ESA-HB-XX-XX-rev.6
2 December 2011

Space engineering, product assurance

Techniques for Radiation Effects Mitigation in ASICs and FPGAs

ESA-ESTEC
Data Systems Division / Microelectronics Section
Noordwijk, The Netherlands

Foreword

This Handbook is one document of the series of ECSS Documents intended to be used as supporting material for ECSS Standards in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

The material in this Handbook is defined in terms of description and recommendation how to organize and perform the work of XXXX….

This handbook has been prepared by the name of group Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this document, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands
Copyright: 2009 © by the European Space Agency for the members of ECSS

Table of contents

1 Scope **10**

2 Normative references **11**

3 Definitions and acronyms **12**

3.1 Specific terms to the present document 12

3.2 Abbreviated terms 15

4 Organisation and purpose **19**

5 Radiation environment and integrated circuits **20**

5.1 Radiation sources 20

5.1.1 Solar flares 20

5.1.2 Coronal mass ejections 21

5.1.3 Solar wind 21

5.1.4 Galactic cosmic rays 21

5.2 Radiation environment 21

5.2.1 Van Allen belts 21

5.2.2 Atmospheric neutrons 23

5.2.3 Terrestrial radiation sources 24

5.3 The different types of interactions 26

5.3.1 Interaction with photons 26

5.3.2 Interaction with neutrons 26

5.3.3 Interaction with charged particles 27

5.4 Radiation effects 27

5.4.1 Definitions 27

5.4.2 Cumulative effects 30

5.4.3 Single Event Effects (SEEs) 30

6 Choosing a design hardening strategy **34**

7 Technology selection and process level mitigation **35**

7.1 Scope 35

7.2 Table of effects vs mitigation techniques 36

7.3 Mitigation techniques 36
7.3.1 Epitaxial layers 36
7.3.2 Silicon On Insulator 37
7.3.3 Triple wells 41
7.3.4 Buried layers 43
7.3.5 Dry thermal oxidation 44
7.3.6 Implantation into oxides 46
7.4 Technology scaling and radiation effects 47
7.4.1 Effects of technology scaling on TID sensitivity 48
7.4.2 Effects of technology scaling on SEE sensitivity 48

8 Layout 50
8.1 Scope 50
8.2 Table of effects vs mitigation techniques 51
8.3 Mitigation techniques 51
8.3.1 Enclosed Layout Transistor 51
8.3.2 Contacts and guard rings 53
8.4 Radiation-hardened libraries 56
8.4.1 ESA Design Against Radiation Effects library 57
8.4.2 CERN 0.24 µm radiation hardened library 58
8.4.3 BAE 0.15 µm radiation hardened library 58
8.4.4 Ramon Chips 0.18 µm and 0.13 µm radiation hardened libraries 58
8.4.5 Aeroflex 600, 250, 130 and 90 nm radiation hardened libraries 59
8.4.6 Atmel MH1RT 0.35 µm and ATC18RHA 0.18 µm CMOS radiation hardened libraries 59
8.4.7 ATK 0.35 µm radiation hardened cell library 60
8.4.8 ST Microelectronics radiation hardened library 60

9 Analogue circuits 61
9.1 Scope 61
9.2 Table of effects vs mitigation techniques 62
9.3 Mitigation techniques 62
9.3.1 Node Separation and Interdigitation 62
9.3.2 Analog Redundancy (Averaging) 66
9.3.3 Resistive Decoupling 68
9.3.4 Filtering 71
9.3.5 Modifications in Bandwidth, Gain, Operating Speed, and Current Drive 72
9.3.6 Reduction of Window of Vulnerability 75

9.3.7 Reduction of High Impedance Nodes 79
9.3.8 Differential Design 81
9.3.9 Dual Path Hardening 84

10 Digital circuits 89
10.1 Scope 89
10.2 Table of effects vs mitigation techniques 90
10.3 Mitigation techniques 90
10.3.1 Spatial redundancy 90
10.3.2 Temporal redundancy 94
10.3.3 Fail-Safe Finite State Machines 97
10.4 Vendor solutions 98
10.4.1 Radhard circuit manufacturers 98
10.4.2 Radhard processors 98
10.4.3 Radhard computers 99

11 Mixed-signal circuits 101
11.1 Scope 101
11.2 Table of effects vs mitigation techniques 101
11.3 Mitigation techniques 101
11.3.1 Triple Modular Redundancy 101

12 Field Programmable Gate Arrays 104
12.1 Scope 104
12.2 Table of effects vs mitigation techniques 106
12.3 Mitigation techniques 106
12.3.1 Local Triple Modular Redundancy 106
12.3.2 Global Triple Modular Redundancy 108
12.3.3 Large grain Triple Modular Redundancy 111
12.3.4 Embedded user memory TMR 113
12.3.5 Voter insertion 114
12.3.6 Reliability-Oriented place and Route Algorithm 117
12.3.7 Temporal redundancy 119
12.3.8 Embedded processor redundancy 121
12.3.9 Scrubbing 122
12.4 Vendor solutions 126
12.4.1 Microsemi’s RTAX-S/SL antifuse-based FPGA 126
12.4.2 Aeroflex’s UT6325 antifuse-based FPGA 126
12.4.3 Microsemi’s ProASIC3/E flash-based FPGA 127

12.4.4 Atmel AT40KEL SRAM-based FPGA 128
12.4.5 Atmel ATF280F SRAM-based FPGA 129
12.4.6 Xilinx Virtex family SRAM-based FPGA (commercial grade) 129
12.4.7 Xilinx Virtex-5Q SRAM-based FPGA (defense grade) 130
12.4.8 Xilinx Virtex-5QV SRAM-based FPGA (space grade) 131
12.5 Device comparison for space applications 132

13 Embedded memories 134

13.1 Scope 134
13.2 Table of effects vs mitigation techniques 135
13.3 Mitigation techniques 135
13.3.1 Resistive hardening 135
13.3.2 Capacitive hardening 137
13.3.3 IBM hardened memory cell 139
13.3.4 HIT hardened memory cell 141
13.3.5 DICE hardened memory cell 142
13.3.6 NASA-Whitaker hardened memory cell 144
13.3.7 NASA-Liu hardened memory cell 146
13.3.8 Scrambling 147
13.3.9 Error Correcting Codes 149
13.4 Comparison between hardened memory cells 151

14 Embedded software 152

14.1 Scope 152
14.2 Table of effects vs mitigation techniques 153
14.3 Mitigation techniques 153
14.3.1 Redundancy at instruction level 153
14.3.2 Redundancy at task level 159
14.3.3 Redundancy at application level 163

15 System architecture 166

15.1 Scope 166
15.2 Table of effects vs mitigation techniques 167
15.3 Mitigation techniques 167
15.3.1 Shielding 167
15.3.2 Watchdog timers 169
15.3.3 Latching current limiters 171
15.3.4 Duplex architectures 173
15.3.5 Triple Modular Redundancy 177

15.3.6 Error Correcting Codes 180
15.4 Commercial solutions 187
15.4.1 Space Micro Proton platform 187
15.4.2 Maxwell SCS750 188
15.5 Examples of adopted architectures onboard satellites 189
15.5.1 Architecture for the MYRIADE satellite 189
15.5.2 Architecture for the REIMEI (INDEX) satellite 190
15.5.3 Architecture for the CALIPSO satellite 190

16 Validation methods 191

16.1 Introduction 191
16.2 Real-life tests 191
16.3 Ground accelerated tests 192
16.3.1 Standards and specifications 192
16.3.2 Test methodologies 193
16.3.3 Test facilities 194
16.3.4 Practical constraints 199
16.3.5 DUT preparation 200
16.4 Fault injection 200
16.4.1 Fault injection at transistor level 201
16.4.2 Fault injection at gate level 201
16.4.3 Fault injection at device level 202
16.4.4 Fault injection at system level 206
16.5 Analytical methods 206

Annex A References 208

Acknowledgements

This Handbook has been authored and agreed upon by the following persons:

M. Alles, University of Vanderbilt (process and layout level)

D. Loveless, University of Vanderbilt (analogue & mixed-signal circuits)

M. Nicolaidis, TIMA laboratory (digital circuits)

F. L. Kastensmidt, Universidade Federal do Rio Grande do Sul (digital circuits & FPGAs)

M. Violante, Politecnico di Torino (embedded software)

M. Pignol, CNES (system architecture)

The ESA-HB-XX-XX-rev.6 has been prepared based on volunteer contributions of the authors.

Introduction

Integrated circuits devoted to space applications require special care during their design, manufacturing and qualification processes as they will be operating in a harsh radiative environment composed of various energetic particles. The diversity in nature and energy of particles present in this environment is a threat for electronic equipment as they can provoke different type of undesired effects. The consequences can either be long term effects due to the accumulation of charges, deposited in the integrated circuits by impinging particles, and leading to a partial or full lose of functionality or they can be the consequence of a unique particle. In this last case the consequences can be different depending on several parameters such as the particle's energy and nature, the circuit's technology and type. They can provoke erroneous results, functionality interruption and even device destruction.

Drastic device shrinking, very low operating voltages, increasing complexities and high clock frequencies make circuits increasingly sensitive to various kinds of failures. Due to these evolutions, radiation sensitivity, considered in the past as a concern only for space applications, became a major source of system failures of electronic products even for those operating at ground level. Consequently, mitigation of radiation effects is becoming mandatory for an increasing number of application domains, including networking, servers, avionics, medical, and automotive electronics. To tackle this problem, integrated circuits and system designers may benefit from several decades of knowledge related R&D from the military and space domains. However, as ground level and aeronautic applications concern high-volume production they are not subject to the same constraints as space applications.

Significant efforts have been made during the past years to cope with the undesired effects induced by radiation. A wide scope of methodologies and tools adapted to address these effects for the different phases of the microelectronic development flow: manufacturing process, design, hardware, software.

The goal of this handbook is to present the techniques and methods devoted to mitigate radiation induced effects on analogue, mixed-signal and digital ASICs and FPGAs.

1 Scope

This handbook describes the up-to-date known validation methods for the mitigation of radiation effects which are applicable to microelectronic components and systems. The presentation of available mitigation methods is organized according to development flow in a bottom-up approach: manufacturing process, layout, schematic, digital design, architecture, embedded software and system architecture.

2 Normative references

The following normative documents contain provisions which, through references in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

AO/1-3240/97/NL/TM	Circumventing radiation effects by logic design: Cookbook, July 1999.
FPGA-003-01	Functional Triple Modular Redundancy (FTMR), Gaisler Research, December 2002
NASA ASIC	NASA ASIC Guide – Radiation Hardening
SPRINGER 2007	Radiation Effects on Embbeded Systems, Raoul Velazco, Pascal Fouillat, Ricardo Reis, 2007, Springer, ISBN: 978-1-4020-5645-1
ECSS-E-HB-10-12A	Calculation of radiation and its Effects and Margin Policy Handbook.
ECSS-Q-ST-60-02C	Space Product Assurance: ASIC and FPGA Development.
ECSS-Q-ST-60C	Electrical, Electronic and Electromechanical (EEE) Components.

3
Definitions and acronyms

3.1 Specific terms to the present document

Levels of abstraction

Building robust systems for space applications requires a lot of stages and techniques aiming at mitigating radiation effects which exist at all levels of the hierarchy from the fabrication process, the circuit design (layout) to the system architecture and the software levels.

Mitigation techniques presented in this handbook are organized according to the following identified levels of abstraction:

- System level: these techniques apply at component level (e.g. microprocessor redundancy), unit level or embedded software level (e.g. computer redundancy).
- Architecture: techniques devoted to this level are most often specific to the circuit's nature (digital, analogue or mixed signal) and/or to the circuit's family (ASICs, FPGAs or embedded memory). Moreover, a majority of them belong to main approaches such as redundancy (hardware or temporal) or Error Detection And Correction (EDAC).
- Layout: techniques aiming at optimizing transistor's layout and placement in order to reduce sensitivity to radiation of the final circuit.
- Process: techniques concerning the manufacturing processes, also known as Radiation Hardening By Process. These approaches generally concern modifications of doping profiles in devices and substrates, optimization of deposition processes for insulators and use of specific materials.

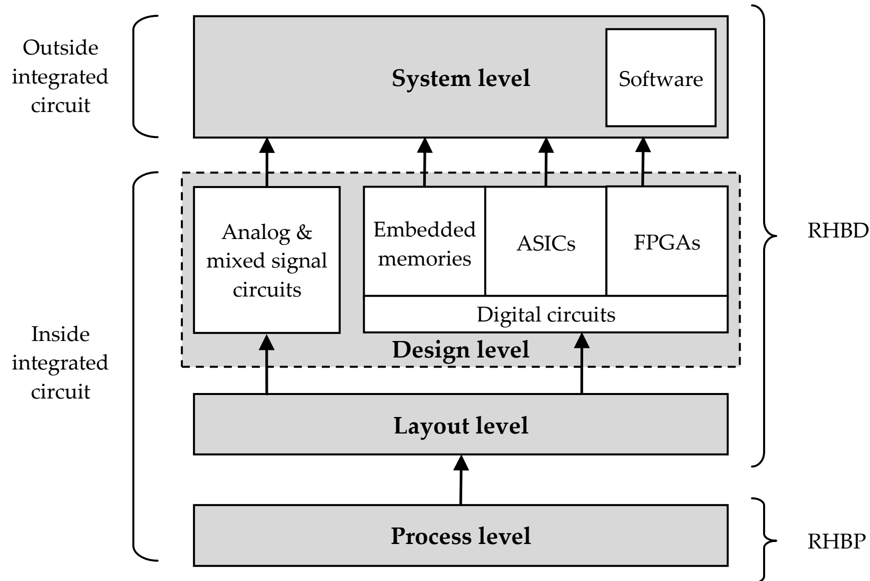


Figure 3-1 : Levels of abstraction

Radiation Hardening By Process / Design

Radiation-Hardening-By-Process (RHBP) concerns modifications at fabrication processes in order to reduce the impact of radiation on integrated circuits. This goal can be achieved by several means such as modifications of doping profiles in devices and substrates, optimization of deposition processes for insulators and use of specific materials. RHBP will mainly address two main effects: Total Ionizing Dose (TID) and Single Event Effect (SEE). Details about the considered effects can be found in chapter 5.4.2 and 5.4.3.

In contrast, Radiation Hardening By Design (RHBD) refers to special circuits design techniques that can be applied at layout level, at architectural level or at system level. RHBD approaches exist both for TID and SEE mitigation. The use of such techniques usually induces a penalty including area, power consumption, frequency, costs or procurement delays.

Critical charge

The critical charge, noted Q_{crit}, is the minimum charge a particle must deposit in an integrated circuit's node to invert its state.

Fault masking

As described in chapter 5.4.3, Single Event Effects are the consequence of the current pulse resulting by the charge deposited by a single particule inpinging a sensitive area of the circuit. The occurrence of an Single Event Transient (SET) in a circuit does not necessarily end up with an error. Indeed, there are three factors that determine whether an SET will propagate and result in an error:

- **Logical masking** occurs, for example, when an SET provoked by a particle is not propagated to an output due the value of the inputs. Figure 1-2 illustrates the logical masking phenomenon for an AND and an OR gate. Whenever an input of the AND gate is "0" it will naturally reject the transient (Figure 1-2 (a)) and when one input is set to "1" the SET will be able to propagate

(Figure 1-2 (b)). For the OR gate, the SET will propagate with an input set to "1" (Figure 1-2 (c)) but will be masked when the input is "0" (Figure 1-2 (d)).

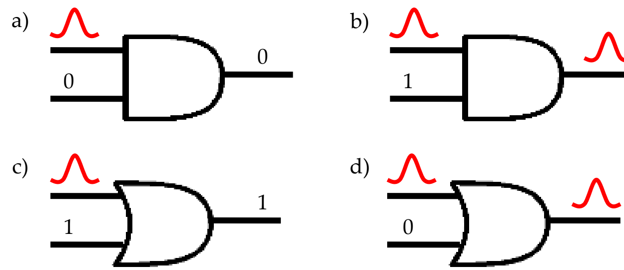


Figure 3-2 : Logical masking of a transient in two logical gates

- **Electrical masking** occurs, for example, if the SET is attenuated as it propagates along a path until it does not affect anymore the result of the circuit. Such a phenomenon is illustrated in Figure 1-3 where an SET is attenuated by each gate. When it reaches the flip-flop, the pulse's amplitude is not sufficient to create an error.

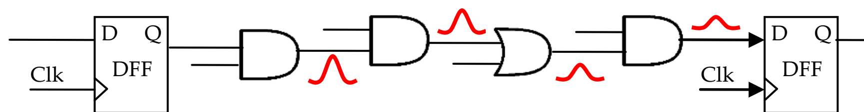


Figure 3-3 : Electrical masking along a path in combinational logic

- **Temporal masking** occurs, for example, if an SET reaches a memory element at an instant other than the clocking window. Figure 1-4 depicts an example of temporal masking in a flip-flop at instant T1 because the SET on its input is not concurrent with a clock rise edge. At instant T2 the SET occurs as the same time than the clock pulse and will thus modify the content of the memory cell. The resulting error may propagate to the circuit output. In this case the SET transforms itself into an Single Event Upset (SEU) also called bit-flip or soft error.

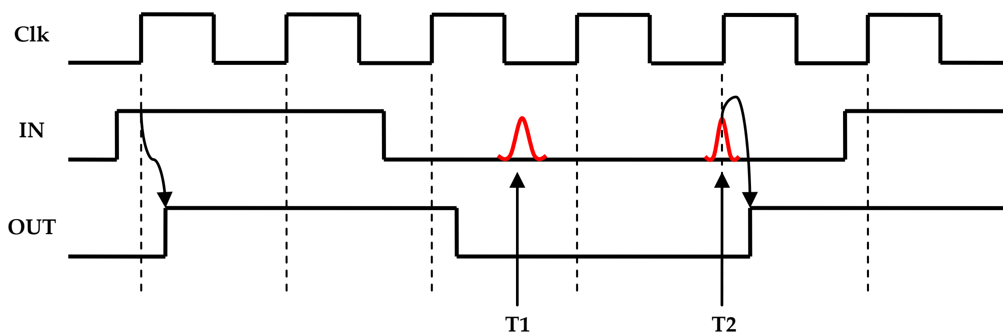


Figure 3-4 : Temporal masking

Consequently, these three factors present a natural barrier to soft errors in integrated circuits.

3.2 Abbreviated terms

For the purpose of this document, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
μP	Microprocessor
ADC	Analogue-to-Digital Converter
ASET	Analogue Single-Event Transient
ASIC	Application Specific Integrated Circuit
BICS	Built-In Current Sensors
Bi-MR	Bi-Modular Redundancy
BJT	Bipolar Junction Transistor
BOX	Buried OXide
CED	Concurrent Error Detection
CEU	Code Emulated Upset
CFCSS	Control Flow Checking by Software Signatures
CLB	Configuration Logic Block
CME	Coronal Mass Ejection
CMOS	Complementary Metal Oxide Semiconductor
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CWSP	Code Word State Preserving
DAC	Digital-to-Analogue Converter
DARE	Design Against Radiation Effects
DCM	Digital Clock Manager
DFF	D-Flip-Flop
DMS	Defense Meteorological Satellite
DMT	"Duplex Multiplexé dans le Temps", i.e. duplex in time
DROM	Demultiplexer-ROuter-Multiplexer
DSP	Digital Signal Processor
DUT	Device Under Test
DWC	Duplication With Comparison
ECC	Error-Correcting Codes
EDAC	Error Detection And Correction
EDDI	Error Detection by Duplicated Instructions
ESA	European Space Agency
ESCIES	European Space Components Information Exchange

	System
ESD	ElectroStatic Discharge
eV	Electron-Volt
FEC	Forward Error Correction
FF	Flip-flop
FIR	Finite Impulse Response
FIT	Failure In Time
FPGA	Field Programmable Gate Array
GCC	GNU Compiler Collection
GCR	Galactic Cosmic Rays
GEO	GEOstationary
GNU	GNU's Not Unix
GPS	Global Positioning Satellite
HBFT	Hypervisor-Based Fault Tolerance
HBT	Heterojunction Bipolar Transistor
HDL	Hardware Description language
HWICAP	HardWare Internal Configuration Access Port
HW	Hardware
I/O	Input/Output
IC	Integrated Circuit
ILO	Injection-Locked Oscillator
IOB	Input/Output Block
ISS	International Space Station
LCL	Latching Current Limiter
LEO	Low Earth Orbit
LET	Linear Energy Transfer
LET_{th}	Linear Energy Transfer threshold
LHC	Large Hadron Collider
LNA	Low-Noise Amplifier
LOCOS	LOCal Oxidation of Silicon
LPF	Low Pass Filter
LUT	Look-Up Table
LVDS	Low-Voltage Differential Signaling
LWS-SET	Living With a Star – Space Environment Testbed
MAJ	MAJority voter
MBU	Multiple Bit Upset
MCU	Multiple Cell Upset

MEO	Medium Earth Orbit
MMU	Memory Management Unit
MOS	Metal Oxyde Semiconductor
MOSFET	Metal-Oxide Semiconductor Field-Effect Transistor
MPTB	Microelectronics and Photonics TestBed
MTBF	Mean Time Between Failures
MUX	Multiplexer
NMOS	N-channel Metal-Oxide Semiconductor
NPOESS	National Polar-orbiting Operational Environmental Satellite System
OA	Operational Amplifier
PCI	Peripheral Component Interconnect
PLL	Phase-Locked Loop
PMCD	Phase-Matched Clock Divider
PMOS	P-channel Metal-Oxide Semiconductor
POA	Post Oxidation Anneal
POR	Power-On Reset
PUC	Processing Unit Core
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RHBD	Radiation Hardening By Design
RHBP	Radiation Hardening By Process
RoRa	Reliability Oriented Place and Route
RS	Reed-Salomon
RTL	Register Transfer Level
SAA	South Atlantic Anomaly
SBIRS	Space Based InfraRed System
SCSI	Small Computer System Interface
SE	Soft Error
SEB	Single Event Burnout
SEC-DED	Single Error Correction-Double Error Detection
SEE	Single Event Effect
SEFI	Single Event Functional Interrupt
SEGR	Single Event Gate Rupture
SEL	Single Event Latchup
SER	Soft Error Rate

SerDes	Serializer/Deserializer
SET	Single Event Transient
SEU	Single Event Upset
SiGe	Silicon Germanium
SNR	Signal-to-Noise Ratio
SoC	System on Chip
SOI	Silicon On Insulator
SOS	Silicon On Sapphire
SPF	Single Point Failure
SPICE	Simulation Program with Integrated Circuit Emphasis
STI	Shallow Trench Isolation
STRV	Space Technology Research Vehicle
SW	Software
TID	Total Ionizing Dose
TMR	Triple Modular Redundancy
TNID	Total Non Ionizing Dose
TPA	Two-Photon Absorption
UMC	United Microelectronics Corporation
USAF	United States Air Force
VCDL	Voltage-Controller Delay Line
VCO	Voltage Controlled Oscillator
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuits
WL	Write Line

4 Organisation and purpose

This document aims at describing state-of-the-art techniques used to mitigate radiation effects in ASICs and FPGAs. Depending on the type of circuit and the nature of the radiation effect, the mitigation technique can be applied at different abstraction levels, such as manufacturing process, layout, design, software and architecture levels. This handbook is organized so that the reader can easily access mitigation techniques suitable to both his profile and the chosen level of abstraction. The reader can refers to Chapter 6 to get guidelines about the choice of the mitigation techniques suitable for a considered project.

This handbook shall serve as a comprehensive reference which will enable microelectronics engineers to choose and check the adequacy of methodologies for radiation hardening, and to improve design techniques where necessary. It describes the available technology choices and mitigation techniques for digital and analogue integrated circuits including but not limited to ASICs and FPGAs.

Everyone who is concerned with reliability of applications devoted to operate in radiation environment, i.e. project managers, semi-conductor manufacturing engineers, hardware and software engineers, quality assurance personnel, should read this handbook.

5 Radiation environment and integrated circuits

Failures induced by radiation, which appeared first in satellite equipments, have become one of the most challenging issues for modern electronic systems, even for ground-level applications. Many efforts have been spent in the last decades to measure, model, and mitigate radiation effects, applying numerous different techniques approaching the problem at various abstraction levels.

This chapter is intended to give the reader a general overview of radiation and its potential effects on integrated circuits. Firstly, existing radiation sources are exposed. The Earth radiation environment (and its neighborhood) is then described followed by an explanation concerning the different types of interaction between particles and matter. Finally, radiation effects on integrated devices are discussed.

5.1 Radiation sources

Radiation sources are multiple: some take their origin in the Sun (e.g. solar flares, coronal mass ejection and solar wind) and others come from outside the solar system [1].

5.1.1 Solar flares

A solar flare is a sudden and rapid release of magnetic energy that has built up in the solar atmosphere (Figure 5-1). It can last from a few seconds up to one hour. The first solar flare was reported in astronomical literature by Richard C. Carrington and Richard Hodgson on September 1, 1859. During this phenomena radiation is emitted through the entire electromagnetic spectrum, from radio waves to X-rays and gamma rays. However, protons and heavy ions should be considered first when analyzing solar flare impacts on integrated circuit reliability.

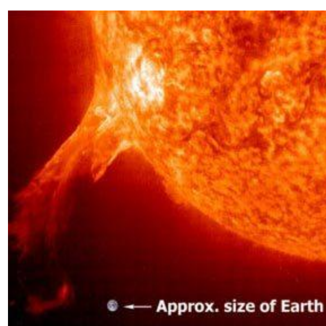


Figure 5-1 : A solar flare

5.1.2 Coronal mass ejections

A Coronal Mass Ejection (CME) is a huge plasma bubble ejected by the Sun (Figure 5-2) over the course of several hours [2]. Coronal events where observed for the first time in 1971 with the use of a coronagraph which produces an artificial eclipse of the Sun by placing an "occulting disk" over the Sun. In this case considered particles are high-energy protons.

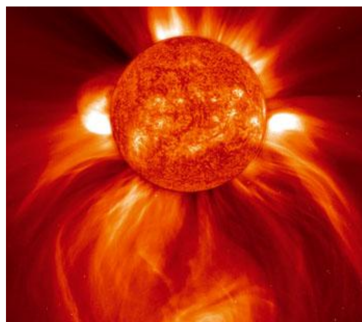


Figure 5-2 : Coronal mass ejections

5.1.3 Solar wind

Coronal mass ejections cause shock waves in the thin plasma of the heliosphere, launching electromagnetic waves and accelerating particles (mostly protons and electrons) to form showers of ionizing radiation that precede the CME. The solar wind streams off of the Sun in all directions at an average speed of approximately 400 km/s. The source of the solar wind is the Sun's corona where the temperature is so high that electrons have sufficient energy to escape the Sun's gravity. As a reaction, protons and heavy ions are ejected in order to maintain the zero electrical charge of the star. The solar wind is not uniform in terms of speed and charge intensity.

5.1.4 Galactic cosmic rays

Galactic cosmic rays (GCRs) are high-energy charged particles coming from outside the solar system and generally from within the Milky Way galaxy [3]. The highest cosmic ray energy measured is over 1020 eV. They are composed of about 89% of hydrogen nuclei (protons), 10% of Helium nuclei, the remaining 1% being fully ionized nuclei of heavier elements and electrons.

5.2 Radiation environment

5.2.1 Van Allen belts

Van Allen Belts are two regions of the magnetosphere, shown in Figure 5-3, where high-energy particles, mainly protons and electrons, are trapped by the Earth's magnetic field. James Van Allen named them after their discovery in 1958.

The inner belt extends from 100 km and 10,000 km above the Earth's surface and is mainly composed of high-energy protons (up to several 100 MeV) and electrons issued from solar wind protons or generated by galactic cosmic ion collisions with atmosphere. Electrons in the range of hundreds of keV are also present in the inner belts.

The outer belt spreads from 13,000 km to 65,000 km of the Earth's surface. Trapped particles are mainly high-energy electrons (0.1 to 10 MeV).

The South Atlantic Anomaly (SAA) is a particularity to be noted as it is a region of very high-energy particle flux about 250 km and higher above the Atlantic Ocean and the coast of Brazil. It comes from several reasons:

- The symmetry of the Van Allen belts with the Earth's magnetic axis.
- The 11° tilt between the Earth's magnetic axis and the Earth's rotation axis.
- The 500 km offset of the Earth's magnetic axis toward Pacific Ocean geographic N-S.

The particle flux is so high in the region that detectors on satellites are often shut off or placed in "safe" mode while passing through.

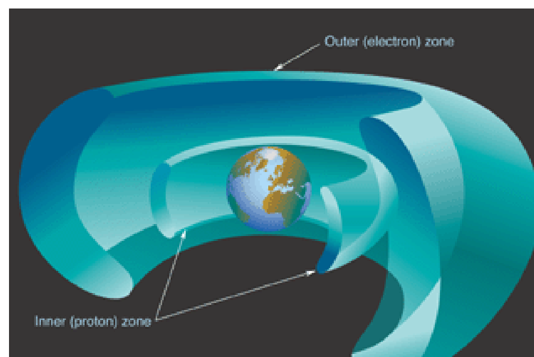


Figure 5-3 : Van Allen radiation belts

5.2.2 Atmospheric neutrons

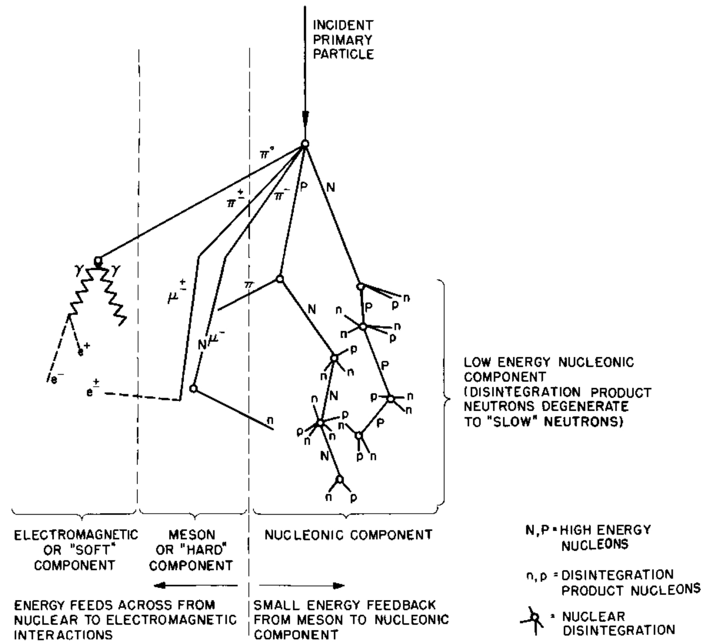


Figure 5-4 : Schematic Diagram of Cosmic Ray Shower

High-energetic cosmic ray particles (mostly protons) can create neutrons, secondary protons, muons and neutrinos by spallation[1] reaction on atmospheric nuclei (Figure 5-4). As most particles are easily stopped, most of the error contribution is arising from the neutron "shower".

The neutron peak flux, 3,600 to 10,000 particles/cm².hour (E > 10 MeV), can be found at an altitude of 18 km (60,000 feet). At 9km (30,000 feet) the neutron flux is equal to about 1/3 of the peak flux. At ground level the observed flux is about 1/400 the peak flux. Note that these figures may change depending on the Sun activity. Indeed, when this activity is high the solar wind increases, which results in strengthening the Earth's magnetic field and, thus repelling further away cosmic rays.

The neutron population in the atmosphere varies with both altitude and latitude as shown in Figure 5-5 and Figure 5-6. The latitude variation of the 1-10 MeV atmospheric neutrons is based on measurements made aboard aircrafts at an altitude of 35,000 feet.

[1] In nuclear physics, spallation is the process in which a heavy nucleus emits nucleons as a result of being hit by a high-energy particle, thus reducing its atomic weight.

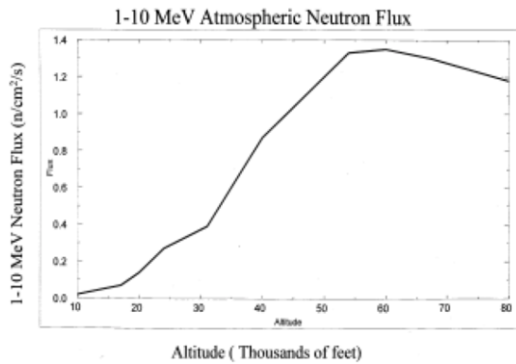


Figure 5-5 : Neutron flux vs. altitude

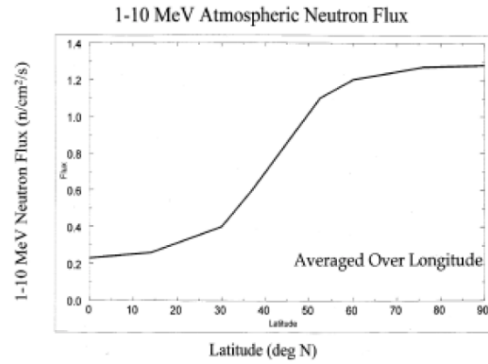


Figure 5-6 : Neutron flux vs. latitude

Neutrons cannot cause errors in integrated circuits through direct ionization, as it is the case with protons and heavy ions, but they can generate errors through nuclear reactions with silicon resulting in recoils which may deposit enough charge in a small volume to trigger an event.

5.2.3 Terrestrial radiation sources

Radioactive materials are found throughout nature: in the soil, water, and vegetation. Low levels of uranium, thorium and their decay products can be found everywhere. These materials are either ingested with food and water, or inhaled like the radon. Natural deposited dose is linked to several parameters such as geographic location, presence of uranium mine, etc.

The major isotopes of concern for terrestrial radiations are uranium and the decay products of uranium, such as thorium, radium, and radon.

Different sources of alpha impurities are present in micro-electronic devices. These sources are mainly wafer process, packaging impurities, chip materials and solder. These alpha emitters are in the low energy spectra (< 5 MeV) and are locally highly ionizing and they may disrupt the functional behavior of the component.

Table 5-1 provides the relevant primary and secondary radiation as a function of radiation effects and mission types.

Table 5-1 : Relevant primary and secondary radiations as a function of radiation effects and mission types

Radiation effects	Mission type	Important primary radiations	Important secondary radiation
Total ionizing dose	LEO	Trapped protons and electrons Solar protons	X-rays from electrons
	High MEO	Trapped electrons Solar protons	X-rays from electrons
	Low MEO	Trapped protons and electrons Solar protons	X-rays from electrons
	GEO	Low energy trapped protons Trapped electrons Solar protons	X-rays from electrons
	Interplanetary space	Cosmic rays Solar energetic particles Other planetary trapped-belts	X-rays from electrons
	Planetary lander	Solar energetic particles	Secondary protons & neutrons
Displacement damage	LEO	Trapped protons Trapped electrons Solar protons	Secondary neutrons
	MEO	Trapped protons (low MEO) Trapped electrons Solar protons	Secondary neutrons
	GEO	Trapped protons (low energy) Trapped electrons Solar protons	Secondary neutrons
	Interplanetary space	Cosmic rays Solar energetic particles Other planetary trapped-belts	Secondary neutrons
	Planetary lander	Cosmic rays Solar energetic particles	Secondary protons & neutrons
Single Event Effects	LEO	Trapped protons Solar energetic particles Cosmic rays	Secondary neutrons
	MEO	Trapped protons Solar energetic particles Cosmic rays	Secondary neutrons
	GEO	Solar energetic particles Cosmic rays	Secondary neutrons
	Interplanetary space	Cosmic rays Solar energetic particles Other planetary trapped-belts	Secondary neutrons
	Planetary lander	Cosmic rays Solar energetic particles	Secondary protons & heavier ions Secondary neutrons

5.3 The different types of interactions

Natural environment interacts in many different ways with electronic devices depending on the radiation type, the particle type and its energy. In the following section, are described the different interactions with material. A more detailed description can be found in [4].

5.3.1 Interaction with photons

Photons are electromagnetic radiation with zero mass, zero charge, and a velocity that is always *c*, the speed of light. Because they are electrically neutral, they do not steadily loose energy via *Coulombic interactions*, also called ionization, with atomic electrons as do charged particles. Instead, they travel a considerable distance before undergoing a more "catastrophic" interaction. Among all the photon interactions, only those leading to partial or total transfer of the photon energy to electron energy are detailed in this document. Thus, three interactions of interest are presented:

- Photoelectric Effect: In the *photoelectric absorption* process, a photon undergoes an interaction with an absorber atom in which the photon completely disappears. In its place, an energetic *photoelectron* is ejected from one of the bound shells of the atom. The interaction leaves an ionized absorber atom with a vacancy in one of its bound shells. This vacancy is quickly filled through the capture of a free electron from the medium and/or rearrangement of electrons from other shells of the atom. The photoelectric process is the predominant mode of interaction for photons of relatively low energy (below a few tens of keV).
- Compton Scattering: The *Compton scattering* interaction takes place between the incident photon and an electron in the absorbing material. It is most often the predominant interaction mechanism for photons having an energy between tens keV and several MeV. The photon transfers a portion of its energy to the electron, which is then known as a recoil electron, or a *Compton electron*.
- Pair Production: If an energetic photon enters matter and has an energy in excess of 1.022 MeV, it may interact by a process called *pair production*. In this mechanism of energy transfer, the photon when passing near the nucleus of an atom, is subjected to strong field effects from the nucleus and may disappear as a photon and reappear as a positive and negative electron pair. Pair production becomes more likely with increasing photon energy.

5.3.2 Interaction with neutrons

As a neutron has no charge, it mainly interacts with the nucleus of the atoms forming the matter it passes through. However, the probability it passes close enough to a silicon nucleus or a dopant nucleus is low. When this happens it can cause two types of interactions: scattering or absorption [5][6]. When a neutron is scattered by a nucleus, its speed and direction change but the nucleus is left with the same number of protons and neutrons it had before the interaction. The nucleus will have some recoil velocity and it may be left in an excited state that will lead to the eventual release of radiation. When a neutron is absorbed by a nucleus, either a wide range of radiation can be emitted or fission can be induced. Three effects are considered as they can affect integrated circuits.

- Elastic Scattering: In elastic scattering a fraction of the neutron's kinetic energy is transferred to the nucleus. This nucleus can then leave the crystalline silicon network if it has gained enough energy from the neutron.
- Inelastic Scattering: Inelastic scattering is similar to elastic scattering except that the nucleus undergoes an internal rearrangement into an excited state from which it eventually releases

radiation. This secondary particle creates a trail of electron-hole pairs able to modify the state of a transistor.

- Absorption: One type of neutron absorption by a nucleus can lead to the mutation of the atom into a heavier element. In case a neutron is absorbed by a boron-10 atom (used as a dopant in CMOS technology), the reaction will produce a gamma photon, an alpha particle and a lithium-7 nuclei. The alpha and the lithium recoil are both capable to interfere with the integrated circuit by ionization process [7].

5.3.3 Interaction with charged particles

When a charged particle enters a matter it will interact with the electrons and nuclei in the medium and begins to lose energy as it travels through. The interaction can be generally thought of as collisions between the charged particle and either the atomic electron or the nucleus. The energy given off will result in ionization, production of ion-electron pairs, in the medium. It can also appear in the form of electromagnetic radiation.

Considered charged particles are protons, alpha-particles and ions. And given their energy, their interaction with matter is ionization. It is important to note that direct ionization from protons is only possible for 90 nm technologies and below. Older technologies will interact through indirect ionization where the effect in the circuit is provoked by the secondary particles. Alpha-particles and ions may generate single events (see following section) from electron-hole pairs issued from direct ionization of the material.

5.4 Radiation effects

This section defines some useful notions related to radiation effects and then describes the different effects radiation can provoke in integrated circuits.

5.4.1 Definitions

Linear Energy Transfer (LET)

When a particle interacts with the matter it passes through, it transfers its energy to the medium. The charge deposition capacity, through ionization, is described in terms of Linear Energy Transfer (LET) which corresponds to the energy deposition by length unit and depends on the materiel density, ϱ:

$$LET = \frac{1}{\rho}.\frac{\Delta E}{\Delta x} \quad \text{(In MeV.cm}^2\text{/mg or MeV/mg/cm}^2\text{)}$$

A detailed explanation of the LET is available in [8].

The deposited energy is given by the following equation where θ is the ion incident angle:

$$\Delta E = \frac{dE}{dx}.\frac{X}{\cos\theta}$$

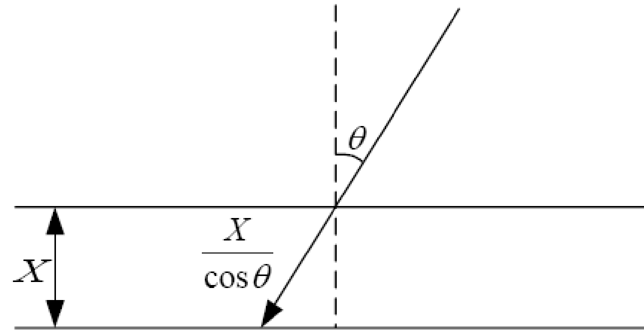


Figure 5-7 : Deposited energy for a heavy ion with a θ incident angle

When ΔE > Ec (critical energy), a single event phenomenon may occur. The LET threshold (LETth) is thus defined by this characteristic LET as the minimum LET required for a particle to create a single event. Consequently, components having a high LETth have a good immunity to single events.

Cross section

The cross section, σ, is a measure of the sensitivity of a device for a given particle LET or energy respectively for heavy-ions and protons. It is defined by the ratio of the number of single events observed on the device by the particle fluence (particles per cm²) received by the component under test. Thus, the cross section can be interpreted as the probability that an impinging particle provokes a single event and is given by the following equation:

$$\sigma_{sat} = \frac{\#\ of\ observed\ events}{fluency}$$

Cross-section curve

The cross-section curve describes the sensitivity of a device for a given effect. It is obtained by plotting the obtained cross-section measures versus incident particle LET, for heavy ions, or energy for protons.

The LET or energy is represented in the x-axis and the cross section in the y-axis. The cross-section curve has two specific values. The first is the *LET threshold,* which is the lowest LET required to trigger an event in the studied circuit. The second is the *saturation cross-section,* which indicates the maximal sensitivity of the device and thus is an image of the total sensitive area of the device.

An example of typical cross-section curve is given in Figure 5-8. The heavy ion cross section can be fit using a Weibull distribution with width (W) and shape (S) parameters. The curve shape equation is the following:

$$\sigma = \sigma_{sat}\left[1 - exp\left(\left(-\frac{LET - LET_{th}}{W}\right)^{S}\right)\right]$$

In the case of proton testing the Bendel model is used either with 1 parameter (threshold energy is the only parameter usable for old devices and low data points number) or with 2 parameters (threshold E and asymptotic cross section):

$$\sigma = \sigma_{sat}\left[1 - exp\left(-0.18\left(\sqrt{{}^{18}/_{E_{th}}}\,(E - E_{th})\right)^{{}^{1}/_{2}}\right)\right]^{4}$$

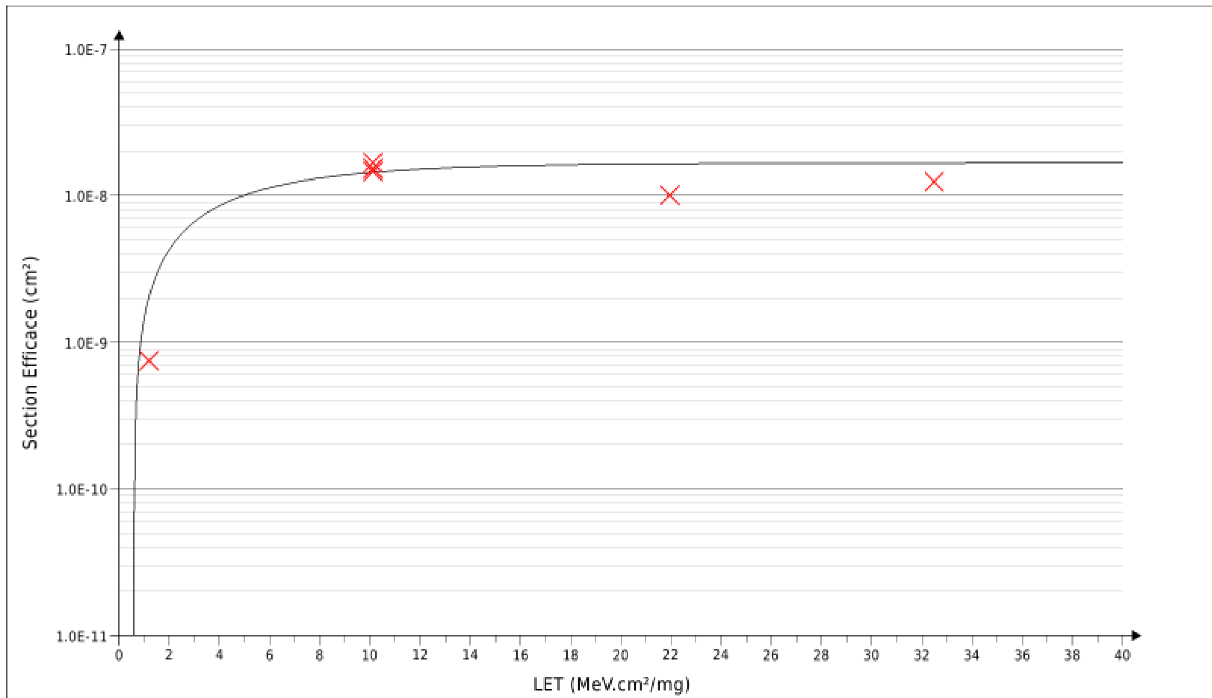


Figure 5-8 : Example of heavy ions typical cross-section curve measure

Integral LET spectrum

The integral LET spectrum is a graph representing for a given environment (orbit, solar activity and shielding) the particle distribution depending on their LET. As shown in Figure 5-9 the particle flux is plotted in the y-axis while the particle LET is plotted in the x-axis. Thus, for a given environment, one can obtain the particle density for a selected LET.

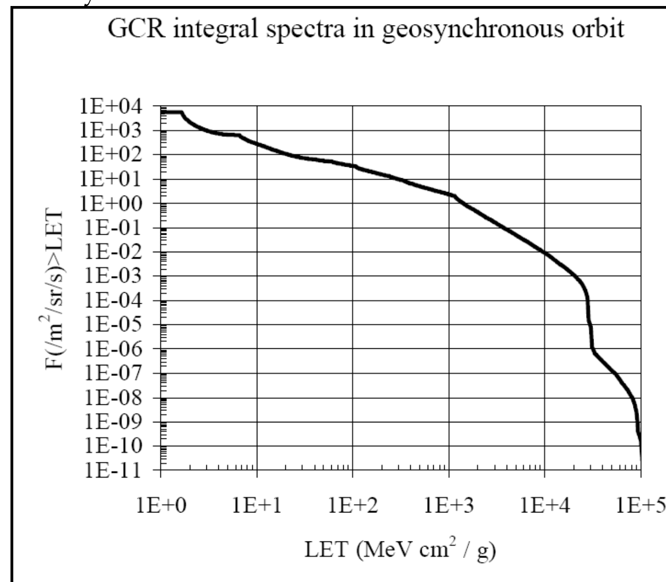


Figure 5-9 : Example of integral LET spectrum

As a conclusion, when an energetic particle passes through an integrated circuit it interacts with its atomic structure. Events issued from this interaction may be classified into two groups: cumulative

effects and effects due to a single particle, also called Single Event Effects (SEEs). The two following sections briefly describe these phenomena.

5.4.2 Cumulative effects

Exposure to radiation produces relatively stable, long-term changes in devices and circuit's characteristics that may result in parametric degradation and functional failures. Ionizing particles will cause Total Ionizing Dose (TID) effects whereas non-ionizing ones will cause displacement damage effects, also called Total Non-Ionizing Dose (TNID).

5.4.2.1 Total Ionizing Dose

The total ionizing dose effect provokes cumulative long term ionizing damages due to protons and electrons. It primarily impacts insulating layers, which may trap charge or produce interface changes. In MOS devices, trapped charges can lead to a shift in the gate threshold voltages. More generally, in semiconductors, interface states can significantly increase device leakage currents. Ultimately, TID provokes permanent functional failures of the device [9].

Table 5-1 provides the estimated TID per year for four different orbits: Geosynchronous orbit (GEO), Global Positioning Satellite (GPS), Low Earth Orbit (LEO) and Defense Meteorological Satellite (DMS) [10].

Table 5-2 : Estimated TID per year from electrons and protons (100 mm Al satellite skin)

Orbit name	GEO	GPS	LEO	DMS
Apogee (km)	35,796	20,189	1,600	946
Perigee (km)	35,795	20,172	1,600	824
Inclination (degrees)	0	55	60	99
Dose rad(Si)/yr	6,600	59,000	17,300	1,260

5.4.2.2 Displacement damage

Non-ionizing energy loss results in displacement damage and defects in both insulator and semiconductor regions. This energy deposited by impinging particles displaces atoms and creates electrically active defects. The overall effect of displacement damage is a change in the minority carrier lifetimes of semiconductors, and increased light absorption and coloration in crystalline optical materials. This effect concerns particularly bipolar devices and opto-electronics.

5.4.3 Single Event Effects (SEEs)

The charge deposited by a single ionizing particle can produce a wide range of effects. Some of them, such as Single-Event Transient (SET), Single-Event Upset (SEU) and Single-Event Functional Interrupt (SEFI) are temporary and can be recovered. Others can lead to permanent damage such as Single-

Event Latchup (SEL) or Single-Event Gate Rupture (SEGR). These effects can be produced either by direct ionization or by secondary particles issued from nuclear reactions or elastic collisions.

5.4.3.1 Single-Event Transient

A single-event transient is an energy pulse issued from the ionization of sensitive volumes in electronic devices. SETs are a major concern for analog and mixed-signal CMOS circuits, analog and digital bipolar circuits and opto-electronics.

Transients can also propagate in combinational logic found in digital CMOS integrated circuits and may be captured by a memory element if they occur during a clock edge. In this case an SET may result in a single-event upset (see below).

5.4.3.2 Single-Event Upset

Single-event upsets may occur when deposited charges, by ions and protons, are collected at sensitive nodes of storage elements such as flip-flops, latches, SRAM cells, etc. SEU may also be the result of an SET being latched on a clock edge after propagating in combinational logic.

The consequence of SEU phenomenon, also called bit-flip may depend on both the instant of occurrence and the purpose of the perturbed cell in the studied circuit of system. Indeed, the SEU can either be silent (unused or yet used perturbed data) or resulting a wide scope of errors including critical errors, such as SEFIs (see section 1.4.3.4).

The sensitivity to SEU of electronic devices greatly varies according to the technologies and several parameters. In particular, reduction of transistor size or supply voltage tends to decrease the critical charge and thus increase the sensitivity to SEEs.

5.4.3.3 Multiple-Bit Upset (MBU) and Multiple-Cell Upset (MCU)

Multiple upsets occur when several bit-flips are triggered by a single particle. Several upsets in a memory word are called MBUs, whereas several upsets in different memory words are referenced as MCUs.

Integrated circuits tend to be increasingly sensitive to multiple upset events as gaps between transistors are becoming smaller. This allows charges deposited by ions and protons to be collected by several sensitive nodes of the circuit and thus results in SEUs in different memory cells.

Error-Correcting Codes (ECCs), such as Hamming codes, are well adapted to mitigate SEUs as they can detect and correct errors in a word. However, MBUs are a real challenge for advanced technologies as they require elaborated and complex ECCs.

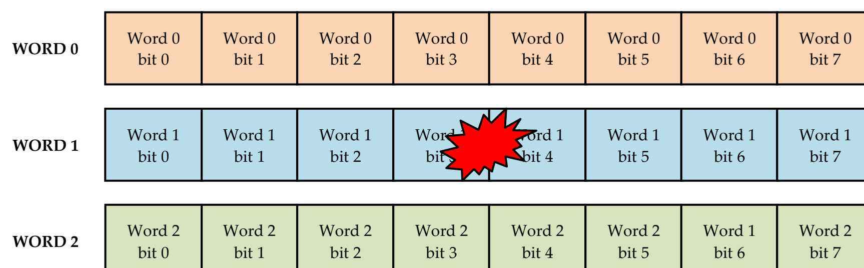


Figure 5-10 : Two upsets in the same word provoked by a single particle (MBU)

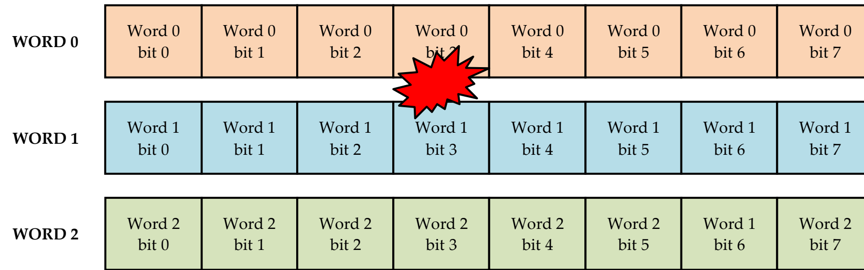


Figure 5-11 : Two upsets in different words provoked by a single particle (MCU)

5.4.3.4 Single-Event Functional Interrupt (SEFI)

In complex circuits such as processors, FPGAs, etc, SEUs may have severe consequences, called single-event functional interrupt (SEFIs). Indeed, an SEU in the device's control circuitry may place the device into a test mode, halt, or undefined state. Another example of SEUs provoking SEFIs in processors is the so-called sequence loss resulting, for instance, of an SEU in the program counter leading to an infinite loop. In such cases, a reset of the application or a power off/on cycle is required to recover the full functionality of the system.

SEFIs were observed and defined for the first time in 1997, see [11], from observations in SDRAM, EEPROMS and Microprocessors. SEFIs were also reported in flash-based memories, SRAM-based FPGAs and microcontrollers.

5.4.3.5 Single-Event Latchup (SEL)

A Single-Event Latchup is the result of the triggering of a parasitic thyristor (PNPN structure) mainly existing in CMOS circuits (Figure 5-12) and potentially in bipolar devices. When it occurs, an important current flows and increases the local temperature of the die, until destruction of the structure. This effect can be stopped by powering-off the circuit.

A specific case of latchup, called micro-latchup, can be encountered when the current is limited by the internal device circuitry. Since the current is limited, the micro-latchup is not destructive but the effect on the functionality may still be significant.

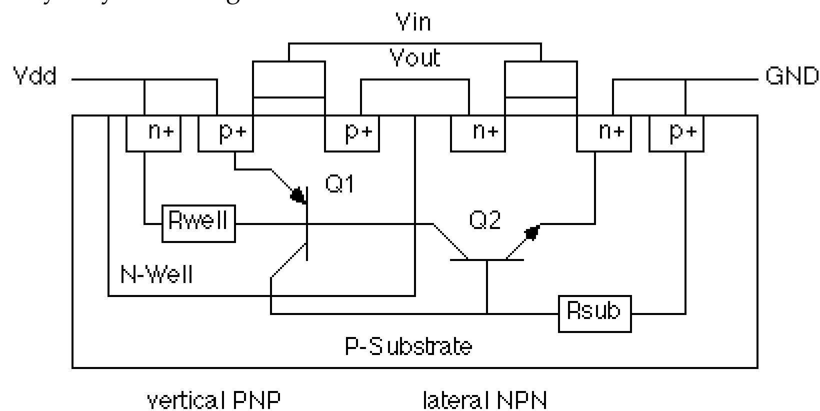


Figure 5-12 : Cross section of the PNPN parasitic structure in standard CMOS technology

5.4.3.6 Single-Event Burnout (SEB)

Another type of destructive effect, called Single-Event Burnout, occurs mainly in power MOSFETs when the source gets forward-biased and the drain-source current is higher than the breakdown voltage of the parasitic structures. The resulting high-current may provoke a local overheating able to destroy the device.

5.4.3.7 Single-Event Gate Rupture (SEGR)

Single event gate rupture occurs when a particle damages (increased leakage current) or ruptures the gate oxide insulation (device destruction) of a power MOSFET.

5.4.3.8 Summary

Table 5-3 provides a list of integrated circuits technologies and families with their respective sensitivity to SEEs.

Table 5-3 : Relevant single event effects as a function of component technology and family

Technology	Family	Function	SEL	SEGR	SEB	SEU	MCU/MBU	SEFI	SET
Power MOS				X	X				
CMOS, BiCMOS and SOI	Digital	SRAM	X*			X	X		
		DRAM	X*			X	X	X	
		FPGA	X*			X	X	X	X
		Flash EEPROM	X*			X		X	
		µP / µcontroller	X*			X	X	X	X
	Mixed signal	ADC	X*			X		X	X
		DAC	X*			X		X	X
	Linear		X*						X
Bipolar	Digital					X			X
	Linear					X			X

*except SOI

6
Choosing a design hardening strategy

This section will be added soon.

7 Technology selection and process level mitigation

7.1 Scope

Radiation-Hardening-By-Process (RHBP) concerns modifications in manufacturing processes in order to reduce the consequences of radiation on integrated circuits. This goal can be achieved by several means such as modifications of doping profiles in devices and substrates, optimization of deposition processes for insulators and use of specific materials. These techniques deal with two main effects: TID and SEEs.

- TID is associated to charge deposition in insulators (e.g. grid oxide and field oxide), thus degrading their properties. This is due to a difference in the mobility and trapping of electrons and holes, resulting in a net positive trapped charge. The result is a current leakage increase either intra-device (within a transistor) or inter-device (between two adjacent transistors). Solutions devoted to reduce the impact of TID focus on modifying insulator's properties and doping levels in active regions nearby interfaces. Currently, Shallow Trench Isolation[2] (STI) is one of the main concerns for TID effects in CMOS technology, particularly the parasitic sidewall and top corner regions. Therefore, most of the presented techniques devoted to mitigate TID concern STI oxide.
- SEEs are associated to instantaneous failures in active regions and thus can be mitigated by modifications of used materials and/or structures or by using alternative substrates such as Epitaxial layers, Silicon On Insulator (SOI) or Silicon On Sapphire (SOS).

The designer must keep in mind that the sensitivity to radiation effects of integrated circuits may also be very dependent on the technology scaling. As an example, in reference [12] is shown that the Soft Error Rate[3] (SER) for DRAMs remains relatively constant with scaling while for SRAMs it significantly increases for each new technology generation.

[2] Shallow Trench Isolation (STI), also known as "box isolation technique", is a feature which prevents electrical current leakage between adjacent transistors. STI is generally used in sub-0.5µm CMOS technology.
[3] A soft error is an error in a memory, for example caused by an upset, which can be recovered by rewriting the correct value or reinitializing the system.

7.2 Table of effects vs mitigation techniques

Mitigation techniques		Radiation effects				Page
		TID	SET	SEU	SEL	
7.3.1	Epitaxial layers				X	36
7.3.2	Silicon On Insulator		X	X	X	37
7.3.3	Triple wells		X	X	X	41
7.3.4	Buried layers		X	X	X	43
7.3.5	Dry thermal oxidation	X				44
7.3.6	Implantation into oxides	X				46

7.3 Mitigation techniques

7.3.1 Epitaxial layers

Description of the concept/implementation

One alternative to bulk substrate is the substrate with an epitaxial layer. This technique consists in growing a thin monocrystalline film on the substrate. Because the substrate acts as a seed crystal, the deposited film takes on a lattice structure and orientation identical to those of the substrate.

Epitaxial layers are used in manufacturing processes both for Bipolar Junction Transistors (BJT) and modern CMOS (Figure 7-1).

The main interest related with radiation hardening is that epitaxial layers reduce the formation of PNPN paths because of the lower substrate resistance, thus reducing the risk of latchup.

Figures/diagrams

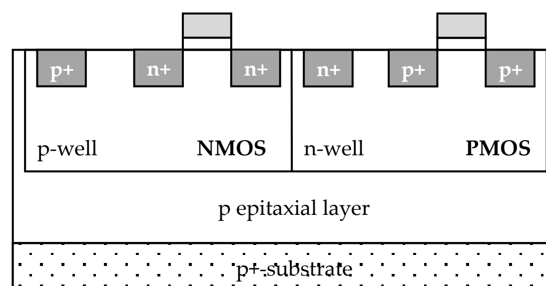


Figure 7-1 : Example of epitaxial layer in CMOS technology

Example(s)

P-type epitaxial layer on P+ substrates are a common choice for latchup mitigation, and require the epitaxial layer be less than about 2.75 μm thick [13][14].

Available Test Data (simulations, radiation testing, in-flight)

Simulation of the device shows the impact of the buried layer on the reduction of charge collection by more than 70% for lightly ionizing events and by more than a factor of ten for highly ionizing events [15].

Known issues (Weaknesses, elements to be considered)

The efficiency of the buried layer depends on:

- The control of the amount and uniformity of the deposition's resistivity and thickness
- The cleanliness and purity of the surface and the chamber atmosphere
- The prevention of the typically much more highly doped substrate wafer's diffusion of dopant to the new layers
- The imperfections of the growth process
- The protection of the surfaces during the manufacture and handling

IC family	Any
Abstraction level	Process
Pros	Increase SEL hardness
Cons	Fabrication cost
Mitigated effects	SEL
Suitable validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	Atmel

7.3.2 Silicon On Insulator

Description of the concept/implementation

The Silicon On Insulator (SOI) technology [16] is an alternative to conventional silicon substrates in CMOS semiconductor manufacturing. In usual CMOS semiconductors, only the very top region of the silicon is used for carrier transport. The inactive part, which represents more than 99% of the wafer, is used as a mechanical support for active regions. Nevertheless, inactive regions contribute in deteriorating performances of the circuit, for example through leakage currents.

In SOI fabrication process, transistors are built on a silicon layer, called Buried OXide (BOX), deposited on silicon dioxide insulating layer (SiO_2) (Figure 7-2 (b-c)). These advantages simplify fabrication steps, improve density and reduce parasitic capacitance.

Fully/partially depleted SOI

Applying a positive voltage to a NMOS transistor’s gate depletes the body of P-type carriers and induces an N-type inversion channel on the surface of the body. If the transistor body depth is thin, due to the insulator layer being close the substrate surface, then the transistor body can be fully depleted (Figure 7-2 (c)).

On the other hand, if the insulated layer is thicker, the inversion region does not extend the full depth of the body, the area is then said to be “partially depleted” (Figure 7-2 (b)). In this case, the most buried part of the body is not depleted, and thus not connecting to anything. However it is coupled to the gate by the gate capacitance and to the source and drain by diode junctions. The voltage relies on the recent transistor electrical activity (“history effects”) as described in [17].

Impact on radiation effects

SEL immunity

SOI inherently eliminates latchup, which can occur in CMOS devices due to a parasitic condition in which at least one PNP and at least one NPN transistor act like a thyristor if turned on as a consequence of prompt dose event or a single event transcient. Because the wells in an SOI device are completely oxide isolated, the parasitic thyristor effect cannot occur.

SET and SEU hardening

SOI's charge collection volume is about 10 times less than that of bulk silicon, so SOI is far less likely to experience bit-switching current pulses. Moreover, this inherent advantage can be improved upon by fabricating a connection to the body of a device that provides a place for ion charges to go to ground. This structure contrasts with most commercial SOI processes, which use a floating body and are less SEU resistant [18]. Commercial SOI generally avoids the body tie because it imposes a 30 percent area penalty, but hardened SOI technology can substantially reduce this penalty by means of specialized techniques.

TID sensitivity

As seen before, SOI helps mitigating SEE. However, the BOX layer presents an additional insulator for charge trapping and a resulting intra-device leakage path along the bottom of the active silicon device layer.

Reference [19] presents how TID charge in partially-depleted device’s BOX layer can reduce the back channel threshold voltage and increase leakage.

Reference [20] shows that the gate oxide and the BOX layer are electrically coupled through the fully depleted silicon body. In this case, trapped charge in the BOX may also cause shifts in the effective threshold voltage of the front gate. Since the silicon is so thin, it is not possible to increase the doping and maintain the fully depleted mode of operation. In this case, mitigation strategies involve either hardening of the BOX insulator (see section 7.3.6 implantation into oxyde), or removal of the substrate and thinning or removal of the BOX layer [21].

Figures/diagrams

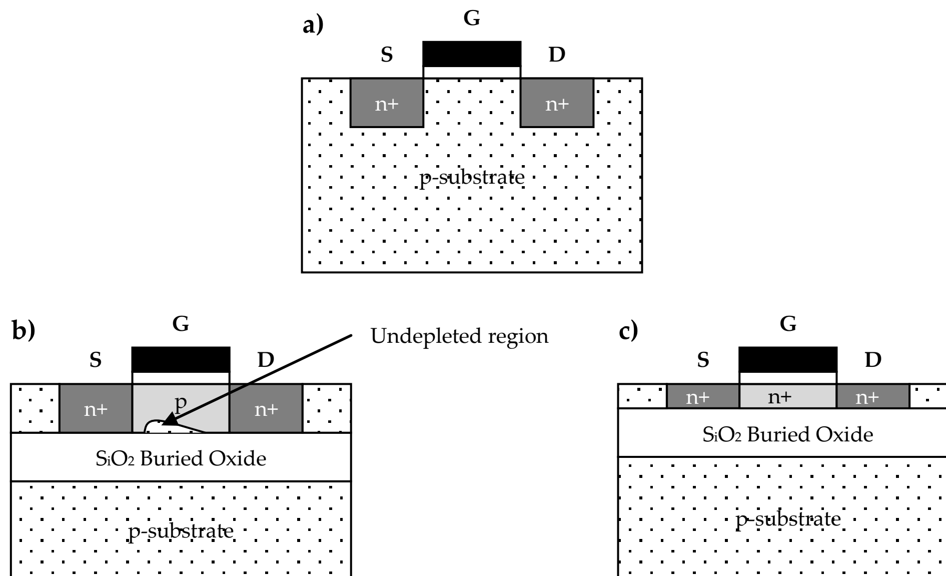


Figure 7-2 : a) Conventional bulk NMOS transistor, b) Partially depleted SOI, c) Fully depleted SOI

Example(s)

As an example, Silicon On Sapphire (SOS) [22] is a hetero-epitaxial[4] technique where a silicon film is grown on a sapphire (Al_2O_3) substrate. SOS was the first mature SOI technology [23][24][25][26]. According to [19], until the 1980s, it was the only SOI technology able to produce LSI-VLSI circuits, such as microprocessors, SRAMs, gate arrays, ADCs, etc.

Due to its inherent resistance to radiation, Silicon On Sapphire is mainly used in aerospace and military applications. One of the most important advantages of SOS, alike SOI, relies on the insulating layer which virtually eliminates the parasitic drain capacitance that is present in bulk silicon. Thus, it leads to an important improvement in transistor performances as this capacitor does not need to be charged and discharged on every cycle. This performance increase allows producing circuits having the same performance than bulk silicon ones but using less advanced manufacturing processes. Finally, another advantage of this technology is that it is manufactured using the same facilities than common bulk silicon wafers. However, due to the high substrate weight, commercial facilities are often not able to produce such wafers.

Finally, SOS requires a more complex manufacturing process than bulk silicon. This reason, combined with the expensive sapphire substrate, prevents this technology from leaving specific applications like military and space applications or some RF devices.

Available Test Data (simulations, radiation testing, in-flight)

- The first SET and SEU experimental results obtained on SRAM devices processed with 2.5 μm partially depleted SOI technology showed error rates comparable to the ones of SOS and lower than those of bulk CMOS[27].

[4] Hetero-epitaxial is an epitaxy performed with materials of different nature.

- The SER for an SRAM, developed with 0.35 μm partially depleted SOI technology (with body ties), was improved by 1.5 orders of magnitude at 1.5V with respect to the one of bulk CMOS SRAMs [28].
- Alpha-particles irradiation performed on a 4M-bit SRAM using a 0.1 μm partially depleted SOI technology with body ties, showed a SER two orders of magnitude lower for SOI than for bulk chips [29].
- Circuit simulations and experimental data were correlated in order to compare the intrinsic hardness of 0.25 μm SOI and bulk technologies [30]. The main conclusion is that bulk and SOI technologies optimized for consumer applications (non-hardened by the use of body ties) exhibit comparable LET threshold for SEU. Nevertheless, due to the smaller saturated cross section (sensitive area), the SOI error rate is significantly lower than the bulk one, even in the worst case when the SOI supply voltage is lower than the one of bulk.
- A study reports the Soft Error Rate (SER) impact of process scaling over four technology generations (0.35, 0.25, 0.18 and 0.13 μm) and provides an experimental assessment of alpha and neutron SER [31]. The results show that SER is reducing on a per-bit basis in future technologies. For the 0.25 μm technology node, partially depleted SOI provides a reduction in SER over its bulk counterpart. However, for the 0.18 μm node, both bulk and partially-depleted SOI technologies are equally sensitive to neutron induced SER.
- A study explored the production and propagation of SETs in digital CMOS circuits [32]. Scaling trends to the 100 nm technology node are explored using three-dimensional mixed-level simulations, including both bulk CMOS and SOI technologies. Transients approaching 1 ns in duration are predicted in bulk CMOS circuits. Body-tied SOI circuits produce much shorter transients than their bulk counterparts, making them more amenable to transient filtering schemes based on temporal redundancy. Body-tied SOI circuits also maintain a significant advantage in single-event transient immunity with scaling.
- The proton response of a 0.35 μm SOI technology on UNIBOND[5] material was investigated [33]. Threshold-voltage shifts of the front-gate and back-gate transistors are observed. The conclusion is that this technology would perform well in a proton-radiation environment.
- Body-ties effects on SEU resistance were analysed for a 0.2 μm fully depleted SOI SRAM [18]. 3D simulations revealed an increase in the threshold LET from 5.8 to 8.1 MeV/(mg/cm^2).

Added value (efficiency)

- Up to 30% lower power consumption, 20% higher performance and 15% higher density than traditional bulk CMOS at the same feature size.

The advantage of using an insulating layer is an increased performance by reducing the junction capacitance as the junction is isolated from the bulk silicon. Moreover the decrease in junction capacitance also reduces the overall power consumption of the circuit.

Known issues (Weaknesses, elements to be considered)

- If SOI improves SEU and SEL hardness, its buried oxide layer increases sensitivity to TID.
- The primary barrier to SOI implementation is the drastic increase in substrate cost, which contributes an estimated 10 - 15% increase to total manufacturing costs compared to bulk substrate device.

[5] UNIBOND is a new type of SOI substrate developed using a thermal oxide and the Smart-Cut process to adjust the silicon-film thickness. This Smart-Cut process is based on wafer-bonding and hydrogen implantation and does not require a specific high-energy and high-flux ion-implant.

IC family	Analogue and digital ASICs
Abstraction level	Process
Pros	Power consumption, performance, density Vs traditional CMOS
Cons	Substrate cost (+ 10-15%)
Mitigated effects	SEL (Immunity), SET and SEU
Suitable validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	SOI : SOITEC, AMD, STM among others SOS : Peregrine, Silanna among others

7.3.3 Triple wells

Description of the concept/implementation

Hardening devices against Single Event Effects may be done by reducing charge collection at critical device nodes. This can be accomplished by introducing extra doping layers to limit substrate collection [13][34]. In SRAMs, triple-well structures have been used to decrease SEU and SEL sensitivity [13] [14] [35].

In CMOS, both NMOS and PMOS transistors are used in association with P-wells and/or N-wells depending on the substrate doping and the process:

- The single-well process, illustrated in Figure 7-3 (a), uses an N-well to build a PMOS in a P-type substrate. This technology is the less expensive to produce circuits, however, at the cost of lower-performance chips because the devices characteristics cannot be optimized. Moreover, it requires a heavily doped substrate, thus increasing the probability of having SEL.
- Twin-well process uses a lightly doped substrate that is either P-type with P-wells for NMOS transistors or N-type with N-wells for NMOS transistors (Figure 7-3 (b)). This technology provides the basis for separate optimization of the NMOS and PMOS transistors, thus making it possible for threshold voltage, body effect and the channel transconductance[6] of both types of transistors to be tuned independently. Because of the lightly doped substrate, thus providing a high resistivity zone, the risk of latchup is decreased compared to the single-well process.
- In the triple well process, assuming a P-type substrate as illustrated in Figure 7-3 (c), the PMOS devices are constructed in a N-well (as in the single or double well process), however the P-well of the NMOS devices is constructed within a deep N-well (the third well). This means that both device types are isolated from the substrate by a reversed biased junction.

Figures/diagrams

[6] Tranconductance is the ratio of the current change at the output port to the voltage change at the input port of a transistor. It is expressed in ampere per volt or Siemens.

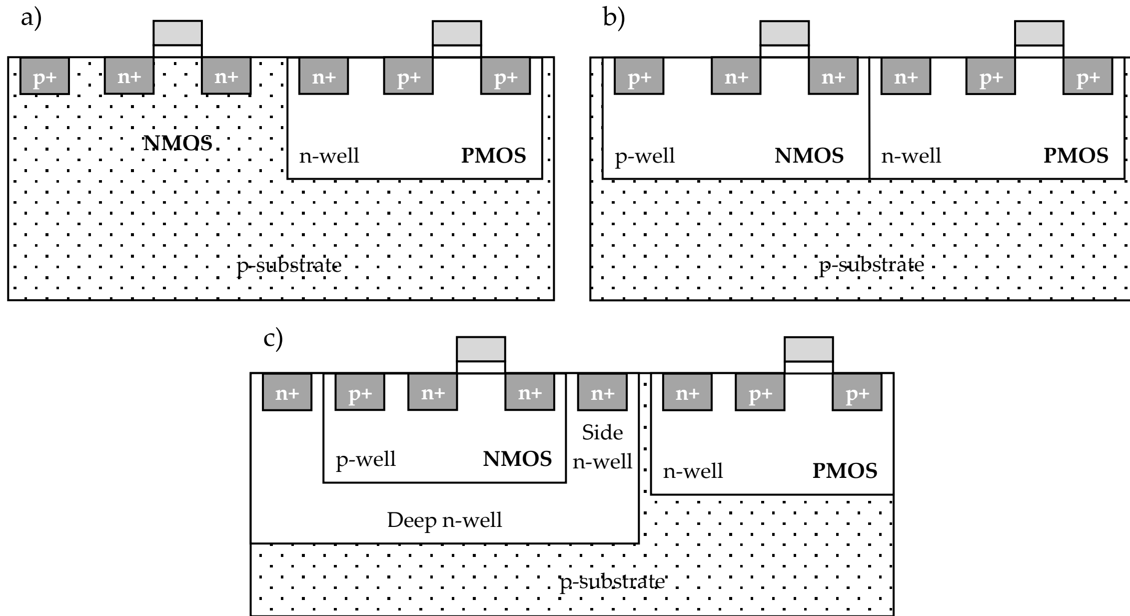


Figure 7-3 : a) single-well technology, b) twin-well technology, c) triple-well technology implementing a deep n-well to isolate the p-well forming the NMOS from the substrate

Available Test Data (simulations, radiation testing, in-flight)

Triple well has been found to result in reduced alpha-particle and neutron Soft Error Rates (SER) in 130 and 90 nm latches and SRAMs [13][36]. A study [36] showed a 40% lower SER (alpha & neutron) for SRAM and latches with triple well.

Known issues (Weaknesses, elements to be considered)

- Triple well has been demonstrated to increase the SER in 150 nm memory devices [37]. This study showed that lower triple-well implant energy produces a higher SER.
- Depending on the well doping and depth, and placement of well contacts, the triple well can increase the well resistance and exacerbate the single event response [14].
- This condition could also be problematic for dose rate photocurrents with the added junction areas. Retrograde wells and buried layers can also be used to provide an internal electric field that opposes collection of charge deposited in the substrate [38][39].

IC family	Any
Abstraction level	Process
Pros	Increase SEU and SEL hardness
Cons	Increase manufacturing cost

Mitigated effects	SET, SEU, SEL
Suitable Validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	N/A

7.3.4 Buried layers

Description of the concept/implementation

Buried layers are, generally highly doped zones buried inside the well or substrate and placed beneath sensitive nodes, such as storage nodes, in order to collect or repel excess charge deposited by particles, diverting it from the devices on the surface.

The use of a buried layer of high doping in a lightly doped substrate is an alternative to the use of highly doped substrates [40]. The doping profiles and the presence of buried layers (which may include doped layers, insulating layers, or layers of modified material properties) can impact the radiation response of devices [13], and must be considered in the study of radiation effects and mitigation options. For example, an increase in the current necessary to trigger electrical latchup results in an increase of Single Event Latchup immunity.

Figures/diagrams

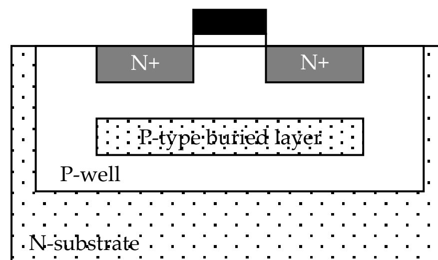


Figure 7-4 : Schematic view of a P-type buried layer in a P-well

Example(s)

- In a vertical BJT structure, the use of a highly doped layer below the collector helps to confine prompt dose collection volumes, so that the base-collector junction current is much less than the collector-substrate junction [41].
- In addition to global buried layers, buried layers may be selectively added below device regions to optimize performance or for radiation effects mitigation. Examples include buried P+ layers (Figure 7-4) within the P-well [42] or an N-grid [43] to reduce alpha particle single event sensitivity. While buried layers in CMOS remain an effective strategy for latchup mitigation, results of [13][35][14][44] suggest limited effectiveness for mitigation of single event errors, and demonstrate that proper triple well designs may be a more effective strategy for advanced CMOS.
- A buried P+ layer below a deep trench isolated SiGe Heterojunction Bipolar Transistor (HBT) has been shown to reduce electrostatic discharge (ESD) and latchup [45], and thus has been

proposed to reduce heavy ion charge collection [15]. Devicesimulation shows that the impact of the buried layer on the charge collection reduction happens at somewhat longer times [15].

- In GaAs technology, a buffer layer grown at Low Temperature (LT) during the epitaxial growth process causes the As to precipitate and form recombination sites, reducing the recombination lifetime in the layer beneath the active device [46]. While this is not a silicon device, the concept is interesting and may be applicable.

Available Test Data (simulations, radiation testing, in-flight)

Simulation of the device shows the impact of the buried layer on the reduction of charge collection happens at somewhat longer times [15].

Added value (efficiency)

Buried layers in CMOS are an effective strategy for latchup mitigation.

Known issues (Weaknesses, elements to be considered)

Buried layers offers limited effectiveness for mitigation of SER, results demonstrate that proper triple well designs may be a more effective strategy for advanced CMOS [13] [35] [14] [44].

IC family	Any
Abstraction level	Process
Pros	Increase SEL and SER hardness
Cons	Increase fabrication costs
Mitigated effects	SET, SEU, SEL
Suitable validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	N/A

7.3.5 Dry thermal oxidation

Description of the concept/implementation

As explained in 7.1 the dominant problem provoked by TID is the net positive charge. Consequently, the general idea is either to increase electro trapping and to increase the overall quality of oxides or to reduce hole trapping. Trapping properties can be adjusted by modifying process recipe parameters (growth/deposition rates and times, temperatures, gas cocktail, etc), or by pre-, co- or post-processing such as specialized implantation or annealing steps

Example(s)

- The growth temperature is an important parameter as it was demonstrated that hole trapping varies inversely with dry-oxygen growth temperatures over 900-1200 °C [47].
- Nitrogen incorporation during growth can degrade the TID hardness, while use of Argon instead does not degrade the hardness [47].
- Post Oxidation Annealing (POA), also dependent on ambient gasses, can alter the trapping properties, generally decreasing the hole trapping as long as the oxygen concentrations are high enough. Otherwise, POA annealing in nitrogen can degrade the hardness more than POA in argon. POA in nitrogen also reduces electron traps. This is common practice for thermal oxides in commercial technologies; however not desirable for hardened technologies [47].
- Nitrogen implantation into silicon prior to oxidation improved the proton radiation hardness of oxynitride gate NMOS transistors [48].

Available Test Data (simulations, radiation testing, in-flight)

Table 7-1 : Impact of thermal oxidation process parameters on TID hardness

Process variable	Value	Impact
Temperature	1/T ($900 < T < 1200$ °C)	Hardness degradation (hole trapping increased)
Ambient gases	N Ar	Hardness degradation No hardness degradation
Post Oxidation Anneal	O N Ar	Hardness degradation Hardness degradation No hardness degradation
Pre-oxidation low energy N_2^+ implant	5keV 10^{14} < Fluence < 10^{15} cm^{-2}	Forms thin SiO_xN_y with improved proton TID hardness up to proton fluences of 10^{12}.cm^{-2} (~7.5 Mrad)

Added value (efficiency)

Silicon Oxynitride gate NMOS transistors formed by nitrogen implantation into Silicon prior to radiation enhance proton induced TID up to fluencies of 10^{12} cm^{-2}, corresponding to 7.5 Mrad.

Known issues (Weaknesses, elements to be considered)

Some parameters degrade hardness, see Table 7-1.

IC family	Any
Abstraction level	Process
Pros	Improved proton TID hardness
Cons	Increased fabrication cost

Mitigated effects	TID
Suitable Validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	N/A

7.3.6 Implantation into oxides

Description of the concept/implementation

Implantation of elements, such as Al, Si, P, Fl and As, into oxides has been shown to improve the TID hardness primarily by increasing electron trapping [49][50][51].

Figures/diagrams

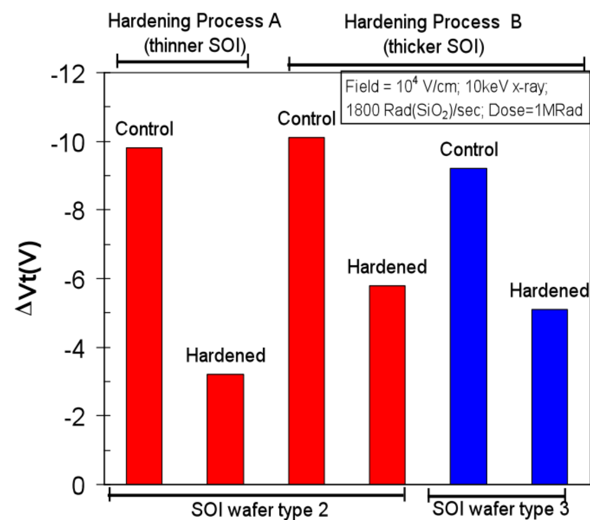


Figure 7-5 : Radiation-induced back channel threshold voltage shifts for different SOI substrates types, SOI layer thickness and hardening process conditions [52]

Example(s)

SOI technology is presently used in many commercial applications, particularly microprocessors, and in some rad-hard CMOS applications. As presented in 7.3.2, SOI helps to mitigate single event effects. However the Buried OXide (BOX) layer presents an additional insulator for charge trapping. This may induce back-channel leakage in partially depleted SOI and front-channel threshold voltage shifts in fully depleted SOI. One strategy is hardening the BOX layer by the mean of Fluorine implantation into the BOX layer. This technique proved its efficiency by improving interface hardness and reducing the transconductance degradation [50]. Test results, illustrated in Figure 7-5, show that the hardening process reduces the radiation-induced threshold-voltage shift (ΔVt) of the BOX layer by 45%-65% compared to the respective unhardened wafer counterparts [52].

Available Test Data (simulations, radiation testing, in-flight)

- Fluorine doping has been shown to improve the radiation hardness of gate and field oxides [50] [53].

- The TID degradation of current gain of lateral PNP transistors is reduced with As implanted SiO_2 passivation on the emitter base junction [50]. The use of SiC passivation has also been demonstrated to improve the TID hardness of bipolar transistors [54].
- Arsenic implanted SiO_2 reduces TID degradation in lateral PNP BJT [51]. However As in MOS gate oxides may be detrimental [55].

Known issues (Weaknesses, elements to be considered)

- Hardness degradation was observed with As implantation in gate oxide [55].
- Boron doping (such as comes from the Boron gate doping in CMOS processes) has been shown to degrade the hardness [7] [56].
- Implantation of Si into oxide was shown to increase the electron trap density [57]. Subsequent analysis of the Si implanted oxides indicated that the mechanism for reduction of flatband voltage shifts is the formation of silicon nanoclusters in the oxide and proton trapping. Note that the analysis of [58] indicates that the reduction in shift with Si dose is due to proton trapping by Si nanoclusters, and not due to the electron traps which have a much smaller capture cross section.

IC family	Any
Abstraction level	Process
Pros	Improved radiation hardness
Cons	Increased fabrication cost
Mitigated effects	TID
Suitable Validation methods	Ground accelerated tests
Automation tools	N/A
Vendor solutions	N/A

7.4 Technology scaling and radiation effects

The impact of technology scaling on the response of integrated circuits to radiation effects cannot be evaluated only by taking into account only the channel size and the geometry of the transistors. As explained in reference [59], studies have shown that differences in size and geometry affects the radiation-induced response of transistors in a non-consensual way. Moreover, the size and the geometry of the transistors are not the only parameters to be taken into account. Indeed, improving manufacturing processes does not strictly consist in reducing the size of the transistors. Change of materials (e.g. substrates) or new process techniques may twist the predictions. For example, removing the borophosphosilicate glass (BPSG) passivation layer in sub-0.25 µm SRAM allowed an important improvement of the SEU immunity for those devices.

The effects of device scaling on soft-error rate depend on several competing factors. Among them the critical charge required to upset a memory bit is expected to decrease as depicts in early studies [60]. In fact, the increase of radiation effect immunity exists but is not less obvious [61]. Another factor to take into account is the charge collection depth which generally decreases with scaling, hence improving robustness of the circuits. Power supply is also decreasing with scaling which generally has a negative effect on radiation effect tolerance. A smaller transistors also means smaller sensitive volume and is, thus, less likely to be hit by a particle, which tends to increase its immunity. One of the advantages of reducing the transistor's channel length is that it allows increasing its switching speed. But increasing the frequency also implies increasing the probability of capturing a transient. Indeed, in low frequency systems most of the upsets are provoked by particles directly hitting the transistors, whereas in fast systems, upsets provoked by propagating SETs must be taken into consideration as they are not negligible anymore [62].

In the following sub-chapters are presented the consequence of technology scaling on the tolerance of faults provoked by TID and by SEEs.

7.4.1 Effects of technology scaling on TID sensitivity

Observations made over several generations of manufacturing processes have shown that total dose degradation increases when the MOSFET channel length decreases [63]. This study puts in evidence large increases in threshold voltage shifts after irradiation as gate lengths are decreased. Moreover this phenomenon has a greater impact on NMOS devices than on their PMOS counterparts.

7.4.2 Effects of technology scaling on SEE sensitivity

SEE sensitivity varies with technology scaling depending on the nature of the components. A general observation is that for most devices the sensitivity of a single bit was decreased over several generations of chips. However, this improvement is counterbalanced by the increase of density and thus, the overall sensitivity for a whole system has not changed or in some cases it has even increased.

Microprocessors

The main effect of heavy ions and protons on microprocessors is the upset in the internal memory cells. Since the last 15 years, the feature size of the CMOS transistors has been reduced by more than one order of magnitude but the LET threshold to generate an upset on these devices has remain unchanged [61]. However, the cross section of the Power PC750 (0.25 μm) is one order of magnitude lower than the one of the Power PC603e (0.35 μm) while both are manufactured using thin epitaxial layers over highly doped substrates. Reference [61] also mentions that the decrease of the device size may potentially increase the upset rate in the terrestrial environment as the range of recoil atoms is increasing when devices become smaller and thus reaction products require lower energy to upset the device.

The study presented in reference [61] concludes on the fact that the cross section generally decreases when devices become smaller but the rise of the frequency makes increase the cross section. However, the magnitude of the frequency dependence decreases as the circuit becomes smaller.

DRAM memories

DRAM is currently one of the most robust devices in term of soft errors [12] [61]. The single bit sensitivity has been reduced by a ratio of about four or five per generation. This is attributed to the shrinking junction volumes, the relatively high node – capacitance and the relatively gradual voltage scaling. From the one-megabit to the one-gigabit DRAM generations, the DRAM cell single error sensitivity has been reduced by a factor of 1,000, thus the overall DRAM system sensitivity has remained essentially unchanged. As frequency continuously increases, transcient errors in bitlines and sense amplifiers will become dominant in the next memory generations, thus soft error immunity is expected to increase.

SRAM memories

Early SRAMs were more robust against SER because of high operating voltage and the fact that data was stored as the state of a bi-stable circuit made up of two large cross-coupled inverters, each strongly driving the other to keep the bit in its programmed state [12]. The evolution through successive generations of SRAM devices showed an increase of the single bit SER due to the shrinking of the cells volume, big reductions in operating voltage and reduction in node capacitance. This happened particularly in products using BPSG as a passivation layer [19]. Most recently, with technologies below 0.25µm, the SRAM single bit SER has saturated and may tend to decrease due to the saturation in voltage scaling, reductions in junction collection efficiency and increased charge sharing due to short-channel effect. But, with the rise of the amount of embedded SRAM in electronics, the overall SRAM system SER is increasing significantly with technology scaling and has now become a significant reliability concern [61]. Error Detecting And Correcting Codes (EDAC) is the best mean to mitigate memory soft errors but the system failure rates may be challenged by the SER in sequential logic.

Sequential and combinational logic

Flip-flops and latches are similar to SRAM cells (they use cross-coupled inverters) but are much more robust against SET because they are usually made of much larger transistors and they are designed with more transistors for each node. Their SER sensitivity tends to increase as the technology is scaled down [12] [61]. Soft errors in logic are a concern for high reliability systems when memory has been protected by error correction mechanism: the peripheral logic failure rate may be dominant. A significant increase in SER was shown with technology scaling from 0.18 µm to 0.13 µm. This trend is high enough to limit the efficacy of memory error correction.

In combinational circuits, radiation-induced charge can generate a short transient in the output which can propagate to the input of a latch or a flip-flop. For older technologies, this was quickly attenuated due to a large load capacitance and large propagation delays. In advanced technologies, with the decrease of the propagation delay, SETs can more easily go through many logic gates, thus increasing the latching probability. In technology nodes beyond 90 nm and at high operating frequencies, there is an increasing risk of soft errors due to latched SET events.

8
Layout

8.1 Scope

This section presents mitigation techniques with respect to the effects of radiation that can be applied at integrated-circuit layout. They are based on modifying the transistor's shapes and inserting protection elements in order to reduce mainly TID and latchup phenomena.

Hardening against TID effects

One of the first concerns about radiation assurance is the TID threat which occurs when charges get trapped in oxides (Figure 8-1), such as gate oxide and Shallow Trench Isolation (STI) oxide [64], or at interface with silicon. It has been demonstrated that the total dose effect decreases as that oxide's thickness scales down [65][66][67]. These studies showed that less than 5 nm thick gate oxides obtained in the latest submicron processes are immune to total dose effects and consequently they do not contribute in the limitation to the use of those devices in applications devoted to operate in radiation environment.

The real obstacle is rather the large density of holes trapped in the thick STI oxide leading to an increase in the leakage current until a loss of functionality of the circuit [68]. This leakage current occurs at the interface between STI oxide and p-doped region, a straightforward solution is thus to avoid contacts between these two zones by changing transistors layout [69]. Several designs are possible but the most commonly used is the Enclosed Layout Transistor (ELT).

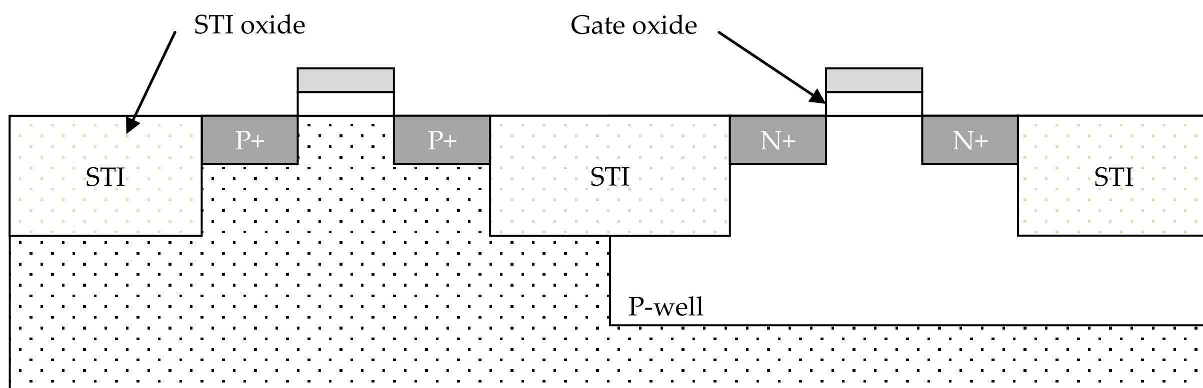


Figure 8-1 : Gate oxide and STI oxide in CMOS technology

Hardening against SEL

The latchup is caused by a pair of parasitic bipolar transistors, hence forming a thyristor. Under certain conditions this thyristor may become conductive, thus creating a low resistance path between V_{DD} and V_{SS}. The risk of latchup can be reduced by inserting contacts and guard rings around the MOS transistors.

8.2 Table of effects vs mitigation techniques

Mitigation techniques		Radiation effects					Page
		TID	SEL	SET	SEU	MBU/MCU	
8.3.1	Enclosed Layout Transistor	X		X	X		51
8.3.2	Contacts and guard rings		X			X	53

8.3 Mitigation techniques

8.3.1 Enclosed Layout Transistor

Description of the concept/implementation

Hardening a design against TID effects can be done by modifying the conventional transistor design. Indeed, avoiding contact between the STI oxide and any p-doped region eliminates current leakage. For instance, one of the two NMOS transistor's n+ diffusion (source or drain) can be surrounded by the thin gate oxide [69]. The most effective layout uses Enclosed Layout Transistor (ELT), also called re-entrant transistor or even Edge-Less Transistor, illustrated in Figure 8-2. Only the n-channel requires a re-entrant design since the p-channel does not experience edge inversion. Reducing the area of the drain allows reducing the device's cross-section and thus the sensitivity to SET and SEU. Consequently, the drain is generally located in the center of the structure.

Figures/diagrams

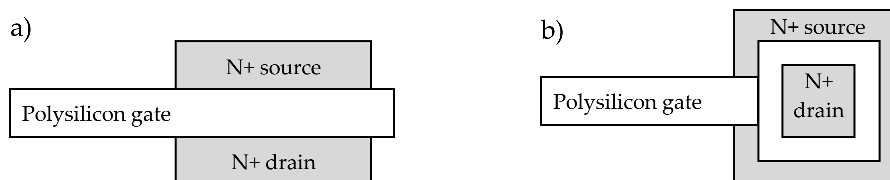


Figure 8-2 : a) Conventional two edge NMOS, b) Enclosed Layout Transistor NMOS

Example(s)

Enclosed Layout Transistor is not the only alternative transistor design aimed at reducing the impact of radiation. Figure 8-3 gives examples of two NMOS transistor designs able to eliminate radiation-

induced leakage current between source and drain doped regions. Ringed source and ringed inter-digitated design have the advantage to offer compact transistors, however they often require violating design rules and are sometimes not completely immune to TID effects [70]. Yet, the most commonly used design is the ELT.

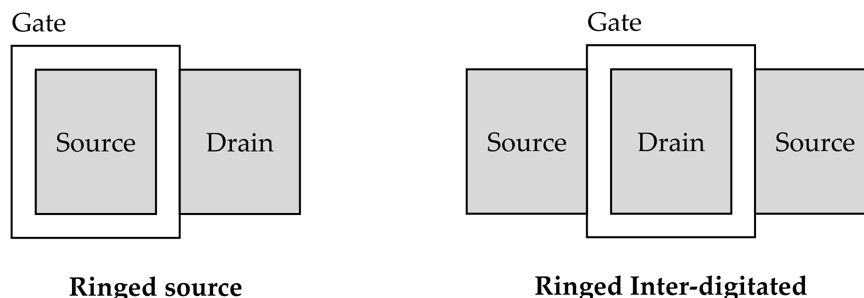


Figure 8-3 : Two examples of NMOS transistor layout eliminating radiation-induced leakage current between source and drain

Available Test Data (simulations, radiation testing, in-flight)

- Using ELT NMOS transistors in combination with guard rings (section 8.3.2) has been demonstrated to provide efficient robustness again the effects of radiations [71][72][73]. One strong advantage of this technique is that it relies on the natural tolerance to TID of the thin gate oxide. Consequently it can be applied to all technologies without requiring specific process care.
- Reference [74] discusses design issues related to the extensive use of Enclosed Layout Transistors (ELT's) and guard rings in deep submicron CMOS technologies, this in order to improve radiation tolerance of ASIC's designed for the LHC experiments (the CERN's Large Hadron Collider). It presents novel aspects related to the use of ELT's: noise measured before and after irradiation up to 100 Mrad (SiO_2), a model to calculate the W/L ratio and matching properties of these devices. Some conclusions concerning the density and the speed of IC's conceived with this design approach are finally drawn. For analog design, the area penalty is important only for long channel ELT devices; a circuit containing few of this kind of transistor will exhibit a non-significant area increase. For digital design, the area penalty factor is generally between 1.5 and 3.5.

Added value (efficiency)

- Eliminates *bird's beak*[7] leakage effect
- Reduces current leakage
- Reduces SET and SEU sensitivity
- Can be applied to all technologies

[7] The bird's beak structure is provoked by a lateral extension of the grown oxide in Local OXidation Of Silicon (LOCOS) process. This results in active area reduction.

Known issues (Weaknesses, elements to be considered)

- Area penalty for analogue circuit: can be non significant or important depending on the number of long channel ELT devices in the circuit.
- Area penalty for digital circuit scales from 1.5 to 3.5.
- Using ELT transistors is not a direct approach. Designers must be aware of the difficulties linked to the peculiarities of the ELT transistor itself, the lack of available commercial libraries using those transistors and the loss of density during integration and the durability of the design. More details about those points can be found in reference [75].

IC family	Any
Abstraction level	Layout
Pros	Reduce current leakage
Cons	Area overhead: non-significant to important depending on the circuit (analogue circuit) and 1.5 to 3.5 (digital circuit)
Mitigated effects	TID
Suitable Validation methods	Radiation ground tests
Automation tools	RHBD libraries: • DARE library (0.18µm technology) [76] • CERN "radtool" (0.24µm technology) [77] • BAE library (0.15 µm technology) [78]
Vendor solutions	N/A

8.3.2 Contacts and guard rings

Description of the concept/implementation

The latchup phenomenon may occur when the two bipolar transistors, forming a parasitic thyristor (shown in Figure 8-4), are conducting due to the presence of parasitic resistors. As a consequence, a low resistance path between V_{DD} and V_{SS} appears and eventually a large current can flow and may lead to a local destruction of the MOS structures.

Preventing latchup from occurring may be done by reducing the gain of the two parasitic transistors and reducing parasitic well and substrate resistors:

- Reducing the parasitic bipolar transistors' gain can be achieved by increasing the distance between the two parasitic complementary transistors. The drawback of such a strategy is that it also reduces the circuit density.
- Reducing parasitic resistor values can effectively be done by using low resistance ground contacts and by surrounding MOS transistors with guard rings (Figure 8-5).

Guard rings form additional collectors for the parasitic transistors. Such collectors are connected either to the positive or negative supply-voltage connection of the integrated circuit. They are placed

considerably closer to the base-emitter region of the transistor to be protected than to the corresponding connections of the parasitic transistor. As a result, the charge carriers injected into one of the two transistors is diverted largely via these auxiliary collectors to the positive or negative supply-voltage connection. These precautions do not completely eliminate the questionable thyristor. However, the thyristor's sensitivity is drastically reduced.

Contacts and guard rings are usually combined with the use of Enclosed Layout Transistors (see 8.3.1).

Figures/diagrams

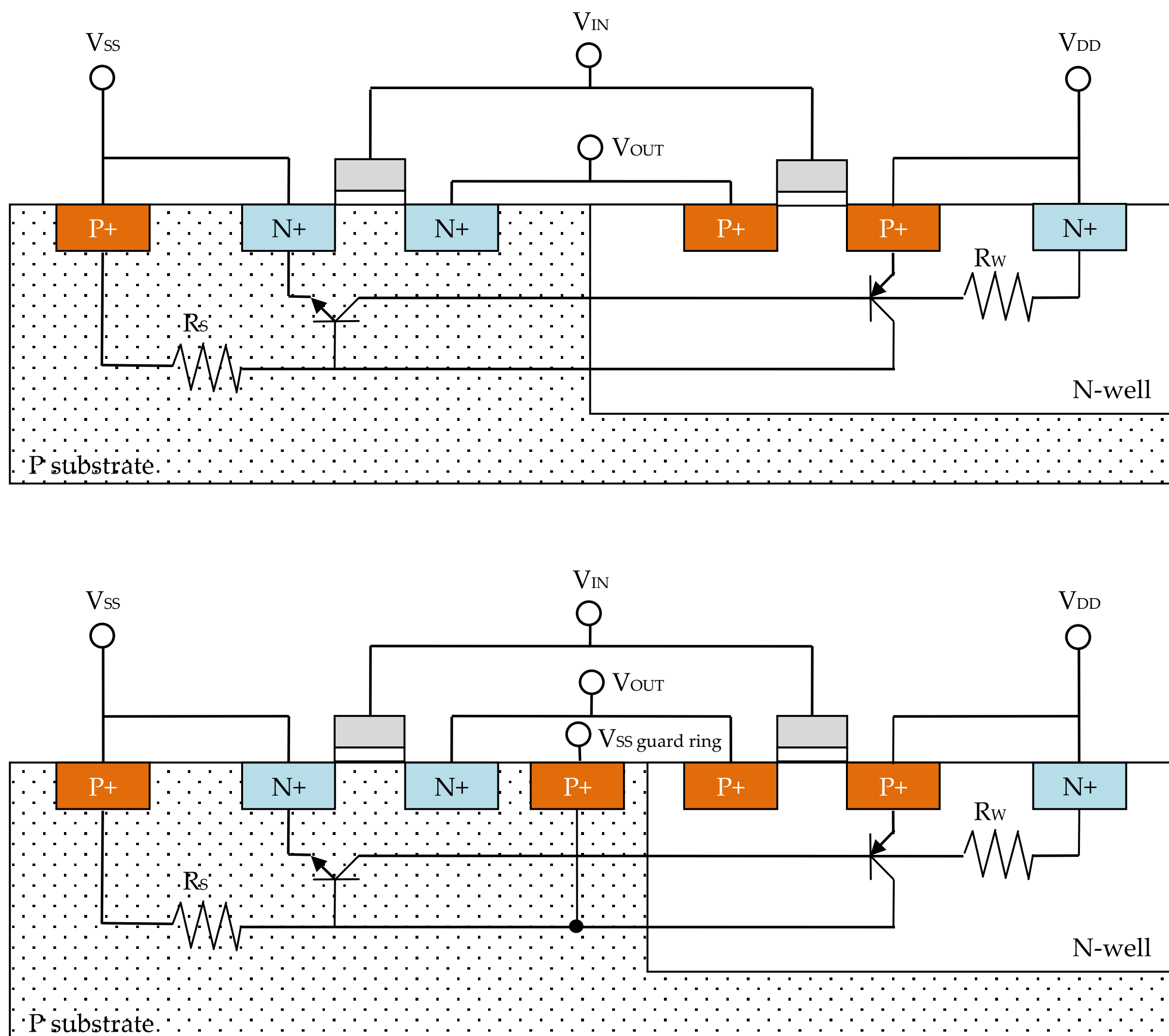


Figure 8-4 : Parasitic thyristor responsible for SEL (top), introduction of P+ guard ring around NMOS transistor (bottom)

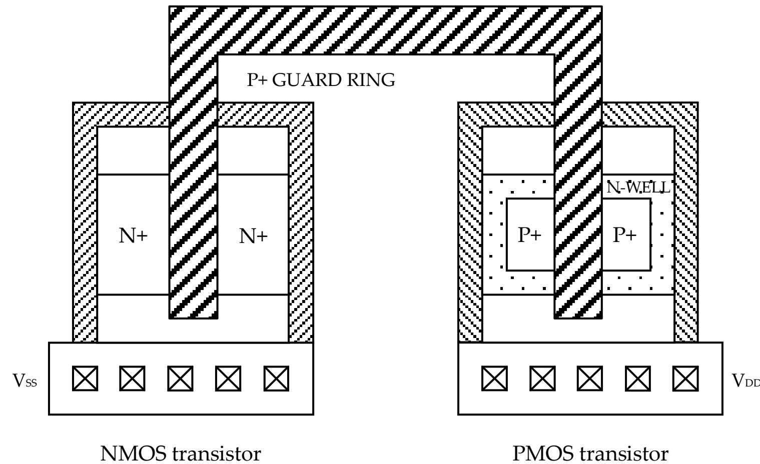


Figure 8-5 : CMOS transistors with guard rings

Example(s)

No data available

Available Test Data (simulations, radiation testing, in-flight)

- Reference [74] discusses design issues related to the extensive use of Enclosed Layout Transistors (ELT's) and guard rings in deep submicron CMOS technologies in order to improve radiation tolerance of ASIC's designed for the LHC experiments (the CERN’s Large Hadron Collider). It presents novel aspects related to the use of ELT's: noise measured before and after irradiation up to 100 Mrad (SiO_2), a model to calculate the W/L ratio and matching properties of these devices. Some conclusions concerning the density and the speed of IC's conceived with this design approach are finally drawn. For analog design, the area penalty is important only for long channel ELT devices; a circuit containing few of this kind of transistor will exhibit a non-significant area increase. For digital design, the area penalty factor is generally between 1.5 and 3.5.
- Reference [79] proposes an analysis of the latchup phenomena with the use of guard ring structures in bulk CMOS substrate. Several structures are analyzed by simulation with and without guard rings.

Added value (efficiency)

- Reference [80] reports that devices implementing guard rings technique usually show very high SEL threshold (LET > 90 MeV.cm^2/mg).
- A significant amount of charge issued from a particle, by direct ionization or as secondary particles, can be collected by diffusion. Adding substrate and well contacts between devices can help prevent MBUs/MCUs.
- Reduces inter-device leakage.
- Reference [81] proposes a methodology to place guard rings in order to reduce substrate coupling noise in mixed-signal circuits. The proposed methodology achieves enhanced isolation

as compared to conventional guard rings by minimizing the number of vertical current paths within the substrate.

- In reference [82] are compared guard ring efficiencies between epitaxial silicon and bulk silicon for sub-quarter micron technology.

Known issues (Weaknesses, elements to be considered)

The cost in cell area for the inclusion of guard rings is typically 10-15% [80].

IC family	Any
Abstraction level	Layout
Pros	SEL robustness up to LET > 90 MeV.cm²/mg
Cons	Area overhead: 10-15%
Mitigated effects	SEL, MBU/MCU
Suitable Validation methods	Radiation ground testing
Automation tools	N/A

8.4 Radiation-hardened libraries

Most of the foundries proposing radiation-hard technologies retired from the market due to both reduced demand by military and aerospace customers and the lack of commercially interesting volumes. An alternative solution is to harden commercial CMOS technologies, hence benefiting from their numerous advantages such as:

- Independent foundries
- Advanced deep sub-micron technologies
- High performance
- Low power
- Low volume/mass
- Low cost

Hardening commercial technology is achieved by combining techniques listed in this layout section. Figure 8-6 illustrates a hardened 2 input NOR gate implementing ELT transistors and guard rings.

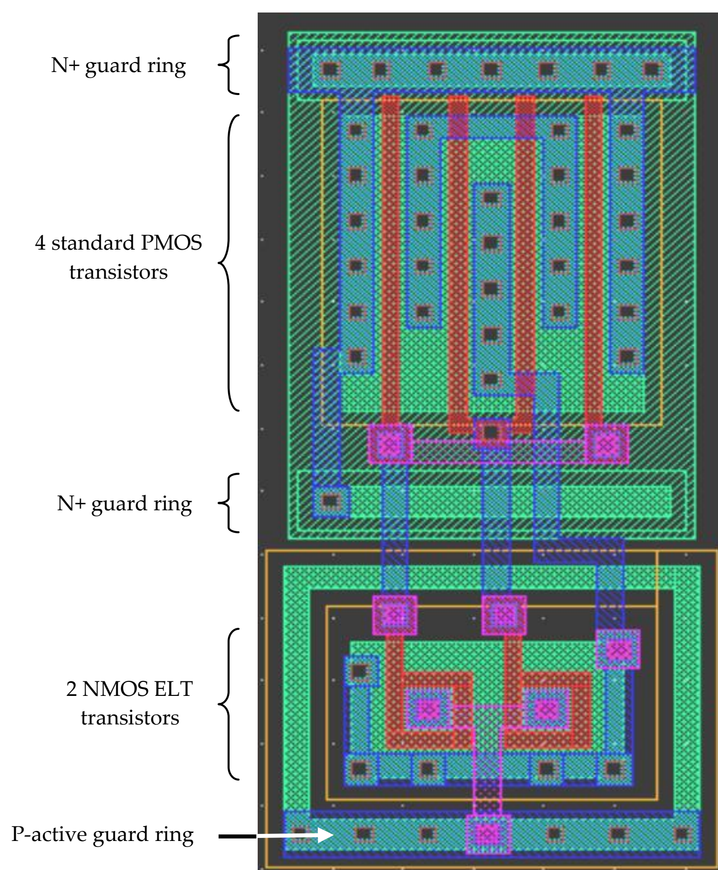


Figure 8-6 : Hardened 2 input NOR gate

In the following, is given a none exhaustive list of well-known radiation hardened libraries.

8.4.1 ESA Design Against Radiation Effects library

The Design Against Radiation Effects (DARE) library development was performed in the framework of an European Space Agency (ESA) Technology and Research Program contract.

DARE library was enhanced with many cells which are often used in typical designs aimed at space applications such as a PLL cell (situated in an I/O cell), I/O pad options with improved ElectroStatic Discharge (ESD) performance including a Low-Voltage Differential Signaling (LVDS) driver and receiver as well as several pull-up and pull-down options. A single-port SRAM compiler is also included in the design kit. Hardened flip-flops based on the Heavy Ion Tolerant (HIT) cell (see section 0) are also proposed in the DARE library [83].

The first use of DARE library for the United Microelectronics Corporation (UMC) 180 nm CMOS 6-layer metal technology in a telecom ASIC, called DROM (an acronym for Demultiplexer-ROuter-Multiplexer), was presented in reference [76]. The area penalty factor between commercial non-hardened cells and DARE cells with the same functionality ranges from 2 to 4. For the DROM core, the penalty factor obtained is 3. The area penalty for the full DROM using in-line pads is 2. There is no speed penalty factor with the DARE library. For DROM, the speed that has been achieved is indeed equivalent to the one with a commercial 0.18 μm library. Power consumption of DARE cells is 2.2 times higher than that of comparable cells in a commercial library. This figure takes into account internal and switching power.

Radiation test results for the DROM core were published in reference [84]. Obtained results demonstrate a level of hardness for the Total Dose higher than 1 Mrad(Si). Concerning SEEs, the ASIC is neither sensitive to SEL nor to SEFIs and the SEU sensitivity observed on flip-flops is compatible with in-orbit use for a geostationary application.

8.4.2 CERN 0.24 µm radiation hardened library

A radiation tolerant 2.0 V standard cell library using a commercial 0.24 µm, 2.5 V CMOS, technology was developed for the Large Hadron Collider (LHC) experiments. Radiation tolerant design techniques, such as ELT transistors and guard rings, have been employed on the layout of the cells to achieve the total dose hardness levels required by LHC experiments.

The library consists of digital core cell elements as well as a number of I/O pad cells. Additionally, it includes a pair of differential driver and receiver pads implementing the LVDS standard. This library features 5 times increase in speed accompanied by 26 times reduction in power consumption as well as an increase of 8 times in gate densities when compared to a currently available 0.8 µm CMOS technology. The penalty that the radiation tolerant techniques introduce in the library cells is estimated to be about 70%.

Radiation tolerance of the cells was evaluated on a few demonstration circuits [77]. As an example for a ring oscillator device, a speed degradation of 5.2 % was measured after 30 Mrad of total dose, while no significant increase in leakage current was observed.

8.4.3 BAE 0.15 µm radiation hardened library

BAE Systems has developed a radiation hardened 150 nm standard cell ASIC library having a total of 391 internal macros and 29 I/O macros [78]. Dual port and single port RAMs are configured using a "RAM assembler" supplied with the design tool kit. The library also includes a radiation hardened 3.125 Gbits/sec SERializer/DESerializer (SerDes) core.

Radiation results show that no parametric or functional degradation was observed through a total dose of 3 Mrad(SiO_2). SEU test results indicated no data upset observed on the tested cell design at various test angles from 0 to 90 degrees in a worst-case SEU radiation environment [85].

8.4.4 Ramon Chips 0.18 µm and 0.13 µm radiation hardened libraries

Ramon Chips has developed a 0.18 µm [86] and a 0.13 µm [87] radiation hardened libraries. The 0.18 µm library is available for 3.3V and 1.8V using the 0.18 µm Tower Semiconductors CMOS process These libraries are composed of 80 logic cells (40 kgates/mm^2), 15 I/O cells, single and dual port SRAM (80 kbits/mm^2).

Radiation tests results show that TID immunity is higher than 300 krad(Si) in all tests, no SEL detected up to 106 MeV.cm^2/mg and error rate is less than 10^{-12} error/bit/day[8] for SEU in flip flops (at Low Earth Orbit), and 2.10^{-7} error/bit/day for SEU in SRAM (at Low Earth Orbit).

[8] The error rate (in units of errors/bit-day) is calculated by taking into account the flux of particles in the environment and the upset cross section curve, which describes the device's sensitivity to that environment.

These libraries were used by Ramon Chips to produce several ASICs such as a microprocessor based on the LEON3FT [88] and a JPEG2000 image compression chip.

The 0.13 μm library supports 2.5V and 1.2V operating voltages. Densities reached are 120 kgates/mm^2 for the logic and 200 kgates/mm^2 for SRAM cells. The power consumption is also reduced by 40% compared to the 0.18 μm library.

8.4.5 Aeroflex 600, 250, 130 and 90 nm radiation hardened libraries

Aeroflex provides advanced 90, 130, 250 and 600 nm CMOS silicon gates processed in a commercial fabrication. Details are the following:

- 600 nm library: radiation tolerance to 300 krads(Si). SEU-immune less than 2.10^{-10} errors/bit-day (based on standard evaluation circuit at 4.5V worst case condition. Non-hard flip-flop typical is 4E-8) [89].
- 250 nm library: radiation hardened from 100 krads(Si) to 1 Mrads(Si). SEU-immune less than 1.10^{-10} errors/bit-day (based on standard evaluation circuit at 2.25V or 3.6V core/3.0V I/O VDD 25°C condition. Non-hard flip-flop typical is 8E-9) [90].
- 130 nm library: radiation hardened from 100 krads(Si) to 300 krads(Si). SEU-immune less than 1.10^{-10} errors/bit-day (based on standard evaluation circuit at 1.1V core/3.0V I/ O VDDIO 25°C condition. Non-hard flip-flop typical is 5x10-8) [91].
- 90 nm library: radiation hardened from 100 krads (Si) to 1 Mrads(Si) [92].

8.4.6 Atmel MH1RT 0.35 μm and ATC18RHA 0.18 μm CMOS radiation hardened libraries

Atmel MH1RT Gate Array and Embedded Array families are fabricated using a radiation hardened 0.35 μm CMOS process with a radiation tolerance of up to 300 krads(Si) and SEU-free cells up to 100 MeV, as well as latch-up immunity up to 100 MeV. It makes use of an extensive library of macro structures, including 95 logic cells, 216 I/O buffers, 11 specific cells (LVDS, PCI) and 9 SEU hardened cells. No Single Event Latch-up below a LET threshold of 80MeV/mg/cm^2 was observed.

The Atmel ATC18RHA is fabricated on a proprietary 0.18 μm CMOS process intended for use with a supply voltage of 1.8V. It contains a library of standard logic and I/O cells, Pads, memory cells, EDAC library, SEU hardened flip-flops. This library offers latch-up immunity and total dose capability better than 100 krads.

8.4.7 ATK 0.35 µm radiation hardened cell library

ATK Microelectronics Application Division has developed a 3.3 V radiation hardened library from the TSMC 0.35 µm standard cell library [93]. This library contains:

- 131 standard cells optimized for the radiation hardened logic synthesis utilizing various drive strength for most standard logic circuits
- 20 regular flip-flops and latched (non radhard)
- 18 regular scan chains (non radhard)
- 10 DICE flip-flops and latches (Dice flip-flops area is more than 3X standard the flip-flop area)
- 18 DICE scan chains and fail-safe chains
- 18 clock buffers and inverters
- 10 I/O pads

Radiation tolerance offered by this library is greater than 200 krads for TID and it is immune to SEL.

8.4.8 ST Microelectronics radiation hardened library

ST Microelectronics is currently developing a radiation hardened version of its 65 nm commercial library cells. Prototype chips are being evaluated [94]. Preliminary results of the evaluation of prototype chips show no current increase due to TID up to 100 krads(Si). Also, no SEL were observed up to 85 MeV.cm^2/mg (at maximum power supply, 125°C junction temperature). Finally, cross sections of 10^{-7} to 10^{-8} were obtained depending on the cells type and patterns.

9 Analogue circuits

9.1 Scope

In mixed-signal (analogue and digital) systems, the effect of a single particle strike is the generation of a transient signal (single-event transient or SET) that competes with the legitimate signals propagating through a circuit or perturbs the functionality of the circuit. In digital circuits, an SET can result in a single-event upset (SEU), that is, an alteration of the state of memory circuits (e.g., a memory cell can be changed from a logic "0" state to a logic "1" state). The SEU can lead to a circuit error if the corrupted data propagates throughout the circuit and is observable at the output. These upsets are often termed "soft errors" as they do not result in permanent failures within the circuit. However, there exists no standard metric for soft errors in analogue and mixed-signal circuits, as the effect of a single event is dependent on the circuit topology, type of circuit, and the operating mode. Moreover the hardening of such components is typically thought to require a "brute force" approach; that is, area and power are often sacrificed through the increase of capacitance, device size, and current drive in order to increase the critical charge required to generate SET, sometimes also called Analogue Single-Event Transients (ASETs).

Generally, ASET mitigation involves one or both of the following, irrespective of the technology:

- Increasing the critical charge (Q_{crit}) required to generate an ASET [95]
- Reducing the amount of collected charge (Q_{col}) at a metallurgical junction [95]

Reducing the amount of collected charge at a device junction can involve modifications of a design layout or the technology process. Some examples include:

- Use of layout alternatives such as guard rings[96][97], drains[98], or diodes[99] around MOS devices. Similarly, the use of n-rings[100], substrate-tap rings [101], and nested minority-carrier guard rings [102] may be utilized in bipolar structures such as in SiGe HBT technology [15]
- Substrate engineering (e.g., use of charge blocking layers in the substrate – shown in [103] for a SiGe HBT technology)
- Use of very thin epitaxial silicon layer (e.g., silicon-on-insulator (SOI)) [95]
- Addition of dummy collector for charge collection in HBT devices [104]
- Use of increased in substrate and well contacts (reduced substrate and well impedances) [105], [106][107].

Increasing the critical charge generally involves the implementation of design-level mitigation techniques through layout or circuit modifications. Conventional, perhaps "brute force" methodology for increasing Q_{crit} include:

- Increasing the transistor sizes (buffering) [108] [109]
- Increasing the drive currents [95]
- Increasing the supply voltage [95]
- Increasing capacitor sizes [95]

The remainder of this chapter outlines various design-level mitigation techniques employed through modifications in the layout, circuit, and/or system.

9.2 Table of effects vs mitigation techniques

Mitigation techniques		Abstraction level	Radiation effects		Page
			SET	SEU	
9.3.1	Node separation and Interdigitation	Design/Layout	X	X	
9.3.2	Analogue Redundancy	Design	X		
9.3.3	Resistive Decoupling	Design	X	X	
9.3.4	Filtering	Design	X	X	
9.3.5	Modifications in Bandwidth, Gain, Operating Speed, and Current Drive	Design	X		
9.3.6	Reduction of Window of Vulnerability	Design	X	X	
9.3.7	Reduction of High Impedance Nodes	Design/Layout	X		
9.3.8	Differential Design and Dual Path Hardening	Design/Layout	X	X	

9.3 Mitigation techniques

9.3.1 Node Separation and Interdigitation

Description of the concept/implementation

Decreased spacing of devices with technology scaling can increase the charge collection at nodes other than the primary struck node. This phenomenon has been termed "charge sharing" and is due to the diffusion of the carriers in the substrate/well. For older generation technologies (generally greater than 130 nm gate lengths), the distances between the hit and adjacent devices are large enough such that most of the charge can be collected at the hit node. However, for sub-100 nm gate length technologies, the close proximity of devices results in diffusion of charge to nodes other than the hit node. With the small amount of charge required to represent a logic-HIGH state (shown to be less than 1 fC in 45 nm SOI [110]), the charge collected due to diffusion at an adjacent node may be significant. Figure 9-1 illustrates a cross section of two adjacent NMOS devices in a bulk CMOS technology. The active node is referred to as the original 'hit' node whereas the passive node refers to any adjacent node that collects charge [111].

One solution for mitigating the amount of charge "shared" between adjacent nodes is nodal separation[111], [98], [104].

Interdigitation, or interleaved layout, is a technique that takes advantage of the benefits of nodal separation while maintaining device density requirements. Provided the designer has knowledge of the circuit nodes (or combinations of nodes) sensitive to SETs as well as those that pose less of a threat, the less sensitive transistors can be placed between pairs of sensitive devices. The nodal spacing between critical devices can be increased while maximizing density [104], [112].

Figures/diagrams

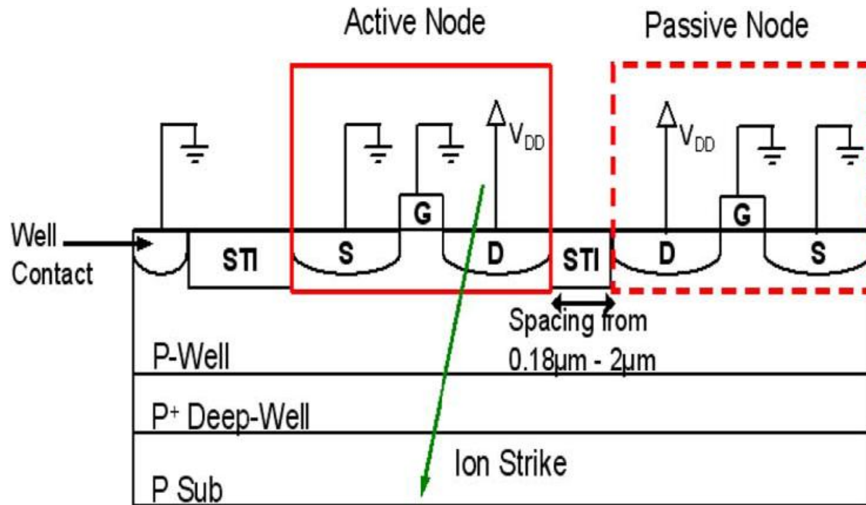


Figure 9-1: Cross section of two adjacent NMOS devices in a bulk CMOS technology (From [115])

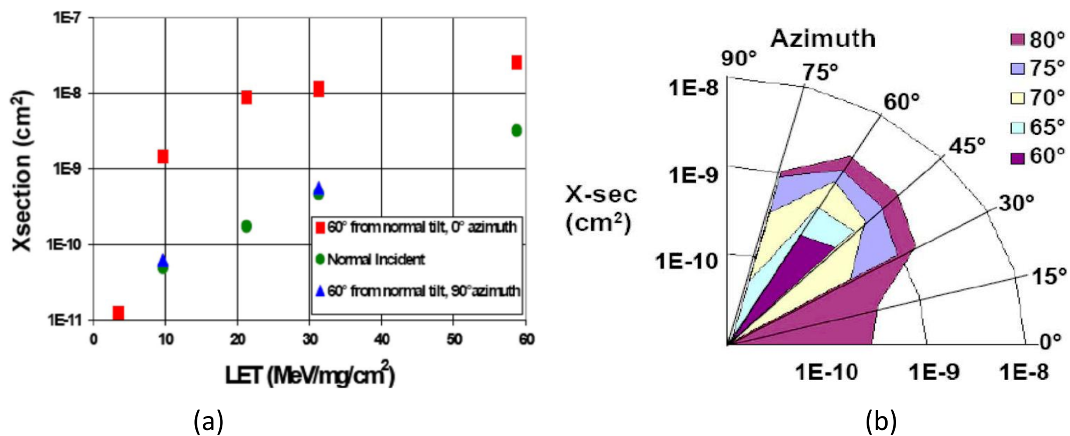


Figure 9-2 : (a) Upset sensitivity data for basic DICE topology implemented in 90 nm CMOS at three angles of incidence [116] and (b) measured upset cross-sections as a function of azimuth angle for the Kr ion (LET of approximately 30 MeV-cm²/mg) in improved DICE implementing nodal spacing [116]

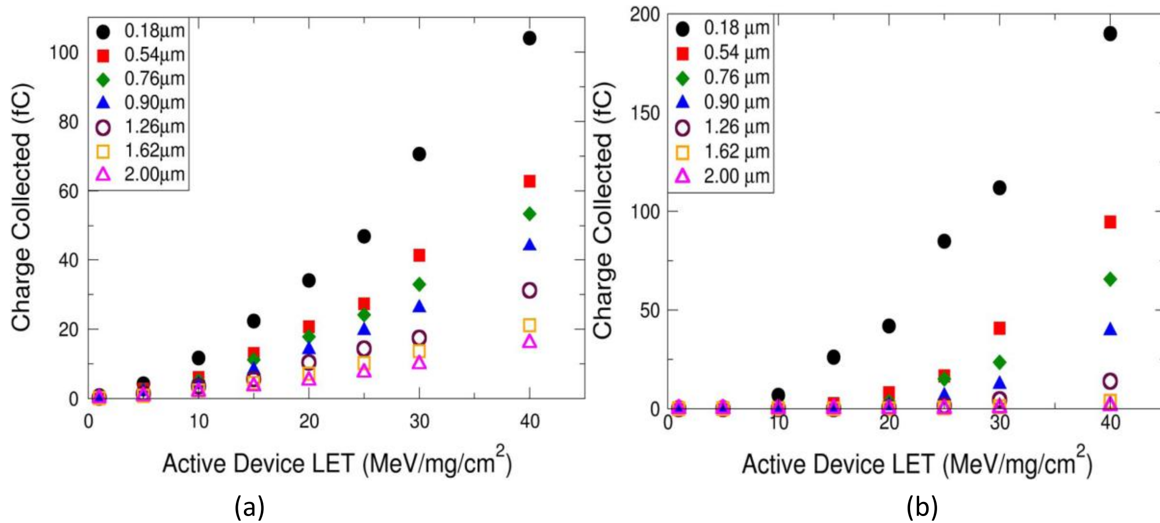


Figure 9-3 : Charge collected on an adjacent transistor for a) PMOS and b) transistors as a function of the distance separating them ([114])

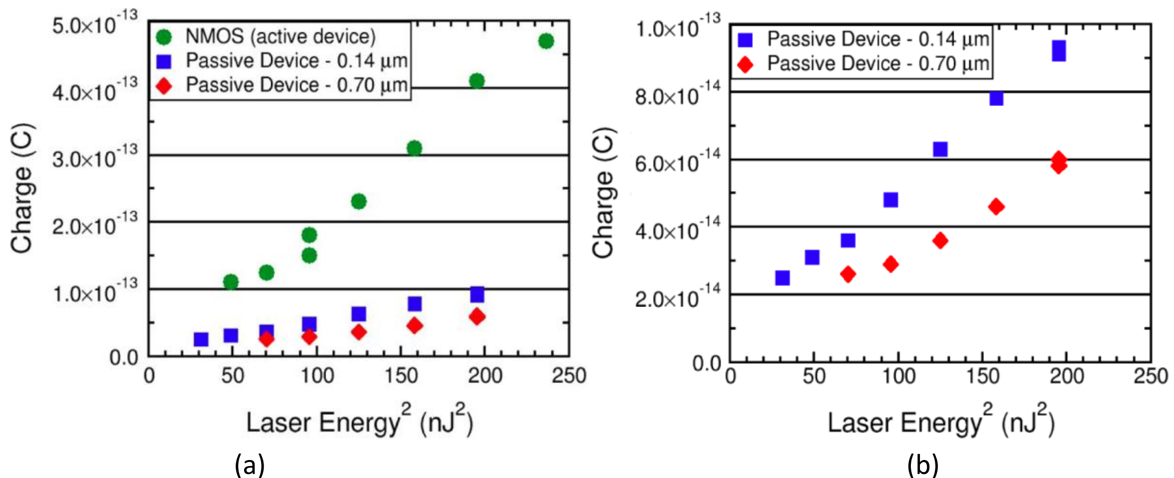


Figure 9-4: (a) Comparison of collected charge for the active and passive NMOS devices following laser-induced charge deposition at the active device. (b) Collected charge for passive NMOS devices verifies the charge sharing effect and shows a nodal spacing dependence for the passive device charge collection ([99])

Example(s)

The angular dependence of single event upset in dual-interlocked memory cells (DICE) has been rigorously investigated[112][113]. The DICE cell is immune to all single-node charge collection [114]. However, the charge-sharing phenomenon has been shown to decrease the DICE cell immunity to single events following the simultaneous collection of charge on multiple nodes within the cell. Figure 9-2(a) shows the upset cross-sections for one version of a DICE latch implemented in a 90 nm bulk CMOS technology [113]. The figure illustrates the strong directional dependence on the upset cross sections. Figure 9-2(b) illustrates the measured cross-sections at an LET of approximately 30 MeV-cm²/mg and at various azimuth angles for a modified version of the DICE latch designed with increased nodal spacing. For example, the cross-section for the design including increased nodal

spacing is reduced from 1e-8 cm^2 (red square at LET of 30 MeV-cm^2/mg in Figure 9-2(a)) to approximately 2e-10 cm^2 at an azimuth angle of 0° (Figure 9-2(b)).

Available Test Data (simulations, radiation testing, flown)

Figure 9-3 illustrates the simulated charge collected on the passive device versus the LET of the incident ion on the active device as a function of nodal separation in a 130 nm bulk CMOS technology ([111]). Both PMOS-to-PMOS and NMOS-to-NMOS charge sharing are illustrated and show a decrease in charge collection with increase in distance between devices.

Results from two-photon absorption laser experiments conducted at the Naval Research laboratory on devices fabricated in a 90 nm bulk CMOS technology are shown in Figure 9-4 ([97]). Following laser-induced charge deposition in the active device, the amount of charge collected on the active and adjacent (passive) device nodes were measured. There is an increase in active NMOS charge collection with increased laser energy. Further, as illustrated in Figure 9-4 (b) the passive NMOS device located 140 nm from the active NMOS device collects more charge than the passive NMOS device that is located at a greater distance (i.e., located 700 nm from the active NMOS device).

Added value (efficiency)

- Node separation reduces charge collection between adjacent transistors

Known issues (Weaknesses, elements to be considered)

- Nodal separation reduces packing densities, hence increasing the manufacturing costs
- Nodal separation also reduces IC speeds

IC family	Analogue and digital circuits
Abstraction level	Layout level
Pros	Reduces charge collection Reduces charge sharing
Cons	Reduces packing densities Increases manufacturing costs Reduces IC speeds Increases wiring complexity
Mitigated effects	SET, SEU
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.2 Analog Redundancy (Averaging)

Description of the concept/implementation

Analog averaging is a form of hardware redundancy for the reduction of spurious transients. The averaging of an analog voltage can be accomplished by replicating and parallelizing a circuit N times, and connecting the replicated nodes together through parallel resistors to a common node, as seen in Figure 9-5. A perturbation (ΔV) due to a particle strike on any one copy of the circuit is reduced to $\Delta V/N$.

Figures/diagrams

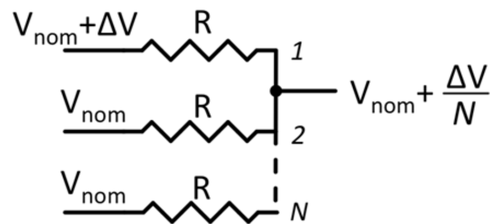


Figure 9-5: Analogue averaging through the use of *N* identical resistors. A perturbation (Δ*V*) due to a particle strike on any one copy of the circuit is reduced to Δ*V*/*N*

Example(s)

This technique has been offered as a solution to the observed vulnerability of a charge pump for Phase-Locked Loops (PLL) [115] and implemented in the bias circuitry of Voltage-Controlled Oscillator (VCO) [116].

In reference [107], a similar approach is proposed to harden the charge pump and VCO blocks of a PLL by including two independent Charge Pump/Low Pass Filter blocks controlling two cross-coupled VCO circuits.

Available Test Data (simulations, radiation testing, flown)

Simulation results issued from reference [116] show that analogue averaging applied on the input stage of a VCO reduces the phase displacement in the output of the VCO by 35%.

Added value (efficiency)

- Predictable decrease in SET magnitude as a function of redundancy

Known issues (Weaknesses, elements to be considered)

- Mismatch between redundant analog blocks can create unwanted noise at the output
- Added thermal noise due to the resistors
- Area increase with each redundant circuit block

IC family	Analogue circuits
Abstraction level	Design level
Pros	Attenuation of SETs
Cons	*Noise and area increase*
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.3 Resistive Decoupling

Description of the concept/implementation

Resistive decoupling was first published in 1982 as a technique for hardening memory cells by introducing series resistors in the cross-coupling lines (see section 13.1) of the inverter pairs [117], [118]. The resistors effectively increase the time constant seen by the two storage nodes and limit the maximum change in voltage during a single-event, thus increasing the minimum charge required to change the state of the memory.

This technique is also used in analogue and mixed-signal circuits for hardening digital latches, such as those present at the output of voltage comparators in an ADC[119]. A similar technique may be used to filter high-frequency transients by decoupling nodes sensitive to ASETs and introducing a time constant through a series resistor or low-pass filter.

Figures/diagrams

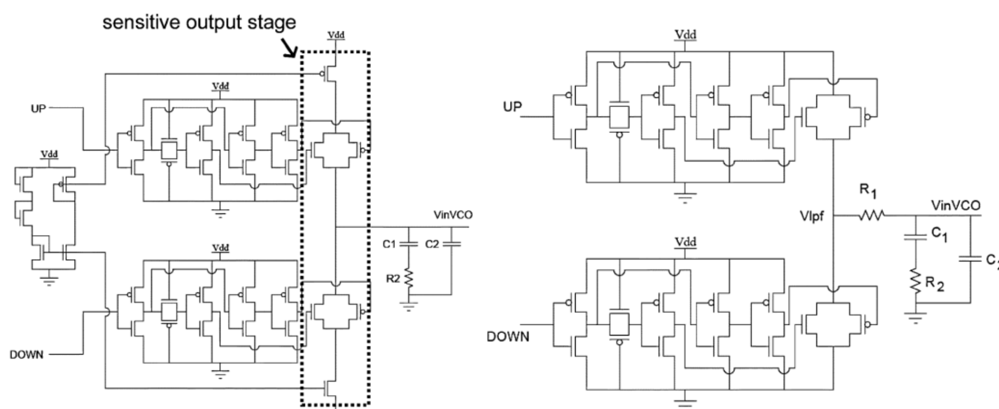


Figure 9-6: (a) A standard current-based charge pump configuration for phase-locked loop circuits. (b) Single-event hardened voltage-based charge pump configuration.

(a) (b)

Figure 9-7: (a) A standard LC Tank Voltage-Controlled Oscillator (VCO) and (b) Single-event hardened configuration utilizing decoupling resistor R_3 (From [120]).

Example(s)

Resistive decoupling was implemented in several studies such as the one presented in references[121] and [122] where the high-impedance output of a charge pump circuit was decoupled from the capacitive input to a voltage-controlled oscillator. As seen in Figure 9-6, the number of sensitive nodes present in the output stage of the charge pump (Figure 9-6(a)) may be reduced and subsequently decoupled from the VCO control voltage (Figure 9-6Figure 9-6(b)).

The technique has also been used to mitigate transients in an LC Tank Oscillator [120]. Figure 9-7(a) displays a standard LC Tank Oscillator created through a cross-coupled differential amplifier and an RLC "tank" load. Transients resulting from strikes to the bias circuit were mitigated by decoupling the bias circuit and tail current source from the differential pair through the insertion of a resistor R3, as shown in Figure 9-7(b). The resistor introduces a delay between the bias circuit and the differential oscillator and consumes a portion of the voltage caused by the single event [120]. Vulnerabilities of the differential pair are discussed in further detail in section 9.3.7.

Available Test Data (simulations, radiation testing, flown)

- Reference [121] presents simulation results on a phase-locked loop designed in a 130 nm process with particle strikes represented by the double-exponential current pulse model for charges up to 500 fC. Obtained results show that the hardened Voltage-switching Charging Pump (V-CP) reduces the voltage perturbation on the input of the voltage-controlled oscillator (VCO). As a result, the amount of phase displacement in the output of the Digital-PLL is reduced by approximately 2 orders of magnitude, thus reducing the number of erroneous pulses below those resulting from strikes in the VCO. With this circuit topology, the Charge Pump module of the Digital-PLL can be eliminated as the most sensitive module within the Digital-PLL.
- Reference [122] presents experimental results issued from radiation experiments performed on two Phase-Locked Loop (PLL) circuits designed a 130 nm process. The first PLL implements a

conventional current-based charge pump technique, the second utilizes a RHBD voltage-based charge pump for improved performance with respect to single events. Results from a through-wafer Two-Photon Absorption (TPA) technique show 2.3 orders of magnitude improvement in the number of erroneous pulses present in the output of the PLL following an SET occurrence in the hardened design. TPA-induced SEU maps indicate that implementing the RHBD voltage-based charge pump over the conventional current-based module reduces the vulnerable area of the charge pump module by approximately 99%. The proposed hardening technique effectively reduces the sensitivity of the charge pump sub-circuit below the upset level of the voltage-controlled oscillator.

- Reference[120] presents simulation and experimental transient results for the standard and hardened LC Tank Oscillators shown in Figure 9-7 and designed in a 90 nm CMOS technology. The threshold energy of the hardened oscillator, defined as the minimum laser energy required to induce a phase shift of at least 10 degrees in the oscillator output, was shown to be approximately 5 times that of the unhardened design.

Added value (efficiency)

- The inclusion of the decoupling resistor has the added benefit of RC filtering (see 9.3.4) with minor topological changes.
- Generally, there is little to no change in overall power consumption following resistive decoupling. For example, the observed power consumption for the standard charge pump and the Voltage-based Charge Pump was approximately equivalent.

Known issues (Weaknesses, elements to be considered)

Some area penalty will be incurred with resistive decoupling. Area penalty can be minimized by implementing minimum width p+ doped poly resistors, hence having a non-significant impact on the overall area. However, a minimum width resistor does result in maximum fluctuation of the final resistance value due to process variation. Care should be taken to determine the circuits vulnerability to process variability. Since simulations showed a minimal impact on overall DPLL performance due to resistor value fluctuations, this was not a concern in [121]. However, if the designer wishes to further decrease this fluctuation, an area tradeoff will be encountered.

IC family	Analogue circuits
Abstraction level	Design level
Pros	Negligible power consumption penalty
Cons	Area penalty: from negligible to noticeable (depending on resistor size requested by the designer)
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.4 Filtering

Description of the concept/implementation

Filtering is a common method for reducing the amplitude and duration of ASETs at design and system-levels. Low-pass or bandpass filter's may be added to critical nodes in order to suppress fast ASETs, where the value of the filter depends on the circuit or system bandwidth [123].

Figures/diagrams

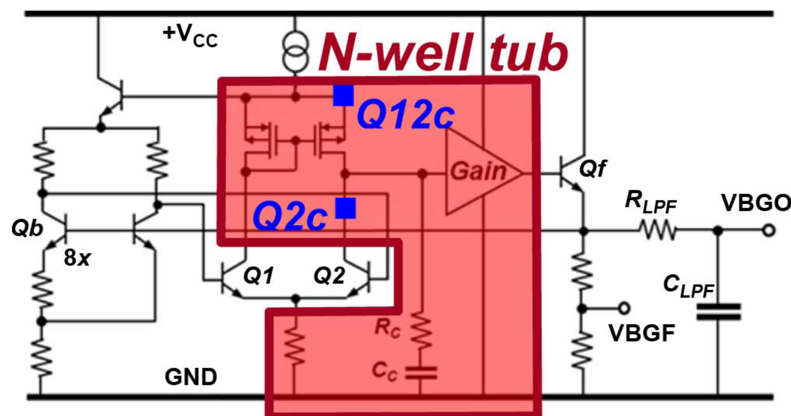


Figure 9-8: Brokaw bandgap reference circuit with an output low-pass filter for improved noise, isolation, and transient suppression (From [130]).

Example(s)

Reference [124] presents a computer-assisted system-level analysis to study the ASET response on an analog power distribution network. Slight modifications to the op-amp passive component networks (i.e., adjustments to the bandwidth) can reduce both the amplitude and duration of ASETs with no modification to steady-state bias conditions.

Figure 9-8 illustrates the bandgap reference circuit ([125]), implemented in triple-well CMOS, which utilizes an output low-pass filter for transient suppression. Interestingly, there is a trade-off in the value of the filter resistance versus the capacitance, indicating that for a desired RC time constant it is preferential to increase the resistance and decrease the capacitance so as to decrease any direct charge coupling to the output node. A similar phenomenon is observed in [121] and [95].

Available Test Data (simulations, radiation testing, flown)

Simulation and experimental results presented in reference[124] lead to the following conclusions:

- Computer simulations fit the experimental results and are thus valuable in the development of hardening methodologies against ASETs in space systems.
- ASET's amplitude and pulse width were reduced by modifications off some parameters on op-amp without perturbing the steady-state bias conditions.
- Performed modifications reduced both ASET's pulse amplitude and pulse duration by a factor of about 2.

Added value (efficiency)

Filtering approach has shown effective in:

- Suppressing high frequency noise and ASETs generated from the charge pump sub-component of a PLL [121], [122].
- Hardening the bias nodes of a SerDes [126].
- The use of Low Pass Filters for the mitigation of SETs in advanced CMOS memory circuits is also shown feasible for suppressing transients ≤ 50 ps.
-

Known issues (Weaknesses, elements to be considered)

The work presented in reference [124] show a significant power consumption increase depending on the applied modifications. As an example, the authors mention a case where a resistor's value of 1 kohms in the original design is reduced to 100 ohms. As a result the power consumption went from 213 mW to 384 mW.

IC family	Analogue circuits
Abstraction level	Design level
Pros	SET filtering
Cons	Power consumption penalty Area penalty
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.5 Modifications in Bandwidth, Gain, Operating Speed, and Current Drive

Description of the concept/implementation

Increasing the capacitance at nodes vulnerable to single-events can reduce the amplitudes of the resulting ASETs by increasing the amount of required charge to induce a voltage perturbation. This is often used when the performance specifications are not adversely affected[124],[127]. The increase of nodal capacitance often alters characteristic parameters such as gain and bandwidth. This section will discuss mitigation techniques when such characteristics are paramount.

One effective way to reduce the circuit's sensitivity to ASETs is to reduce the part's bandwidth, thereby suppressing all transients outside of the frequency band. This concept can be thought generally applicable to analog topologies that can be expressed as closed-loop amplifier structures and has been shown applicable in various studies on Operational Amplifiers (OAs) ([95], [123], [127]) and Phase-Locked Loops (PLLs) ([128], [129]) both of which can be represented as a closed-loop amplifier. However, works presented in references [122] and [127] also discuss the importance of examining the severity of an ASET as defined by the application for which it is a part. For example, the threshold for

an application is typically defined by both ASET amplitude and duration. Sternberg et al. have pointed out that, depending on the origin of the ASET, the duration of the pulse may increase as modifications are placed to decrease the amplitude. Therefore, specific consequences regarding the size of the resistors, compensation capacitors, and stage gains may occur and require special attention. In general, as seen in reference[129] and [127] regarding respectively PLLs and OAs, it appears that maximizing speed and minimizing the open- and closed-loop gains may improve the ASET response.

Operating speed plays a curious role in determining the SET response of analog circuits. As previously mentioned, analog circuits have been shown to exhibit reduced ASET vulnerability for increased operating frequency [127], [129]. This is contrary to that typically observed in digital systems, where increasing error cross-sections as a result of SETs induced in combinational logic have been observed for increasing operating frequency [130]. In digital circuits, an SET can result in an SEU and lead to a circuit error if the corrupted data propagates throughout the circuit and is observable at the output. The ability of the SEU to reach the circuit output depends on the logical and electrical masking as well as the window of vulnerability (latch window masking). The result of latch window masking is that for equivalent SET pulse widths, faster circuits have a higher probability of being latched into memory. In analog electronics, however, increased speed is often accompanied by increased drive current and an improved ability to dissipate the deposited energy, making the circuit less vulnerable. It is thus important to attribute the improvement to either speed or drive strength, as increased bias current is a well-known technique and is often used in A/MS circuits for improved SET performance [124]. The improved performance may or may not be as a result of increased speed, but rather subtle changes in the individual device operating conditions such as bias, current drive, and load.

Reference [129] discusses a more complex example of the importance of device conditions (not just speed) in regard to SET mitigation of mixed-signal PLL circuits. For a particular oscillator design, for example, it is shown that the operating frequency should be maximized within the designed bandwidth (consistent with that shown in [127] for OAs). However, the improved SET performance is fundamentally a result of the subsequent increases in drive strength. On the other hand, the natural frequency of the PLL (analogous to the response time of the closed-loop PLL and not to be confused with the output frequency) is found to amplify transients in the PLL resulting from ionizing radiation and thus should be reduced to improve the SET response of the PLL. The authors go on to provide an analytical expression for determining an upper bound for reasonable radiation performance. Moreover, it is shown in [128] that the error response to transient perturbations in the PLL increases for increasing bandwidth, further indicating the importance of bandwidth in determining the SET response of the topology. Figure 9-9 illustrates the simulated error response (in units of radians) of the PLL versus time for various PLL bandwidths. Increasing the PLL bandwidth is often accompanied by decreases in lock time (improved speed) and increased jitter (can be considered as noise for practical purposes). Trade-offs in operating speed, jitter, settling time, bandwidth, and SET performance should be carefully considered.

Through the efforts depicted in reference [131] in understanding the effects of scaling on the SET sensitivity of high-speed RF circuits, it is shown that the SET performance is not merely set by the bandwidth, but the gain-bandwidth product. For a given bandwidth, large gains result in degraded SET performance. Additionally, for the VCO circuits described, the optimum operating ranges are technology specific; the topologies discussed perform worse than a circuit in the same technology but with a smaller gain-bandwidth product, or worse than a circuit in an older technology at comparable speeds. More importantly, de-rating the frequency in a state-of-the-art technology node does not compensate for the increases radiation vulnerabilities at that node.

Figures/diagrams

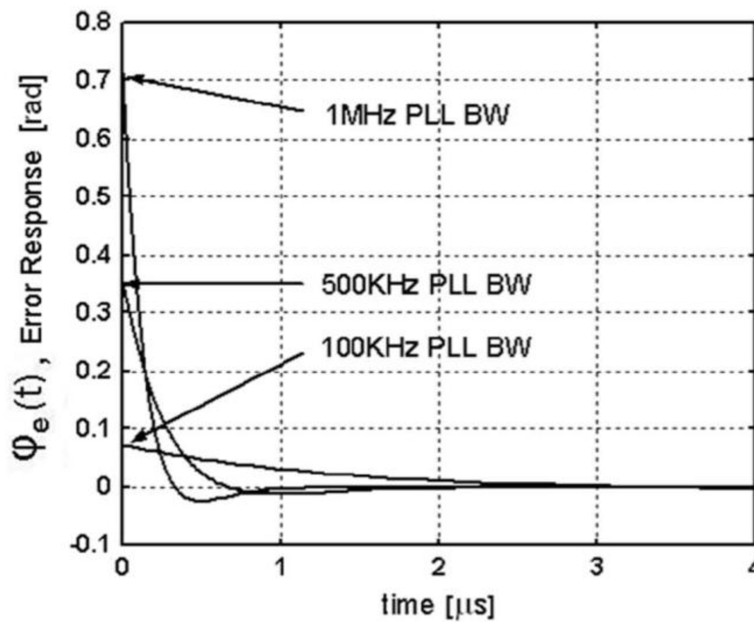


Figure 9-9: Transient PLL error response as a function of PLL bandwidth

Example(s)

Reference [129] puts in evidence that the SET response of a LM124 operational amplifier in an inverting configuration depends on the bandwidth of the amplifier, the gain and the value of the resistors used to program the gain.

Available Test Data (simulations, radiation testing, flown)

Simulation and experimental results using a laser beam on a LM124 OA are presented in reference [129]. SETs in the different stages of the LM124 produce considerably different output transients. They have different pulse shapes, amplitudes, and duration. They also respond differently to changes in the amplifier parameters. Much of this can be explained in terms of the frequency response of the amplifier and the filtering action of the remaining signal path.

Internal parameters of the operational amplifier that are not normally accessible to experimenters were, such as the compensation capacitor, were changed. This has shown that changing the value of the compensation capacitor modifies the high-frequency response of the amplifier, affecting the response of the circuit to heavy ions in different stages of the amplifier.

In the LM124, sensitivity in the input stage increases as the gain increases. An increase in the compensation capacitance will reduce the amplitude but increase the duration. Therefore, the sensitivity may increase or decrease depending on the criteria defined for the application. The gain stage will increase in sensitivity for an increase in both gain and compensation capacitance. The output stage is negligibly affected by changes in the gain or compensation.

As shown in the gain stage, the SET response of the LM124 is also dependent on the values of the resistors used to set the closed-loop gain of the amplifier. Therefore, values of these resistors may be selected which will minimize SET response for a given application without affecting the overall performance. This presents an important opportunity to improve the SET response by making small changes in the circuit design.

Overall, it appears that a faster operational amplifier with a smaller gain will have a better SET response than a slower operational amplifier running at a high gain. It also seems to be best to use the smallest practical values to set the closed-loop gain of the amplifier.

Added value (efficiency)

Observations from [127]-[131] lead to the following general conclusions:

- Reducing bandwidth is desirable when possible to increase the suppression of transients outside of the frequency band
- Minimizing the open- and closed-loop gains may improve the ASET response
- Operating speed and drive strength are closely coupled. Operating circuits faster may in some cases reduce the SET vulnerability due to increased operating currents

Known issues (Weaknesses, elements to be considered)

- It is often difficult to decouple the effects of speed and drive strength on the SET vulnerability
- Rigorous analysis is required to maximize benefits

IC family	Analog circuits
Abstraction level	Design level
Pros	Improved SET tolerance
Cons	Gain, bandwidth, speed, and drive strength are often dependent parameters and may be difficult to decouple
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.6 Reduction of Window of Vulnerability

Description of the concept/implementation

The window of vulnerability (WOV) is a well-known concept in the digital design community and describes the amount of time during a clock cycle a circuit is vulnerable to SEU. Generally, reducing the window of vulnerability improves the SEU performance by reducing the amount of time that a single event transient can result in a single event upset.

The window of vulnerability concept can be applied to analog/mixed-signal (A/MS) circuits when signal clocking is required or in cases where steady-state AC signals are present. Figure 9-10 illustrates the number of vulnerable nodes and the type of vulnerable sub-circuit in a 2-bit flash analog-to-digital converter (ADC) over one conversion cycle (from [132]). The results indicate 9 distinct windows of vulnerability during a single data conversion cycle. The plot demonstrates the

dynamic sensitivity and highlights the specific components vulnerable to single events. Similarly, Figure 9-11 illustrates the number of errors following laser-induced charge deposition in a phase-locked loop circuit (closed-loop oscillator) versus the oscillator cycle time (termed phase-dependent sensitivity or PDS). The results indicate vulnerability during each transition period (From [133]).

Figures/diagrams

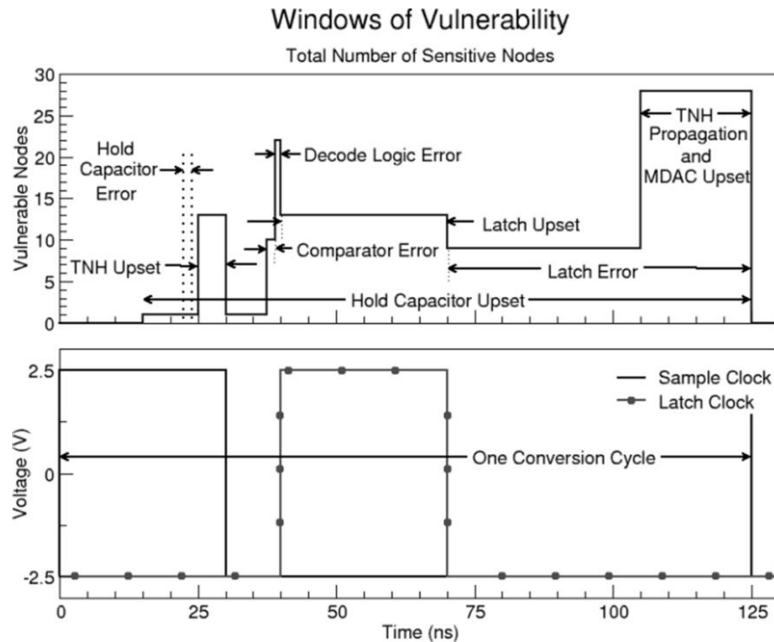


Figure 9-10: Simulated windows of vulnerability over one data conversion cycle in a 2-bit flash ADC (From [132]).

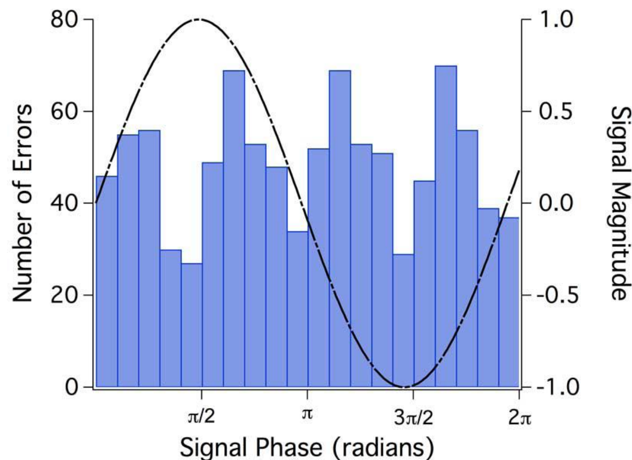


Figure 9-11: The number of errors with respect to cycle time following laser-induced charge deposition in a phase-locked loop (From [133]).

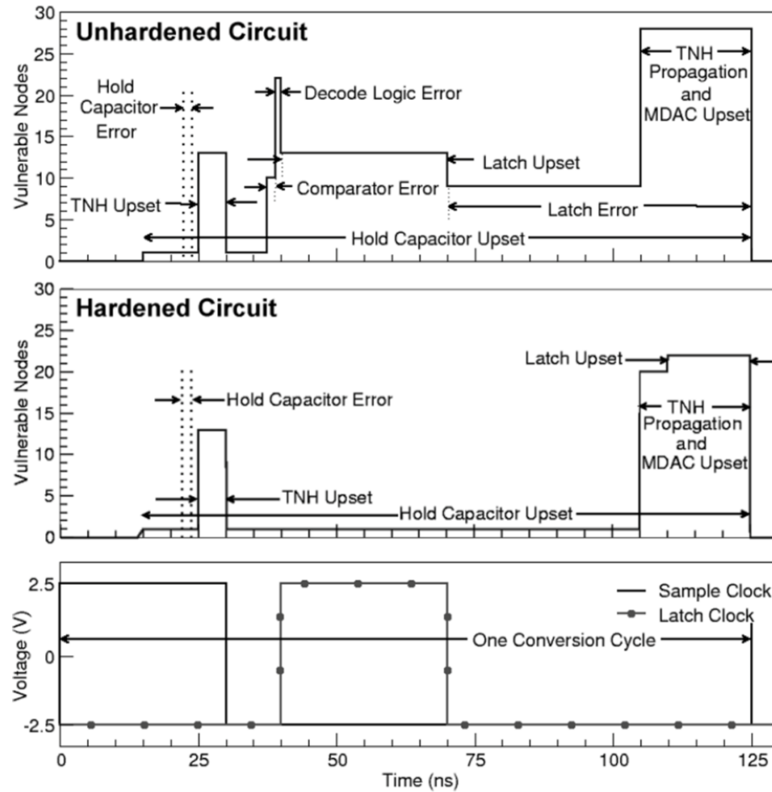


Figure 9-12: Simulated windows of vulnerability over one data conversion cycle for un-hardend and hardened 2-bit flash ADCs (From [132])

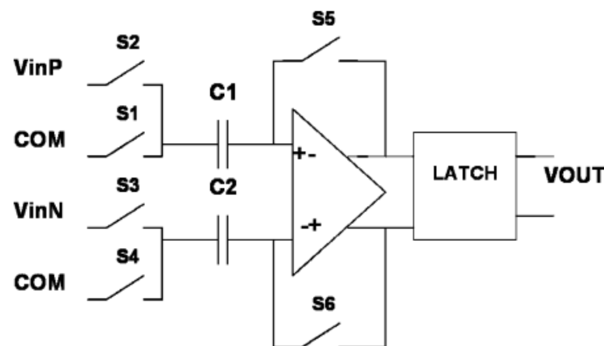


Figure 9-13: Simplified view of the auto-zeroed comparator (From [134])

Example(s)

The results from Figure 9-10 were utilized to apply targeted mitigation techniques to the vulnerable sub-circuits in the 2-bit flash ADC in [132]. The mitigation was achieved by implementing hardened latches and SET filtering. No analog components were hardened. The results from the hardening are displayed in Figure 9-12 and show that all errors in the comparators, digital logic, and latches were eliminated.

This concept is also applied to A/MS designs through the implementation of an auto-zeroed CMOS comparator. Figure 9-13 illustrates the auto-zeroed comparator presented in reference [134]. By sampling and resetting the initial state of the comparator each clock cycle, SET pulse widths are

limited to the length of a single clock period. For example, following a single event strike in the input stage, the transient output error will be corrected during the next auto-zero phase, since the two MOS transistors are biased as diodes during this period. Also, upsets in the output latch will be restored during the next phase of the master clock. In any case, the output is only incorrect for the duration of a single clock cycle [134].

Available Test Data (simulations, radiation testing, flown)

The window of vulnerability of a 2-bit flash ADC was investigated through simulations in [134]. Simulation analyses allows for identification of specific components and the contributions to the overall vulnerability of the circuit. The approach led to the development of a hardened topology by mitigating SET and SEU in all digital blocks.

The phase dependent sensitivity of phase-locked loop and serializer-deserializer (SerDes) circuits was determined experimentally in [133]. This type of analysis allows for a quantification of the vulnerable time during data cycles, which can lead to error rate estimations. Provided that the designer has knowledge of the circuit functionality, the analysis may help identify the mechanisms responsible for the vulnerability.

The WOV concept was applied to harden a comparator in [134]. SET simulations were conducted on the auto-zeroed design and on a folded-cascode comparator for comparison purposes. The comparators are biased so that the output should remain at the positive supply rail, however an SET strike causes the comparators to switch to an incorrect state for a certain amount of time depending on the design. Results show that:

- The folded-cascode switches to an incorrect state for a duration depending on the node impacted by the event. The shortest output transient is 2 ns while the longest is 28 ns.
- The auto-zeroed comparator switched to an incorrect state for a fixed duration of time established by the duration of one clock cycle. On the following clock cycle the output is restored to the correct value.

Added value (efficiency)

- Window of vulnerability (WOV) and phase dependent sensitivity (PDS) analysis highlights specific temporal susceptibilities and can indicate critical sub-circuits in determining the single event vulnerability
- WOV and PDS analysis can be performed asynchronously using a pulsed laser for interrogation of the single event vulnerability [133]

Known issues (Weaknesses, elements to be considered)

- WOV and PDS analysis, while they elucidate information in regard to the circuit vulnerability, they do not directly result in an identification of vulnerable locale. Additional analysis is required in order to determine appropriate mitigation techniques.
- Specific to the comparator study, the area of the auto-zero comparator is quite small (smaller than the folded cascode). However, it does require overhead: a clock and clock generation circuitry (to generate the different phases that are necessary). Also, The auto-zeroed operational amplifier and comparator samples the signal because of its output latch, which is not always possible is some designs (e. g. an operational amplifier in an analog filter or a comparator in an asynchronous circuit).

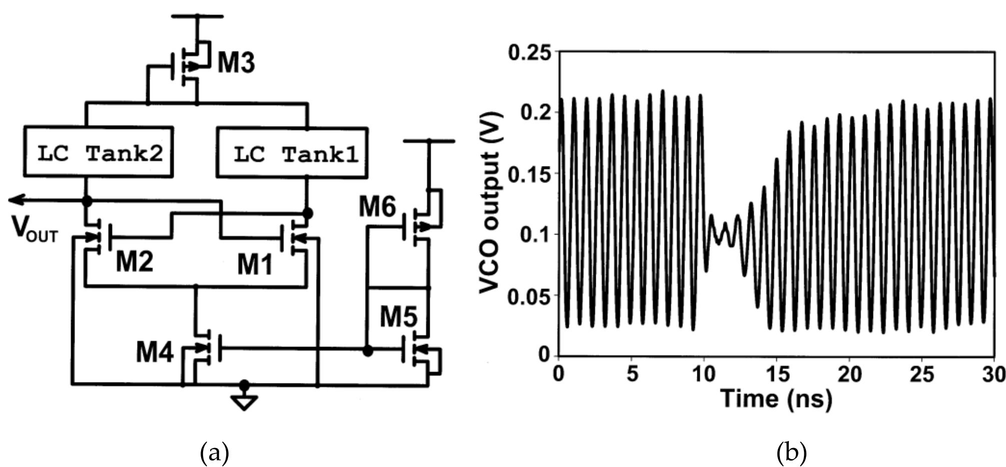
IC family	Analog circuits
Abstraction level	Design level
Pros	Reduces SET duration
Cons	Area penalty: clocking circuitry
Mitigated effects	SET
Suitable Validation methods	Simulations Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.7 Reduction of High Impedance Nodes

Description of the concept/implementation

The aforementioned circuit-level mitigation approaches are based on the modification of characteristic circuit parameters such as gain, bandwidth, frequency, and drive strength. Each technique, though effective, may require special attention in compromising performance tradeoffs (most A/MS circuits already have stringent design requirements with little room for modification). One technique for reducing the nodal sensitivity of A/MS circuits is to reduce or eliminate high impedance nodes, thus improving the recovery time of the circuit following the ion strike[135], [99], [121], [122], [136]. This has shown applicable at the design-level [121], [122], [136] and at layout-level [99].

Figures/diagrams



(a) (b)

Figure 9-14: (a) Simplified schematic of a typical LC Tank VCO and (b) an experimentally observed transient resulting from laser-induced charge injection on transistor M1 (From [137])

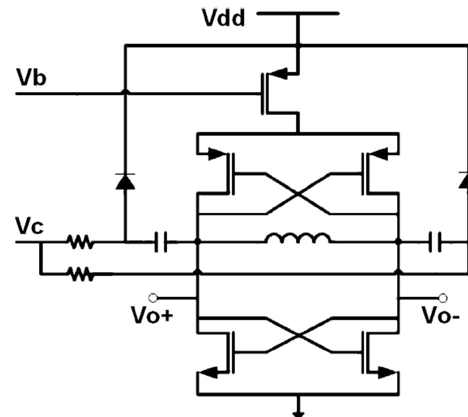


Figure 9-15: Schematic of RHBD CMOS LC Tank VCO (From [136])

Example(s)

- Figure 9-14 shows the schematic of a typical CMOS LC Tank Voltage-Controlled Oscillator (VCO) VCO and an experimentally observed transient resulting from laser-induced charge injection on transistor M1 (From[137]). The design includes a cross-coupled differential amplifier loaded by an LC "tank" circuit typical of a voltage-controlled Colpitts oscillator. Chen et. al shows that the high-impedance outputs (drains of M1 and M2) present significant single event vulnerabilities. The VCO was subsequently hardened, as seen in Figure 9-15 (From [136]), through the addition of a PMOS cross-coupled switching pair at the oscillator output, thus reducing the output impedance, as well as decoupling the tail current source [136].

- Reference [138] describes how a similar approach was implemented in an Injection-Locked Oscillator (ILO) designed using a SiGe BiCMOS process. First, a PMOS cross-coupled pair is utilized to increase the transconductance. Further, the length of ASETs is shown to decrease when operating in the injection locked mode. In general, free running oscillators tend to exhibit poor SET performance when compared to synchronized oscillators such as the injection locked oscillator and VCO implemented in a PLL[138], [139], [116], [115], [122].

- In contrast, reference [99] describes a technique for creating a low impedance path within a SiGe Heterojunction Bipolar Transistor (HBT) device, designed to shunt charge away from the collector terminal. The path is realized by including an additional reverse biased PN junction formed between the p-substrate and guard ring (n-ring) resulting in a secondary electric field.

Available Test Data (simulations, radiation testing, flown)

- The efficiency of the implemented mitigation technique was tested using a laser with 1 ps pulses, a laser wavelength of 800 nm, and a spot diameter of 1.1 μm [136]. The VCO's output was observed using an oscilloscope while the PMOS pair was hit by an incident energy per pulse of 216 pJ (equivalent LET of around 100 MeV·cm²/mg) at 400 Hz. As a result, the laser pulse causes the oscillating output to be distorted for a few nanoseconds. Furthermore, a spectrum analyzer proved that no change in the spectrum were observed, hence proving that an SET has a low impact on the VCO circuit. The LNA was tested for a laser pulse set to 223 pJ at a laser frequency of 100 kHz. Once again no change was recorded in the output spectrum. This is mainly due to the fact that the LNA's frequency is forced by the input frequency. Consequently, a single event strike does not cause any significant non-linearity in the LNA, so the shape of the spectrum is intact.

- The 5.2 GHz Injection-Locked Oscillator [138] implemented in a 0.25 μm SiGe technology was tested experimentally using a laser beam. The circuit was found to be intrinsically radiation-hardened due to its principle of operation.
-

Added value (efficiency)

- The reduction of high impedance nodes is shown to improve the recovery time following the ion strike

Known issues (Weaknesses, elements to be considered)

– Reducing or eliminating high impedance nodes may require additional circuit elements and is thus subject to area and power penalties

IC family	Analog circuits
Abstraction level	Design level / Layout level
Pros	Improved SET recovery time
Cons	Requires additional circuit elements: area and power penalty
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.8 Differential Design

Description of the concept/implementation

As multiple node charge collection, or charge sharing, is becoming more commonplace, methods for utilizing charge sharing for improved SET performance become promising. For technologies where the time constant for device-to-device charge transport is on the order of the gate-to-gate electrical propagation, the layout orientation, device spacing, and electrical signal propagation may be designed to interact as to truncate a propagated voltage transient (pulse quenching)[140]. Pulse quenching, graphically illustrated in Figure 9-16 (From [140]) has been identified as a factor in the analysis and measurement of digital SETs, and may be a reasonable technique to harness for improved radiation performance in A/MS circuits.

Differential circuits, standard in high-performance analogue design due to their improved dynamic output range and better noise rejection over their single-ended counterparts, make possible additional mitigation techniques not possible in single-ended designs. Figure 9-17 depicts a basic differential pair often used as an input to an integrated amplifier. Two transistors are connected such that any differential voltage applied to the inputs is amplified and any common voltage applied to the inputs is rejected. Differential circuits are widespread in analogue design because of this rejection of common mode noise. A single-event, however, occurring in circuitry feeding one of the input gates of the

differential pair (or one of the devices in the differential pair), can perturb the voltage at the input. This voltage perturbation, not being common to both inputs, will result in a transient in the output voltage.

Hypothesized in [102] and shown for the first time through simulations in [141] and experiments in [142], layout of matched transistors in a differential data path can be placed in order to exploit the charge-sharing phenomenon, therefore rejecting any common-mode perturbation. The layout technique, termed Differential Charge Cancellation (DCC) Layout, minimizes the distance between the drains of matched devices in the differential pair and maximizes the likelihood of an ion strike affecting both sides of the differential pair through a configuration similar to common-centroid layout (drain-to-drain distance is not specifically minimized in standard common-centroid configurations).

Figures/diagrams

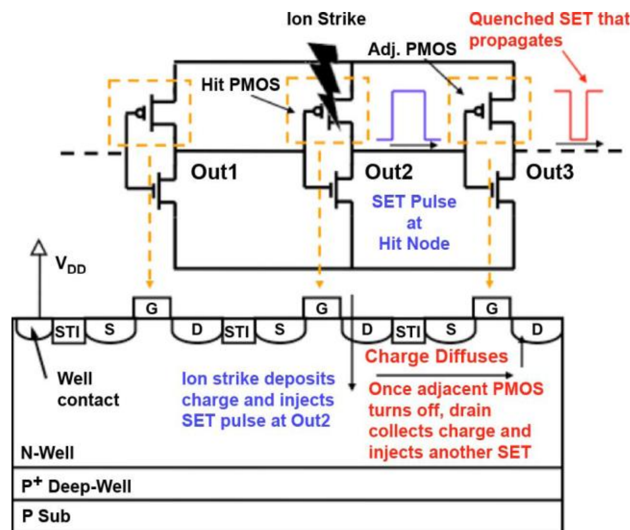


Figure 9-16: Two-dimensional slice of three PMOS transistors depicting the electrical signal and the charge-sharing signal caused by an ion strike, i.e. pulse quenching (From [144]).

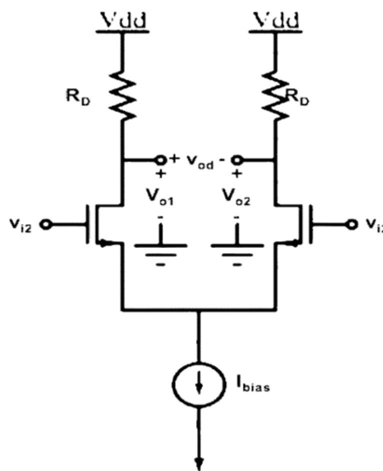


Figure 9-17: Basic differential pair

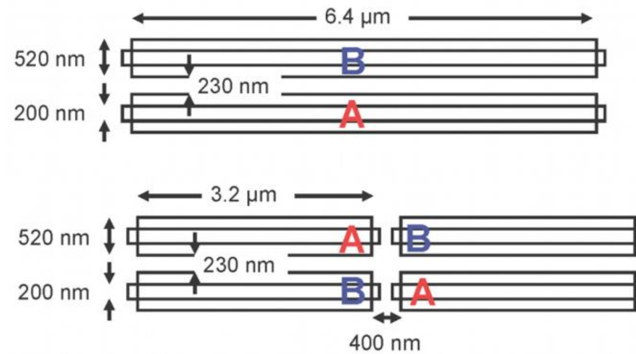


Figure 9-18: Differential pair including devices A and B before and after DCC layout for maximizing charge sharing (From [145]).

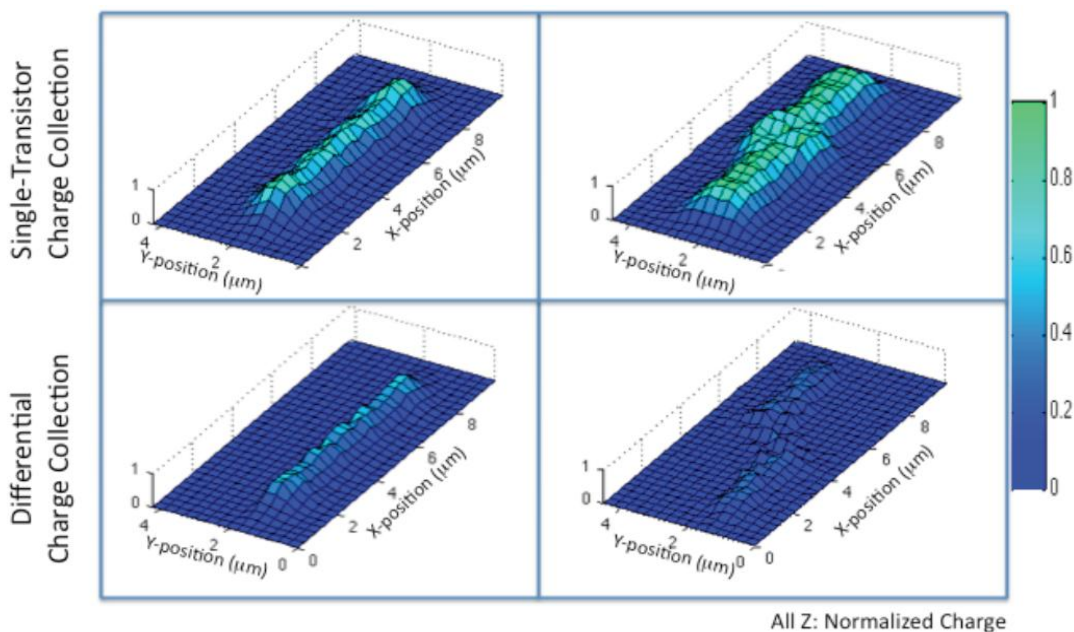


Figure 9-19: Charge collected by a single transistor for single (left) and parallel (right) transistor configuration, is shown in the top row. Differential charge is shown in the bottom row for single (left) and parallel (right) transistor configuration (From [145]).

Example(s)

Figure 9-18 illustrates two layout variations of the differential pair, including devices A and B before and after DCC layout for maximizing charge sharing. Each transistor in the DCC is split into two devices and placed diagonally. The device pairs should be arranged in a common well with drains located as close as possible to promote common-mode charge rejection. Figure 9-19 shows surface plots of experimentally measured charge collected at points in the die scan for transistor A of the differential pair (device dimensions illustrated in Figure 9-18). Charge was injected using a laser two-photon absorption technique. Single-transistor charge collection is shown in the top row for the two-

device configuration (left) and DCC layout (right). Differential charge is shown in the bottom row (From [142]).

Available Test Data (simulations, radiation testing, flown)

Reference [142] provides experimental results for a simple amplifier circuit. The peak voltage excursions from the expected value of the output in the proposed charge-sharing layout are improved by 40-60% over the non-charge-sharing scenario.

The results from this study indicate that a practice of DCC layout with close drain proximity for sister transistors along the differential signal path will greatly reduce the sensitive area of the circuit. Furthermore, a matched layout is also beneficial even when a common-centroid layout approach is not an option. The penalty in both cases is additional wiring overhead and additional capacitance in the cases where common-centroid layout would not normally be employed, but the overall charge sharing, and therefore single-event mitigation, is dramatically enhanced.

Added value (efficiency)

- Reduces charge sharing with nodal separation
- Maintains integration density
- NMOS sensitive area reduced by at least 50% over the baseline case of no charge sharing

Known issues (Weaknesses, elements to be considered)

– Increased wiring complexity

IC family	Analogue-circuits
Abstraction level	Design and IC layout levels
Pros	Maximizes charge sharing for improved common-mode rejection No integration density penalty
Cons	Increases wiring complexity
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

9.3.9 Dual Path Hardening

Description of the concept/implementation

Differential circuits are common for most analog applications as they offer greater dynamic output range and better noise rejection than their single-ended counterparts. One RHBD approach that can

significantly reduce the SET vulnerability of differential switched-capacitor circuits commonly used in high-performance analog and mixed-signal circuits is dual path hardening (local feedback mitigation) [143]. The principle of the technique is to create a dual signal path that provides significant immunity to a voltage perturbation on a single floating node of a switched-capacitor feedback circuit by splitting the input nodes into separate parallel signal paths. This technique is applicable to all differential switched capacitor circuits and has been applied to OAs and comparators in [143] and [144], respectively.

Figures/diagrams

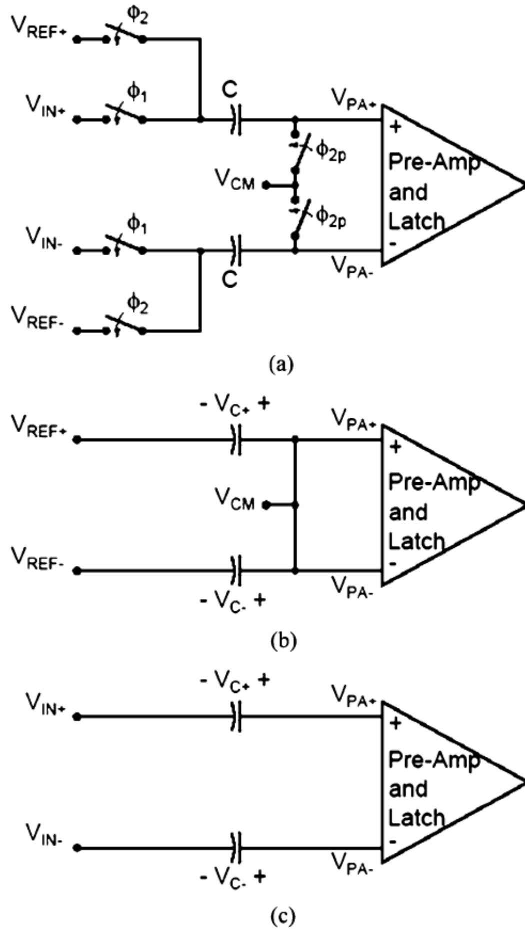


Figure 9-20: (a) The switched-capacitor comparator operates in two phases: (b) reset phase and (c) evaluation phase (From [144])

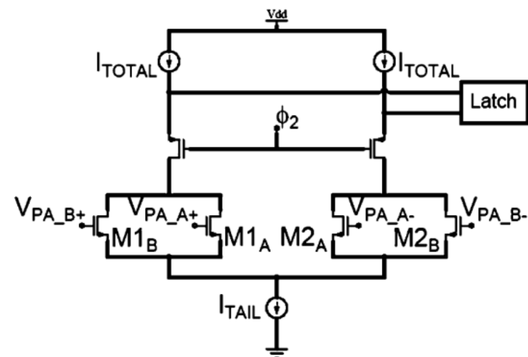


Figure 9-21: Simplified circuit schematic of the differential amplifier showing the split input paths (From[144])

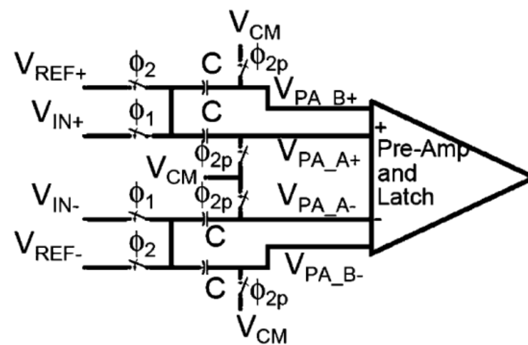


Figure 9-22: The switched-capacitor comparator with split differential amplifier input paths to harden the floating nodes against single-event upsets (From [144])

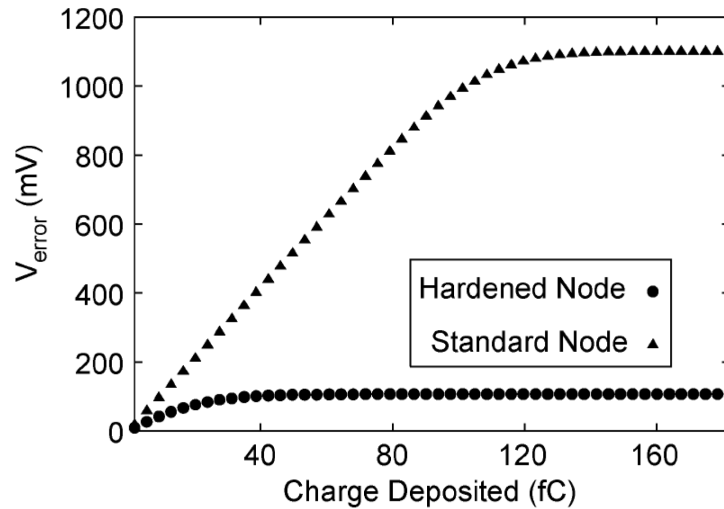


Figure 9-23: Simulated output error voltage versus deposited charge of a sample and hold amplifier with and without dual path hardening (From [143])

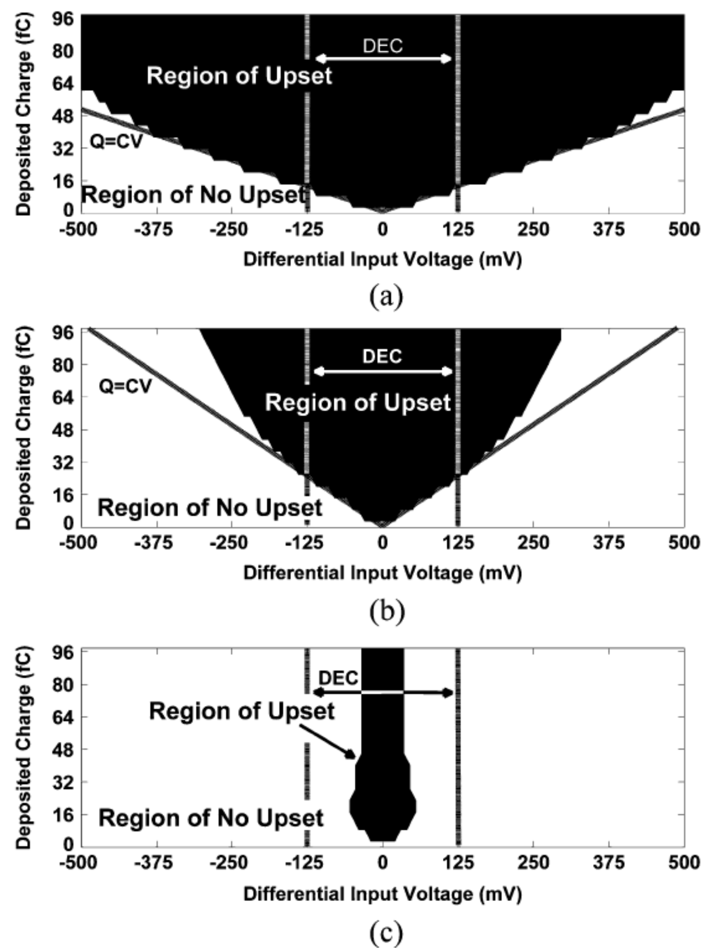


Figure 9-24: Simulated deposited charge required to generate a SEU at the output of the comparator for various differential input voltages for the (a) unhardened

design, (b) the design with increased capacitors (2x), and (c) the design implementing dual path hardening (From [144])

Example(s)

- Figure 9-20 illustrates a standard switched-capacitor comparator design as commonly used in pipelined analog-to-digital converters [144]. The comparator operates in two phases: the reset phase when the common-mode voltage is applied to both inputs, and evaluation phase when the two inputs are compared. A voltage perturbation in the differential data path of the comparator may cause erroneous data to be latched at the comparator output. Dual signal path hardening can be applied to prevent the majority of errors from generating an erroneous latched value.
- Figure 9-21 shows the comparator (pre-amp and latch) with dual inputs employed in the differential input stage. Transistors M1 and M2 have each been split into two identical transistors connected in parallel such that the width-to-length ratio of each parallel device is half the width-to-length ratio of the original transistor. If the gates of M1A and M1B are shorted together, the configuration is identical to a standard differential amplifier. Isolated signal paths can be maintained by duplicating the switched-capacitor differential input network, as shown in Figure 9-22.

Available Test Data (simulations, radiation testing, flown)

Dual path hardening was implemented in a switched-capacitor sample and hold (S/H) amplifier designed in a 90 nm technology in [143]. As seen in Figure 9-23 where the simulated output voltage error is plotted for various amounts of deposited charge, the output error is limited to approximately 100 mV for the hardened design. The unhardened configuration exhibits voltage excursions as large as 1.1 V. The local feedback technique reduces the single event vulnerability of floating nodes by an order of magnitude [143].

Additionally, simulation results indicate significant improvement in single-event performance for switched capacitor comparators implementing dual path hardening [144]. For the design depicted in Figure 9-21 and Figure 9-22, the output perturbation was reduced to values correctable by standard digital error correction. As seen in Figure 9-24, the upset contour depicting the simulated deposited charge required to generate an SEU at the output of the comparator for various differential input voltages is greatly reduced for the design implementing dual path hardening when compared to that of the standard design and a design with doubled capacitor sizes [144].

Added value (efficiency)

- The dual path hardening technique greatly improves the SET tolerance of switched capacitor topologies with floating nodes
- The S/H amplifier with dual path hardening has a negligible area penalty because the sizes of the capacitor elements could be halved
- Device matching, frequency response, and noise performance are unaffected

Known issues (Weaknesses, elements to be considered)

- Unlike the aforementioned S/H amplifier, the comparator design with dual path hardening required a doubling of capacitor sizes because the baseline capacitor dimension were already at minimum dimension and could not be halved. Depending on the application, it may be possible to halve the sizes of the capacitors when splitting the input paths, while still maintaining acceptable matching and noise performance [144].

- There is an increase in wiring complexity with dual path hardening due to the extra elements required for the split data paths

IC family	Analog circuits
Abstraction level	Design level / Layout level
Pros	Improved SET tolerance Identical frequency response as unhardened counterpart Equivalent noise performance
Cons	Area penalty possible (may be negligible in certain designs) Increased wiring complexity
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

10
Digital circuits

10.1 Scope

Four fundamental fault tolerance schemes can be applied for digital ASICs:

- **Spatial redundancy**: resources are replicated in order to process the same task in parallel. A downstream voting circuitry is in charge of error detection and eventually error correction, depending on the number of implemented replicas. Depending on selected architecture, the hardened system can handle a more or less wide scope of errors (SET, SEU, etc).
- **Temporal redundancy**: signals are sampled at different instants and a voting circuitry allows rejecting transients and upsets.
- **Memory cell hardening**: memory cells often represent a huge percentage of the total silicon area occupied by a digital circuit. Hence, designers must take special precaution to ensure their robustness meet the mission criteria. A suitable solution is the replacement of memory cells (flip-flops, registers, etc.) by hardened ones. Section 13 is devoted to present representative rad-hard memory cells.
- **Information redundancy**: error-detecting codes or error-correcting codes are able to protect data from radiation effects. This category of solutions is presented within the section devoted to system architecture (see section 15.3.6).

Fault tolerant techniques presented in this section apply at logic level. This means that they can be implemented in Hardware Description languages (HDL) such as Verilog or VHDL or at schematic description level. The best solution is often not one technique but a combination of several approachs. For this reason, techniques presented hereafter are either based on spatial redundancy, temporal redundancy or both. It is important to notice that these techniques only address non destructive SEEs. Some of them can handle SET, others SEU and others both. Permanent errors due to TID can not been dealt with by these approaches. In reference [145] are described representative mitigation schemes that could help a designer to deal with errors induced by radiation.

10.2 Table of effects vs mitigation techniques

Mitigation techniques		Radiation effects		Page
		SET	SEU	
10.3.1	Spatial redundancy	X	X	90
10.3.2	Temporal redundancy	X	X	94

10.3 Mitigation techniques

10.3.1 Spatial redundancy

Description of the concept/implementation

Spatial redundancy, also called hardware redundancy, is based on replicating sensitive resources and voting the outputs to detect discrepancies (Figure 10-1). Several architectures are available, each of them having advantages and penalties. However, all of them imply an area tradeoff and, as a direct relationship, a power consumption tradeoff.

A mismatch between the results supplied by the different replicas is detected by the voter which basically compares the values using a logical XOR. Hence, as the decision whether the result is correct or not only relies on this element, the voter is the critical part of this architecture. Thus, as shown in the hereafter presented topologies, some architecture may use three output voters.

Spatial redundancy solutions can be classified into two categories whether they can provide:

- **Error detection** only: this is the case for duplex architectures, also called Bi-Modular Redundancy (Bi-MR).
- **Error detection and correction:** as it is the case for architecture having three, called Triple Modular Redundancy (TMR), or more replicas, called N-Modular Redundancy (N-MR).

Examples of Bi-MR and TMR as they are the most commonly implemented architectures in space applications are given hereafter.

Figures/diagrams

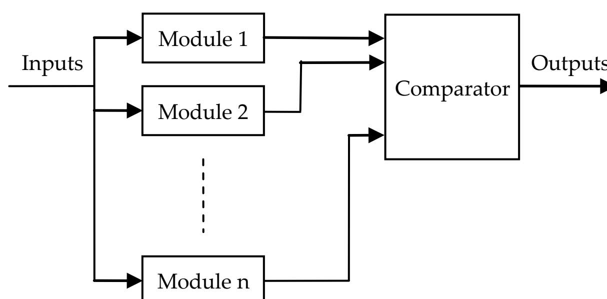


Figure 10-1 : Block diagram of the spatial redundancy architecture

Example(s)

<u>Duplex architectures</u>

Duplex architecture uses two replicas of a processing unit and votes the outputs to detect potential differences provoked by SEEs. This scheme can be applied for both combinational and sequential logic and can provide respectively SET (Figure 10-2 (a)) and SEU (Figure 10-2 (b)) detection.

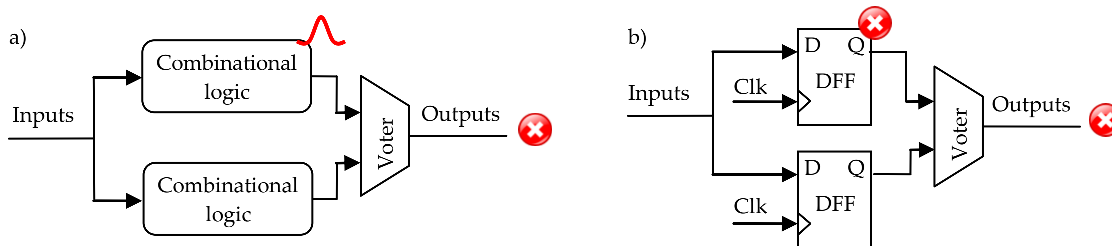


Figure 10-2 : (a) SET and (b) SEU detection with a duplex architecture

The voter being the critical element, it must be robust to faults. Usual solutions are either design it with larger transistors in order to reduce their sensitivity to SEEs or replicate it.

The duplex architecture is mainly a fail-stop architecture as it is able to detect faults but not to recover them. When both results are identical (but not necessarily correct), as illustrated in Figure 10-3 (a) the voter assumes that both are correct. When they differ, the voter detects an error but is not capable of determining the non-faulty one (see Figure 10-3 (b)). In this case two recovery mechanisms can be applied: either to skip this value and move on the next one, or to process the data again in order to obtain the correct value. This choice depends on the result criticism in the application.

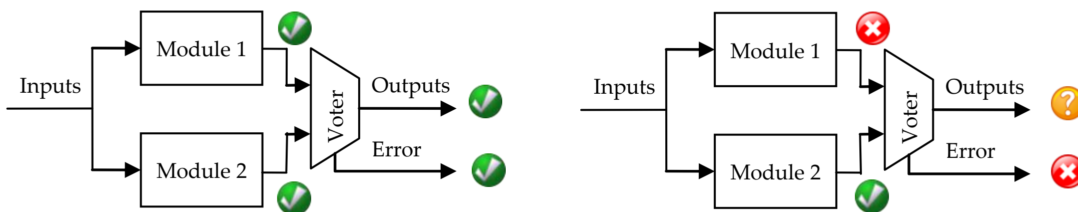


Figure 10-3 : Fault detection by a duplex architecture

A self-checking circuit can be added in order to detect faults occurring in the sensitive elements. For example, parity checking in arithmetic logic functions. This solution, illustrated in Figure 10-4 (a), is composed of the main module (module 1), its self-checking circuit and a spare module. Whenever the self-checking module detects an error in Module 1, its switches the select input of the multiplexer (MUX) in order to output the results issued from the Spare module. Those results are supposed to be fault-free but this cannot be guaranteed. Moreover, the self-checking circuit is often as complex as the circuit it must monitor, increasing the cost of the project. For this reason an alternative, depicted in Figure 10-4 (b), is based on the traditional duplex architecture enhanced with a third identical module used as a Spare module. Whenever a mismatch is detected between module 1 and 2, the MUX switches to output results from the Spare module. Once again this strategy is based on the assumption that the spare module is fault-free. Moreover the area penalty here is quasi identical to the one

obtained with a Triple Modular Redundancy (TMR) but without the error correction capability offered by a TMR.

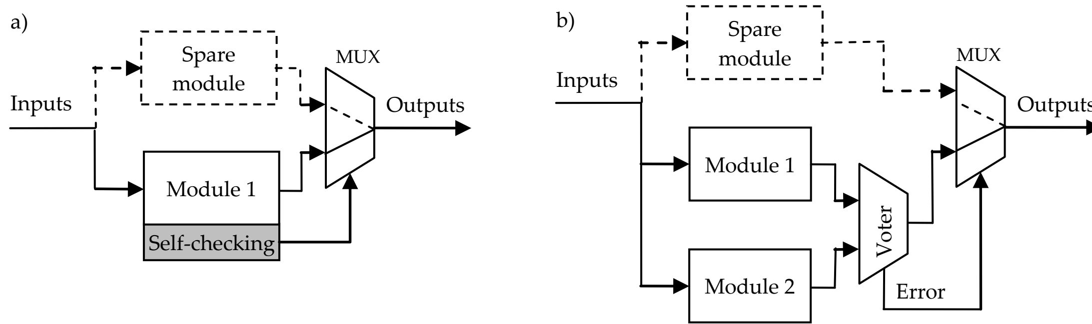


Figure 10-4 : Hot backup (a) and duplication with backup (b) approaches

<u>TMR architectures</u>

The Triple Modular Redundancy (TMR) architecture is based on three redundant elements whose outputs are voted by a majority comparator in order to determine the correct result. When an upset provokes an error, it is expected that at least two results remain correct, allowing the voter to forward the correct result .

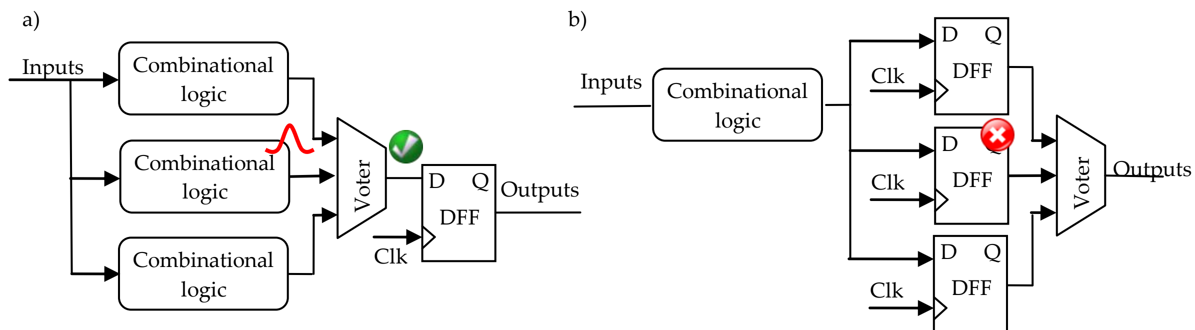


Figure 10-5 : SET (a) and SEU (b) detection with a duplex architecture

The TMR architecture's efficiency regarding fault tolerance suffers from two limitations:

- An SET occurring in the combinational logic and propagating till a TMR structure may be sampled by the three flip-flops if it is concurrent with their sampling clock pulse. Consequently the voter receives three identical faulty results and propagates the error.
- An SET occurring in the voter itself, it may output a wrong value which will be propagated.

The full TMR architecture is an answer to the above identified weaknesses. As depicted in Figure 10-6, it combines a triplication of both the combinational logic and the voters:

- The first example, depicted in Figure 10-6 (a), is a particle provoking an SEU in one of the flip-flops, consequently producing an incorrect value on its output. However the voter is able to reject it and the feedback loop restores the correct value in the flip-flop.
- Figure 10-6 (b) illustrates the case of an SET occurring in the combinational logic and propagating till the flip-flop where it is sampled by the flip-flop. The voter is once again able to reject the fault.

- The last case represented in Figure 10-6 (c) describes an SET occurs in the voter itself. The voter will output the transient for a short period of time. However, since it is a triplicated architecture, only one way out of three is affected and the error will be rejected by the next encountered voter. In case these outputs are also outputs of the chip, then they can be tied together outside the package to form an "analogue voter". So, even if a transient occurs in one of the voters, the two correct outputs will force the faulty output to the correct value.

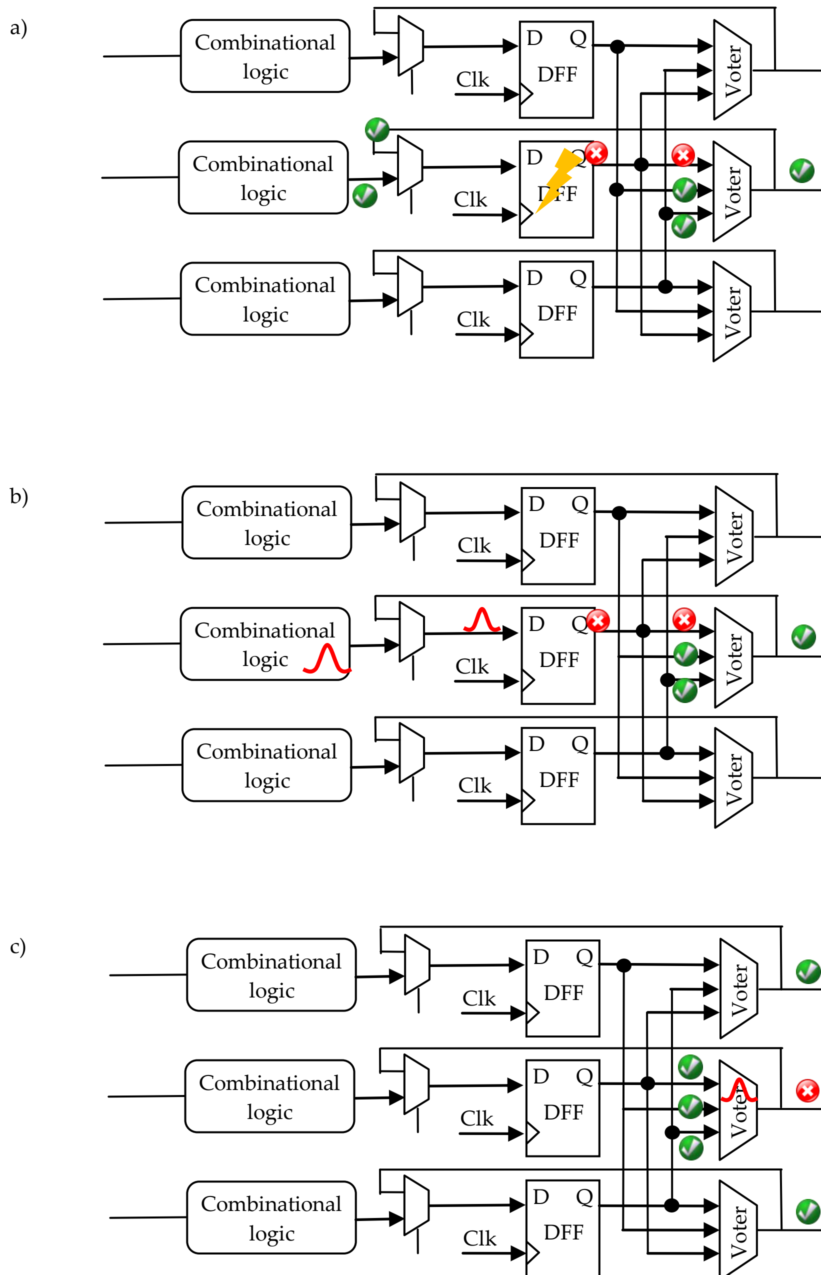


Figure 10-6 : Fault detection en correction in the full TMR architecture

The above examples proved the capability of the full TMR architecture to detect and correct SETs in the combinational logic and SEUs in the flip-flops. Nevertheless, this is not the ideal solution as it still suffers from two weaknesses:

- One of the effects of scaling down the transistors is the increase of the risk of charge sharing between several devices [146]. This may provoke multiple errors capable of affecting several redundant nodes. Increasing the distance between redundant elements during the chip layout is one of the solutions to deal with this threat.
- In case an end-chain voter is required, "the voter of the voters", it can be the source of undetected faults. Even if the probability is low, the designer must keep in mind this weakness. As discussed in references [147] and [148], an alternative is the use of an analogue voter instead of a digital one.

Available Test Data (simulations, radiation testing, in-flight)

No data available

Added value (efficiency)

No data available

Known issues (Weaknesses, elements to be considered)

No data available

IC family	ASICs
Abstraction level	Circuit
Pros	SET and SEU detection and correction
Cons	• Area overhead: depending on the number of redundant nodes • Power consumption
Mitigated effects	SET, SEU
Suitable Validation methods	Radiation ground testing Fault injection
Automation tools	FTI (Fault Tolerant Insersion) and FTIS (Fault Tolerant Injection and Simulation) from the AMATISTA project [149] [150] (p.184)

10.3.2 Temporal redundancy

Description of the concept/implementation

The concept of temporal sampling is based on sampling a data at different instants. An asynchronous voter will then determine the correct value. The advantage of such a strategy is that it protects against SEU (spatial redundancy) but also SET (temporal sampling).

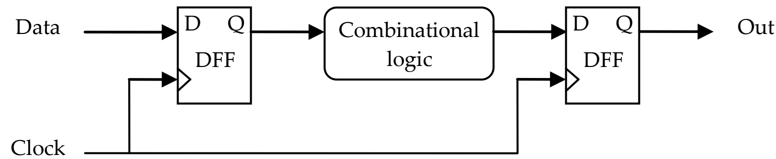


Figure 10-7 : Typical topology for a sequential circuit

As illustrated in Figure 10-7, a flip-flop's input is usually the result of a combinational computation where a transient can propagate along the logic chain. If this transient reaches the flip-flop at a clock edge it may be latched. Protection against this phenomenon can be achieved by sampling the combinational output at three different instants. This can be implemented using delays (ΔT) as depicted in Figure 10-8. Transients can be rejected by ensuring that ΔT is longer than the transient's duration.

Figures/diagrams

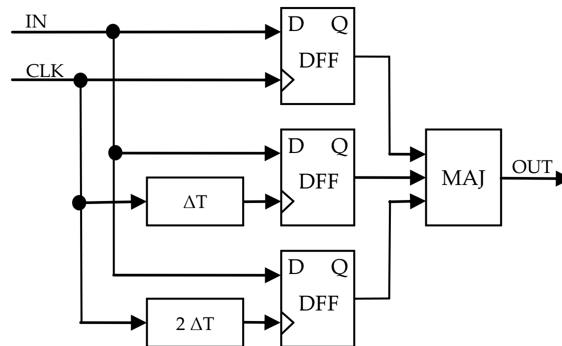


Figure 10-8 : Block diagram of a typical temporal sampling

Example(s)

In reference [151] is done a complete study on the temporal sampling methodology. Different implementations of this technique are presented and the design tradeoffs are discussed in details.

Example 1: Temporal sampling latch

One of the proposed design implementations is illustrated in Figure 10-8. An equivalent design, shown in Figure 10-9, applies delays on the data instead of the clock.

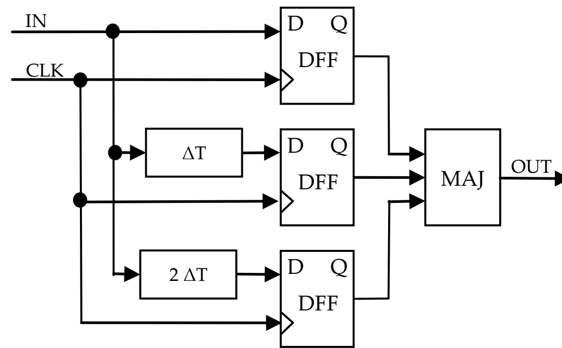


Figure 10-9 : Temporal sampling using delays on data

It should be noted that the input clock nodes of the temporal latches shown in Figure 10-8 and Figure 10-9 are susceptible to single event transient induced errors. If the temporal latch is in blocking mode at the occurrence instant of these transients, incorrect data may be latched into multiple branches of the latch, thus producing an error at the output of the majority gate. The use of these temporal sampling latches should therefore be limited to circuits in which the clock node capacitance and thus its Q_{crit} is sufficiently large, avoiding transients to be generated in the radiation environment.

Flip-flops of the LEON2-FT processor control unit, are protected by temporal redundancy.

Example 2: Minimal level sensitive latch

Another circuit topology, illustrated in Figure 10-10, is able to ensure both an SET-immune clock path and an SEU-immune latch without spatial redundancy. One way to describe a level sensitive transparent latch is as a two-input multiplexer (MUX) with its output fed back to one of its input, the select input controlled by the clock signal. Temporal sampling can be used in this case to replicate in time the function of the MUX and thus achieve SEU immunity equivalent to the one of spatial replication.

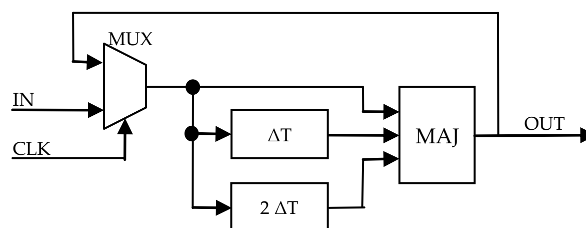


Figure 10-10 : Minimal temporal sampling latch replicating itself in time

This design provides another important improvement compared to the one given in example 1. Indeed, it is also immune to transients occurring on the clock input. Any transients momentarily switching the select input of the MUX may introduce a transient on the output. Being the input on the temporal sampling circuitry, this event is simply rejected by the majority voter. Thus, unlike the temporal latches presented in Figure 10-8 and Figure 10-9, this version does not require SET hardened clock nodes.

Another important feature is the fact that this latch can be made immune to upsets from double node strikes by an appropriate increase of the ΔT value in the sampling delays.

Available Test Data (simulations, radiation testing, in-flight)

No data available

Added value (efficiency)

High SEU immunity.

Known issues (Weaknesses, elements to be considered)

Area penalty

According to reference [151], the area penalty of the two structures presented in example 1 is about four times the area of a conventional D-Flip-Flop (DFF), whereas the minimal level sensitive latch (example 2) is roughly three times larger than a conventional DFF. However, the total chip area will not grow by these numbers as a typical design is not composed exclusively by latches and the combinational logic circuitry remains unchanged. In typical ASICs designs, the authors observed that DFFs usually represents 20% to 40% of the total chip area provoking respectively an increase factor of 1.4 to 1.8.

Speed penalty

The insertion of two extra delays results in a lower clock operating frequency. Reference [151] provides a graph showing the speed penalty as a function of the original design frequency and for four different sampling ΔT values. As an example, a design operating at 50MHz will have its frequency reduced by 2% for a 200 ps sampling delay. However, if the original circuit operates at 500MHz, the speed penalty grows to almost 20 % for the same sampling delay.

SET tolerance depends on the SET duration.

IC family	ASICs
Abstraction level	Circuit
Pros	SET/SEU detection and/or SET/SEU masking
Cons	Area penalty: 1.4x to 1.8x Speed penalty: depending on the operating frequency and sampling delay
Mitigated effects	SET and SEU
Suitable Validation methods	Radiation ground testing
Automation tools	N/A

10.3.3 Fail-Safe Finite State Machines

This section will be added soon.

10.4 Vendor solutions

10.4.1 Radhard circuit manufacturers

Hereafter is provided a non-exhaustive list of radiation tolerant/hardened circuit manufacturers:

- Aeroflex
- ASIC advantage
- Atmel
- BAE Systems
- Boeing
- C-MAC MicroTechnology
- Crane Aerospace & Electronics
- Freescale
- Honeywell
- International Rectifier
- Intersil Corporation
- M.S. Kennedy Corporation
- Maxwell Technologies Inc.
- Microsemi
- Northrop Grumman
- Peregrine Semiconductor Corporation
- SEMICOA
- Space Micro Inc.
- STMicroelectronics
- Texas Instruments
- Xilinx

10.4.2 Radhard processors

Processors	Architecture	SEU	SEL	TID	Missions
Harris RHC-3000	32-bit MIPS R3000	LET_{th} > 80 MeV-cm2 / mg SER < 1E-7 SEU/Device/Day	Immune	>1 MRad (Si)	*Unknown*

Erreur ! Source du renvoi introuvable.[10] including the memory cells that configure the LUT, the ones that control the routing and the CLB customization.

Honeywell RH32	32-bit MIPS R3000	LET_{th} > 35 MeV-cm2/mg SER = 1E-9 SEU/bit/day	Immune up to 165 MeV-cm2/mg	>1 MRad (Si)	Air Force Space Based Infrared System (SBIRS) program
TRW/UTMC RH32	32-bit MIPS R3000	*No data available*	*No data available*	*No data available*	*Unknown*
TI SMJ320C30	32-bit DSP	LET_{th} = 3 35 MeV-cm2/mg SER = 2E-4 SEU/Device/Day	Immune up to 63 MeV-cm2/mg but important increase in current consumption	*No data available*	*Unknown*
Atmel TSC695	32-bit ERC32 SPARC V7	SER > 1.6E-8 SEU/Device/Day (GEO) SER > 8E-10 SEU/Device/Day (LEO)	Immune up to 100 MeV-cm2/mg	300 krad (Si)	• Communication satellites • ESA's SMART-1 lunar mission
Atmel AT697	32-bit LEON2 SPARC V8	SER > 1E-5 SEU/Device/Day (Worst Case)	Immune up to 70 MeV-cm2/mg	300 krad (Si)	*Unknown*
Broad Reach Engineering BRE440	32-bit PPC440	SER > 40 Years/Upset	Immune	>1 MRad (Si)	*Unknown*
Intersil CDP1802A	8-bit RCA1802	*No data available*	*No data available*	*No data available*	Galileo Jupiter
Intersil 80C286	16-bit 80286	*No data available*	*No data available*	*No data available*	*Unknown*
Honeywell RHPPC	32-bit hardened PowerPC 603e	SER = 1.1E-5 SEU/Device/Day (GEO orbit)	Immune	*No data available*	*Unknown*
Honeywell HX1750	16-bit MIL-STD-1750A	SER < 1.E-5 SEU/Device/Day	Immune	> 100 krad (Si)	• ESA Rosetta space probe • NASA Cassini orbiter • USAF Titan-4 Guidance Computer

10.4.3 Radhard computers

Computers	Processor	SEU	SEL	TID	Missions
Space Micro Inc. Proton200k (see section 15.4.1)	Proton 200k: TI 320C6XXX Series DSP processor	1 E-4 Errors/Board/Day	> 70 meV.cm²/mg	>100 Krad (Si)	Lockheed Martin ANGELS nanosat
Space Micro Inc. Proton400k	Freescale e500 dual-core	1 E-4 Errors/Board/Day	> 70 meV.cm²/mg	>100 Krad (Si)	*Unknown*
IBM System/4 Pi	Based on IBM System/360 mainframe computer	*No data available*	*No data available*	*No data available*	• Space shuttle • Skylab • USAF B52 and F-15

BAE Systems RAD6000	32 bits RISC IBM Power architecture	7.4E-10 errors/bit-day (90% W.C. GEO)	Immune	>1 MRad (Si)	• IBM System/4 Pi Mars Pathfinder lander • Deep Space 1 probe
BAE RAD750	32-bit IBM PowerPC 750	1.9 E-4 Errors/Board/Day (90% W. C. GEO) varies with orbit	Immune	>100 Krad (Si)	• Deep Impact comet chasing spacecraft • Mars Reconnaissance Orbiter spacecraft
Maxwell SCS750 (see section 15.4.2)	32-bit IBM PowerPC 750	One board upset every 100 years in LEO or GEO orbit	> 80 meV-cm2/mg - all parts except SDram ≈ 50 meV-cm2/mg - SDram	> 100 krad (Si) - orbit dependent	• NASA Glory earth sciences • National Polar-orbiting Operational Environmental Satellite System (NPOESS)
Boeing Spaceway	32-bit IBM PowerPC 750	*No data available*	*No data available*	*No data available*	Communication satellites

11 Mixed-signal circuits

11.1 Scope

A mixed-signal circuit is an integrated circuit having both an analogue part and a digital part on a single chip. Hence, mitigation techniques devoted to both analogue circuits (see section 9) and digital circuits (see section 10) can be applied to mixed-signal ICs. Details of the implementation of the Triple Modular Redundancy technique are exposed in this chapter.

11.2 Table of effects vs mitigation techniques

Mitigation technique		Abstraction level	Radiation effects	Page
			SET	
11.3.1	Triple Modular Redundancy	Design	X	101

11.3 Mitigation techniques

11.3.1 Triple Modular Redundancy

Description of the concept/implementation

While more common in digital circuits, Triple Modular Redundancy (TMR) has been successfully used in mixed-signal circuits with digital output signatures, such as the voltage comparator. A detailed description of the TMR concept is available in section 10.3.1.

Example(s)

The TMR approach was adopted in [152] where a single comparator was replaced by three parallel comparators driving a CMOS majority-voting block. The voting circuit was hardened by oversizing the transistors [95] [152].

Another example of TMR implementation within a mixed-signal circuit is described in reference [153]. This article presents a Voltage-Controlled Oscillator (VCO) topology hardened to single-events using an approach based on TMR. Rather than running three stand-alone VCOs in parallel, three voltage-controlled-delay-lines (VCDLs), each with independent bias stages, are implemented in parallel with a single feedback path for jitter reduction. The design is shown to reduce the output phase displacement following ion strikes to below the normal operating noise floor.

Figures/diagrams

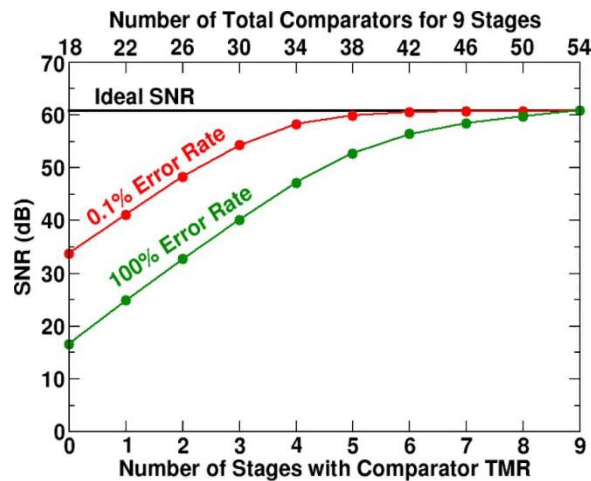


Figure 11-1 : Signal-to-noise ratio improvement for increasing use of comparator TMR in a 10-bit pipelined ADC.

Available Test Data (simulations, radiation testing, in-flight)

Reference [154] presents an evaluation of the tradeoffs of comparator redundancy when implemented in a pipelined Analogue-to-Digital Converter (ADC). While TMR is effective at mitigating transients in the comparators, the single-event improvement reaches a point of diminishing return when comparator TMR is applied to the first half of the pipelined. The Signal-to-Noise Ratio (SNR) can generally be utilized to compare the single-event hardness of different mixed-signal circuit designs. By randomly injecting upsets into the circuit (in the design phase), and analyzing the response in the frequency domain, the SNR indicates the impact of the SEs on the overall response of the circuit. It is important to note that while this technique requires somewhat of an arbitrary SE injection rate, this technique does allow for comparisons between designs. Figure 11-1 shows the SNR improvement for increasing use of comparator TMR in a 10-bit pipelined ADC. Results shown are for a model with an individual comparator upset probability of 0.1% and 100%. The upset probability refers to probability of an SE strike during each data cycle. Figure 11-1 indicates that the application of comparator TMR to the first half of the 10-bit pipelined ADC produces the best tradeoff in decreasing single event vulnerability versus increasing area and power. Note that even assuming extremely high comparator upset rates, comparator TMR is most effective when applied to the first 50% to 70% of the total number of stages. The authors show similar results regardless of ADC resolution. In conclusion, when used in pipelined ADCs, comparator TMR is best utilized in the first 50% of pipelined stages, regardless of the ADC resolution.

Added value (efficiency)

No data available

Known issues (Weaknesses, elements to be considered)

Area penalty: ~3x + majority voter

Power consumption penalty: ~3x + majority voter

IC family	Mixed-signal circuits
Abstraction level	Design level
Pros	*No data available*
Cons	Area penalty: ~3x + majority voter Power consumption penalty: ~3x + majority voter
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

12 Field Programmable Gate Arrays

12.1 Scope

General description

A *Field Programmable Gate Array* (FPGA) is an integrated circuit that can be configured by the user rather than in the semiconductor fab. during manufacturing process. It is composed of interconnected programmable elements, called "logic blocks" (Figure 12-1).

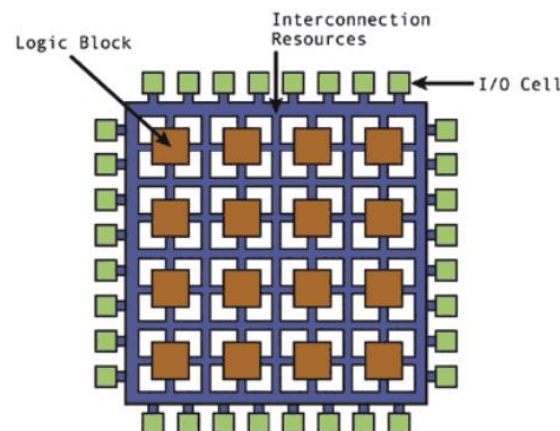


Figure 12-1 : High-level description of an FPGA structure

Logic blocks can be configured to perform complex combinational functions (combinational logic) and they include memory elements (sequential logic). Moreover, the most advanced chips also embed processors, DSPs and high speed communication interfaces.

FPGAs are composed of two "layers" (see Figure 12-2): an operative layer containing the user logic and memory and a configuration layer determining the functionality of the user logic. The nature of the configuration layer depends on the type of FPGA:

- Antifuse FPGAs use electrical structures, called antifuse, performing the opposite function to a fuse. Whereas the initial condition of a fuse is a low resistance path and is designed to permanently break an electrically conductive path (typically when the current through the path exceeds a specified limit), an antifuse starts with a high resistance and is designed to permanently create an electrically conductive path (typically when the current through the antifuse exceeds a certain level). The drawback of this technology is that the configuration is not reversible. However, in terms of radiation tolerance this is an advantage as the configuration layer is immune to bit-flips provoked by radiation.
- SRAM-based of Flash-based memory cells offer the advantage to be reconfigurable making possible "on-line" configuration of the FPGAs. According to the memory cell technology, it can be more or less sensitive to radiation. Indeed, bit-flips occurring in the configuration memory

may have an impact on the application behaviour in case the perturbed bit is used. In such case, even a reset of the application will not allow recovering a normal behaviour. Such a permanent mutation may thus have critical consequences and requires an FPGA reconfiguration to recover the nominal configuration.

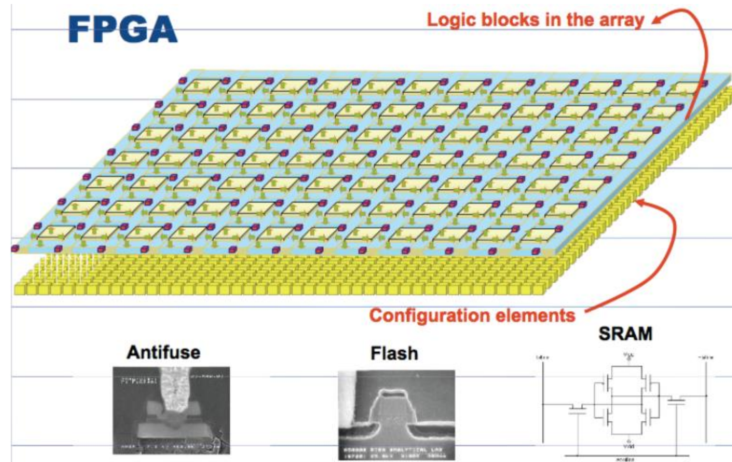


Figure 12-2 : Schematic representation of the two layers composing an FPGA

Table 12-1 summarizes for each family the main characteristics and representative manufacturers of FPGAs available on the market.

Table 12-1 : FPGAs characteristics and representative manufacturers

Configuration memory nature	Antifuse	Flash	SRAM
Characteristics	• Electrically programmable switch which forms a low resistance path between two metal layers • Configuration is NON volatile • One-time programmable	• Electrically programmable transistors which hold the configuration that controls a pass transistor or multiplexer connected to predefined metal layers • Configuration is NON volatile • Re-configurable	• The state of a static latch controls a transistor or multiplexer connected to predefined metal layers • Configuration is volatile • Re-configurable
Representative manufacturers	Aeroflex Actel Microsemi	Actel Microsemi	Xilinx Atmel

Note: a few other companies (e.g. Altera, Lattice, etc) manufacture SRAM-based FPGAs. However, they have not proposed until now a hardened FPGA solution. Consequently, this section will address only SRAM-based FPGAs manufactured by Xilinx and Atmel.

12.2 Table of effects vs mitigation techniques

Mitigation techniques		Abstraction level	Radiation effects			Page
			SET	SEU	SEFI	
12.3.1	Local TMR	HDL		X		106
12.3.2	Global TMR	HDL	X	X		108
0	Large grain TMR	HDL	X	X		111
0	Embedded user memory TMR	HDL	X	X		113
12.3.5	Voter insertion	HDL	X	X		114
12.3.6	Reliability-Oriented place and Route Algorithm	FPGA layout	X	X		117
12.3.7	Temporal redundancy	HDL	X			119
12.3.8	Embedded processor redundancy	HDL	X	X	X	121
12.3.9	Scrubbing	System		X		122

12.3 Mitigation techniques

12.3.1 Local Triple Modular Redundancy

Description of the concept/implementation

Triple Modular Redundancy (TMR) is an architecture belonging to the spatial redundancy family which is widely presented in section 10.3.1. It consists in implementing three identical flip flops processing the same task and whose outputs are compared by a majority voter. The main advantage of the technique is its capability to detect and correct single event transients and upsets.

Figures/diagrams

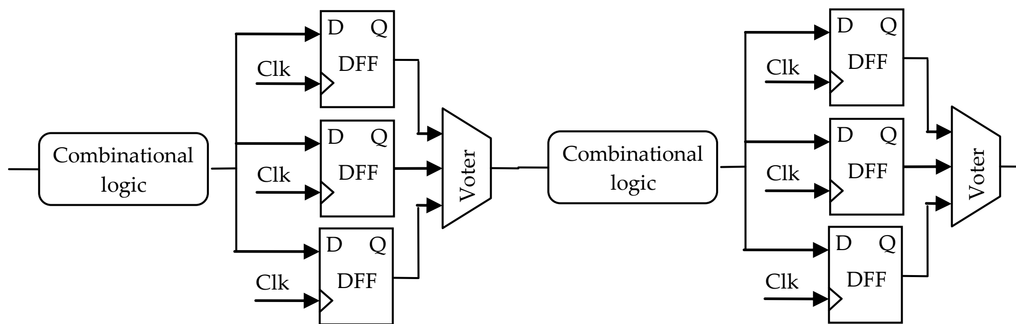


Figure 12-3 : Local TMR – single combinational logic but triplicated registers

Example(s)

The local TMR technique (Figure 12-3) consists in triplicating only flip-flops and voting their outputs. It can be applied by the FPGA's manufacturer in the silicon matrix (e.g. Microsemi RTAX-S/SL and Microsemi RTSXS) or by the user in the HDL description of the application for FPGAs that do not embed a hardening scheme for flip-flops (e.g. flash-based FPGAs such as the Actel ProASIC3). This technique may be used for designs running at low frequencies and thus with low probability of capturing SETs in the flip-flops. Examples of implementation of this technique are given in reference [155].

Available Test Data (simulations, radiation testing, in-flight)

In reference [156] are presented experimental data obtained on the Actel RTAX-S anti-fuse based FPGA which implements TMR at each flip-flop. Heavy ions tests performed with the tested circuit operating at different frequencies put in evidence the impact of frequency in the circuit cross section. As an example, for high LET, when the frequency rises from 15 MHz to 150 MHz, the cross section increased around three times.

Added value (efficiency)

- The advantage of a local TMR is that the area penalty is limited to registers as combinational logic is not replicated.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

Local TMR partially protects against SEUs in the flip-flops (FF). Indeed, an SET occurring in the combinational logic would propagate to the FFs and if concurrent with the sampling clock pulse the error will be latched and the voter will have three identical, but false, results and consequently it will not detect the error. A solution to this issue is the global TMR strategy (see section 12.3.2).

Local TMR will not protect against a multiple bit upset that can disrupt to flip-flops replicas[157]. In most cases for present technologies, the rate of SET capture adheres to requirements. It is expected that SET susceptibility will become more of a concern as device geometry shrinks.

IC family	FPGAs
Abstraction level	Local TMR: IC architecture or HDL level
Pros	Eliminate SEU in registers.
Cons	Area penalty: limited to registers. 3 times flip-flops.
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	Mentor Precision Rad-Tolerant
Vendor solutions	Microsemi RTAX-S/SL & Microsemi RTSXS

12.3.2 Global Triple Modular Redundancy

Description of the concept/implementation

Global TMR is based on the spatial redundancy concept detailed in section 10.3.1. Global TMR consists in triplicating all the resources of an application, including clock tree and IOBs. It can be applied in the design's HDL description either by the user or through the use of dedicated tools such as Xilinx X-TMR tool or Mentor Precision Rad-Tolerant which are both able to automatically apply Global TMR technique to the user's design.

Figure 12-4 illustrates a typical global TMR implemented in an FPGA. The entire processing chain is triplicated from the input pins to the outputs pins. Flip-flops are hardened, as explained in section 12.3.2, using three redundant FF, three voters and feedback paths for fault recovery. The final stage, called TMR output voter, controls the enable input of a tri-state buffer [158]. This buffer is used in high-impedance mode whenever a faulty result is encountered, hence avoiding the output of an erroneous result.

The only sensitive part of the architecture is its output voter. However, the three outputs being connected together operate like an "analogue voter": two correct results force the output value to the correct logical level.

Figures/diagrams

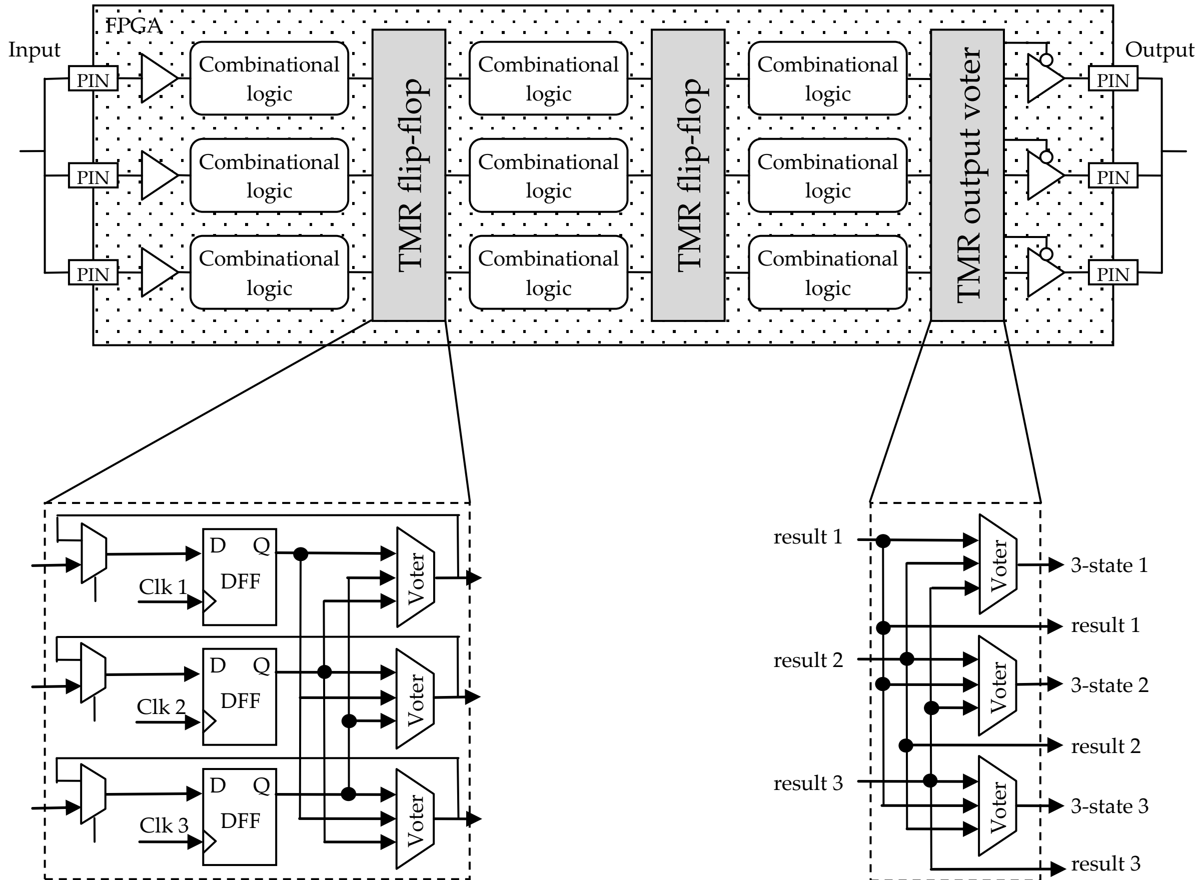


Figure 12-4 : Global TMR implemented in an FPGA

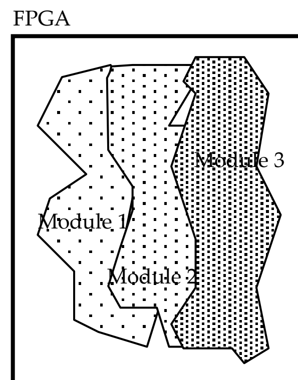


Figure 12-5 : Physical implementation of a local or global TMR inside an FPGA

Available Test Data (simulations, radiation testing, in-flight)

Experimental results issued from tests of PicoBlaze unhardened and global TMR hardened versions performed with alpha source show a significant decrease, up to one order of magnitude, of the error probability at the hardened version circuit outputs[157].

Added value (efficiency)

- Protect whole design from SET in combinational logic and SEU in registers.
- This technique helps mask upsets in the configuration memory. It is to be noted that this is not correcting upsets in configuration.

Known issues (Weaknesses, elements to be considered)

Global TMR requires having frequent interconnections between the three replicas of the TMR. It is, thus, almost impossible to physically separate the three replicas in the implementation of the design in the FPGA. Figure 12-5 illustrates how a design using TMR would look like once implemented in an FPGA: the three replicas would overlap and resources from the three domains would be mixed within the same logic blocks. This has two main consequences: the first is that partial scrubbing (see section 12.3.9) cannot be used and the second is the increase of the risk to encounter domain crossing events (see section 12.3.5).

IC family	FPGAs
Abstraction level	HDL or Gate level (implementation and tool dependant)
Pros	Eliminates SET and SEU
Cons	Area penalty, need to do clock skew management, power, validation (not easy to validate)
Mitigated effects	SET, SEU, configuration is masked
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	Xilinx X-TMR tool Mentor Precision Rad-Tolerant
Vendor solutions	RTAX include hardened clock

12.3.3 Large grain Triple Modular Redundancy

Description of the concept/implementation

Large grain TMR is based on the spatial redundancy concept presented in section 10.3.1. This particular implementation of TMR consists in triplicating a design, but unlike local and global TMR, the flip-flops are not voted. Instead, a unique voter is placed at the end of an entire module (Figure 12-6).

One challenge of the large grain TMR is to resynchronize an erroneous replica with the others. This is done as follows [159]:

1. Identify the erroneous module by modified majority voter
2. Reconfigure the faulty module if the upset took place in the configuration memory
3. Synchronize the module with the other two

Figures/diagrams

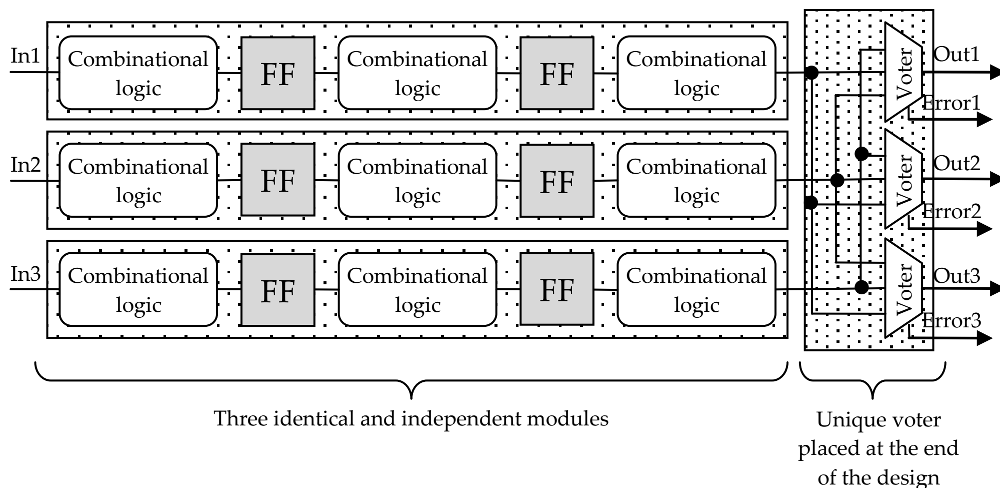


Figure 12-6 : Large grain TMR

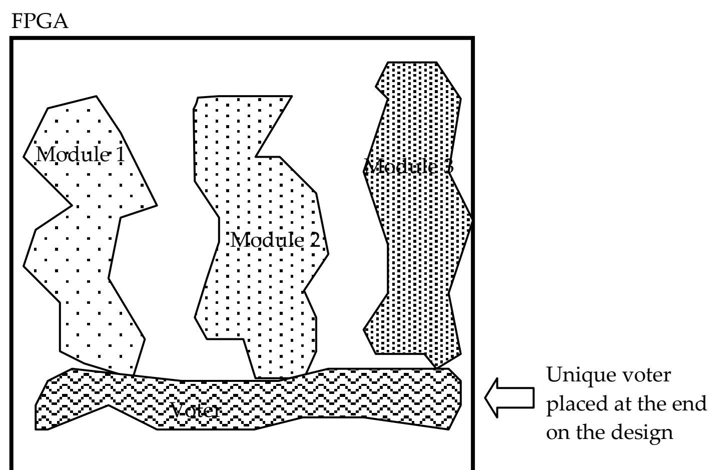


Figure 12-7 : Physical implementation of a large grain TMR inside an FPGA

Example(s)

No data available

Available Test Data (simulations, radiation testing, in-flight)

Experimental results performed with alpha source, issued from tests of two versions of PicoBlaze, one unhardened and the other hardened by one-voter TMR (large grain), show a little improvement of the hardened circuit robustness: the probability of an error at the circuit output is reduced by a factor up to two [157].

Added value (efficiency)

- Local placement and routing for each TMR redundant domain allowing physical separation of each replica as illustrated in Figure 12-7.
- A consequence of the previous mentioned added value is the possibility of using partial reconfiguration (see section 12.3.9) to scrub only at redundant domain that has the error, thus, reducing the scrubbing time and energy.
- Minimal points of domain crossing (see section 12.3.5) means reduced vulnerable bit-flips that can upset the TMR.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

Large grain TMR may fail if two sensitive bits belonging to two different replicas are upset.

IC family	FPGAs
Abstraction level	HDL level
Pros	Limits domain crossing event
Cons	Area penalty
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	Mentor Precision Rad-Tolerant
Vendor solutions	None

12.3.4 Embedded user memory TMR

Description of the concept/implementation

Embedded user memories, such as Block SelectRAM (BRAM) memories in Xilinx FPGAs, are resources available for the designers. Those memories are based on SRAM cells and are consequently sensitive to SEEs. Hence, they require a special care from the designers as the scrubbing techniques cannot protect them from SEUs (see section 12.3.9). The solution consists in applying the TMR concept combined with a refreshing mechanism of their content [158]. Figure 12-8 illustrates an example of implementation in Xilinx FPGAs using counters (that need to be protected) and voters for the refresh mechanism. The method consists in constantly refreshing the memory contents. Since these are dual port memories, one of the ports could be dedicated to error detection and correction. But this also means that the BRAM could only be used as single port memories by the rest of the user logic. To refresh the memory contents, a counter may be used to cycle through the memory addresses incrementing the address once every n clock cycles. The data content of each address is voted at a determined frequency and the majority voter value is written back into the cells.

Figures/diagrams

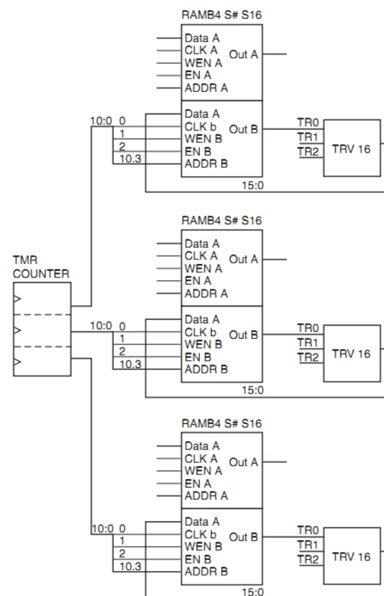


Figure 12-8 : BRAM TMR

Example(s)

No data available

Available Test Data (simulations, radiation testing, in-flight)

No data available

Added value (efficiency)

This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

Area penalty: ~3x (memory only).

IC family	SRAM-based FPGAs
Abstraction level	HDL level
Pros	Increased SEU hardness
Cons	Area penalty: ~3x (memory only)
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	Mentor TMR counters mask and correct SET

12.3.5 Voter insertion

Description of the concept/implementation

This technique is intended to reduce the probability of occurrence of Domain Crossing Events (DCE) [160]. To understand the problematic, domain crossing events are first explained. Then the voter insertion technique will be presented.

Domain crossing events:

Domain Crossing Events occur in applications mitigated by TMR when two replicas of the TMR are corrupted by SEE. This can result in an incorrect choice in the voter as two results of the TMR are false. They can be observed under the following conditions:

- When a SEE modifies the signal routing (short-cuts connections or opens connections) among different blocks of the TMR.
- When multiple bit upsets (MBU) occur due to the high density and small dimensions of the configuration memory cells or due to charge sharing.

When a new path is created as a result of a MBU, it may create an error within the same replica of the TMR. In this case as illustrated in Figure 12-9, the voter is still able to reject the fault because the two other replicas are still able to provide correct results.

A routing defect may also occur between two different replicas of a TMR. As a consequence both modules supply wrong results and thus, the voter is not able to reject the error. In the best case the two faulty results are different, thus all three outputs are different and the voter is not able to decide which result is correct. In the worst case both wrong results are the same and the voter will propagate the error as it assumes it is the correct result.

Domain crossing events are more likely to occur in full TMR designs than in large grain designs. As illustrated in Figure 12-10, the TMR flip-flops of a full TMR design require frequent interconnections

between the different replicas of the TMR, thus the replicas cannot be physically separated inside the FPGA.

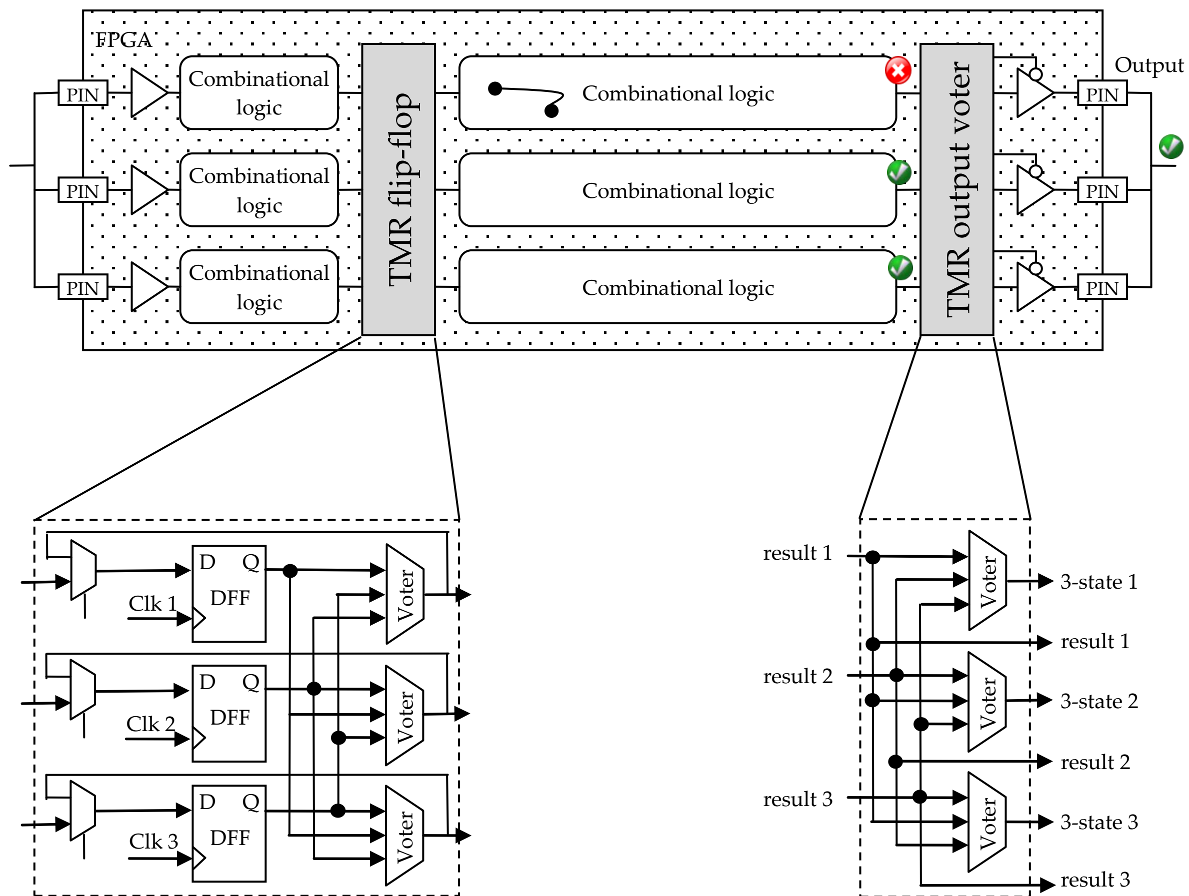


Figure 12-9 : Routing defect within the same module

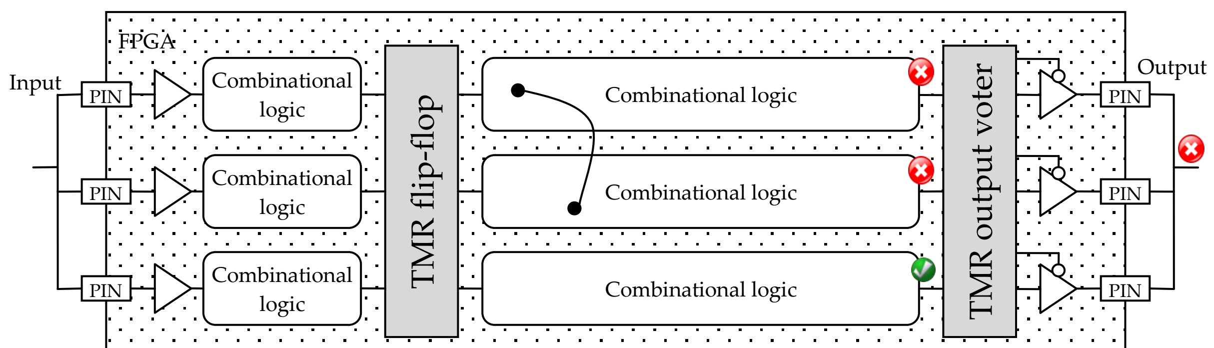


Figure 12-10 : Domain Crossing Event as a consequence of routing defect affecting two different modules

One solution to reduce the risk of DCE is to physically separate the TMR domains as illustrated in Figure 12-7. However, this is almost impossible to apply to a local or a global TMR (see sections 12.3.1 and 12.3.2). Thus, the voter insertion technique is intended for these cases.

The voter insertion technique:

The voter insertion technique consists in creating a barrier of voters to reduce the probability of a bit-flip in the routing causing a short-cut connection among two or more redundant blocks of a TMR (Figure 12-10).

Figure 12-11 illustrates the voter insertion technique applied to the example provided in Figure 12-10 where a DCE provokes an error in the combinational logic *tr1_2* and *tr2_3*. The voter after *tr1_2* is able to reject the fault based on the correct outputs of *tr2_2* and *tr2_3*. Hence the input of *tr1_3* is correct and even if the output of *tr2_3* is wrong, the final voter still has two correct outputs from *tr1_3* and *tr3_3* to provide a correct answer.

Figures/diagrams

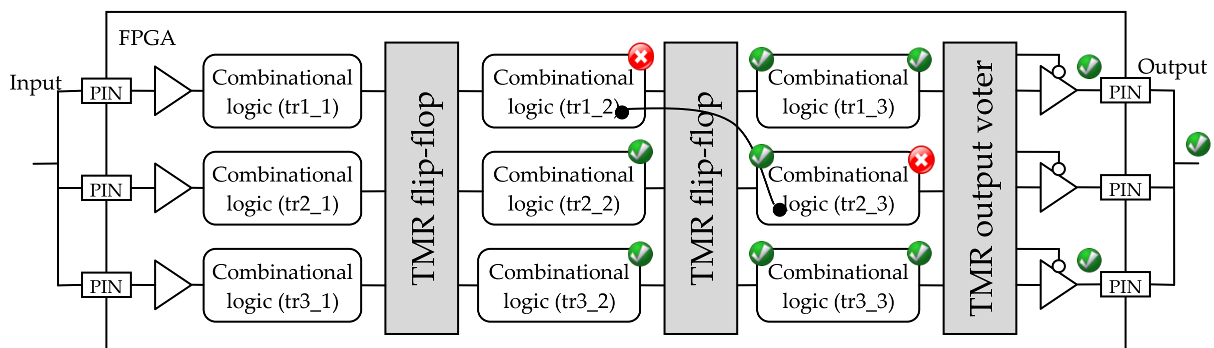


Figure 12-11 : Inserting voters reduces the risk of domain crossing events

Example(s)

No data available

Available Test Data (simulations, radiation testing, in-flight)

No data available

Added value (efficiency)

- Reduce the probability of occurrence of Domain Crossing Events by inserting barriers of voters.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

No data available

IC family	SRAM-based FPGAs
Abstraction level	HDL level
Pros	Increase SEU hardness
Cons	Area penalty: inserted voters
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	Reliability-Oriented place and Route Algorithm
Vendor solutions	N/A

12.3.6 Reliability-Oriented place and Route Algorithm

Description of the concept/implementation

Triple Modular Redundancy (TMR) design technique is the high-level SEU mitigation technique often used to protect designs in SRAM-based FPGA since memory elements, interconnections and combinational gates are all susceptible to SEUs. Among FPGA resources, about 90% of the configuration memory bits are devoted to configure the routing and are thus more likely to be affected by SEUs than any other resources. TMR is able to mitigate only partially the effects of SEUs affecting routing resources. Detailed analysis of the FPGA resources [161], and extensive fault-injection experiments [162], have put in evidence that one SEU may provoke multiple errors. This phenomenon depends on many factors: the architecture of the adopted FPGA family, the organization of configuration memory bits, the application that is mapped on the FPGA device, and the memory bit affected by the SEU. References [161] and [162] report that about 10% of the faults that may affect the FPGA routing resources produce multiple errors that the TMR is not able to mask [162]. As shown in [160], a clever selection of the TMR architecture helps in reducing the number of escaped faults, but it is still unable to reduce it to zero.

Based on those observations, the Reliability-Oriented place and Route Algorithm (RoRA) [163] was developed in order to optimize the place and route process in the design flow. First, RoRA performs a reliability-oriented placement of each logic function and, using design constraints, it routes the signals between functions in such a way that no multiple errors affecting two different connections can occur. Figure 12-12 illustrates RoRA's design flow which consists in applying a global TMR scheme after synthesis of the RTL code. Then, floorplan constraints are provided to ISE's Place and Route utility and finally RoRA's router completes routing the design. Details about the Reliability-Oriented place and Route Algorithm can be found in reference [164].

Figures/diagrams

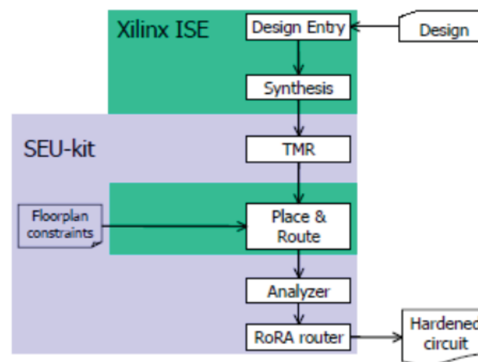


Figure 12-12 : RoRA's design flow

Example(s)

No data available

Available Test Data (simulations, radiation testing, in-flight)

RoRA's effectiveness was evaluated on some benchmark circuits by means of fault-injection experiments in the FPGA's configuration memory. The results exposed in reference [164] show a drastic reduction in the number of SEUs causing circuit misbehaviour with respect to those observed for the same circuits when the TMR design technique is adopted. For the considered benchmarks, the capability of tolerating SEU effects in the FPGA's configuration memory increases up to 85 times with respect to the standard TMR design technique. This improvement comes without any additional logic resources with respect to the TMR design technique, while a performance penalty of about 22% was observed.

Added value (efficiency)

- RoRA increases hardness to SEUs in SRAM designs by a factor up to 85 compared to a standard TMR implementation.
- RoRA is an automatic tool, thus being transparent to the designer.
- No logic resource penalty. RoRA does not introduce any overhead with respect to the traditional TMR solution.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

Performance penalty: ~22%

IC family	SRAM-based FPGAs
Abstraction level	HDL level
Pros	No area penalty
Cons	Performance penalty: ~22%
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	RoRA, Mentor Graphics, Synopsis
Vendor solutions	N/A

12.3.7 Temporal redundancy

Description of the concept/implementation

SETs occur in combinational logic and may propagate till they reach a register. If concurrent with a clock pulse, this transient may be latched and cause an SEU which will propagate in the rest of the design. A solution to filter SET is to implement a temporal redundancy scheme. It consists in processing the same data at different intervals of time (a detailed definition of the concept is provided in section 10.3.2). The simplest scheme is the use of two flip-flops controlled respectively by a clock and a delayed clock (the delay must be larger than the transient pulse width) are used to latch the combinational output at two different instants, thus allowing the detection of an SET.

At low frequencies the predominant effects are SEUs while SETs have only a little chance to be captured by registers. However, with the increase in frequency, SETs become a significant problem as put in evidence in a work done on Microsemi RTAX-S family [156]. Indeed, the higher is the number of clock pulses by unit of time, the higher will be the chance of an SET to be latched.

A proper implementation of the temporal redundancy applied to FPGAs is illustrated in Figure 12-13. The signal issued from a combinational logic block is applied to three memory cells:

- The first directly receives data signal
- The second receives the data signal after a ΔT delay. ΔT being larger than the transient pulse with.
- The third receives the data signal after a 2 ΔT delays.

A single (or triple) majority voter is used to reject an eventual fault.

Figures/diagrams

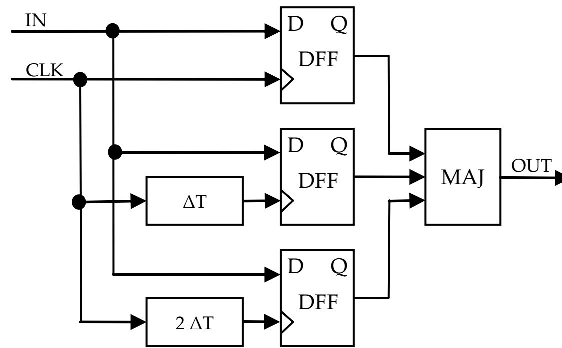


Figure 12-13 : Block diagram of a typical temporal sampling

Example(s)

Xilinx 5QV and RTAX-4000D. Temporal redundancy is implemented on DSP block.

Available Test Data (simulations, radiation testing, in-flight)

RTAX-4000D (test data are not published yet).

Xilinx 5QV: see http://radhome.gsfc.nasa.gov/

Added value (efficiency)

- Temporal redundancy eliminates SET in combinational logic.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

Known issues (Weaknesses, elements to be considered)

Temporal redundancy only filters SET up to a certain limit.

It reduces the maximum clock frequency.

IC family	FPGAs
Abstraction level	HDL
Pros	SET filtering
Cons	Area penalty Time penalty (longer critical path)
Mitigated effects	SET
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	Virtex-4000D (DSP blocks).

12.3.8 Embedded processor redundancy

Description of the concept/implementation

The latest FPGA families embed hardwired processors which are, like their ASIC counterparts, sensitive to SETs, SEUs and SEFIs. Several solutions are possible:

- Purely software-based approaches as the one presented in section 14. Those techniques generally imply little hardware overhead but require modifications of the software.
- Spatial redundancy-based solutions are presented at architecture level in section 10.3.1. They require having several processors performing the same task in order to compare their outputs, and thus to detect faults. In case of mismatch the task can be performed again.
- Hybrid approach such as the one described in reference [165].

Figures/diagrams

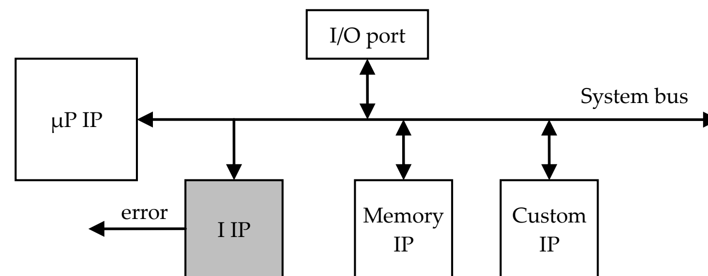


Figure 12-14 : Hybrid architecture using a fault detection-oriented I-IP

Example(s)

Software-based techniques

Redundancy at instruction, task or application level (see section 14).

Spatial redundancy

Dual-Modular Redundancy such as Lockstep, DT2, etc (see section 15.3.4).

Hybrid approach

This approach, presented in reference [165], mixes software and hardware modifications in order to achieve radiation tolerance. The architecture presented in Figure 12-14 presents the hardware modification part which consists in adding the I-IP module. This IP (Intellectual property) is mapped on the same FPGA that the one hosting the μP and it is connected to the system bus as an I/O peripheral interface. Thus, the I-IP can observe all the operations performed on the bus by the processor, and can be the target for some write operations performed by the processor at specific addresses of the memory or I/O address space (depending on the adopted I/O scheme). When the I-IP detects an error, it activates an error signal which can be sent either to the processor or to the outside, depending on the preferred recovery scheme. Details about the architecture of the I-IP core can be found in reference [165].

Software modifications include the addition of control flow checking and data checking such as those described in section 14.

Available Test Data (simulations, radiation testing, in-flight)

The above described hybrid technique was implemented on a Virtex-II Pro FPGA using the embedded PowerPC [165]. Both the processor and the I-IP core work at 100 MHz. The implementation of the I-IP module requires 1366 slices, corresponding to about 10% of the target device's logical resources. Four applications were chosen as benchmarks (matrix multiplication, Fifth-order elliptical wave filter, Lempel-Ziv-Welch data compression algorithm and Viterbi Algorithm). Depending on the application, execution time, code size and data size are multiplied by a factor of two to three when applying the software hardening scheme.

Experiments based on 100.000 fault injections were performed. As a result, the hybrid technique reduces timeouts by a factor of 1.5 to 3. Moreover, no wrong answers are supplied by the processor (which is the case with the unhardened version of the software) and the I-IP core proved its efficiency by detecting all the faults.

Added value (efficiency)

- Mitigate SETs, SEUs and SEFIs
- This technique helps mitigating upsets in the configuration memory and in the user logic.

IC family	FPGAs
Abstraction level	HDL
Pros	Increased hardness to SET, SEU and SEFI
Cons	FPGA resource penalty: ~10% (I-IP core) Memory penalty: ~2x to 3x (code ad data size) Time penalty: ~2x to 3x
Mitigated effects	SET, SEU and SEFI
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	N/A

12.3.9 Scrubbing

Description of the concept/implementation

Spatial redundancy by itself is not sufficient to avoid errors in the SRAM-based FPGA. Indeed, it allows rejecting transients in the combinational logic and upsets in registers (see sections 12.3.1 and 12.3.2). However, the SRAM-based configuration memory of FPGAs is also sensitive to the effects of radiations, which may create a mutation of the application by changing, for example, the nature of a logical function implemented in a LUT. It is then mandatory to periodically reload the bitstream in order to avoid the accumulation of faults in the configuration memory. This continuous load of the

bitstream is called scrubbing. The scrubbing, as explained in Xilinx Application Notes 138 and 151 [166][167], allows a system to repair bit-flips in the configuration memory[10] without disrupting its operation. Configuration scrubbing prevents multiple configuration faults and reduces the time in which an invalid circuit configuration is allowed to operate.

As illustrated in Figure 12-15, the whole configuration memory of a Xilinx Virtex FPGA is divided into several frames representing the minimal amount of resources, which can be configured. Such structure allows reconfiguring either the full device (full scrubbing) or only a part of the design (partial scrubbing). The selection of the scrubbing mode mainly depends on the selected spatial redundancy scheme.

Nowadays, scrubbing has become the most important technique for improving reliability regarding radiation effects in SRAM-based FPGAs. This is due to the important size of the configuration memory compared to user flip-flops and embedded memory (the configuration memory for the Xilinx Virtex-6 family is about four to eight times larger than the user memory). However, it is important to notice that scrubbing is not sufficient to protect a SRAM-based FPGA from particle effects as it only avoids accumulation of faults in the configuration memories. Indeed, faults may occur between two scrubbings and provoke errors in the application until the next refresh of the configuration memory. Moreover, scrubbing cannot correct faults in user registers and in embedded RAM. Consequently, a TMR strategy should be used as a complement to scrubbing.

Full scrubbing

As explained in sections 12.3.1 and 12.3.2, local and global TMR require having frequent interconnections between the three replicas because of the TMR flip-flops. The consequence is that physical separation of the different replicas inside the FPGA is almost not possible and a partial scrubbing has, in this case, little interest. Full scrubbing is generally the selected method for local and global TMR.

Partial scrubbing

Large grain TMR (see section 0) is intended to have the three replicas physically separated inside the FPGA, only one final voter is common to the three replicas. Thus, partial scrubbing is advised as the voter is able to detect the faulty replica and can order the scrubbing supervisor to reconfigure only the part on the FPGA containing the error [168].

[10] including the memory cells that configure the LUT, the ones that control the routing and the CLB customization.

Figures/diagrams

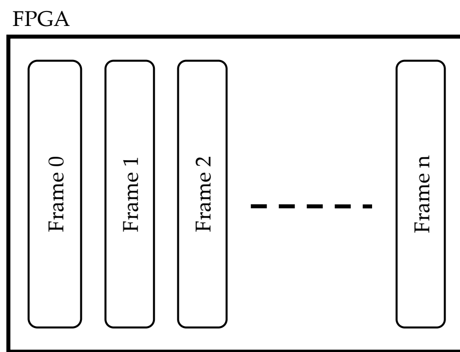


Figure 12-15 : Organization of the configuration memory for the Xilinx Virtex family

Example(s)

It is recommended to scrub at least 10 times faster than worst-case SEU rate. The frequency at which scrubbing must be performed depends on the particle flux and cross-section of the device.

Figure 12-16 illustrates a basic overview of a possible implementation for an SEU correcting design. The memory storing the FPGA configuration is connected to the Virtex SelectMAP[11] interface through a configuration controller. This controller features a memory interface, a Cyclic Redundancy Check calculator and comparator (see section 15.3.6) and a finite state machine to control the operations.

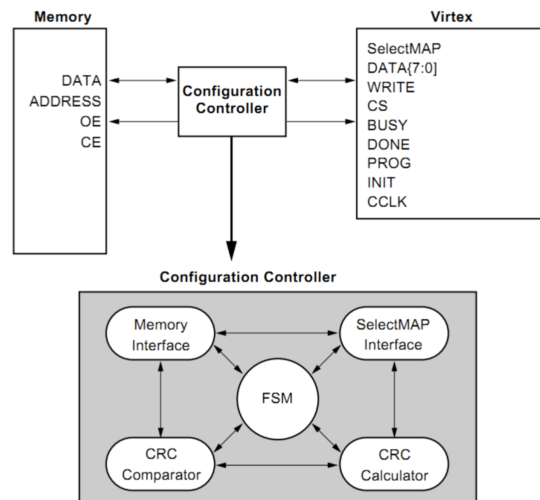


Figure 12-16 : Simple configuration and SEU correction design

For recent Xilinx FPGAs, the HardWare Internal Configuration ACcess Port (HWICAP) module can also be used to reconfigure parts of the configuration matrix from inside the FPGA controlled by the embedded processor (hard core Power-PC or soft core Microblaze). The ICAP is able to load partial bitstream without interrupting the application and to configure them. The ICAP module is connected to the embedded processor by the available local bus OPB and the EDK tool can be used for that task. The advantage of the feature is that the FPGA does not require any external supervisor to reconfigure itself.

[11] A parallel interface used to configure and readback the FPGA.

Available Test Data (simulations, radiation testing, in-flight)

In reference [169], two versions of the Microblaze soft core processor, with and without BRAM scrubbing (continuous external configuration scrubbing, functional-block design triplication and independent internal BRAM scrubbing, also triplicated), were implemented and tested using a proton beam of 63.3 MeV. The use of BRAM scrubbing to protect the code greatly reduced the occurrence of code corruption even at the accelerated fluxes used in beam testing.

Added value (efficiency)

- Prevent SEU accumulation in the configuration memory.
- On recent devices, scrubbing can be done from outside the FPGA. Moreover, on recent Xilinx devices scrubbing can be achieved from inside the FPGA using the HardWare Internal Configuration Access Port (HWICAP).
- No application interruption required.
- This technique helps mitigating upsets in the configuration memory and but not in the user logic.

Known issues (Weaknesses, elements to be considered)

- Scrubbing requires an external controller to perform the scrubbing process on devices not featuring an internal controller such as the ICAP provided by Xilinx since the Virtex-II.
- Scrubbing does not correct upsets in embedded memories (BRAMs) and in CLB's flip-flops as their content is dynamic and depends where the application is in its execution flow. A solution named BRAM TMR is recommended to cope with this issue (see section 0).
- Upsets occuring between two scrubbings may provoke errors. For this reason TMR must be implemented as a complementary technique to scrubbing.

IC family	SRAM-based FPGAs
Abstraction level	System architecture
Pros	Avoid fault accumulation in the configuration memory
Cons	May require an external controller
Mitigated effects	SEU, MBU/MCU
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

12.4 Vendor solutions

12.4.1 Microsemi's RTAX-S/SL antifuse-based FPGA

General characteristics

- 0.15 μm CMOS antifuse process technology [170]
- 7 metal layers
- 1.5 V core supply voltage
- Embedded memory
- 350 MHz

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-2: Suitable mitigation techniques for Microsemi RTAX-S/SL [170]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Not sensitive	None	None
Control logic	SET	None	Logic redundancy design
User flip-flops	SEU	Hard-wire triple redundant flip-flop	None
Embedded SRAM	SEU	• EDAC macro in FPGA design software (ACTgen) • Hamming code (detect 2errors and correct & error) • SECDED	EDAC at HDL-level

12.4.2 Aeroflex's UT6325 antifuse-based FPGA

General characteristics

- 0.25 μm ViaLinkTM epitaxial CMOS [171]
- 5-metal layers
- 2.5 V core supply voltage
- RadTol Embedded SRAM memory
- 120 MHz

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-3 : Suitable mitigation techniques for Aeroflex UT6325 [172]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Not sensitive	None	None
Control logic	SET	None	SET filtering with localized TMR in the flip-flops
User flip-flops	Not sensitive	Hardened memory cells (DICE)	None
Embedded SRAM	Not sensitive	Hardened by the manufacturer	None

12.4.3 Microsemi's ProASIC3/E flash-based FPGA

General characteristics

- 130 nm CMOS [173]
- 1.5 V core supply voltage
- 504 kbits SRAM embedded memory

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-4 : Suitable mitigation techniques for Microsemi ProASIC3/E [173]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Not sensitive	None	None
Control logic	design > 100 MHz: main effect SET	None	• SET filtering with localized TMR in the flip-flops or guard-gates • Global TMR, TMR IOBs in different banks
User flip-flops	design < 50 MHz: main effect SEU	None	Local TMR of the flip-flops + single voter
Embedded SRAM	SEU	None	TMR, EDAC at HDL-level

12.4.4 Atmel AT40KEL SRAM-based FPGA

General characteristics

- 0.35 μm CMOS [174]
- 3.3 V core and I/O supply voltage
- Up to 18 kbits of embedded SRAM-memory

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-5 : Suitable mitigation techniques for Atmel AT40KEL [174]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Not sensitive	Hardened memory cells	None
Control logic	SET	TMR	None
User flip-flops	Not sensitive	Hardened memory cells	None
Embedded SRAM	Not sensitive	Hardened memory cells	None

12.4.5 Atmel ATF280F SRAM-based FPGA

General characteristics

- 0.18 μm CMOS [175]
- 3.3 V core and I/O supply voltage
- Up to 115 kbits of embedded SRAM-memory

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-6 : Suitable mitigation techniques for Atmel AT40KEL [175]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Not sensitive	Hardened memory cells	None
Control logic	SET	TMR	None
User flip-flops	Not sensitive	Hardened memory cells	None
Embedded SRAM	Not sensitive	Hardened memory cells	None

12.4.6 Xilinx Virtex family SRAM-based FPGA (commercial grade)

General characteristics

- From 0.18-0.22 μm for Virtex-1 to 40 nm for Virtex-6 [176]
- From 2.5V for Virtex-1 to 1V for Virtex-6
- From 100kbits for Virtex-1 to 20Mbits for Virtex-6 of embedded SRAM-memory

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-7 : Suitable mitigation techniques for commercial Xilinx Virtex [176]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	SEU	None	• Global TMR • DTMR (distributed TMR)
User's combinational logic and user flip-flops	SET and SEU	None	Global TMR (XTMR), IOBs in different banks
Embedded SRAM	SEU	None	BRAM TMR
Power On Reset	SEFI	None	Reconfigure device
SelectMap and JTAG controllers	SEFI	None	Reconfigure device
PowerPC	SEFI, SEU, SET	None	• Software-level techniques • Power-PC redundancy with error detection and recomputation

12.4.7 Xilinx Virtex-5Q SRAM-based FPGA (defense grade)

General characteristics

- 65 nm CMOS [177]
- 1V core supply voltage
- 10Mbits embedded SRAM-memory

Sensitivity to SEEs and corresponding mitigation techniques

Table 12-8 : Suitable mitigation techniques for defense grade Xilinx Virtex [177]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	SEU	None	Scrubbing (TMR not possible because configuration cells are not accessible to the user)
User's combinational logic and user flip-flops	SET and SEU	None	• Global TMR, IOBs in different banks
Embedded SRAM	SEU	Embedded EDAC with parity checker and correction	None
Power On Reset	SEFI	None	Reconfigure device
SelectMap and JTAG controllers	SEFI	None	Reconfigure device
PowerPC	SEFI, SEU, SET	None	• Software-level techniques • Power-PC redundancy with error detection and recomputation

12.4.8 Xilinx Virtex-5QV SRAM-based FPGA (space grade)

General characteristics

- 65 nm CMOS [178]
- 1V core supply voltage
- 10Mbits embedded SRAM-memory

Radhard tolerance

- SEU Latch-up Immunity (LETTH) : > 100 MeV.cm^2/mg [178] [179] [180]
- Configuration Cell Upset Rate (GEO) : < 3.8 x 10^{-10} Upsets/Bit-Day
- Functional Interrupt Rate (GEO) : < 10^{-10} Upsets/Bit-Day
- Total Ionizing Dose : > 1 Mrad(Si)
- Dose Rate Upset : > 10^9 Rad(Si)/s

- Dose Rate Latch-up : > 10^{10} Rad(Si)/s

<u>**Sensitivity to SEEs and corresponding mitigation techniques**</u>

Table 12-9 : Suitable mitigation techniques for space grade Xilinx Virtex [178]

FPGA structures	Type of effects	Vendor's solutions	User's solutions
Configuration cells	Significantly reduced	DICE	GTMR or DTMR
User's combinational logic and user flip-flops	SET SEU	DICE	GTMR or DTMR Correct and mask
Embedded SRAM	SEU	Embedded EDAC with parity checker and correction	None
Power On Reset	SEFI reduced	None	Reconfigure device
SelectMap and JTAG controllers	SEFI reduced	TMR hardened logic and ECC protected registers	None

12.5 Device comparison for space applications

This section provides radiation ground test results for the devices presented in the previous section. Those data are issued from the manufacturer's datasheets and white papers.

Sensitivity to SEUs

The table hereafter summarizes results on the sensitivity to upsets measured for the embedded memory and the flip-flops of the different FPGAs. The saturated cross-section and the LET threshold characterizing the cross-section curve are provided followed by the error rate par bit for each device. The final error rate of an application implemented on a FPGA depends on the user's final design.

	Antifuse		Flash	SRAM		
	Aeroflex UT6325	**Microsemi RTAX-S/SL**	**Microsemi ProASIC3/E**	**Xilinx Virtex-4QV**	**Atmel AT40KEL**	**Atmel ATF280F**
Saturated cross-section (cm²/bit)						
Embedded memory	$2E^{-7}$	$4E^{-9}$	$4E^{-8}$	$3E^{-8}$	*No data*	$6.5E^{-8}$
Flip-flop	$5E^{-7}$	$1E^{-9}$	$2E^{-7}$	$7E^{-7}$	*No data*	*No data*
LETth (MeV.cm²/mg)						
Embedded memory	64	30	1	0.2	*No data*	*No data*
Flip-flop	42	37	6	0.5	*No data*	*No data*
Error rate per bit						
Embedded memory	$4.8E^{-11}$	$1.4E^{-12}$	$4E^{-8}$	$7E^{-7}$	*No data*	*No data*
Flip-flop	$2.8E^{-10}$	$7.0E^{-13}$	$5E^{-9}$	$2E^{-6}$	*No data*	*No data*

Sensitivity to TID and SEL

The table below presents TID and SEL sensitivity for the different FPGAs.

	Antifuse		Flash	SRAM		
	Aeroflex UT6325	**Microsemi RTAX-S/SL**	**Microsemi ProASIC3/E**	**Xilinx Virtex-4QV**	**Atmel AT40KEL**	**Atmel ATF280F**
TID (krad(Si))	300	300	< 40	300	300	300
SEL (MeV.cm²/mg)	< 120	< 117	< 96	< 125	< 70	< 80

13 Embedded memories

13.1 Scope

Memory cells (SRAM cells, latches, flip-flops, etc) are sensitive to the effects of radiation. Because most of digital designs include a huge number of memory cells, strategies based on spatial redundancy are often not adequate as they may not fit the hardware requirements. Alternative solutions present in the state-of-the-art can be classified in three categories.

Optimization of the cell layout

This category proposes fault mitigation by modifying the cell itself by several means:

- Adding resistors or capacitances on the feedback loop of the cell to increase its critical charge, and thus to increase its bit-flip threshold.
- Using specific transistor sizing. As a consequence, these cells do not scale easily as the device size is shrinking. The area cost of these cells may also be high.
- Increasing the number of nodes of the cell, and thus allowing easier scaling. These solutions also induce lower area and power penalties. These cells are usually based on two fundamental concepts: redundant storage of the information and feedback paths in order to restore the correct data.

Optimization of the memory layout

This relies on techniques devoted to mitigate multiple errors in memories by a specific arrangement of the memory cells within the chip.

Error Detection And Correction (EDAC)

This family of techniques aims at protecting the content of memory cells by the use of Error-Correcting Codes (ECC). ECC, also called Forward Error Correction (FEC), relies on adding redundant data, or parity data, to a piece of data, in such a way it can be recovered even when a number of errors (up to the capability of the code being used) occurs, either during the process of transmission, or on storage [181]. Error-correcting codes are frequently used in lower-layer communication, as well as for reliable storage in media such as CDs, DVDs, hard disks, and RAMs in order to reduce Soft Error Rate (SER).

Given that this set of techniques do not apply directly to the memory cell itself, but rather at a higher level of abstraction, these techniques are described at architectural level in section 15.3.6.

All the hereafter presented techniques have their advantages and penalties, hence none of them is a "perfect" solution. Depending on the desired level of robustness and the mission constraints, the designer may find the optimal solution by combining several of these techniques.

13.2 Table of effects vs mitigation techniques

Mitigation techniques		Abstraction level	Radiation effects		Page
			SEU	MBU	
13.3.1	Resistor memory cell	Design	X		135
13.3.2	Capacitor memory cell	Design	X		137
13.3.3	IBM hardened memory cell	Design	X		139
0	HIT hardened memory cell	Design	X		141
13.3.5	DICE hardened memory cell	Design	X		142
13.3.6	NASA-Whitaker hardened memory cell	Design	X		144
0	NASA-Liu hardened memory cell	Design	X		146
13.3.8	Scrambling	Architectural	X	X	147

13.3 Mitigation techniques

13.3.1 Resistive hardening

Description of the concept/implementation

Resistive hardening has been shown to be an effective way of increasing the SEU tolerance of SRAM cells. Resistive hardening involves the use of polysilicon intra-cell decoupling resistors (Figure 13-1) to slow the regenerative feedback response of the bistable flip-flop so that it can discriminate between a short upset-causing voltage transient and a longer legitimate write signal [118]. The decoupling resistors slow the regenerative feedback response of the cell, so the cell can discriminate between an upset caused by a voltage transient pulse and a real write signal. These extra resistors can be realized by passive components, for instance highly resistive polysilicon [182]. High value resistors can be implemented at the cost of a low silicon area increase. Moreover, DRAM-like stacked capacitors on top of the memory cell increase the decoupling capacitor without any area penalty [183].

Figures/diagrams

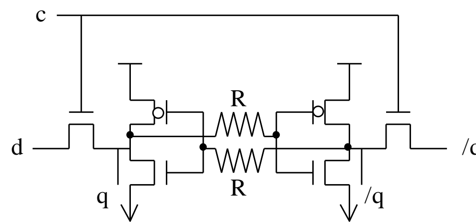


Figure 13-1 : Resistor memory cell

Example(s)

SEU tolerant memory cells protected by resistors were proposed for ASICs [184] and for FPGAs [185].

Available Test Data (simulations, radiation testing, in-flight)

- Reference [184] presents theoretical and experimental results performed on an improved version of the above presented resistor-based rad-hard memory cell. Samples using a 2 µm technology were manufactured in order to perform radiation ground testing. Results confirm the robustness with respect to SEU of the proposed memory cell hardened with resistors. The SEU sensitivity was about an order of magnitude smaller than the standard memory cells with the same transistor geometry currently employed in SRAM.
- According to reference [186], resistor-based rad-hard memory cells were proven to be immune to particles having LETs of about 45 MeV.cm^2/mg.

Added value (efficiency)

An important advantage of this structure is the low area penalty of the cell.

Known issues (Weaknesses, elements to be considered)

The main drawback of the above hardening approaches is that they require extra process steps, thus, having a non negligible impact on fabrication cost. In addition to the cost issue, implementing resistors often impacts the cell's speed and power.

Another issue reported in reference [184] is the large variation in the value of resistors across the wafer. As an example, the mean value was 13 kΩ but most samples were between 10 kΩ and 20 kΩ.

IC family	Memories
Abstraction level	Design
Pros	SEU robustness: LET_{th} up to 45 MeV.cm²/mg Little area penalty
Cons	Increased manufacturing cost
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection Spice simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.2 Capacitive hardening

Description of the concept/implementation

Capacitor memory cells are based on the same principle, increasing the critical charge, as the one used for resistor memory cells described in 13.3.1. Extra capacitances can be added either by using extra transistors and connecting their gates to the cell nodes (exploiting this way the gate capacitance of CMOS transistors), or by adding metal-metal capacitances on top of the cells. As an example, the SRAM-C cell is depicted in Figure 13-2 [187]. These techniques allow reducing of the SER rate at the cost of performance degradation, significant area increase and/or the loss of two metal layers on the top of the memory (for memory cells) or of the logic (for latches and flip-flops).

Figures/diagrams

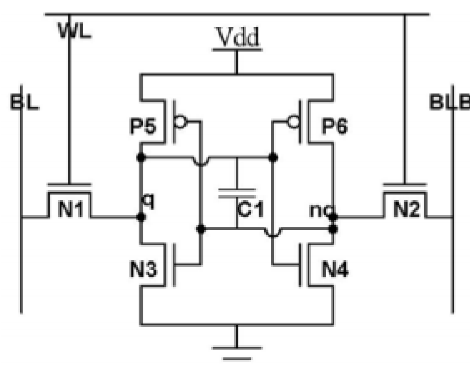


Figure 13-2 : Hardened SRAM cell using a capacitor (SRAM-C cell)

Example(s)

Reference [188] proposes an optimized structure, called SRAM-tct, in order to reduced the write time penalty introduced by the SRAM-C cell. As shown in Figure 13-3, this approach consists of a regular SRAM cell with an addition of two CMOS transistors connected in series with two NMOS transistors and a vertically stacked capacitor. The CMOS transistors act as switches to turn on and off the capacitor. The NMOS transistors that are connected to the WL (Write Line) signals are used to discharge the capacitor during a write phase when WL is high. During a standby mode the capacitor is connected to the SRAM cell and acts as a charge buffer. When a write mode is activated, the CMOS switch transistors isolate the capacitor from the SRAM cell. Simultaneously, the NMOS transistors discharge the capacitor by connecting both capacitor terminals to ground. Once the write mode is finished the capacitor is re-introduced into the system.

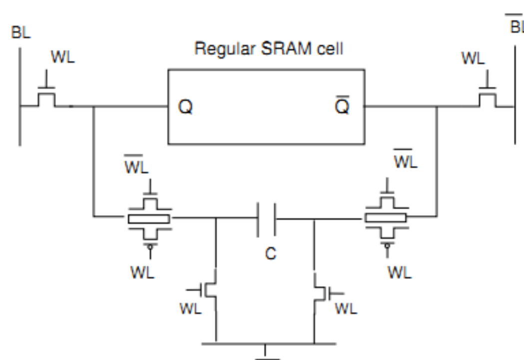


Figure 13-3 : The SRAM-tct cell

A 65 nm SRAM cells hardened by two capacitors were used to improve the SEU hardness in conjunction with the strong intrinsic TID hardness. Heavy ions testings confirmed that the higher the added capacitor per cell, the lower the SEU cross-section is. Using this 65 nm RHBD technique, electrical performances and radiation-hardness are both met. The calculated error rate shows a decrease of about 3 orders of magnitude [189].

Available Test Data (simulations, radiation testing, in-flight)

Reference [188] presents a performance comparison obtained from the simulation of three different memory cells: a standard SRAM, the SRAM-C cell and the SRAM-tct cell.

A first experiment focused on the write time penalty introduced by the two hardened cells compared to the standard SRAM. Simulations showed that writing a logical '1' into the standard SRAM required 0.13 ns while the same operation on the SRAM-C cell (with a 20 fF capacitor) required 1.14 ns. The SRAM-tct equipped with the same 20 fF capacitor performed the same write operation in 0.14 ns. Moreover increasing the capacitor value increased the write time in the SRAM-C but not on the SRAM-tct.

The second experiment concerned the evaluation of the critical charge, a direct indicator of the cell immunity to SEU, for each the three previously mentioned cells. Results showed that the SRAM-tct can achieve the same level of robustness than the SRAM-C using a smaller capacity value. As an example, the level of robustness reached by a 20 fF SRAM-C cell can be obtained by a 17 fF SRAM-tct cell (gain of 15%). Similarly the robustness achieved by a 2.5 fF SRAM-C cell is equivalent to the one reached by a 0.5 fF SRAM-tct cell (gain of 80%).

Added value (efficiency)

Improved SEU robustness.

Known issues (Weaknesses, elements to be considered)

Performance penalty: increased write time for the SRAM-C depending on the added capacitor value (see results from reference [188]).

IC family	SRAM Memories
Abstraction level	Design
Pros	Improved SEU immunity
Cons	Speed penalty
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection Spice simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.3 IBM hardened memory cell

Description of the concept/implementation

IBM hardened memory cell is protected by an appropriate feedback devoted to restore the data when it is corrupted by the consequent of an energetic particle [190]. The cell, illustrated in Figure 13-4, is composed of six transistors in charge of storing the data (identical to a standard cell), six extra transistors to provide robustness to SEU and four additional transistors for read/write operations (not shown on the figure).

Figures/diagrams

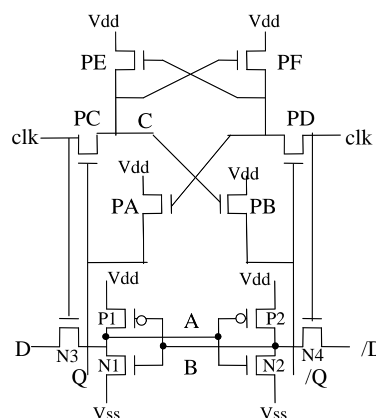


Figure 13-4 : IBM hardened memory cell

Available Test Data (simulations, radiation testing, in-flight)

Reference [190] presents experimental results for a shift register implementing 144 design-hardened latches and also unhardened-latches. An SEU threshold of 25 MeV·cm²/mg was observed for unhardened latches and no upsets were recorded for the hardened cells. However, no further details are provided about the hardened cells sensitivity threshold.

Added value (efficiency)

- No significant power consumption increase compared to the standard cell.
- Little performance penalty compared to the standard cell.
- Good SEU robustness.
- No specific process or design rules needed (RHBD solution).

Known issues (Weaknesses, elements to be considered)

- Area overhead: 100% (according to reference [191]).
- Increased transistor's size.

IC family	Memories
Abstraction level	Design
Pros	SEU hardness
Cons	Power consumption penalty: not significant Speed penalty: little Area penalty: 100%
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.4 HIT hardened memory cell

Description of the concept/implementation

The Heavy-Ion Tolerant (HIT) cell is composed of 12 transistors organized in two storage nodes interconnected by feedback paths [191] [192]. This cell offers a good robustness to SEU without degradation of electrical parameters and with reasonable silicon area overhead.

Figures/diagrams

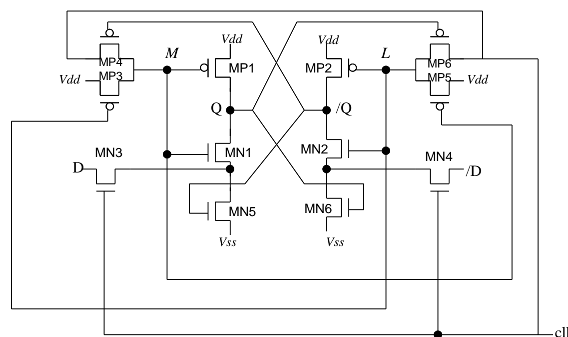


Figure 13-5 : HIT memory cell

Example(s)

- HIT cell was used in the space qualified high performance 32-bit floating point digital signal processor TSC21020E which is compatible with the ADSP-21020 from Analog Devices Inc [193].
- The TSC21020E was used in the Rosetta mission launched in 2004 and that is supposed to be landing in 2014 on the Churyumov Gerasimenko comet.
- HIT cell is included in the DARE library (see section 8.4.1) [83].

Available Test Data (simulations, radiation testing, in-flight)

According to experimental results provided in reference [191], HIT cell is less sensitive to upsets, at least by a factor of 10, than the standard SRAM cell. This immunity gain factor has been proved to be close to 5000 for particles having medium LET values (15 MeV.cm²/mg).

Added value (efficiency)

- Due to its specific architecture and transistor sizes, the HIT cell can be used without I/O buffers.
- Area penalty: ~10% compared to standard cell.
- No specific process or design rules needed (RHBD solution).

Known issues (Weaknesses, elements to be considered)

- Power consumption penalty: ~30% compared to standard cell.
- The HIT cell suffers from the drawback that the transistor sizes are critical in restoring the correct value after a SEU.

IC family	Memories
Abstraction level	Design
Pros	SEU hardness
Cons	Area penalty: ~10% Power consumption penalty: ~30%
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.5 DICE hardened memory cell

Description of the concept/implementation

The Dual Interlocked storage CEll (DICE) embeds 12 transistors for a memory cell structure [194] [114]. This cell, illustrated in Figure 13-6, consists in a symmetric structure of four CMOS inverters, where each inverter has the n-channel transistor and the p-channel transistor separately controlled by two adjacent nodes storing the same logic state.

It has no constraints on transistor sizing and is suitable for replacing both latches and flip-flops in ASICs' logic blocks.

Figures/diagrams

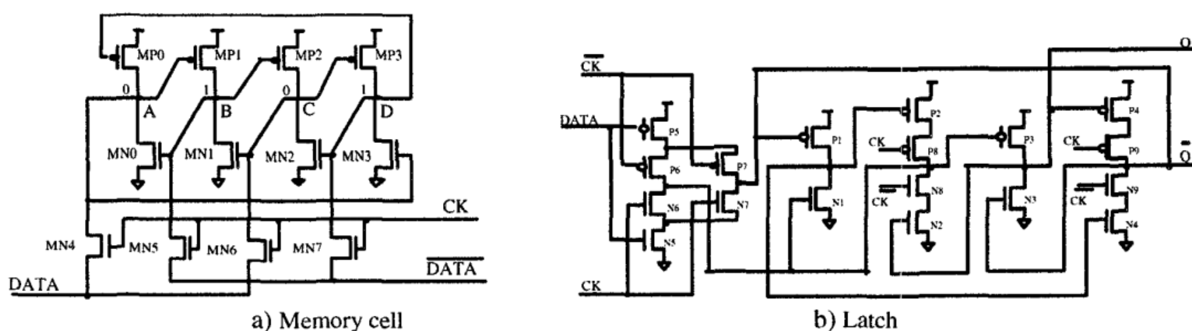


Figure 13-6 : DICE hardened cell structure

Example(s)

DICE cell is implemented in various hardened integrated circuits. One representative example is Aeroflex UT6325 [195].

Available Test Data (simulations, radiation testing, in-flight)

In reference [194] , are described two prototypes, a static RAM and a register array with DICE cells (see Figure 13-6) designed using a 1.2 μm CMOS/epi process. The first prototype is a 2 Kbit CMOS SRAM circuit composed of two l Kbit sections with standard 6-transistor SRAM cells and DICE cells. The second prototype chip comprises three shift registers. One of the registers is built from standard, unhardened latches. The other two registers use two different DICE cell designs, with and without constraints for transistor size and topology, respectively.

Experimental results were obtained at the 88-inch cyclotron of Lawrence Berkeley Laboratories, Berkeley, USA. A LET threshold of 50 MeV·cm²/mg was observed for the DICE cell while unhardened cell had a LET_{th} lower than 10 MeV.cm²/mg.

In reference[196] are provided evidence of the immunity to SEU of DICE cells. Test were performed in Brookhaven National Laboratorys Tandem Van de Graaff (TVG) Accelerator Facility, DICE-latch shift register chains were tested with Br, Ni, Cl, I, and Au at various angles to achieve an effective linear energy transfer (LET) range from 11 to 84 MeV cm mg. The components were tested under nominal voltage conditions and at room temperature. Under static operating conditions this DICE-based latch structure is completely SEU immune.

Added value (efficiency)

Power consumption penalty: low

Known issues (Weaknesses, elements to be considered)

Charge sharing increases the vulnerability of DICE cells to SEUs. Nodal separation can be used to reduce charge sharing and thus significantly increases LET threshold [197].

IC family	Memories
Abstraction level	Design
Pros	Power consumption penalty: low
Cons	*No data available*
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.6 NASA-Whitaker hardened memory cell

Description of the concept/implementation

The Whitaker cell is based on the data storage redundancy principle combined with feedback paths in order to restore the correct value in the corrupted node of the cell. This structure, illustrated in Figure 13-7, was first implemented in a Reed Solomon Encoder designed for the Space Station and Explorer platforms [198] [199] [186].

This cell is independent of the manufacturing process and presents no serious degradations. The hardening is accomplished through the design of a new structure and by ratioing the strengths of transistors within the cell.

Figures/diagrams

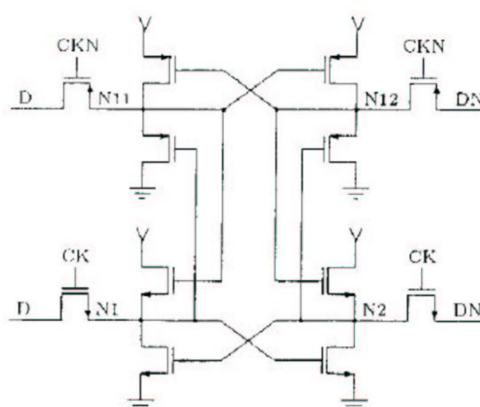


Figure 13-7 : NASA-Whitaker hardened memory cell

Example(s)

This cell was used to implement a D flip-flop in the control section of a Reed Solomon Encoder. The encoder chip containing this SEU immune cell was manufactured using commercial foundries at Hewlett Packard's Circuit Technology Group. This encoder was designed to be used in the NASA XTE (X-Ray Timing Explorer) and EUVE **(**Extreme-Ultraviolet Explore**)** missions as well as in the Space Station [198].

Available Test Data (simulations, radiation testing, in-flight)

Experimental results were conducted at Brookhaven National Labs, Brookhaven, USA on prototype ICs consisting of five shift registers. Three of the shift registers used Flip-Flops created from the memory cell of Figure 13-7 while the other two were standard shift-register designs used as a reference.

Experiments were conducted using several ion species beamed at various angles. The LET was steadily increased from 20 to 120 MeV·cm²/mg over the course of the experiment. The non-hardened designs exhibited upsets under every condition. The SEU threshold of the hardened designs was higher than 120 MeV·cm²/mg. No latchup was observed in any of the parts subjected to radiation, demonstrating an SEL threshold in excess of 120 MeV.cm²/mg.

Added value (efficiency)

This cell uses standard size transistors.

Known issues (Weaknesses, elements to be considered)

High power consumption penalty.

IC family	Memories
Abstraction level	Design
Pros	SEU hardness
Cons	Power consumption penalty: high
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.7 NASA-Liu hardened memory cell

Description of the concept/implementation

This cell, illustrated in Figure 13-8, is an improvement of the Whitaker's SEU hardened CMOS memory cell [199]. This development focused on correcting the power consumption issue on the NASA-Whitaker cell.

Complementary transistors have been inserted between the power supply Vdd (Vss) and n-type (p-type) memory structures. These transistors do not affect the SEU sensitivity of the memory cell. Hence, the DC path in this cell can be disconnected, thus eliminating power consumption.

Figures/diagrams

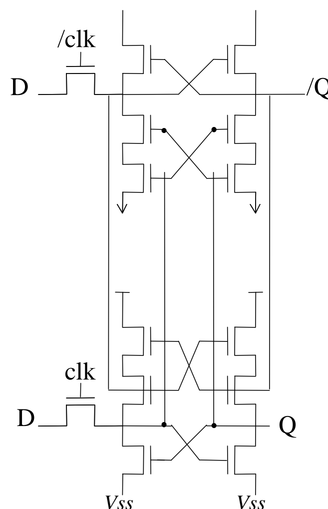


Figure 13-8 : NASA-Liu hardened memory cell

Example(s)

In addition to several test chips, three "full function" rad-tolerant VLSI processors have been developed at the NASA Institute for Advanced Microelectronics using the Liu cell for SEU immunity.

- a Error-correcting code (ECC) encoder that supports the Reed-Solomon (RS 16) for Telemetry Channel Coding
- programmable Reed-Solomon ECC encoder/decoder (EDAC). This chip has been designed into solid-state recorders in support of EOS-AM, LandSat 7, and the Hubble '97 Upgrade Package
- a 1024 channel autocorrelator chip used in the Naval Research Laboratories (NRL) Orbiting High Frequency Radio Interference Monitor (OHFRIM) experiment [200].

Available Test Data (simulations, radiation testing, in-flight)

Experimental results were obtained at Brookhaven National Laboratories. Experiments were conducted using Ni and Si ions beamed at various angles. No disruptions in shift register functionality were observed below 30 MeV.cm²/mg. However, above 30 MeV.cm²/mg, the test chip latched up [199].

Added value (efficiency)

This cell uses standard size transistors.

Known issues (Weaknesses, elements to be considered)

The number of transistors required for the SEU-hardened data latch shown make it impractical for large static memory arrays. However, the design can easily be used to create SEU-hardened master-slave D-flip flops to design finite state machine controllers and other data path elements.

IC family	Memories
Abstraction level	Design
Pros	SEU hardness
Cons	*No data available*
Mitigated effects	SEU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	N/A
Vendor solutions	N/A

13.3.8 Scrambling

Description of the concept/implementation

Error Detection And Correction (EDAC) algorithms allow detecting and correcting a number of errors depending on the number of used redundant bits. Commonly used EDAC scheme (see section 15.3.6), such as Hamming codes, are able to detect two errors and correct one error in a single data word. Nevertheless, transistor scaling down increases the risk to obtain MBUs and thus brings a new challenge for error correcting codes. However, detecting and correcting more faults in a single word is possible but it requires more hardware which is what designers want to avoid. Scrambling or interleaving means that the logical structure, as seen by the user from the outside of the chip, differs from the physical or topological internal structure of the chip. In other words, logically adjacent addresses may not be physically adjacent (this is called address scrambling) and that logically adjacent data bits are not physically adjacent (this is called data scrambling) [201].

Figure 13-9 is an illustration of a particle generating charges which may be collected by four adjacent memory elements. In this case, there is a probability to get two upsets in word 0 and word 1. In such conditions, common error correcting codes are able to detect both errors but not to correct them. On the other hand, in a memory embedding data scrambling (as shown on Figure 13-10), a unique particle cannot provoke MBUs and error correcting codes are able to handle the threat.

Figures/diagrams

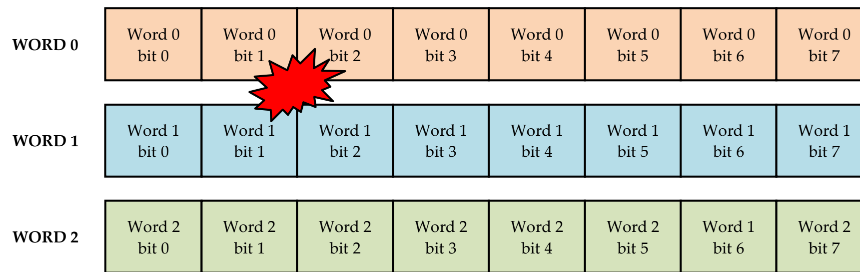


Figure 13-9 : Standard memory topology

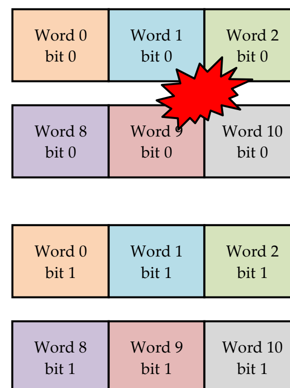


Figure 13-10 : Example of memory topology with scrambling

Example(s)

A SRAM memory with bit-scrambling processed in commercial 65 nm CMOS technology is presented in reference [202].

Available Test Data (simulations, radiation testing, in-flight)

Experimental test results with neutron and alpha particles, presented in [202] show that no MBU were detected as the tested memory uses scrambling.

Experimental results obtained in a SRAM 150 nm device, presented in [203] show that the adopted interleaving leads to a MBU reduction of more than 98% [203].

Added value (efficiency)

- Address decoder optimisation [201]
- Contact and well sharing [201]

Known issues (Weaknesses, elements to be considered)

In some cases, it may negatively impact floorplanning, access time, and/or power consumption [204].

IC family	Memories
Abstraction level	Design
Pros	Avoid MBU
Cons	*No data available*
Mitigated effects	MBU
Suitable Validation methods	Accelerated ground tests
Automation tools	N/A
Vendor solutions	N/A

13.3.9 Error Correcting Codes

Description of the concept/implementation

Memory may provide increased protection against soft errors by relying on error correcting codes. Such error correcting memories, known as ECC or EDAC-protected memories is particularly suitable for high fault-tolerant applications, such as space applications due to increased radiation. Error correcting memory controllers generally use Hamming codes, although some use tripe modular redundancy.

ECC is a widely used technique to protect SRAM despite the surface loss and higher power consumption.

The Error Correcting Codes technique, figures and diagrams, available test data, added values, known issues and references are detailed in section 15.3.6.

Example

The LEON2-FT (AT697) design is made of 0.18 μm CMOS process of ATMEL and reaches a frequency of 100MHz. The large embedded memory blocks used for the register files, the data and instruction caches are very sensitive to SEU, especially with a higher frequency of operation that increases the probability to latch SETs.

Among the error mitigation techniques applied to the LEON2-FT, the following are linked to the memory blocks:

- EDAC protection on the register file (7-bit EDAC checksum) every time a fetched register value is used in an instruction. If a correctable error is detected, the erroneous data is corrected before being used. At the same time, the corrected register value is also written back to the register file. A correction operation incurs a delay 4 clock cycles, but has no other software visible impact.
- EDAC protection on external memory interface.
- Parity protection on instruction and data caches: The cache parity mechanism is transparent to the user, but in case of a cache parity error, a cache miss is generated and an access to external memory is performed to reload the cache entry, implying some delay.

Radiation Performance

– Total dose radiation capability (parametric & functional): 60 krads (Si)

– SEU error rate better than 1 E-5 error/device/day

– No Single Event Latchup below a LET threshold of 70 MeV.cm2/mg

Ref: ATMEL Rad-Hard 32 bit SPARC V8 Processor AT697E, Atmel, rev 5 Aug.2011

http://www.atmel.com/dyn/products/product_docs.asp?category_id=172&family_id=641&subfamily_id=1478&part_id=3178

13.4 Comparison between hardened memory cells

Table 13-1 summarizes the main characteristics, advantages and drawbacks for the previously presented SEU hardened memory cells.

Table 13-1 : Comparison between state-of-the-art SEU hardened memory cells

Cell names	Number of transistors	Advantages	Drawbacks
IBM memory cell	16 (6 transistors for memory part, 6 transistors for SEU hardening and 4 transistors for read/write)	• Low static power consumption • SEU LET_{th}: 74 MeV.cm²/mg	• Large number of transistors • Size of the transistors
HIT memory cell	12 (two storage structures interconnected by feedback paths)	• Small number of transistors • SEU LET_{th}: 52 MeV.cm²/mg (less sensitive at least by a factor of 10 comparing to unhardened cell)	*No data available*
DICE memory cell	12 (symmetric structure of four CMOS inverters)	• Small number of transistors • Low power consumption • SEU LET_{th}: 50 MeV.cm²/mg	*No data available*
NASA-Whitaker memory cell	16 (constructed of two parts: p-channel transistors in top half part and n-channel transistors in bottom half part)	• SEU LET_{th}: 120 MeV.cm²/mg	• Large number of transistors • Size of the transistors • High static power consumption
NASA-Liu memory cell	14	• Low static power consumption • Reduced number of transistors	• Size of the transistors • Above 30 MeV.cm²/mg the test chip latched up

14 Embedded software

14.1 Scope

For processor-based architectures, when hardware redundancy is limited or not affordable at all, temporal redundancy can be a viable solution to deal with non-destructive SEEs. The general idea is to execute the parts of the application software several times on the same processing unit before comparing the results. The key points of this methodology are a limited hardware overhead but a significant time overhead. The software needs to be modified to apply the technique which is not applicable for all types of software (e.g. software must not use interrupts or dynamic memory allocation). As dynamic memory allocation is avoided in space software application, the only limitation is related with the use of interrupt signals. Usually, interrupt signals are not used on payload computers to guarantee static sequencing. However, some of the solutions described in the following are compatible with the use of interruptions and thus are suitable for applications such as command/control computers which are generally based on interrupt signals.

The term Software-Implemented hardware Fault Tolerance (SIFT) refers to a set of techniques that allows a piece of software to detect and possibly to correct faults affecting the hardware on which the software is running.

SIFT can be applied to Commercial-Off-The-Shelf (COTS) processors, or Intellectual Property (IP) processors, which either do not embed any detection/correction technique for the faults of concern, or to integrate the existing detection/correction features to further extend the robustness of the system, in case the budget constraints of the application (e.g., power consumption, or area occupation) are such that hardware-based redundancy, like Triple Modular Redundancy (TMR), cannot be adopted.

SIFT provides support by implementing an active redundancy scheme:

a. The software running on the faulty hardware detects the occurrence of misbehaviours, with the possible support of an additional hardware module different from that running the software (e.g., a watchdog timer implemented on a dedicated chip working in parallel with the processor running the SIFT-enabled software).

b. Suitable actions are initiated for removing the fault from the hardware, and bring the system back to a healthy state (e.g., by roll-back the system state to a known good state previously saved).

The common denominator to all SIFT techniques is to insert in the original program code redundant instructions allowing fault detection. Transients and upsets being the considered types of faults, redundancy is obtained by selectively duplicate computations and by inserting consistency checks to detect differences among the computations. Duplication can be performed at different levels of granularity:

- Instruction-level redundancy applies on statements of the program source code, and inserting consistency checks that work on the output of pairs of replicated statements.
- Task-level redundancy applies on each task composing the program, and in placing consistency checks that works on the output of pairs of replicated tasks.
- Application level redundancy can be applied when the program source code is not available like it is often the case for third-party software such as special libraries or operating systems.

14.2 Table of effects vs mitigation techniques

Mitigation techniques		Radiation effects				Page
		SET	SEU	MBU	MCU	
14.3.1	Redundancy at instruction level	X	X	X	X	153
14.3.2	Redundancy at task level	X	X	X	X	159
14.3.3	Redundancy at application level	X	X	X	X	163

Note 1: Software level techniques are applied at a high level of abstraction. Consequently, they cannot determine the source of the errors (SET or SEU) but they can only notice their impact on the computation.

Note 2: These techniques generally protect from SETs occurring in combination logic but not from SETs in the clock tree or on the reset line. However, DMT and DT2 solutions, presented in the following, may detect and recover from SETs occurring in the clock/reset lines.

14.3 Mitigation techniques

14.3.1 Redundancy at instruction level

Description of the concept/implementation

Time redundancy scheme can be chosen as a viable solution whenever redundant processing units are not affordable. This technique consists in executing consecutively the same operation several times and then comparing the results. Given that only one processing unit is available, proposed solutions mainly rely on software techniques.

The general concept of temporal redundancy consists in executing an instruction n times and then comparing the results. A potential error occurring during one of the executions would hence be detected. When $n = 2$ it is possible to detect faults, but not to correct them. In this case a third computation is required in order to determine the correct result. If $n \geq 2$, faults can be detected and corrected.

Figure 14-1 illustrates the mechanism when $n = 3$. A unique processor executes successively three identical instructions (called A1, A2 and A3). The three obtained results are then compared, and the correct one is stored before moving to the following set of three identical instructions (called B1, B2 and B2) and so on.

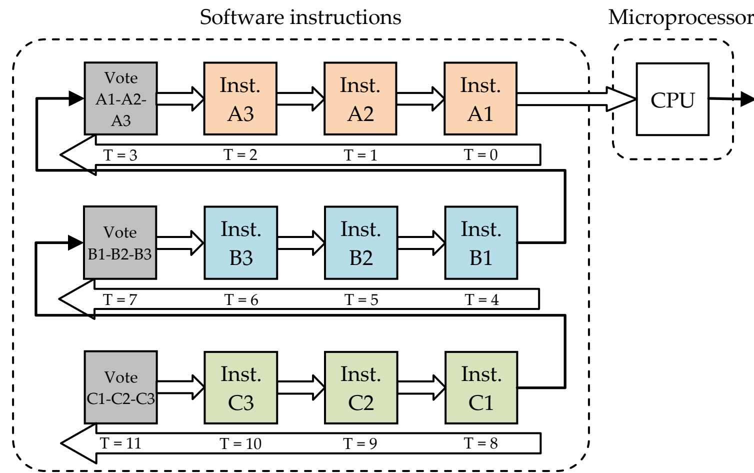


Figure 14-1 : Time redundancy at instruction level

General idea:

The general idea of time redundancy at instruction level relies on detecting faults in the data by systematically applying the following coding rules:

- All the data structure in the original software must be duplicated, obtaining a SIFT-enabled software having two replicas R0 and R1 of each data structure.
- All the write operations to a data structure in the original software must be duplicated, so that both replicas R0 and R1 are updated.
- Arithmetic, logic and Boolean statements must be replicated.
- All the data structures involved in read operations must be checked for consistency by testing whether R0 and R1 match, after each read operation.

It must be noticed that specific ordering of the instructions must be respected. As a result, very aggressive optimization techniques implemented by compilers (like GCC – GNU Compiler Collection) can produce an executable code where either the needed instruction sequencing is compromised, or redundancy removed. To overcome this problem, two solutions are possible:

- In case SIFT, for data faults, is exploited on a high-level language, such as C, compiler optimization must be disabled. The obtained executable code will retain the needed redundant instructions, and will preserve the needed ordering, however its performance is likely to be in the worst-case 10x lower than that of the original software compiled with optimization. Despite the performance penalty, the advantage of this solution lies in the portability of the SIFT-enabled code, which can be reused on different processors with very low implementation efforts. Moreover, coding rules can be applied manually on highly readable code, although a source-to-source compiler that takes care of SIFT implementation can greatly improve the quality of the obtained software.
- In case high performance is mandatory, SIFT for data faults can be applied on the intermediate code (RT-code) produced by the compiler after optimization took place. In this case, redundancy is introduced after the optimization process, and therefore it will be preserved by the following phases needed to generate the executable code. The major drawback of this approach lies in the need for a software tool for code modification, as SIFT coding rules can be hardly applied manually on RT level code, which is very close to assembly code.

A further consideration should be devoted to third-party code[12], only available under the form of library (e.g., library for floating point emulation, or operating system). As SIFT coding techniques mandate the access to either the high-level or RT-level source code, they cannot be applied to third-party software when only the binary code is available. In some cases, task-level redundancy can be adopted, as for example in the case when third-party libraries are used.

Other restrictions apply to dynamic memory allocation, and floating point:

- To successfully use SIFT techniques, it is recommended to avoid dynamic memory allocation. In a SIFT program, the two replicas of a dynamic structure can be allocated by calling sequentially the `malloc()` function or equivalent, thus obtaining two different addresses. As this function is a part of the C library, or equivalent, SIFT cannot be applied over it, and very limited detection capabilities are available to handle possible faults arising during the execution of the memory allocation function. In case `malloc()` returns a `NULL` pointer, error detection is possible, however, an unexpected side effect can be produced in case the returned address is not valid (e.g., the returned address points to a portion of the program stack).
- As far as floating point is considered, particular care must be placed in the consistency check function as rounding errors may apply. As a result, a threshold based acceptance test should replace consistency checks based on binary equivalence of results (e.g., the two replicas of the same data are considered identical if they differ no more than a given quantity ε).

Commercial products are available from SpaceMicro Inc. which offers single board computers (the Proton product family) based on commercial-of-the-shelf processors, where techniques for data faults (and others for execution flow faults) are implemented by means of a custom compiler, while a dedicated radiation hardened core implements Single Event Functional Interrupt (SEFI) (see 5.4.3.4) detection and recovery mechanisms (see example 4).

Fault coverage:

SIFT techniques are able to detect 100% of Single Event Upsets resulting in data used by the application (for instance, in a register in the processor, a word in the cache memory, or in the main memory). However, there are many common elements to the 4 instructions (triplication + voting) and thus, an error occurring on them (such as the comparison instruction or an error propagating between the four instructions) may not be detected.

Optimizing instruction-level redundancy:

Although effective from the fault detection point of view, instruction-level SIFT introduces significant time overhead due to both the duplication of operations, corresponding to an 2x execution time increase, and the need for disabling compiler optimizations, which can bring up to a 10x execution time increase.

In order to optimize the performance of the SIFT-enabled software, consistency checks can be delegated to the external hardware already implementing the SEFI error detection mechanisms, resulting in a system architecture illustrated in Figure 14-2 and composed of:

- Processor, memory and I/O, where the SIFT-enabled software runs.
- A smart watchdog in charge of managing the watchdog timer, and running the consistency checks that SIFT techniques requires for data and execution flow faults.

Consistency checks needed for data fault detection can be accelerated as follows:

[12] Software developed by someone else.

- All the data structures in the original software are duplicated as explained above. The two replica R0 and R1 are placed in memory in two different areas at a known offset `DELTA`, so that every data at address `X` in R0 has its replica at address `X+DELTA` in R1.
- All the operations are duplicated as explained above.
- The smart watchdog is inserted between the processor and the main memory, so that every read/write operation is monitored. Every time a data is read/written from/to memory, the target address and the associated data are stored in the smart watchdog in a Context Addressable Memory (CAM). After a new entry is added, the smart watchdog looks for the corresponding entry in the CAM, and if found it compares the associated data. In case of mismatch, a data fault is detected and a corrective action initiated.

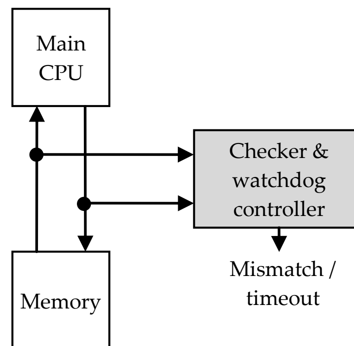


Figure 14-2 : Optimized architecture for temporal redundancy applied at instruction level

Consistency checks needed for execution flow fault detection can be accelerated by delegating to the smart watchdog the computation of the operations needed by the test and set functions, and by replacing them in the SIFT-enabled software with write operations sending the signature and the basic block identified to the smart watchdog.

By exploiting these approaches, the time overhead due to instruction-level redundancy is about 2.5x.

As an example, the fragment of C code reported in Figure 14-3 is considered.

```
00: #define N     100
01: int a[N];
02: int b[N];
03: int c[N];
04:
05: void main( void )
06: {
07:   int   i;
08:
09:   // a and b are initialized with input data
10:
11:   for( i = 0; i < N; i++ )
12:   {
13:         c[i] = a[i]*b[i];
14:   }
15: }
```

Figure 14-3 : Example of code

The code presented in Figure 14-4 implements the above described technique. All data structures (arrays and variables) are duplicated, and all the statements are duplicated. It must be noticed that complex statements such as on line 11 of Figure 14-3 may contain read and write operations, and therefore the proper rules must be applied. In the case of line 11 of Figure 14-3, two write operations are inserted in the SIFT-enabled code (lines 19 and 20 of Figure 14-4); the Boolean statement is duplicated (line 22 of Figure 14-4); involved variables are checked after every read operation (lines 24 and 36 of Figure 14-4) by inserting the consistency check in every possible path in the program stemming from the read statement. In the case of the statement of line 22 of Figure 14-4, the execution flow can proceed to line 24 or line 36, depending on the outcome of the Boolean statement where `i0` and `i1` are read. As a result, the consistency check stemming from the read operation of `i0` and `i1` must be duplicated.

```
00: #define N     100
01:
02: // replica R0
03: int a0[N];
04: int b0[N];
05: int c0[N];
06:
07: // replica R1
08: int a1[N];
09: int b1[N];
10: int c1[N];
11:
12: void main( void )
13: {
14:   int   i0;
15:   int   i1;
16:
17:   // a and b are initialized with input data
18:
19:   i0 = 0;
20:   i1 = 0;
21:
22:   while( i0 < N && i1 < N )
23:   {
24:         CONSISTENCY_CHECK( i0, i1 );
25:         c0[i0] = a0[i0]*b0[i0];
```

```
26:         c1[i1] = a1[i1]*b1[i1];
27:
28:         CONSISTENCY_CHECK( i0, i1 );
29:         CONSISTENCY_CHECK( a0[i0], a1[i1] );
30:         CONSISTENCY_CHECK( b0[i0], b1[i1] );
31:
32:         i0 = i0+1;
33:         i1 = i1+1;
34:         CONSISTENCY_CHECK( i0, i1 );
35:    }
36:    CONSISTENCY_CHECK( i0, i1 );
37: }
```

Figure 14-4 : Example of code with instruction level redundancy

Detailed information can be found in references [205], [206], [207] and [208].

Example(s)

Example 1: Error Detection by Duplicated Instructions

The Error Detection by Duplicated Instructions (EDDI) approach developed by Stanford University [209], is another example of time replication at instruction level. The EDDI microprocessor is based on a R3000 instruction set (IDT-3081 COTS processor). The Control Flow Checking by Software Signatures (CFCSS) technique was developed in order to enhance the detection of errors in the control-flow. Results obtained onboard a satellite can be found in the “available test data” section below.

Example 2: Time-Triple Modular Redundancy

The Proton platform, by Space Micro, implements a technique, called Time Triple Modular Redundancy, combining spatial and temporal redundancy. This platform is detailed in section 15.4.1.

Available Test Data (simulations, radiation testing, in-flight)

The EDDI approach was implemented on the ARGOS large satellite for USAF (launched in 1999). EDDI was able to detect 321 errors during a 350-day operational period. 98.7% were corrected [210].

The Proton200k single-board computer from Space Micro, implementing a TTMR and a real-time processor functionality monitoring, offers the following performances with respect to radiation [211]:

- TID > 100 krad (Si) (orbit dependent)
- SEL_{th} > 70 MeV.cm^2/mg
- SEU < 10^{-4} (orbit dependent)
- 100% SEFI mitigation

Added value (efficiency)

Area overhead resulting by the use of the external checker and the watchdog is negligible.

Known issues (Weaknesses, elements to be considered)

- Not compatible with third-party libraries, OS
- Errors during interrupt processing may not be detectable
- Heavy software modifications

IC family	Microprocessors
Abstraction level	Software
Pros	Fault coverage: 100% for data, >95% for execution flow
Cons	Memory overhead: >2x Time overhead: 2.2x-4.5x Not compatible for applications using interrupts Errors on clock/reset signals not detectable
Mitigated effects	SET, SEU and MBU/MCU
Suitable Validation methods	Ground accelerated tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	Space Micro Proton platform (100k, 200k, etc)

14.3.2 Redundancy at task level

Description of the concept/implementation

Task-level redundancy exploits a duplication scheme with a level of granularity much coarser than instruction-level redundancy. Applications must be split in three tasks:

- Data acquisition task, during which input data are collected.
- Data processing task, during which computation takes place.
- Data presentation task, during which data are issued to the end user.

Redundancy is applied at task level, and consistency checks are inserted at task level, so that acquired data are compared before starting data processing, and produced results are compared before starting data presentation. A scheduler orchestrates the overall operation, as illustrated in Figure 14-5.

Task-level redundancy is potentially less expensive to implement than instruction-level redundancy, as modifications are applied at function level. Moreover, a single technique provides coverage for both affecting data and execution flow faults. It is compatible with third-party code as libraries, and compiler optimizations can be exploited, as task-level redundancy does not require any specific ordering of instructions.

Task-level redundancy has the same limitations than instruction-level redundancy with respect of interrupt and trap handling.

When implementing task redundancy, particular care must be placed to the following aspects:

- As consistency checks are performed at task completion, faults are potentially detected with higher latency than in the case of instruction-level redundancy. As a result, fault effects may propagate in the system for a longer period of time, and they may affect multiple computations. By letting the fault effects propagating in the system, it is possible to have the corruption of both replicas of the same output. In case the fault effect is such that both the replicas bear the same faulty result, the detection mechanism will not be able to recognize the presence of the fault. As a result, in order to successfully implement task redundancy a memory protection unit (MPU), or a memory management unit (MMU) is needed so that:
    1. Data memory is partitioned in two not overlapping sections, R0 and R1.
    2. The first instance of each task works on R0, while the MPU/MMU forbids any access to R1.
    3. The second instance of each task works on R1, while the MPU/MMU forbids any access to R0.
- Consistency checks are potential single points of failure, as they access to both replicas R0 and R1. As a result, they should be implemented resorting to a comparator module working in parallel with the SIFT-enabled system, for example embedded in the smart watchdog implementing SEFI detection (Figure 14-6).

Figures/diagrams

```
00: acquire( *data )                // data acquisition task
01: process( *input, *output )      // data processing task
02: present( *data0 )               // data presentation task
03:
04: void scheduler( void )
05: {
06:   acquire( data0 );
07:   acquire( data1 );
08:   CONSISTENCY_CHECK( data0, data1 );
09:
10:   process( data0, result0 );
11:   process( data1, result1 );
12:   CONSISTENCY_CHECK( result0, result1 );
13:
14:   present( data0 );
15: }
```

Figure 14-5 : Task-level redundancy

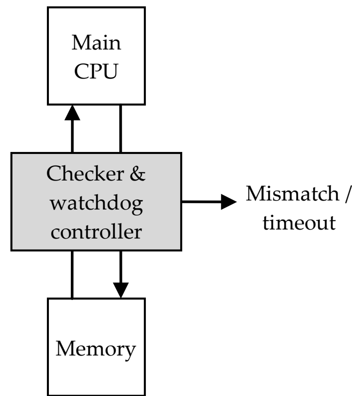


Figure 14-6 : Architecture for temporal redundancy applied at task level

Example(s)

DMT (*Duplex Multiplexé dans le Temps*, i.e. duplex in time) is a CNES patented architecture [212] [213] [214] [215] aiming at, but not limited to, scientific missions and small satellites [216]. It is based on time replication of operational tasks. In DMT architecture (Figure 14-7), each task is successively executed twice, each execution being called "virtual channel".

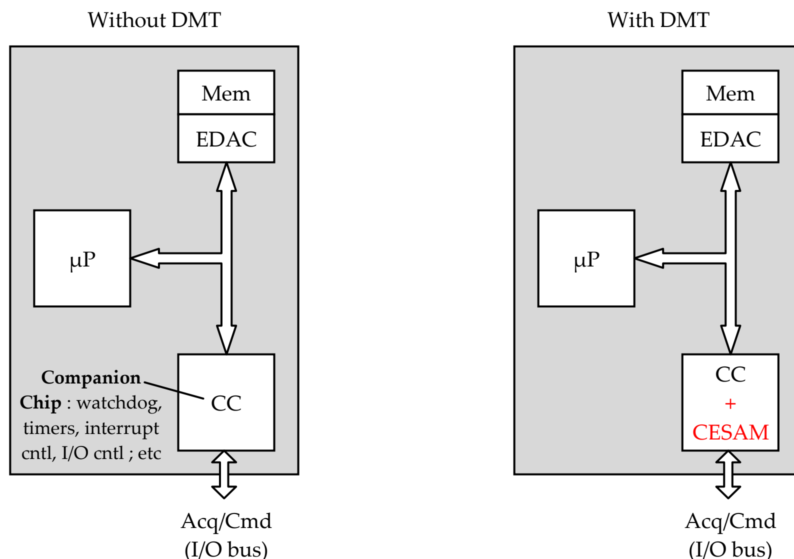


Figure 14-7 : DMT architecture

In conventional space architecture, inputs are read from sensors during acquisition phase, then data are processed and commands to actuators might be output during the whole processing phase. DMT differs in the way that processing and output phases are two different phases (Figure 14-8).

If some sensors are implemented with COTS components, it is possible to protect them against SEU/SET, depending on the sensor type, thanks again to fault detection of the IN phase based on time replication. Then, threshold based comparison allows consistency checking.

Error detection for the processing phase is based on a bit-to-bit comparison after each pair of executed tasks. Only major results, such as commands to actuators, other task's parameters, etc, are compared. Variables related to the local task are not checked, thus reducing the amount of data to be processed.

A duplex architecture is mainly a fail-stop architecture as it is able to detect faults but not to recover them. Thus, specific recovery mechanisms based on a safe context storage independent for each virtual channel are implemented in DMT:

- The external memory is considered as SEU-free as it is protected by EDAC.
- Memory accesses are protected by a hardware support mechanism, called CESAM, implemented inside a SEE-free FPGA or ASIC and operating as a Memory Management Unit (MMU).

Two recovery modes are implemented: "forward recovery" (the faulty applicative task is skipped and the program execution jumps to next applicative task), and "backward recovery" (the faulty applicative task is processed again). Then a mix of the two recovery modes will be well suited in the same application software, where some scientific tasks can be satisfied with the simpler "forward recovery", and the other tasks specifically control-command tasks will require the more time-consumming "backward recovery". During a recovery phase, no data exchange is required between the two virtual channels as each one has its own safe context storage inside a CESAM protected part of the memory to avoid fault propagation between channels.

It should be noticed that the DMT architecture described in the present section maximise the software implementation; a new version, reusing the harware fonction CLOPES (including an hardware comparator and an input-output controller) developed for DT2 architecture (see 15.3.4), allows to reduce the software impact of the fault protection, and to increase the reachable fault coverage.

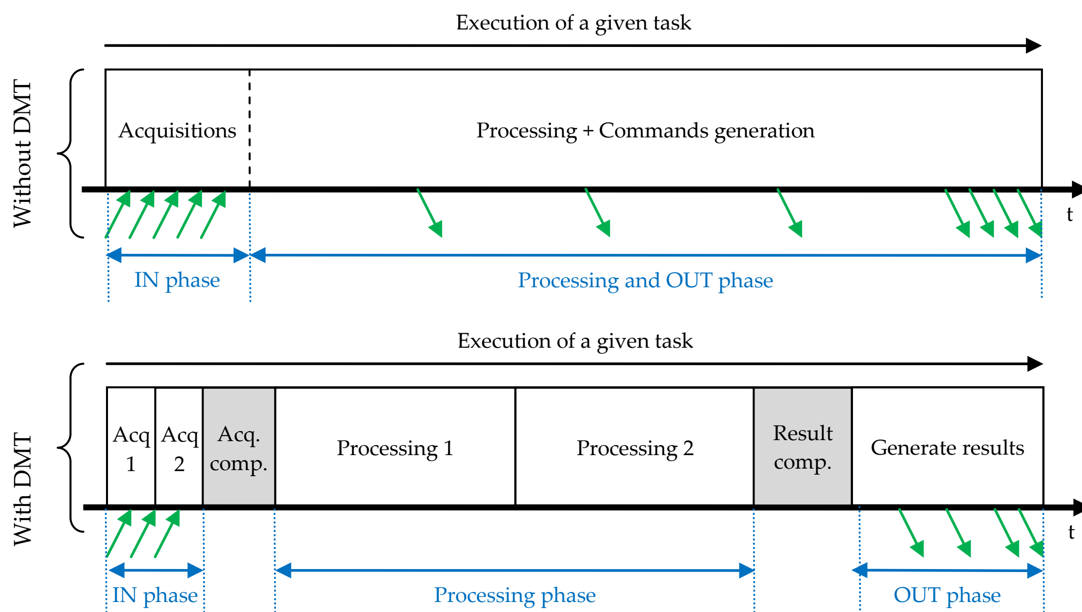


Figure 14-8 : Scheduling and fault detection in DMT architecture

Available Test Data (simulations, radiation testing, in-flight)

95 % fault coverage if only the applicative software (not the OS) is protected by the DMT concept (§ 5.9 and 5.10 in [192]).

Added value (efficiency)

- Fault coverage: close to 100%. Lock-stepping TMR [212] reaches 100% fault coverage.

Known issues (Weaknesses, elements to be considered)

- Need software architecture modifications to differentiate IN//PROC/OUT phases (preferred optimised implementation, but not mandatory); the main management parts (specifically time-replication and checking management) are hidden to the user thanks to a generic reusable middleware.
- Compliant with µP having an internal MMU (associated to a fault coverage decreasement), compliant with µP having no MMU (as DSP), compliant with multi-core µP, compliant with CPU board having a memory bridge.
- Compliant with third-party libraries, OS, interrupts.
- Compliant with SEU/SET in the interrupt logic, SET in the clock and reset trees.

IC family	Microprocessors
Abstraction level	Software
Pros	Fault coverage: close to 100%
Cons	Area overhead: negligible Time overhead: ~2.2x for detection (duplication) and ~4.5x for detection and correction
Mitigated effects	SET, SEU and MBU/MCU
Suitable Validation methods	Ground accelerated tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	DMT CNES licencing with industrial support available from DTSO". *(Note : DTSO = Delta-Technologies Sud-Ouest)*

14.3.3 Redundancy at application level

Description of the concept/implementation

Whenever the cost of two processors cannot be afforded, and features as interrupts and operating system must be supported, a possible solution can be found in hypervisor-based fault tolerance [217].

The general idea consists in employing a hypervisor to implement two virtual machines (Figure 14-9). Each virtual machine executes the program in its own address space, acquiring its set of data, processing it, and producing its set of results, as in the task-level redundancy.

In this case:

- Applications can be coded as in the lockstep architecture, without any particular care to specific coding techniques.

- Interrupts are dispatched to the two virtual machines by the hypervisor, and thus two instances of the interrupt service routine are executed providing redundancy.
- Operating systems can be used provided that the hypervisor supports them (e.g., RTEMS for Xtratum, VxWorks/Linux for Wind River hypervisor).

The hypervisor takes care of memory and resource protection, so that each virtual machine is segregated in its own address space. In case a fault affects one of them, it cannot interfere with the other virtual machine.

Figures/diagrams

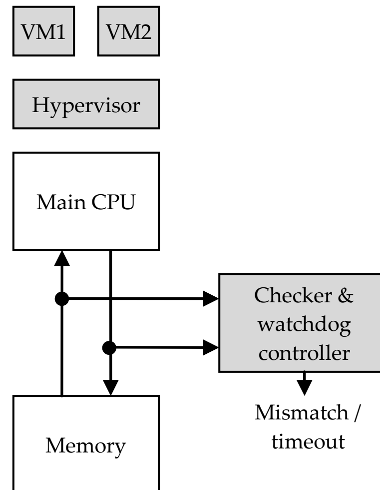


Figure 14-9 : Time redundancy at application level

Example(s)

Hypervisor-Based Fault Tolerance system based on LEON3 processor

Reference [218] presents an implementation of an Hypervisor-Based Fault Tolerance (HBFT) system based on the LEON3 processor and the XtratuM hypervisor[13] [[219]. This architecture does not leverage any particular mechanism provided by the LEON3/XtratuM combination and therefore it is general and portable to other processor/hypervisor combinations. Fault injection experiments, comparing an unhardened system with a robust version obtained using this architecture, are performed showing the effectiveness of the proposed approach. Moreover, by analyzing the time overhead this architecture entails, the authors observe that it is very close to the minimum possible overhead for a system based on duplication (100% overhead). Finally, analyzing the vulnerability of the architecture allows estimating that 96.2% of the possible SEUs affecting the system should be detected without any timeout. The remaining 3.8% of SEU is expected to be detected by a watchdog timer, leading to a system reset (more details are available below in the “Available Test Data” section).

[13] XtratuM is a hypervisor designed for embedded systems to meet safety critical real-time requirements.

Available Test Data (simulations, radiation testing, in-flight)

Reference [218] presents fault injection results on the HBFT system based on the LEON3 processor. Faults are injected in the processors' registers while running two versions (original and hardened) of a Finite Impulse Response (FIR) application. Results show that the original version produces in some cases wrong results while in the hardened version all errors are detected and no wrong result is provided. Concerning the time overhead, the hardened application implies a 108% time overhead, which is very close to the minimum overhead for a duplication system (100%).

Added value (efficiency)

- Fault coverage: >96%
- No software modification required
- Compatible with third-party libraries, Operating Systems and interrupts

Known issues (Weaknesses, elements to be considered)

Time overhead: ~2.5x (detection)

Memory overhead: >2x

IC family	Microprocessors
Abstraction level	Software
Pros	Fault coverage: >96% Area overhead: negligible
Cons	Time overhead: ~2.5x Memory overhead: ~2x
Mitigated effects	SET, SEU and MBU/MCU
Suitable Validation methods	Ground accelerated tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	N/A

15 System architecture

15.1 Scope

Mitigation techniques at architecture level refer to solutions aiming at reducing the effect of radiation on electronic equipments and that can be applied to the hardware or to the software. Many different techniques and solutions are presented in this section in order to mitigate a wide variety of radiation-induced effects.

Reducing the threat:

Shielding aims at reducing the particle's energy hitting the integrated circuits' sensitive area. Usually, space applications use both shielded packages for ICs and shield lids for systems. Such a solution is potentially able to address all types of hazards (TID, SET, SEL, SEU, SEFI, etc).

Hardware protection and SEFI recovery:

Those techniques basically add some hardware in order to monitor the system. Some examples can be mentioned such as current limiters monitoring the system's current consumption to detect potential SELs or watchdog timers able to recover SEFIs.

Spatial redundancy:

Spatial replication consists in multiplying hardware resources in order to have multiple processing units able to process the same data in parallel. Depending on the mission requirements with respect to availability and available hardware resources, designers have the choice between two architectures: a duplex topology or a Triple Modular Redundancy (TMR). A duplex requires doubling the hardware resources and is limited to fault detection. In this case fault correction is generally achieved by processing the data again, which implies a time overhead. A TMR architecture requires three times the initial amount of hardware resources and provides fault detection and correction without time overhead.

Error Detection And Correction (EDAC):

Memories represent the largest sensitive areas with respect to radiation effects, since they reach the highest possible densities, and are therefore a priority to reduce SER. Common strategies based on spatial redundancies (duplication or triplication) are usually not well suited for memories because it exceeds hardware limitations. Consequently, alternative solutions can be found with Error-Correcting Code (ECC) or Forward Error Correction (FEC) to protect data in memories or as a complementary solution to previously mentioned redundancy scheme for high reliability systems. ECCs are based on

spatial redundancy but they use algorithms capable of detecting and correcting one or several errors in a word by adding extra bits to the original user data. The memory overhead depends on the algorithms and the desired number of mitigated errors in a word.

The result of the work presented in reference [203] shows that the memory architecture is critical in affecting the single-bit EDAC effectiveness. In particular the bit-interleaving scheme implemented in the device under test prevents physical MBU from being observed as data word MBUs. Physical MBUs are detected as SBUs in different data words.

15.2 Table of effects vs mitigation techniques

Mitigation techniques		Abstraction level	Radiation effects					Page
			TID	SEL	SET	SEU	SEFI	
15.3.1	Shielding	Architecture	X	X	X	X	X	167
15.3.2	Watchdog timers	Architecture					X	169
15.3.3	Latching current limiters	Architecture		X				171
15.3.4	Duplex architectures	Architecture			X	X	X	173
15.3.5	Triple Modular Redundancy	Architecture			X	X	X	177
15.3.6	Error Correcting Codes	Architecture			X	X		180

15.3 Mitigation techniques

15.3.1 Shielding

Description of the concept/implementation

Exposure to radiation environment of electronic devices can be reduced by shielding the circuit's package and/or the entire system. The vast majority of solar energetic particles are stopped by modest depths of shielding. However, Galactic Cosmic Rays (GCR), composed of highly-charged and highly-energetic particles, are much more challenging. Hydrogenous materials, such as Polyethylene (CH_2), have been shown to be more effective shields against GCR-like irradiation than aluminium. For this reason, CH_2 is now used by NASA as a reference material for comparison with new developed materials.

Example(s)

Commonly used materials in satellites are:

- Aluminium (low/medium atomic number) for light shielding
- Tungsten (high atomic number), for heavy shielding

- New hydrogenous materials, such as Polyethylene (CH_2), showed a better effectiveness than aluminium for protection against particles issued from GCR.

Available Test Data (simulations, radiation testing, in-flight)

- Reference [220] presents calculations and experimental data on the shielding effectiveness of shielded integrated circuit packages against electrons and protons typical of the natural space environment. As a conclusion, the authors found a good correlation between the estimations and the measurements.
- SEE rates for GCR and solar flare protons using realistic models of satellite shielding are calculated in reference [221]. The first conclusion is that with the considered shield distribution, shield thicknesses should exeed 0.3 inch. The second conclusion is that shielding is more efficient for protons than for GCR.
- A study presented two representative spacecraft-shielding materials: aluminium representing low/medium-Z material and tungsten representing high-Z material [222]. Calculation results indicate that, for the radiation attenuation required for typical electronics used in a Jupiter mission, the low-Z material and the low/high-Z combination are a less-efficient shield per the same areal mass than the high-Z material in the Jovian radiation environment. When massive shielding (>10 $g.cm^{-2}$) is required to protect very radiation-sensitive electronics, then the low-/high-Z combination is a better shield per the same areal mass.
- The lunar soil's space radiation shielding properties were recently studied [223]. The aim of this study is to determine the efficiency of lunar soil as shielding against GCR heavy ions for astronauts on future lunar missions. The measurements and model calculations indicated that a modest amount of lunar soil affords substantial protection against primary GCR nuclei and Solar Particle Event (SPE), with only modest residual dose issued from surviving charged fragments of the heavy particles. The results suggest that the use of *in situ* resources on the lunar surface holds promise for radiation protection.
- Reference [224] proposes a comparison between several shielding materials, including hydrogenous media, with respect to their effectiveness to reduce the dose. Conclusions highlight the good results in dose reducing obtained by hydrogenous and low-Z materials which perform better than aluminium.
- Reference [225] describes the natural radiation environment inside spacecrafts. LET spectra are given as a function of the orbit and the aluminium shielding thickness. The conclusion of this study is that shielding helps reducing the threat from solar flares but it is not really helpful against highly energetic particles from galactic cosmic rays. According to the authors, shielding is also effective in reducing the severity of the exomagnetospheric environment and its variability.

Added value (efficiency)

No data available

Known issues (Weaknesses, elements to be considered)

- The obvious impact of shielding is the weight overhead.
- Primary particles, such as protons or neutrons, hitting shielding material will produce secondary particles which are a potential threat to electronic devices. Reference [226] presents a study on the displacement damage in silicon due to production of secondary neutrons, pions,

deuterons, and alphas resulting from proton interactions with shielding media. Results indicate that neutrons are the dominant secondary particle. The additional contribution to the displacement damage energy produced by secondary pions, deuterons, and alphas turned out to be less than 5%.

IC family	Any
Abstraction level	Architecture
Pros	Reduction of particle density in IC's active zones
Cons	Weight increase
Mitigated effects	TID, SEEs
Suitable Validation methods	Accelerated ground tests
Automation tools	SPENVIS (Space ENVironment Information System): estimation of shielding requirements FASTRAD (perform optimum shielding analysis from 3D model of the system)
Vendor solutions	N/A

15.3.2 Watchdog timers

Description of the concept/implementation

Systems based on a processor may suffer service interruption (SEFIs) due to many reasons; one of them being the effect of radiation. In such a case the system must be able to recover a normal operating mode on its own. Watchdog timers can be employed to perform a hard reset of a system unless some sequence is performed that generally indicates the system is alive, such as a write operation from an onboard processor. During normal operations, software schedules a write to the watchdog timer at regular intervals to prevent the timer from running out. If the radiation causes the processor to operate incorrectly, it is unlikely that the software will work correctly enough to clear the watchdog timer. The watchdog eventually times out and forces a hard reset to the system.

Figures/diagrams

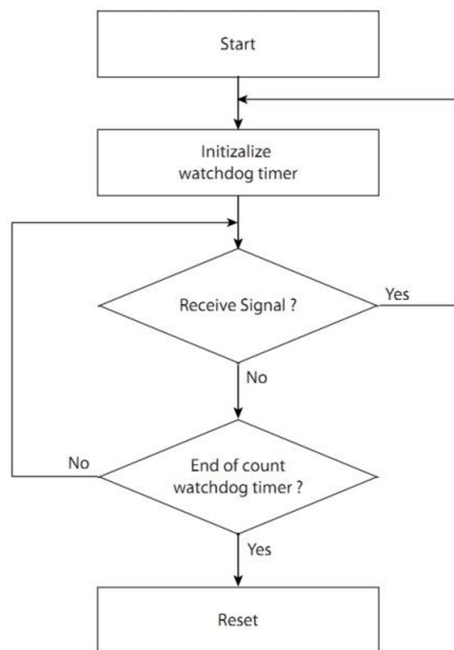


Figure 15-1 : Watchdog Timer

Example(s)

- Reference [227] presents two standard watchdog timer systems, the monostable-based timer and the windowed watchdog timer, and introduces a new one. The monostable-based timer embeds the timer which changes its logical state whenever it reaches its maximum value. The system must reset the timer before it reaches maturity to prove his healthiness. If the system fails to reset the timer an action is taken whether to change the state of an output or to immediately restart the system. Due to the unpredicted effect of transient faults, this watchdog may be reset too fast, thus affecting its fault coverage. A watchdog with a time window helps overcome this problem by allowing the system to reset the timer only within a preset time window. Yet, windowed watchdog timers are unable to detect resets which occur within their safe window. Therefore a new design, called sequenced watchdog timer, adopting a new supervisory system, based on two timers instead of one, is proposed to solve this issue. Results issued from fault injection campaigns proved the efficiency of the new design which succeeds where the standard systems fails.
- Some commercial products are available such as the Intersil IS-705RH which is a radiation hardened power up/down microprocessor reset circuit incorporating a watchdog.
- Space Micro inc developed the H-Core™ system which has an embedded watchdog.

Available Test Data (simulations, radiation testing, in-flight)

Radiation data provided by the manufacturer for the Intersil IS-705RH:

- TID > 100 krad (Si)
- SEL (th) > 90 MeV.cm²/mg

Radiation data results about the H-Core were published for three commercial microprocessors: Intel Pentium III, Texas Instruments TMS320C6713 and Equator BSP-15 [228]. In all the cases H-Core was able the recover the system after a SEFI.

Known issues (Weaknesses, elements to be considered)

The watchdog timer is a critical part of the system because if an SET or an SEU alter its normal function, the whole system could become inoperable. Therefore, it is mandatory to design a reliable watchdog.

IC family	Microprocessors
Abstraction level	System
Pros	SEFI recovery: 100%
Cons	Area overhead: watchdog circuitry
Mitigated effects	SEFI
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	Intersil IS-705RH Space Micro inc. H-Core™

15.3.3 Latching current limiters

Description of the concept/implementation

Latching Current Limiters (LCL) are active overload protections for power lines in satellites [229]. These devices are placed at the power input of any subsystem inside of a satellite. Their generic role is to provide overload protections without generating dangerous voltage transients. In applications sensitive to Single Event Latchup (SEL), they are mandatory in order to detect the phenomena and to rapidly recover it by switching off the power supply before devices get permanently damaged.

As illustrated in Figure 15-2, A LCL is based on a power MOSFET which is saturated during ON condition, open during OFF condition and in linear mode during limitation. A low ohmic sense resistor measures input current. The small voltage observed on the resistor is then amplified in order to drive the power MOSFET. The reaction time of the limiter must be as short as possible (<10 μsec). Whenever the overload limitation is reached, the power MOSFET is switched off.

Another interesting feature shown on Figure 15-2 is the ON/OFF command (CMD). This signal can be generated by the hypervisor in order to conveniently power on/off the circuit or system protected by the LCL.

Figures/diagrams

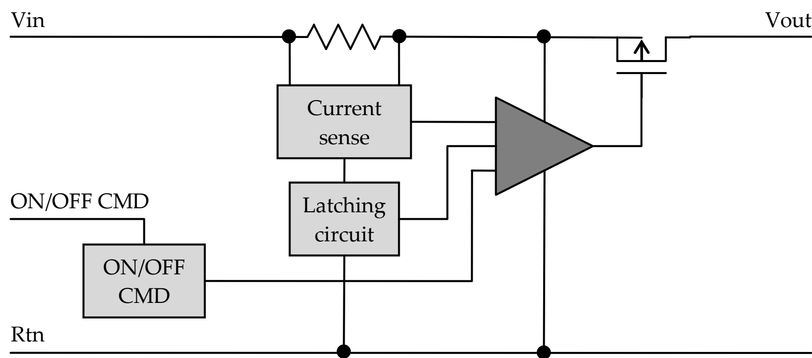


Figure 15-2 : Block diagram of a LCL

Example(s)

MAXIM MAX892 circuit is used as current limiter for MYRIADE micro-satellite (see section 15.5.1).

Available Test Data (simulations, radiation testing, in-flight)

- A study proved the LCL's efficiency to protect against SEL non radiation hardened circuits [230].
- Heavy ion SET test results are available for the MAX892 from Maxim. Detailed results can be obtained from the European Space Components Information Exchange System (ESCIES) [231].

Added value (efficiency)

- The primary functionality of a LCL is to offer protection against SEL. Moreover, LCL can provide an ON/OFF feature allowing the satellite's supervisor to easily switch on/off any subsystem at any time. This feature can be used after detection of a SEFI whenever a soft reset does not permit to regain a normal functional state.
- Operating the power MOSFET in linear mode during the sub-system's start-up allows limiting inrush current spikes.

Known issues (Weaknesses, elements to be considered)

- The LCL is a critical safety element for the satellite and therefore special attention must be paid during selection of its parts to ensure that they meet the required radiation immunity according to the mission.
- When setting the current threshold, the designer must take into account the supply current increase caused by TID.

IC family	Any
Abstraction level	Architecture
Pros	Current overload protection
Cons	Area overhead: LCL circuitry
Mitigated effects	SEL
Suitable Validation methods	Ground accelerated test
Automation tools	None
Vendor solutions	Maxim MAX892

15.3.4 Duplex architectures

Description of the concept/implementation

The Bi-MR (Bi-Modular Redundancy), also called duplex architecture, is issued from the spatial redundancy concept present in section 10.3.1. It uses two replicas of a processing unit and votes the outputs to detect potential differences provoked by SEEs (Figure 15-2). Such an architecture is mainly a fail-stop architecture as it is able to detect faults but not to recover them.

Figures/diagrams

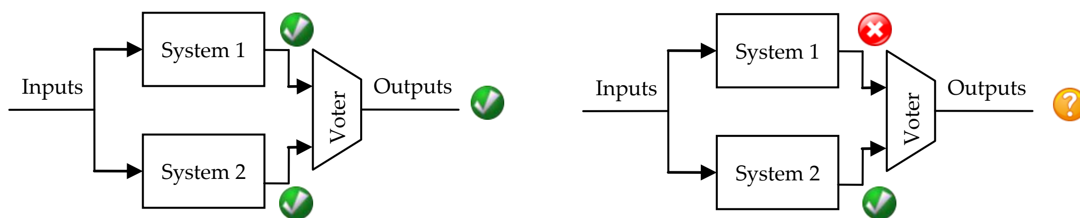


Figure 15-3 : Block diagram of a duplex architecture

Example(s)

<u>Lockstep</u>

The idea of lockstep is to implement redundant software execution by means of duplicated processors. A primary processor and a backup one run the same software (without any modification, possibly including the operating system). Both the primary and the backup processors have read access to the memory, while only the master is allowed to write the memory. Both processors work in parallel and they are synchronized at clock level: each time primary and backup perform a bus cycle, an ad-hoc hardware checker compares the address, data and control buses looking for mismatches. In case a fault is detected a proper corrective action is taken, otherwise the execution proceeds.

The approach mandates two processors, and a hardware checker able to synchronize the operations of the two processors (see Figure 15-3). However, as the software running on each processor does not require any specific coding rules, both interrupts/traps and operating systems are supported.

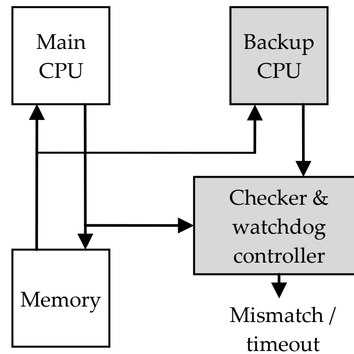


Figure 15-4 : Lockstep architecture

No particular restrictions are needed for the processor, however in order to minimize fault latency (i.e., the time spanning from the occurrence of the fault and its detection), in case cache memory is used, it is preferable to configure it as write-through[14].

This topology is particularly suitable in the following cases:

- When two CPUs are available within a SoC (e.g. two PPC405 in the Xilinx Virtex-4).
- When two IP cores can be integrated in the same FPGA (e.g. two LEON3 in a Xilinx Virtex-4).

A Lockstep system has the following advantages:

- 100% fault coverage (fault detection)
- Does not require software modifications
- Compatible with third-party libraries, OS, interrupts

A Lockstep system implies the following penalties:

- Area overhead: 1 CPU + checker
- Time overhead: 0 to 2.5x depending on the application

A drawback of this technique is to require a μP having the lockstepping capability (clock synchronisation or other mechanisms, full predictibility, …), capability less and less compliant with deep sub-micron technologies. This technique was implemented on some μP such as the ATMEL ERC32, Intel Pentium, Intel i960, IBM RH6000, IBM PowerPC750FX, etc.

Double Duplex Tolerant to Transients

The Double Duplex Tolerant to Transients (DT2) is a CNES patented architecture aiming at, but not limited to application missions and large satellites [212]. DT2 is a “structural mini-duplex”:

[14] In a write-through cache, every write to the cache causes a synchronous write to the backing store. Alternatively, in a write-back cache, writes are not immediately mirrored to the store.

- Hardware redundancy is limited to the Processing Unit Core (PUC), i.e. the microprocessor, its memory and its companion chip.
- Each PUC runs asynchronously the same flight software.
- The two PUC's synchronisation is made only on external I/O data flow (e.g. sensors and actuators data).

Two specific hardware functions are required in DT2, they must be implemented in a SEE-free ASIC or FPGA (Figure 15-4):

- CESAM, a simplified version of the DMT's CESAM (see section 14.3.1).
- SYCLOPES is in charge of macro-synchronisation, comparison and intelligent I/O coupler.

DT2, alike DMT, has two recovery strategies based on a safe context storage independent for each physical channel supported by CESAM and EDAC. At any time, each PUC knows whether the other PUC is healthy or faulty. When SYCLOPES detects an error, each PUC can enter simultaneously either backward recovery mode (roll-back the faulty iteration) or forward recovery mode (jump to next iteration). No data exchange is required between the two PUCs as each one has its own safe context storage inside its own memory to avoid fault propagation between channels.

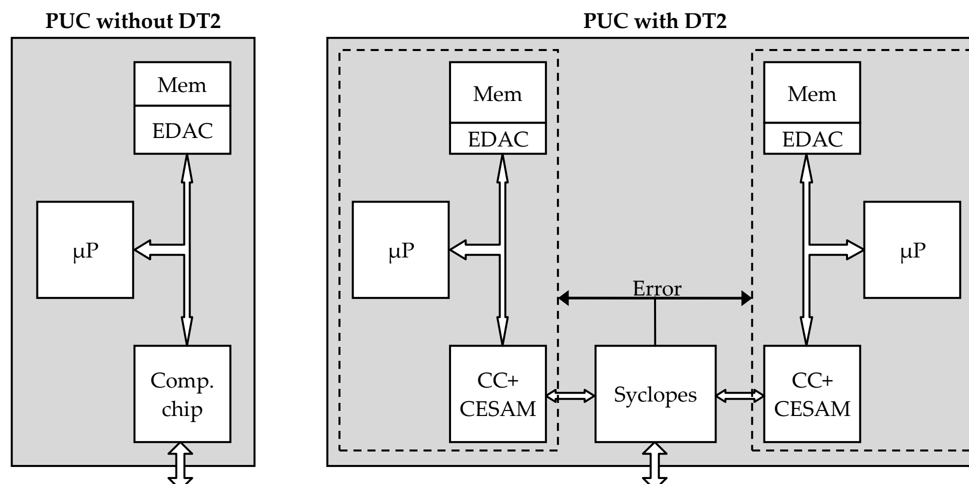


Figure 15-5 : DT2 hardware architecture

DT2 has the following advantages:

- >99% fault coverage if voter is radiation immune

DT2 implies the following penalties:

- Area overhead: 1 entire PUC + Syclopes, knowing that it is possible to implement 2 CESAM + 1 Syclopes into a single companion chip
- Time overhead: ~1 for detection and ~1.3 for detection and correction

<u>Double duplex</u>

A double duplex architecture is based on two identical duplex units. One is called the master unit and the second, called slave unit, is used as a backup. When the two channels of the master unit disagree,

the second duplex becomes the master and processes the data (Figure 15-5). Meanwhile, the faulty duplex can be reinitialized.

A double duplex architecture was used for the Ariane 5 launcher telemetry generation unit called UCTM-C/D and developed by IN-SNEC. The UCTM-C/D is based on a radiation sensitive DSP.

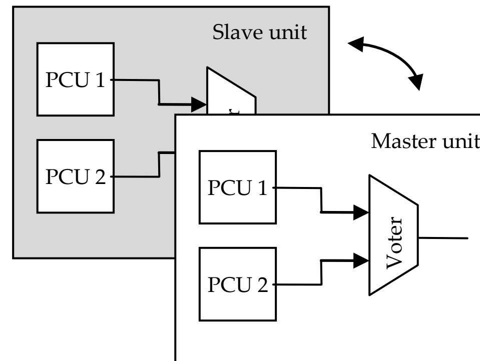


Figure 15-6 : UCTM-C/D architecture

Available Test Data (simulations, radiation testing, in-flight)

Reference [232] presents two new incremental approaches for the implementation of systems tolerant to radiation induced faults, using the lockstep technique combined with checkpoints and rollback recovery[15]. The selected strategies reduce the number of checkpoints and the amount of data to be stored during each checkpoint. Consequently the time dedicated to checkpoint is decreased, and the performance overhead for the application is less severe.

Added value (efficiency)

Fault coverage: >99% if voter is radiation immune

Known issues (Weaknesses, elements to be considered)

- Area overhead: 1 entire system
- A duplex architecture is mainly a fail-stop architecture as it is able to detect faults but not to recover them.

[15] The system's state is regularly stored and whenever an error occurs it is restored to the last saved state and the execution starts again from this checkpoint.

IC family	Any
Abstraction level	Architecture
Pros	Fault coverage: >99% if voter is radiation immune
Cons	Area overhead: about ~1 (one additional system) Time overhead: ~1.5 for detection and ~3 for detection and correction
Mitigated effects	SET, SEU, MBU/MCU, SEFI
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	N/A
Vendor solutions	DT2 CNES licencing with industrial support available from DTSO

15.3.5 Triple Modular Redundancy

Description of the concept/implementation

Triple Modular Redundancy (TMR) is based on the spatial redundancy concept which is detailed in section 10.3.1. In a TMR-based system, hardware resources are triplicated in order to perform three identical tasks in parallel. Figure 15-6 illustrates a TMR architecture embedding three identical microprocessors executing concurrently the same tasks (Task A at T=0, then Task B at T=1, etc). A comparator determines whether the three outputs are identical or if an error occurred. The hardware penalty induced by TMR is about 200% the original design size, whereas it is 100% for a duplex. However, the advantage of a TMR over a duplex is its capability to produce a correct result on two branches when the third one is faulty, thus, not breaking the computational chain. Moreover the system is still able to deliver full functionality on two branches while the faulty one is recovering.

Figure 15-7 depicts a Full TMR system where the comparators are also triplicated. In this case, the outputs can be tied together in order to obtained an “analog comparator”. If one of the outputs is different from the two others, then the output will be forced by the correct value.

Figures/diagrams

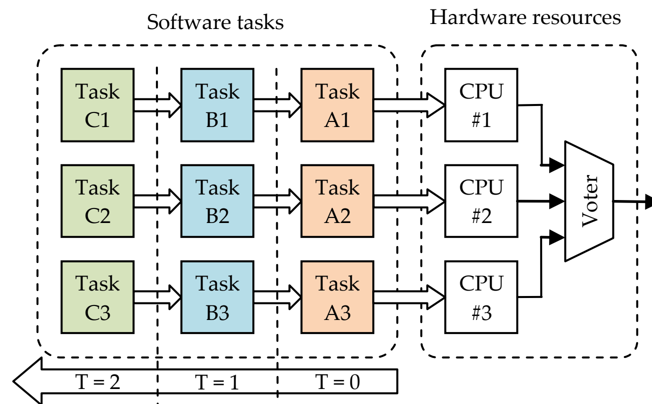


Figure 15-7 : Triple Modular Redundancy

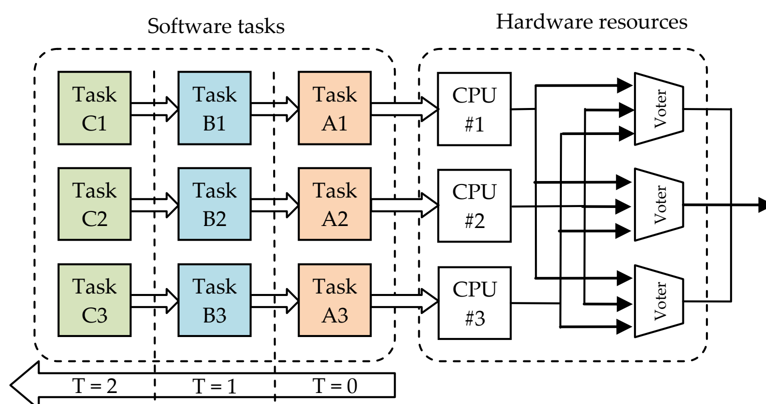


Figure 15-8 : Full Triple Modular Redundancy

Example(s)

In the following are presented some examples of TMR architecture used by commercial products and space agencies for their projects:

- Hermès European space shuttle project embeds the USR quadruplex computer (3 processors + 1 backup processor) developed by EADS-Astrium for CNES [233]. This architecture was then used to produce the DMS-R command-control computer for the Russian module on the ISS (International Space Station). DMS-R consists in two triplex computers, both based on the ERC32 processor (Atmel).
- The GUARDS architecture designed for critical applications such as rail, nuclear and space systems [234].
- Japanese INDEX micro-satellite's computer is based on the Hitachi SH-3 commercial micro-controller. A "light" triplex architecture (centralized voter integrated into a radiation-hardened FPGA) was used to protect the satellite [235].
- The SCS750 space-qualified board, developed by Maxwell technologies [236], is based on three IBM PowerPC750FX microprocessors using TMR. The centralized voter is embedded in a radiation tolerant FPGA immune to SEE. This board was selected by Northrop Grumman Space

Technology for spacecraft control and payload data management for the National Polar-orbiting Operational Environmental Satellite System (NPOESS). This platform is detailed in the section 15.4.1.

- The Proton platform, by Space Micro, implements a technique combining spatial and temporal redundancy called Time Triple Modular Redundancy. This platform is detailed in the section 15.4.1.

Available Test Data (simulations, radiation testing, in-flight)

Radiation test results for the SCS750 rev7 board [237]:

- TID > 100 krad (Si) (orbit dependent)
- SEL_{th} > 80 $MeV.cm^2/mg$ (all parts except SDRAM) & ~ 50 $MeV.cm^2/mg$ (SDRAM)
- SEU : one upset every 100 years (LEO or GEO orbit)

Proton200k offers the following performances with respect to radiation [211]:

- TID > 100 krad (Si) (orbit dependent)
- SEL (th) > 70 MeV.cm2/mg
- SEU < 10-4 (orbit dependent)
- 100% SEFI mitigation

Added value (efficiency)

TMR architecture grants almost a complete immunity to SET, SEU, MCU/MBU and SEFI. However this architecture has a weak point: the output comparator (see known issues section below).

Known issues (Weaknesses, elements to be considered)

- The weakness of a TMR architecture is the comparator as it is the only part without redundancy. Therefore, the designer must pay special care when implementing the final voter. One solution to harden the voter is to use oversized transistors in order to reduce their sensitivity towards radiation. Another solution is to use the full TMR implementation with voter’s outputs being tied together. Finally, the voters can be implemented in a radiation-hardened FPGA.

IC family	Any
Abstraction level	Architecture
Pros	Fault coverage close to 100%
Cons	Area overhead: ~3x (two additional systems)
Mitigated effects	SEFI, SET, SEU, MCU/MBU
Suitable Validation methods	Ground accelerated test HW/SW fault injection
Automation tools	N/A
Vendor solutions	Maxwell SCS750 Space Micro inc. Proton platform (Proton100k, proton200k, etc)

15.3.6 Error Correcting Codes

Description of the concept/implementation

Error-Correcting Codes (ECC) or Forward Error Corrections (FEC) are algorithms capable of detecting and/or correcting errors in data by adding some redundant data or parity data to the original data. When the original data is read, its consistency can be checked with the additional data. ECC is a very wide subject which cannot be entirely covered by this handbook, more complete information can be found in references [238] [239] [240] [181] [241]. Most commonly used ECC in space and aeronautic applications are given in the example section below.

Each ECC has its own characteristics in terms of fault detection and fault correction, however they all impact the system by adding an area overhead to store the redundant data and a time overhead to compute these data and check original data for consistency.

There are two main families of ECC: block codes and convolutional codes. Convolutional codes are mainly used for data transfer such as digital video, mobile communication and satellite communication, whereas the block codes are rather used for protection of data storage. Consequently ECC presented in this section are block codes which can be classified in two groups whether they are limited to error detection or they can achieve error detection and/or correction, depending on the amount of redundant data (see Table 15-1).

There is not one ECC which is the solution to every problem. Each application has its own requirements and only one code may meet all of them. When several codes fit the conditions, the designer have to carefully examine each of them and make his own choice. Some examples of applications are provided:

- Parity checking: Slow communication (RS232)
- CRC: Networks
- Hamming codes: Used for communications on the French Minitel, data protection in computers (DRAM, hard-drives, SCSI bus), etc
- Reed-Solomon: Complex photographs transfer, data protection in computers (CD-ROM drive, associated to the RAR compression protocol in order to rebuild missing data), etc

- Reed-Muller: Used on Mariner 9 to transmit black and white photographs of Mars, etc

Figures/diagrams

Table 15-1 : Error detection and correction capability for some ECC

ECC	Error detection	Error correction
Parity check	X	
N-of-M code	X	
Cyclic Redundancy Check	X	
BCH codes	X	X
Hamming codes	X	X
Reed-Solomon codes	X	X

Example(s)

Parity check:

A parity bit is a bit that is added to ensure that the number of bits with the value "1" in a set of bits is even or odd. Parity bits are used as the simplest form of error detecting code.

There are two variants of parity bits: even parity bit and odd parity bit:

- Even parity, the parity bit is set to 1 if the number of ones in a given set of bits (not including the parity bit) is odd, making the entire set of bits (including the parity bit) even.
- Odd parity, the parity bit is set to 1 if the number of ones in a given set of bits (not including the parity bit) is even, keeping the entire set of bits (including the parity bit) odd.

In other words, an even parity bit will be set to "1" if the number of 1's + 1 is even, and an odd parity bit will be set to "1" if the number of 1's +1 is odd.

Even parity check is a special case of a Cyclic Redundancy Check (CRC), where the single-bit CRC is generated by the divisor x+1.

Because of its simplicity, parity is used in many hardware applications where an operation can be repeated in case of difficulty, or where simply detecting the error is helpful. For example, the Small Computer System interface (SCSI) and Peripheral Component Interconnect (PCI) buses use parity to detect transmission errors, and many microprocessor instruction caches include parity protection.

In serial data transmission, a common format is 7 data bit, an even parity bit, and one or two stop bits. This format neatly accommodates all the 7-bit ASCII characters in a convenient 8-bit byte. Other formats are possible; 8 bits of data plus a parity bit can convey all 8-bit byte values.

In serial communication contexts, parity is usually generated and checked by interface hardware (e.g., a UART) and, on reception, the result made available to the CPU (and so to, for instance, the operating system) via a status bit in a hardware register in the interface hardware. Recovery from the error is usually done by retransmitting the data, the details of which are usually handled by software (e.g., the operating system I/O routines).

Parity data is also used by some Redundant Array of Independent Disks (RAID) levels to achieve redundancy in storage systems. If a drive in the array fails, remaining data on the other drives can be combined with the parity data (using the Boolean XOR function) to reconstruct the missing data (e. g. RAID 5).

Let us consider the 7-bit data “1010001”. This number is odd because it contains three “1”.

- Applying even parity will set the parity bit to “1” in order to have an even number (four) of “1” and the data will become “**1**1010001”.
- Applying odd parity will set the parity bit to “0” in order to have an odd number (three) of “1” and the data will become “**0**1010001”.

Some other examples are given in Table 15-2.

Table 15-2 : Some examples of parity check applied to a 7-bit word

7 bits of data	Number of “1”	8-bits including parity bit	
		even	odd
000 0000	0	**0**000 0000	**1**000 0000
101 0001	3	**1**101 0001	**0**101 0001
110 1001	4	**0**110 1001	**1**110 1001
111 1111	7	**1**111 1111	**0**111 1111

Parity check is a very simple ECC, it is limited to detect an odd number of flipped bits. Indeed an even number of bit-flips will make the parity bit appear correct even though the data is erroneous.

M-of-N code:

An M of N code is a separable error detection code with a code word length of n bits, where each code word contains exactly m instances of a "one." A single bit error will cause the code word to have either m+1 or m-1 “ones”. An example M-of-N code is the 2 of 5 code used by the United States Postal Service.

The simplest implementation is to append a string of ones to the original data until it contains M ones and then append zeros to create a code of length N.

Table 15-3 presents a three bit data word and its corresponding three-bit word in order to build a 3-of-6 code. The appended word is calculated in order to obtain a final word having exactly three “ones”.

Table 15-3 : Construction of a 3 of 6 code

Original 3 data bits	Appended bits
000	111
001	110
010	110
011	100
100	110
101	100
110	100
111	000

M-of-N code is not suitable for multiple-bit hardening

Cyclic Redundancy Check:

A Cyclic Redundancy Check (CRC) is an-error-detecting (not correcting) cyclic code and non-secure hash function designed to detect accidental changes to digital data in computer networks. It is characterized by specification of a so-called generator polynomial, which is used as the divisor in a polynomial long division over a finite field, taking the input data as the dividend, and where the remainder becomes the result [181].

Cyclic codes have favorable properties as they are well suited for detecting burst errors[16]. CRCs are particularly easy to implement in hardware, and are therefore commonly used in digital networks and storage devices such as hard disk drives.

Table 15-4 provides some examples of commonly used CRCs and the applications they apply to.

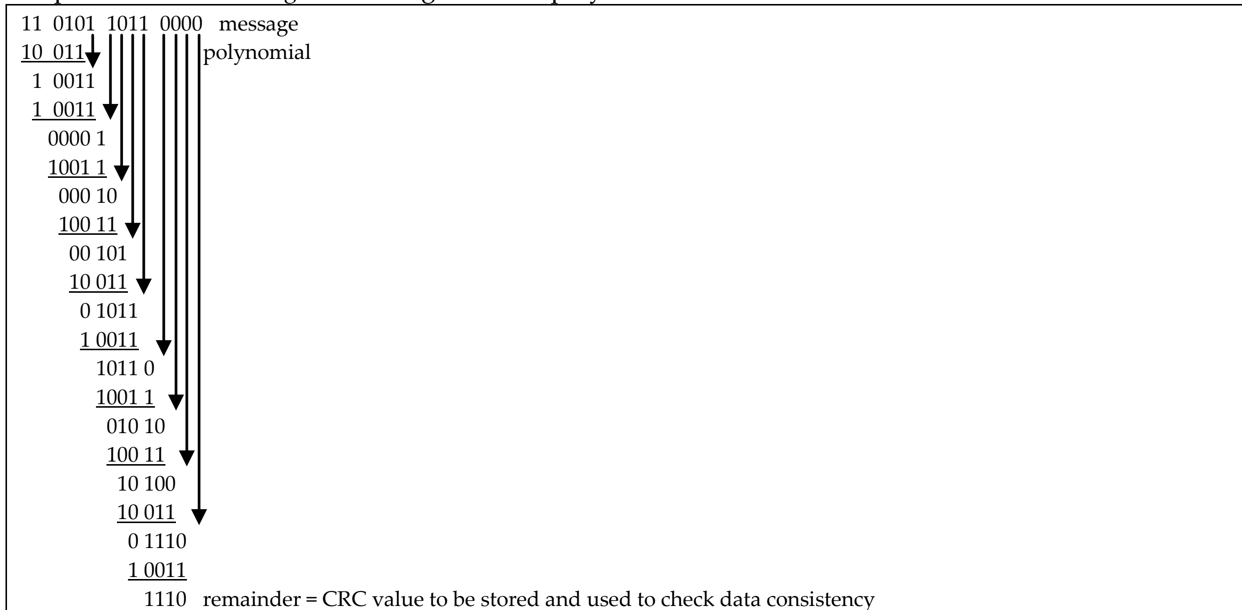
Table 15-4 : Some example of commonly used CRCs

Name	Polynomial	Some applications
CRC-1	$x + 1 = 0x3$	Parity check
CRC-4-ITU	$x^4 + x + 1 = 0x13$	ITU-T G.704 standard
CRC-8-CCITT	$x^8 + x^2 + x + 1 = 0x107$	ISDN header Error Control
CRC-16-CCITT	$x^{16} + x^{12} + x^5 + 1 = 0x1021$	HDLC, Bluetooth, SD memory cards
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 = 0x04C11DB7$	Ethernet, SATA, MPEG-2

Even parity check is a special case of a cyclic redundancy check, where the single-bit CRC is generated by the divisor x+1.

[16] A burst error is a continuous sequence of data containing errors.

In the following is an example of a CRC computation on a binary message "1101011011" using the CRC-4-ITU polynomial ("10011"). The first step is to append n bits to the message where n is the order of the polynomial. The order of a polynomial is the power of the highest non-zero coefficient. The order of the CRC-4-ITU polynomial is 4. Thus, the message becomes "1101011011**0000**". The following step consists in *XORing* the message and the polynomial:



BCH codes:

BCH codes [239][181][242] form a class of parameterized error-correcting codes which have been the subject of much academic attention in the last fifty years. BCH codes were invented in 1959 by Hocquenghem, and independently, in 1960, by Bose and Ray-Chaudhuri. The acronym BCH comprises the initials of these inventors' names. Reed-Solomon codes, presented below, are a special case of BCH codes.

The principal advantage of BCH codes is the ease with which they can be decoded, via an elegant algebraic method known as syndrome decoding[17]. This allows very simple electronic hardware to perform the task, obviating the need for a computer, and meaning that a decoding device may be made small and low-powered.

In technical terms a BCH code is a multilevel cyclic variable-length digital error-correcting code used to correct multiple random error patterns.

Hamming codes:

Hamming codes were introduces by Richard W. Hamming in 1950. The code stemmed from his work as a theorist at Bell Telephone laboratories in the 1940s. Hamming invented the code in 1950 to provide an error-correcting code to reduce the wasting of time and valuable computer resources [181].

Today, Hamming code really refers to a specific (7,4) code that encodes 4 bits of data into 7 bits by adding 3 parity bits. Hamming Code adds three additional check bits to every four data bits of the message. Hamming's (7,4) algorithm can correct any single-bit error, or detect all single-bit and two-bit errors. In other words, the Hamming distance between the transmitted and received words must be no greater than one to be correctable. This means that for transmission medium situations where

[17] Syndrome decoding is a highly efficient method of decoding a linear code over a noisy channel

burst errors do not occur, Hamming's (7,4) code is effective (as the medium would have to be extremely noisy for 2 out of 7 bits to be flipped).

Hamming noticed the problems with flipping two or more bits, and described this as the "distance" (it is now called the Hamming distance). Parity has a distance of 2, as any two bit flips will not be detectable. The (3,1) repetition has a distance of 3, as three bits need to be flipped in the same triple to obtain another code word with no visible errors. A (4,1) repetition (each bit is repeated four times) has a distance of 4, so flipping two bits can be detected, but not corrected. When three bits flip in the same group there can be situations where the code corrects towards the wrong code word.

Hamming was interested in two problems at once; increasing the distance as much as possible, while at the same time increasing the code rate as much as possible. During the 1940s he developed several encoding schemes that were dramatic improvements on existing codes. The key to all of his systems was to have the parity bits overlap, such that they managed to check each other as well as the data.

SEC-DED codes

As a single error correcting code would not be satisfactory for many applications, SEC-DED is the most often used in computer memories as these codes can detect two errors and correct one.

These codes have a minimum distance of 3, which means that the code can detect and correct a single error, but a double bit error is indistinguishable from a different code with a single bit error. Thus, they can detect double-bit errors but cannot correct them.

The Hamming code can be converted to a SEC-DED code including an extra parity bit: it increases the minimum distance of the Hamming code to 4. This gives the code the ability to detect and correct a single error and at the same time detect (but not correct) a double error. It could also be used to detect up to 3 errors but not correct any.

Reed-Solomon codes

Reed–Solomon (RS) codes [181] are non-binary cyclic error-correcting codes invented by Reed and Solomon. They described a systematic way of building codes that could detect and correct multiple random errors. By adding t check symbols to the data, an RS code can detect any combination of up to t erroneous symbols, and correct up to t/2 symbols. Furthermore, RS codes are suitable as multiple-burst bit-error correcting codes, since a sequence of b+1 consecutive bit errors can affect at most two symbols of size b. The choice of t is up to the designer of the code, and may be selected within wide limits.

In Reed-Solomon coding, source symbols are viewed as coefficients of a polynomial $p(x)$ over a finite field. The original idea was to create n code symbols from k source symbols by oversampling $p(x)$ at $n > k$ distinct points, transmit the sampled points, and use interpolation techniques at the receiver to recover the original message. That is not how RS codes are used today. Instead, RS codes are viewed as cyclic BCH codes, where encoding symbols are derived from the coefficients of a polynomial constructed by multiplying $p(x)$ with a cyclic generator polynomial. This gives rise to an efficient decoding algorithm, which was discovered by Elwyn Berlekamp and James Massey, and is known as the Berlekamp-Massey decoding algorithm.

Reed–Solomon codes, which are a special case of BCH codes, are used in many different applications from consumer electronics to satellite communication. They are prominently used in consumer electronics such as CDs, DVDs, Blu-ray Discs, in data transmission technologies such as DSL & WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems. RS codes are also well known for their role in encoding pictures of Saturn and Neptune

during Voyager space missions. In fact, RS codes are incorporated in the NASA Standard. These and several other applications of RS codes are described in [243].

Arithmetic codes

Arithmetic codes are very useful when it is desired to check arithmetic operations such as additions, multiplications and divisions. The data presented to the arithmetic operation is encoded before the operations are performed twice in parallel. After completing the arithmetic operations, the resulting code words are checked to make sure that they are valid. If they are not, an error condition exists.

Arithmetic codes are interesting for checking arithmetic operations because they are preserved under such operations. Indeed, they have the following property: A(a*b) = A(a) * A(b) where a and b are operands, A(x) is the arithmetic code of x and * is an operation such as addition, multiplication or division. Among the arithmetic codes, the so-called *separable codes* are the most practical. They are obtained by associating a check part issued from a suitable generator, to an information part. The arithmetical operation is performed separately on both the original and the coded operands. Comparison of results allows to detect potential errors. Most common arithmetic codes are *residues* defined by R(N) = N mod m. Figure 15-9 depicts an arithmetic function using an arithmetic code for error detection.

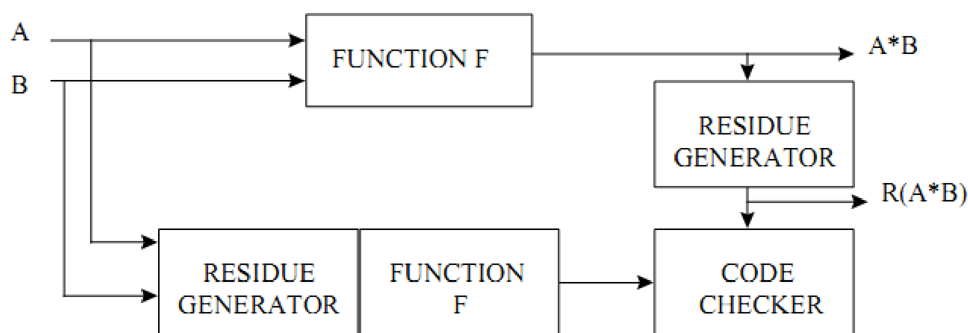


Figure 15-9 : An arithmetic function using an arithmetic code as error detection mechanism

These codes have specific interest to design arithmetic units that are self checking. Nevertheless, using arithmetic codes have limited interest in SEU protection since the area overhead applies in registers and on the combinatorial part, and it is not applicable for logic function protection [reference to "Circumventing radiation effects by logic design"].

Available Test Data (simulations, radiation testing, in-flight)

- Reference [244] provides synthesis and routing results for parallel Reed-Solomon encoders and decoders implemented in Microsemi and Xilinx FPGAs.
- Reference [245] presents Hamming and Reed-Solomon codes. Their improvements in data rate are compared to tradeoffs in complexity and decoding lag. Different types of modulation are used to make comparisons in the performance of each ECC code.

Added value (efficiency)

No data available

Known issues (Weaknesses, elements to be considered)

Area and time overhead depending on the selected ECC and the number of faults to be detected and/or corrected.

IC family	Memories
Abstraction level	Architecture
Pros	Data storage protection
Cons	Area and time overhead (depending on the ECC and the amount of redundant data)
Mitigated effects	SET, SEU, MBU/MCU
Suitable Validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	N/A GECO (Automatic Generation of Error Control Codes for Computer Applications) [246]
Vendor solutions	N/A

15.4 Commercial solutions

15.4.1 Space Micro Proton platform

Description

Space Micro proton platform is based on the Time-Triple Modular Redundancy (TTMR) system, patented by Space Micro Inc. [247]. It is an error detection and correction system capable of being implemented in Very Long Instruction Word (VLIW) Digital Signal Processors (DSPs). In one embodiment, the VLIW DSP includes specialized software routines known as "ultra long instruction word" and/or "software controlled instruction level parallelism". These software routines include parallel functional units configured to execute instructions simultaneously wherein the instruction scheduling decisions are moved to the software compiler. The TTMR system combines time redundant and spatially redundant instruction routines together on a single VLIW DSP [248].

The system depicted in Figure 15-8 executes an instruction on the first slot using an ALU. Then an identical instruction is executed during the following time-slot on another independent ALU. The results from the two instructions are compared and if they do not match a third identical instruction is executed on a third ALU. Finally the result is compared with the previous ones and the correct value is determined.

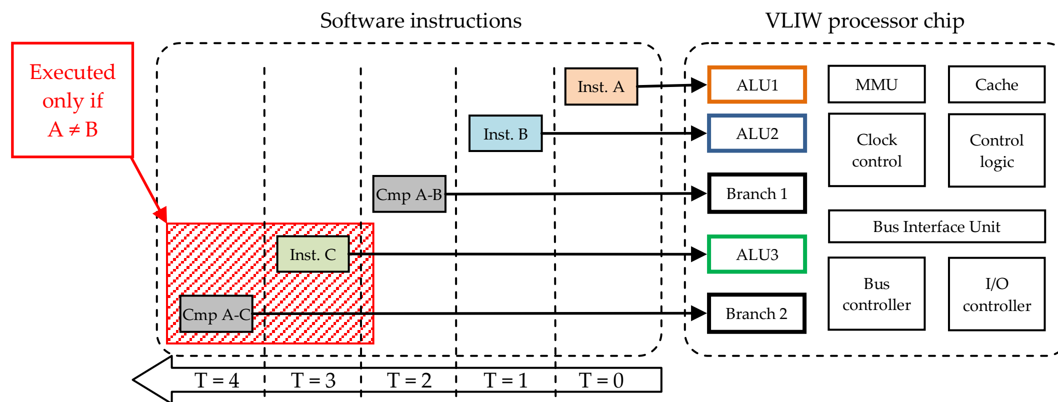


Figure 15-10 : Improved TTMR architecture

The TTMR algorithm is coded into the "post-compiler" which must be developed for each supported DSP. The Proton100k system is able to cope with SEEs and SEFIs. SEFIs are addressed using a radiation hardened watchdog circuit.

The Proton100k is used on USAF Roadrunner experimental satellite and onboard the International Space Station (ISS).

Available Test Data

Proton200k offers the following performances with respect to radiation [211]:

- TID > 100 krad (Si) (orbit dependent)
- SEL > 70 MeV.cm²/mg
- SEU < 10^{-4}
- 100% SEFI mitigation

15.4.2 Maxwell SCS750

Description

The SCS750 space-qualified board, developed by Maxwell technologies [236], is based on three IBM PowerPC750FX microprocessors organized in a TMR architecture and working in lockstep. The centralized voter is embedded in a radiation tolerant FPGA immune to SEE. Other mitigation solutions, such as SOI based-components and Microsemi RTAX-S Radiation tolerant FPGAs were used.

This board was selected by Northrop Grumman Space Technology for spacecraft control and payload data management for the National Polar-orbiting Operational Environmental Satellite System (NPOESS).

Available Test Data

Radiation test results for the SCS750 rev7 board [237]:

- TID > 100 krad (Si) (orbit dependent)

- SEL_{th} > 80 MeV.cm²/mg (all parts except SDRAM) & ~ 50 MeV.cm²/mg (SDRAM)
- SEU : one upset every 100 years (LEO or GEO orbit)

15.5 Examples of adopted architectures onboard satellites

15.5.1 Architecture for the MYRIADE satellite

MYRIADE is a typical example of a computer developed with commercial components and protected by a mix of mechanisms for a mission without hard constraints with respect to availability.

	TID	SET	SEL	SEU	MBU/MCU	SEFI
System	Switch-off sensitive ICs when not used					
System			Current limiters			
System		Watchdog implemented at different levels (local & global for I/Os, local & global for µP)				
Processor	Protected with a 2 mm tungsten shield					
Analog acquisitions		Time redundancy + average value computation				
link/bus data exchanges				Checksum/CRC and recovery protocols		
Flash and FRAM		Redunded data, checksum or CRC Flash and FRAMS are switched-off after the boot of the flight software		Redunded data, checksum or CRC Flash and FRAMS are switched-off after the boot of the flight software		
FPGA's critical registers				TMR		
Critical data in µP's memory				TMR on flight SW memory		

15.5.2 Architecture for the REIMEI (INDEX) satellite

REIMEI is a small Japanese fault-tolerant COTS-based satellite for aurora observation and technology demonstration, launched in 2005. The following fault tolerant schemes were implemented in REIMEI:

- COTS microprocessor = Hitachi SH-3
- TMR architecture
- Voter is a SPF[18] (Single Point of Failure)
- Reinsertion phase: stop the computer for 2 sec

15.5.3 Architecture for the CALIPSO satellite

CALIPSO is a joint U.S. (NASA) and (CNES) spacecraft based on a CNES PROTEUS mini-satellite platform. It was launched in 2006 for cloud, aerosol and infrared observations. The COTS-based payload computer developed by GDAIS embeds the following mitigation solutions:

- COTS microprocessor = Freescale PowerPC603r
- 4-MR architecture (quadruplex), including 4 microprocessors working in lock-step
- The voter is duplicated (it is not a SPF)

[18] A Single Point of Failure (SPF) is a part of a system that, if it fails, will stop the entire system from working.

16 Validation methods

16.1 Introduction

Applications intended to operate in harsh environment and critical applications (for example involving human lives) must be qualified with respect to radiation to determine if they meet the constraints imposed by the final environment. While *real-life tests* provide accurate results, they also require long time experiments. Consequently, radiation ground tests, also called *accelerated tests*, are generally preferred for their capability to reproduce with huge fluxes of particles, and thus in short time, the effects of natural environment on integrated circuits.

16.2 Real-life tests

Real-life tests consist in operating a target application in its final environment. Different solutions are available depending on the considered environment:

- Onboard scientific satellites: some projects accept applications devoted to study the behavior of the radiation on circuits and their software if they have one. Among them can be mentioned MPTB (Microelectronics and Photonics Testbed) [249], STRV (Space Technology Research Vehicles) [250] and [251], LWS-SET (Living With a Star – Space Environment Testbed) [252], etc.
- Onboard stratospheric balloons: they are able to operate in the stratosphere during long periods of time and at an altitude between 12 and 45km. Such altitudes are too low for satellite and too high for conventional airplanes. Therefore stratospheric balloons offer the unique chance to perform experiments at high altitude. Some balloons are bigger than a football field and are able to lift payloads of two tones to altitudes of 40 km. A generic platform devoted to detect upsets in two successive technological generations of SRAMs is presented in reference [253]. Preliminary results obtained in commercial fights were successfully compared to those issued from a state-of-the-art predicting tool (The MUSCA SEP3[19] tool [254]).
- Ground experiments: they provide high flexibility capabilities because they are not tied by weight, volume and power consumption constraints as it could be the case for the two previously presented platforms. An example of real life component qualification is the Rosetta experiments by Xilinx [255]. It consists of several hundreds of FPGAs being monitored to detect upsets in their configuration memories. These testbeds are installed at different altitudes, from -550m to 2550m, in the US and in France.

Results from real-life experiments are relatively long to obtain because of the low particle fluencies found in natural environment. A solution is to increase the sensitive volume exposed to the

[19] The Multi-Scales Single Event Phenomena Predictive Platform (MUSCA SEP3) aims at calculating both the SEE cross section and SER. The approach consists in modelling the whole device, its local and global environment (shielding, package) and the detailed characteristics of the radiative environment.

particles but this is often not compatible with the constraints imposed by embedded missions such as satellites and stratospheric balloons. This, combined with the cost of such experiments, explains why alternative solutions, such as accelerated tests, HW/SW fault injections, etc. are preferred.

16.3 Ground accelerated tests

Accelerated tests are performed in facilities, such as synchrotrons, linear accelerators, etc. providing important fluxes of different kind of particles, such as protons, heavy ions, neutrons, gamma and alpha. It is important to note that they are not able to create particles identical (in energy, LET, etc) to the ones found in space. However, the important parameter characterizing the interaction between a particle and matter beeing the LET, particle accelerators are calibrated to provide particles having similarities than the ones of particles present in the natural environment

16.3.1 Standards and specifications

Several standards describe the test methods for devices and the result reporting according to each type of considered particles.

Table 16-1 depicts the different standards and their field of application, used to qualify integrated circuits with respect to radiation. As it can be seen, there is currently no method for displacement damage testing; this is mainly due to the following reasons:

- Modes of degradation are very complex
- Induced electrical effects are mainly application dependent
- Annealing mechanisms occur depending on the type of devices and applications

Table 16-1 : The different standards for IC qualification and their field of application

Standard reference	Standard name	Particle source
ESA/SCC 25100	SEE testing of integrated circuits and discrete semiconductors devoted to space applications	Protons Heavy ions
JEDEC JESD57	Test Procedures for the Measurement of Single-Event Effects in Semiconductor Devices from Heavy Ion Irradiation	Heavy ions
ESA/ESCC 22900	Total Dose Steady-State Irradiation Test Method	Gamma
MIL-STD-883/ 1019.4	Ionizing radiation (total dose) test procedure	Gamma
JEDEC JESD89A	Measuring and reporting of alpha particle and terrestrial cosmic ray-induced soft errors in semiconductor devices	Alpha Neutrons

16.3.2 Test methodologies

Two types of tests can be performed on the Device Under Test (DUT) to evaluate its sensitivity to upsets. They are addressed as static test and dynamic test and deal with circuits having memory cells such as processors, FPGAs, memories.

16.3.2.1 Static test

A static test is performed by initializing all the DUT's memory cells before exposing it to the particles. During exposition the device is powered but left in an idle mode (without activity). After a period of time, the beam is shut down and the DUT's memory cells are compared with the expected values (Figure 16-1).

This test is used to obtain the static cross-section curve. This graph represents the worse case sensitivity because real applications do not use all the device's resources and the content of each memory element is not critical at any instant. The result of a static test characterizes the device itself, independently of the final application.

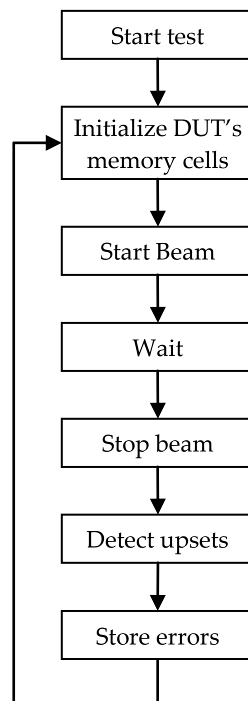


Figure 16-1 : Flow chart of a typical static test

16.3.2.2 Dynamic test

The purpose of a dynamic test is to evaluate the error-rate of a system operating in conditions similar to the ones of the final application. As shown on Figure 16-2, this is performed by running the final application under beam until an error is detected on the application's outputs. The drawback of this strategy is that any change in the application may require performing a new test campaign.

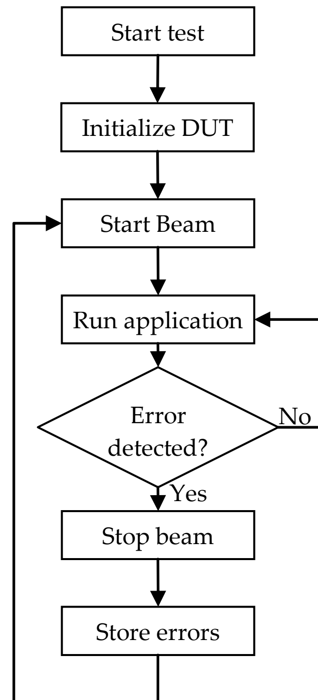


Figure 16-2 : Flow chart for a typical dynamic test

16.3.3 Test facilities

Test methodologies strongly differ depending on the phenomenon to analyze. Moreover the application's final environment defines the population of particles to be taken into account. Consequently this has an impact on the number of facilities capable to perform the required tests:

Total Ionizing Dose: for this kind of characterization, parameters need to be measured at different dose levels. Main used source for this is Cobalt 60, but proton accelerators are also suitable. The problem with protons is that they generate displacement damage at the same time.

Single Event Effect: requires on-line testing of the different device parameters and functionalities. Particle accelerators have to be used either with protons or heavy ions.

Displacement Damage: parameters need to be measured at different particle fluencies corresponding to different displacement damage doses. Particle accelerators are used (electrons, protons and neutrons).

16.3.3.1 Total ionizing dose

Different potential sources exist for total dose testing. Among them, can be mentioned particle accelerators (electrons and protons), X-ray machines and radioactive sources. Advantages and drawbacks of each are summarized in Table 16-2.

Table 16-2 : Main features of the radiation sources available for TiD testing

Radiation sources	Advantages	Drawbacks
Electrons (accelerator)	High dose rate available Representative of some orbits	Costly Not suitable for low dose rate
Protons (accelerator)	High dose rate available Representative of some orbits	Displacement damage contribution Costly
X-rays (photons)	High dose rate available Low cost	Dose enhancement effect Not suitable for low dose rate
Cs137 & Co60 (gamma rays)	Very large dose rate range Dose uniformity	Heavy shielding required Non-dominant in orbit

Particle accelerators have the advantage to provide high dose rates which are representative of some orbits. On the other hand such facilities are associated to a non-negligible cost. Moreover, protons may provoke displacement damage in the target device, adding an extra-degradation to the one issued from the dose.

X-rays generators are convenient, but due to the low energy of the emitted photons, the deposited dose is not uniform over the depth near each interface between different materials. This effect is called “dose enhancement” effect [256].

Radioactive Cs137 and Co60 sources deliver gamma rays and, even if this type of radiation is minor in space environments, present two strong advantages: firstly they provide a very wide range of dose rates, secondly the total dose is well controlled in the device thickness. As photons delivered by Co60 have a large energy, 1.17 and 1.33 MeV, dose uniformity is ensured. Gamma sources (mainly Co60) are the most widely used facilities for TID testing and can be found in two features.

16.3.3.2 Single event effects

Single event effects are mainly studied using particle accelerators which are able to produce different types of beams such as heavy ions, protons, neutrons, etc. It is important to note that in-air irradiation is not possible in most of the heavy ion facilities due to the limited energy and range of the particles. Consequently target devices must be placed in a vacuum chamber with cable feedthroughs.

In the following is given a list of accelerators available in Europe and the US classified by particle types and energy ranges:

Heavy ions

A non exhaustive list of heavy ion facilities is given in Table 16-3.

Table 16-3 : Non-exhaustive list of worldwide heavy-ion facilities

Facility	Energy
GANIL - France	100 MeV/amu[20]
CYCLONE - Belgium	10 MeV/amu
JYFL - Finland	10 MeV/amu
IPN - France	≤ 10 MeV/amu
LNL - Italy	≤ 10 MeV/amu
Texas A&M University - USA	15, 25 and 40 MeV/amu
Brookhaven National Laboratory - USA	85 MeV/amu
Berkeley - USA	32.5 MeV/amu

Protons

Several facilities are available for device testing using protons. A non-exhaustive list is given in Table 16-4. As energy losses for proton in the air are low, all irradiations are performed in the air avoiding the complexity of the vacuum system.

Table 16-4 : Non-exhaustive list of worldwide proton facilities

Facility	Energy
CYCLONE - Belgium	Up to 70 MeV
JYFL - Finland	Up to 60 MeV
CPO - France	Up to 200 MeV
IPN - France	Up to 20 MeV
SIRAD - Italy	Up to 28 MeV
PSI/OPTIS - Switzerland	Up to 63 MeV
PSI/PIF - Switzerland	Up to 300 MeV
Crocker Nuclear Laboratory - USA	Up to 68 MeV
Lawrence Berkeley Laboratory - USA	Up to 55 MeV
Indiana University - USA	Up to 200 MeV
Triumf - Canada	Up to 520 MeV
GNPI - Russia	Up to 1 GeV

[20] Atomic Mass Unit, which corresponds to 1/12 of a carbon atom with 12 nucleons. 1 AMU = 1.66054×10^{-27} Kg

Neutrons

Neutron tests mainly concern avionic applications but start to be a major concern for all electronic equipments, even those operating at ground level. The JEDEC standard JESD89 [257] states that the preferred facility to perform the neutron test is WNR (Los Alamos - USA) because its energy spectra is close to the neutron spectra at sea level (Figure 16-3). However, the same standard explains how to reach data using quasi-mono-energetic neutron beams, which is available in Europe.

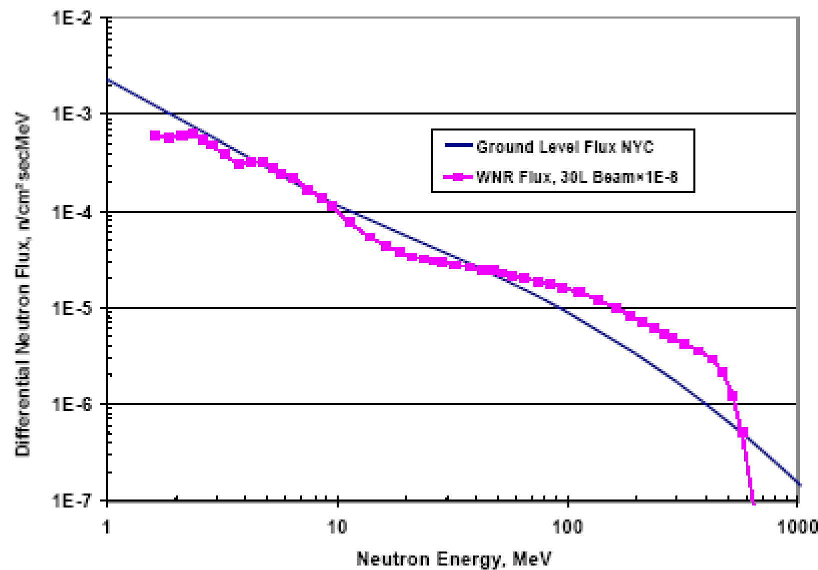


Figure 16-3 : neutron fluxes in NY City and at LANL (reduced with a factor 1E8)

Two accelerators are equipped with neutron beam lines in Europe:

- CYCLONE (Belgium) has a quasi-mono-energetic line and a high flux line.
- Svedberg Laboratory (Sweden) has a large range of quasi-mono-energetic in the energy range 20 - 180 MeV.

Californium-252 and Americium-241 can be used to get a preliminary estimation of the SEE sensitivity of studied circuits. As an example, can be mentioned the ESTEC Californium Assessment for Single event Effects (CASE) System which produce a wide range of high-energy particles having an average LET of 43 MeV/(mg/cm^2).

Complementary tools

Aside from the standard facilities used for SEE testing, some complementary tools bring some additional help when dealing with SEE.

SEE characterization using heavy ion beams is a global approach. It allows getting the circuit cross-section, which is mandatory for the estimation of the circuit sensitivity on the final environment, but it does not provide information (instant of occurrence, location) of events having provoked the observed errors. Unlike the broad-beam approach which consists in irradiating the whole surface of a device, alternative tools such as lasers or microbeams, allows performing localized exposure (spot diameter of the order of 1 μm) and then correlating a structure to an observed failure mode.

Laser beams

A small laser spot and a precise localization of the laser light impact allow sensitive device nodes to be pinpointed with submicron accuracy [258][259][260][261]. The major problems of this technique is that

the laser light is reflected by metallization layers and the penetration depth is only a few micron (a 815 nm laser penetrates 12μm in Si).

The test process generally starts using a defocused beam to define sensitive regions. A tightly focused laser spot at higher magnification is then used to pinpoint sensitive nodes within the regions identified previously.

During classical SEE characterization using heavy ion beams, the cross section is plotted as a function of the LET which is not straightforward with lasers. An energy calibration needs to be performed in order to obtain a correlation between the laser energy and LET. It is to note that this calibration needs to be performed for each laser wavelength. Using a heavy ion micro-beam overcomes this problem.

A laser can be triggered by the test application permitting the temporal characterization of the anomaly [262] [263].

Microbeam

A microbeam is a narrow beam of radiation, of micrometer or sub-micrometer dimensions. Such facilities permit exposing circuits to heavy-ion beams to address specifically the impact on a reduced area of the application.

In Europe, only one facility is equipped with a microbeam: GSI (Darmstadt, Germany). This facility uses its linear accelerator to produce ions from carbon to uranium energies between 1.4 MeV/amu and 11.4 MeV/amu.

In conclusion, laser beams and microbeams are not suitable to characterize a device (measure of the σ(LET) sensitivity curve). However these tools are very useful to help understanding failure modes. A summary of the characteristics of each type of beam is given in Table 16-5.

Table 16-5 : Summary of the characteristics of laser and microbeams

	Heavy Ion Beams	**Laser**	**Heavy Ion Micro-beam**
Beam diameter on DUT	A few cm	Down to 1 μm	Down to 1 μm
Limitations	Range several tenths of μm	Small penetration depth	Range several tenths of μm
Localization of sensitive areas	NO	YES	YES
Study of rare phenomena	NO	YES	YES
Cross section determination	YES	NO	YES

Californium-252

Californium-252 is an artificial radioactive element that spontaneously fissions into several fragments (Figure 16-4), alpha particles and neutrons. Fission fragments that represent only 3% of the total amount of fission products are useful for SEE purpose.

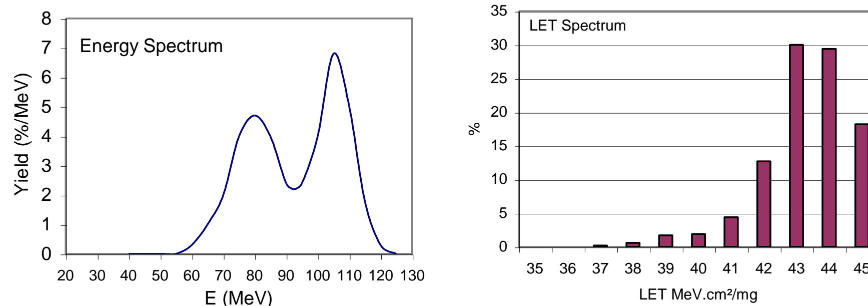


Figure 16-4 : Fragments energy spectrum (left) and LET spectrum (right)

Because of their low energy, the emitted ions are easily stopped (range of about 15µm in Silicon) and they are not representative of particles in space. However, the mean LET value (around 43MeV/mg.cm²) allows inducing errors in devices and debugging test set-up before moving to the accelerator site.

Americium-241

Americium-241 is used as an alpha particle emitter in order to simulate the radioactivity of packages. For this purpose, it is recommended in the recent JEDEC JESD89 standard that addresses the avionics and terrestrial SEE issues.

16.3.4 Practical constraints

Particle accelerators impose some constraints the designer must be aware of as they must be taken into account when designing the DUT test platform:

- Heavy-ion testing, except for high-energy beams, is performed under vacuum. This implies the use of specific connectors available on the vacuum chamber. These connectors may not meet the requirements (in term of impedance, speed, etc) of some applications.
- Another consequence of vacuum is the temperature control issue. It must be taken into account that the only way the dissipation energy is by conduction by using power-planes on the board and the chassis holding the testbed. Temperature has a large influence on SEL testing as an increasing temperature will decrease the LET threshold and increase the cross-section saturation [264]. Several facilities propose a water cooling system to cope with the heat dissipation issue.
- Unlike heavy-ion beams which keep focused, during proton and neutron irradiation the whole tester may be exposed to particles. Consequently special care needs to be taken such as shielding in order to protect the acquisition and monitoring system. Another solution is to deport the DUT from the tester, but this is not always possible as it strongly depends on the constraints imposed by the application.
- Proton and neutron lines are always placed in well shielded caves for radiation safety issues. It means that the whole test system must be remotely controlled.

- Electrical noise may be a critical issue while working around accelerators due to the proximity of intense electromagnetic fields in the accelerator. In order to avoid problem during experiments, it is needed to optimize test systems by efficient grounding techniques and eventually shielding for critical applications.
- It is important to note the non-negligible impact of the DUT operation frequency during the radiation ground testing. From example, in reference [196] is described a test done at different frequencies on a DICE-latch shift register chain (0.25 μm). The error rate increased almost 1000 times for the DICE type flip-flop structure when the test frequency increased from 1 to 200 MHz.

16.3.5 DUT preparation

Depending on the nature of the used beam, the sample may require a preparation in order to expose sensitive area of the die to the particles. It is the case for heavy ions and low energy protons (below 10MeV) which require opening the packages. This operation can be easily done for circuits having a metallic lid Plastic and ceramic packages require mechanical or chemical processes to expose the die. Such attacks may have destructive consequences, in some cases requiring the rebounding of the chip.

If the DUT's die is mounted in a flip-chip package, then the penetration length of the particles must be taken into account. Indeed, if the particle track length becomes too short, the observed device's sensitivity might be underestimated. In the worst case, the particles may not even reach the active volumes and no effect is generated. A die thinning process must be performed using grinding machines in order to cope with this problem whenever the particle's penetration length is below or close to the bulk thickness. However, this method has drawbacks such as weakening the device and creating thickness variations. During grinding, samples will have thickness variations across the surface. This induces LET variations from part to part of the device, and thus data will be influenced.

16.4 Fault injection

Fault injection is defined as the deliberate insertion of faults into an operational system in order to observe its response [265]. Two main reasons may motivate such experiments: either anticipate the behaviour towards radiation of the device being designed in order to operate some adjustments before manufacturing the chip; or to validate the circuits and the embedded mitigation techniques.

A fault injection scheme can take place at several abstraction levels:

- Transistor level: the DUT is a single transistor.
- Gate level: the DUT is a set of transistors realizing a simple function (logical gates, memory cells, etc) or complex functions (arithmetic or logical units, bus structures, etc).
- Device level: the DUT is the whole device.
- System level: the DUT is considered to be a whole system.

More details about each technique can be found in reference [266].

16.4.1 Fault injection at transistor level

Fault injection is an attractive technique for the evaluation of design characteristics such as reliability, safety and fault coverage [267].

16.4.1.1 Physical level 2D/3D device simulation

Fault injection at transistor level aims at simulating the effects of an energetic particle hitting the transistor. More precisely, it considers the interactions between the particle and the device depending on its geometry. The desired result is a probability distribution as a function of the charge deposited in the sensitive volume. Such a study can be carried both for analogue and digital circuits.

Physical level 2D/3D device simulation is possible using commercial tools. They are able to simulate ion tracks with different locations, directions and ranges for a single transistor or an entire logic cell [268][269][270][271]. The structure of the device is represented in 2D/3D and the simulation can be performed either manually or semi automatically to a certain extent.

An exact 2D/3D representation of the structure of the device is made out of the real device layout for any given technology. This type of simulation allows obtaining the corresponding transient current generated by a collision between a charged particle and a transistor (or an entire logic cell). This is useful for designers willing to found out the most vulnerable nodes of their transistors and to determine the minimum critical energy of charged particles. However this methodology requires important costs in terms of CPU computing power.

16.4.1.2 Transient fault injection simulations at electrical level

This type of fault injection focuses on the consequence of a collision between an energetic particle and a transistor's sensitive volume: the resulting transient current pulse. Each circuit element (memory cell, logic gate, etc) must be simulated to determine the magnitude and the shape of the potential voltage transient that may appear on the cell's outputs. This voltage transient is a function of the transient current pulse whose characteristics can be obtained from physical 2D/3D simulation.

Electrical level fault simulations are generally performed using electrical models such as SPICE (Simulation Program with Integrated Circuit Emphasis) using built-in technology parameters (such as Vth, Tox, Vdd, etc). A current generator configured to reproduce the current pulse issued from physical level 2D/3D simulation is added to the DUT electrical model. Such simulations can be obtained from any commercial, freeware SPICE or analog simulator. Injection points can be chosen either manually or automatically by means of simulation scripts.

Electrical simulations are much faster than physical 2D/3D simulations. However it is still a time consuming process and dependability analysis on a complex circuit is not affordable due to the important number of nodes to take into account. Nevertheless it is a powerful tool for designers willing to compute the electrical masking factors while building the complete FIT (Failure In Time) model calculation.

16.4.2 Fault injection at gate level

Fault injection simulation at gate level consists in evaluating the DUT response to the presence of a fault using simulation tools. The fault injection strategy can be implemented in two different ways:

- The HDL (Hardware Description Language) model of the DUT, written in Verilog or VHDL, is modified in order to be able to simulate bit-flips or transients in the model. Several tools adopting such a strategy are available [272][273][274][275].

- Fault injection is performed by using simulation commands. Nowadays, some simulators directly integrate in their instruction set commands to force values within the DUT model [276]. The advantage of this method is that it is not intrusive. Indeed, both the simulation tool and the DUT model are left unchanged.

16.4.3 Fault injection at device level

At device level, fault injection is performed directly on the physical device, this is why these techniques are also called hardware/software fault injection. Consequently, this level of abstraction requires having the DUT manufactured and a board embedding the DUT, the tester, developed.

The objective is to inject faults directly in the final application. As a consequence, the main advantages are the following:

- Faults are not injected in a simulation, but on the real final application. Consequently the accuracy of the results does not rely on the used models and parameters.
- Performances are neither CPU limited nor DUT complexity dependent.
- The methodology allows qualifying the device and its application at the same time which can be useful in case mitigation techniques are applied both on the hardware and the software.

State-of-the-art techniques mainly target complex digital devices such as processors and SRAM and Flash-based FPGAs.

16.4.3.1 Fault injection in processors

This section deals with architectures organized around a device (a processor) capable of executing instruction sequences and with the possibility of taking into account asynchronous signals (i.e. interruptions, exceptions). In principle, this processor can be programmed to directly or indirectly perform read and write operations of any of the external SRAM locations, as well as its internal registers and memory area.

The following will present the CEU (Code Emulated Upsets) method [277]. This methodology combines two concepts in order to provide a prediction for the error rate of processor architectures (the device and its associated application). The first concept defines how bit-flips can be simulated in the DUT while the second concept combines the results obtained from the fault injection with the DUT's sensitivity measured in particle accelerators to predict the application error-rate.

The fault injection mechanism

For most existing processors, bit-flips can be injected by software means concurrently with the execution of a program, as the result of the execution, at a desired instant, of dedicated sequences of instructions. In the following, such software simulated bit-flips will be called CEU. The piece of code able to provoke the CEU occurrence will be called CEU code. The memory location in which the upset is injected will be called CEU target.

Typically, injecting a bit-flip at a general purpose register or at directly addressable internal or external memory location needs only a few instructions to perform the following tasks:

a. Reading the existing content of the CEU target.

b. XOR-ing it (perform the exclusive-or logic operation) to an appropriate mask value (having "1" for those bits that are to be flipped and "0" elsewhere).

c. Writing the corrupted value back to the CEU target location.

The only remaining step required to emulate an upset is to trigger the execution of the CEU code at the desired instant. If the CEU code is located in a suitable memory space (external SRAM for instance) at a predefined address, pointed to by the interruption vector (or an equivalent mechanism), this step can be achieved by asserting an interruption. Indeed, in response to an interrupt signal assertion, the processor will perform the following tasks:

a. Suspending the program execution after completion of the currently executed instruction.

b. Save the context (at least the program counter content), for instance in the stack if available.

c. Jump to the CEU code and execute it, provoking the upset.

d. Restore the context from the stack and resume the program execution.

As a result of this four-step activity, the program will be executed under very close conditions to those appearing when a bit flip occurs as the result of a particle having enough energy to provoke an SEU, hitting the circuit at the same considered instant and target bit.

The drawback of this concept is that the prediction accuracy relies on the capability of the processor's instruction set to access all its registers and internal memory elements. Indeed, faults occurring in a register not accessible by the instruction set cannot be perturbed by this method and consequently is not included in the prediction. In this case the prediction under-estimates the real error-rate.

<u>**Application error-rate prediction**</u>

The result of a fault injection, performed as described above, is a number of errors on the application outputs as a function of the number of injected bit-flips. This is the application error-rate, called τ_{inj}, and can be defined by the following equation:

$$\tau_{inj} = \frac{\#errors}{\#injected\ bit\ flips} \quad (1)$$

τ_{inj} can also be interpreted as the average number of bit-flips required to provoke an error in the program. However this figure provides only the error-rate for the application, not for the whole system, i.e. the device and its application. Indeed the system error-rate would be defined as the average number of particles required to provoke an error in the application. The missing data in the equation is the probability for a particle to generate an upset in the device. As a matter of fact this is the definition of the static cross-section measure whose equation is reminded here:

$$\sigma_{sta} = \frac{\#\ of\ observed\ bitfips}{fluency} \quad (2)$$

Thus, the complete system error-rate is obtained by combining (1) and (2):

$$\sigma_{seu} = \tau_{inj} * \sigma_{sta} \quad (3)$$

The main advantage of the CEU method relies on the fact that particle accelerator campaigns need to be done only once to obtain the static cross-section. The remaining part of the prediction does not require a beam. Moreover, future versions of the application software can be evaluated without further tests in beam facilities.

The CEU method was recently applied to a complex processor, the PowerPC 7448 [278], and the predicted results were close to the measures obtained from particle accelerator campaigns.

16.4.3.2 Fault injection in FPGAs

Several fault-injection approaches are documented in the state-of-the-art. The process involves inserting faults into particular targets in a system and monitoring the results to observe the produced effects. All these approaches emulate the effects of Single Events in the FPGA's memory such as bit-flips in the bitstream that is downloaded in the FPGA during its programming phase. Some of them use run-time re-configuration [279], while others modify the bitstream before downloading it in the device configuration memory or during download operations [162][280]. Although the fault-injection approaches permit to evaluate the effects of SEs in all the memory bits, the time needed by the fault-injection process is still huge (from a few days to several weeks depending on the complexity of the device and of the application.), even in the case the process is optimized by the use of partial re-configuration.

As an example, the CEU method devoted to processors, presented in section 16.4.3.1, can be adapted to reprogrammable FPGAs (whose configuration memory is based on SRAM or Flash technology) and will be detailed is the following. As for processors, the purpose of fault injection in FPGAs is double: on one hand evaluating the application sensitivity and its weaknesses and on the other hand predicting the system error-rate.

Indeed, the error-rate calculation method remains the same. Only the fault injection mechanism must fit the FPGA architecture. As long as the device's configuration memory can be written and read by third party software, faults can be injected using these built-in functions.

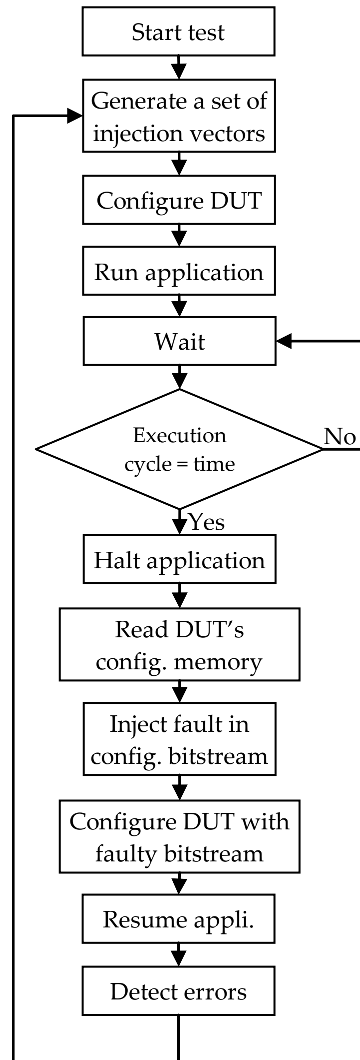


Figure 16-5 : Flow chart for fault injections in FPGAs

As depicted in Figure 16-5, a fault injection sequence starts by generating the vectors characterizing the fault to be injected, which are called *injection vectors*. One vector specifies the instant of fault injection while the second vector is the target bit inside the memory configuration bitstream. The DUT is then configured and the application started. When the execution clock cycle meets the instant stated by the injection vector, the application is halted in order to perform a read of the configuration memory. The fault in then injected into the target memory bit according to the target injection vector. Finally the DUT is configured with the faulty bitstream and the application resumed. An analysis of the application's outputs allow to conclude on the impact of the injected fault.

The main advantage of the CEU method applied to FPGAs over the CEU method applied to processor is a full fault coverage as for FPGAs the set of potential sensitive cells is accessible through the configuration memory. Consequently the error-rate predictions are very close to results obtained from radiation test campaigns performed in particle accelerators [281].

However, one drawback is that some manufacturers do not supply complete description about the bitstream format. This prevents from knowing the nature of the resources impacted by the injected fault and a correlation cannot be made between the target memory bit and its function in the application.

16.4.4 Fault injection at system level

A representative example of integrated design and fault-injection environment at system level is DEPEND [282]. This tool is able to model fault-tolerant architectures and perform extensive fault-injection experiments.

The components of the studied system, as well as their interactions, are described by resorting to a collection of interacting processes. This approach has several benefits:

- It is an effective way to model system behavior, repair schemes, and system software in detail.
- It simplifies modeling of inter-component dependencies, especially when the system is large and the dependencies are complex.
- It allows programs to be executed within the simulation environment.

DEPEND has a library of build-in objects. Some simpler items perform basic tasks such as fault injection and result analysis. Some of the more complex objects are listed hereafter:

- Processors
- Self-checking processors
- N-modular redundant processors
- Communication links
- Voters
- Memories

The work of the designer is to describe his system's behavior by instantiating the library's objects in a control program written in C++. The program is then compiled and linked to the DEPEND objects and the run-time environment.

It can then be executed in a simulated parallel run-time environment where the system's behavior is evaluated. Faults are injected, repair schemes are initiated and reports classifying faults' effects are generated during this process.

16.5 Analytical methods

Predicting effects of soft errors on SRAM-based FPGAs

Although the fault-injection approaches (see section 16.4.3.2) allow the evaluation of the effects of soft errors in all the memory bits, the time needed by the fault-injection process is still important, even in the case the process is optimized by the use of partial re-configuration of the device.

To overcome the time-consuming processes needed by the fault-injection approaches and to avoid the high cost of radiation testing, analytical approaches based on synthesis tools and software programs are proposed in [283] [284] [285].

In [283] a static estimation of the design's susceptibility to soft errors is proposed assuming that all the bits of a design are susceptible at all times.

Differently, in [284] an approach is proposed that identifies the paths sensitive to soft errors by calculating the error-rate probability of all circuit nodes and by combining it with the error-propagation probability of each net within the design. Then, the obtained information is coupled with the sensitivity of the FPGA's configuration memory bits.

In [285] the authors developed an approach able to analyze the topology of the design implemented on the SRAM-based FPGA, in particular when TMR design techniques are adopted [286] [287]. The

analysis is then coupled with a set of reliability constraints. According to the authors this technique is able to achieve the same accuracy than more time-consuming approaches, like fault injection, while the execution time is orders of magnitude smaller. The philosophy of this method is based on analyzing the effects of soft errors in all the resources a SRAM-based FPGA embeds, as soon as a model of the placed and routed design is available.

Annex A References

[1] J. Barth, "The Radiation Environment," *http://radhome.gsfc.nasa.gov/radhome/papers/apl_922.pdf*, 1999.

[2] R. L. Moore A. C. Sterling, "Initiation of Coronal Mass Ejections," *Solar Eruptions and Energetic Particles AGU Geophysical Monograph Series 165*, pp. 43-57, 2006.

[3] R. A. Mewaldt, "Cosmic Rays," *Macmillan Encyclopedia of Physics, http://www.srl.caltech.edu/personnel/dick/cos_encyc.html*, 1996.

[4] F. V. Dos Santos, "Techniques de conception pour le durcissement des circuits intégrés face aux rayonnements," *Thèse de doctorat de l'Université Joseph Fourier*, 1998.

[5] R. D. Evan, *The Atomic Nucleus*. New York: McGraw-Hill, 1955.

[6] W. E. Meyerhof, *Elements of Nuclear Physics*. New York: McGraw-Hill, 1967.

[7] R. C. Baumann E. B. Smith, "Neutron-induced boron fission as a major source of soft errors in deep submicron SRAM devices," *Reliability Physics Symposium, 2000. Proceedings. 38th Annual 2000 IEEE International*, p. 152, 2000.

[8] "Circumventing Radiation Effects By Logic Design: Cookbook," *ESA contract 12495/97/NL/FM*, Jul. 1999.

[9] "Calculation of Radiation and its Effects and Margin Policy Handbook," *ECSS-E-HB-10-12A*.

[10] D. G. Mavis D. R. Alexander, "Employing radiation hardness by design techniques with commercial integrated circuit processes," *Digital Avionics Systems Conference, 1997*, vol. 1, pp. 15-22, Oct. 1997.

[11] R. Koga, S. H. Penzin, K. B. Crawford, W. R. Crain, "Single event functional interrupt (SEFI) sensitivity in microcircuits," *Radiation and Its Effects on Components and Systems, 1997. RADECS 97. Fourth European Conference on*, pp. 311-318, Sep. 1997.

[12] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies ," *Radiation-induced soft errors in advanced semiconductor technologies* , vol. 5, no. 3, pp. 305-316, 2005.

[13] P. Roche G. Gasiot, "Impacts of front-end and middle-end process modifications on terrestrial soft error rate," *Device and Materials Reliability, IEEE Transactions on*, vol. 5, no. 3, p. 382, Sep. 2005.

[14] H. Puchner, R. Kapre, S. Sharifzadeh, J. Majjiga, R. Chao, D. Radaelli, S. Wong, "Elimination of Single Event Latchup in 90nm SRAM Technologies," *Reliability Physics Symposium Proceedings, 2006. 44th Annual., IEEE International* , p. 721, Mar. 2006.

[15] J. A. Pellish, et al., "Substrate Engineering Concepts to Mitigate Charge Collection in Deep Trench Isolation Technologies," *Nuclear Science, IEEE Transactions on* , vol. 53, no. 6, p. 3298, Dec. 2006.

[16] E. Simoen, A. Mercha, C. Claeys, N. Lukyanchikova, "Low-frequency noise in silicon-on-

insulator devices and technologies," *Solid State Electronics*, vol. 51, pp. 16-37, 2007.

[17] S. Cristoloveanu S. S. Li, *Electrical Characterization of Silicon-On-Insulator Materials and Devices*. Springer, 1995.

[18] K. Hirose, H. Saito, S. Fukuda, Y. Kuroda, S. Ishii, D. Takahashi, K. Yamamoto, "Analysis of body-tie effects on SEU resistance of advanced FD-SOI SRAMs through mixed-mode 3-D Simulations," *Nuclear Science, IEEE Transactions on*, vol. 51, no. 6, pp. 3349-3353, Dec. 2004.

[19] J. R. Schwank, V. Ferlet-Cavrois, M. R. Shaneyfelt, P. Paillet, P. E. Dodd, "Radiation effects in SOI technologies," *Nuclear Science, IEEE Transactions on*, vol. 50, no. 3, pp. 522-538, Jun. 2003.

[20] V. Ferlet-Cavrois, G. Gasiot, C. Marcandella, C. D'Hose, O. Flament, O. Faynot, J. du Port de Pontcharra, C. Raynaud, "Insights on the transient response of fully and partially depleted SOI technologies under heavy-ion and dose-rate irradiations," *Nuclear Science, IEEE Transactions on* , vol. 49, no. 6, p. 2948, Dec. 2002.

[21] P. Gouker, J. Burns, P. Wyatt, K. Warner, E. Austin, R. Milanowski, "Substrate removal and BOX thinning effects on total dose response of FDSOI NMOSFET," *Nuclear Science, IEEE Transactions on* , vol. 50, no. 6, p. 1776, Dec. 2003.

[22] J. Roig, D. Flores, S. Hidalgo, J. Rebollo, J. Millan, "Thin-film silicon-on-sapphire LDMOS structures for RF power amplifier applications," *Microelectronics J.*, vol. 35, pp. 291-297, 2004.

[23] H. M. Manasevit W. I. Simpson, "Single-crystal silicon on a sapphire substrate," *Journal of Applied Physics*, vol. 35, no. 4, p. 1349, 1964.

[24] F. P. Heiman, "Thin-film silicon-on-sapphire deep depletion MOS transistors," *Electron Devices, IEEE Transactions on*, vol. 13, no. 12, pp. 855-862, Dec. 1966.

[25] T. Sato, J. Iwamura, H. Tango, K. Doi, "CMOS/SOS VLSI technology," *Material Research Society Proceedings*, vol. 33, p. 3, 1984.

[26] J. E. A. Maurits, "SOS wafers—Some comparisons to silicon wafers," *Electron Devices, IEEE Transactions on*, vol. 25, no. 8, pp. 859-863, Aug. 1978.

[27] G. E. Davis, L. R. Hite, T. G. W. Blake, C. .-E. Chen, H. W. Lam, R. DeMoyer, "Transient Radiation Effects in SOI Memories ," *Nuclear Science, IEEE Transactions on* , vol. 32, no. 6, pp. 4431-4437, Dec. 1985.

[28] T. Ikeda, S. Wakahara, Y. Tamaki, H. Higuchi, "A soft error immune 0.35 µm PD-SOI SRAM technology compatible with bulk CMOS," *SOI Conference, 1998. Proceedings., 1998 IEEE International* , pp. 159-160, 1998.

[29] Y. Hirano, T. Matsumoto, S. Maeda, T. Iwamatsu, T. Kunikiyo, K. Nii, K. Yamamoto, Y. Yamaguchi, T. Ipposhi, S. Maegawa, M. Inuishi, "Impact of 0.10 µm SOI CMOS with body-tied hybrid trench isolation structure to break through the scaling crisis of silicon technology," *Electron Devices Meeting, 2000. IEDM Technical Digest. International* , p. 467, 2000.

[30] G. Gasiot, V. Ferlet-Cavrois, P. Roche, P. Flatresse, C. D'Hose, O. Musseau, J. du Port de Poncharra, "Comparison of the sensitivity to heavy ions of 0.25 µm bulk and SOI technologies," *Radiation and Its Effects on Components and Systems, 2001. 6th European Conference on* , pp. 211-216, 2001.

[31] S. Hareland, J. Maiz, M. Alavi, K. Mistry, S. Walsta, C. D., "Impact of CMOS process scaling and SOI on the soft error rates of logic processes ," *VLSI Technology, 2001. Digest of Technical Papers. 2001 Symposium on* , pp. 73-74, 2001.

[32] P. E. Dodd, M. R. Shaneyfelt, J. A. Felix, J. R. Schwank, "Production and propagation of single-event transients in high-speed digital logic ICs ," *Nuclear Science, IEEE Transactions on* , vol. 51, no. 6, pp. 3278-3284, Dec. 2004.

[33] Y. Li, G. Niu, J. D. Cressler, J. Patel, P. W. Marshall, H. S. Kim, M. S. T. Liu, R. A. Reed, M. J. Palmer, "Proton radiation effects in 0.35 µm partially depleted SOI MOSFETs fabricated on

UNIBOND," *Nuclear Science, IEEE Transactions on* , vol. 49, no. 6, pp. 2930-2936, Dec. 2002.

[34] S.-W. Fu, A. M. Mohsen, T. C. May, "Alpha-particle-induced charge collection measurements and the effectiveness of a novel p-well protection barrier on VLSI memories," *Electron Devices, IEEE Transactions on* , vol. 32, no. 1, p. 49, Jan. 1985.

[35] D. Burnett, C. Lage, A. Bormann, "Soft-error-rate improvement in advanced BiCMOS SRAMs," *Reliability Physics Symposium, 1993. 31st Annual Proceedings., International* , p. 156, Mar. 1993.

[36] Y. Tosaka, H. Ehara, M. Igeta, T. Uemura, H. Oka, N. Matsuoka, K. Hatanaka, "Comprehensive study of soft errors in advanced CMOS circuits with 90/130 nm technology," *Electron Devices Meeting, 2004. IEDM Technical Digest. IEEE International* , p. 941, Dec. 2004.

[37] H. Puchner, D. Radaelli, A. Chatila, "Alpha-particle SEU performance of SRAM with triple well," *Nuclear Science, IEEE Transactions on* , vol. 51, no. 6, p. 3525, Dec. 2004.

[38] T. Kishimoto, M. Takai, Y. Ohno, T. Nishimura, M. Inuishi, "Control of Carrier Collection Efficiency in n+p Diode with Retrograde Well and Epitaxial Layers," *Japanese Journal of Applied Physics*, vol. 36, no. 1, p. 3460–3462, 1997.

[39] M. Takai, T. Kishimoto, Y. Ohno, H. Sayama, K. Sonoda, S. Satoh, T. Nishimura, H. Miyoshi, A. Kinomura, Y. Horino, K. Fujii, "Soft error susceptibility and immune structures in dynamic random access memories (DRAMs) investigated by nuclear microprobes ," *Nuclear Science, IEEE Transactions on* , vol. 43, no. 2, p. 696, Apr. 1996.

[40] W. Morris, L. Rubin, D. Wristers, "Buried layer/connecting layer high energy implantation for improved CMOS latch-up," *Ion Implantation Technology. Proceedings of the 11th International Conference on* , p. 796, Jun. 1996.

[41] D. R. Alexander, "Transient ionizing radiation effects in devices and circuits," *Nuclear Science, IEEE Transactions on* , vol. 50, no. 3, p. 565, Jun. 2003.

[42] H. Momose, T. Wada, I. Kamohara, M. Isobe, J. Matsunaga, H. Nozawa, "A P-type buried layer for protection against soft errors in high density CMOS static RAMs," *Electron Devices Meeting, 1984 International* , vol. 30, p. 706, 1984.

[43] M. R. Wordeman, R. H. Dennard, G. A. Sai-Halasz, "A buried N-grid for protection against radiation induced charge collection in electronic circuits," *Electron Devices Meeting, 1981 International* , vol. 27, p. 40, 1981.

[44] H. Puchner, Y. .-C. Liu, W. Kong, F. Duan, R. Castagnetti, "N-Well Engineering to Improve Soft-Error-Rate Immunity for P-Type Substrate SRAM Technologies," *Solid-State Device Research Conference, 2001. Proceeding of the 31st European* , p. 295, Sep. 2001.

[45] S. Voldman, L. Lanzerotti, W. Morris, L. Rubin, "The influence of heavily doped buried layer implants on electrostatic discharge (ESD), latchup, and a silicon germanium heterojunction bipolar transistor in a BiCMOS SiGe technology," *Reliability Physics Symposium Proceedings, 2004. 42nd Annual. 2004 IEEE International* , p. 143, Apr. 2004.

[46] D. McMorrow, T. R. Weatherford, A. R. Knudson, S. Buchner, J. S. Melinger, L. H. Tran, A. B. Campbell, P. W. Marshall, C. J. Dale, A. Peczalski, S. Baiers, "Charge-collection characteristics of GaAs heterostructure FETs fabricated with a low-temperature grown GaAs buffer layer," *Radiation and its Effects on Components and Systems, 1995. RADECS 95., Third European Conference on* , p. 373, Sep. 1995.

[47] H. L. Hughes J. M. Benedetto, "Radiation effects and hardening of MOS technology: devices and circuits," *Nuclear Science, IEEE Transactions on* , vol. 50, no. 3, p. 500, Jun. 2003.

[48] J. A. Diniz, J. G. Fo, M. B. P. Zakia, L. Doi, J. W. Swart, "Proton Radiation Hardening of Silicon Oxynitride Gate nMOSFETs Formed by Nitrogen Implantation into Silicon Prior to Oxidation," *Radiation and Its Effects on Components and Systems, 2001. 6th European Conference on* , p. 229, Sep. 2001.

[49] B. J. Mrstik, H. L. Hughes, P. J. McMarr, R. K. Lawrence, D. I. Ma, I. P. Isaacson, R. A. Walker, "Hole and electron trapping in ion implanted thermal oxides and SIMOX," *Nuclear Science, IEEE Transactions on* , vol. 47, no. 6, pp. 2189-2195, Dec. 2000.

[50] Y. Nishioka, K. Ohyu, Y. Ohji, M. Kato, E. F. ,. J. da Silva, T. P. Ma, "Radiation hardened micron and submicron MOSFETs containing fluorinated oxides," *Nishioka, Y.; Ohyu, K.; Ohji, Y.; Kato, M.; da Silva, E.F., Jr.; Ma, T.P.;* , vol. 36, no. 6, p. 2116, Dec. 1989.

[51] M. Kato, K. Watanabe, T. Okabe, "Radiation effects on ion-implanted silicon-dioxide films," *Nuclear Science, IEEE Transactions on* , vol. 36, no. 6, p. 2199, Dec. 1989.

[52] M. Alles, B. Dolan, H. Hughes, P. McMarr, P. Gouker, M. Liu, "Evaluating manufacturability of radiation-hardened SOI substrates," *SOI Conference, 2001 IEEE International* , p. 131, 2001.

[53] Y. Nishioka, T. Itoga, K. Ohyu, M. Kato, T. .-P. Ma, "Radiation effects on fluorinated field oxides and associated devices," *Nuclear Science, IEEE Transactions on* , vol. 37, no. 6, p. 2026, Dec. 1990.

[54] M. R. Shaneyfelt, M. C. Maher, R. C. Camilletti, J. R. Schwank, R. L. Pease, B. A. Russell, P. E. Dodd, "Elimination of Enhanced Low-Dose-Rate Sensitivity in Linear Bipolar Devices Using Silicon-Carbide Passivation," *Nuclear Science, IEEE Transactions on* , vol. 53, no. 6, p. 2027, Aug. 2006.

[55] B. L. Draper, M. R. Shaneyfelt, R. W. Young, T. J. Headley, R. Dondero, "Arsenic ion implant energy effects on CMOS gate oxide hardness," *Nuclear Science, IEEE Transactions on* , vol. 52, no. 6, p. 2387, Dec. 2005.

[56] R. C. Baumann, T. Hossain, S. Murata, H. Kitagawa, "Boron compounds as a dominant source of alpha particles in semiconductor devices," *Reliability Physics Symposium, 1995. 33rd Annual Proceedings., IEEE International*, pp. 297-302, 1995.

[57] T. N. Bhar, R. J. Lambert, H. L. Hughes, "Electron trapping in Si implanted SlMOX," *Electronics Letters*, vol. 10, pp. 1026-1027, May 1998.

[58] B. J. Mrstik, H. L. Hughes, P. Gouker, R. K. Lawrence, P. J. McMarr, "The role of nanoclusters in reducing hole trapping in ion implanted oxides," *Nuclear Science, IEEE Transactions on* , vol. 50, no. 6, p. 1947, Dec. 2003.

[59] M. R. Shaneyfelt, D. M. Fleetwood, P. S. Winokur, J. R. Schwank, T. L. Meisenheimer, "Effects of device scaling and geometry on MOS radiation hardness assurance ," *Nuclear Science, IEEE Transactions on* , vol. 40, no. 6, pp. 1678-1685, 1993.

[60] E. L. Petersen, P. Shapiro, J. H. Adams, E. A. Burke, "Calculation of Comic-Ray Induced Upset and Scaling in VLSI Devices," *IEEE Trans. Nucl. Sci.*, 1982.

[61] A. H. Johnston, "Scaling and Technology Issues for Soft Error Rates," *4th Annual Research Conference on Reliability, Stanford University*, pp. 4-5, Oct. 2000.

[62] A. R. Duncan, V. Srinivasan, A. Sternberg, L. W. Massengill, B. Bhuva, W. H. Robinson, "The Effect of Frequency and Technology Scaling on Single Event Vulnerability of the Combinational Logic Unit in the LEON2 SPARC V8 Processor," *Workshop on Hardened Electronics and Radiation Technology (HEART'05)*, Mar. 2005.

[63] J. W. Schrankler, R. K. Reich, M. S. Holt, D. H. Ju, J. S. T. Huang, G. D. Kirchner, H. L. Hughes, "CMOS Scaling Implications for Total Dose Radiation ," *Nuclear Science, IEEE Transactions on* , vol. 32, no. 6, pp. 3988-3990, 1985.

[64] M. R. Shaneyfelt, P. E. Dodd, B. L. Draper, R. S. Flores, "Challenges in hardening technologies using shallow-trench isolation," *Nuclear Science, IEEE Transactions on*, vol. 45, no. 6, p. 2584, Dec. 1998.

[65] N. S. Saks, M. G. Ancona, J. A. Modolo, "Radiation Effects in MOS Capacitors with Very Thin Oxides at 80Â°K," *Nuclear Science, IEEE Transactions on*, vol. 31, no. 6, p. 1249, 1984.

[66] N. S. Saks, M. G. Ancona, J. A. Modolo, "Generation of Interface States by Ionizing Radiation in Very Thin MOS Oxides," *Nuclear Science, IEEE Transactions on*, vol. 33, no. 6, p. 1185, Dec. 1986.

[67] F. Faccio, "Radiation issues in the new generation of high energy physics experiments," *International journal of high speed electronics and systems*, vol. 14, no. 2, pp. 379-399, 2004.

[68] T. R. Oldham, A. J. Lelis, H. E. Boesch, J. M. Benedetto, F. B. McLean, J. M. McGarrity, "Post-Irradiation Effects in Field-Oxide Isolation Structures," *Nuclear Science, IEEE Transactions on*, vol. 34, no. 6, p. 1184, Dec. 1987.

[69] D. R. Alexander, "Design issues for radiation tolerant microcircuits for space," *Short Course of the Nuclear and Space Radiation Effects Conference (NSREC)*, Jul. 1996.

[70] R. N. Nowlin, S. R. McEndree, A. L. Wilson, D. R. Alexander, "A new total-dose-induced parasitic effect in enclosed-geometry transistors," *Nuclear Science, IEEE Transactions on* , vol. 52, no. 6, p. 2495, Dec. 2005.

[71] G. Anelli et al., "Total dose behaviour of submicron and deep submicron CMOS technologies," *Workshop on Electronics for LHC Experiments*, p. 139, 1997.

[72] F. Faccio et al., "Total dose and single event effects in a 0.25µm CMOS," *Workshop on Electronics for LHC Experiments*, pp. 105-113, Sep. 1998.

[73] N. Nowlin, J. Bailey, B. Turfler, D. Alexander, "A total-dose hardening-by-design approach for high-speed mixed-signal CMOS integrated circuits," *International journal of high speed electronics and systems*, vol. 14, no. 2, pp. 367-378, 2004.

[74] G. Anelli, M. Campbell, M. Delmastro, F. Faccio, S. Floria, A. Giraldo, E. Heijne, P. Jarron, K. Kloukinas, A. Marchioro, P. Moreira, W. Snoeys, "Radiation tolerant VLSI circuits in standard deep submicron CMOS technologies for the LHC experiments: practical design aspects," *Nuclear Science, IEEE Transactions on* , vol. 46, no. 6, pp. 1690-1696, Dec. 1999.

[75] F. Faccio, "Design Hardening Methodologies for ASICs," in *Radiation Effects on Embedded Systems*, Springer, Ed. 2007.

[76] S. Redant, R. Marec, L. Baguena, E. Liegeon, J. Soucarre, B. Van Thielen, G. Beeckman, P. Ribeiro, A. Fernandez-Leon, B. Glass, "The design against radiation effects (DARE) library," *RADECS2004 Workshop*, Sep. 2004.

[77] K. Kloukinas, F. Faccio, A. Marchioro, P. Moreira, "Development of a radiation tolerant 2.0-V standard cell library using a commercial deep submicron CMOS technology for the LHC," *4th Workshop on Electronics for LHC Experiments*, pp. 574-580, Sep. 1998.

[78] L. R. Rockett D. J. Kouba, "Radiation Hardened 150nm Standard Cell ASIC Design Library for Space Applications," *Aerospace Conference, 2008 IEEE* , Mar. 2008.

[79] F. C. Mixcoatl A. T. Jacome, "Latchup prevention by using guard ring structures in a 0.8 µm bulk CMOS process," *Superficies y Vacio*, pp. 17-22, Dec. 2004.

[80] J. W. Gambles, K. J. Hass, S. R. Whitaker, "Radiation hardness of ultra low power CMOS VLSI," *11th NASA Symposium on VLSI Design*, May 2003.

[81] E. Salman E. G. Friedman, "Methodology for placing localized guard rings to reduce substrate noise in mixed-signal circuits ," *Research in Microelectronics and Electronics, 2008. PRIME 2008. Ph.D.* , pp. 85-88, 2008.

[82] G. F. E. Gene, N. C. Lee, T. K. Tong, D. Sim, "Impact on Latchup Immunity due to the Switch From Epitaxial to Bulk Substrate," *Semiconductor Manufacturing, 2006. ISSM 2006. IEEE International Symposium on* , pp. 156-159, 2006.

[83] S. Redant, B. Van Thielen, S. Dupont, L. Baguena, E. Liegeon, R. Marec, A. Fernandez-Leon, B. Glass, "HIT-based flip-flops in the DARE library," *SEE symposium*, 2004.

[84] S. Redant, R. Marec, L. Baguena, E. Liegeon, J. Soucarre, B. Van Thielen, G. Beeckman, P.

Ribeiro, A. Fernandez-Leon, B. Glass, "Radiation test results on first silicon in the design against radiation effects (DARE) library," *Nuclear Science, IEEE Transactions on* , vol. 52, no. 2, pp. 1550-1554, Dec. 2005.

[85] T. Hoang, J. Ross, S. Doyle, D. Rea, E. Chan, W. Neiderer, A. Bumgarner, "A Radiation Hardened 16-Mb SRAM for Space Applications," *Aerospace Conference, 2007 IEEE* , Mar. 2007.

[86] R. Ginosar. (2008, Sep.) MAPLD - Converting PLD-based SoC into RadSafe ASIC. [Online]. https://nepp.nasa.gov/mapld_2008/presentations/i/05%20-%20Ginosar_Ran_mapld08_pres_1.pdf

[87] R. Ginosar. (2010, Sep.) AMICSA'10 - Development process of RHBD cell libraries for advanced SOCs. [Online]. http://microelectronics.esa.int/amicsa/2010/6am/Development%20process%20of%20RHBD%20cell%20libraries%20for%20advanced%20SOCs%20rev1.ppt

[88] Aeroflex Gaisler. [Online]. http://www.gaisler.com/cms/index.php?option=com_content&task=view&id=194&Itemid=139

[89] Aeroflex. (2009, Nov.) Datasheet : UT0.6µCRH Commercial RadHard Gate Array Family. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/ut06crhsrh.pdf

[90] Aeroflex. (2009, Nov.) Advanced Data Sheet: UT0.25µHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/ut025asic.pdf

[91] Aeroflex. (2010, Aug.) Advanced Data Sheet: UT130nHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/UT130nmHBD.pdf

[92] Aeroflex. (2010, Jul.) Advanced Data Sheet: UT90nHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/UT90nHBDdatasheet.pdf

[93] ATK, "Application Note for the 0.35µ Radiation Hardened Standard Cell Library," Jan. 2004.

[94] L. Dugoujon. (2010, Mar.) ST Microelectronics: DSM ASIC Technology & HSSL (KIPSAT). [Online]. http://microelectronics.esa.int/mpd2010/day2/DSM65nm.pdf

[95] S. Buchner D. McMorrow, "Single-Event Transients in Bipolar Linear Integrated Circuits," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3079-3102, Dec. 2006.

[96] B. D. Olson, O. A. Amusan, S. Dasgupta, L. W. Massengill, A. F. Witulski, B. L. Bhuva, M. L. Alles, K. M. Warren, D. R. Ball, "Analysis of Parasitic PNP Bipolar Transistor Mitigation Using Well Contacts in 130 nm and 90 nm CMOS Technology," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 4, pp. 894-897, 2007.

[97] O. A. Amusan, M. C. Casey, B. L. Bhuva, D. McMorrow, M. J. Gadlage, J. S. Melinger, L. W. Massengill, "Laser Verification of Charge Sharing in a 90 nm Bulk CMOS Process," *Nuclear Science, IEEE Transactions on*, vol. 56, no. 6, pp. 3065-3070, Dec. 2009.

[98] O. A. Amusan, L. W. Massengill, M. P. Baze, B. L. Bhuva, A. F. Witulski, J. D. Black, A. Balasubramanian, M. C. Casey, D. A. Black, J. R. Ahlbin, R. A. Reed, M. W. McCurdy, "Mitigation Techniques for Single-Event-Induced Charge Sharing in a 90-nm Bulk CMOS Process," *Device and Materials Reliability, IEEE Transactions on* , vol. 9, no. 2, pp. 311-317, Jun. 2009.

[99] A. K. Sutton, M. Bellini, J. D. Cressler, J. A. Pellish, R. A. Reed, P. W. Marshall, G. Niu, G. Vizkelethy, M. Turowski, A. Raman, "An Evaluation of Transistor-Layout RHBD Techniques for SEE Mitigation in SiGe HBTs," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2044-2052, Dec. 2007.

[100] R. R. Troutman, *Latchup in CMOS technology: the problem and its cure*, Springer, Ed. 1986.

[101] A. Hastings, *The Art of Analog Layout*, 2nd ed., Prentice-Hall, Ed. New York, 2005.

[102] B. Mossawir, I. R. Linscott, U. S. Inan, J. L. Roeder, J. V. Osborn, S. C. Witczak, E. E. King, S. D. LaLumondiere, "A TID and SEE Radiation-Hardened, Wideband, Low-Noise Amplifier," *Nuclear Science, IEEE Transactions on* , vol. 53, no. 6, p. 3439, Dec. 2006.

[103] M. Varadharajaperumal, G. Niu, X. Wei, T. Zhang, J. D. Cressler, R. A. Reed, P. W. Marshall, "3-D Simulation of SEU Hardening of SiGe HBTs Using Shared Dummy Collector," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2330-2337, 2007.

[104] O. A. Amusan, L. W. Massengill, B. L. Bhuva, S. DasGupta, A. F. Witulski, J. R. Ahlbin, "Design Techniques to Reduce SET Pulse Widths in Deep-Submicron Combinational Logic," *Nuclear Science, IEEE Transactions on* , vol. 54, no. 6, p. 2060, Dec. 2007.

[105] B. Narasimham, R. L. Shuler, J. D. Black, B. L. Bhuva, R. D. Schrimpf, A. F. Witulski, W. T. Holman, L. W. Massengill, "Quantifying the Reduction in Collected Charge and Soft Errors in the Presence of Guard Rings," *Device and Materials Reliability, IEEE Transactions on*, vol. 8, no. 1, pp. 203-209, Mar. 2008.

[106] B. Narasimham, B. L. Bhuva, R. D. Schrimpf, L. W. Massengill, M. J. Gadlage, O. A. Amusan, W. T. Holman, A. F. Witulski, W. H. Robinson, J. D. Black, J. M. Benedetto, P. H. Eaton, "Characterization of Digital Single Event Transient Pulse-Widths in 130-nm and 90-nm CMOS Technologies," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2506-2511, Dec. 2007.

[107] M. J. Gadlage, J. R. Ahlbin, B. Narasimham, B. L. Bhuva, L. W. Massengill, R. A. Reed, R. D. Schrimpf, G. Vizkelethy, "Scaling Trends in SET Pulse Widths in Sub-100 nm Bulk CMOS Processes," *Nuclear Science, IEEE Transactions on*, vol. 57, no. 6, pp. 3336-3341, Dec. 2010.

[108] Q. Zhou K. Mohanram, "Transistor Sizing for Radiation Hardening," *Proc. of 42nd IEEE IPRS*, 2004.

[109] J. D. Black, A. L. Sternberg, M. L. Alles, A. F. Witulski, B. L. Bhuva, L. W. Massengill, J. M. Benedetto, M. P. Baze, J. L. Wert, M. G. Hubert, "HBD layout isolation techniques for multiple node charge collection mitigation," *Nuclear Science, IEEE Transactions on* , vol. 52, no. 6, pp. 2536-2541, Dec. 2005.

[110] T. D. Loveless, M. L. Alles, D. R. Ball, K. M. Warren, L. W. Massengill, "Parametric Variability Affecting 45 nm SOI SRAM Single Event Upset Cross-Sections," *IEEE TNS, to be published*, Dec. 2010.

[111] O. A. Amusan, A. F. Witulski, L. W. Massengill, B. L. Bhuva, P. R. Fleming, M. L. Alles, A. L. Sternberg, J. D. Black, R. D. Schrimpf, "Charge Collection and Charge Sharing in a 130 nm CMOS Technology," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3253-3258, Dec. 2006.

[112] O. A. Amusan, L. W. Massengill, M. P. Baze, B. L. Bhuva, A. F. Witulski, S. DasGupta, A. L. Sternberg, P. R. Fleming, C. C. Heath, M. L. Alles, "Directional Sensitivity of Single Event Upsets in 90 nm CMOS Due to Charge Sharing," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2584-2589, Dec. 2007.

[113] M. P. Baze, B. Hughlock, J. Wert, J. Tostenrude, L. Massengill, O. Amusan, R. Lacoe, K. Lilja, M. Johnson, "Angular Dependence of Single Event Sensitivity in Hardened Flip/Flop Designs," *Nuclear Science, IEEE Transactions on*, vol. 55, no. 6, pp. 3295-3301, Dec. 2008.

[114] T. Calin, M. Nicolaidis, R. Velazco, "Upset hardened memory design for submicron CMOS technology," *Nuclear Science, IEEE Transactions on*, vol. 43, no. 6, pp. 2874-2878, Dec. 1996.

[115] Y. Boulghassoul, L. W. Massengill, A. L. Sternberg, B. L. Bhuva, W. T. Holman, "Towards SET Mitigation in RF Digital PLLs: From Error Characterization to Radiation Hardening Considerations," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 4, pp. 2047-2053, Aug. 2006.

[116] T. D. Loveless, L. W. Massengill, W. T. Holman, B. L. Bhuva, "Modeling and Mitigating Single-Event Transients in Voltage-Controlled Oscillators," *Nuclear Science, IEEE Transactions on*, vol.

54, no. 6, pp. 2561-2567, Dec. 2007.

[117] J. L. Andrews, J. E. Schroeder, B. L. Gingerich, W. A. Kolasinski, R. Koga, S. E. Diehl, "Single Event Error Immune CMOS RAM," *Nuclear Science, IEEE Transactions on*, vol. 29, no. 6, pp. 2040-2043, Dec. 1982.

[118] S. E. Diehl, A. Ochoa, P. V. Dressendorfer, R. Koga, W. A. Kolasinski, "Error Analysis and Prevention of Cosmic Ion-Induced Soft Errors in Static CMOS RAMs," *Nuclear Science, IEEE Transactions on*, vol. 29, no. 6, pp. 2032-2039, Dec. 1982.

[119] A. L. Sternberg, L. W. Massengill, M. Hale, B. Blalock, "Single-Event Sensitivity and Hardening of a Pipelined Analog-to-Digital Converter," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3532-3538, Dec. 2006.

[120] T. Wang, K. Wang, L. Chen, A. Dinh, B. Bhuva, R. Shuler, "A RHBD LC-Tank Oscillator Design Tolerant to Single-Event Transients," *Nuclear Science, IEEE Transactions on*, vol. 57, no. 6, pp. 3620-3625, Dec. 2010.

[121] T. D. Loveless, L. W. Massengill, B. L. Bhuva, W. T. Holman, A. F. Witulski, Y. Boulghassoul, "A Hardened-by-Design Technique for RF Digital Phase-Locked Loops," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3432-3438, Dec. 2006.

[122] T. D. Loveless, L. W. Massengill, B. L. Bhuva, W. T. Holman, R. A. Reed, D. McMorrow, J. S. Melinger, P. Jenkins, "A Single-Event-Hardened Phase-Locked Loop Fabricated in 130 nm CMOS," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2012-2020, Dec. 2007.

[123] Y. Boulghassoul, P. C. Adell, J. D. Rowe, L. W. Massengill, R. D. Schrimpf, A. L. Sternberg, "System-level design hardening based on worst-case ASET Simulations," *Nuclear Science, IEEE Transactions on* , vol. 51, no. 5, pp. 2787-2793, Oct. 2004.

[124] S. E. Armstrong, B. D. Olson, J. Popp, J. Braatz, T. D. Loveless, W. T. Holman, D. McMorrow, L. W. Massengill, "Single-Event Transient Error Characterization of a Radiation-Hardened by Design 90 nm SerDes Transmitter Driver," *Nuclear Science, IEEE Transactions on* , vol. 56, no. 6, pp. 3463-3468, Dec. 2009.

[125] A. Zanchi, S. Buchner, C. Hafer, S. Hisano, D. B. Kerwin, "Investigation and Mitigation of Analog SET on a Bandgap Reference in Triple-Well CMOS Using Pulsed Laser Techniques," *Nuclear Science, IEEE Transactions on*, pp. 1-7, 2011.

[126] T. Uemura, R. Tanabe, Y. Tosaka, S. Satoh, "Using Low Pass Filters in Mitigation Techniques against Single-Event Transients in 45nm Technology LSIs," *On-Line Testing Symposium, 2008. IOLTS '08. 14th IEEE International*, pp. 117-122, Jul. 2008.

[127] A. L. Sternberg, L. W. Massengill, R. D. Schrimpf, Y. Boulghassoul, H. J. Barnaby, S. Buchner, R. L. Pease, J. W. Howard, "Effect of amplifier parameters on single-event transients in an inverting operational amplifier," *Nuclear Science, IEEE Transactions on* , vol. 49, no. 3, pp. 1496-1501, Jun. 2002.

[128] H. H. Chung, W. Chen, B. Bakkaloglu, H. J. Barnaby, B. Vermeire, S. Kiaei, "Analysis of Single Events Effects on Monolithic PLL Frequency Synthesizers," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3539-3543, Dec. 2006.

[129] T. D. Loveless, L. W. Massengill, W. T. Holman, B. L. Bhuva, D. McMorrow, J. Warner, "A Generalized Linear Model for Single Event Transient Propagation in Phase-Locked Loops," *IEEE TNS, to be published*, Oct. 2010.

[130] M. J. Gadlage, P. H. Eaton, J. M. Benedetto, M. Carts, V. Zhu, T. L. Turflinger, "Digital Device Error Rate Trends in Advanced CMOS Technologies," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3466-3471, Dec. 2006.

[131] Y. Boulghassoul, L. W. Massengill, A. L. Sternberg, B. L. Bhuva, "Effects of technology scaling on the SET sensitivity of RF CMOS Voltage-controlled oscillators," *Nuclear Science, IEEE Transactions on* , vol. 52, no. 6, pp. 2426-2432, Dec. 2005.

[132] J. S. Kauppila, L. W. Massengill, W. T. Holman, A. V. Kauppila, S. Sanathanamurthy, "Single event Simulation methodology for analog/mixed signal design hardening," *Nuclear Science, IEEE Transactions on*, vol. 51, no. 6, pp. 3603-3608, Dec. 2004.

[133] S. E. Armstrong, T. D. Loveless, J. R. Hicks, W. T. Holman, D. McMorrow, L. W. Massengill, "Phase-Dependent Single-Event Sensitivity Analysis of High-Speed A/MS Circuits Extracted from Asynchronous Measurements," *Nuclear Science, IEEE Transactions on* , vol. 58, no. 3, pp. 1066-1071, Jun. 2011.

[134] E. Mikkola, B. Vermeire, H. J. Barnaby, H. G. Parks, K. Borhani, "SET Tolerant CMOS Comparator," *Nuclear Science, IEEE Transactions on* , vol. 51, no. 6, pp. 3609-3614, Dec. 2004.

[135] J. Popp, "Developing Radiation Hardened Complex System on Chip ASICs in Commercial Ultra Deep Submicron CMOS Processes," in *NSREC'2010 Short Course*, Denver, CO, USA, 2010.

[136] W. Chen, V. Pouget, G. K. Gentry, H. J. Barnaby, B. Vermeire, B. Bakkaloglu, K. Kiaei, K. E. Holbert, P. Fouillat, "Radiation Hardened by Design RF Circuits Implemented in 0.13 µm CMOS Technology," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, pp. 3449-3454, Dec. 2006.

[137] W. Chen, V. Pouget, H. J. Barnaby, J. D. Cressler, G. Niu, P. Fouillat, Y. Deval, D. Lewis, "Investigation of single-event transients in voltage-controlled oscillators," *Nuclear Science, IEEE Transactions on*, pp. 2081-2087, Dec. 2003.

[138] H. Lapuyade, V. Pouget, J. B. Beguevet, P. Hellmuth, T. Taris, O. Mazouffre, P. Fouillat, Y. Deval, "A Radiation-Hardened Injection Locked Oscillator Devoted to Radio-Frequency Applications," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 4, pp. 2040-2046, Aug. 2006.

[139] H. Lapuyade, O. Mazouffre, B. Goumballa, M. Pignol, F. Malou, C. Neveu, V. Pouget, Y. Deval, J. B. Begueret, "A Heavy-Ion Tolerant Clock and Data Recovery Circuit for Satellite Embedded High-Speed Data Links," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2080-2085, Dec. 2007.

[140] J. R. Ahlbin, L. W. Massengill, B. L. Bhuva, B. Narasimham, M. J. Gadlage, P. H. Eaton, "Single-Event Transient Pulse Quenching in Advanced CMOS Logic Circuits," *Nuclear Science, IEEE Transactions on* , vol. 56, no. 6, pp. 3050-3056, Dec. 2009.

[141] A. T. Kelly, P. R. Fleming, W. T. Holman, A. F. Witulski, B. L. Bhuva, L. W. Massengill, "Differential Analog Layout for Improved ASET Tolerance," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2053-2059, Dec. 2007.

[142] S. E. Armstrong, B. D. Olson, W. T. Holman, M. L., "Demonstration of a Differential Layout Solution for Improved ASET Tolerance in CMOS A/MS Circuits," *IEEE NSREC'2010*, Jul. 2010.

[143] P. R. Fleming, B. D. Olson, W. T. Holman, B. L. Bhuva, L. W. Massengill, "Design Technique for Mitigation of Soft Errors in Differential Switched-Capacitor Circuits," *Circuits and Systems II: Express Briefs, IEEE Transactions on* , vol. 55, no. 9, pp. 838-842, Sep. 2008.

[144] B. D. Olson, W. T. Holman, L. W. Massengill, B. L. Bhuva, P. R. Fleming, "Single-Event Effect Mitigation in Switched-Capacitor Comparator Designs," *Nuclear Science, IEEE Transactions on* , vol. 55, no. 6, pp. 3440-3446, Dec. 2008.

[145] M. Nicolaidis, "Design for soft error mitigation," *Device and Materials Reliability, IEEE Transactions on* , vol. 5, no. 3, pp. 405-418, Sep. 2005.

[146] D. Rossi, M. Omana, F. Toma, C. Metra, "Multiple transient faults in logic: an issue for next generation ICs? ," *Defect and Fault Tolerance in VLSI Systems, 2005. DFT 2005. 20th IEEE International Symposium on* , pp. 352-360, 2005.

[147] C. A. L. Lisboa, E. Schuler, L. Carro, "Going Beyond TMR for Protection Against Multiple Faults ," *Integrated Circuits and Systems Design, 18th Symposium on* , p. 80, Sep. 2005.

[148] E. Schüler L. Carro, "Reliable Circuits Design Using Analog Components," *Proceedings of the 11th Annual IEEE International Mixed-Signals Testing Workshop – IMSTW 2005*, vol. 1, pp. 166-170, Jun. 2005.

[149] I. Gonzalez L. Berrojo, "Supporting Fault Tolerance in an industrial environment: the AMATISTA approach," *On-Line Testing Workshop, 2001. Proceedings. Seventh International*, pp. 178-183, Jul. 2001.

[150] C. Lopez-Ongil, L. Entrena, M. Garcia-Valderas, M. Portela-Garcia, "Automatic Tools for Design Hardening," in *Radiation Effects on Embedded Systems*, Springer, Ed. 2007.

[151] D. G. Mavis P. H. Eaton, "Soft error rate mitigation techniques for modern microcircuits," *Reliability Physics Symposium Proceedings, 2002. 40th Annual* , p. 216, 2002.

[152] N. W. Van Onno B. R. Doyle, "Design considerations and verification testing of an SEE-hardened quad comparator," *Nuclear Science, IEEE Transactions on*, vol. 48, no. 6, pp. 1859-1864, Dec. 2001.

[153] T. D. Loveless, L. W. Massengill, B. L. Bhuva, W. T. Holman, M. C. Casey, R. A. Reed, S. A. Nation, D. McMorrow, J. S. Melinger, "A Probabilistic Analysis Technique Applied to a Radiation-Hardened-by-Design Voltage-Controlled Oscillator for Mixed-Signal Phase-Locked Loops," *Nuclear Science, IEEE Transactions on* , vol. 55, no. 6, pp. 3447-3455, Dec. 2008.

[154] B. D. Olson, W. T. Holman, L. W. Massengill, B. L. Bhuva, "Evaluation of Radiation-Hardened Design Techniques Using Frequency Domain Analysis," *Nuclear Science, IEEE Transactions on* , vol. 55, no. 6, pp. 2957-2961, Dec. 2008.

[155] Actel, *Application note C128: Design Techniques for radiation-hardened FPGAs*.

[156] M. Berg, J. J. Wang, R. Ladbury, S. Buchner, H. Kim, J. Howard, K. LaBel, A. Phan, T. Irwin, M. Friendlich, "An Analysis of Single Event Upset Dependencies on High Frequency and Architectural Implementations within Actel RTAX-S Family Field Programmable Gate Arrays," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 6, p. 3569, Dec. 2006.

[157] A. Manuzzato, "Single Event Effects on FPGAs, Phd," 2009.

[158] Xilinx, *Application note 197: Triple Module Redundancy Design Techniques for Virtex FPGAs*. 2001.

[159] C. Pilotto, J. R. Azambuja, F. L. Kastensmidt, "Synchronizing triple modular redundant designs in dynamic partial reconfiguration applications," *Proceedings of the 21st annual symposium on Integrated circuits and system design (SBCCI '08)*, 2008.

[160] F. L. Kastensmidt, L. Sterpone, L. Carro, M. S. Reorda, "On the optimal design of triple modular redundancy logic for SRAM-based FPGAs," *Design, Automation and Test in Europe, 2005. Proceedings*, p. 1290, Mar. 2005.

[161] N. Battezzati, L. Sterpone, M. Violante, F. Decuzzi, "A new software tool for static analysis of SET sensitiveness in Flash-based FPGAs," *VLSI System on Chip Conference (VLSI-SoC), 2010 18th IEEE/IFIP*, p. 79, Nov. 2010.

[162] P. Bernardi, M. S. Reorda, L. Sterpone, M. Violante, "On the evaluation of SEU sensitiveness in SRAM-based FPGAs," *On-Line Testing Symposium, 2004. IOLTS 2004. Proceedings. 10th IEEE International*, pp. 115-120, Jul. 2004.

[163] L. Sterpone, *Electronics System Design Techniques for Safety Critical Applications*, Springer, Ed. 2008.

[164] L. Sterpone M. Violante, "A new reliability-oriented place and route algorithm for SRAM-based FPGAs," *Computers, IEEE Transactions on* , vol. 55, no. 6, p. 732, Jun. 2006.

[165] P. Bernardi, L. Sterpone, M. Violante, M. Portela-Garcia, "Hybrid Fault Detection Technique: A Case Study on Virtex-II Pro's PowerPC 405," *Nuclear Science, IEEE Transactions on* , vol. 53, no. 6, p. 3550, Dec. 2006.

[166] Xilinx, *Application note 138: Virtex FPGA Series Configuration and Readback*. 2005.

[167] Xilinx, *Application note 151: Virtex Series Configuration Architecture User Guide*. 2004.

[168] C. Carmichael, M. Caffrey, A. Salazar, "Correcting Single-Event Upset through Virtex Partial

Reconfiguration," *Xilinx Application Notes, XAPP216*, 2000.

[169] S. Rezgui, G. Swift, K. Somervill, J. George, C. Carmichael, G. Allen, "Complex Upset Mitigation Applied to a Re-Configurable Embedded Processor," *Nuclear Science, IEEE Transactions on*, vol. 52, no. 6, pp. 2468-2474, 2005.

[170] Microsemi. (2009, Oct.) Axcelerator Family FPGAs v2.8. [Online]. http://www.actel.com/documents/AXGenDesc_DS.pdf

[171] Aeroflex. (2010, Mar.) Datasheet: UT6325 RadTol Eclipse FPGA. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/RadTolEclipseFPGA.pdf

[172] Aeroflex. (2006, Jun.) Aeroflex ECLIPSE Single Event Effects (SEE) High-Speed Test Results. [Online]. http://radhome.gsfc.nasa.gov/radhome/papers/T022205_Aeroflex_Eclipse.pdf

[173] Microsemi. (2009, Oct.) Datasheet: ProASIC3 Flash Family FPGAs with Optional Soft ARM Support. [Online]. http://www.actel.com/documents/PA3_DS.pdf

[174] Atmel. (2006, Jun.) Datasheet: Rad Hard Reprogrammable FPGAs with FreeRAM AT40KEL040. [Online]. http://www.atmel.com/dyn/resources/prod_documents/doc4155.pdf

[175] Atmel. (2010, Oct.) Datasheet: Rad Hard Reprogrammable FPGA ATF280F Advance Information. [Online]. http://www.atmel.com/dyn/resources/prod_documents/doc7750.pdf

[176] Xilinx. (2011, Mar.) Virtex-6 Family Overview. [Online]. http://www.xilinx.com/products/silicon-devices/fpga/virtex-6/index.htm

[177] Xilinx. (2010, Mar.) Virtex-5Q Family Overview. [Online]. http://www.xilinx.com/products/silicon-devices/fpga/virtex-5q/index.htm

[178] Xilinx. (2011, Jul.) Radiation-Hardened, Space-Grade Virtex-5QV Device Overview. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds192.pdf

[179] G. R. Allen, L. Edmonds, C. W. Tseng, G. Swift, C. Carmichael, "Single-Event Upset (SEU) Results of Embedded Error Detect and Correct Enabled Block Random Access Memory (Block RAM) Within the Xilinx XQR5VFX130 ," *Nuclear Science, IEEE Transactions on* , vol. 57, no. 6, pp. 3426-3431, Dec. 2010.

[180] Jet Propulsion Laboratory, Reports on Radiation Effects in Xilinx FPGAs. [Online]. http://parts.jpl.nasa.gov/organization/group-5144/radiation-effects-in-fpgas/xilinx/

[181] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley-Interscience, 2005.

[182] M. S. Liu, G. A. Shaw, J. Yue, "Fabrication of stabilized polysilicon resistors for SEU control," Patent United States Patent 5212108, May 18, 1993.

[183] P. Roche, F. Jacquet, C. Caillat, J. P. Schoellkopf, "An alpha immune and ultra low neutron SER high density SRAM," *Reliability Physics Symposium Proceedings, 2004. 42nd Annual. 2004 IEEE International*, p. 671, Apr. 2004.

[184] H. T. Weaver, C. L. Axness, J. D. McBrayer, J. S. Browning, J. S. Fu, A. Ochoa, R. Koga, "An SEU Tolerant Memory Cell Derived from Fundamental Studies of SEU Mechanisms in SRAM," *Nuclear Science, IEEE Transactions on* , vol. 34, no. 6, pp. 1281-1286, Dec. 1987.

[185] L. R. Rockett, "A design based on proven concepts of an SEU-immune CMOS configurable data cell for reprogrammable FPGAs," *Microelectronics Journal, Elsevier*, pp. 99-111, 2000.

[186] J. Canaris S. Whitaker, "Circuit techniques for the radiation environment of space," *Custom Integrated Circuits Conference, 1995., Proceedings of the IEEE 1995*, pp. 77-80, 1995.

[187] L. Geppert, "A Static RAM Says Goodbye to Data Errors," *IEEE Spectrum*, Feb. 2004.

[188] Y. Shiyanovskii, F. Wolff, C. Papachristou, "SRAM Cell Design Protected from SEU Upsets," *On-Line Testing Symposium, 2008. IOLTS '08. 14th IEEE International*, p. 169, Jul. 2008.

[189] P. Roche, G. Gasiot, S. Uznanski, J. .-M. Daveau, J. Torras-Flaquer, S. Clerc, R. Harboe-Sørensen, "A Commercial 65 nm CMOS Technology for Space Applications: Heavy Ion, Proton and

Gamma Test Results and Modeling," *Nuclear Science, IEEE Transactions on*, vol. 57, no. 4, pp. 2079-2088, 2010.

[190] L. R. Rockett, "An SEU-hardened CMOS data latch design," *Nuclear Science, IEEE Transactions on*, vol. 35, no. 6, pp. 1682-1687, Aug. 2002.

[191] R. Velazco, D. Bessot, S. Duzellier, R. Ecoffet, R. Koga, "Two CMOS memory cells suitable for the design of SEU-tolerant VLSI circuits," *Nuclear Science, IEEE Transactions on* , vol. 41, no. 6, pp. 2229-2234, Dec. 1994.

[192] D. Bessot R. Velazco, "Design of SEU-hardened CMOS memory cells: the HIT cell," *Radiation and its Effects on Components and Systems, 1993.,RADECS 93., Second European Conference on* , pp. 563-570, Sep. 1993.

[193] P. Armbruster, T. K. Pike, R. Harboe Sorensen, "The European Programme for the Development of a Radiation Tolerant High Performance 32-Bit Digital Signal Processor - Phase I Results," *Electronic Component Conference - EECC'97, Proceedings of the 3rd ESA Electronic Component Conference*, p. 305, Apr. 1997.

[194] T. Calin, R. Velazco, M. Nicolaidis, S. Moss, S. D. LaLumondiere, V. T. Tran, R. Koga, K. Clark, "Topology-related upset mechanisms in design hardened storage cells ," *Radiation and Its Effects on Components and Systems, 1997. RADECS 97. Fourth European Conference on* , pp. 484-488, 1997.

[195] M. D. Berg, K. A. LaBel, H. Kim, M. Friendlich, A. Phan, C. Perez, "A Comprehensive Methodology for Complex Field Programmable Gate Array Single Event Effects Test and Evaluation," *Nuclear Science, IEEE Transactions on* , vol. 56, no. 2, pp. 366-374, 2009.

[196] J. Benedetto, P. Eaton, K. Avery, D. Mavis, M. Gadlage, T. Turflinger, P. E. Dodd, G. Vizkelethyd, "Heavy ion-induced digital single-event transients in deep submicron Processes," *Nuclear Science, IEEE Transactions on*, vol. 51, no. 6, pp. 3480-3485, 2004.

[197] S. Uznanski, G. Gasiot, P. Roche, J. Autran, V. Ferlet-Cavrois, "Monte-Carlo Based Charge Sharing Investigations on a Bulk 65 nm RHBD Flip-Flop," *Nuclear Science, IEEE Transactions on*, vol. 57, no. 6, pp. 3267-3272, 2010.

[198] S. Whitaker, J. Canaris, K. Liu, "SEU hardened memory cells for a CCSDS Reed-Solomon encoder," *Nuclear Science, IEEE Transactions on*, vol. 38, no. 6, pp. 1471-1477, Dec. 1991.

[199] M. N. Liu S. Whitaker, "Low power SEU immune CMOS memory circuits," *Nuclear Science, IEEE Transactions on*, vol. 39, no. 6, pp. 1679-1684, Dec. 1992.

[200] J. W. Gambes G. K. Maki, "Rad-tolerant flight VLSI from commercial foundries," *Circuits and Systems, 1996., IEEE 39th Midwest symposium on*, vol. 3, pp. 1227-1230, 1996.

[201] A. J. Van de Goor I. Schanstra, "Address and data scrambling: causes and impact on memory tests," *Electronic Design, Test and Applications, 2002. Proceedings. The First IEEE International Workshop on*, p. 128, Jan. 2002.

[202] G. Gasiot, D. Giot, P. Roche, "Multiple Cell Upsets as the Key Contribution to the Total SER of 65 nm CMOS SRAMs and Its Dependence on Well Engineering," *Nuclear Science, IEEE Transactions on*, vol. 54, no. 6, pp. 2468-2473, 2007.

[203] D. Radaelli, H. Puchner, S. Wong, S. Daniel, "Investigation of multi-bit upsets in a 150 nm technology SRAM device," *Nuclear Science, IEEE Transactions on*, vol. 52, no. 6, pp. 2433-2437, 2005.

[204] A. Dutta N. A. Touba, "Multiple Bit Upset Tolerant Memory Using a Selective Cycle Avoidance Based SEC-DED-DAEC Code," *VLSI Test Symposium, 2007. 25th IEEE*, pp. 349-354, 2007.

[205] O. Golubeva, M. Rebaudengo, M. Sonza Reorda, M. Violante, *Software-Implemented Hardware Fault Tolerance*. Media, Springer Science+Business, 2006.

[206] N. Oh, S. Mitra, E. J. McCluskey, "ED4I: error detection by diverse data and duplicated

instructions," *Computers, IEEE Transactions on* , vol. 51, no. 2, p. 180, Feb. 2002.

[207] P. Bernardi, L. M. V. Bolzani, M. Rebaudengo, M. Sonza Reorda, F. L. Vargas, M. Violante, "A new hybrid fault detection technique for systems-on-a-chip," *Computers, IEEE Transactions on*, vol. 55, no. 2, p. 185, Feb. 2006.

[208] N. Oh, P. P. Shirvani, E. J. McCluskey, "Control-flow checking by software signatures," *Reliability, IEEE Transactions on* , vol. 51, no. 1, p. 111, Mar. 2002.

[209] N. Oh, P. P. Shirvani, E. J. McCluskey, "Error detection by duplicated instructions in super-scalar processors," *Reliability, IEEE Transactions on* , vol. 51, no. 1, pp. 63-75, Mar. 2002.

[210] M. N. Lovellette, K. S. Wood, D. L. Wood, J. H. Beall, P. P. Shirvani, N. Oh, E. J. McCluskey, "Strategies for fault-tolerant, space-based computing: Lessons learned from the ARGOS testbed," *Aerospace Conference Proceedings, 2002. IEEE* , vol. 5, pp. 2109-2119, 2002.

[211] Space Micro inc. - Space Electronics Division Products. [Online]. http://www.spacemicro.com/space_div/se_div.htm

[212] M. Pignol, "DMT and DT2: Overview of two CNES Fault-Tolerant Architectures Intended for Electronic COTS Components in Space Applications," *IEEE Proceedings on Dependable System and Networks*, pp. B34-B35, 2003.

[213] M. Pignol, "CNES Fault Tolerant Architectures Intended for Electronic COTS Components in Space Applications," *Proc. European Commercialisation of Military and Space Electronics Conf.*, pp. 39-48, 2002.

[214] M. Pignol, "DMT and DT2: two fault-tolerant architectures developed by CNES for COTS-based spacecraft supercomputers," *On-Line Testing Symposium, 2006. IOLTS 2006. 12th IEEE International* , Jul. 2006.

[215] M. Pignol, T. Parrain, V. Claverie, C. Boleat, G. Estaves, "Development of a Testbench for Validation of DMT and DT2 Fault-Tolerant Architectures on SOI PowerPC7448," *On-Line Testing Symposium, 2008. IOLTS '08. 14th IEEE International* , p. 182, Jul. 2008.

[216] M. Pignol, "COTS-based applications in space avionics," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2010*, pp. 1213-1219, 2010.

[217] T. C. Bressoud F. B. Schneider, "Hypervisor-based fault tolerance," *ACM Transactions on Computer Systems*, vol. 14, no. 1, pp. 80-107, 1996.

[218] S. Campagna, M. Hussain, M. Violante, "Hypervisor-Based Virtual Hardware for Fault Tolerance in COTS Processors Targeting Space Applications," *Defect and Fault Tolerance in VLSI Systems (DFT), 2010 IEEE 25th International Symposium on* , p. 44, Oct. 2010.

[219] M. Masmano, I. Ripoll, A. Crespo, "XtratuM: a Hypervisor for Safety Critical Embedded Systems," Instituto de Informatica Industrial, Universidad Politecnica de Valencia.

[220] J. P. Spratt, B. C. Passenheim, R. E. Leadon, S. Clark, D. J. Strobel, "Effectiveness of IC shielded packages against space radiation," *Nuclear Science, IEEE Transactions on* , vol. 44, no. 6, p. 2018, Dec. 1997.

[221] E. C. Smith, "Effects of realistic satellite shielding on SEE rates ," *Nuclear Science, IEEE Transactions on* , vol. 41, no. 6, pp. 2396-2399, 1994.

[222] M. Cherng, I. Jun, T. Jordan, "Optimum shielding in Jovian radiation environment," *Nuclear Instruments and Methods in Physics Research Section A*, vol. 580, no. 1, pp. 633-636, 2007.

[223] J. Miller, L. Taylor, C. Zeitlin, L. Heilbronn, S. Guetersloh, M. DiGiuseppe, Y. Iwata, T. Murakami, "Lunar soil as shielding against space radiation," *Radiation Measurements*, vol. 44, no. 2, pp. 163-167, Feb. 2009.

[224] S. B. Guetersloh, C. Zeitlin, L. H. Heilbronn, J. Miller, "Effectiveness of shielding materials for dose reduction," *Aerospace Conference, 2006 IEEE* , 2006.

[225] J. H. Adams, "The Natural Radiation Environment inside Spacecraft," *Nuclear Science, IEEE*

Transactions on, vol. 29, no. 6, p. 2095, Dec. 1982.

[226] I. Jun W. McAlpine, "Displacement damage in silicon due to secondary neutrons, pions, deuterons, and alphas from proton interactions with materials," *Nuclear Science, IEEE Transactions on*, vol. 48, no. 6, p. 2034, Dec. 2001.

[227] A. M. El-Attar G. Fahmy, "An improved watchdog timer to enhance imaging system reliability in the presence of soft errors," *Proceedings of the 2007 IEEE International Symposium on Signal Processing and Information Technology*, pp. 1100-1104, Dec. 2007.

[228] D. R. Czajkowski, M. P. Pagey, P. K. Samudrala, M. Goksel, M. J. Viehman, "Low Power, High-Speed Radiation Hardened Computer & Flight Experiment," *Aerospace Conference, 2005 IEEE* , Mar. 2005.

[229] G. F. Volpi, "Power Line Protection Devices in Space Applications ," *EUROCON, 2007. The International Conference on "Computer as a Tool"*, pp. 1636-1640, Sep. 2007.

[230] P. J. Layton, D. R. Czajkowski, J. C. Marshall, H. F. D. Anthony, R. W. Boss, "Single event latchup protection of integrated circuits," *Radiation and Its Effects on Components and Systems, 1997. RADECS 97. Fourth European Conference on* , p. 327, Sep. 1997.

[231] B. Johlander. (2004) ESCIES. [Online]. https://escies.org/GetFile?rsrcid=879

[232] F. Abate, L. Sterpone, C. A. Lisboa, L. Carro, M. Violante, "New Techniques for Improving the Performance of the Lockstep Architecture for SEEs Mitigation in FPGA Embedded Processors," *Nuclear Science, IEEE Transactions on*, vol. 56, no. 4, p. 1992, Aug. 2009.

[233] P. David C. Guidal, "Development of a fault tolerant computer system for the HERMES space shuttle," *Fault-Tolerant Computing, 1993. FTCS-23. Digest of Papers., The Twenty-Third International Symposium on* , p. 641, Jun. 1993.

[234] D. Powell, *A Generic Fault-Tolerant Architecture for Real-Time Dependable Systems*. Boston: Kluwer Academic Publishers, 2001.

[235] H. Saito, Y. Masumoto, T. Mizuno, A. Miura, M. Hashimoto, H. Ogawa, S. Tachikawa, T. Oshima, A. Choki, H. Fukuda, M. Hiraharaa, S. Okanob, "INDEX: Piggy-Back Satellite for Aurora Observation and Technology Demonstration," *51th IAF International Astronautical Congress*, 2000.

[236] R. Hillman, G. Swift, P. Layton, M. Conrad, C. Thibodeau, F. Irom, "Space processor radiation mitigation and validation techniques for an 1,800 MIPS processor board," *Radiation and Its Effects on Components and Systems, 2003. RADECS 2003. Proceedings of the 7th European Conference on* , p. 347, Sep. 2003.

[237] Maxwell Technologies. [Online]. http://about.maxwell.com/microelectronics/products/sbc/scs750.asp

[238] J. Baylis, *Error Correcting Codes: A Mathematical Introduction*. Boca Raton, FL: CRC Press, 1998.

[239] E. R. Berlekamp, *Algebraic Coding Theory*, Revised edition ed. Aegean Park Pr, 1984.

[240] F. J. MacWilliams N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland Mathematical Library, 1977.

[241] R. Schriebman, "Error Correcting Codes," Apr. 2006.

[242] E. R. Berlekamp, "Nonbinary BCH decoding," *Information Theory, IEEE Transactions on*, vol. 14, no. 2, pp. 242-242, Mar. 1968.

[243] S. B. Wicker V. K. E. Bhargava, *Reed-Solomon codes and their applications*, 1st ed. IEEE press, Piscataway, 1994.

[244] P. White A. Kisin, "Parallel RS Encoders and Decoders in SDRAM Memory for Space Applications," *MAPLD Conference*, 2003.

[245] G. Mitchell, "Investigation of Hamming, Reed-Solomon, and Turbo Forward Error Correcting

Codes," Army Research Laboratory ARL-TR-4901, 2009.

[246] F. Fummi, D. Sciuto, C. Silvano, "Automatic Generation of Error Control Codes for Computer Applications," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 6, no. 3, pp. 502-506, 1998.

[247] D. R. Czajkowski. (2008, Jan.) PatentStorm. [Online]. http://www.patentstorm.us/patents/7318169/description.html

[248] D. R. Czajkowski, P. K. Samudrala, M. P. Pagey, "SEU mitigation for reconfigurable FPGAs," *Aerospace Conference, 2006 IEEE*, 2006.

[249] S. Duzellier, S. Bourdarie, R. Velazco, B. Nicolescu, R. Ecoffet, "SEE in-flight data for two static 32KB memories on high earth orbit," *Radiation Effects Data Workshop, 2002 IEEE*, pp. 1-6, 2002.

[250] C. S. Dyer, A. Sims, C. Underwood, "Measurements of the SEE environment from sea level to GEO using the CREAM and CREDO experiments," *Nuclear Science, IEEE Transactions on* , vol. 43, no. 2, pp. 383-402, Apr. 1996.

[251] C. S. Dyer, P. Truscott, C. J. Peerless, C. J. Watson, H. E. Evans, P. Knight, M. Cosby, C. Underwood, T. Cousins, R. Noulty, "Updated measurements from CREAM and CREDO and implications for environment and shielding models," *Nuclear Science, IEEE Transactions on* , vol. 45, no. 3, pp. 1584-1589, Jun. 1998.

[252] B. Sherman M. Cuviello, "NASA's LWS/SET technology experiment carrier," *Aerospace Conference, 2003. Proceedings. 2003 IEEE* , vol. 1, Mar. 2003.

[253] G. Hubert, R. Velazco, P. Peronnard, "A generic platform for remote accelerated tests and high altitude SEU experiments on advanced ICs: Correlation with MUSCA SEP3 calculations," *On-Line Testing Symposium, 2009. IOLTS 2009. 15th IEEE International* , p. 180, Jun. 2009.

[254] G. Hubert, S. Duzellier, C. Inguimbert, C. Boatella-Polo, F. Bezerra, R. Ecoffet, "Operational SER Calculations on the SAC-C Orbit Using the Multi-Scales Single Event Phenomena Predictive Platform (MUSCA SEP3)," *IEE TNS.*, vol. 56, no. 6, pp. 3032-3042, 2009.

[255] A. Lesea, S. Drimer, J. J. Fabula, C. Carmichael, P. Alfke, "The rosetta experiment: Atmospheric soft error rate testing in differing technology FPGAs," *Device and Materials Reliability, IEEE Transactions on*, vol. 5, no. 3, pp. 317-328, Dec. 2005.

[256] J. C. Garth, E. A. Burke, S. Woolf, "The Role of Scattered Radiation in the Dosimetry of Small Device Structures," *Nuclear Science, IEEE Transactions on*, vol. 27, no. 6, pp. 1459-1464, Dec. 1980.

[257] JEDEC standard, *Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices*. JESD89, 2001.

[258] D. McMorrow, J. S. Melinger, S. Buchner, T. Scott, R. D. Brown, N. F. Haddad, "Application of a Pulsed Laser for Evaluation and Optimization of SEU-Hard Designs," *Nuclear Science, IEEE Transactions on*, vol. 47, no. 3, pp. 559-565, Jun. 2000.

[259] J. S. Melinger, D. McMorrow, A. B. Campbell, S. Buchner, L. H. Tran, A. R. Knudson, W. R. Curtice, "Pulsed laser-induced single event upset and charge collection measurements as a function of optical penetration depth," *Journal of Applied Physics*, vol. 84, no. 2, pp. 690-703, Jul. 1998.

[260] G. C. Messenger M. S. Ash, *Single Event Phenomena*. New York: Chapman-Hall, 1997.

[261] T. F. Miyahira, A. H. Johnston, H. N. Becker, S. D. LaLumondiere, S. C. Moss, "Catastrophic Latchup in CMOS Analog-to-Digital Converters," *Nuclear Science, IEEE Transactions on* , vol. 48, no. 6, pp. 1833-1840, Dec. 2001.

[262] S. Duzellier, D. Falguere, L. Guibert, V. Pouget, P. Fouillat, R. Ecoffet, "Application of Laser Testing In Study of SEE Mechanisms In 16-Mbit Drams," *Nuclear Science, IEEE Transactions on* ,

vol. 47, no. 6, pp. 2392-2399, Dec. 2000.

[263] A. Makihara, H. Shindou, N. Nemoto, S. Kuboyama, S. Matsuda, T. Oshima, T. Hirao, H. Itoh, S. Buchner, A. B. Campbell, "Analysis of Single-Ion Multiple-Bit Upset in High-Density DRAMs," *Nuclear Science, IEEE Transactions on*, vol. 47, no. 6, pp. 2400-2404, Dec. 2000.

[264] A. H. Johnston T. F. Miyahira, "Latchup Test Considerations for Analog-to-Digital Converters," *SEE symposium*, Apr. 2000.

[265] J. A. Clark D. K. Pradhan, "Fault Injection: A method for Validating Computer-System Dependability," *IEEE Computer*, vol. 28, no. 6, pp. 47-56, Jun. 1995.

[266] L. Anghel, M. Rebaudengo, M. S. Reorda, M. Violante, "Multi-level Fault Effects Evaluation," in *Radiation Effects on Embedded Systems*. Springer, 1997, ch. 4, pp. 69-88.

[267] D. K. Pradhan, *Fault-Tolerant Computer System Design*. Prentice Hall, 1994.

[268] "Davinci Three Dimensional Device Simulation Program Manual," *Synopsys*, 2003.

[269] "Taurus Process/Device User Manual," *Synopsys*, 2003.

[270] "Athena/Atlas User's Manual," *Silvaco int*, 1997.

[271] "DESSIS User's Manual," *ISE release 6*, vol. 4, 2000.

[272] E. Jenn, J. Arlat, M. Rimen, J. Ohlsson, J. Karlsson, "Fault injection into VHDL models: the MEFISTO tool," *Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., Twenty-Fourth International Symposium on*, pp. 66-75, Jun. 1994.

[273] T. A. Delong, B. W. Johnson, J. A. Profeta III, "A fault injection technique for VHDL behavioral-level models," *Design & Test of Computers, IEEE*, vol. 13, no. 4, pp. 24-33, 1996.

[274] D. Gil, C. Baraza, J. V. Busquets, P. J. Gil, "Fault injection into VHDL models: analysis of the error syndrome of a microcomputer system," *Euromicro Conference, 1998. Proceedings. 24th*, vol. 1, pp. 418-425, Aug. 1998.

[275] J. Boue, P. Petillon, Y. Crouzet, "MEFISTO-L: a VHDL-based fault injection tool for the experimental assessment of fault tolerance," *Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on*, pp. 168-173, Jun. 1998.

[276] B. Parrotta, M. Rebaudengo, M. S. Reorda, M. Violante, "New techniques for accelerating fault injection in VHDL descriptions," *On-Line Testing Workshop, 2000. Proceedings. 6th IEEE International*, pp. 61-66, 2000.

[277] R. Velazco, S. Rezgui, R. Ecoffet, "Predicting error rate for microprocessor-based digital architectures through C.E.U. (Code Emulating Upsets) injection," *Nuclear Science, IEEE Transactions on*, vol. 47, no. 6, pp. 2405-2411, Dec. 2000.

[278] P. Peronnard, R. Ecoffet, M. Pignol, D. Bellin, R. Velazco, "Predicting the SEU error rate through fault injection for a complex microprocessor," *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on*, pp. 2288-2292, Jul. 2008.

[279] F. Lima, C. Carmichael, J. Fabula, R. Padovani, R. Reis, "A fault injection analysis of Virtex FPGA TMR design methodology," *Radiation and Its Effects on Components and Systems, 2001. 6th European Conference on*, pp. 275-282, Sep. 2001.

[280] M. Alderighi, S. D'Angelo, M. Mancini, G. R. Sechi, "A fault injection tool for SRAM-based FPGAs," *On-Line Testing Symposium, 2003. IOLTS 2003. 9th IEEE*, pp. 129-13, Jul. 2003.

[281] R. Velazco, G. Foucard, P. Peronnard, "Combining Results of Accelerated Radiation Tests and Fault Injection to Predict the Error Rate of Applications Implemented in SRAM-Based FPGAs," *47th Nuclear and Space Radiation Effects Conference (NSREC'10)*, Jul. 2010.

[282] K. K. Goswami, "DEPEND: a simulation-based environment for system level dependability analysis," *Computers, IEEE Transactions on*, vol. 46, no. 1, pp. 60-74, Jan. 1997.

[283] P. Sundararajan B. Blodget, "Estimation of mean time between failure caused by single event upset," *Xilinx Application Notes, XAPP559*, Jan. 2005.

[284] G. Asadi M. B. Tahoori, "An analytical approach for soft error rate estimation of SRAM-based FPGAs," *Military and Aerospace Applications Programmable Logic Devices Conference*, Sep. 2004.

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

[286] C. Carmichael, "Triple module redundancy design techniques for virtex FPGAs," *Xilinx Application Notes, XAPP197*, Nov. 2001.

[287] "TMRTool User Guide," *Xilinx User Guide, UG156*.

[288] R. Kumar, V. Karkala, R. Garg, T. Jindal, S. P. Khatri, "A radiation tolerant Phase Locked Loop design for digital electronics," *Computer Design, 2009. ICCD 2009. IEEE International Conference on*, pp. 505-510, Oct. 2009.

[289] NASA - CALIPSO satellite. [Online]. http://www-calipso.larc.nasa.gov/

[290] JAXA - REIMEI (INDEX) satellite. [Online]. http://www.jaxa.jp/projects/sat/index/index_e.html

[291] CNES MYRIADE satellite. [Online]. http://smsc.cnes.fr/MYRIADE/GP_plateforme.htm

[292] ESA. (2009) SPENVIS. [Online]. http://www.spenvis.oma.be/intro.php

[293] B. Cooke, "Reed-Muller Error Correcting Codes," *MIT Undergraduate Journal of Mathematics*, pp. 21-26, 2006.

[294] J. Szmidt, "Electronic properties of nanocrystalline layers of wide-band-gap materials," *Chaos, Solitons & Fractals*, vol. 10, no. 12, pp. 2099-2152, Dec. 1999.

[295] W. Kern R. K. Smeltzer, "Borophosphosilicate glasses for integrated circuits," *Microelectonics Reliability*, vol. 26, pp. 792-792, 1996.

[296] F. T. Brady, J. D. Maimon, M. J. Hurt, "A scaleable, radiation hardened shallow trench isolation," *Nuclear Science, IEEE Transactions on*, vol. 46, no. 6, p. 1836, Dec. 1999.

[297] M. Turowski, A. Raman, R. D. Schrimpf, "Nonuniform total-dose-induced charge distribution in shallow-trench isolation oxides," *Nuclear Science, IEEE Transactions on*, vol. 51, no. 6, p. 3166, Dec. 2004.

[298] J. D. Hayden, et al., "A quadruple well, quadruple polysilicon BiCMOS process for fast 16 Mb SRAM's," *Electron Devices, IEEE Transactions on* , vol. 41, no. 12, p. 2318, Dec. 1994.

[299] Q. Zhou K. Mohanram, "Gate sizing to radiation harden combinational logic," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 155-166, 2006.

[300] P. Shivakumar, M. Kistler, S. W. Keckler, D. Burger, L. Alvisi, "Modeling the effect of technology trends on the soft error rate of combinational logic," *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, pp. 389-398, 2002.

[301] N. Cohen, T. S. Sriram, N. Leland, D. Moyer, S. Butler, R. Flatley, "Soft error considerations for deep-submicron CMOS circuit applications ," *Electron Devices Meeting, 1999. IEDM Technical Digest. International* , pp. 315-318, 1999.

[302] Atmel. (2007, Nov.) Datasheet: MH1RT - Rad Hard 1.6M Used Gates 0.35 µm CMOS Sea of Gates/Embedded Array. [Online]. http://www.atmel.com/dyn/resources/prod_documents/doc4110.pdf

[303] Atmel. (2011, Feb.) Datasheet: ATC18RHA - Rad Hard 0.18 µm CMOS Cell-based ASIC for Space Use. [Online]. http://www.atmel.com/dyn/resources/prod_documents/doc4261.pdf

[304] Microsemi. (2007, Aug.) Actel RTAX-S/SL RadTolerant FPGAs. [Online]. http://www.tdelektronics.com/public/media/content_documents/actel/rtaxs_pb.pdf

[305] G. M. Swift, G. R. Allen, C. W. Tseng, C. Carmichael, G. Miller, J. S. George, "Static Upset Characteristics of the 90nm Virtex-4QV FPGAs," *Radiation Effects Data Workshop, 2008 IEEE* ,

pp. 98-105, Jul. 2008.

[306] R. Azambuja, A. Lapolli, L. Rosa, F. L. Kastensmidt, "Detecting SEEs in Microprocessors Through a Non-Intrusive Hybrid Technique," *Nuclear Science, IEEE Transactions on*, vol. 58, no. 3, pp. 993-1000, 2011.

[307] M. Pignol, "Radiation Effects on Digital Systems," in *Space Radiation Environment and its Effects on Spacecraft Components and Systems (SREC'04), Space Technology Course of CNES / ONERA / RADECS Association*, G. Joseph, Ed. Toulouse, France: Cépaduès, 2004, ch. III-03, pp. 411-459.

[308] R. DeCoursey, R. Melton, R. Estes, "Non Radiation hardened Microprocessors in Space-Based Remote Sensing Systems," *Proc. SPIE Sensors, Systems and Next-Generation Satellites X*, vol. 6361, 2006.

[309] B. Narasimham, J. W. Gambles, R. L. Shuler, B. L. Bhuva, L. W. Massengill, "Quantifying the Effect of Guard Rings and Guard Drains in Mitigating Charge Collection and Charge Spread," *Nuclear Science, IEEE Transactions on*, vol. 55, no. 6, pp. 3456-3460, Dec. 2008.