of any logic design can be realized in Look-Up Tables, flip-flops, and routing, there are other special features specific to the Virtex architecture that allow for more efficient and higher performance implementations. These features include BRAM, LUTRAM, shift-registers, arithmetics, and clock DLLs. The special architectural features of the Virtex technology have been discussed to some extent earlier in section 3.

4.3.2.1   Input/output logic and flip-flops

The Input/Output Block (IOB) provides a large flexibility, but can also be vulnerable to SEUs. The potential risks are that inputs are reconfigured to outputs etc., which can lead to part stress. Also from a logical perspective, loss of functionality of an input or an output can lead to failures

on the application level. Note also that IOB have built-in flip-flops that can contribute to user logic upsets. Simulation of the SEU sensitivity of the IOB has been presented in [RD78], concluding that there is no sever effect of a single configuration bit being altered by an SEU.

4.3.2.2 BRAM

The BRAMs are sensitive to SEUs and they can be used in several ways in a given design. They are accessible from the user logic as well as via the configuration interfaces.

4.3.2.3 Clock buffers

SEUs on the clock lines or buffers in an FPGA can cause unwanted behaviour.

4.3.2.4 Clock DLLs

The DLLs can be used in conjunction with the clock buffers to re-synchronize the clock signal to its own path skew or an external reference to decrease clock-to-output delays. However, an SEU in the DLL circuitry can have the effect of unsynchronizing the DLL. This can result in jitter or complete loss of the output clock signal.

4.3.2.5 Arithmetic carry chains

Arithmetics, such as counters and adders, are most efficiently implemented using the carry-chains embedded within the CLBs. The typical user is not likely to build carry-chain structures at the primitive level, but will likely instantiate library macros that utilize these features or infer their usage when synthesizing a design. However, neither the standard Xilinx library nor synthesis libraries take SEU issues into account.

4.3.2.6 Distributed LUTRAM and shift-register LUTs

LUTs may be used as small blocks of distributed LUTRAM elements (e.g., RAMS16x1) or as dynamically addressable shift-registers (e.g., SRL16) in the user's design. When a LUT is used for this type of operation, the user's data content is dynamically stored and manipulated in configuration memory cells.

4.3.2.7 V_{CC} and GND extraction

A typical FPGA design is implemented with signals that were resolved to a logic constant but which could not be entirely optimised out of the design. When V_{CC}s and/or GNDs are implemented by the place and route tools, they are implemented in a way that maximizes device resource utilization. This is accomplished by utilizing keeper circuits that exist at the input pins of all CLBs and IOBs.

Keepers lie in series with routing channels and logic block input pins. When the routing channel carries an active signal, the keeper is transparent. But when the channel is unused, the keepers keep its last known value, which was determined when the device was initially powered-up or re-initialized by activating the FPGA input Program pin.

When a logic element (e.g., flip-flop) inside a logic block (CLB or IOB) requires a logical constant, such as a V_{CC} or GND, this logical constant can be obtained from the keeper circuit

of an unused pin of the logic block. Its polarity can be selected by programmable inversion within the logic block.

An SEU can upset or alter the state of a keeper circuit either by direct ionization, or indirectly by momentarily connecting an active routing channel to the input of the keeper. In either case, the result is a functional disturbance that cannot be detected by readback nor corrected by partial reconfiguration. Therefore, this type of error is known as a persistent error, and it can only be corrected by completely re-initializing the FPGA.

4.4   Single Event Functional Interrupt

Several different types of Single Event Functional Interrupts (SEFI) are discussed in [RD83] and are summarised hereafter.

4.4.1   Device de-configuration

The Power-On Reset (POR) circuitry contains three SRAM cells and one flip-flop register that signal when a successful power-up has completed. This signal will initiate an initialization process, which clears configuration memory to prepare the device for configuration. Upsetting one of these four storage elements will re-initiate the initialization process requiring that the device be re-configured. This phenomenon was observed during heavy ion testing.

4.4.2   Interruptions from JTAG operations

The JTAG/Boundary-Scan circuitry has a standard susceptibility similar to that present on any device technology which utilizes this functionality. The standard TAP controller implementation is a 4-bit binary encoded state-machine. A single event upset to one of these registers can move the controller to any of the available TAP states. This carries the possibility of activating the boundary-scan registers and disengaging the I/Os from standard operation. A discussion on failures related to SEU induced problems in the JTAG TAP controller is also provided in [RD42] and [RD71].

4.4.3   Activating output drivers on an input pin

For any given single input multiple configuration cells must be upset to activate the output driver for a single IOB. Though this condition is extremely unlikely, such a condition could cause bus contention. As listed in [RD67], an SEU may cause two output drivers internal to the chip to be connected, resulting in an unintentional high-current state which may exceed current density requirements for reliable operation.

4.5   Other potential problems

There has not been much discussion on the impact of software tools for designing the Xilinx FPGAs. Experiences from once-only programmable technologies have shown that the impact on SEU issues can be rather severe. One observed effect is that the synthesis tools actually remove the redundancy circuitry that has been added to mitigate the effects of SEUs in the first place. It has also been reported that some place-and-route tools even insert flip-flops in the design, which could ruin any SEU mitigation technique. A general discussion on this subject is provided in [RD91].

5   SINGLE EVENT UPSET MITIGATION TECHNIQUES

To counter act the consequences of SEUs in the Xilinx Virtex technology two very different approaches can be taken as will be discussed hereafter. By detecting and correcting SEUs in the configuration memory, one ensures that the functionality of a design is not corrupted. By detecting and correcting SEUs in the user logic, one ensures that the data being processed by a design is not corrupted. The best results seem however to have been obtained by combining the two approaches as will be discussed in section 6. These techniques are presented in [RD18], [RD19] and [RD65]. [RD83] also provides a discussion on some of the different techniques presented in this section. A good summary is provided in [RD44].

5.1   Configuration memory protection

In [RD19], the correction of SEUs through partial re-configuration of the configuration memory is presented in detail. To better understand the discussion, a careful review of [RD15] and [RD16] is recommended.

In [RD83], an approach to SEU correction is discussed which leads to complete re-configuration of the FPGA design. This includes the de-configuration of the FPGA, which would lead to loss of data and context, as well as interruption of operation that is not desirable. The reset of this section will concentrate on partial re-configuration which can be performed while the device is operating without interrupting its operation.

In [RD19], two SEU correction methods are discussed: SEU detection and single frame correction, and SEU scrubbing.

In the first method of SEU correction is to use configuration memory readback to detect when an upset to the configuration memory has occurred. When an upset is detected only the data frame that contains the effected bit need be corrected. Using this method of writing only a single data frame, and only after an upset has occurred, means that the configuration logic will be in write mode for the shortest amount of time. Most of the time the configuration logic will be in read mode. This decreases the probability of an upset to the configuration logic itself from having any adverse effects to the configuration memory array. However, this method also requires system overhead and support for the readback and detection of SEUs in the configuration memory. Using readback for SEU detection requires a hardware implementation of algorithms for reading and evaluating each data frame. Additionally, memory space is needed to store constants and variables.

In the second method of SEU correction, readback and detection of SEUs is committed and the entire CLB Frame segment is reloaded at a chosen interval. This is called scrubbing. Scrubbing requires substantially less overhead in the system, but does mean that the configuration logic is likely to be in write mode for a greater percentage of time. However, the cycle time for a complete scrub can be made relatively short as the SelectMAP interface is capable of operating at a high throughput. Additionally, the chosen interval for scrub cycles should be based on the expected static upset rate for a given application or mission, and may be fairly infrequent. A longer cycle interval and shorter cycle time decreases the total percentage of time that the configuration logic is in write mode. Scrubbing is discussed in [RD77] in view of an application.

As discussed in [RD83], an additional method of SEU detection could be for the FPGA to signal the host system when an upset occurs. This can be done without the use of readback and provides the additional capability of identifying SEFI, or transient upsets, which readback and verification would be oblivious to.

5.2 User logic protection

As stated in [RD83], in some systems SEU detection and correction alone can achieve an acceptable level of reliability. However, for applications where an even higher level of reliability is needed, or simply that any interrupt in service is unacceptable, SEU mitigation techniques may be applied. A good SEU mitigation technique should filter out the effects of upsets, during their short existence, as well as filter out the results of transient upsets or other SEFI effects.

A commonly known method for SEU mitigation is Triple Module Redundancy (TMR) with voting. This mitigation scheme uses three identical logic circuits performing the same task in tandem with corresponding outputs compared through a majority vote circuit. The most common example of TMR is a D-type flip-flop that has been triplicated and to which a voter has been added on its output. By replacing all flip-flops in design with the circuit shown in figure 3, one would protect the design against SEUs in the flip-flops. However, this would not protect against SEUs in the combinatorial logic connecting such flip-flops. The application of TMR to different levels of the design is discussed in the subsequent sections.
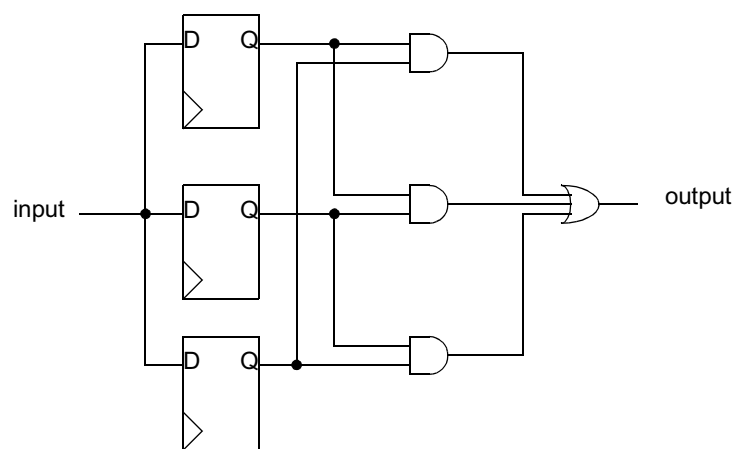

Figure 3: *Triple Modular Redundancy with voting*

5.2.1 Module level mitigation

In [RD83], several approaches to mitigation implementation of varied complexities along with their associated trade-offs, advantages and disadvantages are presented. These approaches are summarised in the subsequent sub-sections.

It should be noted that all of these approaches can be graded to have a coarse granularity of protection, since discussing the mitigation on functional block level. This type of mitigation does not automatically allow that the internal state of an application is maintained after an SEU because the detection and correction of the error is made on module level.

5.2.1.1 Module redundancy and mitigation

A very simple method for implementing SEU mitigation in a user's FPGA design is to replicate redundant instances of an entire module and mitigate the final outputs of the modules. In this case a module may represent either the entire design for a particular device or a sub-component of that design. This is a very effective means of SEU mitigation that is easy to implement and can be performed entirely within a single device as long as the user's design does not utilize more than a third of the total device. It is however not possible to restore the state of a module that has been upset without elaborate correction methods.
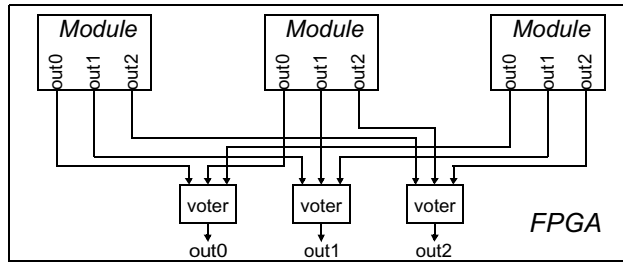
Figure 4:   *Module redundancy*

5.2.1.2 Logic partitioning for mitigation

In the case where the total design is more than a third of the device size, the design could be partitioned into modules small enough to be replicated and mitigated within a single device, and spread across several devices.
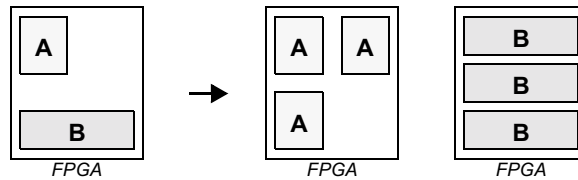
Figure 5:   *Logic partitioning for mitigation*

5.2.1.3 Logic duplication and mitigation

In the case where the design is less than half the size of the total device, an alternative to logic partitioning is logic duplication. If logic is duplicated and outputs are compared, whenever one set of outputs differ an SEU or SEFI has been detected. An advantage to this method is that it is a form of device redundancy without the need for any external mitigation devices. This is significant because in the case of a device failure the redundant device would continue processing. A disadvantage may be additional noise due to skew in the output transitions times.
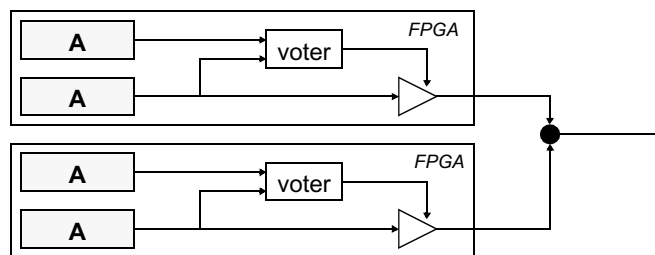
Figure 6:   *Logic duplication for mitigation (the outputs are tri-stated on error detection)*

5.2.1.4 Device redundancy and mitigation

Triple device redundancy and mitigation is the most solid mitigation method. It has the highest reliability for filtering single and multiple event upsets, multiple transient upsets, and any other functional interrupts including total device failure. However, this is also the most costly solution and provides only a marginal actual improvement over alternative methodologies.
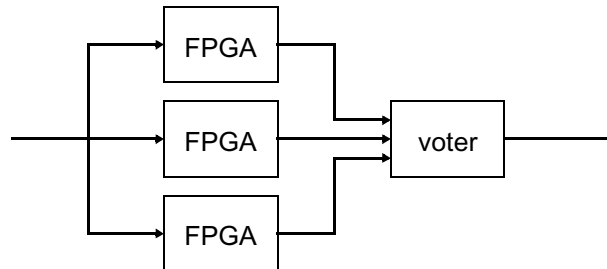

Figure 7:   *Device redundancy*

5.2.1.5 Module level mitigation disadvantages

The disadvantage of all module level mitigation techniques is that they do not provide a simple and robust recovery mechanism after an error has been detected in one of the modules. In general logic with sequential elements, it is not ensured that the error will be detected until it is manifested on the output of the module where it is compared with the outputs of the redundant modules. The internal state of the erroneous module can at that stage be very much different from the state of the redundant modules. Any further execution will be meaning less since the erroneous state will not be automatically recovered from. The probable consequence is that the application has to be reset or some other means of action has to be take to resynchronise the modules. This will lead to loss of data and operational down time.

5.2.2 Gate level mitigation

In [RD18], mitigation techniques are discussed from the architectural view point for the Xilinx Virtex technology. Emphasis is put on protecting the user logic on the gate-level. These approaches are summarised hereafter. An interesting discussion on TMR is provided in [RD82].

5.2.2.1 Logic replication and voting

A distinction between *through logic* (or combinatorial logic) and *sequential logic* (such as the flip-flops in an FSM) is made. Since SEUs can affect both the sequential logic and the through logic, the through logic needs to be made redundant as well. The importance of feeding back the voted result to all voted sequential elements is discussed. This is done to restore the state of all redundant sequential elements and to avoid error build up. The voting for the redundant through logic can be performed after the sequential elements, before the sequential elements or through out the through logic, depending on what level of protection that is required.
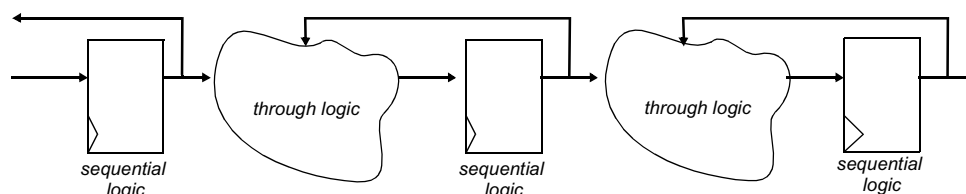

Figure 8:   *Sequential and through logic (combinatorial or combinational logic)*

An approach to using tri-state buffers for implementing the voting circuitry is discussed, noting that the buffers are actually implemented with a logic tree. This is an important feature since these tri-state buffers do not consume any logic resources for implementing voting cicuitry.
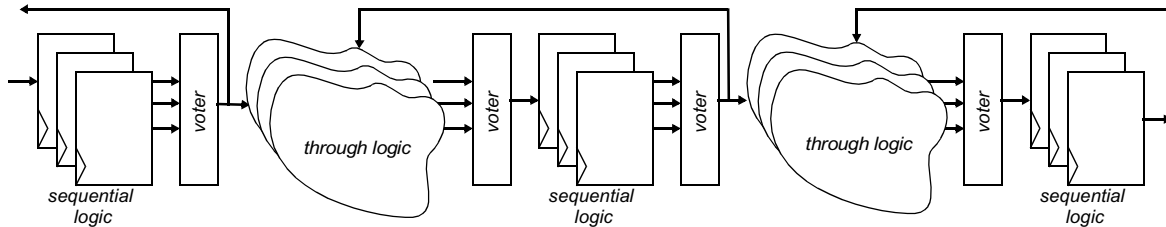

Figure 9:   *TMR for sequential and through logic at gate level*

5.2.2.2   Implementing TMR for I/O logic

A further discussion is provided on protecting input and outputs applying TMR, the basic idea being to use redundant tri-state drivers for the output that are voted by means of logic and impedance state on the printed circuit board. It is mentioned that the sequential elements in the IOBs should not be used, since it is not possible to implement TMR with them. A discussion on inter-FPGA communication is also provided.

5.2.2.3   Special architecture features

[RD18] also discusses the protection of BRAMs, providing two dissimilar approaches. One method is to not include any error detection and correction, but instead use triple redundant BRAMs and majority voters on the outputs. This will be sufficient for an application that is likely to write new data to all memory addresses within the time that upsets could be expected in similar addresses in the redundant blocks. This method relies on the statistical upset rate and is not the most safe and secure. However, it does allow for maximum feature usability, because no additional overhead is introduced to refresh the memory blocks. A more reliable method is to constantly refresh the BRAM contents. Since these are dual port memories, one of the ports can be dedicated to error detection and correction. But this also means that the BRAMs can only be used as single port memories by the rest of the user logic. Further discussions are provided on clock management, suggesting the use of three different clock buffers for the three different flip-flops in a TMR configuration.

Since space applications depend on the use of partial reconfiguration for SEU detection and correction in the configuration memory, it is recommended that users do not use LUTs as distributed LUTRAM elements or as dynamically addressable shift-registers, as it can cause data corruption in the configuration memory. It is recommended to use the BRAM memories for all memory functions and flip-flops for shift-registers.

5.2.2.4   Gate level mitigation advantages

The advantage of gate level mitigation techniques is that the voting between different logic elements takes place between the sequential elements. The voted result is normally fed back to the sequential elements, avoiding that an error is propagated between sequential elements. The synchronisation between the redundant parts is thus maintained. This is because each error is detected within a clock period and the state of the redundant parts will thus not differ for more than a clock period.

5.3   Alternative mitigation techniques

There are several SEU mitigation techniques that are being developed, targeting reconfigurable devices. Some of the interesting publications have been summarised hereafter in order to provide a flavour of what type of research is being conducted in this field.

A synthesis technique for designing FSMs with parity checking is presented in [RD51]. The output logic and the next-state logic of the FSM are checked independently. By checking parity on the present state instead of the next state, this technique allows detection of errors in bi-stable elements while requiring no changes in the original machine specifications.

Redundancy techniques are commonly used to design dependable systems to ensure high reliability, availability and data integrity. TMR is a widely used redundancy technique that masks faults. In [RD98], the authors present a new voter design called the word-voter that has some distinct advantages over the bit-by-bit voting schemes used in conventional TMR systems. They demonstrate the usefulness of the word-voter design in increasing the data integrity (reducing the probability of corrupt outputs) of TMR systems. The area and delay overhead of the word-voter design is compared to that of the bit-by-bit voter.

In [RD39], the authors describe logic synthesis techniques for designing diverse implementations of combinational logic circuits in order to maximize the data integrity of diverse duplex systems in the presence of common-mode failures.

5.4   Fault-tolerance in reconfigurable systems

There are several publications discussion the benefits of using the reconfiguration capabilities for improving fault-tolerance of systems. Some publications have been listed hereafter, concentrating on different techniques for locating and mitigating errors in FPGAs.

In [RD48], the authors describe the fault-tolerant computing research currently active at Stanford University. Focus is on tolerating hardware faults by means of software and targets faults caused by radiation induced upsets. An experiment evaluating the techniques developed, is currently running on the ARGOS satellite. Another focus is on fault-tolerance techniques for adaptive computing systems implemented with FPGAs.

In [RD29], the authors present a novel approach for rapidly testing the interconnect in the FPGAs each time the system is reconfigured. A low-cost configuration-dependent test method is used to both detect and locate faults in the interconnect. In [RD38], the authors present two column-based precompiled configuration techniques for tolerating permanent faults in FPGA-based systems. By compiling alternative configuration versions in the design phase, these approaches ensure fast reconfiguration, and thus an increase in system availability.

In [RD47], the authors describe a new technique for locating faulty LUTs in FPGA-based reconfigurable systems. The technique is in-place (does not alter the routing structure of the LUT network) where each configured LUT is tested exhaustively. The technique involves selective reprogramming of the LUTs and takes advantage of partial reconfiguration. In [RD30], the authors investigate memory coherence problem and propose a memory coherence technique that does not impose extra constraints on the placement of memory-configured LUTs.

6   TEST RESULTS

Various test have been performed on the Xilinx Virtex and XC4000 FPGA families from which the results will be presented in this section. The emphasis will still be on the Virtex technology, although the XC4000 family will be discussed for those cases when other results than for the Virtex have been presented.

The tests have been performed with a couple of different target applications in mind. Initial tests were performed on the commercial grade XC4000 family with the aim of investigating their suitability for high altitude avionics applications. Quite a few tests on commercial grade XC4000 and Virtex devices have been performed for various equipment to be used in the Large Hadron Collider (LHC) at CERN. The most interesting test have been performed on the radiation hard XQVR Virtex family, in which various SEU mitigation techniques have been used as will be further discussed. As will be seen hereafter, also different types of particles have been used for the SEE tests. The following presentation of test results has been subdivided in TID, SEL and SEU measurements. Tests have also been done on the PROMs used for storing the configuration data which are read by a Xilinx FPGA at configuration. The corresponding results are presented herein.

6.1   Total Ionizing Dose (TID)

Total Ionizing Dose (TID) measurements of the Virtex family have been performed either with a ^{60}Co source or as a side effect of proton testing.

In [RD70], TID measurements results for the commercial grade Virtex XCV200 devices have been presented. In a test suite using a ^{60}Co source, one device worked correctly up to 73 krad(Si), but was not possible to program any more at 83 krad(Si), for which a strong increase in current was observed. A second device worked correctly up to 65 krad(Si), but failed as the aforementioned devices at 72 krad(Si). All in all, three devices worked correctly up to 60 krad(Si) without any observed problems. All problems disappeared after twelve hours of heated annealing.

Some TID results are presented in [RD65], being produced as a result of proton testing. The device tested was the XQVR300 Virtex FPGA. At a given fluence, the accumulated TID if the part was 118 krads(Si). Increasing I_{CC} began to lower the V_{CC} requiring that the test be paused to allow the I_{CC} to return to within operating specifications and then the test would resume. This was repeated several times until a high fluence was achieved which brought the accumulated TID to 136 krads(Si).

As reported in [RD22], using a ^{60}Co source, severe problems to initialise the XQVR300 Virtex devices were observed after 45 krad(Si) accumulated total dose. To overcome the problem, a slow power-up ramp was required with the possibility to deliver more current than specified. These results are in conflict with earlier total dose tests that indicate total dose tolerance to about 100 krad(Si). However, no power cycling had been performed in earlier tests. Parameter drift measurements indicated failures at about 80 krad(Si). According to [RD96] and [RD66], the TID performance for the XQVR Virtex technology should be 100 krads(Si).

To confirm the above results, in [RD21] the power-up behaviour was studied for two XQVR300 Virtex devices in a number of total dose irradiation steps up to 95 krad(Si). The results are in

line with the earlier performed test. After a cumulated total dose of 45 krad(Si) both devices failed to power-up using a power-up ramp rate of 2 ms. By using a power-up ramp of 4 ms a cumulated dose of 55 krad(Si) was reached before first failure.

According to Xilinx, the above TID tests failed because the power supply failed to achieve a minimum voltage to power the device. This occurred because the current supply was too limited for the voltage ramp rate used in the test. A stated specification of the minimum ramp rate allowed and the maximum current allowed during power up would have resolved this issue. As a result of this experiment Xilinx will characterise the necessary requirements so that the test can be repeated using the correct power up procedure.

In [RD96], TID of 100 krads(Si) has been reported for XQVR300E Virtex-E devices.

In [RD94], test results were reported for the commercial grade XC4036XL and XC4036XLA devices. The first errors occurred after an absorbed dose of about 60 krad(Si) for the XL devices and 42 krad(Si) for the XLA devices. Most of the errors were soft errors that could be cleared with a circuit reset without having to reload the circuit configuration.

In [RD95], test results were reported for the commercial grade XC4036XL devices. An average total dose of 41 krad(Si) was absorbed before the power supply current began to increase, and 60 krad(Si) before first error occurred. Also in [RD55], test results were reported for the commercial grade XC4036XL devices, explaining the difference between hard and soft errors.

Test results of the XQR4036XL device, 0,35 μm technology with 7 μm epitaxial layer, were provided in [RD42], stating a total dose capability of 60 krads (Si) while meeting functional and parametric specifications. In [RD73], results reported for the XQR4036XL showed tolerance beyond 60 krad(Si). According to [RD96], the TID performance for XQR4000 is 60 krads(Si).

6.2   Single Event Latchup (SEL)

In [RD71], test results are reported for the XQRV300 Virtex device concluding that no SEL was observed up to an LET of 125 MeV-cm^2/mg. There was a current increase due to internal contention created by logic upsets that are accumulating throughout each run. This was observed during lower LET SEU testing. Similar results were reported in [RD66] and [RD72] According to Xilinx representatives, the XQVR300E device has been tested at Texas A&M University Cyclotron Institute and U. C. Leuven Cyclotron Facility with similar results.

In [RD62], commercial grade XC4036XLA parts were irradiated with protons. To search for SEL, one device was exposed at a maximum energy of 105 MeV to a total fluence of 5,9x10^{11} proton/cm^2. One SEL was observed. Similar results are reported in [RD85]. Test results of the XQR4036XL device were reported in [RD42], stating no SEL at an LET of 100 MeV-cm^2/mg at 125°C. In [RD73], test results reported for the XQR4036XL showed no SEL or micro-latchup even at 125°C for LETs up to 120 MeV-cm^2/mg.

6.3   Single Event Upset (SEU)

There have been several measurements of the Single Event Upset (SEU) properties of Xilinx devices. The results here after have been grouped after the type of particle source that has been used during the measurements.

6.3.1   Neutron

In [RD61], neutrons have been used for the SEU tests of the XC4010E and XC4010XL device types. When irradiating the XC4010E devices using 14 MeV neutrons, with the neutron flux $6x10^{-6}cm^{-2}s^{-1}$, no SEUs were detected. Irradiating the XC4010E and XC4010XL devices with quasi-monoenergetic 100 MeV neutrons, with a flux of $9,3x10^{-3}cm^{-2}s^{-1}$ resulted in six SEUs being recorded during nine hours. One SEU is believed to have disabled the readback capability of the affected device, not allowing further readback of configuration data during the test.

6.3.2   Proton

In [RD79], a commercial grade XCV50 Virtex device received a total of $9,9x10^{10}$ cm^{-2} of 63 MeV protons. SEUs were detected, corresponding to a cross-section of $1,7x10^{-10}$ cm^2. In [RD70], two commercial grade XCV200 Virtex devices were irradiated with 60 MeV protons. A cross-section of $1,25x10^{-8}$ cm^2 per device was obtained.

In [RD66], the XQVR300 device has been irradiated with proton with energies up to 63 MeV. The results from these measurements will be further discussed when talking about mitigation techniques during testing in section 6.4. These tests, or similar, were reported in [RD65].

In [RD62], commercial grade XC4036XLA parts were irradiated with protons of energy between 18 MeV and 105 MeV. The saturation cross-section and threshold energy were determined to be $2,7x10^{-9}$ upsets-cm^2/device and 22 MeV respectively. The FPGA was loaded with a real application that was used during the measurements. SEU detection was implemented using the built-in diagnostic in the application. After detecting an SEU, if three successive resets did not restore the circuit to an operating condition, where no errors were detected, the FPGA was reconfigured. If a circuit reset could clear an upset, the upset was assumed to have occurred in the sequential elements of the user logic. If a reset would not clear the upset, it was assumed to have occurred in the configuration memory, which would not be affected by a reset. A difference in cross-sections was observed for the sequential elements and the configuration memory. A detailed discussion on different types of SEU prediction models is also provided. Similar results have also been documented in [RD63]. In [RD64], the same application as above was used for testing XQR4036XL and XQVR300 devices, although with different proton energy levels. Being a draft document, it was not clear from the text for which of the two devices types some of the results were reported.

6.3.3   Heavy ion

In [RD66], static and dynamic SEU measurements have been performed on the XQVR300 Virtex device using heavy ions. Measurements for SEFI showed an LET threshold between 8 and 16 MeV-cm^2/mg and occurred only if the fluence exceeded 10^5 ions/cm^2. In [RD71], a characterisation of the different memory elements in the XQVR300 Virtex device, and it was concluded that the CLBs have an LET threshold of 5,0 MeV-cm^2/mg and a saturation cross-section of $6,5x10^{-8}$ cm^2, the LUTs have an LET threshold of 1,8 MeV-cm^2/mg and a saturation cross-section of $21x10^{-8}$ cm^2, the BRAMs have an LET threshold of 1,2 MeV-cm^2/mg and a saturation cross-section of $16x10^{-8}$ cm^2, the routing bits have an LET threshold of 1,2 MeV-cm^2/mg and a saturation cross-section of $8x10^{-8}$ cm^2. On the average, the part had an LET threshold of 1,2 MeV-cm^2/mg and a saturation cross-section of $8x10^{-8}$ cm^2.

In [RD52], heavy ion test were performed on the XQVR300 Virtex device. For a design with no mitigation techniques applied, configuration errors were detected at the lowest irradiation level corresponding to 2,97 MeV-cm^2/mg. Errors were also detected in the user logic, of which data swap errors were about 25% of all errors, at greater an LET greater than 2,97 MeV-cm^2/mg and with a saturation cross-section of 10^6 cm^2. An estimate of the LET threshold for SEFI errors was provided in [RD22], being around 5 MeV-cm^2/mg.

6.4   Mitigation technique validation

Various SEU mitigation techniques suggested for the Virtex devices have been validate using proton or heavy ion irradiation. In the subsequent section some of the test objects and the achieved results will be presented.

6.4.1   Counters and multiplexer application

In [RD65], the test object comprised eight multiplexed 4x8 counters, for which the state was captured in parallel and serially shifted out. The non-mitigated design occupied about a third of the XQRV300 device, to allow for TMR implementation. CLB resources were used to implement the flip-flops. The goal of the TMR version of the design was to implement identical functionality as the first design but with complete immunity to single event upsets. This is accomplished by tripling all the logic of the design. The TMR method used is specific for this architecture. Every logic node is tripled, and majority voters are placed inside register feedback paths. Additionally, a TMR output scheme is used to disable discrepant outputs. The TMR design was scrubbed by the XQRV18V04 PROM. Tests were performed using protons.

The non-TMR design was tested without configuration memory upset correction. Two different error signatures were observed. All errors were functional failures. The first category, soft errors, recovered operation with reset. The second category, hard errors, required complete reconfiguration of the device to recover operation. Soft failures cannot be attributed to configuration upset errors, or recovery with reset would not be possible. On average six configuration memory upsets are required to upset a design with no mitigation of any kind. Soft errors, those not due to configuration errors, accounted for 45% of the total errors in all tests with no mitigation (TMR or configuration memory bitstream scrubbing).

The TMR design was also tested in the same fashion, without configuration memory correction. There were two significant differences observed for the TMR test. The first difference was that no soft errors were observed. All functional errors were due to accumulated errors in the configuration memory and required reconfiguration in order to recover. The second difference was a dramatic increase in the number of accumulated configuration bit errors prior to functional error. The observed minimum number of configuration upsets to functional error was 23, with an average of 139 bit upsets. This demonstrates that the TMR design is functionally immune to SEUs in the configuration memory, CLB flip-flops, and combinatorial logic.

Scrubbing of the configuration memory was then used to correct configuration errors in the TMR design as they occurred. Based on previous observations the expectation was that there would be no functional errors observed other than upsets in the control logic. The desire for these test runs was to test until the control logic was upset. No SEU related functional errors observed nor was the control logic successfully upset. No significant difference can be achieved with either TMR or scrubbing by themselves. However, combing TMR with scrubbing the

design was observed to be functionally immune to upsets. However, this mitigation scheme is not immune to control logic upsets (architectural).

6.4.2   Finite Impulse Response filter application

In [RD66], a design used in the XQRV300 device was made up of a Finite Impulse Response (FIR) filter. One section of BRAM stored data and coefficients, and another section stored expected results. A comparator circuit detected failure when the filter output disagreed with the expected value. Both with and without redundancy, the design self checked for errors with a redundant comparator. TMR was implemented in all areas of the function; filter, BRAM, and comparator. The filter outputs flow into a redundant comparison circuit, all of which reside in the test object. Should an error occur in one of the redundant digital filter legs, the comparator latches an error condition. Should an error occur in the redundant comparator the then an error flag is also raised. A self-testing design was amenable to the test fixture and simple to test.

In [RD66], a second design is reported. The goal of the second design was to develop a configuration for the device under test that utilized a large proportion of the resources in order to give the results statistical significance. The principal resources being considered are the CLB flip-flops, BRAM, LUTs and DLLs. The design is actually a combination of two, including one exclusively for LUTs and flip-flops and one focusing on the BRAM. The BRAM portion treated each block as a 511x8 FIFO that is filled with a random number generator. Once full the output of the FIFO is continuously compared to an identical random number generator, the comparison providing an indication of upset. No differentiation is made between an upset that occurs in the random number generator, the FIFO, or the comparison circuit. The outputs of 16 test FIFOs were logically OR-ed together and monitored by software. For each FIFO, the input generator operated from a different DLL than the generator that sourced the comparison to determine any increase sensitivity from the clock management circuit. The BRAM test configuration utilized 100% of the available BRAM and 24% of the available logic slices. The CLB portion partitions the available CLBs into two large shift-registers where the shift register used both LUTs and CLB flip-flops. Each shift register was clocked with the clock from a separate DLL. Each shift register was fed by the same oscillating flip-flop. Output from the two shift-registers was compared to detect upset, with an output monitored by software. This design utilized 95% of the available slices. Similar, or identical designs, were described in [RD71] and [RD72].

Several observations were made after the test. First, no significant difference exists between the first and second non-TMR test designs. Given that the second design utilizes much more of the available resources of the XQVR300 it could have been expected that its sensitivity would have been greater. With only two designs tested, more work is required to determine how much the device sensitivity varies from one design to another. Second, the first design without TMR performs no better with configuration memory mitigation. No advantage is demonstrated by the use of scrubbing techniques alone. The FIR with TMR design showed improvement with redundancy alone and even more improvement with configuration memory mitigation incorporated. It is clear that there is still a significant cross-section even with both mitigation techniques employed, suggesting another (perhaps architectural) avenue for error introduction. The dynamic cross-section is less than the static cross section as would be expected from the discussion above, i.e. not every configuration upset contributes to a failure.

6.4.3   Shift-register application

In [RD52] and [RD22], a design comprising 14 shift-registers with 144 elements is described. The registers are implemented using D-type CLB flip-flops only. The design also comprises a self-test module. The design utilises about a third of a XQVR300 devices. The non-TMR design is a standard design practice without any redundancies or circuits for SEU mitigation.

The corresponding TMR design utilises full internal triple redundancy. The outputs of the TMR design use triple tri-state drivers to filter data errors from the output. The TMR version uses the TMR design techniques that Xilinx recommends for use with the Virtex FPGA. It use the same design rules as have been used in SEU tests reported in [RD66].

During the irradiation tests, the test controller was continuously scrubbing the test object configuration memory with new configuration data from the PROM. All data from the PROM to the test object was transferred through the parallel SelectMAP interface, which supports the partial configuration feature making it possible to continuously scrub the device with new configuration data during operation.

For the TMR design tests, with the exception of one test run, the SEFI error was the only observable error. This demonstrated that the TMR design method effectively eliminated all non-SEFI configuration induced errors. The SEFI error is believed to be an SEU in the power-on reset control register, clearing the whole device from configuration data. All I/Os are tri-stated in this state and this was detected at the read out data, which slowly went from read high state to read low state after some test cycles. In one test run a routing error was observed. With a too high flux/scrub-cycle ratio we have an increased risk to have errors in two modules at the same time, which could give error in the majority voting circuit. The observed routing error is most likely an artifact of the flux/scrub-cycle ratio. Only one error in the flip-flops was observed. No other flip-flop errors were recorded in absence of a SEFI error. The flip-flop error was recorded in the same test run as the routing error was recorded and it is considered that this error is the result of the flux/scrub-cycle ratio as previously mentioned.

6.4.4   Real applications

As can be seen in the preceding sections, few tests, e.g. [RD63], have been performed on actual applications. The design used during tests have all been oriented towards simplifying the test procedures, which is understandable. However, to be able to assess the benefits of the various mitigation techniques, more complex and realistic applications need to be developed and tested. A candidate application could be the LEON SPARC microprocessor [RD56], since it is already designed to accommodate TMR on flip-flop level etc.

Another characteristic of the preceding tests is that they have been designed, in general, to detect any errors due to SEUs and to diagnose the cause. In real applications, the diagnostics might not be of great importance, as long as the error is eventually corrected by scrubbing the configuration memory and there is no loss of functionality.

A test on a real application would cover all aspects of using re-programmable devices, since issues such as I/Os, DLLs, clock trees etc. would have to be addressed in a realistic manner. This would also cover issues around system availability etc. as discussed to some extent in [RD72].

6.5   Xilinx PROM

As stated in [RD88], the configuration PROM is critical for space applications, because any errors in the PROM will cause erroneous configuration of the FPGAs with which it interfaces. The continuous monitoring capability proposed by Xilinx requires checking the on-chip configuration memory contents against a known good copy, presumably from the off-chip PROM. Thus, the various PROM upset phenomena observed and discussed hereafter will cause malfunctions of configuration monitoring, making spacecraft usage more problematic.

6.5.1   Xilinx XQ1701L PROM

This section is entirely based on the test results and conclusions reported in [RD88].

In [RD88], test results are presents for the 3.3 V 1 Mbit serial XQ1701L PROM [RD10] that is designed to interface with Xilinx FPGAs and provide the initialization sequence. This device has a storage capacity of 1048576 bits and is fabricated on a bulk substrate. It can be operated in a low-current stand-by mode as well as in a normal mode. The device is a one-time-programmable read-only memory with a serial output. It is compatible with the configuration requirements of a number of 3.3 V Xilinx XC4000 and 2.5 V Virtex FPGAs.

The device was tested for single event effects with heavy ions. Latchup was observed with an LET threshold of 55 MeV-mg/cm^2 and a saturated cross-section of 10^5 cm^2. Three types of upsets were measured: address errors, premature end-of-program signals, and functional interrupt. The first two types of errors could be recovered from by applying a reset signal to the device, but the third type of error could only be recovered from by cycling the power. Several events were observed where part functionality was lost, and the operating current decreased to very low values, implying that the device had been triggered into a standby-like operating mode. However, the only way to recover from this mode was to initiate power cycling, which is not required to recover from normal standby.

All three types of functional errors had similar threshold LET values and cross sections. The PROM is also susceptible to latchup, but only at relatively high LET (40 MeV-cm^2/mg). Because of the high threshold LET, the probability of latchup is relatively low in these devices, and the risk is probably acceptable for most applications.

Proton testing was not done, but other devices on bulk substrates have been sensitive to proton upset when the LET threshold was below approximately 8 MeV-cm^2/mg. Although proton testing was not done, the low threshold LET makes it likely that protons will cause all three upset phenomena in the PROM to occur.

One way to mitigate SEU effects in these devices is to control the time period during which they operate. Since they are only used to initialize FPGA devices during start-up periods, it is relatively straightforward to minimize the time which they are powered. An alternative approach is to cycle the power in the PROM just before configuring or reconfiguring the FPGA devices that are driven by the PROM to avoid the functionality errors that can be induced by SEU effects. However, this is less desirable because latchup, if it occurs, would continue for extensive periods until the next power cycle occurs. Either approach precludes continuous comparison of the FPGA configuration with the PROM.

SEE effects in the XQ1701L do not preclude its use in space, but designers must choose between assuming the small risk of mission failure or assuring that the functional errors caused by heavy ions do not cause catastrophic system effects.

6.5.2   Xilinx R1701L PROM

This section is entirely based on the test results and conclusions reported in [RD87] and summarised in [RD23].

In [RD87], the results are reported from the irradiation testing of the Xilinx R1701L 3.3 V 1 Mbit serial PROM [RD10] which took place at the SEE Test Facility, Brookhaven National Lab. The R1701L is a special version of the standard commercial XQ1701L PROM that is fabricated on an epitaxial substrate, 7 µm thick, in order to reduce susceptibility to latchup. Latchup was not observed in the R1701L part up to an LET of 120 MeV-cm^2/mg (σ_{LU}<5x10^{-8}cm^2), indicating that the processing change was successful in improving the latchup hardness of the device. According to the manufacturer's data sheet [RD10] the R1701 configuration PROM is single event bit upset immune.

In [RD23] it is however concluded that the radiation characteristics specifies SEFI$_{MAX}$ as 1,2x10^{-5} cm^2/*device* as the heavy ion saturation cross section, with 10% of the saturated cross section at an LET of 6.0 MeV-cm^2/mg. For these tests there were five possible error modes: latchup, bit stream error, address failure, end-of-pass assertion failure, and SEFI. Of these, only the last three were observed in the XQR1701L testing. Single event latchup was not seen with a total fluence of 2x10^7/cm^2 ions at a LET of 120 MeV-cm^2/mg. No clearly identifiable bit-stream errors were seen (cross-section less than 5x10^{-6} cm^2/*device* based on counting statistics).

The first error mode seen was address failure. Most of the time this appeared to result from a single bit upset in the internal address register (or counter). However, a significant fraction (~40%) of address errors were a reset (to zero) of the address register. Occasionally, two or more bits of the address register were upset; this appears to be consistent with Poisson statistics.

The second error mode observed was the end-of-part (EOP) assertion failure. An EOP error is constituted by a discrepancy between the end-of-data (indicated by the device pin) and the actual known end-of-data as verified by address location. Virtually all end-of-part failures were an assertion of the end-of- part pin signal when the data stream was reading out from other parts of the device.

The third and most important error seen on this hardened version of the device was low current functionality interrupt, designated as *stuck at 0* because the output hangs low. Two features of this mode are the apparent continued operation of the internal address register, and an occasional logical high reading at the output pin. The first feature suggests that this interrupt may only be turning off the output pin. The second seems to confirm this. It seems likely that the output pin is being tri-stated by the error condition, leading to the possibility that occasional high output value may be latched into the testing circuitry.

It is stated in [RD87], that it is important to note that latchup may not be the greatest concern for this device, depending on the application, because the special version of the part is still susceptible to single-event upset effects. Careful consideration must be given when using these devices for space applications to allow for the various single event upset effects and their impact

on FPGA devices that are interfaced to the PROM. Total ionizing dose measurements for the device have been presented in [RD96], claiming usability in applications up to 60 krads (Si).

6.5.3 Xilinx XC1802 ISPROM

This section is entirely based on the test results reported in [RD79], [RD70] and [RD12].

In [RD79], SEE and TID measurements for the Xilinx 3.3 V XC1802 in-system programmable configuration PROM [RD13] have been presented. One device received at total ionizing does of up to 26.1 krad (Si) during proton irradiation. SEUs were observed during proton irradiation. None of the three errors observed were related to the chip memory. During the last 30% of exposure readback errors were observed on the PROM, yet the device loaded the Virtex FPGA properly and the FPGA showed no memory errors.

Radiation tests of the XC18V02 PROM have been reported in [RD70]. The devices were irradiated with 60 MeV protons at the Cyclotron of Louvain-la-Neuve of the Université Catholique de Louvain, in Belgium. A total fluence of $8x10^{11}$ protons/cm^2 was divided among four devices. No SEU was observed with a limit for the cross-section/bit less than $6x10^{-19}$cm^2. After about $2x10^{11}$ protons (corresponding to a total dose of 28 krad for protons of 60 MeV in silicon) the programming feature stopped to work. The ^{60}Co source in the Istituto Superiore di Sanita' in Rome was used for the total ionizing dose tests. The source gives a rate of 380 rad/minute. Two devices were tested and the behavioural of the devices was very similar. The current sinked from the device started to increase at 20 krad, and at the 33 krad it was impossible to reprogram the device. The device stopped to work at a total dose of 33 krad. This value is similar with the measurements with protons (28 krad). The devices restarted to work after a few hours of annealing and after one day returned to normal current levels.

6.5.4 Xilinx XQR18V04 ISPROM

A radiation hardened version of the XC1802 PROM is available from Xilinx, XQR18V04. In [RD12], it is claimed to be latch-up immune to a LET of > 120 MeV-cm^2/mg and to have a guaranteed TID level of 40 krad (Si). According to Xilinx representatives, the XQV18V04 part has been tested at the Texas A&M University Cyclotron Institute with heavy ions. Also [RD80].

6.6 Estimated on-orbit performance

Estimated upset rates for the Virtex XQVR300 device in on-orbit scenarios have been presented in [RD71], basically stating between 2 and 6 upsets per device day, and between 20 and 80 upsets per device day when taking solar flare into account. These values are predicted without any mitigation techniques and are based on static cross-section measurements.

In [RD66], the authors present on-orbit estimates assuming dynamic cross-section. Their conclusion is that with TMR and scrubbing, the Virtex XQVR300 device should stay at 100% reliability, except for architectural upsets that can be catastrophic.

In [RD65], the authors present on-orbit estimates also based on dynamic cross-section. The expected upset rate is between 0,1 and 1,0 upsets per device day for an orbit of 3000 km at 60 degrees angle. This does not take architectural upsets into account. Similar results are presented in [RD72]. This last paper also provides a discussion on the issue of system availability of a device as a function of the SEU rate.

7   OTHER ISSUES

7.1   Proper use of mode-pin pull-up resistors

The Xilinx XC4000 series mode pins have an internal pull-up resistor that guarantees a logic High level on an unconnected mode pin during power-up. After configuration, the default configuration memory bitstream turns these resistors off. Subsequent re-configurations can, therefore, fail. For all modes except Master Serial (where all three mode pins are being pulled low), it is recommend either external pull-up resistors to guarantee a high level upon reconfiguration, or an explicit change of the configuration memory bitstream.

7.2   Ground bounce

Ground bounce problems have been observed for Xilinx Virtex devices. There is some information regarding ground bounce with Xilinx devices available at *www.klabs.org*. See also [RD43].

7.3   Start-up transients and requirements

In [RD24], the start up requirements are discussed and have been summarised hereafter.

There are two sets of requirements for the power-on transient for Xilinx XQR4000XL and Virtex 2,5 V FPGAs. They are the rise time and current capability of the power supply. It should be noted that unlike other types of devices where slower power supply rise times result in higher current values, in Xilinx devices, faster rise times result in higher current values. Lastly, the Xilinx devices have current rise time requirements.

For the XQR4000XL series, the slowest power supply rise time for this series of parts is 50 ms. While many power supplies can meet this specification easily, note that some space borne power supplies may have longer rise times. Considerations for power supply designers include in-rush currents on capacitors as well as system-level EMC requirements. The minimum current for XQR4000XL series devices is broken into two groups: XQR4013-36XL and the XQR4062XL. Note that according to the specification, the values refer to commercial and industrial grade products only, with the transition measured from 0 VDC to 3,6 VDC. Actual currents may be higher than the minimums specified.

For the XQVR Virtex series, complete power supply requirements are not yet specified in the radiation hard data sheet. The following information is taken from the commercial data sheet. The slowest power supply rise time for this series of parts is also 50 ms. The fastest suggested ramp rate is 2 ms. This is considered slow for some power supplies. The parameter measurement criteria on the radiation hard data sheet is from 1 VDC to 2,375 VDC. The data sheet only specifies a minimum required current supply for Virtex devices at a power supply rise time of 50 ms. According to the non-military specification, it is 500 mA for commercial grade devices and 2 A for industrial grade parts. Additionally, shorter power supply rise times will result in higher currents. The duration of peak currents will be less than 3 ms.

7.4   Reliability

There is some information regarding reliability of Xilinx devices available at *www.klabs.org*. This issue is however not discussed in this document.

8   RECOMMENDATIONS

Reprogrammable FPGAs open up a new exciting dimension for space applications. The design of such FPGAs is however a much more complex task than what has been the case with once-only programmable FPGAs. The main reason is their susceptibility towards single event upsets in the on-chip configuration memory.

Mitigation techniques have been developed to overcome this obstacle and have been proven efficient by means of irradiation testing. Test result indicate that the proposed mitigation techniques can eliminate most of the consequences of upsets, except for some sever architectural upsets that can cause catastrophic errors.

The effect of the proposed mitigation techniques on silicon area consumption is substantial. The theoretical lower bound for the area increase is a factor of three, although some result suggest larger overheads. This will seriously decrease the effective capacity of these FPGAs when used for space applications.

Currently there is little work done regarding the implementation of such mitigation techniques using high level hardware description languages. This area needs to be studied further to facilitate the development of complex application that can utilise the advantage of the large gate count offered by reprogrammable devices. The methodology and design style that must be employed to utilise reprogrammable FPGAs are quite different than what would be used with conventional ASICs or once-only programmable devices.

Irradiation testing has so far been done on designs tailored to simplify diagnostics and to obtain accurate numerical values for the single event upset sensitivity of the devices. More complex designs need to be tested in order to evaluate the suggested mitigation techniques.

The impact of mitigation techniques on power consumption needs to be further assessed.

One should note that current mitigation techniques do not cover some of the catastrophic errors caused by upsets in the architectural control logic of the investigated devices. This is an area that requires further studies.

Recent total ionizing dose tests have shown that the initial high tolerance reported for the devices has to be reassessed since not taking power-up current into account.

The meagre radiation performance of the PROM devices used for configuring the FPGAs needs to be taken into account developing flight applications.

To conclude, the current reprogrammable FPGAs available to the space market should be possible to use provided that they are designed with care, taking necessary precautions into account. Any project using such devices should also fully understand and appreciate the potential risks that cannot be mitigated by design techniques available.