ECSS-E-HB-20-40A
11 October 2023

EUROPEAN COOPERATION

ECSS

FOR SPACE STANDARDIZATION

Space engineering

Engineering techniques for radiation effects mitigation in ASICs and FPGAs handbook

ECSS Secretariat
ESA-ESTEC
Requirements & Standards 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 descriptions and recommendations how to organize and perform the work of choosing and applying techniques in order to mitigate the harmful effects of radiation on Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs).

This handbook has been prepared by the ECSS-Q-HB-60-02A Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority. It was published in 2016 as ECSS-Q-HB-60-02A. On 11 October 2023 the newly published ECSS-E-ST-20-40C and its associated ECSS-Q-ST-60-03C superseded former ECSS-Q-ST-60-02C (31 July 2008) and, on that same date, this handbook was renumbered and its title modified in order to link it to ECSS-E-ST-20-40C.

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 Section
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-Q-HB-60-02A 1 September 2016	First issue
ECSS-E-HB-20-40A 11 October 2023	Second issue Coinciding with the publication of ECSS-E-ST-20-40C and ECSS-Q-ST-60-03C (1 October 2023) the former handbook numbered ECSS-Q-HB-60-02A has been renumbered and its title changed to reposition it as an engineering handbook linked to ECSS-E-ST-20-40C.

Table of contents

Figures

Tables

1 Scope

This handbook provides a compilation of different techniques that can be used to mitigate the adverse effects of radiation in integrated circuits (ICs), with almost exclusive attention to Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) to be used in space, and excluding other ICs like power devices, MMIC or sensors.

The target users of this handbook are developers and users of ICs which are meant to be used in a radiation environment. Following a bottom-up order, the techniques are presented according to the different stages of an IC development flow where they can be applied. Therefore, users of this handbook can be IC engineers involved in the selection, use or development of IC manufacturing processes, IC layouts and ASIC standard cell libraries, analogue and digital circuit designs, FPGAs, embedded memories, embedded software and the immediate electronic system (printed circuit board) containing the IC that can experience the radiation effects.

In addition, this handbook contains an overview of the space radiation environment and its effects in semiconductor devices, a section on how to validate the good implementation and effectiveness of the mitigation techniques, and a special section providing some general guidelines to help with the selection of the most adequate mitigation techniques including some examples of typical space project scenarios.

The information given in this ECSS Handbook is provided only as guidelines and for reference, and not to be used as requirements. ECSS Standards provide requirements that can be made applicable, while, ECSS Handbooks provide guidelines.

2 References

ECSS-S-ST-00-01	ECSS system - Glossary of terms
ECSS-E-ST-10-04	Space engineering - Space environment
ECSS-E-ST-10-12	Space engineering - Methods for the calculation of radiation received and its effects, and a policy for design margins
ECSS-E-HB-10-12	Space engineering - Calculation of radiation and its effects and margin policy handbook
ECSS-E-ST-20-40	Space engineering – ASIC, FPGA and IP Core engineering
ECSS-Q-ST-60	Space product assurance - Electrical, electronic and electromechanical (EEE) components
ECSS-Q-ST-60-03	Space product assurance – ASIC, FPGA and IP Core product assurance
ECSS-Q-ST-60-15	Space product assurance - Radiation hardness assurance - EEE components
ESCC 22900	ESCC Basic Specification: Total dose steady-state irradiation test method
ESCC 25100	ESCC Basic Specification: Single event effects test method and guidelines
JEDEC JESD57	Test Procedures for the Management of Single-Event Effects in Semiconductor Devices from Heavy Ion Irradiation
JEDEC JESD89A	Measuring and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices
MIL-STD-883/ 1019	Test Method Standard Microcircuits / Ionizing radiation (total dose) test procedure

3 Terms, definitions and abbreviated terms

3.1 Terms from other documents

a. For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01 apply.

b. For the purpose of this document, the terms and definitions from ECSS-E-ST-20-40 apply, in particular for the following terms:

1. **application specific integrated circuit (ASIC)**
2. **cell**
3. **cell library**
4. **HDL model**
5. **intellectual property (IP) core**
6. **netlist**

3.2 Terms specific to the present document

3.2.1 burst error

burst error is a continuous sequence of data containing errors

3.2.2 critical charge (Q_{crit})

minimum charge a particle deposits in an integrated circuit's node to corrupt its state

3.2.3 data block

group of bits that have an entity of their own, a pre-defined structure and can be subjected to mitigation mechanisms to detect or correct bit errors when verifying the structure correctness

NOTE 1 The term is synonymous to "data groups".

NOTE 2 Examples of groups of bits that have entity of their own include "data frames", "data packets", "data files", "memory pages", "memory words".

NOTE 3 Examples of pre-defined structure are a given bit group size, headers and tails.

NOTE 4 Examples of mitigation mechanisms include EDAC functions and ECC.

3.2.4 data groups

See "**data block**"

3.2.5 fault masking

phenomena happening when the occurrence of a Single Event Transient (SET) in a circuit does not result in a functional error at the output(s) of the circuit

NOTE 1 Fault masking can happen spontaneously thanks to a “natural” filtering away of the SET caused by the circuitry and the inputs at the time of the SET occurrence, or can be the result of deliberately introduced SET mitigation techniques.

NOTE 2 There are three types of “natural” fault masking phenomena, as explained in 12.2.3 : digital, electrical and temporal fault masking.

3.2.6 memory block

array of multiple memory cells normally organised in sets of bits that can be addressed independently to be read or overwritten in one go

NOTE These sets of bits are often called “words”.

3.2.7 memory cell

basic element of the integrated circuit where one bit of information can be stored, read and written

3.2.8 radiation hardening by design (RHBD)

design techniques that can be applied at physical layout level, at circuit architecture level or at electronic system level in order to mitigate radiation effects

NOTE 1 RHBD addresses both for TID and SEE mitigation.

NOTE 2 The use of RHBD techniques usually introduces a penalty in IC area, power consumption, timing, costs and/or longer development times.

3.2.9 radiation hardening by process (RHBP)

modifications at IC manufacturing process level in order to reduce radiation impact on integrated circuits

NOTE 1 This goal can be achieved by several means such as modifications of doping profiles in devices and substrates, deposition processes optimization for insulators and use of specific materials.

NOTE 2 RHBP mainly addresses TID and SEE effects.

3.3 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
A/MS	analogue/mixed signal
ADC	analogue-to-digital converter
APS	active pixel sensor
ASET	analogue single-event transient
ASIC	application specific integrated circuit
ATSC	Advanced Television Systems Committee
BICS	built-in current sensors
BJT	bipolar junction transistor
BOX	buried oxide
BPSG	borophosphosilicate glass
BRAM	block select RAM
CAD	computer aided design
CCD	charge-coupled device
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
CNES	Centre National d'Etudes Spatiales
COTS	commercial off-the-shelf
CPU	central processing unit
CRC	cyclic redundancy check
CWSP	code word state preserving
DAC	digital-to-analogue converter
DARE	design against radiation effects
DCC	differential charge cancellation
DCE	domain crossing event
DCM	digital clock manager
DFF	D-flip-flop
DICE	dual interlocked storage cell
DMR	dual modular redundancy
DMS	defense meteorological satellite
DMT	“Duplex Multiplexé dans le Temps”, Dual Multiplexing in Time
DRAM	dynamic random-access memory

Abbreviation	Meaning
DROM	demultiplexer-router-multiplexer
DSET	digital SET
DSL	digital subscriber line
DSP	digital signal processor
DT2	double duplex, tolerant to transients
DUT	device under test
DVB	digital video broadcasting
DWC	duplication with comparison
ECC	error-correcting codes
EDA	electronic design automation
EDAC	error detection and correction
EDDI	error detection by duplicated instructions
EEPROM	Electrically Erasable Programmable Read-Only Memory
ELT	enclosed layout transistor
ESA	European Space Agency
ESCIES	European Space Components Information Exchange System
ESD	electrostatic discharge
eV	electron-volt
FEC	forward error correction
FF	flip-flop
FIFO	first in, first out
FIR	finite impulse response
FIT	failure in time
FSM	finite state machine
FOX	field oxide
FPGA	field programmable gate array
FTI	Fault tolerant insertion
FTIS	fault tolerant injection and simulation
GCC	GNU compiler collection
GCR	galactic cosmic rays
GEO	geostationary orbit
GNU	GNU's not unix
GPS	Global Positioning System
HBFT	hypervisor-based fault tolerance
HBT	heterojunction bipolar transistor
HDL	hardware description language

Abbreviation	Meaning
HIT	heavy-ion tolerant
HW	hardware
HWICAP	hardware internal configuration access port
I/O	input/output
IC	integrated circuit
ILO	injection-locked oscillator
IOB	input/output block
ISRO	Indian Space Research Organisation
ISS	international space station
LCL	latching current limiter
LDPC	low density parity codes
LED	light-emitting diode
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
LTMR	local TMR
LUT	look-up table
LVDS	low-voltage differential signalling
LWS-SET	living with a star - space environment testbed
MAJ	majority voter
MBU	multiple bit upset
MCU	multiple cell upset
MDAC	Multiplying digital-to-analogue converter
MEO	medium earth orbit
MMU	memory management unit
MOS	metal oxide 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

Abbreviation	Meaning
N-MR	N-modular redundancy
OA	operational amplifier
PCI	peripheral component interconnect
PDS	phase dependent sensitivity
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
PVT	process, voltage and temperature
RAID	redundant array of independent disks
RAM	random access memory
RAR	Roshal ARchive
RHBD	radiation hardening by design
RHBP	radiation hardening by process
RoRa	reliability oriented place and route
RS	Reed-Solomon
RTL	register transfer level
SAA	South Atlantic anomaly
SEDR	single event dielectric rupture
SEGR	single event gate rupture
SEHE	single event hard error
SESB	single event snapback
SBIRS	space based infrared system
SCSI	small computer system interface
SE	soft error
SDRAM	synchronous dynamic random-access memory
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 latch-up
SER	soft error rate
SerDes	serializer/deserializer

Abbreviation	Meaning
SET	single event transient
SEU	single event upset
SIFT	software implemented hardware fault tolerance
SiGe	Silicon Germanium
SNR	signal-to-noise ratio
SoC	system on chip
SOI	silicon on insulator
SOS	silicon on sapphire
SPE	Solar particle event
SPF	single point failure
SPICE	Simulation Program with Integrated Circuit Emphasis
SRAM	Static Random Access Memory
SSD	solid-state drive
STI	shallow trench isolation
STRV	space technology research vehicle
SW	software
S/H	sample on hold
TID	total ionizing dose
TMR	triple modular redundancy
TNH	track and hold
TNID	total non-ionizing dose
TPA	two-photon absorption
UART	universal asynchronous receiver-transmitter
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
WOV	window of vulnerability

4 Radiation environment and integrated circuits

4.1 Overview

Failures induced by radiation have become one of the most challenging issues for modern electronic systems, in particular for space applications. Many efforts have been spent in the last decades to measure, model, test and mitigate radiation effects, applying numerous different techniques approaching the problem at various abstraction levels.

Section 4 gives the reader a general overview of radiation in space and its effects on integrated circuits. Firstly, the radiation environment is briefly summarised. It is then followed by a discussion on the major radiation effects on integrated devices. Finally, the test and validation methods are shortly exposed.

The content of this section is not exhaustive. It is only informative with the purpose to provide generic information on sources of radiation in space and their effects on ICs.

NOTE The text of this handbook contains several bibliographic references, indicated with "[#]".To find the appropriate title of the referenced document click on the "[#]".

4.2 Radiation environment in space

This section provides a brief summary of information from ECSS-E-ST-10-04, ECSS-E-ST-10-12 and ECSS-E-HB-10-12.

The radiation environment [1] takes its origin either in the Sun (e.g. solar flares, coronal mass ejection [2] and solar wind) or from outside the solar system (e.g. the galactic cosmic rays [3]). Energetic charged particles, mainly electrons, protons and heavy ions, are encountered throughout the Earth's magnetosphere, in interplanetary space and in the magnetospheres of other planets. Part of the particle spectra with energies in the MeV range or above are able to traverse spacecraft shielding and irradiate electronic components. In particular, spacecraft orbiting the Earth crosses the Earth's radiation belts (also named Van Allen belts), that extend from 100 km to 65000 km and consist principally of electrons and protons.

In addition to these primary particles, secondary radiation, such as X-rays produced by the interaction of electrons with shielding (e.g. Bremsstrahlung photons) are able to deposit large radiation doses in EEE components. Another example of secondary radiation are the secondary ionising particles (protons, ions) produced by the interaction of high energy protons with the component materials [4]. Some neutrons are also encountered in space, for example ejected by the Sun, or as secondary radiation in planetary environment, such as around Mars or the Earth. For LEO orbits around the Earth (incl. ISS), neutrons can be significant depending on the geomagnetic latitude and the solar activity. They come from the Earth's atmosphere, some of them being emitted back into space as atmospheric albedo neutrons.

The flux of particles in the Earth atmosphere at avionic and ground levels (from the cosmic ray shower in the atmosphere, and from the Earth telluric activity) are several orders of magnitude lower than the flux of particles encountered in space. Hardening of electronics at ground or avionic levels are not addressed here. This handbook only considers radiation effects and mitigation for the space radiation environment.

For each space mission, the radiation environment is specific; it is established including all types of radiation, depending on the orbit or voyage characteristics, the mission duration and possible shielding. Note that the space radiation environments are highly dynamic, depending on solar activity and "flares" (more correctly, solar particle events), and for specific missions (for example in the vicinity of Jupiter's moons) significant uncertainties remain. Therefore it is important that these large variations of the space radiation exposure are considered in the radiation design margins for EEE components selection and test.

4.3 Radiation Effects in ICs

4.3.1 Overview

This section provides a brief summary of information from ECSS-E-HB-10-12, ECSS-E-ST-10-12 and ECSS-Q-ST-60-15. It applies to EEE components in the spacecraft payload and launcher.

Radiation effects in EEE components can be separated into cumulative effects, which lead to a progressive degradation of the component characteristics, and single event effects, which gather different types of events, destructive or non-destructive, induced by a single particle.

4.3.2 Cumulative effects

Exposure to primary and secondary radiation produces relatively stable, long-term changes in devices and circuit's characteristics that can result in parametric degradation and ultimately in functional failure. Cumulative effects include both Total Ionizing Dose (TID) and displacement damage (DD), also called Total Non-Ionizing Dose (TNID):

- TID effects are induced by the transfer of ionising energy from the radiation exposure, which thermalized in the creation of electron-hole pairs in the component material. These charges typically get trapped in dielectric layers (e.g. oxides or nitrides) either in the bulk of the dielectric, or at or near the interface with the semiconductor where the electrostatic effect on the device operation is maximum. This produces a variety of effects on the device characteristics such as flatband and threshold voltage shifts, leakage currents and timing skews. TID is expressed in Gray (Gy) or rad (100 rad = 1 Gy), with 1 Gy = 1 J/kg. TID effects in semiconductors are discussed further in Clause 7 of ECSS-E-ST-10-12C, Section 6 of ECSS-E-HB-10-12C. TID test methods are described in ESCC22900. TID engineering approach for radiation hardness assurance is given in ECSS-Q-ST-60-15, section 5.1 TID effects are of concern for integrated circuits. Depending on the spacecraft mission and orbit, and the device shielding, the received TID typically ranges from few krad(Si) to several 100's krad [8]. Mitigation techniques to TID are addressed in this Handbook.
- TNID effects are induced by the non-ionising transfer of energy, i.e. by the interaction of primary and secondary energetic particles with component atoms, eventually creating damage and stable electrically active defects in the semiconductor crystal lattice. This gives rise to a variety of effects in bipolar devices and all types opto-electronics including CCD and APS detectors, LED and laser diodes. Typically ASICs and FPGAs are not be affected by TNID. This Handbook does not address mitigation techniques for TNID.

4.3.3 Single Event Effects (SEEs)

4.3.3.1 Overview

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 Latch-up (SEL) or Single-Event Gate Rupture (SEGR).

These effects can be produced, as also illustrated in Figure 4-1.

- By direct ionization, for example in the case of heavy ions and low energy protons (for deep sub. The heavy ion ionising effect is usually expressed by the linear energy transfer (LET), in EV*cm^2/mg, which is the ionising energy transferred along the ion path, normalised by the material volumetric mass density.
- By secondary particles issued from nuclear reactions or elastic collisions, as typically produced by protons. In this case particle (e.g. proton) energy is usually expressed in MeV.

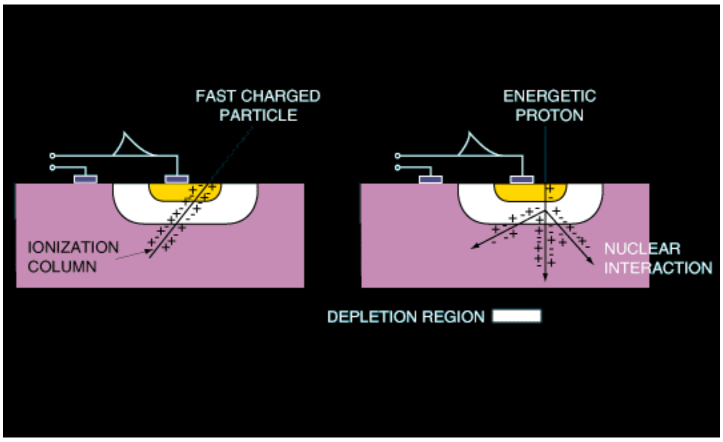


Figure 4-1: Schematic showing how galactic cosmic rays deposit energy in an electronic device, after Lauriente and Vampola [321]

The sensitivity of a device to SEE is often expressed by the cross-section σ as a function of the ion LET or proton energy. σ is defined by the ratio of the number of observed single events by the particle fluence (particles per cm^2) received by the component under test as explained in ESCC25100[5]:

σ = number of events / fluence

The cross-section represents the probability that an impinging particle provokes a single event. The unit of SEE cross-section is cm^2 for all types of circuits. In the particular case of upsets in memories, it can be normalised by the number of bits, i.e. expressed in cm^2/bit. When SEE are induced by direct ionisation from ions, the cross-section is representative of a sensitive area. For indirect ionisation from high energy protons, the SEE cross-section also includes the probability of nuclear interaction, which renders its interpretation more complex.

A non-exhaustive list of destructive and non-destructive SEE effects is provided in 4.3.3.2. These are summarised from Clause 9 of ECSS-E-ST-10-12C, Section 8 of ECSS-E-HB-10-12C, and ESCC25100. Other information about SEE test methods are exposed in ESCC25100, and SEE engineering approach for radiation hardness assurance in ECSS-Q-ST-60-15, Clause 5.3.

The non-destructive SEEs, also called soft errors, such as Single-Event Transient (SET), Single-Event Upset (SEU) and Single-Event Functional Interrupt (SEFI) are temporary and can be recovered. The destructive SEEs, such as Single-Event Latch-up (SEL), Single-Event Burnout (SEB) or Single-Event Gate Rupture (SEGR), lead to permanent damage. Those of interest for this handbook are detailed, while others, rarely encountered in ASICS and FPGA, are only shortly described.

4.3.3.2 Non-destructive SEE

4.3.3.2.1 Single-Event Transient (SET)

A SET is a temporary voltage excursion (voltage spike) at a node in an integrated circuit. It is generated by a single particle ionising the semiconductor and passing through or near a sensitive junction. SETs are usually separated in two categories:

- Analogue SET (ASET) in analogue and RF designs, and opto-electronics.
- Digital SET (DSET) in digital design, including all functions of combinatorial and sequential logic.

SETs are non-destructive. They result in a large variety of effects at the circuit level, ranging from a SEU (see 4.3.3.2.2) if the SET is captured by a storage element, to spurious voltage transients, false signal or miss counts, temporary disability of the circuit, or at worst SEFI (see 4.3.3.2.4).

4.3.3.2.2 Single-Event Upset (SEU)

An SEU is a single bit flip, i.e. the change of state of a storage element, such as flip-flops, latches or SRAM cells. SEUs can be either silent if unused or corrected by error correction code (ECC), or result in different types of effects at the circuit level, including circuit malfunction or SEFI.

As for SETs, the sensitivity to SEU greatly varies depending on the technology, design and electrical operation. In particular, small transistor dimensions and reduced supply voltage tend to decrease the critical charge (i.e. the minimum charge collected at a sensitive node able to induce a state change), and thus increase the sensitivity to SEEs.

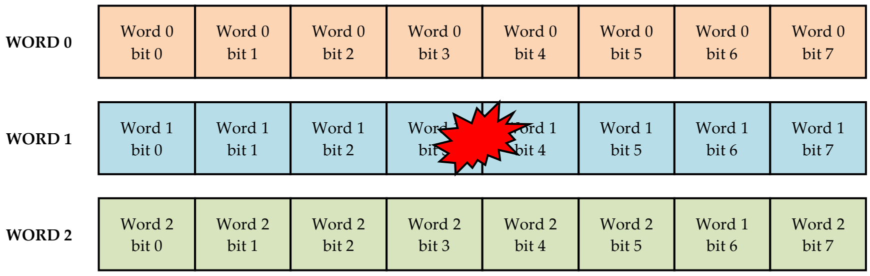
4.3.3.2.3 Multiple-Cell Upset (MCU) and Multiple-Bit Upset (MBU)

- MCU is the change of state of two or more logic cells induced by a single particle strike. The corrupted cells are usually, but not always, physically adjacent.
- MBU is a particular case of MCU when the corrupted cells are in the same word. Note that MBU cannot be corrected by a simple (single-bit) error correction code.

Integrated circuits tend to be increasingly sensitive to multiple upsets as gaps between transistors are becoming smaller with technology scaling. Charge deposited by an energetic particle can be collected by several sensitive nodes and thus results in SEUs in several memory cells.

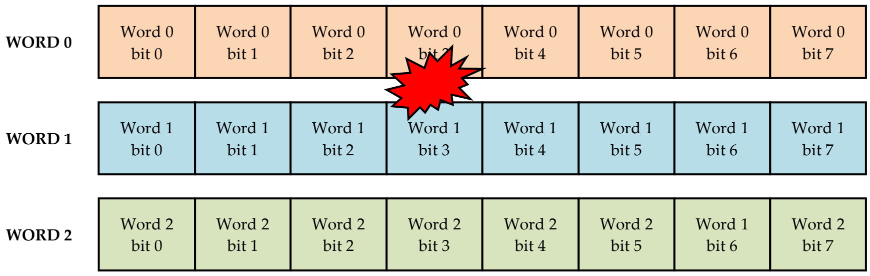
4.3.3.2.4 Single-Event Functional Interrupt (SEFI)

As defined in ECSS-E-HB-10-12, a SEFI is a soft error that causes the component to reset, lock-up, or otherwise malfunction. SEFI typically occurs in complex devices with built-in state/control sections like in modern memories (e.g. SDRAM, DRAM or NOR- and NAND-Flash), all types of processors, FPGA or ASICs, or mixed-signal devices [9]. Two main types of SEFI are distinguished depending on the actions required to restore operability: reset by software or by power cycling. The stored data can or cannot be lost.



WORD 0	Word 0 bit 0	Word 0 bit 1	Word 0 bit 2	Word 0 bit 3	Word 0 bit 4	Word 0 bit 5	Word 0 bit 6	Word 0 bit 7
WORD 1	Word 1 bit 0	Word 1 bit 1	Word 1 bit 2	Word 1 bit 3	Word 1 bit 4	Word 1 bit 5	Word 1 bit 6	Word 1 bit 7
WORD 2	Word 2 bit 0	Word 2 bit 1	Word 2 bit 2	Word 2 bit 3	Word 2 bit 4	Word 2 bit 5	Word 1 bit 6	Word 2 bit 7

Figure 4-2: Two upsets in the same word induced by a single particle (MBU)



WORD 0	Word 0 bit 0	Word 0 bit 1	Word 0 bit 2	Word 0 bit 3	Word 0 bit 4	Word 0 bit 5	Word 0 bit 6	Word 0 bit 7
WORD 1	Word 1 bit 0	Word 1 bit 1	Word 1 bit 2	Word 1 bit 3	Word 1 bit 4	Word 1 bit 5	Word 1 bit 6	Word 1 bit 7
WORD 2	Word 2 bit 0	Word 2 bit 1	Word 2 bit 2	Word 2 bit 3	Word 2 bit 4	Word 2 bit 5	Word 1 bit 6	Word 2 bit 7

Figure 4-3: Two upsets in the different words induced by a single particle (MCU)

4.3.3.3 Destructive SEE

4.3.3.3.1 Single-Event Latch-up (SEL)

A Single-Event Latch-up is the result of the triggering of a parasitic thyristor (PNPN or NPNP structures) mainly existing in CMOS circuits [345]. When it occurs, a high current flows and if the power supply is maintained, the device can be destroyed by thermal effect. The SEL signature is a self-sustainable current flowing in the low impedance path of the triggered parasitic thyristor structure whose gain increases with temperature. The only way to remove SEL is to power-reset the circuit. SEL are not to be mistaken with temporary current spikes resulting from SET induced logic conflicts or SEFI.

4.3.3.3.2 Single Event Snap-Back (SESB)

Another type of potentially destructive SEE, very similar to SEL with a self-sustainable current signature but less common, is the single event snap-back (SESB). The SESB is the result of the triggering of a parasitic bipolar structure (NPN or PNP). For example when each transistor is dielectrically isolated from its neighbours, SOI MOS is not sensitive to SEL, but it can be sensitive to SESB because of floating body effects when body contacts are insufficient.

4.3.3.3.3 Single Event Hard Error (SEHE)

As per ECSS-E-HB-10-12 and ESCC25100, a SEHE (also called “stuck bit” or hard error) is an unalterable change of state associated with a permanent or semi-permanent damage of a cell by an ion strike. This is typically encountered in all types of memories and digital devices.

4.3.3.3.4 Single Event Burnout (SEB)

As defined in ECSS-E-HB-10-12, SEB is the triggering of the parasitic bipolar structure in a power transistor (typically n-channel), accompanied by regenerative feed-back, avalanche and high current condition. SEB is potentially destructive unless suitably protected.

SEB is not frequent in ASICs and FPGAs, except in the case of embedded lateral or vertical power devices.

4.3.3.3.5 Single Event Gate Rupture (SEGR) or Single Event Dielectric Rupture (SEDR)

As defined in ECSS-E-HB-10-12, SEGR or SEDR is the destructive rupture of a gate oxide or any dielectric layer by a single ion strike. This leads to leakage currents under bias and can be observed in power MOSFETs, linear integrated circuits (with internal capacitors), or as stuck bits in digital devices. The energy transfer and damage induced by energetic heavy ions in dielectrics is so fast (<< ps) compared to the time response of any electrical protection (e.g. filtering), that there is no possible protection against SEGR / SEDR.

4.3.3.4 Summary

Table 4-1 summarises the major single event effects (SEEs) typically encountered in different types of component technologies and families.

Table 4-1: Summary of single event effects (SEE) as a function of component technology and family

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

5 Choosing a device hardening strategy

5.1 The optimal strategy

In the vast majority of cases, not just one but several mitigation techniques are applied to protect ASICs or FPGAs from the radiation effects.

There are multiple parameters that determine what makes one group of techniques more or less suitable in each case. There are always compromises to be made between the technical requirements and goals, and the actual financial, development time and resources constraints.

There is no ideal decision-flow-chart or recipe to guide a system and/or component designer about which techniques are the best ones for his/her case, however this Section gives some general guidelines on what to consider. Multiple aspects, expertise and inputs are taken into account:

- Space radiation environment experts and system engineers providing the radiation environment requirements,
- System and product assurance engineers providing the reliability, performance and availability (can the system tolerate pauses in its operation?) targets,
- Vendor provided information on the radiation effects sensitivity of the candidate technologies (or existing part) to be used,
- Any independent or internally acquired complementary information about the sensitivity of the technology to be used (more radiation effects tests results),
- Experience (and access to relevant IC design tools) of the actual IC designers in applying safely and efficiently rad effects mitigation,
- Experience (and access to relevant PCB/electronic system design tools) of the system engineers where the device is intended to be used in applying safely and efficiently rad effects mitigation.

A simplified flow to make correct decisions over which mitigations can be applied (or selected) can look like this:

1. Define the radiation environment that can affect your IC (what radiation levels for my orbit, mission duration?).
2. Define the reliability targets, i.e. how many errors (of a given fault class) per time unit (e.g. year) can be tolerated by the user.
3. Identify candidate IC technologies or existing parts and collect data on their sensitivity to TID and SEE.
4. Identify and quantify all the effects (pros and cons) of mitigation techniques which can be introduced at the various levels.
5. Choose the best compromise of mitigation that allows to meet the reliability targets while also respecting the rest of the requirements. In doing this, the expected levels of final fault tolerance (e.g. error rates) are estimated by analysis, simulation or tests.
6. Once implemented, validate the selected approach by fault-injection and/or radiation testing.

The best choice of basic technology and mitigation that allows to meet all technical requirements and cost and schedule constraints often requires several iterations along points 3 - 6 above.

While insufficient protection can cause costly corrections at a late stage in the flow, it is emphasised here that over-protecting can be equally detrimental to the success of a development, as it can lead to excessive complexity, performance degradation or long development times.

In the following sections these steps are explained and linked to the rest of the sections of this handbook.

5.2 How to use this handbook

This handbook has been written and structured as a compilation of known mitigation techniques, preceded by an overview of basic concepts about the radiation environment and its potential negative effects in ASICs and FPGAs (Section 4) and ending with guidelines to validate that those mitigation techniques are working as expected (Section 16).

It is important to understand that these mitigation techniques can be applied at "different levels" or stages of the creation or use of the integrated circuit, and therefore by different types of specialists. Mitigation techniques presented in this handbook are classified according to the following identified "levels" of abstraction:

- Manufacturing Process level: techniques concerning manufacturing processes, also known as Radiation Hardening By Process. These approaches generally concern modifications of doping profiles in devices and substrates, deposition processes optimization for insulators and use of specific materials.
- Physical Layout level: techniques aiming at optimizing transistor's layout and placement in order to reduce radiation sensitivity of the final circuit.
- Circuit Architecture level: techniques devoted to this level are most often specific to circuit's nature (digital, analogue or mixed signal) and/or to 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).
- Electronic System level: these techniques apply at component level (e.g. microprocessor redundancy), unit level or embedded software level (e.g. computer redundancy).

These different "levels" and the naming conventions used in this handbook are explained graphically in Figure 5-1.

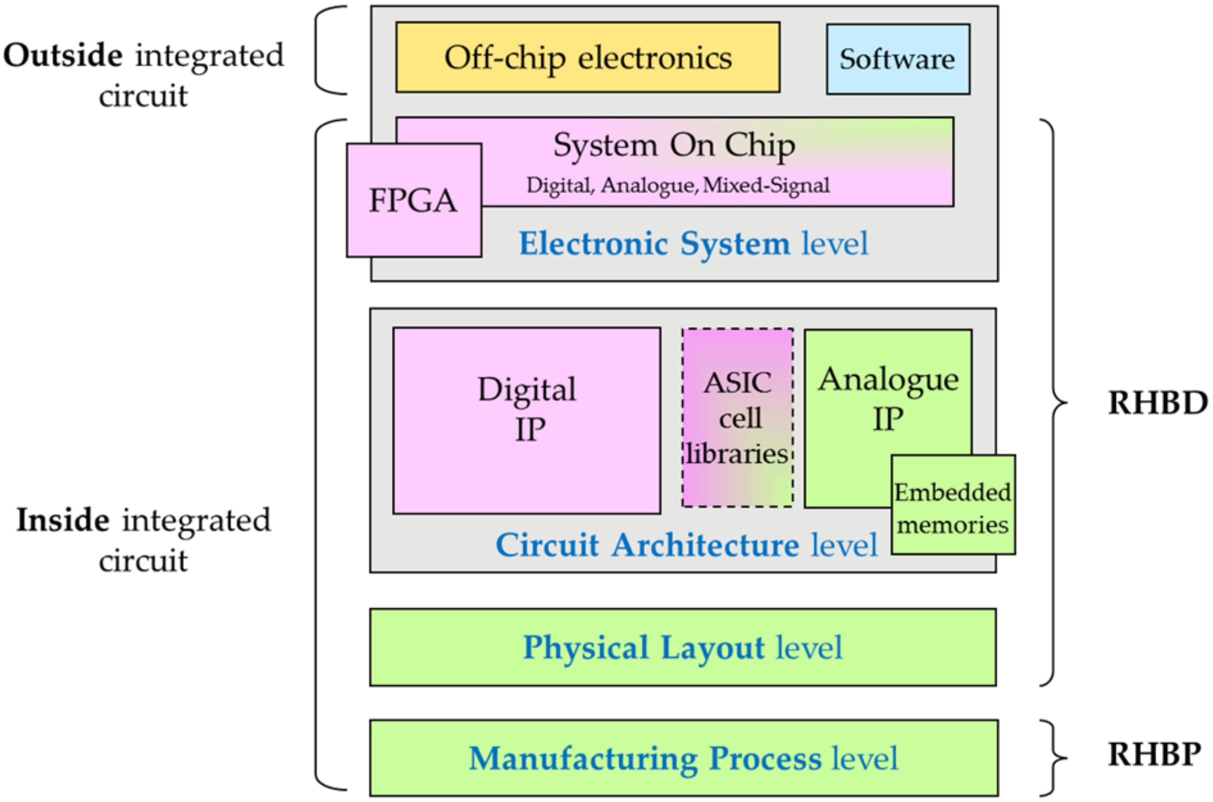


Figure 5-1: Different abstraction levels where mitigation techniques can be applied and naming convention for this Handbook.

In fact, it was difficult to decide how to classify and present to the readers the various mitigation techniques, since many of them, conceptually are the same, and yet, can be applied at different "levels". For example, the well-known "TMR" technique (hardware redundancy and voting), can be applied at "cell" level, by designers creating a rad hard flip-flop for an ASIC cell library or rad-hard memory elements to be pre-diffused in rad-hard FPGAs. This work is done by IC designers who do design at transistor, full-custom analogue level. However, the same TMR concept can be applied at a higher-level by the IC designers making use of the ASIC or FPGA design kits, and choosing to triplicate non-rad-hard cells and majority vote afterwards. At an even higher-level of abstraction, we can choose to triplicate an entire non-rad hard ASIC or FPGA on the PCB, and majority vote on their outputs, to discard a bad output due to radiation.

In an effort to avoid repetitions, the strategy adopted in this handbook is to explain each mitigation technique only once, in the Section corresponding to the level where the technique is most often applied. In other abstraction levels addressed in other Sections of this handbook where the same technique can be applied, a cross-reference is made to where the technique is fully described.

Depending on the actual background and role of the reader of this handbook, one or another Section is more relevant in order to find, decide or apply the relevant mitigation techniques according to his/her area of expertise and his/her role in the ASIC or FPGA development or utilisation.

Depending on the orbit type, the mission duration and the expected solar activity during the mission, the worst case radiation levels are investigated and communicated to the system and component engineers who have to decide how to protect the ICs. If standard components are developed, it is important to consider multiple orbit types. Section 4 gives an overview on the radiation environment affecting ICs and the expected radiation effects. Section 4 also includes a list of the standards and handbooks that explain how the radiation levels can be calculated and the relevant modelling tools (e.g.

dose depth curves, 3D Monte Carlo, SHIELDOSE2, Geant4, Novice, SPENVIS or OMERE) and the physical parameters and units used to quantify these effects (e.g. LET threshold and SEU cross-sections).

Different ASIC and FPGA vendors offer different levels of (intrinsic) radiation protection, depending on their exact ASIC or FPGA family type, the choice of library cells and the package type.

Annex A provides the link to the several vendors of ASIC and FPGA technology that already incorporate radiation effects mitigation techniques in their technology and which either have acquired or are pursuing some level of qualification for use in space. These are examples, the list is certainly not complete, and it is of course subject to future updates as new company or institution provided solutions become available, and some technology or tools become obsolete or discontinued.

Sections 6, 7, 8, 9 and 10 describe some of the techniques that are often applied by ASIC and FPGA vendors but also by IC designers, at different levels, in order to achieve various levels of radiation hardness. The datasheets of these products normally indicate to the users/designers, what is the sensitivity per device or per cell inside the device, for a given typical orbit case or radiation profile. However, detailed information is often not contained in public datasheets, it can only be provided on request and under Non-Disclosure-Agreement (NDA). Users are therefore advised to contact the vendors to provide the necessary details over the actual radiation tests and results obtained when characterising the technology.

Mitigation introduced by the IC designer. In addition to selecting a base technology or existing part, additional mitigation that can be added by the IC designer (for new designs) is explained in sections 8, 11, 12 and 13.

All sections in the handbook try to summarise which are the costs and the added value of applying each method. Some concrete examples, including sometimes improvements on the failure rate, are provided for many of the proposed techniques. However, it is emphasised that the actual cost and benefit of each individual measure can strongly vary depending on technology, design, radiation environment and the implementation details. The effect is therefore to be evaluated for every individual case.

As Sections 14 and 15 explain, there are additional mitigation techniques that can be applied by the software and hardware system engineers. Moreover, many applications already contain an intrinsic fault-tolerance, e.g. the forward error correction present in many communication protocols. Together with technology selection and mitigation during IC-design, it is important to assess the system-level mitigation in a holistic approach, in order to determine the optimal strategy.

6
Technology selection and process level mitigation

6.1 Overview

Section 6 provides guidance for the selection or modification of existing processes in order to reduce the consequences of radiation in integrated circuits. Radiation-Hardening-By-Process (RHBP), as this approach is sometimes named, 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. The effects of technology scaling for TID and SEE are discussed at the end of this section.

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 (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).

A summary of mitigation techniques and the radiation effects they address are given in Table 6-1.

Table 6-1: Summary of mitigation techniques at manufacturing process level and the radiation effects they address

Mitigation techniques		Radiation effects			
		TID	SET	SEU	SEL
6.2.1	Epitaxial layers				X
6.2.2	Silicon On Insulator		X	X	X
6.2.3	Triple wells			X	X
6.2.4	Buried layers		X	X	X
6.2.5	Dry thermal oxidation	X			
6.2.6	Implantation into oxides	X			

6.2 Mitigation techniques

6.2.1 Epitaxial layers

6.2.1.1 Description of the concept

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 6-1).

For radiation hardening, the main interest of epitaxial layers is in the reduction of the gain in the PNPN thyristor parasitic structures that benefits from the lower substrate resistance. The epi layer acts as a higher resistivity barrier between the heavily doped P+ substrate and the N-well, thus reducing the risk of latch-up.

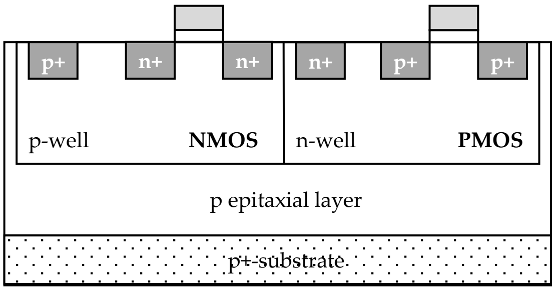


Figure 6-1: Example of epitaxial layer in CMOS technology

P-type epitaxial layer on P+ substrates is a common choice for latch-up mitigation, and it is important to tune and optimise this epitaxial layer.

6.2.1.2 Available test data (simulations, radiation testing, in-flight)

In the case presented in [12] the EPI layer needed to be thinner than 2.75um to eliminate soft-error induced single event latchup. Other test cases are presented in [11].

6.2.1.3 Known issues (weaknesses, elements to be considered)

The efficiency of the epitaxial 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.

The brief summary of key characteristics for epitaxial layers is given in the Table 6-2.

Table 6-2: Summary of key characteristics for epitaxial layers

Abstraction level	Manufacturing process
Pros	Increase SEL hardness
Cons	Fabrication cost
Mitigated effects	SEL
Suitable validation methods	Ground accelerated tests

6.2.2 Silicon On Insulator

6.2.2.1 Description of the concept

6.2.2.1.1 Overview

The Silicon On Insulator (SOI) technology [14] is an alternative to bulk silicon substrates in CMOS semiconductor manufacturing In Silicon On Insulator (SOI) fabrication process, transistors are implemented in a silicon layer, built over a silicon dioxide insulating layer (SiO_2), called Buried OXide (BOX), (Figure 6-2(b-c)). This substrate architecture can improve device density and eliminates current paths to parasitic devices.

6.2.2.1.2 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 6-2(c)).

On the other hand, if the insulated layer is thicker, the inversion region does not extend the full depth of the body, the volume is then said to be "partially depleted" (Figure 6-2(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 [15].

6.2.2.2 Impact on radiation effects

6.2.2.2.1 SEL immunity

SOI inherently eliminates latch-up, 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 transient. Because the wells in an SOI device are completely oxide isolated, the parasitic thyristor effect cannot occur.

6.2.2.2.2 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 [16]. 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 where the area penalty of body-ties can be reduced [285].

6.2.2.2.3 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 [17] presents how TID charge in partially-depleted device's BOX layer can reduce the back channel threshold voltage and increase leakage.

Reference [18] 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 can 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 6.2.6 implantation into oxide), or removal of the substrate and thinning or removal of the BOX layer [19].

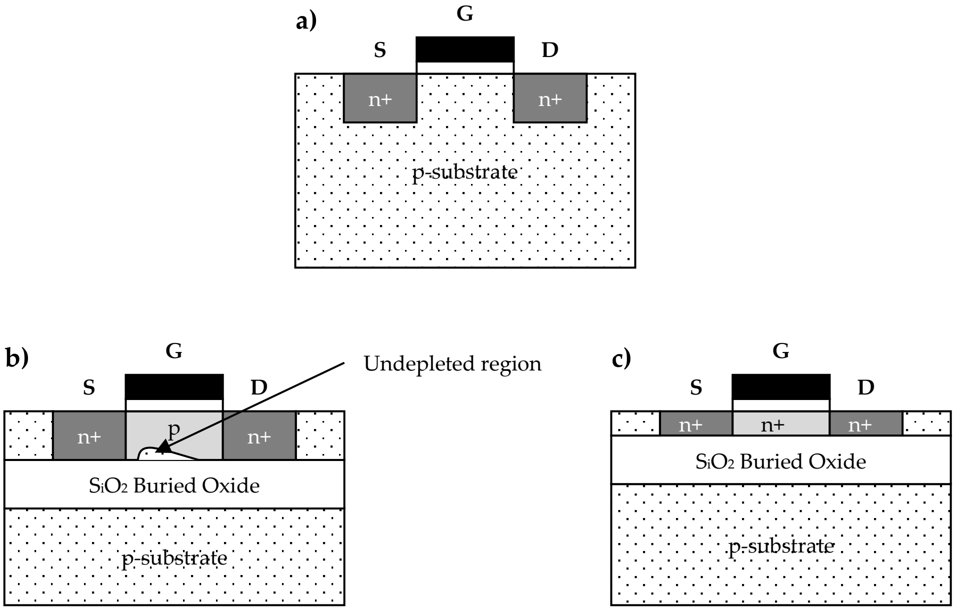


Figure 6-2: a) Conventional bulk NMOS transistor, b) Partially depleted SOI, c) Fully depleted SOI

As an example, Silicon On Sapphire (SOS) [20] is a hetero-epitaxial technique where a silicon film is grown on a sapphire (Al_2O_3) substrate. SOS was the first mature SOI technology [21], [22], [23], [24]. According to [17], until the 1980s, it was the only SOI technology able to produce LSI-VLSI circuits, such as for example microprocessors, SRAMs, gate arrays or ADCs.

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 performance as this capacitor does not need to be charged and discharged on every cycle. This performance increase allows producing circuits with the same performance as 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.

SOS is produced by 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.

6.2.2.3 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 [25].
- The Soft Error Rate (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 [26].
- 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 [27].
- Circuit simulations and experimental data were correlated in order to compare the intrinsic hardness of 0,25 µm SOI and bulk technologies [28]. 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 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 [29]. 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 [30]. 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 material was investigated [31]. Threshold-voltage shifts of the front-gate and back-gate transistors are observed. The conclusion is that this technology can perform well in a proton-radiation environment.
- Body-ties effects on SEU resistance were analysed for a 0,2 µm fully depleted SOI SRAM [16]. 3D simulations revealed an increase in the threshold LET from 5,8 MeV/(mg/cm^2) to 8,1 MeV/(mg/cm^2).

6.2.2.4 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.

6.2.2.5 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.

The brief summary of key characteristics for silicon on insulator is given in the Table 6-3.

Table 6-3: Summary of key characteristics for silicon on insulator

Abstraction level	Manufacturing 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

6.2.3 Triple wells

6.2.3.1 Description of the concept

Hardening devices against Single Event Effects can be done by reducing charge collection at critical device nodes. This can be accomplished by introducing extra doping layers to limit substrate collection [11], [32]. In SRAMs, triple-well structures have been used to decrease SEU and SEL sensitivity [11], [12], [33].

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. We now describe three different well structures:

- The single-well process, illustrated in Figure 6-3 (a), uses an N-well to build a PMOS in a P-type substrate. This technology can make use of a heavily doped substrate, which increases the probability of having SEL due to PNPN parasitic paths that use the low resistivity substrate.
- 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 PMOS transistors (Figure 6-3(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 of both types of transistors to be tuned independently. Because of the lightly doped substrate, thus providing a high resistivity zone, the risk of latch-up is decreased compared to the single-well process.
- In the triple well process, assuming a P-type substrate as illustrated in Figure 6-3 (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.

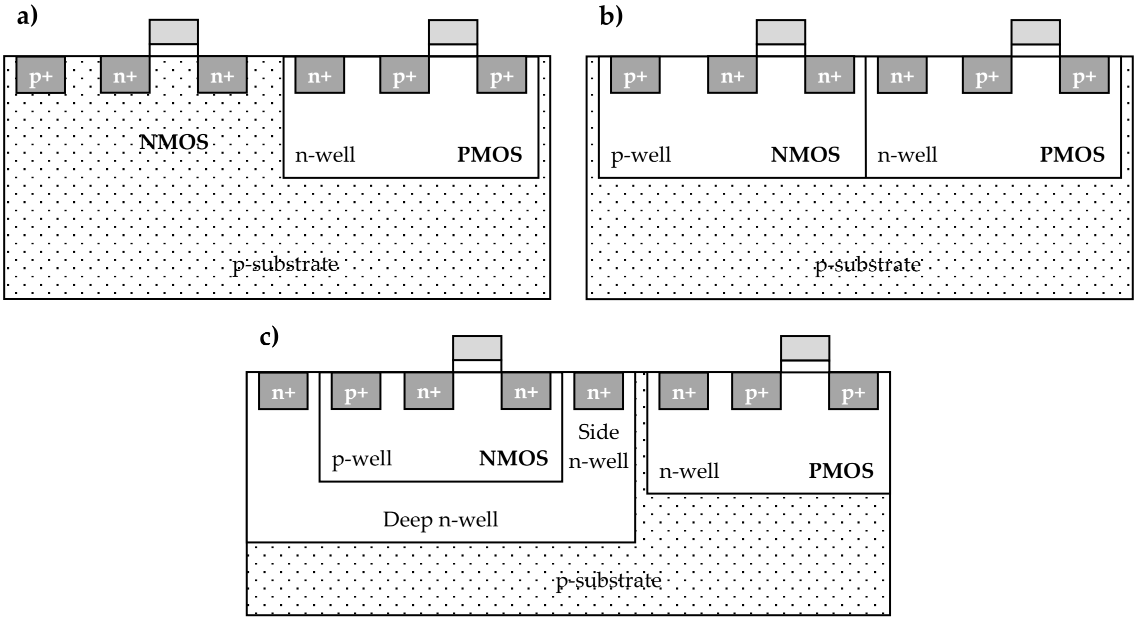


Figure 6-3: a) single-well technology, b) twin-well technology, c) triple-well technology implementing a deep n-well to isolate the p-well forming the NMOS from the substrate

6.2.3.2 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 nm and 90 nm latches and [11], [34]. A study [34] showed a 40 % lower SER (alpha & neutron) for SRAM and latches with triple well.

6.2.3.3 Known issues (weaknesses, elements to be considered)

- Triple-well has been demonstrated to increase the SER in 150 nm memory devices [35]. 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 [12].
- This condition can 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 [36], [37].

The brief summary of key characteristics for triple wells is given in the Table 6-4**.**

Table 6-4: Summary of key characteristics for triple wells

Abstraction level	Manufacturing process
Pros	Increase SEU and SEL hardness
Cons	Increase manufacturing cost, in some cases SET can increase
Mitigated effects	SEU, SEL
Suitable validation methods	Ground accelerated tests

6.2.4 Buried layers

6.2.4.1 Description of the concept

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 [38]. The doping profiles and the presence of buried layers (which can include doped layers, insulating layers, or layers of modified material properties) can impact the radiation response of devices [11], and therefore it is important to consider this in the study of radiation effects and mitigation options. For example, an increase in the current necessary to trigger electrical latch-up results in an increase of Single Event Latch-up immunity.

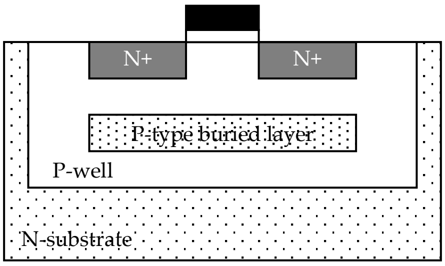


Figure 6-4: Schematic view of a P-type buried layer in a P-well

A few examples:

- 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 [39].
- In addition to global buried layers, buried layers can be selectively added below device regions to optimize performance or for radiation effects mitigation. Examples include buried P+ layers (Figure 6-4) within the P-well [40] or an N-grid [41] to reduce alpha particle single event sensitivity. While buried layers in CMOS remain an effective strategy for latch-up mitigation, results of [11], [33], [12], [42] suggest limited effectiveness for mitigation of single event errors, and demonstrate that proper triple well designs can 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 latch-up [43], and thus has been proposed

to reduce heavy ion charge collection [13]. Device simulation shows that the impact of the buried layer on the charge collection reduction happens at somewhat longer times [13].

- 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 [44]. While this is not a silicon device, the concept is interesting and can be applicable.

6.2.4.2 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 [13].

6.2.4.3 Added value (efficiency)

Buried layers in CMOS are an effective strategy for latch-up mitigation.

6.2.4.4 Known issues (weaknesses, elements to be considered)

Buried layers offers limited effectiveness for mitigation of SER, results demonstrate that proper triple well designs can be a more effective strategy for advanced CMOS [11], [33], [12], [42]. Brief summary of key characteristics for buried layers is given in the Table 6-5.

Table 6-5: Summary of key characteristics for buried layers

Abstraction level	Manufacturing process
Pros	Increase SEL and SER hardness
Cons	Increase fabrication costs
Mitigated effects	SET, SEU, SEL
Suitable validation methods	Ground accelerated tests

6.2.5 Dry thermal oxidation

6.2.5.1 Description of the concept

As explained in section 6.1 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 (e.g. growth/deposition rates and times, temperatures, gas cocktail), or by pre-, co- or post-processing such as specialized implantation or annealing steps

A few examples:

- The growth temperature is an important parameter as it was demonstrated that hole trapping varies inversely with dry-oxygen growth temperatures over 900 °C - 1200 °C [45].
- Nitrogen incorporation during growth can degrade the TID hardness, while use of Argon instead does not degrade the hardness [45].
- 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 [45].

- Nitrogen implantation into silicon prior to oxidation improved the proton radiation hardness of oxynitride gate NMOS transistors [46].

These process parameters are verified by test. There are several other parameters that play a role during thermal oxidation, like defects due to contamination or internal wafer stress which could also impact the TID hardness. In addition, other oxidation processes applied during the back-end (e.g. CVD or PVD) could also have an impact in the final TID hardness of the oxides.

6.2.5.2 Available test data (simulations, radiation testing, in-flight)

The available test data presented in [45] and [46] showing impact of thermal oxidation process parameters on TID hardness is summarised in the Table 6-6.

Table 6-6: Impact of thermal oxidation process parameters on TID hardness

Process variable	Value	Impact
Temperature	1/T (900 °C < 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	5 keV 10^{14} cm^{-2} < 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)

6.2.5.3 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.

6.2.5.4 Known issues (weaknesses, elements to be considered)

For some parameters that degrade hardness, see Table 6-7. The brief summary of key characteristics for dry thermal oxidation is given in Table 6-7.

Table 6-7: Summary of key characteristics for dry thermal oxidation

Abstraction level	Manufacturing process
Pros	Improved proton TID hardness
Cons	Increased fabrication cost
Mitigated effects	TID
Suitable validation methods	Ground accelerated tests

6.2.6 Implantation into oxides

6.2.6.1 Description of the concept

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 [47], [48], [49].

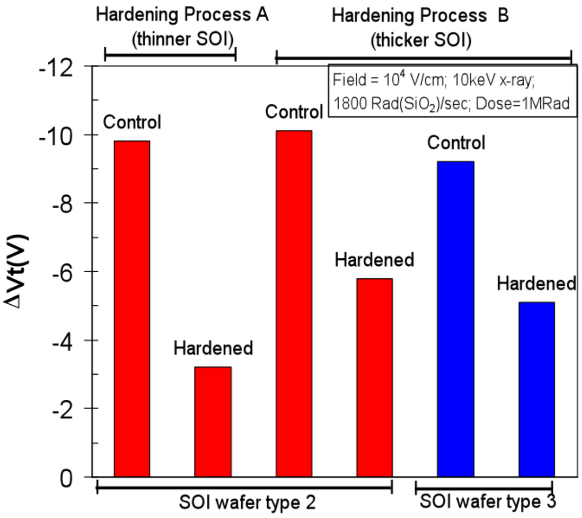


Figure 6-5: Radiation-induced back channel threshold voltage shifts for different SOI substrates types, SOI layer thickness and hardening process conditions [1]

SOI technology is presently used in many commercial applications, particularly microprocessors, and in some rad-hard CMOS applications. As presented in 6.2.2, SOI helps to mitigate single event effects. However the Buried OXide (BOX) layer presents an additional insulator for charge trapping. This can 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 [48]. Test results, illustrated in Figure 6-5, 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 [50].

6.2.6.2 Available test data (simulations, radiation testing, in-flight)

- Fluorine doping has been shown to improve the radiation hardness of gate and field oxides [48], [51].
- The TID degradation of current gain of lateral PNP transistors is reduced with As implanted SiO_2 passivation on the emitter base junction [48]. The use of SiC passivation has also been demonstrated to improve the TID hardness of bipolar transistors [52].
- Arsenic implanted SiO_2 reduces TID degradation in lateral PNP BJT [49]. However As in MOS gate oxides can be detrimental [53].

6.2.6.3 Known issues (weaknesses, elements to be considered)

- Hardness degradation was observed with As implantation in gate oxide [53].
- Boron doping (such as comes from the Boron gate doping in CMOS processes) has been shown to degrade the hardness [6], [54].
- Implantation of Si into oxide was shown to increase the electron trap density [55]. 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 [56] 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.

The brief summary of key characteristics for implantation into oxides is given in the Table 6-8.

Table 6-8: Summary of key characteristics for implantation into oxides

Abstraction level	Manufacturing process
Pros	Improved radiation hardness
Cons	Increased fabrication cost
Mitigated effects	TID
Suitable validation methods	Ground accelerated tests

6.3 Technology scaling and radiation effects

6.3.1 General

The impact of technology scaling on the response of integrated circuits to radiation effects cannot be evaluated only by taking into account the channel size and the geometry of the transistors. As explained in reference [57], studies have shown that differences in size and geometry affect 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 can twist the predictions. The effects of device scaling on soft-error rate depend on several competing factors. Among them the critical charge necessary to upset a memory bit is expected to decrease as depicted in early studies [58]. In fact, the increase of radiation effect immunity exists but is not less obvious [59]. Another factor to take into account is the charge collection depth which generally decreases with scaling, hence improving robustness of the circuits [61]. 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 are important to take into consideration as they are not negligible anymore[60].

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.

6.3.2 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 remained unchanged [59]. 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 [59] also mentions that the decrease of the device size can potentially increase the upset rate in the terrestrial environment as the range of recoil atoms is increasing when devices become smaller and thus the energy level at which the device is upset is lower.

The study presented in reference [59] concludes on the fact that the cross-section generally decreases when devices become smaller but the rise of the frequency increases the cross-section. However, the magnitude of the frequency dependency decreases as the circuit becomes smaller.

6.3.3 DRAM memories

DRAM is currently one of the most robust devices in term of soft errors[10], [59]. 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 1000, thus the overall DRAM system sensitivity has remained essentially unchanged. As frequency continuously increases, transient errors in bit lines and sense amplifiers around the memory cells become dominant in the next memory generations, thus soft error rate is expected to increase.

6.3.4 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 [10]. 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 [17]. Most recently, with technologies below 0,25 μm, the SRAM single bit SER has saturated and can 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

[59]. Error Detection And Correction (EDAC) codes is the best means to mitigate memory soft errors but the system failure rates can be challenged by the SER in sequential logic.

6.3.5 Sequential and combinatorial 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 [10], [59]. 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 can 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 efficiency of memory error correction.

In combinatorial 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.

7 Layout

7.1 Overview

7.1.1 General

Section 7 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 latch-up phenomena, though SET and SEU effects are also mitigated. Section 8 takes the next level of complexity, discussing mitigation techniques accomplished by design constructs using making use of transistors and other basic circuit elements.

7.1.2 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 7-1), such as gate oxide and Shallow Trench Isolation (STI) oxide [62], [282], or at interface with silicon. It has been demonstrated that the total dose effect decreases as that oxide's thickness scales down[63], [64], [65]. These studies showed that less than 5 nm gate oxide thickness obtained in submicron processes of 250 nm and below are far less sensitive to total dose effects than larger technology nodes. Consequently these type of gate oxides do not exhibit significant TID effects when used in radiation environments.

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 [66]. This leakage current occurs at the interface between STI oxide and p-doped regions, a straightforward solution is thus to avoid contacts between these two zones by changing transistors layout [67]. Several designs are possible but the most commonly used is the so called Enclosed Layout Transistor (ELT).

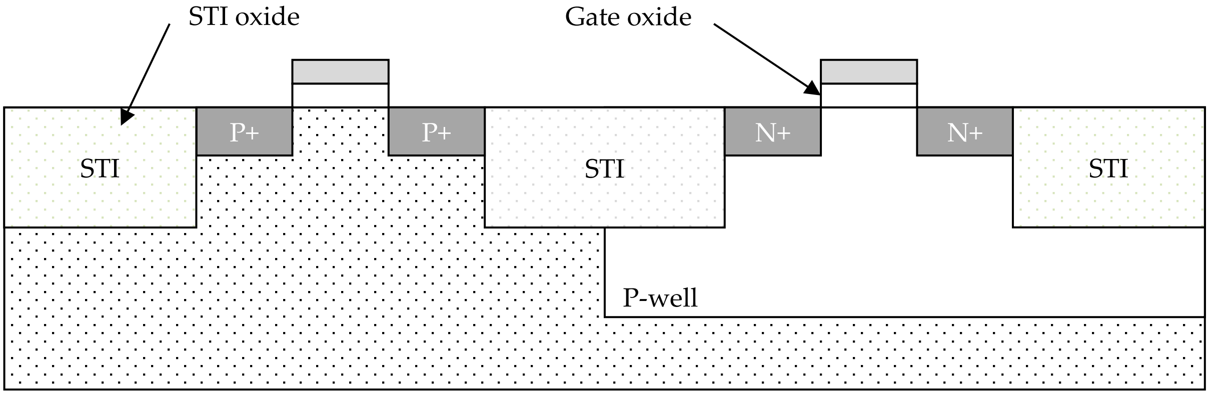


Figure 7-1: Gate oxide and STI oxide in CMOS technology

7.1.3 Hardening against SEL

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

A summary of mitigation techniques and the radiation effects they address is given in the Table 7-1.

Table 7-1: Summary of mitigation techniques at physical layout level and the radiation effects they address

Mitigation techniques		Radiation effects				
		TID	SEL	SET	SEU	MBU/MCU
7.2.1	Ringed or Enclosed Layout Transistor	X		X	X	
7.2.2	Contacts and guard rings	X	X	X		X
7.2.3	Dummy transistors		X	X		
7.2.4	Transistors Gate W/L ratio sizing	X				

7.2 Mitigation techniques

7.2.1 Ringed or Enclosed Layout Transistor

7.2.1.1 Description of the concept

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 [67]. The most effective layout uses Enclosed Layout Transistor (ELT), also called Re-entrant Transistor, Ringed Transistor or Edge-Less Transistor, illustrated in Figure 7-2. A re-entrant design is only used for the n-channel, 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 centre of the structure.

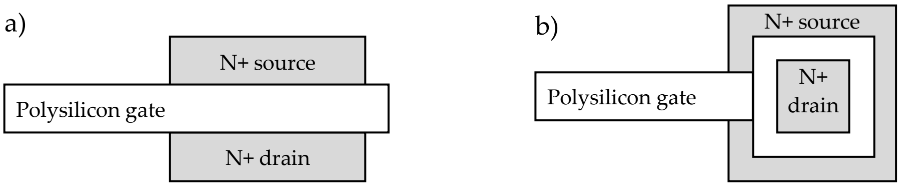


Figure 7-2: a) Conventional two edge NMOS, b) Enclosed Layout Transistor NMOS

Enclosed Layout Transistor is not the only alternative transistor design aimed at reducing the impact of radiation. Figure 7-3 gives examples of two NMOS transistor designs able to eliminate radiation-induced leakage current between source and drain doped regions. Ringed source and ringed interdigitized design have the advantage to offer compact transistors, however they often violate design rules and are sometimes not completely immune to TID effects [68]. Yet, the most commonly used design is the ELT.

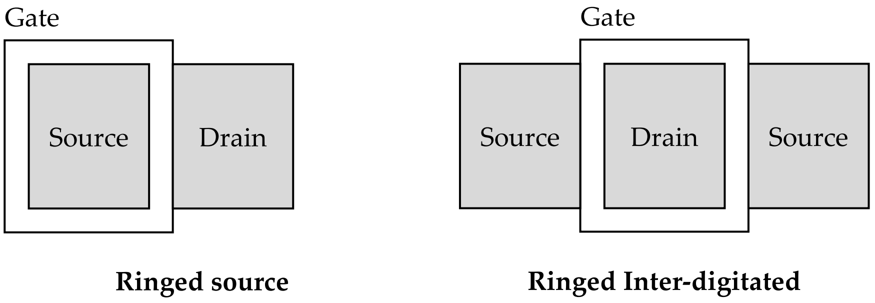


Figure 7-3: Two examples of NMOS transistor layout eliminating radiation-induced leakage current between source and drain

Several vendors offer rad-hard ASIC libraries which contain digital and analogue functional cells that are built with ELT. Examples of these libraries can be found in Section 10.

7.2.1.2 Available test data (simulations, radiation testing, in-flight)

Using ELT NMOS transistors in combination with guard rings (section 7.2.2) has been demonstrated to provide efficient robustness against the effects of radiation [69], [70], [71]. 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 specific process care.

Reference [72] 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 analogue design, the area penalty is important only for long channel ELT devices; a circuit containing a few of this kind of transistor exhibits a non-significant area increase. For digital design, the area penalty factor is generally between 1,5 and 3,5.

7.2.1.3 Added value (efficiency)

- Reduces current leakage [72]
- Reduces SET and SEU sensitivity
- Can be applied to all technologies

7.2.1.4 Known issues (weaknesses, elements to be considered)

Area penalty for analogue circuit: can be small or important depending on the number of long channel ELT devices in the circuit.

Area and power of digital circuits increase by a factor of 1,5 to 3,5.

Using ELT transistors is not a direct approach. It is important that designers are 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 [73].

In some deep submicron technologies, the manufacturing design rules can sometimes make difficult or even impossible the implementation of ELT.

The brief summary of key characteristics for enclosed layout transistor is given in the Table 7-2.

Table 7-2: Summary of key characteristics for enclosed layout transistor

Abstraction level	Physical 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

7.2.2 Contacts and guard rings

7.2.2.1 Description of the concept

The latch-up phenomenon can occur when the two bipolar transistors, forming a parasitic thyristor (shown in Figure 7-4), 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 can lead to a local destruction of the MOS structures.

Preventing latch-up from occurring can 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 7-5).

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 remove possibility of latch-up but the thyristor's sensitivity is drastically reduced.

Guard rings around NMOS are normally helping to mitigate TID. The reason is that the thick oxide FOX parasitic NMOS can get inverted by charges in the oxide and cause leakage between nodes, and this effect is blocked by the guard ring.

Guard rings also mitigate SETs, since ion-induced charges are collected by the guard electrode, once they pass over the STI. The smart placement of "dummy transistors" can result in an improvement to this charge collection (see 7.2.3).

Contacts and guard rings are usually combined with the use of Enclosed Layout Transistors (see 7.2.1).

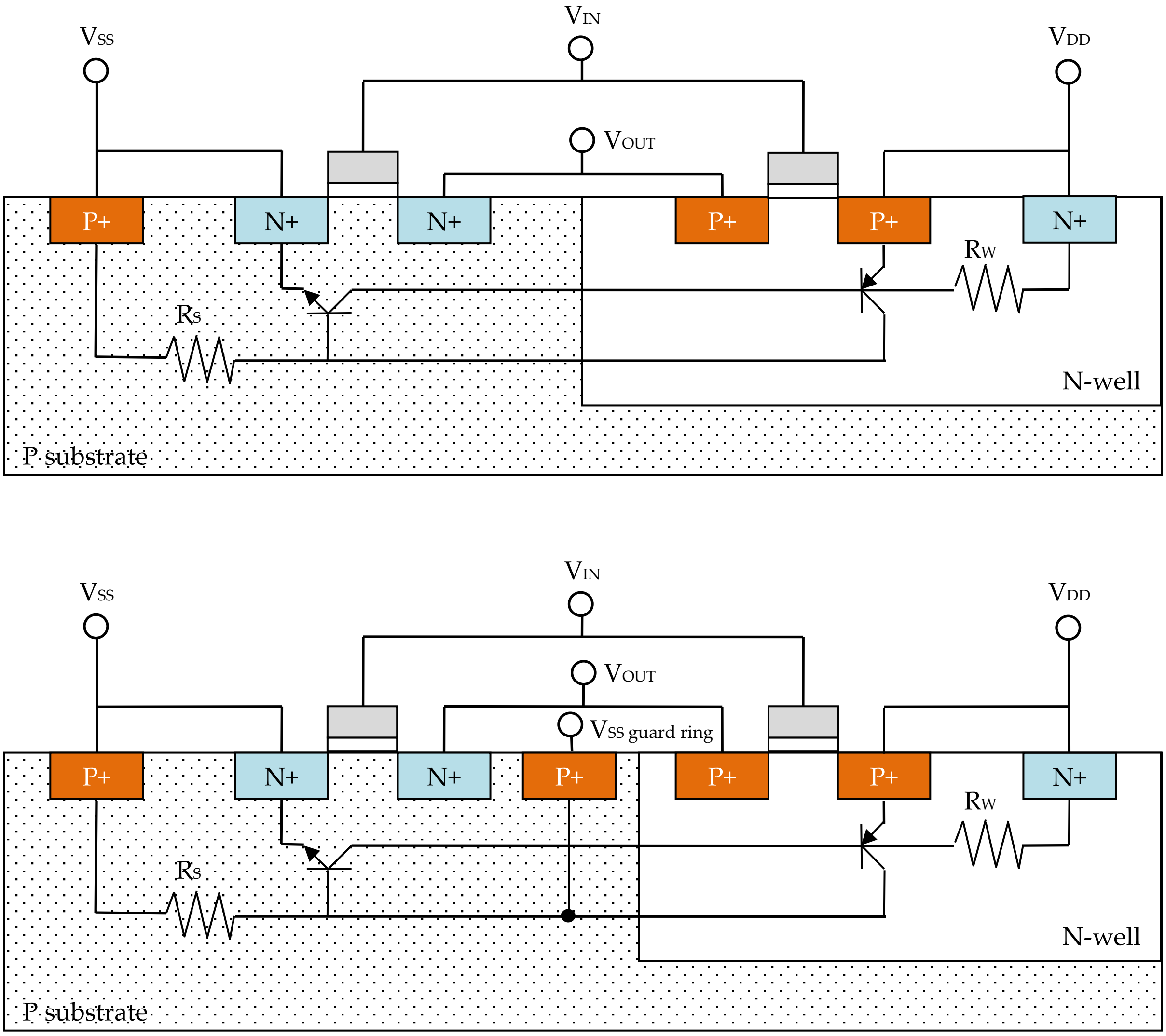


Figure 7-4: Parasitic thyristor responsible for SEL (top), introduction of P+ guard ring around NMOS transistor (bottom)

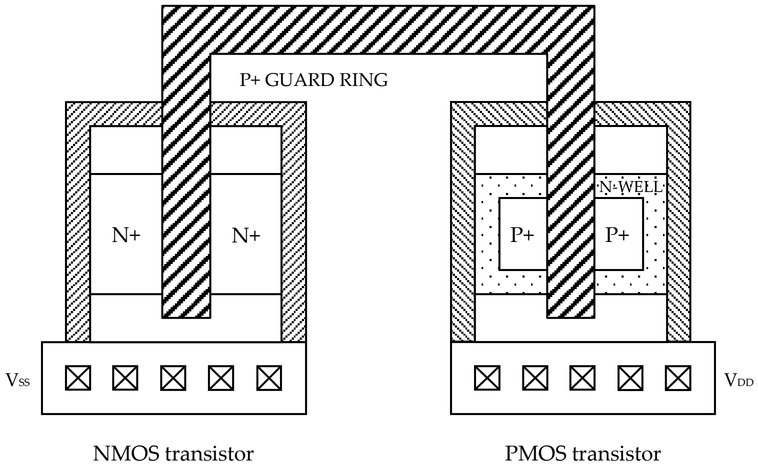


Figure 7-5: CMOS transistors with guard rings

7.2.2.2 Available test data (simulations, radiation testing, in-flight)

Reference [72] discusses design issues related to the extensive use of Enclosed Layout Transistors (ELT's) and guard rings in deep submicron CMOS technologies.

Reference [77] proposes an analysis of the latch-up phenomena with the use of guard ring structures in bulk CMOS substrate. Several structures are analyzed by simulation with and without guard rings.

7.2.2.3 Added value (efficiency)

Reference [78] 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 [79] 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 [80] are compared guard ring efficiencies between epitaxial silicon and bulk silicon for sub-quarter micron technology.

7.2.2.4 Known issues (weaknesses, elements to be considered)

The cost in cell area for the inclusion of guard rings is typically 10 % - 15 % [78].

The brief summary of key characteristics for contacts and guard rings is given in the Table 7-3.

Table 7-3: Summary of key characteristics for contacts and guard rings

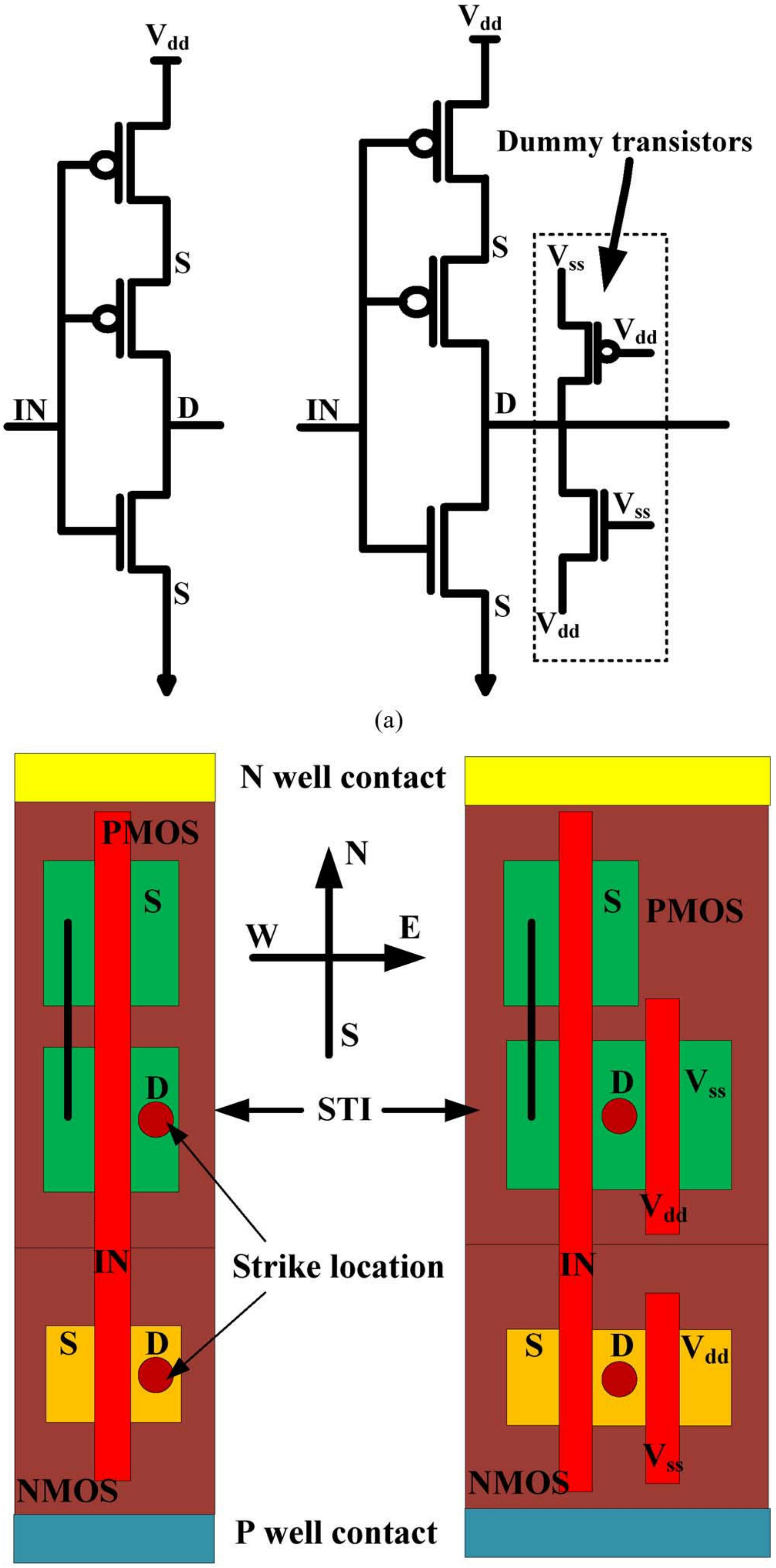
Abstraction level	Physical layout
Pros	SEL robustness up to LET > 90 MeV*cm^2/mg
Cons	Area overhead: 10-15%
Mitigated effects	SEL, MBU/MCU
Suitable validation methods	Radiation ground testing
Automation tools	

7.2.3 Dummy transistors

7.2.3.1 Description of the concept

In common two-transistor (2T) inverters, experiments have shown that maximum SETs occur when an ion strikes a PMOS but not an NMOS [287] transistor. This is because charge collection is enhanced by the well-known bipolar effect that is found in PMOS but not in NMOS devices that involve aP substrate twin-well process [291], [292]. In order to reduce the large SET, a three-transistor (3T) inverter can be used. As shown on the left in Figure 7-6:(b), in a 3T inverter layout, the bipolar effect is mitigated substantially due to the source region being isolated via Shallow trench isolation (STI) in the PMOS region, so leading to the effective reduction of a P-hit SET [288], [289], [290].

Based on this 3T inverter approach, [286] proposes a novel RHBD technique to produce additional SET mitigation. The technique calls for the addition of an off-state idle PMOS and a NMOS transistor to the circuit, connected to the drain, as shown on the right in Figure 7-6. The source of the added PMOS transistor is connected to the ground supply voltage (Vss), while the gate is connected to the power supply voltage (Vdd). Meanwhile, the source of the additional NMOS transistor is connected to Vdd, and its gate is connected to Vss. Therefore, the addition of these transistors has no net effect on the circuit function and appears to have negligible influence in the light of the circuit-level hardened design. However, in the layout design, the additional guard electrodes are cleverly positioned close to the drain in the layout, so that they can efficiently collect any ion-induced charges and thus help to reduce charges collected by the drain, leading to a decrease in WSET. In the “guard drain” technique, despite the fact that the added guard electrodes enclose the drain, they are isolated via STI, so that any ion-induced charges have to pass over a trench before they can be collected by the guard electrode. By contrast, in our proposed layout technique, the guard electrode and the drain are located in the same active area and are very close to each other, with the consequence that ion-induced charges can diffuse directly towards the guard electrode and be readily collected. This results in an enhanced hardening benefit in the proposed layout technique for SET mitigation, so that it can be regarded as an improvement over the “guard drain” layout technique.



(a)

(b)

Figure 7-6: RHBD technique using dummy transistors. (a) The circuits, (b) the layouts (layout1 on the left, layout2 on the right), after J. Chen [286].

The brief summary of key characteristics for dummy transistors is given in the Table 7-4.

Table 7-4: Summary of key characteristics for dummy transistors

Abstraction level	Physical layout
Pros	Lower SET sensitivity
Cons	Additional area
Mitigated effects	SET
Suitable validation methods	Radiation ground testing
Automation tools	

7.2.4 Transistors Gate W/L ratio sizing

7.2.4.1 Description of the concept

[283] presents an experimental study of a gate-level radiation hardening technique for cost-effective reduction of the soft error failure rate in combinational logic circuits. The key idea is to exploit the asymmetric logical masking probabilities of gates, hardening gates that have the lowest logical masking probability to achieve cost-effective trade-offs between overhead and soft error failure rate reduction. The asymmetry in the logical masking probabilities at a gate is leveraged by decoupling the physical from the logical (Boolean) aspects of soft error susceptibility of the gate.

7.2.4.2 Available test data (simulations, radiation testing, in-flight)

In [283] a full set of experimental results for process technologies ranging from 180 nm to 70 nm demonstrates the cost-effective trade-offs that can be achieved. On average, the proposed technique has a radiation hardening overhead of 38,3 %, 27,1% and 3,8 % in area, power, and delay for worst case SEUs across the four process technologies studied.

7.2.4.3 Known issues (weaknesses, elements to be considered)

The brief summary of key characteristics for large W/L ratio transistors is given in the Table 7-5.

Table 7-5: Summary of key characteristics for large W/L ration transistors

Abstraction level	Physical layout
Pros	Reduced sensitivity to leakage and Vth shift
Cons	Area, power and delay overheads
Mitigated effects	TID
Suitable validation methods	Radiation ground testing
Automation tools	

8 Analogue circuits

8.1 Overview

In mixed-signal (analogue combined with digital circuits) 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. Unfortunately, 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 a 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 [93]
- Reducing the amount of collected charge (Q_{col}) at a metallurgical junction [93]

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) [106], [107]
- Increasing the drive currents [93]
- Increasing the supply voltage [93]
- Increasing capacitor sizes [93]

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 [94], [95], drains [96], or diodes [97] around MOS devices. Similarly, the use of n-rings [98], substrate-tap rings [99], and nested minority-carrier guard rings [100] can be utilized in bipolar structures such as in SiGe HBT technology [13].
- Substrate engineering (e.g., use of charge blocking layers in the substrate – shown in [101] for a SiGe HBT technology).
- Use of very thin silicon layer like the one found on silicon-on-insulator (SOI) wafers [93].
- Addition of dummy collector for charge collection in HBT devices [102].
- Use of increased substrate and well contacts (reduced substrate and well impedances),[103], [104], [105].

Those techniques are however explained in more detail in Section 6 (Process level mitigation) and Section 7 (Layout level mitigation).

The remainder of this Section outlines various design-level mitigation techniques employed through modifications in the full custom layouts of the basic cells and/or the architecture of analogue circuits.

As a last general remark, some analogue designs (e.g. rad hard PLLs can be replaced by entirely digital and functionally equivalent designs (e.g. Digital PLL [[113], All-digital PLL [294]), and then the radiation effects are mitigated by the techniques described in Section 9 (Digital design mitigation).

A summary of mitigation techniques and the radiation effects they address is given in the Table 8-1.

Table 8-1: Summary of mitigation techniques at analogue design circuit architecture level and the radiation effects they address

Mitigation techniques		Radiation effects	
		SET	SEU
8.2.1	Node Separation and Inter-digitation	X	X
8.2.2	Analogue redundancy (averaging)	X	
8.2.3	Resistive decoupling	X	X
8.2.4	Filtering	X	X
8.2.5	Modifications in bandwidth, gain, operating speed, and current drive	X	
8.2.6	Reduction of window of vulnerability	X	X
8.2.7	Reduction of high impedance nodes	X	
8.2.8	Differential design	X	X
8.2.9	Dual path hardening	X	

8.2 Mitigation techniques

8.2.1 Node Separation and Inter-digitation

8.2.1.1 Description of the concept

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 [108]), the charge collected due to diffusion at an adjacent node can be significant. Figure 8-1 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 [109].

One solution for mitigating the amount of charge “shared” between adjacent nodes is nodal separation [96], [102], [109].

Interdigitation, or interleaved layout, is a technique that takes advantage of the benefits of nodal separation while maintaining device density limitations. 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 [102], [110].

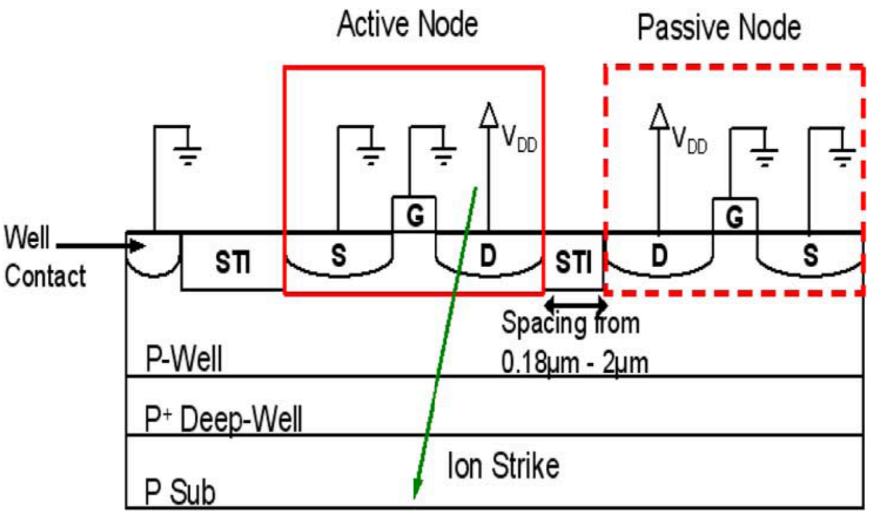


Figure 8-1: Cross-section of two adjacent NMOS devices in a bulk CMOS technology (From [109])

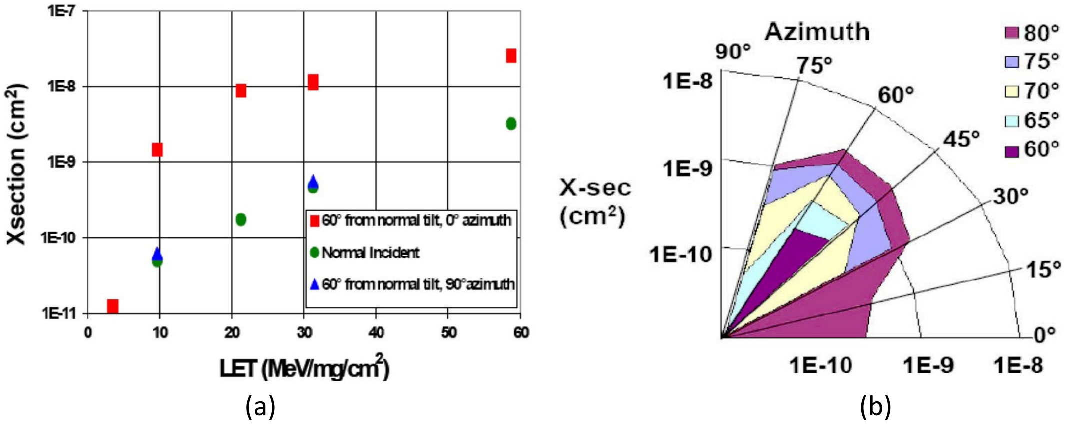


Figure 8-2: (a) Upset sensitivity data for basic DICE topology implemented in 90 nm CMOS at three angles of incidence [114] and (b) measured upset cross-sections as a function of azimuth angle for the Kr ion (LET of approximately 30 MeV*cm²/mg) in improved DICE implementing nodal spacing [114]

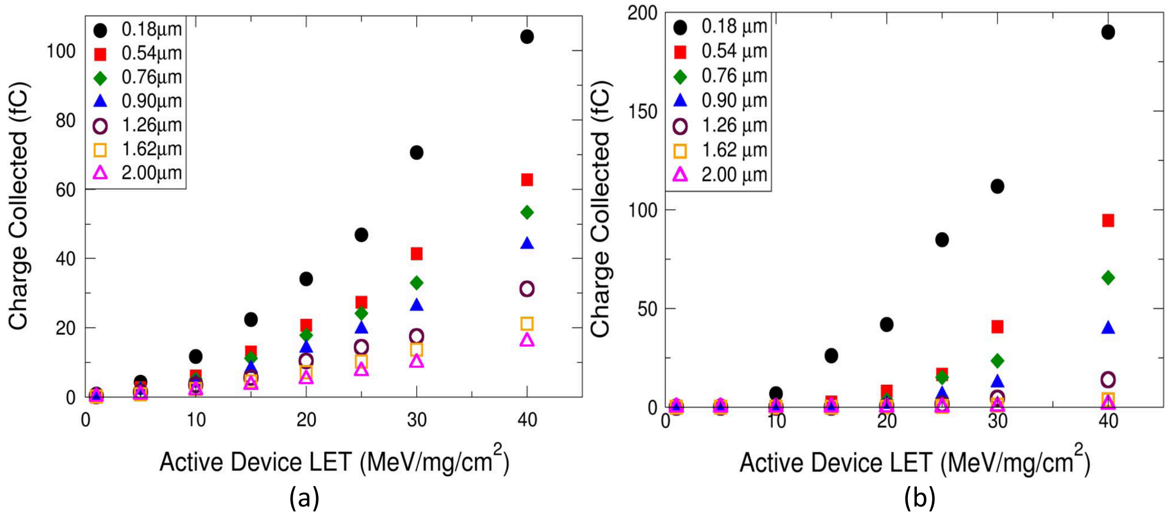


Figure 8-3: Charge collected on an adjacent transistor for a) PMOS and, b) transistors as a function of the distance separating them ([112])

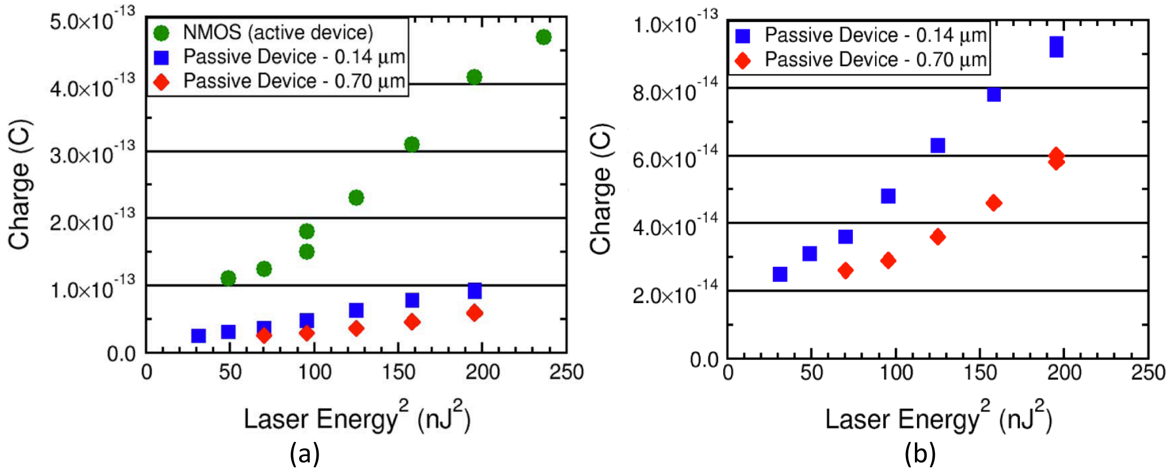


Figure 8-4: (a) Comparison of collected charge for the active and passive NMOS devices following laser-induced charge deposition at the active device. (b) Collected charge for passive NMOS devices verifies the charge sharing effect and shows a nodal spacing dependence for the passive device charge collection ([95])

The angular dependence of single event upset in dual-interlocked memory cells (DICE) has been rigorously investigated[110], [111]. The DICE cell is immune to all single-node charge collection [2]. 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 8-2(a) shows the upset cross-sections for one version of a DICE latch implemented in a 90 nm bulk CMOS technology [111]. The figure illustrates the strong directional dependence on the upset cross-sections. Figure 8-2(b) illustrates the measured cross-sections at an LET of approximately 30 MeV*cm^2/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 8-2(a)) to approximately 2e-10 cm^2 at an azimuth angle of 0° (Figure 8-2(b)).

8.2.1.2 Available test data (simulations, radiation testing, flown)

Figure 8-3 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 ([109]). 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 8-4 ([95]). 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 8-4(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).

8.2.1.3 Added value (efficiency)

- Node separation reduces charge collection between adjacent transistors

8.2.1.4 Known issues (weaknesses, elements to be considered)

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

The brief summary of key characteristics for node separation and interdigitation is given in the Table 8-2.

Table 8-2: Summary of key characteristics for node separation and inter-digitation

Abstraction level	Physical Layout
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

8.2.2 Analogue redundancy (averaging)

8.2.2.1 Description of the concept

Analogue averaging is a form of hardware redundancy for the reduction of spurious transients. The averaging of an analogue 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 8-5. A perturbation (ΔV) due to a particle strike on any one copy of the circuit is reduced to $\Delta V/N$.

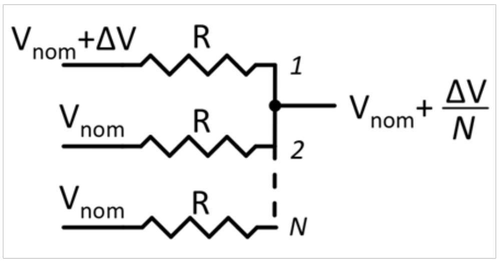


Figure 8-5: Analogue averaging through the use of *N* identical resistors. A perturbation (ΔV) due to a particle strike on any one copy of the circuit is reduced to $\Delta V/N$

This technique has been offered as a solution to the observed vulnerability of a charge pump for Phase-Locked Loops (PLL) [113] and implemented in the bias circuitry of Voltage-Controlled Oscillator (VCO) [114].

In reference [105], 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.

8.2.2.2 Available test data (simulations, radiation testing, flown)

Simulation results issued from reference [114] show that analogue averaging applied on the input stage of a VCO reduces the phase displacement in the output of the VCO by 35 %.

8.2.2.3 Added value (efficiency)

- Predictable decrease in SET magnitude as a function of redundancy

8.2.2.4 Known issues (weaknesses, elements to be considered)

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

The brief summary of key characteristics for analogue redundancy is given in the Table 8-3.

Table 8-3: Summary of key characteristics for analogue redundancy

Abstraction level	Circuit architecture
Pros	Attenuation of SETs
Cons	Noise and area increase
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests

8.2.3 Resistive decoupling

8.2.3.1 Description of the concept

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 9.1) of the inverter pairs [115], [116]. 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 that changes 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 [117]. A similar technique can 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.

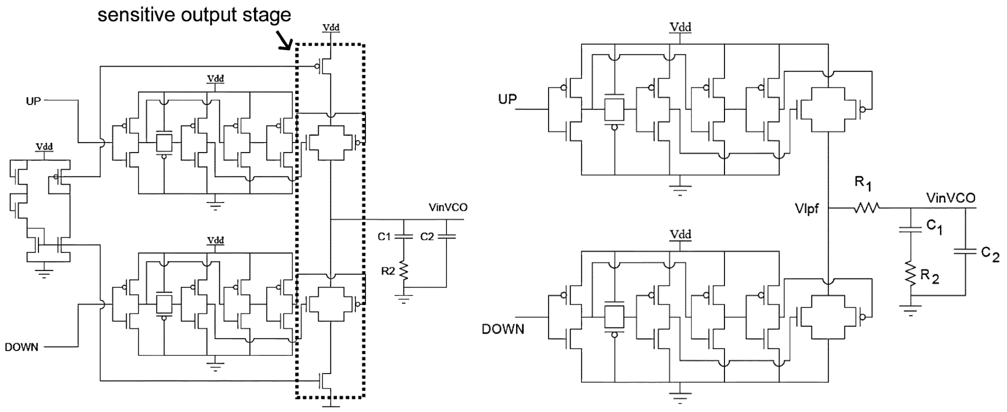
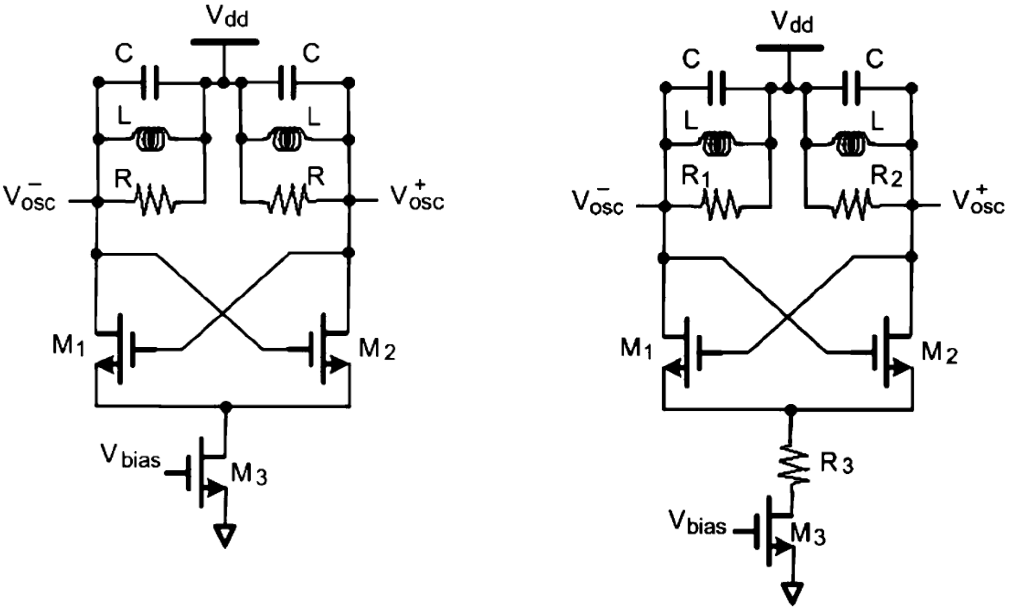


Figure 8-6: (a) A standard current-based charge pump configuration for phase-locked loop circuits. (b) Single-event hardened voltage-based charge pump configuration



(a)

(b)

Figure 8-7: (a) A standard LC Tank Voltage-Controlled Oscillator (VCO) and (b) Single-event hardened configuration utilizing decoupling resistor R_3 (From [118]).

Resistive decoupling was implemented in several studies such as the one presented in references [119] and [120] 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 8-6, the number of sensitive nodes present in the output stage of the charge pump (Figure 8-6(a)) can be reduced and subsequently decoupled from the VCO control voltage (Figure 8-6(b)).

The technique has also been used to mitigate transients in an LC Tank Oscillator [118]. Figure 8-7(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 8-7(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 [118]. Vulnerabilities of the differential pair are discussed in further detail in section 8.2.7.

8.2.3.2 Available test data (simulations, radiation testing, flown)

- Reference [119] 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 [120] presents experimental results issued from radiation experiments performed on two Phase-Locked Loop (PLL) circuits designed in 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 [118] presents simulation and experimental transient results for the standard and hardened LC Tank Oscillators shown in Figure 8-7 and designed in a 90 nm CMOS technology. The threshold energy of the hardened oscillator, defined as the minimum laser energy that induces a phase shift of at least 10 degrees in the oscillator output, was shown to be approximately 5 times that of the unhardened design.

8.2.3.3 Added value (efficiency)

- The inclusion of the decoupling resistor has the added benefit of RC filtering (see 8.2.4) 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.

8.2.3.4 Known issues (weaknesses, elements to be considered)

Some area penalty is 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. It is important to take care in the determination of 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 [119]. However, if the designer wishes to further decrease this fluctuation, an area trade-off is encountered.

The brief summary of key characteristics for resistive decoupling is given in the Table 8-4.

Table 8-4:Summary of key characteristics for resistive decoupling

Abstraction level	Circuit architecture
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

8.2.4 Filtering

8.2.4.1 Description of the concept

Filtering is a common method for reducing the amplitude and duration of ASETs at design and system-levels. Low-pass or bandpass filters can be added to critical nodes in order to suppress fast ASETs, where the value of the filter depends on the circuit or system bandwidth [121].

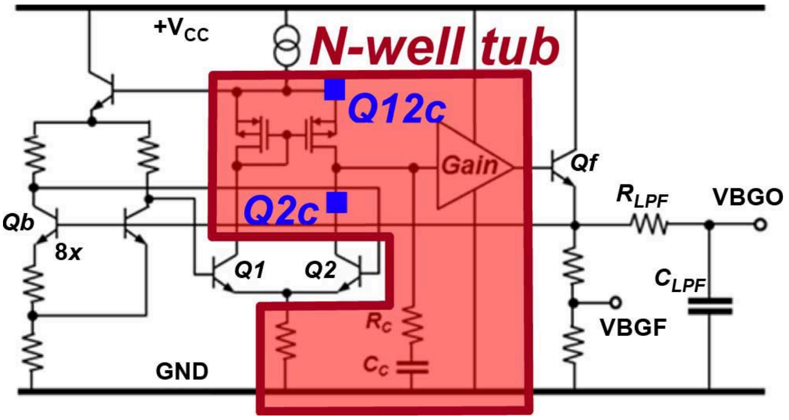


Figure 8-8: Brokaw bandgap reference circuit with an output low-pass filter for improved noise, isolation, and transient suppression (From[128]).

Reference [122] presents a computer-assisted system-level analysis to study the ASET response on an analogue 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 8-8 illustrates the bandgap reference circuit ([123]), 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 [119] and [93].

8.2.4.2 Available test data (simulations, radiation testing, flown)

Simulation and experimental results presented in reference[122] 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 two.

8.2.4.3 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 [119], [120].
- Hardening the bias nodes of a SerDes [124].
- 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.

8.2.4.4 Known issues (weaknesses, elements to be considered)

The work presented in reference [122] shows 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.

The brief summary of key characteristics for filtering is given in the Table 8-5.

Table 8-5: Summary of key characteristics for filtering

Abstraction level	Circuit architecture
Pros	SET filtering
Cons	Power consumption penalty Area penalty
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests

8.2.5 Modifications in bandwidth, gain, operating speed, and current drive

8.2.5.1 Description of the concept

Increasing the capacitance at nodes vulnerable to single-events can reduce the amplitudes of the resulting ASETs by increasing the amount of charge that induces a voltage perturbation. This is often used when the performance specifications are not adversely affected [122], [125]. The increase of nodal capacitance often alters characteristic parameters such as gain and bandwidth. This section discusses 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 analogue topologies that can be expressed as closed-loop amplifier structures and has been shown applicable in various studies on Operational Amplifiers (OAs) ([93], [121] and [125]) and Phase-Locked Loops (PLLs) ([126], [127]) both of which can be represented as a closed-loop amplifier. However, works presented in references [120] and [125] 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 can increase as modifications are placed to decrease the amplitude. Therefore, specific consequences regarding the size of the resistors, compensation capacitors, and stage gains can occur and require special attention. In general, as seen in reference [125] and [127] regarding respectively PLLs and OAs, it appears that maximizing speed and minimizing the open- and closed-loop gains can improve the ASET response.

Operating speed plays a curious role in determining the SET response of analogue circuits. As previously mentioned, analogue circuits have been shown to exhibit reduced ASET vulnerability for increased operating frequency [125], [127]. This is contrary to that typically observed in digital systems, where increasing error cross-sections as a result of SETs induced in combinatorial logic have been observed for increasing operating frequency [128]. 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 analogue 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 [122]. The improved performance can or cannot 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 [127] 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 important to maximize the operating frequency within the designed bandwidth (consistent with that shown in [125] 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) can amplify transients in the PLL resulting from ionizing radiation. Therefore it is important to reduce the frequency of the PLL in order to improve the SET response. The authors go on to provide an analytical expression for determining an upper bound for reasonable radiation performance. Moreover, it is shown in [126] 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 8-9 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). It is important to carefully consider trade-offs in operating speed, jitter, settling time, bandwidth, and SET performance.

Through the efforts depicted in reference[129] 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.

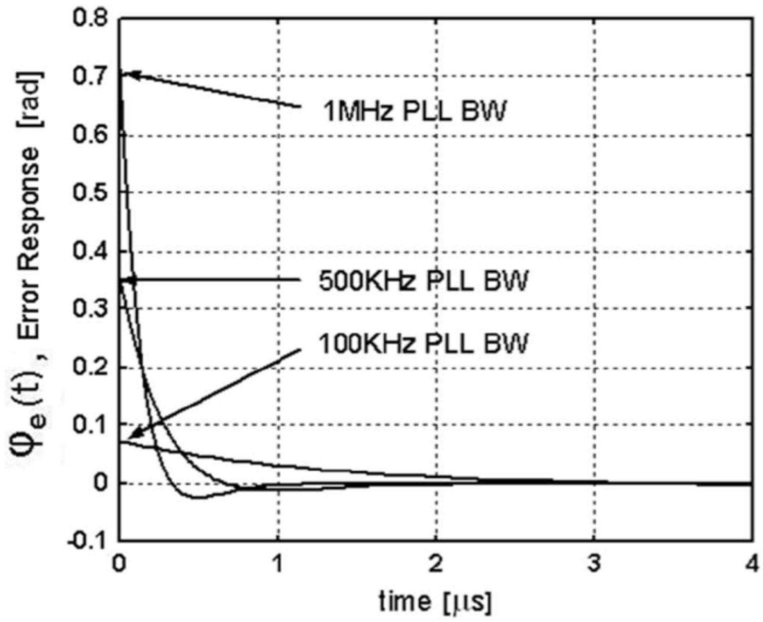


Figure 8-9: Transient PLL error response as a function of PLL bandwidth

Reference [127] 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.

8.2.5.2 Available test data (simulations, radiation testing, flown)

Simulation and experimental results using a laser beam on a LM124 OA are presented in reference [127]. 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 reduces the amplitude but increases the duration. Therefore, the sensitivity can increase or decrease depending on the criteria defined for the application. The gain stage increases 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 can be selected which minimizes 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 has 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.

8.2.5.3 Added value (efficiency)

Observations from [125] -[129] 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 can improve the ASET response.
- Operating speed and drive strength are closely coupled. Operating circuits faster can in some cases reduce the SET vulnerability due to increased operating currents.

8.2.5.4 Known issues (weaknesses, elements to be considered)

- It is often difficult to decouple the effects of speed and drive strength on the SET vulnerability.

The brief summary of key characteristics for bandwidth, gain, operating speed, and current drive is given in the Table 8-6.

Table 8-6: Summary of key characteristics for modifications in bandwidth, gain, operating speed and current drive

Abstraction level	Circuit architecture
Pros	Improved SET tolerance
Cons	Gain, bandwidth, speed, and drive strength are often dependent parameters and can be difficult to decouple
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests

8.2.6 Reduction of window of vulnerability

8.2.6.1 Description of the concept

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 analogue/mixed-signal (A/MS) circuits when signal clocking is used or in cases where steady-state AC signals are present. Figure 8-10 illustrates the number of vulnerable nodes and the type of vulnerable sub-circuit in a 2-bit flash analogue- to-digital converter (ADC) over one conversion cycle (from [130]). 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 8-11 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 [131]).

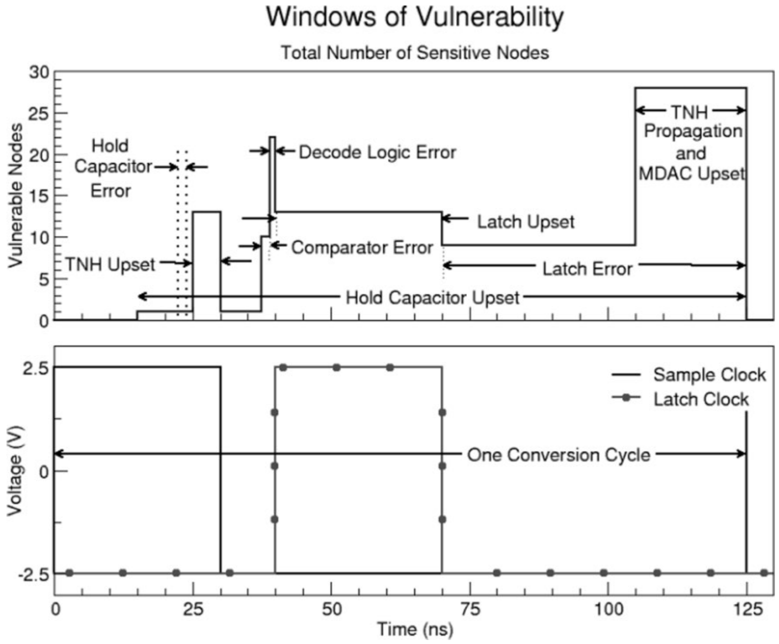


Figure 8-10: Simulated windows of vulnerability over one data conversion cycle in a 2-bit flash ADC (From [130]).

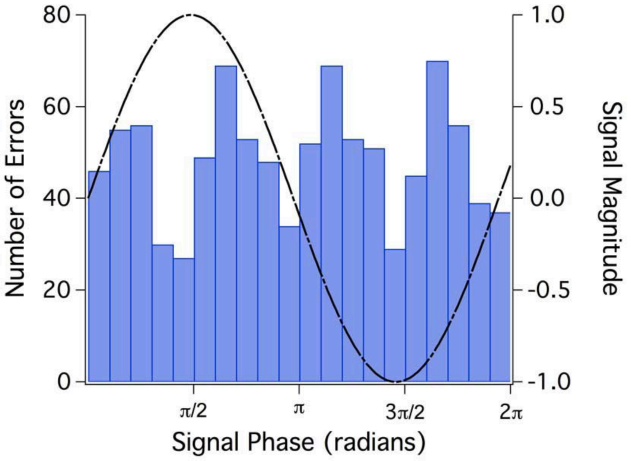


Figure 8-11: The number of errors with respect to cycle time following laser-induced charge deposition in a phase-locked loop (From [131]).

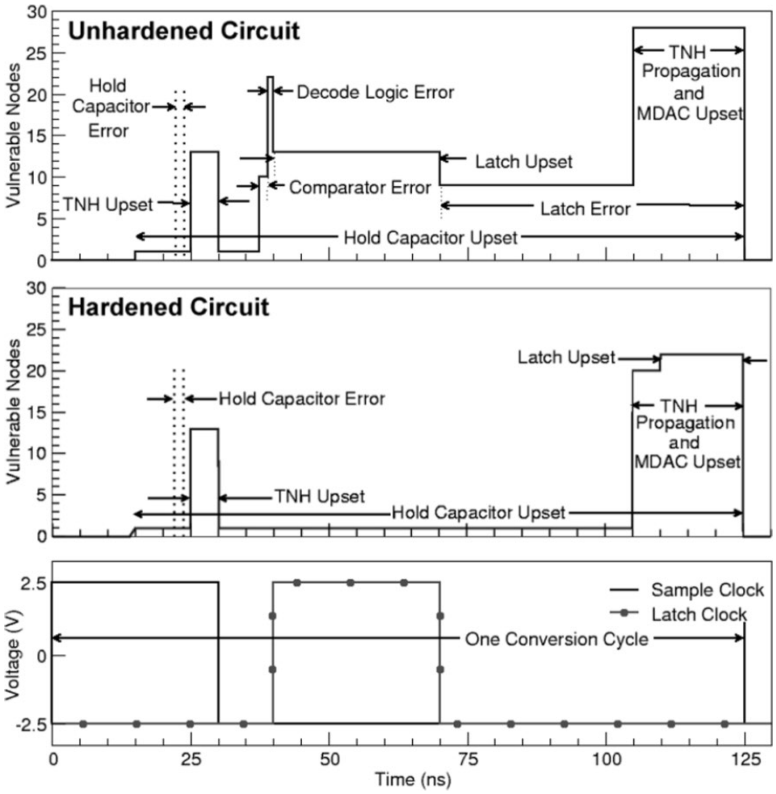


Figure 8-12: Simulated windows of vulnerability over one data conversion cycle for un-hardened and hardened 2-bit flash ADCs (From [132])

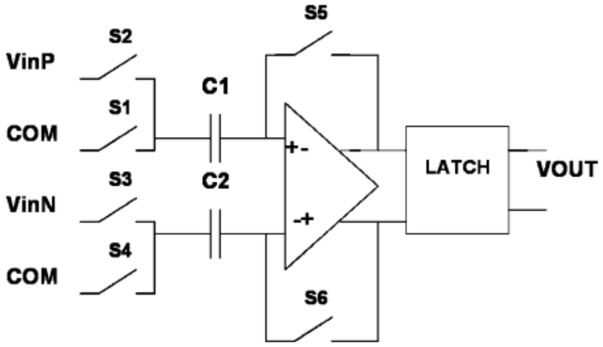


Figure 8-13: Simplified view of the auto-zeroed comparator (From [134])

The results from Figure 8-10 were utilized to apply targeted mitigation techniques to the vulnerable sub-circuits in the 2-bit flash ADC in [130]. The mitigation was achieved by implementing hardened latches and SET filtering. No analogue components were hardened. The results from the hardening are displayed in Figure 8-12 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 8-13 illustrates the auto-zeroed comparator presented in reference [132]. 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 errors are 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 are 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 [132].

8.2.6.2 Available test data (simulations, radiation testing, flown)

The window of vulnerability of a 2-bit flash ADC was investigated through simulations in [132]. 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 [131]. 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 can help identify the mechanisms responsible for the vulnerability.

The WOV concept was applied to harden a comparator in [132]. 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 remains 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.

8.2.6.3 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 [131].

8.2.6.4 Known issues (weaknesses, elements to be considered)

- WOV and PDS analysis, whilst elucidating information in regard to the circuit vulnerability, does not directly result in an identification of vulnerable location. Additional analysis is therefore undertaken 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 involve an 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 in some designs (e. g. an operational amplifier in an analogue filter or a comparator in an asynchronous circuit).

The brief summary of key characteristics for reduction of window of vulnerability is given in the Table 8-7.

Table 8-7: Summary of key characteristics for reduction of window of vulnerability

Abstraction level	Circuit architecture
Pros	Reduces SET duration
Cons	Area penalty: clocking circuitry
Mitigated effects	SET
Suitable validation methods	Simulations Accelerated ground tests

8.2.7 Reduction of high impedance nodes

8.2.7.1 Description of the concept

The aforementioned circuit-level mitigation approaches are based on the modification of characteristic circuit parameters such as gain, bandwidth, frequency, and drive strength. It is important for each technique applied to asses any compromises in performance through a trade-off analysis (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[133], [97], [119], [120], [134]. This has shown applicable at the design-level [119], [120], [134], and at layout-level [97].

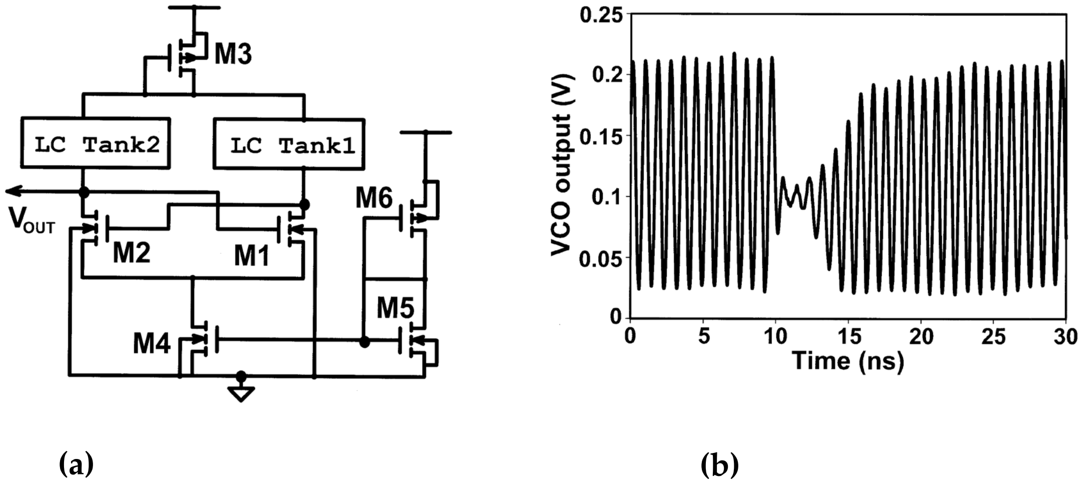


Figure 8-14: (a) Simplified schematic of a typical LC Tank VCO and (b) an experimentally observed transient resulting from laser-induced charge injection on transistor M1 (From [135])

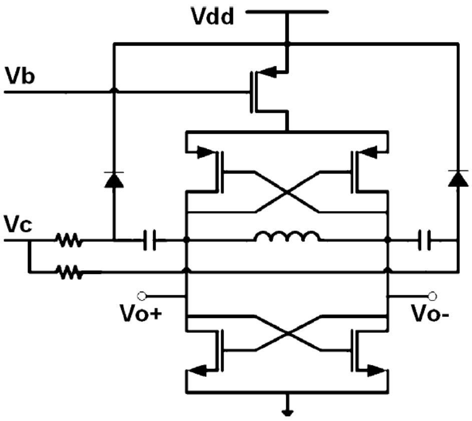


Figure 8-15: Schematic of RHBD CMOS LC Tank VCO (From [134])

Some examples:

- Figure 8-14 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[135]). 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 8-15 (From [134]), 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 [134].
- Reference [136] 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 [136], [137], [114], [113], [120].
- In contrast, reference [97] 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.

8.2.7.2 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 [134]. 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*cm^2/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 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.
- The 5,2 GHz Injection-Locked Oscillator [136] 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.

8.2.7.3 Added value (efficiency)

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

8.2.7.4 Known issues (weaknesses, elements to be considered)

- Reducing or eliminating high impedance nodes can involve the addition of circuit elements and is thus subject to area and power penalties.

The brief summary of key characteristics for reduction of high impedance nodes is given in the Table 8-8.

Table 8-8: Summary of known issue for reduction of high impedance nodes

Abstraction level	Circuit architecture/Physical layout
Pros	Improved SET recovery time
Cons	Requires additional circuit elements: area and power penalty
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests

8.2.8 Differential design

8.2.8.1 Description of the concept

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 can be designed to interact as to truncate a propagated voltage transient (pulse quenching)[138]. Pulse quenching, graphically illustrated in Figure 8-16 (From [138]) has been identified as a factor in the analysis and measurement of digital SETs, and can 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 8-17 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, results in a transient in the output voltage.

Hypothesized in [100] and shown for the first time through simulations in [139] and experiments in [140], 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).

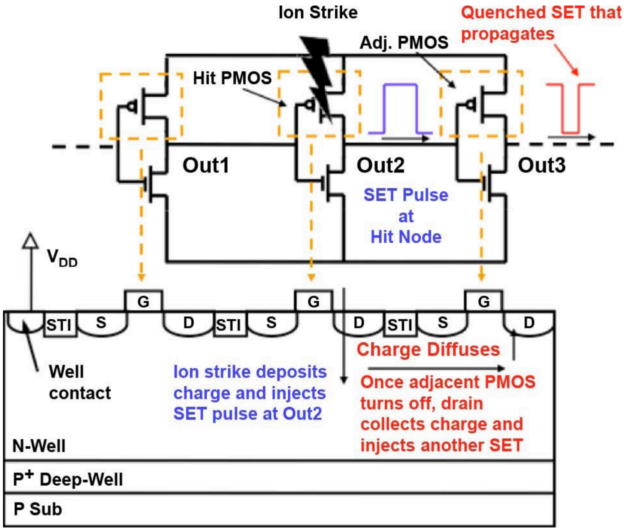

Ion Strike
Quenched SET that propagates
Adj. PMOS
Hit PMOS
Out1
Out2
Out3
SET Pulse at Hit Node
V_{DD}
G
G
G
STI
S
D
STI
S
D
STI
S
D
Charge Diffuses
Well contact
Ion strike deposits charge and injects SET pulse at Out2
Once adjacent PMOS turns off, drain collects charge and injects another SET
N-Well
P^+ Deep-Well
P Sub

Figure 8-16: 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 [142]).

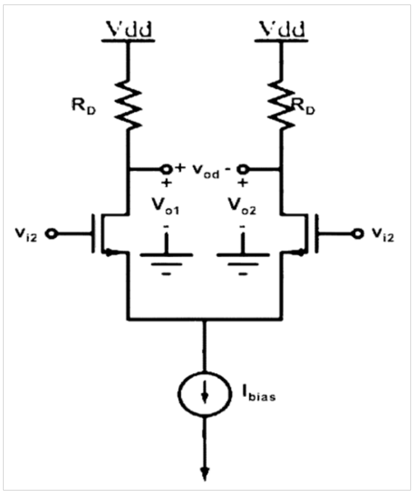


Figure 8-17: Basic differential pair

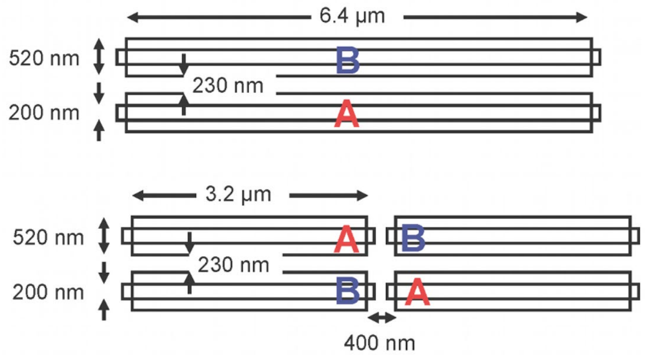


Figure 8-18: Differential pair including devices A and B before and after DCC layout for maximizing charge sharing (From [143])

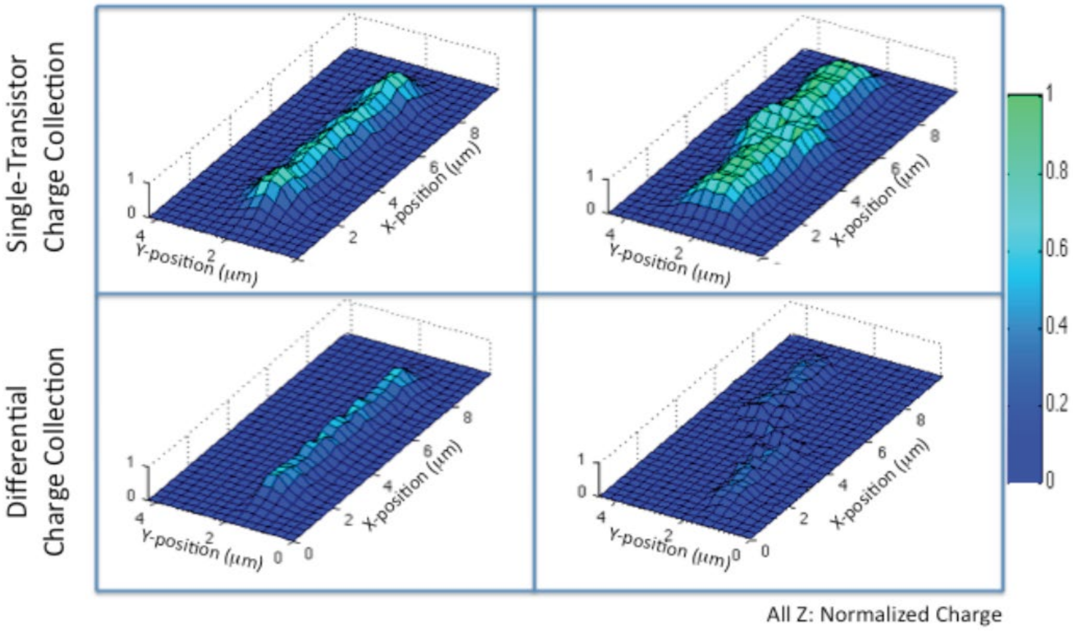


Figure 8-19: Charge collected by a single transistor for single (left) and parallel (right) transistor configuration, is shown in the top row. Differential charge is shown in the bottom row for single (left) and parallel (right) transistor configuration (From [143])

Figure 8-18 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 are arranged in a common well with drains located as close as possible to promote common-mode charge rejection. Figure 8-19 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 8-18). 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 [140]).

8.2.8.2 Available test data (simulations, radiation testing, flown)

Reference [140] 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 greatly reduces 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 cannot normally be employed, but the overall charge sharing, and therefore single-event mitigation, is dramatically enhanced.

8.2.8.3 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

8.2.8.4 Known issues (weaknesses, elements to be considered)

- Increased wiring complexity

The brief summary of key characteristics for differential design is given in the Table 8-9**.**

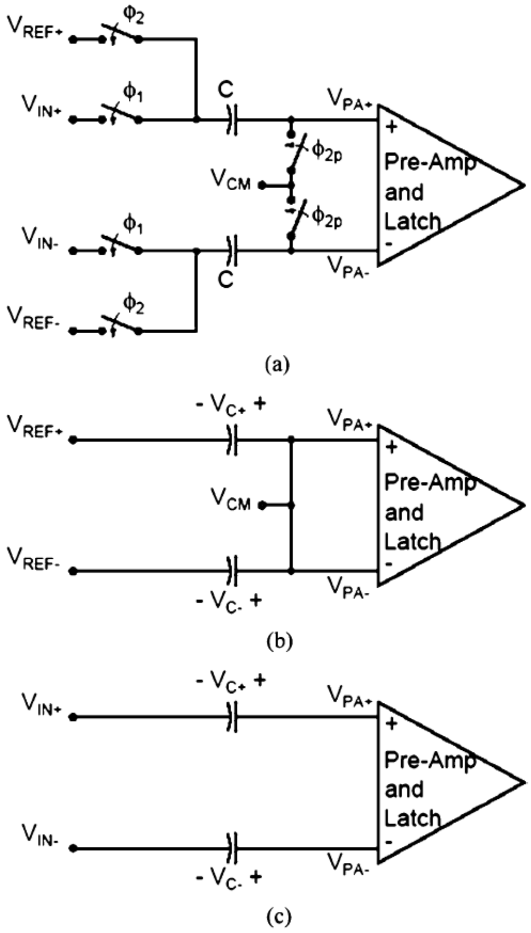
Table 8-9: Summary of key characteristics for differential design

Abstraction level	Circuit architecture/Physical layout
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

8.2.9 Dual path hardening

8.2.9.1 Description of the concept

Differential circuits are common for most analogue 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 analogue and mixed-signal circuits is dual path hardening (local feedback mitigation) [141]. 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 [141] and [142], respectively.



(a)

(b)

(c)

Figure 8-20: (a) The switched-capacitor comparator operates in two phases: (b) reset phase and (c) evaluation phase (From [142])

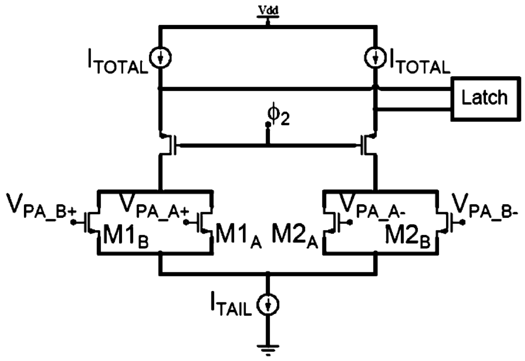


Figure 8-21: Simplified circuit schematic of the differential amplifier showing the split input paths (From [142])

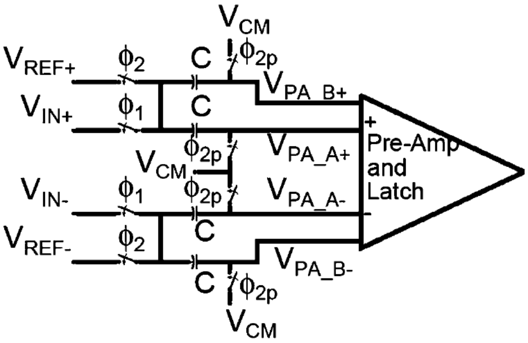


Figure 8-22: The switched-capacitor comparator with split differential amplifier input paths to harden the floating nodes against single-event upsets (From [142])

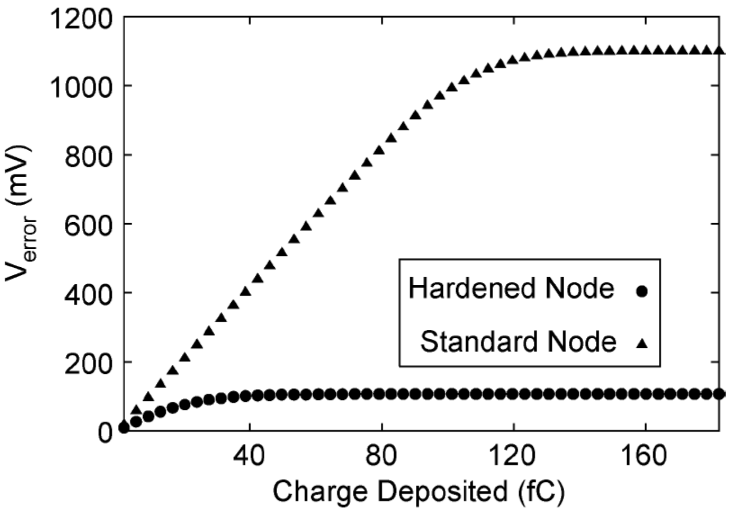


Figure 8-23: Simulated output error voltage versus deposited charge of a sample and hold amplifier with and without dual path hardening (From [141])

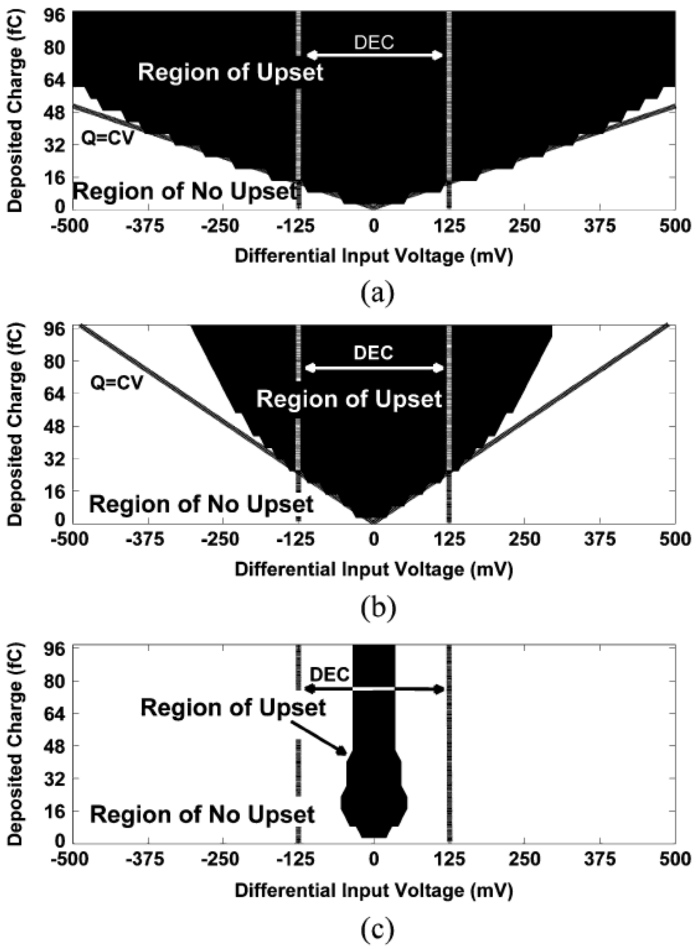


Figure 8-24: Simulated deposited charge required to generate a SEU at the output of the comparator for various differential input voltages for the (a) unhardened design, (b) the design with increased capacitors (2x), and (c) the design implementing dual path hardening (From [142])

Figure 8-20 illustrates a standard switched-capacitor comparator design as commonly used in pipelined analogue- to-digital converters [142]. 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 can 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 8-21 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 8-22.

8.2.9.2 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 [141]. As seen in Figure 8-23 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 [141].

Additionally, simulation results indicate significant improvement in single-event performance for switched capacitor comparators implementing dual path hardening [142]. For the design depicted in Figure 8-21 and Figure 8-22, the output perturbation was reduced to values correctable by standard digital error correction. As seen in Figure 8-24, 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[142].

8.2.9.3 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 can be halved.
- Device matching, frequency response, and noise performance are unaffected.

8.2.9.4 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 dimensions were already at minimum dimension and cannot be halved. Depending on the application, it can be possible to halve the sizes of the capacitors when splitting the input paths, while still maintaining acceptable matching and noise performance [142].
- There is an increase in wiring complexity with dual path hardening due to the extra elements required for the split data paths.

The brief summary of key characteristics for dual path hardening is given in the Table 8-10.

Table 8-10: Summary of key characteristics for dual path hardening

Abstraction level	Circuit architecture/Physical layout
Pros	Improved SET tolerance Identical frequency response as unhardened counterpart Equivalent noise performance
Cons	Area penalty possible (can be negligible in certain designs) Increased wiring complexity
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests

9
Embedded memories

9.1 Overview

Memory cells (e.g. SRAM cells, latches, flip-flops) are sensitive to the effects of radiation, mainly SEUs. Because most digital designs include a huge number of memory cells organised in arrays that form "memory blocks", mitigation strategies based on spatial redundancy are often not adequate as they cannot fit the IC area and power requirements. Alternative solutions present in the state-of-the-art can be classified in several categories. Some techniques pursue to harden the individual bit storage cells while others aim to prevent or restore bit errors appearing in arrays of memory cells and the data groups (e.g. "words") stored inside.

All the 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 can find the optimal solution by combining several of these techniques.

Table 9-10 is provided at the end of this Section to compare the different types of rad hard by design memory cells.

A summary of effects versus mitigation techniques is given in Table 9-1.

Table 9-1: Summary of mitigation techniques for embedded memories and the radiation effects they address

Mitigation techniques		Radiation effects	
		SEU	MBU(*)
9.2.1	Hardening of individual memory cells	X	
9.2.1.2	Resistive hardening	X	
9.2.1.3	Capacitive hardening	X	
9.2.1.4	IBM hardened memory cell	X	
9.2.1.5	HIT hardened memory cell	X	
9.2.1.6	DICE hardened memory cell	X	
9.2.1.7	NASA-Whitaker hardened memory cell	X	
9.2.1.8	NASA-Liu hardened memory cell	X	
9.2.2	Bit-interleaving in memory arrays		X
9.2.3	Data scrubbing	X	X
(*) all SEU mitigation techniques help to reduce MBUs, but in this table we reserve the X in the MBU box for those techniques which are specifically addressing multiple bit upsets			

9.2 Mitigation techniques

9.2.1 Hardening of individual memory cells

9.2.1.1 Overview

This category proposes fault mitigation by modifying the bit *storage 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 can 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.

Registers and flip-flops designs not only contain basic storage cells but also additional functions to control the saving, reset and output of the information stored in them. Mitigating the multiple radiation effects that can occur in these circuits can involve the application of additional mitigation techniques at other levels, as explained in the sections 8 and 11.

9.2.1.2 Resistive hardening

9.2.1.2.1 Description of the concept

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 (see Figure 9-1) 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 [116]. 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 [169], [170]. High value resistors can be implemented at the cost of a low silicon area increase. Depending on the actual technology node being used, the additional area taken when applying this technique can be large (deep submicron) or relatively insignificant compared to the area of the active devices [170]. SEU tolerant memory cells protected by resistors were proposed for ASICs [171] and for FPGAs [172].

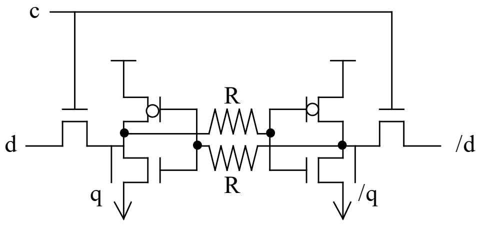


Figure 9-1:Resistor memory cell

9.2.1.2.2 Available test data (simulations, radiation testing, in-flight)

- Reference [171] presents theoretical and experimental results performed on an improved version of the presented resistor-based rad-hard memory cell in 9.2.1.2.1. 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 [173], resistor-based rad-hard memory cells were proven to be immune to particles having LETs of about 45 MeV*cm^2/mg.

9.2.1.2.3 Added value (efficiency)

An important advantage of this structure is the low area penalty of the cell (compared to other techniques) but only when used with *large* (> 0,5 µm) technology nodes.

9.2.1.2.4 Known issues (weaknesses, elements to be considered)

The main drawback of the resistive 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. Cell speed can also slow down at low T, due to the negative T coefficient of the poly-silicon used to make the resistors.

Another issue reported in reference [171] 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.

The brief summary of key characteristics for resistive hardening is given in the Table 9-2.

Table 9-2: Summary of key characteristics for resistive hardening

Abstraction level	Circuit architecture
Pros	High SEU robustness
Cons	Increased manufacturing cost, lower speed
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.3 Capacitive hardening

9.2.1.3.1 Description of the concept

Capacitor memory cells are based on the same principle, increasing the critical charge, as the one used for resistor memory cells described in 9.2.1.2.1. 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), DRAM-like stacked capacitors [174] or by adding metal-metal capacitances on top of the cells. As an example, the SRAM-C cell is depicted in Figure 9-2. These techniques allow reducing of the SER 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).

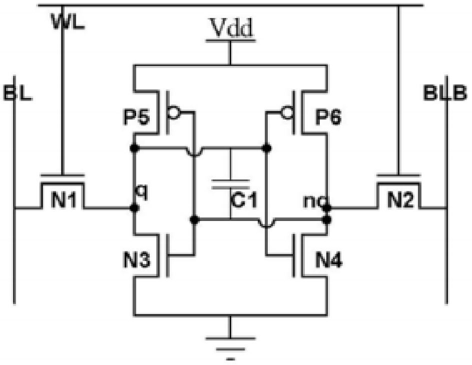


Figure 9-2: Hardened SRAM cell using a capacitor (SRAM-C cell)

Reference [175] proposes an optimized structure, called SRAM-tct, in order to reduce the write time penalty introduced by the SRAM-C cell. As shown in Figure 9-3, 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.

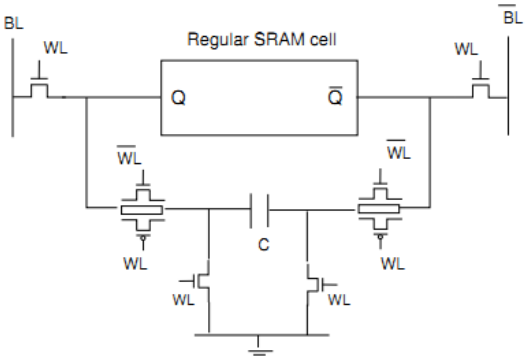


Figure 9-3: The SRAM-tct cell

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 testing 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 [176].

9.2.1.3.2 Available test data (simulations, radiation testing, in-flight)

Reference [175] 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%).

9.2.1.3.3 Added value (efficiency)

- Improved SEU robustness.

9.2.1.3.4 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 [175]).

The brief summary of key characteristics for the capacitive hardening is given in the Table 9-3.

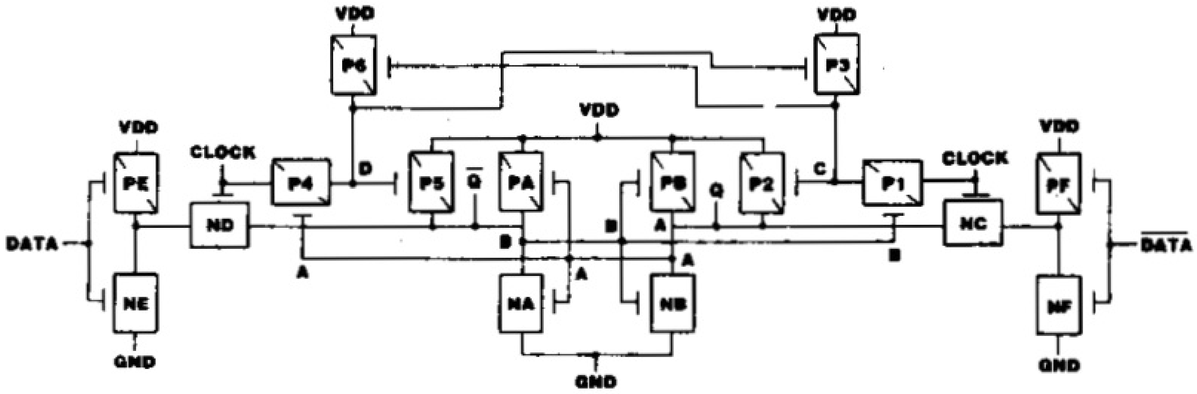
Table 9-3: Summary of key characteristics for capacitive hardening

Abstraction level	Circuit architecture
Pros	Improved SEU immunity
Cons	Speed penalty. Area penalty for SRAM-tct
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.4 IBM hardened memory cell

9.2.1.4.1 Description of the concept

IBM hardened memory cell is protected by an appropriate feedback devoted to restore the data when it is corrupted by the consequence of an energetic particle [177]. The cell, illustrated in Figure 9-4, 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).



N* - n-FETs in grounded p-substrate

P* - p-FETs in Vdd-biased n-well

Figure 9-4: IBM hardened memory cell (after original picture in [177])

9.2.1.4.2 Available test data (simulations, radiation testing, in-flight)

Reference [177] presents experimental results for a shift register implementing 144 design-hardened latches and also unhardened-latches. An SEU threshold of 25 MeV*cm^2/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.

9.2.1.4.3 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).

9.2.1.4.4 Known issues (weaknesses, elements to be considered)

- Area overhead: 100% (according to reference [178]).

The brief summary of key characteristics for IBM hardened memory cell is given in the Table 9-4.

Table 9-4: Summary of key characteristics for IBM hardened memory cell

Abstraction level	Circuit architecture
Pros	SEU hardness
Cons	Power consumption penalty: not significant Speed penalty: little Area penalty: 100 %
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.5 HIT hardened memory cell

9.2.1.5.1 Description of the concept

The Heavy-Ion Tolerant (HIT) cell is composed of 12 transistors organized in two storage nodes interconnected by feedback paths [178], [179]. This cell offers a good robustness to SEU without degradation of electrical parameters and with reasonable silicon area overhead.

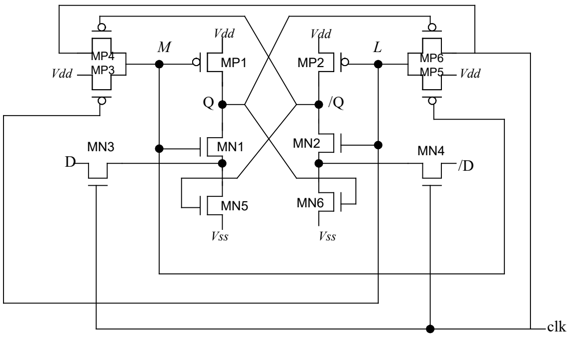


Figure 9-5: HIT memory cell

Examples:

- 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 [180].
- The TSC21020E was used in the Rosetta mission launched in 2004 and that successfully arrived in 2014 to the Churyumov Gerasimenko comet.
- HIT cell is included in the DARE 180 nm library [74] (see section 10.2) [81].

9.2.1.5.2 Available test data (simulations, radiation testing, in-flight)

According to experimental results provided in reference [178], 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*cm^2/mg).

9.2.1.5.3 Added value (efficiency)

- Due to its specific architecture and transistor sizes, the HIT cell can be used without I/O buffers.
- Area penalty: ~100 % compared to standard cell of 6 transistors.

- No specific process or design rules needed (RHBD solution).

9.2.1.5.4 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.

A brief summary of key characteristics for HIT hardened memory cell is given in the Table 9-5.

Table 9-5: Summary of key characteristics for HIT hardened memory cell

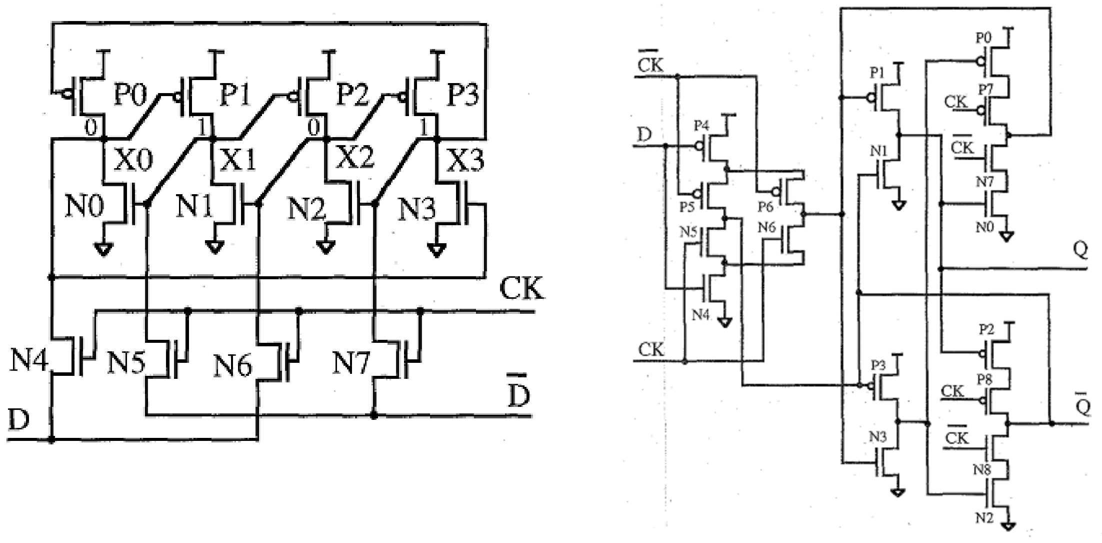
Abstraction level	Circuit architecture
Pros	SEU hardness
Cons	Area penalty: ~100 % Power consumption penalty: ~30 %
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.6 DICE hardened memory cell

9.2.1.6.1 Description of the concept

The Dual Interlocked storage CEll (DICE) embeds 12 transistors for a memory cell structure [181], [112]. This cell, illustrated in Figure 9-6, 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.



a) Memory cell

b) Latch

Figure 9-6: DICE hardened cell structure

Example(s):

DICE cell is implemented in various hardened integrated circuits and several rad hard vendor ASIC libraries as Microchip Atmel and Cobham (former Aeroflex). One representative example is Cobham UT6325 [182].

9.2.1.6.2 Available test data (simulations, radiation testing, in-flight)

In reference [181], two prototypes are described, a static RAM and a register array with DICE cells (see Figure 9-6) 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*cm^2/mg was observed for the DICE cell while unhardened cell had a LET$_{th}$ lower than 10 MeV*cm^2/mg.

Evidence of the immunity to SEU of DICE cells is provided in reference [183]. Test were performed in Brookhaven National Laboratory 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 MeV 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.

9.2.1.6.3 Added value (efficiency)

- Power consumption penalty: low

9.2.1.6.4 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 [184].

The brief summary of key characteristics for DICE hardened memory cell is given in the Table 9-6.

Table 9-6: Summary of key characteristics for DICE hardened memory cell

Abstraction level	Circuit architecture
Pros	Power consumption penalty: low
Cons	Area (100%) and power consumption increase (low)
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.7 NASA-Whitaker hardened memory cell

9.2.1.7.1 Description of the concept

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 9-7, was first implemented in a Reed Solomon Encoder designed for the Space Station and Explorer platforms [185], [186], [173].

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 adapting the strengths of transistors within the cell.

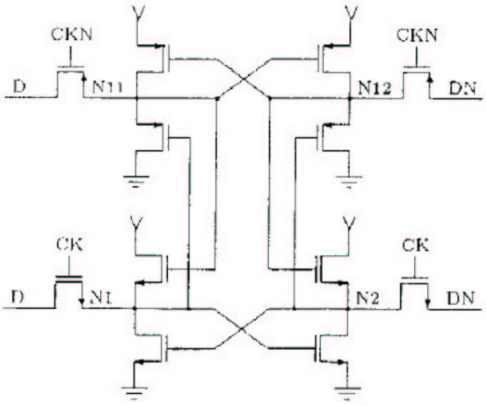


Figure 9-7: NASA-Whitaker hardened memory cell

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 [185].

9.2.1.7.2 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 9-7 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*cm^2/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*cm^2/mg. No latch-up was observed in any of the parts subjected to radiation, demonstrating an SEL threshold in excess of 120 MeV*cm^2/mg.

9.2.1.7.3 Added value (efficiency)

- This cell uses standard size transistors.

9.2.1.7.4 Known issues (weaknesses, elements to be considered)

- High power consumption penalty.

The brief summary of key characteristics for NASA-Whitaker hardened memory cell is given in the Table 9-7.

Table 9-7: Summary of key characteristics for NASA-Whitaker hardened memory cell

Abstraction level	Circuit architecture
Pros	SEU hardness
Cons	Power consumption penalty: high
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.1.8 NASA-Liu hardened memory cell

9.2.1.8.1 Description of the concept

This cell, illustrated in Figure 9-8, is an improvement of the Whitaker's SEU hardened CMOS memory cell [186]. 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.

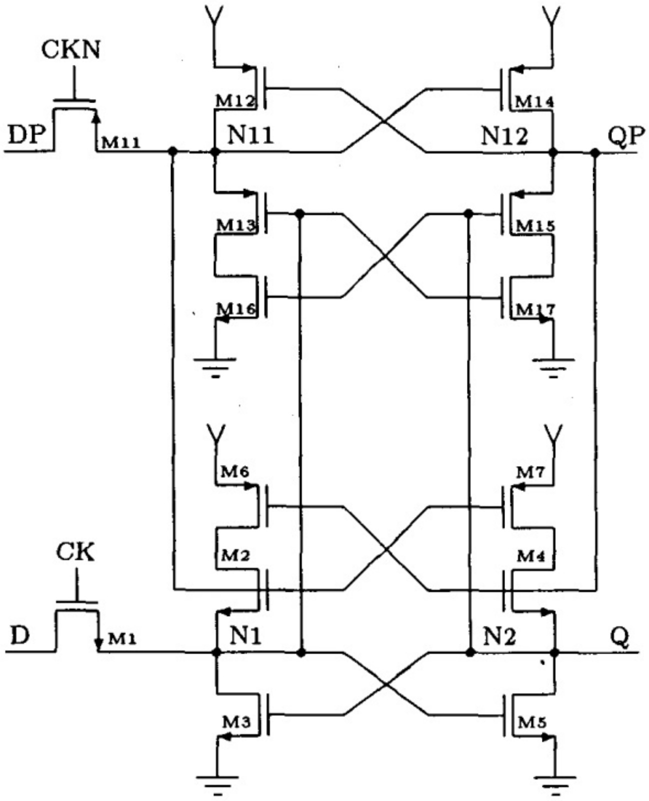


Figure 9-8: NASA-Liu hardened memory cell (after original picture in [186]

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:

- an Error-Correcting Code (ECC) encoder that supports the Reed-Solomon (RS 16) for Telemetry Channel Coding;
- programmable Reed-Solomon ECC encoder/decoder. 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 [187].

9.2.1.8.2 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*cm^2/mg. However, above 30 MeV*cm^2/mg, the test chip latched up [186].

9.2.1.8.3 Added value (efficiency)

This cell uses standard size transistors.

9.2.1.8.4 Known issues (weaknesses, elements to be considered)

The number of transistors required for the NASA-Liu SEU-hardened data latch makes 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.

The brief summary of key characteristics for NASA-Liu hardened memory cell is given in Table 9-8.

Table 9-8: Summary of key characteristics for NASA-Liu hardened memory cell

Abstraction level	Circuit architecture
Pros	SEU hardness, improved power consumption with respect to Whitaker hardened memory cell
Cons	
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests SW fault injection with Spice simulation

9.2.2 Bit-interleaving in memory arrays

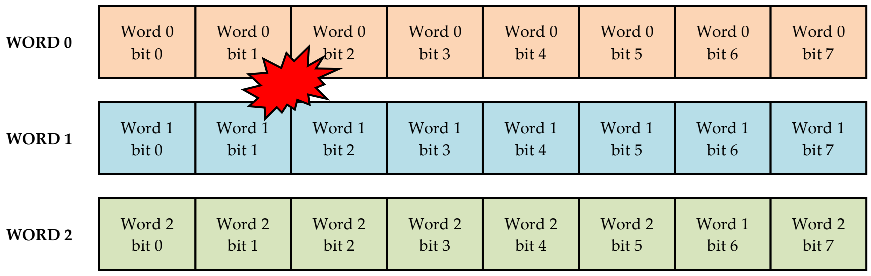
9.2.2.1 Description of the concept

Memory blocks (arrays of bit memory cells) can be a very sensitive part inside our IC with respect to radiation effects, since they often exhibit a very high density of memory units, and are therefore a priority when trying to reduce SEU effects. Mitigation strategies based on spatial redundancy (duplication or triplication) are usually not well suited for large arrays of memory cells because of the high area cost. A less area costly alternative solution is the use of error correction codes (see section 12.2.1) often combined with "bit-interleaving" or "data bit scrambling".

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 12.2.1), 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 [339]. 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 memory block, differs from the physical or topological internal structure of the memory block. In other words, logically adjacent "addresses" (i.e. data groups, words) cannot be physically adjacent (this is called address scrambling) and that logically adjacent "data bits" are not physically adjacent (this is called data scrambling [188]).

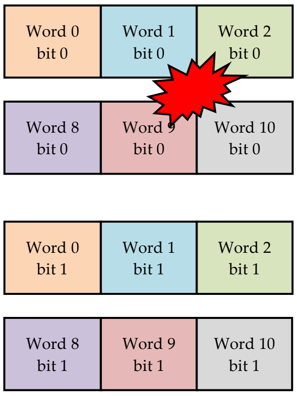
Figure 9-9 is an illustration of a particle generating charges which can be collected by four adjacent memory elements. In this case, there is a probability to get two upsets in word 0 and word 1. In such conditions, common error correcting codes are able to detect both errors but not to correct them.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

Choosing an optimal EDAC/ECC approach involves knowing what kind (if any) of bit-interleaving is present in the memory blocks that are used. Sometimes this is known to the user, as the vendor of the memory blocks makes this information available. In some other cases unfortunately, the bit scrambling or interleaving characteristics of the memory array are not known.



WORD 0	Word 0 bit 0	Word 0 bit 1	Word 0 bit 2	Word 0 bit 3	Word 0 bit 4	Word 0 bit 5	Word 0 bit 6	Word 0 bit 7
WORD 1	Word 1 bit 0	Word 1 bit 1	Word 1 bit 2	Word 1 bit 3	Word 1 bit 4	Word 1 bit 5	Word 1 bit 6	Word 1 bit 7
WORD 2	Word 2 bit 0	Word 2 bit 1	Word 2 bit 2	Word 2 bit 3	Word 2 bit 4	Word 2 bit 5	Word 1 bit 6	Word 2 bit 7

Figure 9-9: Standard memory topology



Word 0 bit 0	Word 1 bit 0	Word 2 bit 0
Word 8 bit 0	Word 9 bit 0	Word 10 bit 0
Word 0 bit 1	Word 1 bit 1	Word 2 bit 1
Word 8 bit 1	Word 9 bit 1	Word 10 bit 1

Figure 9-10: Example of memory topology with scrambling

A SRAM memory with bit-scrambling processed in commercial 65 nm CMOS technology is presented in reference [189].

In this other case study [322] a procedure to estimate the optimal inter-leaving distance in large memory arrays of 65 and 45nm technology is presented.

9.2.2.2 Available test data (simulations, radiation testing, in-flight)

Experimental test results with neutron and alpha particles, presented in [189] show that no MBU were detected as the tested memory uses scrambling.

Experimental results obtained in a SRAM 150 nm device, presented in [190] show that the adopted interleaving leads to a MBU reduction of more than 98 %. The result of the work presented in this example shows that the memory physical architecture is critical in affecting the single-bit EDAC effectiveness. In particular the bit-interleaving scheme implemented in the device under test prevents MBUs from affecting the same data word. These MBUs are detected as SEUs in different data words.

9.2.2.3 Added value (efficiency)

Bit-interleaving, address-scrambling and / or data-bit scrambling can be effective ways to reduce the probability of MBU in a same data-bit group (word), and thus to allow single-error codes (e.g. EDAC) to perform their intended mitigation job.

9.2.2.4 Known issues (Weaknesses, elements to be considered)

In some cases, it negatively impacts the chip floorplan, access time, and/or power consumption [191].

The brief summary of key characteristics for bit-interleaving in memory arrays is given in Table 9-9.

Table 9-9:Summary of key characteristics for bit-interleaving in memory arrays

Abstraction level	Circuit Architecture
Pros	Avoid MBU
Cons	Can affect chip floorplan, access time, and/or power consumption
Mitigated effects	MBU
Suitable Validation methods	Accelerated ground tests

9.2.3 Data scrubbing

One other way to mitigate data corruption in memory banks inside our ICs is to re-write (completely or partially) those memory bits with “golden values” that are stored in a safe place (e.g. a radiation hard memory chip). The operation to overwrite the bits with their good values, commonly referred to as “data scrubbing” is performed with a time frequency that is appropriate for the expected rate of radiation induced faults and in a way that does not compromise the good operation of the IC. Scrubbing prevents the accumulation of corrupted bits in memory banks that are storing known configuration data or any other data which is not refreshed spontaneously and frequently enough (as to prevent error accumulation) by the IC itself as part of its expected operation. This mitigation technique is therefore often used to refresh the configuration memory bits of SRAM-based FPGAs.

A detailed description of it is given in 13.2.8.

9.3 Comparison between hardened memory cells

Table 9-10 summarizes the main characteristics, advantages and drawbacks for the previously presented SEU hardened memory cells.

Table 9-10: 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*cm^2/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*cm^2/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*cm^2/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*cm^2/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*cm^2/mg the test chip latched up

10 Radiation-hardened ASIC libraries

10.1 Introduction

Most of the foundries proposing specialised radiation-hard manufacturing processes 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 the basic functional "cells" that can then be manufactured in one or more commercial ASIC processes, 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 these cells and therefore the "ASIC libraries" where they a packaged for the use of ASIC designers, is achieved by combining several techniques listed in the Layout section, but also the Analogue circuits and Embedded Memory sections. Figure 10-1 illustrates a radiation hardened two input NOR gate implementing ELT transistors and guard rings.

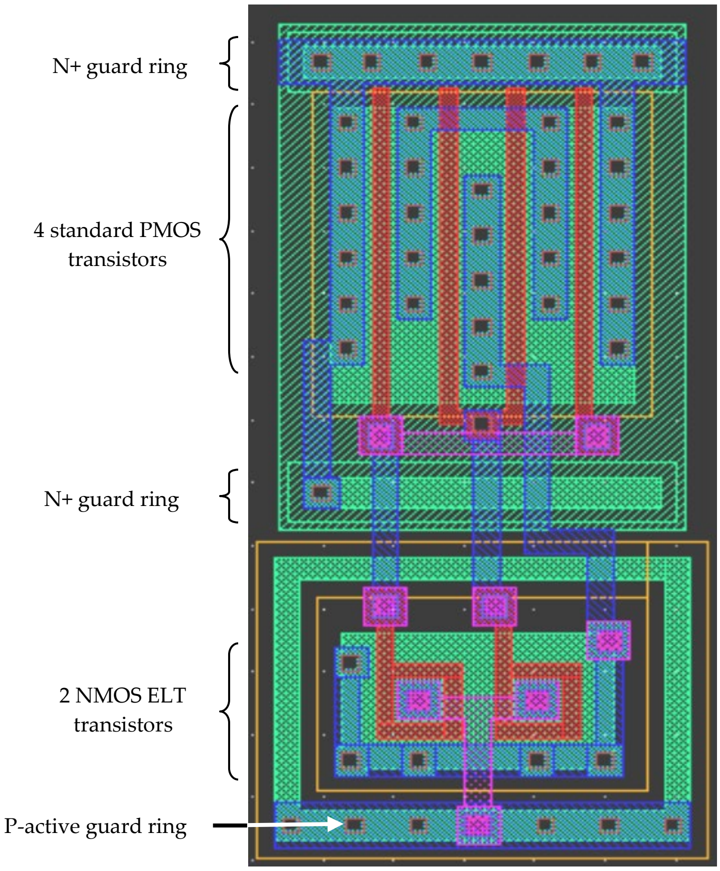


Figure 10-1: Hardened 2 input NOR gate

What follows is a non-exhaustive list of some well-known radiation hardened ASIC libraries that have been used to develop space ASICs and that are included in this handbook as examples. Annex A provides the link to a short list of these libraries and a few more, some of them under development or qualification for its use in space at the time of editing this handbook.

10.2 IMEC Design Against Radiation Effects (DARE) library

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

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 Signalling (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 13) are also proposed in the DARE library [81].

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 [74]. 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 [82]. 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.

10.3 CERN 0,25 μm radiation hardened library

A radiation tolerant 2,5 V standard cell library using a commercial 0,25 μm 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 LHC experiments total dose hardness levels.

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 the previously available radiation hardened technology. The area increase 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 [75]. 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.

10.4 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 [76]. 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 tests results show that no parametric or functional degradation was observed through a total dose of 3 Mrad(SiO2). 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 [83].

10.5 Ramon Chips 0,18 μm and 0,13 μm radiation hardened libraries

Ramon Chips has developed a 0,18 μm [84] and a 0,13 μm [85] radiation hardened libraries. The 0,18 μm library is available for 3,3 V and 1,8 V 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 for SEU in flip flops (at Low Earth Orbit), and 2,10^{-7} error/bit/day for SEU in SRAM (at Low Earth Orbit). 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 [86] 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.

10.6 Cobham (former Aeroflex) 600, 250, 130 and 90 nm radiation hardened libraries

Cobham (former 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 2E-10 errors/bit/day (based on standard evaluation circuit at 4,5V worst case condition. Non-hard flip-flop typical is 4E-8) [87].
- 250 nm library: radiation hardened from 100 krads(Si) to 1 Mrads(Si). SEU-immune less than 1E-10 errors/bit/day (based on standard evaluation circuit at 2,25V or 3,6V core/3,0V I/O V_{DD} 25 °C condition. Non-hard flip-flop typical is 8E-9) [88].
- 130 nm library: radiation hardened from 100 krads(Si) to 300 krads(Si). SEU-immune less than 1E-10 errors/bit/day (based on standard evaluation circuit at 1,1V core/3,0V I/O V_{DD} 25 °C condition. Non-hard flip-flop typical is 5E-8) [89].
- 90 nm library: radiation hardened from 100 krads (Si) to 1 Mrads(Si) [90].

10.7 Microchip Atmel MH1RT 0,35 µm and ATC18RHA 0,18 µm CMOS and ATMX150RHA 0,15 µm SOI CMOS radiation hardened libraries

Microchip Atmel MH1RT Gate Array and Embedded Array families were 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*cm^2/mg, as well as latch-up immunity up to 100 MeV. MH1RT ASIC technology made 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 80 MeV*cm^2/mg was observed. This technology is present in several catalogue ICs of Microchip Atmel, but the technology was discontinued in 2011, and no new ICs can be manufactured with this technology any more.

The Microchip Atmel ATC18RHA is fabricated on a proprietary 0,18 µm CMOS process intended for use with a supply voltage of 1,8 V. It contains a library of standard logic and I/O cells, Pads, memory cells and SEU hardened flip-flops. This library offers latch-up immunity and total dose capability better than 100 krads.

Most recently, Microchip Atmel is developing a mixed-signal set of ASIC libraries based on UMC 150nm SOI CMOS process, called ATMX150RHA

10.8 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 [91]. 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 higher than 200 krads for TID and it is immune to SEL.

10.9 ST Microelectronics C65SPACE 65 nm radiation hardened library

ST Microelectronics is currently offering a radiation hardened version of its 65 nm commercial library cells. Prototype chips have been evaluated [92]. 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, saturation cross-sections of 10^{-7} cm^2 to 10^{-8} cm^2 were obtained depending on the cells type and patterns.

10.10 RedCat Devices radiation hardened libraries

RedCat Devices rad-hard libraries are designed to be used in ASICs for space applications. All cells can be placed by using standard Place&Route tools such as Cadence Encounter or Tanner L-Edit. Some of these libraries have been used in Russia for digital applications in projects funded by ROSCOSMOS (SSD controllers and also rad-hard microprocessors) and underwent evaluation by ISRO in India. The libraries are offered for 0,18 and 0,13 nodes for TowerJazz and X-Fab.

11 Digital circuits

11.1 Overview

Fault tolerant techniques presented in this section apply mostly at “circuit architecture level” and are applied to one digital design or soft IP block. This means that they can be implemented in Hardware Description languages (HDL) such as Verilog or VHDL or during logic synthesis. Inter-block mitigation and higher complexity circuit level mitigation techniques are discussed in the "System on a Chip" Section 12. The best solution to protect digital circuits from radiation effects is often a combination of several mitigation techniques.

Techniques presented hereafter are either based on spatial redundancy, temporal redundancy or both. In addition the important case of FSMs and how to wisely choose the different types of digital cells available in the IC digital design kits is presented. 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 cannot be mitigated with these techniques.

Three other groups of mitigation techniques targeting individual memory cells, array of memory cells and information redundancy are also important for the digital circuit designer, but are presented in Sections 12 and 13.2.4. A nice overview of many representative mitigation schemes that can help a digital IC designer to deal with soft errors induced by radiation is given in reference [143].

Therefore, several fault tolerance techniques out of one or more of these five groups can be applied for digital ICs:

- **Spatial redundancy**: resources are replicated in order to process the same task in parallel. A downstream comparison or voting circuitry is in charge of error detection and eventually error correction, depending on the number of implemented replicas. Depending on the selected architecture, the hardened system can handle a more or less wide scope of errors (e.g. SET and SEU).
- **Temporal redundancy**: signals are sampled (or full functions executed) at different instants and a voting/comparison circuitry allows rejecting single event transients and upsets.
- **Memory cell hardening**: memory cells often represent a large percentage of the total silicon area occupied by a digital circuit. Hence, it is important that designers take special precaution to ensure their radiation robustness meets the mission criteria. A suitable solution is the replacement of memory cells (e.g. flip-flops, registers or latches) by radiation-hardened ones. Section 9.2.1 presents mitigation techniques for individual memory cells.
- **Memory block hardening**: to prevent radiation induced errors in more than one bit of a “data block” residing in a memory cell array we can implement mitigation techniques at memory block level, trying to avoid that bits belonging to a same “data block” are stored physically too close to each other, and therefore can be altered by the same radiation event. This is explained in section 12.2.2.
- **Information redundancy**: error-detecting codes and error-correcting codes are able to protect the integrity of data blocks that reside in arrays of memory cells from radiation effects. This is covered in sections 12.2.1 and12.2.2.

A summary of mitigation techniques for digital designs is given in Table 11-1.

Table 11-1: Summary of mitigation techniques at digital design circuit architecture level and the radiation effects they address

Mitigation techniques		Radiation effects	
		SET	SEU
11.2.1	Spatial redundancy	X	X
11.2.1.2	Duplex architectures	X	
11.2.1.3	Triple Modular Redundancy architectures	X	X
11.2.1.3.2	Basic TMR	X	X
11.2.1.3.3	Full TMR	X	X
11.2.2	Temporal redundancy	X	X
11.2.2.1.2	Triple Temporal Redundancy combined with spatial redundancy	X	X
11.2.2.1.3	Minimal level sensitive latch	X	X
11.2.3	Fail-safe, deadlock-free finite state machines		X
11.2.4	Selective use of logic cells, clock and reset lines hardening	X	X

11.2 Mitigation techniques

11.2.1 Spatial redundancy

11.2.1.1 Description of the concept

Spatial redundancy, also called hardware redundancy, is based on replicating sensitive functional modules and comparing their outputs to detect discrepancies (Figure 11-1). Several architectures are available, each of them having advantages and penalties. However, all of them imply an area trade-off and, as a direct relationship, a power consumption trade-off. In addition, some timing degradation occurs due to the comparator logic and in some cases higher layout congestion.

A mismatch between the results supplied by the different replicas is detected by the comparator or voter. Hence, as the decision whether the output is correct or not only relies on this element, the voter is a critical part of this architecture.

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

- **Error detection** only: this is the case for duplex architectures, also called Dual Modular Redundancy (DMR).

- **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 DMR and TMR which are commonly implemented in space applications are given hereafter.

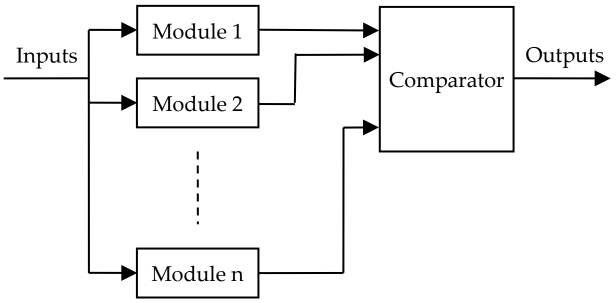


Figure 11-1: Block diagram of the spatial redundancy architecture

11.2.1.2 Duplex architectures

Duplex architecture uses two replicas of a processing unit and compares the outputs to detect potential differences provoked by SEEs and then either flag the difference or prevent a wrong value from propagating (by going into high impedance mode). This scheme can be applied for both combinatorial and sequential logic and can provide respectively SET (Figure 11-2(a)) and SEU (Figure 11-2(b)) detection.

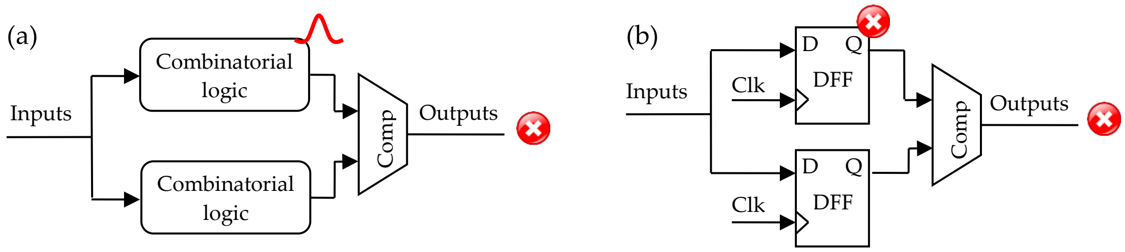


Figure 11-2: (a) SET and (b) SEU detection with a duplex architecture

The comparator being the critical element is 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 11-3(a) the comparator assumes that both are correct. When they differ, the comparator detects an error but is not capable of determining the non-faulty one (see Figure 11-3(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 critical risk to the application.

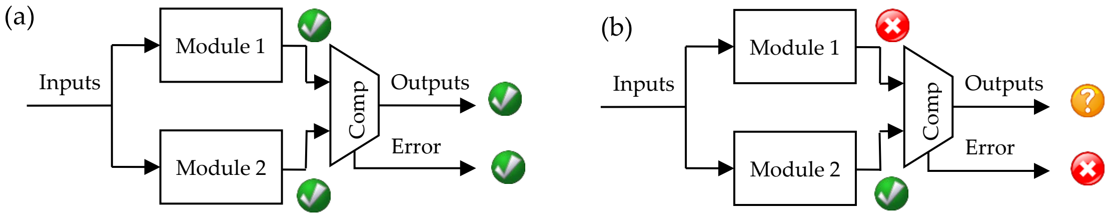


Figure 11-3: Fault detection by a duplex architecture

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 11-4(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, it 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 monitors, increasing the cost of the project. For this reason an alternative, depicted in Figure 11-4(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. Of course this strategy is based on the assumption that the third spare module is fault-free. This is in practice what we call TMR, which is the subject of the next section.

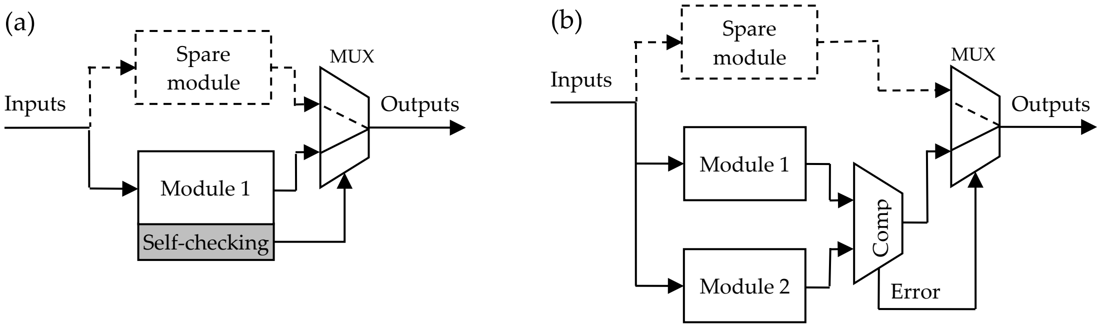


Figure 11-4: Hot backup (a) and duplication with backup (b) approaches

11.2.1.3 Triple Modular Redundancy architectures

11.2.1.3.1 General

Triple Modular Redundancy or TMR is one of the most popular and simpler mitigation techniques applied by digital circuits designers, but also sometimes used in mixed-signal circuits (see 12.2.5). It can be implemented in different ways depending on the level of fault tolerance specified and the overheads that the chosen TMR approach introduces while still meeting the chip area, power and performance requirements. Different styles of TMR with different names can be found in the technical literature, and this handbook aims to present the most representative or widely used. In this section we introduce the basic TMR concept (we call it “basic TMR”), one style that also protects against SETs in the data paths and SEU accumulation (“full TMR”), and other styles where TMR is combined with delays in the clock or data lines (see 11.2.2.1.2). In sections 13.2.1 to 13.2.5 the handbook elaborates in five other variants of TMR, this time when being applied inside FPGAs, and with the main differentiation factor being the level of granularity of the functional blocks being triplicated and voted: “local TMR”, “global TMR” and “large grain TMR”, and the special cases of “embedded user memory TMR” and “additional voters in TMR datapaths”. Lastly, Section 15 indicates that TMR can be used at higher electronic system level, triplicating the ICs and voting their outputs.

11.2.1.3.2 Basic TMR

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, as depicted in Figure 11-5.

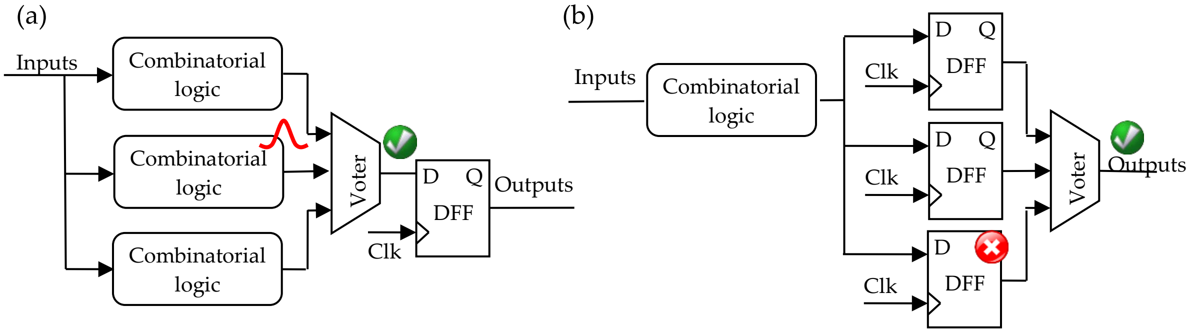


Figure 11-5: SET (a) and SEU (b) detection with a TMR architecture

The efficiency regarding fault tolerance of the basic and most simple TMR architecture as presented in Figure 11-5 suffers from three limitations:

- An SET occurring in the combinatorial logic and propagating to the TMR memory structure can 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 can result in a wrong TMR output value.
- SEU-induced wrong values in the memory elements of the TMR structures can accumulate in time if they are not refreshed with good values. Sometimes this can happen spontaneously with the arrival of a new clock edge and the new good data input, but in some cases it can be necessary to do this refresh more systematically with a slightly more complex TMR architecture.

11.2.1.3.3 Full TMR

The Full TMR architecture is an answer to the identified weaknesses in basic TMR. As depicted in Figure 11-6, it combines a triplication of all the elements: the combinatorial logic, the flip-flops and the voters. In addition, a feedback loop from the voters' outputs to the data inputs of the flip-flops can be optionally added in order to ensure a timely refresh of a flip-flop corrupted by radiation, whenever this is necessary or appropriate (e.g. for configuration registers that are written only occasionally, and where wrong values due to SEUs can accumulate unless they get refreshed).

- The first example, depicted in Figure 11-6(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 11-6(b) illustrates the case of an SET occurring in the combinatorial 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 11-6(c) illustrates an SET which occurs in the voter itself. The voter generates that 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 is 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 force the faulty output to the correct value.

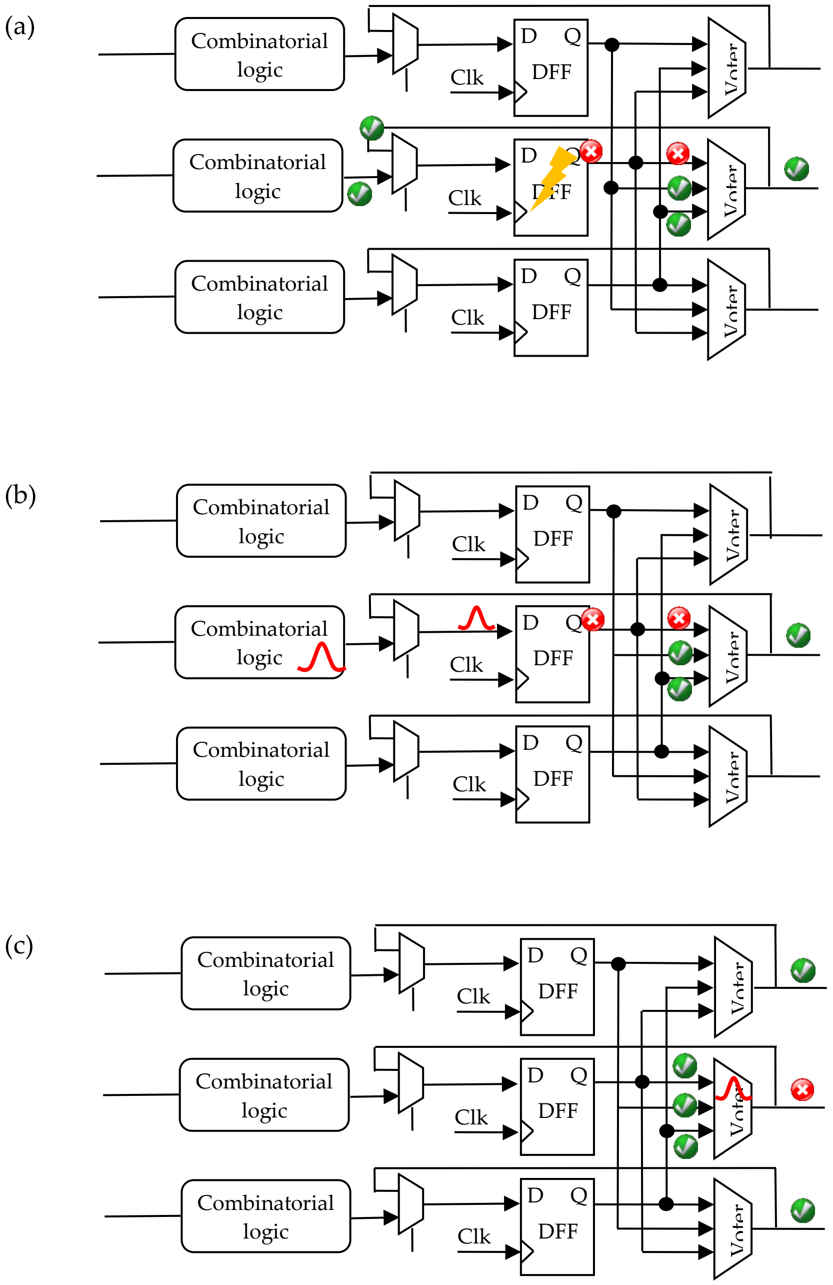


Figure 11-6: Fault detection and correction in the full TMR architecture

These examples of full TMR proved the capability of the full TMR architecture to detect and correct SETs in the combinatorial logic and SEUs in the flip-flops.

Nevertheless, full TMR is not always the ideal solution for every IC case. There are many other techniques based on spatial redundancy applied at circuit architecture level, for example:

- University of Nebrija presents an "offset Double Modular Redundancy" mitigation technique for transform-based convolutional functions, such as FFT, in [323].
- RLEON2-FT IP core contains TMR-FFs as an option [324].

- Reduced Precision Redundancy (RPR) is a technique based on spatial redundancy of only the some significant bits in a DSP computation data group, and use this a sanity check for the entire full precision set of bits. This technique was also used inside the Cibola Flight Experiment Satellite and is presented in [325].
- An example of a 45nm SEU-tolerant latch that uses a Muller-C element and DMR is explained in [330], including results of SPICE simulations of the power dissipation, reliability and propagation delays. Its transistor level circuit diagram is reproduced in Figure 11-7.

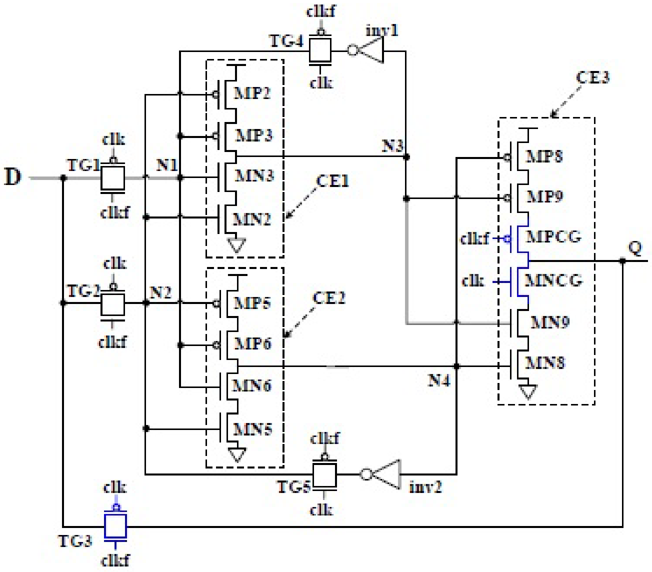


Figure 11-7: SEU-tolerant latch based on DMR (CE1 and CE2) and a Muller-C element (CE3)

11.2.1.4 Available test data (simulations, radiation testing, in-flight)

See [319] and [321] for simulation, fault injection and in-flight test data of some digital circuits protected with DMR and TMR techniques.

11.2.1.5 Added value (efficiency)

Spatial redundancy is a mitigation technique that can be applied at different stages of the development of digital ICs. During the HDL coding phase IC designers can decide if it is applied everywhere (as in Full TMR) or only locally and selectively, depending on the area, power and performance requirements. The simple concept behind, high efficiency, the flexibility and different modalities in which spatial redundancy can be applied are added values that have made of this mitigation technique one of the most popular and frequently used by digital IC designers.

11.2.1.6 Known issues (weaknesses, elements to be considered)

Besides the large area overhead that TMR can imply in some cases, “full TMR” also has these two known weaknesses:

- One of the effects of scaling down the transistors is the increase of the risk of charge sharing between several devices [144]. This can 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.

- Whenever an end-chain voter is used, known as the “the voter of the voters”, this can become an additional source of undetected faults. Even if the probability is low, it is important that the designer keeps in mind this weakness. As discussed in references [145] and [146], an alternative is the use of an analogue voter instead of a digital one.

The brief summary of key characteristics for spatial redundancy is given in Table 11-2.

Table 11-2: Summary of key characteristics for spatial redundancy

Abstraction level	Circuit architecture
Pros	SET and SEU detection and correction
Cons	• Area overhead: depending on the number of redundant nodes • Power consumption • Timing degradation
Mitigated effects	SET, SEU
Suitable validation methods	Radiation ground testing Fault injection
Automation tools	FTI (Fault Tolerant Insertion) and FTIS (Fault Tolerant Injection and Simulation) from the AMATISTA project [147],[148] Some IC Design Tools allow automatic TMR insertion, as configured by the IC designer: • Xilinx XTMR • Mentor Precision Hi-Rel • Synopsys Synplify Premier Xilinx IDF, IVT and SEM IP help in the isolated instantiation of redundant functional blocks (for DMR and TMR for example).

11.2.2 Temporal redundancy

11.2.2.1 Description of the concept

11.2.2.1.1 Overview

The concept of temporal redundancy is based on sampling the same data at slightly different instants. An asynchronous comparator or voter then determines the correct value. Multiple sampling (dual, triple or larger), can be achieved by having multiple parallel instantiations of the function to be protected (which can be anything from a simple memory element to a much more complex processing circuit), and in addition, branching off into multiple parallel clock (or data) inputs to these functions. These parallel inputs are identical, except that a timing skew difference (making sure that the delay is larger than the transient pulse width) between them ensures that even if one SET is affecting one of the function instantiations, the majority of the rest latch the good (nominally expected) value. The special case of using time redundancy with skew in data lines to filter away SETs is explained in detail in 12.2.3.

Alternatively, if the function to be protected is more complex, and perhaps too large in size to replicate it inside the chip, instead of this relatively simple clock (or data) time skewing, a more sophisticated mechanism can be put in place to repeat sequentially the operation of the function (without having to have spatial redundancy), and later decide which results are kept as the good ones, to carry on with the rest of the chip functionalities. This second style of time redundancy is applied more often to chips that contain microprocessors, and it is handled by the software that drives these processors. Section 13 elaborates on this concept of time redundancy.

In reference [149] complete study on the temporal sampling methodology is done. Different implementations of this technique are presented and the design trade-offs are discussed in detail.

11.2.2.1.2 Triple Temporal Redundancy combined with spatial redundancy

This strategy protects against SEU when combined with spatial redundancy but also against SET thanks to the temporal redundant sampling.

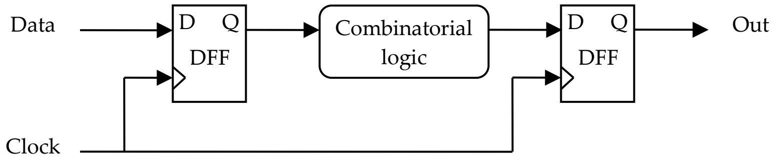


Figure 11-8: Typical topology for a sequential circuit

As illustrated in Figure 11-8, a flip-flop's input is usually the result of a combinatorial computation where a transient can propagate along the logic chain. If this transient reaches the flip-flop at a clock edge the transient can be latched (an SET that turns into an SEU). Protection against this phenomenon can be achieved by sampling the combinatorial output at three different instants and placing a majority voter. This can be implemented using delays (ΔT) as depicted in Figure 11-9. Transients can be rejected by ensuring that ΔT is longer than the transient's duration.

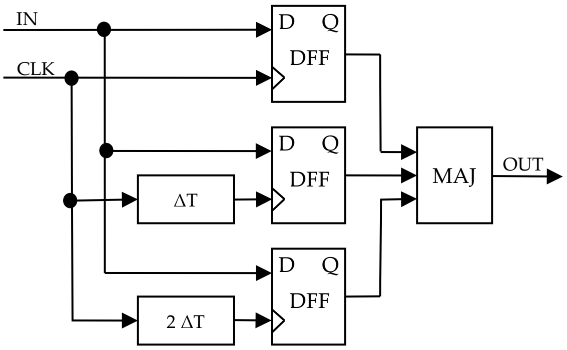


Figure 11-9: Temporal sampling using delays on clocks and TMR

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, for example, in a work done on Microsemi RTAX-S family [154]. Indeed, the higher the number of clock pulses by unit of time, the higher the chance of an SET to be latched.

Alternatively, as shown in Figure 11-10, the delays can be applied on the data lines instead of the clocks, in the case that we want to protect the triplicated flip-flops from latching a same SET pulse that can arrive on the data inputs. In this way, short SET pulses get filtered away from the active edge of the clock, while "real data" (wider pulses) are still latched by the three FFs.

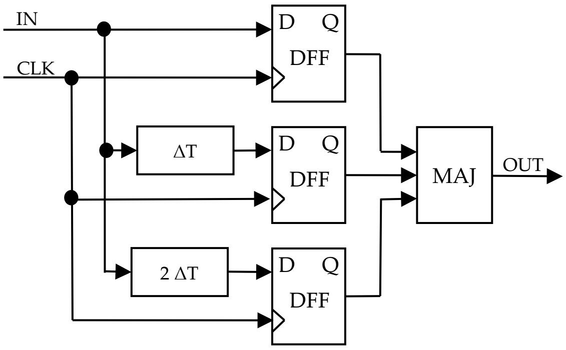


Figure 11-10: Temporal sampling using delays on data

It is important to note that the input clock nodes of the temporal latches shown in Figure 11-9 and Figure 11-10 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 can 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 is therefore be limited to circuits in which the clock node capacitance and thus its Qcrit is sufficiently large, avoiding transients to be generated in the radiation environment.

11.2.2.1.3 Minimal level sensitive latch

Another circuit topology, illustrated in Figure 11-11, 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 inputs, 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.

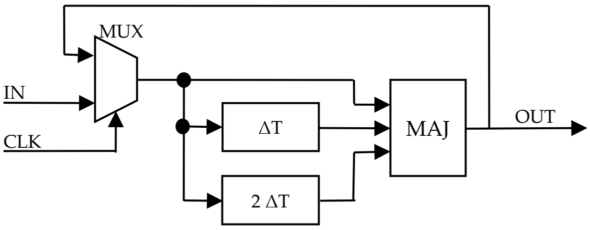


Figure 11-11: Minimal temporal sampling latch replicating itself in time

This design provides another important improvement compared to the one given in the mitigated FF architectures explained in 11.2.2.1.2. Indeed, it is also immune to transients (ΔT or shorter) occurring on the clock input. Any transients momentarily switching the select input of the MUX can 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 and spatial mitigated latches presented in Figure 11-9 and Figure 11-10, this version does not use 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.

Some examples:

- Flip-flops of the LEON2-FT processor control unit and several chips containing this IP Core (e.g. Microchip Atmel AT697), are protected by temporal redundancy, where the clock lines of the triplicated FFs have been skewed.

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

For other examples of rad-hard memory cells implemented with analogue circuit architecture level techniques, see section 9.2.1.

11.2.2.2 Available test data (simulations, radiation testing, in-flight)

- Microsemi RTAX-4000D rad test reports available in www.microsemi.com
- Xilinx 5QV: see http://radhome.gsfc.nasa.gov/

11.2.2.3 Added value (efficiency)

High SEU and some SET immunity.

11.2.2.4 Known issues (weaknesses, elements to be considered)

11.2.2.4.1 Area penalty

According to reference [149] the area penalty of the two structures presented in 11.2.2.1.2 is about four times the area of a conventional D-Flip-Flop (DFF), whereas the minimal level sensitive latch (11.2.2.1.3) is roughly three times larger than a conventional DFF. However, the total chip area does not grow by these numbers as a typical design is not composed exclusively of latches and the combinatorial logic circuitry remains unchanged. In typical ASIC designs, the authors observed that DFFs usually represent 20 % to 40 % of the total chip area, therefore the application of temporal redundancy can result in an increase factor of 1,4 to 1,8 of the total chip area.

11.2.2.4.2 Speed penalty

The insertion of two extra delays results in a lower clock operating frequency. Reference [149] 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 50 MHz has its frequency reduced by 2 % for a 200 ps sampling delay. However, if the original circuit operates at 500 MHz, the speed penalty grows to almost 20 % for the same sampling delay. SET tolerance depends on the SET duration.

11.2.2.4.3 IC Design Tool difficulties

The Process, Voltage and Temperature (PVT) variations during the manufacturing of ASICs can affect adversely the timing skews introduced in the circuit, as they tend to be very small. This can impair the timing redundancy as it was intended by the IC designer. Likewise, and even more importantly so, the tools used during the IC design flow to do the mapping to specific technology gates (“netlist synthesis”), and the subsequent place and route optimizations, can also impair the artificially introduced skew, when these tools try to optimize other IC parameters such as global area or timing, and setup time or hold time rules of the gates.

The brief summary of key characteristics for temporal redundancy is given in the Table 11-3.

Table 11-3: Summary of key characteristics for temporal redundancy

Abstraction level	Circuit architecture
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, fault injection

11.2.3 Fail-safe, deadlock-free finite state machines

11.2.3.1 Description of the concept / implementation

FSMs are usually the “brain” which controls the rest of the integrated circuit and its data-paths, therefore radiation induced failures in FSMs can have severe consequences on the operation of the IC system where these FSMs are performing control functions.

For an FSM with N states, at least $\log_2(N)$ bits (rounded up to next integer) are used to store the state vector. Unless N is a power of two, “illegal states” exist. Illegal states are values of the state vector which can never be reached by the mathematical model of the FSM or in other words, states where the FSM is not supposed to enter during its intended normal operation. For example, an FSM with 5 states needs at least 3 bits to store the state vector. These 3 bits allow for up to 8 states, hence 3 of the 8 states are illegal states.

SEUs in the FSM memory elements can cause the following problems:

- “**illegal transitions**” between legal states are those which occur when the nominal sequence of states is modified. The new state, resulting from an illegal transition is a legal state, but it is not what is expected according to the previous state and the inputs. Therefore, this can result in a malfunction in the rest of the logic affected by the FSM state and output vectors.
- transitions into “**illegal states**”. Depending on how the FSM is implemented and on the input vectors following the entry into an illegal state, two cases can be distinguished:
  - the illegal state reverts to a legal state after one or more clock cycles. Malfunctions can occur before the FSM goes back to a correct state.
  - the illegal state is persistent, the FSM remains locked in this state and can be recoverable only by a system reset. If this persistent FSM “deadlock” is not detected and reset, malfunctions can occur.
- the FSM output vector can also take an undefined (illegal) value.

Several FSM-specific techniques can be put in place to mitigate some of the problems described before and in order to create what is sometimes called “fail-safe”, “fault tolerant” or “deadlock-free” state machines.

Some state of the art HDL synthesis tools can recognise FSM structures and their unreachable (thus illegal) states and can be configured by the user in order for the HDL synthesiser to create additional circuitry that:

- brings the FSM out of any illegal state into, for example, a legal idle state or another FSM dead-lock recovery procedure.
- creates an illegal-state-reached signal

The term “fail-safe” can be misleading, because even if a full deterministic decoding of all possible illegal states is done to avoid that the FSM enters a persistent dead-lock situation, the disruption in the nominal sequence of states and an eventual corruption of the output vectors can always lead to a temporary malfunction of the IC design where the FSM is embedded.

FSMs are digital ICs that can be also protected against radiation effects by other more generic mitigation methods explained in this section 11 such as using rad-hard flip-flops, TMR, DMR with parity, Hamming codes or using appropriate gate types for SET protection.

In many cases, the pure control FSMs only take a minor part of the resources when compared to the resources used for the data path and data storage, such that selecting the highest available protection level for the FSMs (i.e. applying several mitigation techniques) in a design is often also an affordable choice because it does not introduce significant area, power or performance overheads. For example, it has been seen in some designs that all FSM flip-flops were protected by TMR, whereas the data-path flip-flops use a 'lighter' protection, such as error detection with a simple parity bit.

The tool options presented in this section are based on the Synopsys Synplify tool, but similar options exist in other tools, such as in Mentor Precision Rad-Tolerant tools.

Using the “default” or “when others” section in Verilog or VHDL respectively is a prerequisite to ensure a deterministic way out of illegal states. It is however – in general – not sufficient because present synthesis tools are able to recognise illegal states and therefore can optimise away the associated logic unless certain HDL coding and synthesis steps are done.

The synthesis tool option “Preserve and Decode Unreachable States” prevents the tool from optimising away logic associated to illegal states. Note that this works only in conjunction with the proper coding (default / when others) to actually define what to do next when an illegal state is reached. The equivalent to this synthesiser user-configurable option is the attribute “syn_safe_case = 1” which can be added as a comment in the HDL code of the FSM and which affects only locally to an HDL architecture or module declaration, where the FSM is coded.

FSMs can be coded with a “Hamming distance of 3” by an setting another synthesiser implementation option (globally) or by setting locally in the HDL code the attribute “syn_fsm_correction”.

To implement TMR and DMR or DWC (Duplication With Compare), the attribute 'syn_radhardlevel' can be used at architecture / module level. For FSM it is important to enable the voting of feedback loops ('syn_vote_loops').

As the HDL synthesys tools change relatively rapidly with time, it is important that the user carefully studies what attributes and synthesis constraints options are offered by the HDL synthesiser tool in order to recognise FSMs, implement them with the desired code-style and Hamming distance and to ensure a proper way out of illegal states.

The following extract of VHDL code is an example for a simple FSM (counter from 0 to 4), using

- the '**when others' clause is used to define the behaviour for illegal states**, and
- the **'syn_safe_case' attribute to make sure synthesis preserves the intended behaviour**

```
architecture rtl of counter5 is

attribute syn_safe_case: boolean;

attribute syn_safe_case of rtl : architecture is "TRUE";
[..]
    case cnt is

        when "000" => ncnt <= “001”;
        when "001" => ncnt <= “010”;
        when "010" => ncnt <= “011”;
        when "011" => ncnt <= “100”;
        when "100" => ncnt <= “000”;

        – for illegal states (“010”, “101”,”110”and “111”), restart the counter
        – and raise error flag
        when others =>
            ncnt <= “000”;
            error <= '1';
    end case;

[..]
```

In Figure 11-12 we can see in green the legal states and legal states transitions, and in red the illegal states that a single SEU can put the FSM in. The red arrows show illegal state transitions that a single SEU can provoke. An SEU can also cause a legal transition but at the wrong time, and that can be another kind of potential illegal transition which is not reflected in Figure 11-12 not to over complicate the illustration. Finally, the dashed green arrows show legal transitions that were introduced by the HDL sentence “when others” in order to take the FSM out of any of the possible illegal state and put it in this case in the legal initial state “000”. This helps to prevent a deadlock situation for those cases when the FSM does not get out of its illegal states spontaneously during its nominal intended operation.

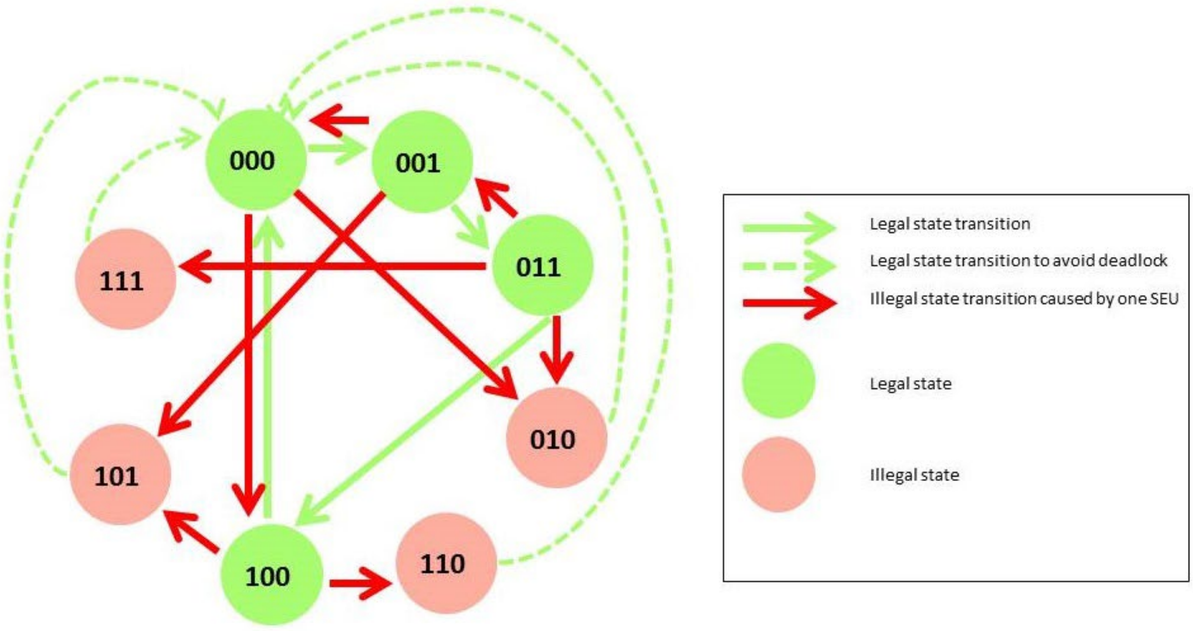

000
001
011
010
100
110
101
111
Legal state transition
Legal state transition to avoid deadlock
Illegal state transition caused by one SEU
Legal state
Illegal state

Figure 11-12: 4 states FSM bubble-diagram showing legal and illegal states, and states transitions

11.2.3.2 Available test data (simulations, radiation testing, in-flight)

The NASA study [331] on Heavy-Ion Single Event Effects for a Variety of Finite State-Machine Mitigation" presents SEU test data on FSMs in Microsemi ProASIC FPGAs, using various mitigation schemes. The key conclusion is that Local TMR (LTMR) and Hamming3 mitigation work very well at low clock frequency, but with increasing clock frequency, the protection effect is partially masked by SET effects in the combinatorial logic which are apparently latched into the flip-flops. Moreover, it was observed that the Hamming3 protection, compared to local TMR, while using more flip-flops, is more susceptible to frequency dependent upsets, such as SETs, due to its higher combinatorial complexity.

11.2.3.3 Added value (efficiency)

The added value of "fail-safe" FSM implementations is to provide a deterministic way out of certain types of radiation induced state transitions in FSMs. However, they neither prevent reaching an illegal state, nor correct it, and they are totally inefficient against illegal transitions between legal states. It is important that they are therefore always used in conjunction with other SEU mitigation and/or error recovery at higher system level.

11.2.3.4 Known issues (weaknesses, elements to be considered)

- The word 'safe' in synthesis attributes like 'syn_safe_case' or equivalent tool options can be misleading, FSMs implemented with such options are not completely safe of any malfunctions due to radiation. Since combinatorial logic is usually added, the SET sensitivity can increase and it is important to consider this secondary effect.
- Whatever protection method has been chosen, it is usually based on adding redundancy. There is always a risk that some smart optimisation algorithm in the synthesis CAD tool tries to remove this redundancy. For example, even if a way out from illegal states to a legal idle state is coded in the HDL code, the associated logic can be optimised away during automatic HDL synthesis in order to reduce the design cost (area, timing, power). Other mitigations being applied to the FSM (not exclusively) can also be unintendedly remove during netlist optimisations: TMR stripped-off or rad-hard FFs be replaced by soft-FF. It is therefore very important to carefully verify the final results produced by the tools: the post-layout netlist before submitting it to ASIC manufacturing or FPGA programming.

The brief summary of key characteristics for fail-safe, deadlock-free finite state machines is given in the Table 11-4.

Table 11-4: Summary of key characteristics for fail-safe, deadlock-free finite state machines

Abstraction level	Circuit architecture
Pros	SET and SEU detection and correction
Cons	Area overhead, Higher Power consumption
Mitigated effects	SET, SEU
Suitable validation methods	Radiation ground testing Fault injection
Automation tools	Synopsys Synplify, Mentor Precision

11.2.4 Selective use of logic cells, clock and reset lines hardening

11.2.4.1 Description of the concept

A wise selection of the cells available in the vendor-provided ASIC libraries or in the pre-diffused cells inside the FPGAs is often an effective and easy to implement mitigation technique. The idea is of course to minimise the use of cells that are more sensitive to radiation effects and to maximise the use of those cells that are less sensitive. This, which can sound at first a bit obvious, implies having a good knowledge of what cells are available for the gate-level-netlist to be generated, and a good control of the synthesis tools when generating the netlist. Every ASIC and FPGA Design Kit vendor normally makes this information available to the IC designers, so that they can choose the best cell options and avoid using the ones that can create problems. It is important as a final verification step, to do a careful inspection of the final gate-level netlist to ascertain that indeed the correct cells were chosen and placed inside the netlist. EDA tools often allow multiple synthesis configurations, and not always deliver what the designer is expecting. Typical mitigation approaches that fall into this category are:

- Selecting or maximising the use of **rad-hard flip-flops** (or any other existing rad-hard cell) and/or avoiding to use the non-rad-hard flip-flops, when doing the ASIC or FPGA gate-synthesis.
- Selecting or maximizing the use of **higher drive / higher fan-out strength cells** for the distribution of critical asynchronous control signals such as clocks and reset lines. This type of cells are normally made of larger size transistors for which the amount of charge induced by radiation that can result in SET phenomena (critical charge) is larger, and therefore the probability to experience SETs in these critical signals is lower.
- Avoiding or minimizing the use of **memory elements with asynchronous resets/sets** if there is significant risk of SETs in these control lines.

See examples of radiation-hardened ASIC libraries at the ESCIES website with the link provided by Annex A.

11.2.4.2 Available test data (simulations, radiation testing, in-flight)

[326] is an interesting paper by University of Southern California and Vanderbilt University where the implications of using different fan-out cells with respect to SET phenomena is studied, modelled and simulated for commercial 90 nm ASIC library cells.

11.2.4.3 Added value (efficiency)

This technique is based in using (or not using) vendor-ready solutions with the help of EDA tools, so it is in principle an easy to apply technique.

11.2.4.4 Known issues (weaknesses, elements to be considered)

As with many other mitigation techniques, radiation hardened cells tend to be larger in size and to consume more power. In addition, it is important that the gate-level netlist engineer always performs a netlist inspection to verify that the expected cells were selected, since the EDA tools employed for the synthesis sometimes do not deliver exactly what the designer was expecting, due to unknown tool bugs or to an incorrect interpretation of the tool manual by the user.

The brief summary of key characteristics for selective use of logic cells is given in the Table 11-5**.**

Table 11-5: Summary of key characteristics for selective use of logic cells

Abstraction level	Circuit architecture

Pros	Easy to do, with vendor-ready solutions (libraries and EDA gate-synthesis tools)
Cons	Area, power overheads
Mitigated effects	SEU, SET being latched and resulting in an SEU-like effect
Suitable validation methods	Inspection of synthesised gate-level netlist
Automation tools	EDA IC Synthesis tools include user configurable parameters that allow control over which cells can and cannot be used for the gate-mapping

12
System on a chip

12.1 Overview

With the scaling the technology nodes for fabricating integrated chip more and more things are combined on a single die of silicon. This is driven by mixed-signal and RF process technologies that allow to combine digital, mixed-signal and full custom design analogue blocks. As a consequence design expertise that used to be the responsibility of the PCB or system designer is now also needed when developing a radiation hardened system on a chip. Additionally special precautions can be needed at the system on a chip (SoC) level to meet the specified radiation tolerance.

Although definitions of SoC differ widely for this section we define it as any chip that combines different soft or hard IP blocks, digital and analogue, into a single chip.

A summary of effects versus mitigation techniques are given in the Table 12-1

Table 12-1: Summary of mitigation techniques at System-on-Chip level and the radiation effects they address

Mitigation techniques		Radiation effects		
		SET	SEU	TID
12.2.1	Error Correcting Codes		X	
12.2.1.1.2	Parity check		X	
12.2.1.1.3	Cyclic Redundancy Check		X	
12.2.1.1.4	BCH codes		X	
12.2.1.1.5	Hamming codes		X	
12.2.1.1.6	SEC-DED codes		X	
12.2.1.1.7	Reed-Solomon codes		X	
12.2.1.1.8	Arithmetic codes		X	
12.2.1.1.9	Low Density Parity Codes			
12.2.2	Mitigation for Memory Blocks		X (MBU)	
12.2.3	Filtering SET pulses in data paths	X		
12.2.4	Watchdog timers	X	X	X
12.2.5	TMR in mixed-signal circuits	X		

12.2 Mitigation techniques

12.2.1 Error Correcting Codes

12.2.1.1 Introduction to multiple options

12.2.1.1.1 General

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 errors are detected and corrected, the term EDAC (Error Detection And Correction) is used.

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 [168]. 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).

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 [225], [226], [227], [168], [228]. Most commonly used ECC in space and aeronautic applications are given in the sub-sections of section 12.2.1.

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 12-2).

There is not one ECC which is the solution to every problem. Each application has its own requirements and only one code can meet all of them. When several codes fit the conditions, the designer has 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: data protection in computers (DRAM, hard-drives, SCSI bus)
- Reed-Solomon: Complex pictures transfer, data protection in computers (CD-ROM drive, associated to the RAR compression protocol in order to rebuild missing data)
- Reed-Muller [281]: Used on Mariner 9 to transmit black and white pictures of Mars
- Low Density Parity codes have been proposed for error correction in high density memories

Table 12-2: Error detection and correction capability for some ECC

ECC	Error detection	Error correction
Parity check	X	
Cyclic Redundancy Check	X	
BCH codes	X	X
Hamming codes	X	X
Reed-Solomon codes	X	X
Low Density Parity codes	X	X

12.2.1.1.2 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 is set to "1" if the number of 1's + 1 is even, and an odd parity bit is 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 an error is detected, 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 as commanded by the CPU and its software, (e.g., the operating system I/O routines).

Let us consider the 7-bit data “1010001”. This number is odd because it contains three “1”.

- Applying even parity sets the parity bit to “1” in order to have an even number (four) of “1” and the data becomes “**1**1010001”.
- Applying odd parity sets the parity bit to “0” in order to have an odd number (three) of “1” and the data becomes “**0**1010001”.

Some other examples are given in Table 12-3.

Table 12-3: 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	0000 0000	1000 0000
101 0001	3	1101 0001	0101 0001
110 1001	4	0110 1001	1110 1001
111 1111	7	1111 1111	0111 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 make the parity bit appear correct even though the data is erroneous.

12.2.1.1.3 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 [168].

Cyclic codes have favourable properties as they are well suited for detecting burst errors (a burst error is a continuous sequence of data containing errors.) 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 12-4 provides some examples of commonly used CRCs and the applications they apply to.

Table 12-4: 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.

Figure 12-1 gives 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:

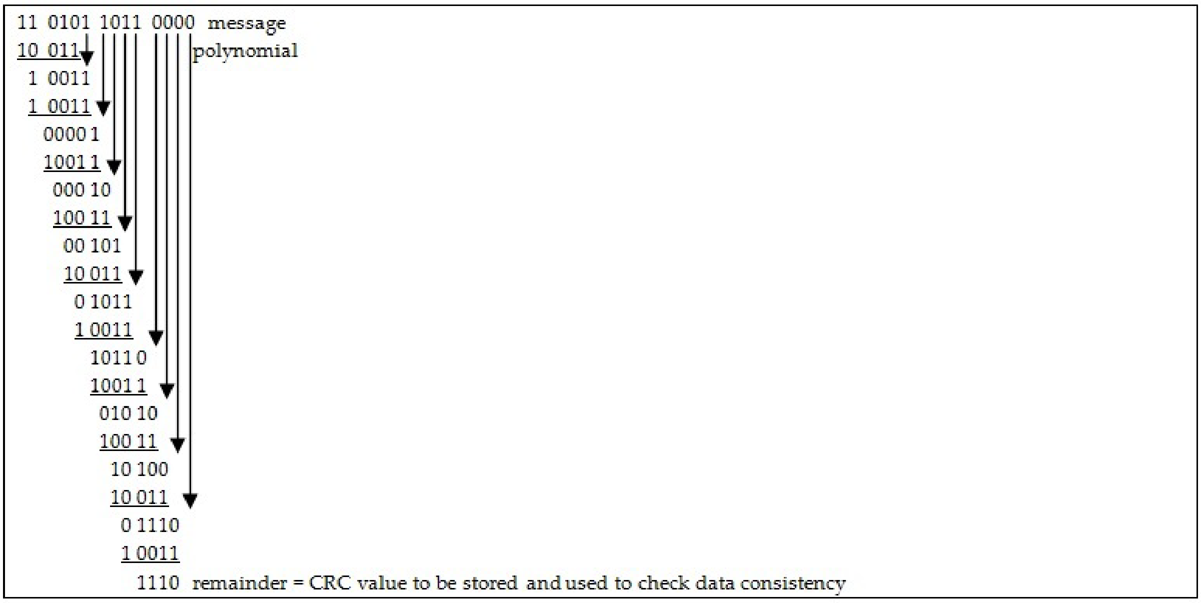


Figure 12-1: Example of a CRC computation on a binary message "1101011011"

12.2.1.1.4 BCH codes

BCH codes [226], [168], [229] 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 12.2.1.1.7, 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 (syndrome decoding is a highly efficient method of decoding a linear code over a noisy channel). This allows very simple electronic hardware to perform the task, obviating the need for a computer, and meaning that a decoding device can 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.

12.2.1.1.5 Hamming codes

Hamming codes were introduced 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 [168].

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 is not greater than one to be correctable. This means that for transmission medium situations where burst errors do not occur, Hamming's (7,4) code is effective (as the medium can 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 are not detectable. The (3,1) repetition has a distance of 3, as at least three bits are flipped in the same triplet 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.

12.2.1.1.6 SEC-DED codes

As a single error correcting code is not 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 three, 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. There are many good publications explaining SEC-DED codes, for example [309] and [310].

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 can also be used to detect up to 3 errors but not correct any.

12.2.1.1.7 Reed-Solomon codes

Reed–Solomon (RS) codes [168] are non-binary cyclic error-correcting codes invented by Reed and Solomon. They described a systematic way of building codes that can 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 can 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 [230].

12.2.1.1.8 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 12-2 depicts an arithmetic function using an arithmetic code for error detection.

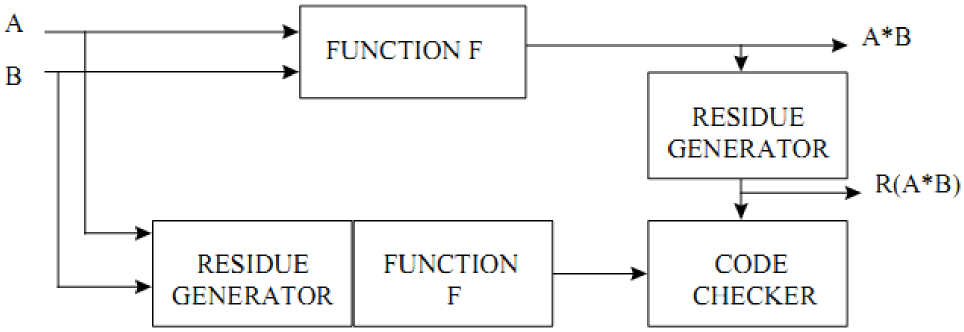


Figure 12-2: An arithmetic function using an arithmetic code as error detection mechanism

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 [7].

12.2.1.1.9 Low Density Parity Codes

This type of codes has been proposed to correct errors in high density memory blocks implemented in deep submicron technology that Table 12-5 can exhibit a high fault rate [311], [312]. Their high error correction capability, when compared to other ECC codes like Hamming, can be adjusted to find a compromise with operation speed and power consumption. An advantage of LDPC when compared to other high error correction rates codes such as Reed-Solomon or BCH is their simpler algebraic principles, making it easier to implement them in programmable logic arrays (e.g. FPGA) and using less computational time, and therefore being suitable as an error correction strategy with high speed memories.

Examples:

EDAC in LEON microprocessor: the Microchip Atmel space microprocessor AT697 device based on a LEON2FT IP Core and manufactured with 0,18 μm CMOS process can reach a frequency of 100 MHz. The large embedded memory blocks used for the register files, the data and instruction caches are sensitive to SEU, especially with a higher frequency of operation that increases the probability to latch SETs.

Among the error mitigation techniques applied in this device, 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.

12.2.1.2 Available test data (simulations, radiation testing, in-flight)

- References [231] and [232] provide synthesis and routing results for parallel Reed-Solomon encoders and decoders implemented in Microsemi and Xilinx FPGAs.
- Reference [232] presents Hamming and Reed-Solomon codes. Their improvements in data rate are compared to trade-offs in complexity and decoding lag. Different types of modulation are used to make comparisons in the performance of each ECC code.

12.2.1.3 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 corrected. Hamming codes use XOR logic extensively so timing closure and maximum operating frequency will be affected if encoding/decoding is done in the critical path. The EDAC data path can always be registered first, and then proceed with the decoding and error correction in order to pipeline the operation.

The brief summary of key characteristics for error correcting codes is given in the Table 12-5.

Table 12-5: Summary of key characteristics for error correcting codes

Abstraction level	Circuit 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	GECO (Automatic Generation of Error Control Codes for Computer Applications)[233]

12.2.2 Mitigation for Memory Blocks

Memory blocks (arrays of bit memory cells) can be a very sensitive part inside our IC with respect to radiation effects, since they often exhibit a very high density of memory units, and are therefore a priority when trying to reduce SEU effects. Mitigation strategies based on spatial redundancy (duplication or triplication) are usually not well suited for large arrays of memory cells because of the high area cost. A less area costly alternative solution is the use of error correction codes (see section 12.2.1) often combined with “bit-interleaving” or “data scrambling”. The ECC ensures that single bit data corruption within a given bit data group (for example the words being written and read out of the memory block) can be detected and corrected. The “bit interleaving” technique aims at preventing that when a single ion hit provokes several physically adjacent bit flips (Multiple Cell Upset or MCU) inside the memory bank, those close-by bits do not belong to the same data group (word) that the EDAC logic is protecting. If that was the case, we were talking about having a Multiple Bit Upset or MBU (see 4.3.3.2.3).

EDAC can normally only restore words where only one bit got corrupted, hence the usefulness of adding bit interleaving as a complementary mitigation technique, in particular when the technology and physical architecture of the memory array are such that the probability of MCUs is considered high enough as to pose a risk for the good functioning of the system and the environment where the IC is used.

Bit-interleaving is described in detail in section 12.2.1.

12.2.3 Filtering SET pulses in data paths

12.2.3.1 Description of the concept

SET pulses can be filtered away by introducing dedicated filtering circuitry in the data path that leads to the memory elements that are meant to latch and store this data. There are multiple alternatives, depending on the types of SETs pulses (their time width and voltage amplitude) that are expected and that want to be filtered. There are many patented solutions.

In addition to the SET filtering introduced deliberately by the circuit designer, "natural" fault masking of SETs can occur depending on where exactly and when the SET occurs in the circuit, and what are the logical inputs affecting the logic at the time the SET is generated and/or propagating. We can distinguish three main typical types of natural fault masking where the SET does not propagate too far as to result in a functional error that becomes visible at the circuit final outputs:

- **Logical masking** occurs, for example, when a SET provoked by a particle is not propagated to an output due the inputs values. Figure 12-3 illustrates the logical masking phenomenon for an AND and an OR gate. Whenever the AND gate input is "0" it naturally rejects the transient (Figure 12-3(a)), and when one input is set to "1" the SET is able to propagate (Figure 12-3(b)). For the OR gate, the SET propagates with an input set to "0" (Figure 12-3(d)) but is masked when the input is "1" (Figure 12-3(c)).

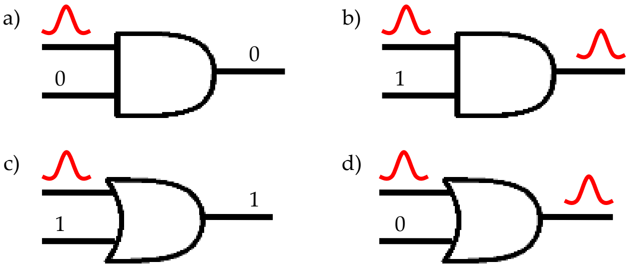


Figure 12-3: Logical masking of a transient in two logical gates

- **Electrical masking** occurs, for example, if the SET is attenuated as it propagates along a path until it does not affect anymore the circuit result. Such a phenomenon is illustrated in Figure 12-4 where a SET is attenuated by each gate. When it reaches the flip-flop, the pulse's amplitude is not sufficient to create an error.

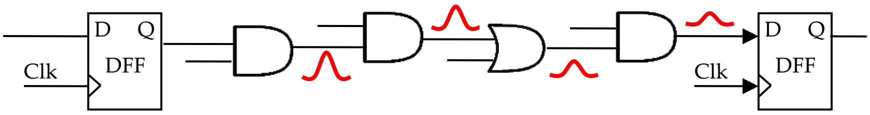


Figure 12-4: Electrical masking along a path in combinatorial logic

- **Temporal masking** occurs, for example, if an SET reaches a memory element at an instant other than the clocking window. Figure 12-5 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 rising edge. At instant T2 the SET occurs in the same time than the clock pulse and thus modifies the content of the memory cell. The resulting error can propagate to the circuit output. In this case the SET transforms itself into a Single Event Upset (SEU) also called bit-flip or soft error.

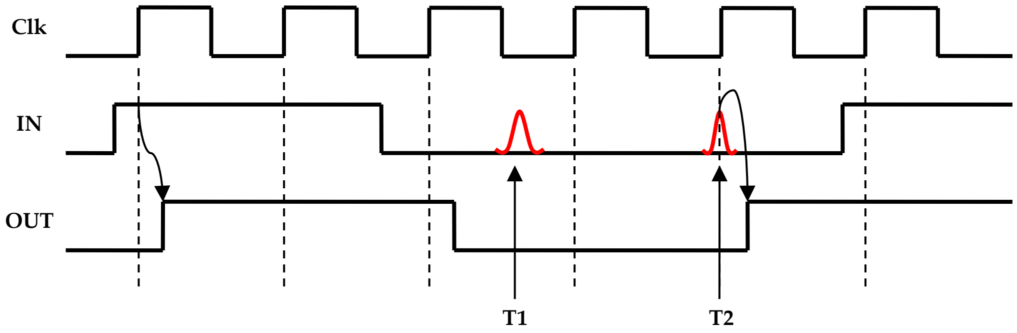


Figure 12-5: Temporal masking

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

There are many patented SET filter solutions. For example:

- Single event transient mitigation and measurement in integrated circuits, by Actel Corporation (now Microsemi), US7772874, Aug 2010, [327]
- Method and system for reducing glitch effects within combinational logic, by Honeywell International, Inc., US7193451, Mar 2007, [328]

In this paper [329], Actel (now Microsemi) presented novel SET filtering approaches that where carefully tested in preparation for their Flash-based RTA3P FPGAs. The SET filtering is done, as depicted in Figure 12-6, by a dual lane delay line and a guard gate that is be placed immediately before the memory cell.

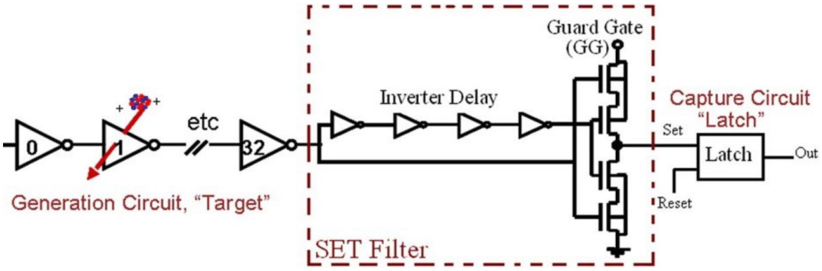


Figure 12-6: SET Filter proposed by Actel Corporation for their Flash-based FPGAs, as per S. Rezgui et al. in [329]

12.2.3.2 Available test data (simulations, radiation testing, in-flight)

As presented in [329], SET pulse widths were measured and SET cross-section calculated on an 130 nm CMOS Flash-based FPGA, independently of the frequency. The obtained results showed that SET pulse widths for LET < 43 MeV*cm^2/mg shorter than 3 ns. Beyond this LET, SET pulse widths can be wider than

3 ns but always shorter than 4 ns; but with a very low underlying cross-section (cm /smallest cell unit). Wide SET event (that can last for 250 ns) was also observed on the enable signal of each single IO bank. The efficiency of the proposed SET filters was proven and validated in beam. No FPGA's reconfiguration was performed due to beam irradiation.

12.2.3.3 Added value (efficiency)

Eliminating unwanted SETs in the data paths prevents that they are latched further down the signal propagation and storage line and thus transform themselves into anomalous memory states. This anomalous memory states can only be eliminated when the good data is refreshed by a clock.

12.2.3.4 Known issues (weaknesses, elements to be considered)

SET filtering extra combinatorial logic always results in a higher IC area, higher power consumption and some degradation in timing performance.

The brief summary of key characteristics for filtering SET pulses in data paths is given in the Table 12-6.

Table 12-6: Summary of key characteristics for filtering SET pulses in data paths

Abstraction level	Circuit architecture
Pros	Mitigate that SET transform into SEUs
Cons	Area, power and timing overheads
Mitigated effects	SETs that can transform into SEUs
Suitable validation methods	Accelerated ground tests SET fault injection (inserting SET pulse generators), netlist inspection

12.2.4 Watchdog timers

12.2.4.1 Description of the concept

Systems based on a processor IC can suffer service or functional interruptions (SEFIs) due to many reasons; one of them being the effect of radiation. In such a case the system is able to recover a normal operating mode on its own. Watchdog timers either:

- perform a hard reset of a sub-system inside the IC, or
- flag the existence of a radiation induced anomaly through an output signal of the IC in order to let the circuitry outside the IC do something about it (see section 14) whenever some signals which are constantly being monitored by the watchdog timer are not detected as they were expected, thus indicating that there was a radiation induced problem (corrupted data, resulting in erroneous information or wrong states in control circuits.

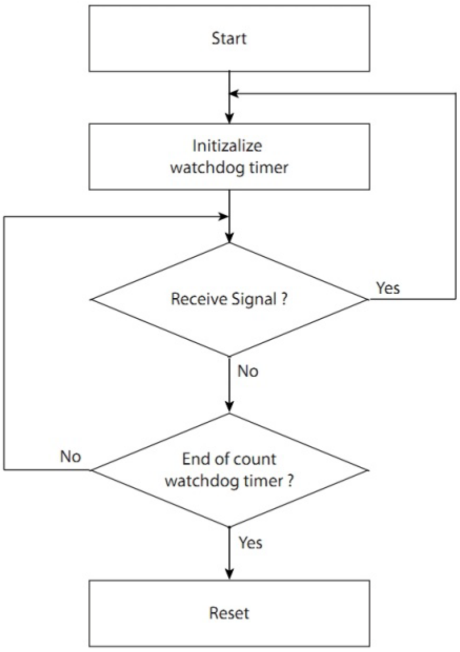


Figure 12-7: Watchdog Timer

Reference [214] 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 is to 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 can 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.

12.2.4.2 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*cm^2/mg

Radiation data results about the H-Core were published for three commercial microprocessors: Intel Pentium III, Texas Instruments TMS320C6713 and Equator BSP-15 [215]. In all the cases H-Core was able to recover the system after a SEFI.

12.2.4.3 Known issues (weaknesses, elements to be considered)

The watchdog timer is a critical part of the system because if an SET or an SEU alters its normal function, the whole system can become inoperable. Therefore, it is very important to design a reliable watchdog using rad hard cells and/or TMR.

The brief summary of key characteristics for watchdogs timers is given in the Table 12-7

Table 12-7: Summary of key characteristics for watchdog timers

Abstraction level	Circuit architecture, Electronic system
Pros	SEFI recovery: 100%
Cons	Area overhead: watchdog circuitry
Mitigated effects	SEFI
Suitable validation methods	Accelerated ground tests HW/SW fault injection

12.2.5 TMR in mixed-signal circuits

12.2.5.1 Description of the concept

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 11.2.1.

The TMR approach was adopted in [150] where a single voltage comparator was replaced by three parallel comparators driving a CMOS majority-voting block, as shown in Figure 12-8. The voting circuit was hardened by oversizing the transistors [93], [150].

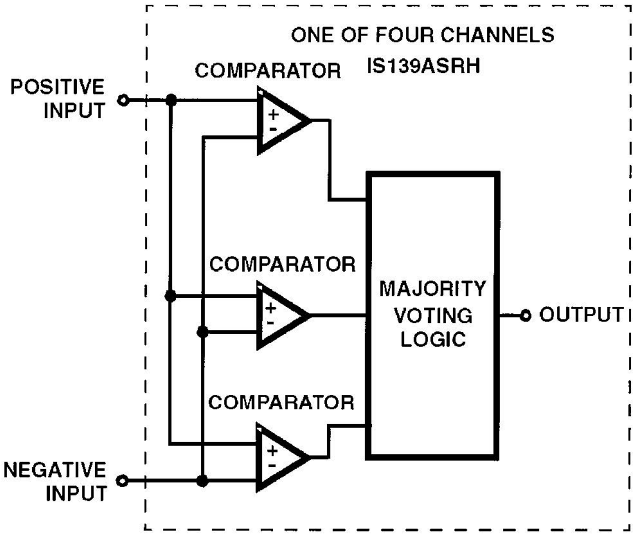


Figure 12-8: Functional block diagram of the IS139ASRH SEE-hardened voltage comparator

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.

12.2.5.2 Available test data (simulations, radiation testing, in-flight)

Reference [152] presents an evaluation of the trade-offs 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 pipeline. 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 uses an arbitrary SE injection rate, this technique does allow for comparisons between designs. Figure 12-9 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 12-9 indicates that the application of Comparator TMR to the first half of the 10-bit pipelined ADC produces the best trade-off 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.

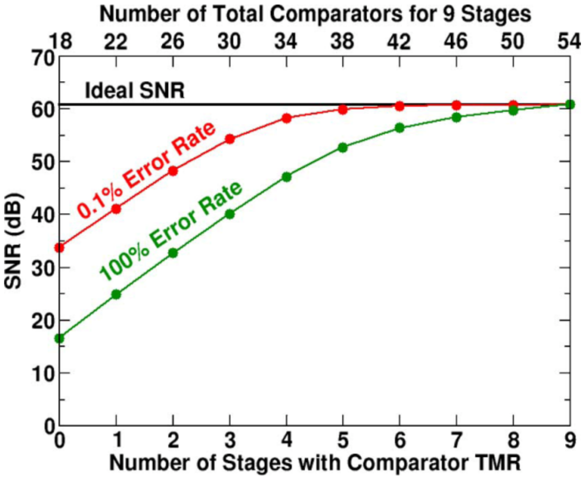


Figure 12-9: Signal-to-noise (SNR) ratio improvement when increasing use of Comparator TMR in a 10-bit pipelined ADC

12.2.5.3 Added value (efficiency)

SET mitigation, SNR improvement

12.2.5.4 Known issues (weaknesses, elements to be considered)

- Area penalty: ~3x + majority voter

- Power consumption penalty: ~3x + majority voter
- The brief summary of key characteristics for TMR in mixed-signal circuits is given in the

Table 12-8: Summary of key characteristics for TMR in mixed-signal circuits

Abstraction level	Electronic system
Pros	SET mitigation, SNR improvement
Cons	Area penalty: ~3x + majority voter Power consumption penalty: ~3x + majority voter
Mitigated effects	SET
Suitable validation methods	Accelerated ground tests, fault injection

13
Field programmable gate arrays

13.1 Overview

Since FPGAs are intended to host user's digital designs inside, most of the mitigation techniques described in Section 11 (Digital Design) and Section 12 (SoC) are readily applicable to FPGAs as well. This Section contains a list of mitigation techniques that are either specific for FPGA only, or that even if they are used also in ASICs, are worth mentioning again shortly to indicate specific considerations for their use with FPGA technology.

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 13-1).

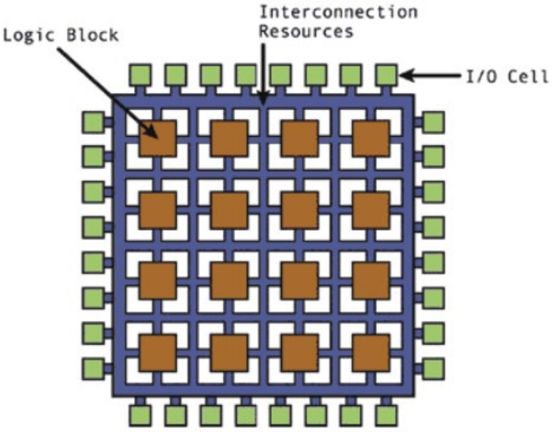


Figure 13-1: High-level description of an FPGA structure

Logic blocks can be configured to perform complex combinatorial functions (combinatorial 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 13-2): 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 or 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 can

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

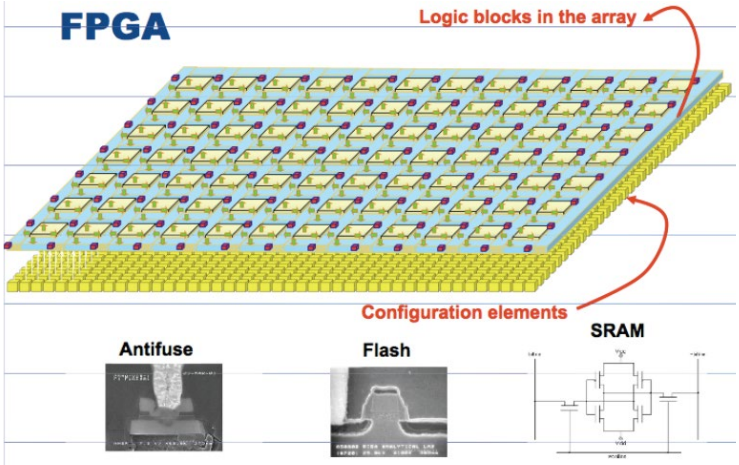


Figure 13-2: Schematic representation of the two layers composing an FPGA

Table 13-1 summarizes for each family the main characteristics and representative manufacturers of FPGAs available on the market.

Table 13-1: 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	Cobham (former Aeroflex) Microsemi	Microsemi	Xilinx Microchip Atmel

NOTE: A few other companies (e.g. Altera, Lattice) manufacture SRAM-based FPGAs. However, they have not proposed until now a radiation hardened FPGA solution. Consequently, section 13 addresses only SRAM-based FPGAs manufactured by Xilinx and Microchip Atmel.

A summary of mitigation techniques and the radiation effects they address is given in Table 13-2

Table 13-2: Summary of mitigation techniques for FPGAs and the radiation effects they address

Mitigation techniques	Radiation effects

		SET	SEU
13.2.1	Local Triple Modular Redundancy		X
13.2.2	Global Triple Modular Redundancy	X	X
13.2.3	Large grain Triple Modular Redundancy	X	X
13.2.4	Embedded user memory Triple Modular Redundancy	X	X
13.2.5	Additional voters in TMR data-paths to minimise DCE	X	X
13.2.6	Reliability-oriented place and Route Algorithm (RoRA)	X	X
13.2.7	Embedded processor protection	X	X
13.2.8	Partial reconfiguration or Scrubbing of configuration memory		X

13.2 Mitigation techniques

13.2.1 Local Triple Modular Redundancy

13.2.1.1 Description of the concept

Triple Modular Redundancy (TMR) is an architecture belonging to the spatial redundancy which is presented in detail in section 11.2.1. 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.

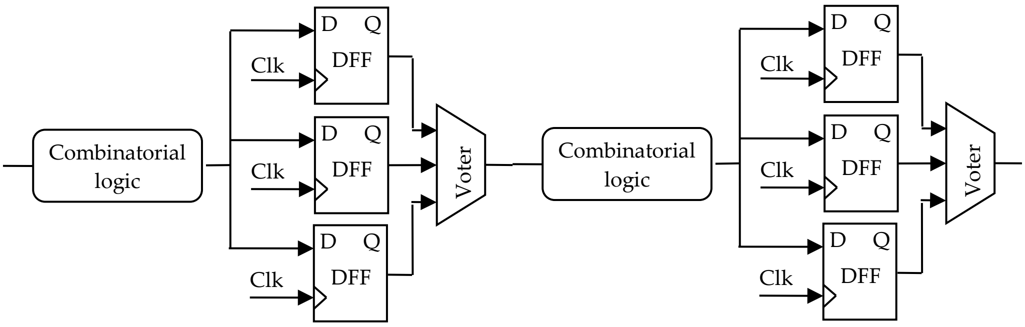


Figure 13-3: Local TMR – single combinatorial logic but triplicated registers

The local TMR technique (Figure 13-3:) consists in triplicating only flip-flops and voting their outputs. Some vendors offer FPGAs with flip-flops that have already been hardened at transistor level (see these techniques in 9.2.1) so that the FPGA user can think of these flip-flops as “locally-TMRed-FFs” (e.g. Microsemi RTAX-S/SL and Microsemi RTSXS). Figure 13-14 is extracted from Microsemi RTAX Radiation-Tolerant FPGAs Data Sheet [332] and illustrates how this local TMR is implemented by the vendor in this case. In other cases where FPGAs that do not embed a local hardening scheme for their flip-flops (e.g. commercial grade FPGAs) local TMR can be applied by the FPGA user in the HDL description of the IC design. This simplest TMR technique can be used for designs running at low frequencies and thus with low probability of capturing SETs in the flip-flops. Some examples of how the implementation of this technique can be done in legacy devices of Microsemi are given in reference [153].

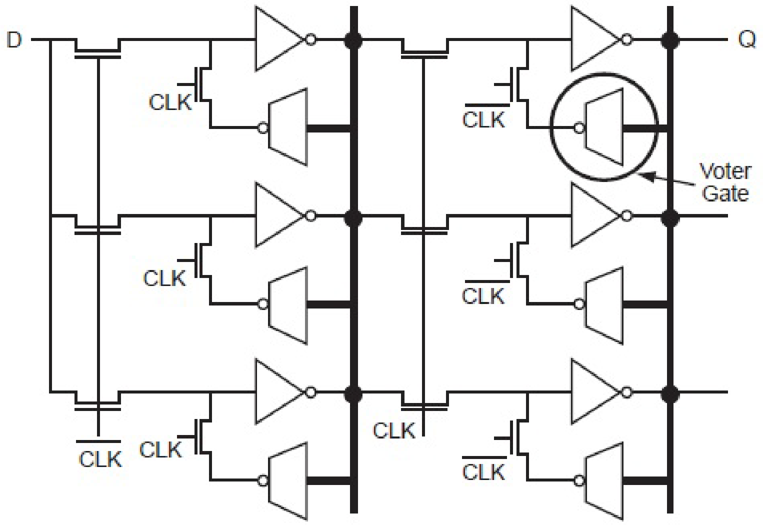


Figure 13-4: RTAX-S/SL/DSP R-cell Implementation of D Flip-Flop Using Voter Gate Logic

13.2.1.2 Available test data (simulations, radiation testing, in-flight)

Experimental data obtained on the Microsemi RTAX-S anti-fuse based FPGA which implements TMR at each flip-flop is presented in reference [154]. 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.

13.2.1.3 Added value (efficiency)

- The advantage of a local TMR is that the area penalty is limited to registers as combinatorial logic is not replicated.
- This technique helps mitigating upsets in the user’s logic.

13.2.1.4 Known issues (weaknesses, elements to be considered)

Local TMR protects against SEUs in the flip-flops (FF). However an SET occurring in the combinatorial logic propagates to the FFs and if concurrent with the sampling clock pulse the error is latched and the voter has three identical, but false, results and consequently it does not detect the error. A solution to this issue is the “global TMR” strategy (see section 13.2.2).

Local TMR is not protects against a Multiple Bit Upset (MBU) that affects flip-flops of the same TMR triplet [155].

This technique does not protect against upsets in the “configuration logic” when the FPGA uses SRAM or EEPROM configuration memory cells, which cannot be hardened by the user by applying local TMR. Other hardening techniques can however be applied by the vendor, like in the case of Xilinx XQRV5.

The brief summary of key characteristics for local Triple Modular Redundancy is given in the Table 13-3.

Table 13-3: Summary of key characteristics for local Triple Modular Redundancy

Abstraction level	Circuit architecture
Pros	mitigate SEU in registers
Cons	Area penalty: 3 times more flip-flops plus the additional voting logic per triplet.
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests HW/SW fault injection HDL simulation
Automation tools	Mentor Precision Rad-Tolerant, Xilinx XTMR, Synopsys Synplify

13.2.2 Global Triple Modular Redundancy

13.2.2.1 Description of the concept

Global TMR is based on the spatial redundancy concept detailed in section 11.2.1. 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 13-5 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 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 [156]. 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. Other voting techniques can also be implemented with the redundant outputs at board level, thus completing the mitigation strategy with "system level" (off-chip) measures.

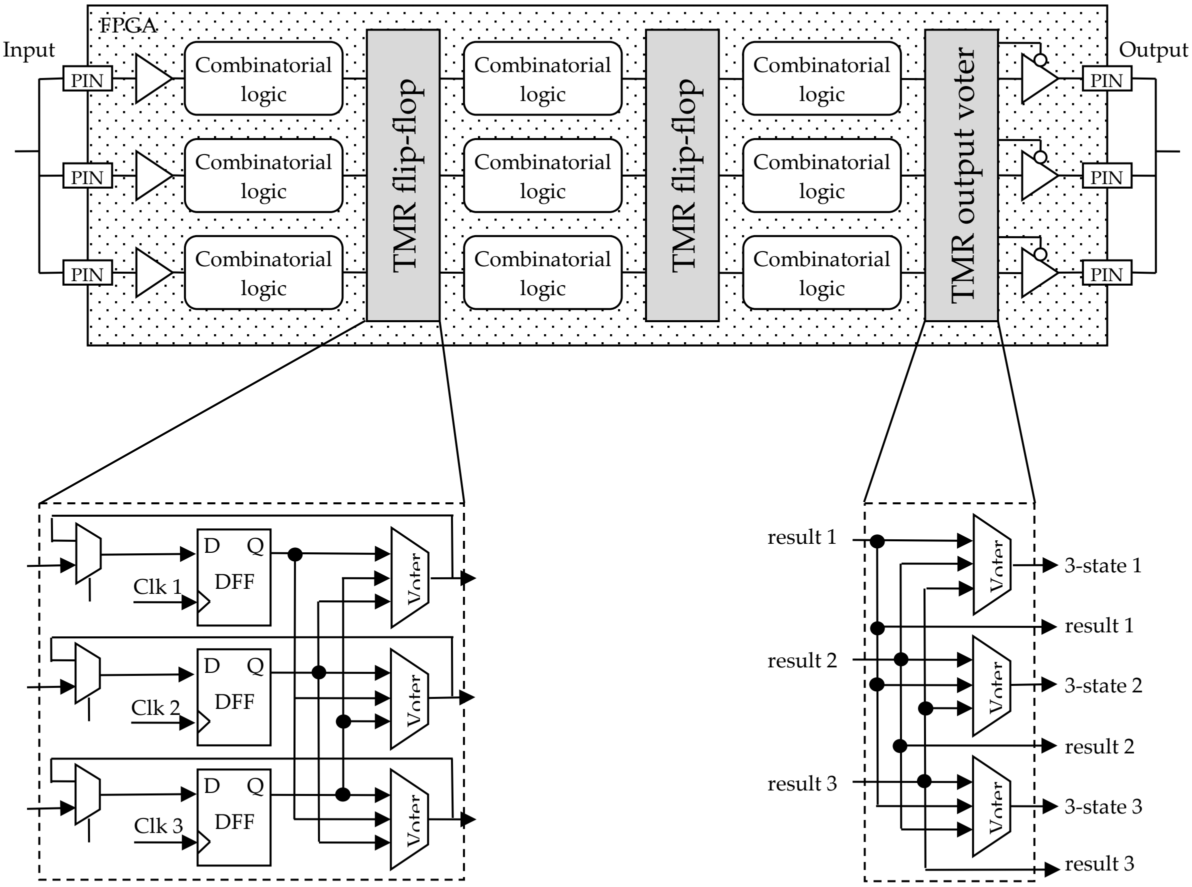


Figure 13-5: Global TMR implemented in an FPGA

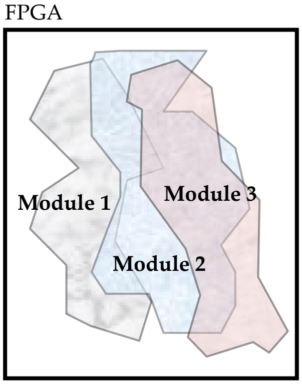


Figure 13-6: Physical implementation of global TMR inside an FPGA

13.2.2.2 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 [155].

There are several radiation reports available at ESCIES repository of Xilinx Virtex-II using XTMR mitigation technique, such as[333] or [334].

13.2.2.3 Added value (efficiency)

- Protect whole design from SET in combinatorial logic and SEU in registers.
- This technique helps to mask but not to correct upsets in the configuration memory.

13.2.2.4 Known issues (weaknesses, elements to be considered)

Global TMR implies 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 13-6: illustrates how a design using TMR looks like once implemented in an FPGA: the three replicas overlap and FPGA resources from the three domains are mixed within the same logic blocks. This has two main consequences: the first is that partial scrubbing (see section 13.2.8) cannot be used and the second is the increase of the risk to encounter domain crossing events (see section 13.2.5).

The brief summary of key characteristics for global Triple Modular Redundancy is given in the Table 13-4.

Table 13-4: Summary of key characteristics for global Triple Modular Redundancy

Abstraction level	Circuit architecture, Electronic system
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

13.2.3 Large grain Triple Modular Redundancy

13.2.3.1 Description of the concept

Large grain TMR is based on the spatial redundancy concept presented in section 11.2.1. 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 13-7).

One challenge of the large grain TMR is to resynchronize an erroneous replica with the others. This is done as follows[157]:

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

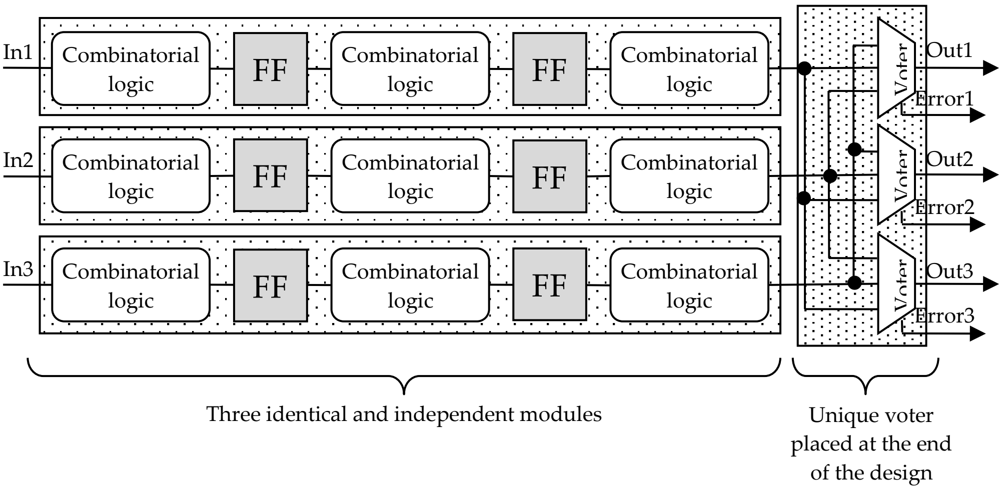


Figure 13-7: Large grain TMR

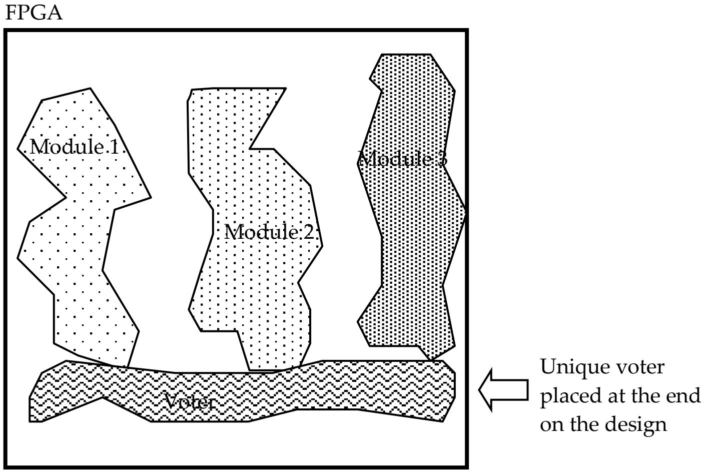


Figure 13-8: Physical implementation of a large grain TMR inside an FPGA

13.2.3.2 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 [155].

13.2.3.3 Added value (efficiency)

- Local placement and routing for each TMR redundant domain allowing physical separation of each replica as illustrated in Figure 13-8.
- A consequence of the previous mentioned added value there is the possibility of using partial reconfiguration (see section 13.2.8 to scrub only a redundant domain that has the error, thus, reducing the scrubbing time and energy.
- Minimal points of domain crossing (see section 13.2.5) means reduced vulnerable bit-flips that can upset the TMR.
- This technique helps mitigating upsets in the configuration memory and in the user logic.

13.2.3.4 Known issues (weaknesses, elements to be considered)

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

The brief summary of key characteristics for large grain Triple Modular Redundancy is given in the Table 13-5.

Table 13-5: Summary of key characteristics for large grain Triple Modular Redundancy

Abstraction level	Circuit architecture
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; Xilinx IDF,IVT and SEM IP

13.2.4 Embedded user memory Triple Modular Redundancy

13.2.4.1 Description of the concept

Embedded user memories, such as BRAM (Block SelectRAM) memories in Xilinx FPGAs, are resources available for the designers. Those memories are based on SRAM cells and are consequently sensitive to SEEs. Hence, a special care from the designers is important as the configuration memory scrubbing techniques cannot protect them from SEUs (see section 13.2.8). The proposed mitigation technique consists in applying the TMR concept combined with a refreshing mechanism of their content [156].

Data refresh is only necessary if long time storage is needed. Depending on the radiation requirements and the number of expected bit-flip anomalies, for “short time” storage (e.g. FIFO) data refresh is not necessary.

Figure 13-9 illustrates an example of implementation in Xilinx FPGAs using counters (that we want to protect) 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 can be dedicated to error detection and correction. But this also means that the BRAM can only be used as single port memories by the rest of the user logic. To refresh the memory contents, a counter can 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.

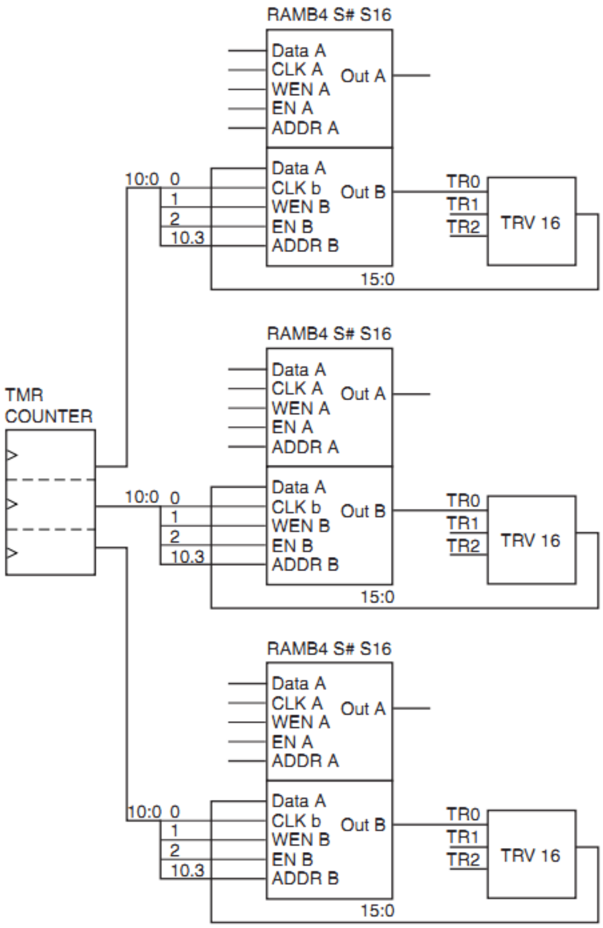


Figure 13-9: BRAM TMR

13.2.4.2 Added value (efficiency)

This technique helps mitigating upsets in the configuration memory that have an influence in the user memory and in the user logic.

13.2.4.3 Known issues (weaknesses, elements to be considered)

Area penalty: ~3x (memory only), but also the counters and voting additional logic. If the memory size is small, the triplication can take place one same memory block. Other mitigation techniques, such as EDAC (see sections 12.2.1 and 12.2.2), can consume less FPGA resources, depending on the actual size of the memory blocks to be protected, and the ancillary logic to be added around.

The brief summary of key characteristics for embedded user memory Triple Modular Redundancy is given in the Table 13-6.

Table 13-6: Summary of key characteristics for embedded user memory Triple Modular Redundancy

Abstraction level	Circuit architecture, Electronic system
Pros	Increased SEU hardness
Cons	Area penalty: ~3x (memory only)
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests HW/SW fault injection

13.2.5 Additional voters in TMR data-paths to minimise DCE

13.2.5.1 Description of the concept

13.2.5.1.1 General

This technique is intended to reduce the probability of occurrence of Domain Crossing Events (DCE) [158]. To understand the problem, domain crossing events are first explained. Then the voter insertion technique is presented.

13.2.5.1.2 Domain Crossing Events

Domain Crossing Events occur in applications mitigated by TMR when two replicas of the same TMR group are corrupted by SEE in the configuration memory of the FPGA. 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 same TMR group.
- When multiple bit upsets (MBU) occur within the same TMR group 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 can create an error within the same replica of the TMR. In this case as illustrated in Figure 13-10, the voter is still able to reject the fault because the two other replicas are still able to provide correct results.

A routing defect can 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 propagates 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 13-11, the TMR flip-flops of a full TMR design uses frequent interconnections between the different replicas of the TMR, thus the replicas cannot be physically separated inside the FPGA.

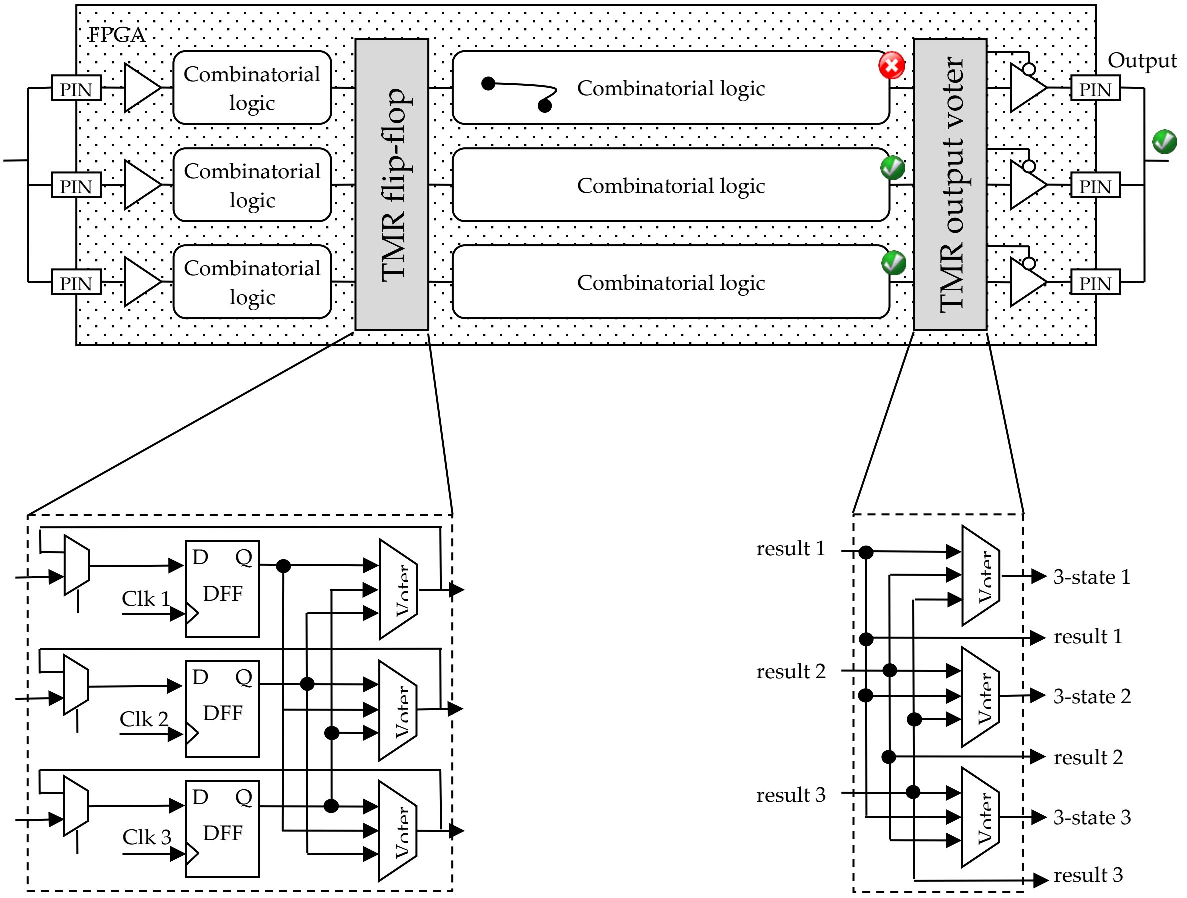


Figure 13-10: Routing defect within the same module

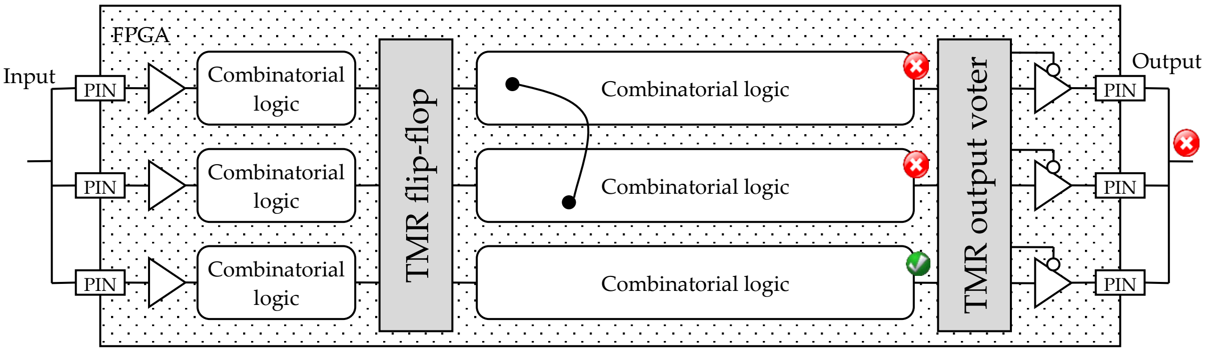


Figure 13-11: Domain Crossing Event as a consequence of routing defect affecting two different modules

One solution to reduce the risk of DCE is to physically separate the TMR domains as illustrated in Figure 13-8. However, this is almost impossible to apply to a local or a global TMR (see sections 13.2.1 and 13.2.2). Thus, the voter insertion technique is intended for these cases.

13.2.5.1.3 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 13-11).

Figure 13-12 illustrates the voter insertion technique applied to the example provided in Figure 13-11 where a DCE provokes an error in the combinatorial 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.

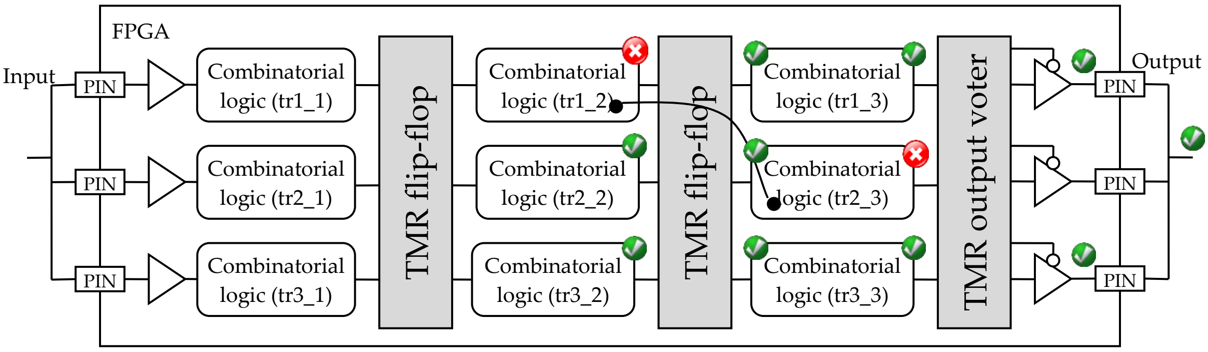

FPGA
Input
PIN
PIN
PIN
Combinatorial logic (tr1_1)
Combinatorial logic (tr2_1)
Combinatorial logic (tr3_1)
TMR flip-flop
Combinatorial logic (tr1_2)
Combinatorial logic (tr2_2)
Combinatorial logic (tr3_2)
TMR flip-flop
Combinatorial logic (tr1_3)
Combinatorial logic (tr2_3)
Combinatorial logic (tr3_3)
TMR output voter
Output
PIN
PIN
PIN

Figure 13-12: Inserting voters reduces the risk of domain crossing events

13.2.5.2 Available test data (simulations, radiation testing, in-flight)

For the case study in [158] circuit, the best partition is the medium partition (TMR_p2). This version of the TMR design presents a small sensitivity to routing upsets (0,98 %, a four times improvement over normal TMR) and small performance degradation (about 10 %) compared to the standard version (not protected*)*.

13.2.5.3 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.

13.2.5.4 Known issues (weaknesses, elements to be considered)

A large number of voters does not always mean larger protection against upsets. There is an optimal logic partition for each circuit that can reduce the propagation of the upset effect in the routing [158]**.**

The brief summary of key characteristics for additional voters in TMR data-paths to minimise DCE is given in the Table 13-7.

Table 13-7: Summary of key characteristics for additional voters in TMR data-paths to minimise DCE

Abstraction level	Circuit architecture
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

13.2.6 Reliability-oriented place and Route Algorithm (RoRA)

13.2.6.1 Description of the concept

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 combinatorial 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 [159], and extensive fault-injection experiments [160], have put in evidence that one SEU can 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 [159] and [160] report that about 10 % of the faults that can affect the FPGA routing resources produce multiple errors that the TMR is not able to mask [160]. As shown in [158], 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) [161] was developed (initially for Xilinx FPGAs, later being extended to other SRAM and Flash based FPGAs) in order to optimize the place and route process in the design flow in a way that minimises the Domain Crossing Evens already explained in 13.2.5. 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 13-13 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 Xilinx 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 [162].

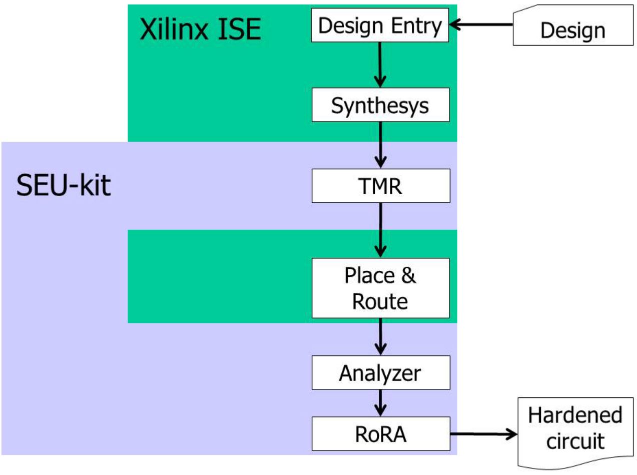


Figure 13-13: RoRA's design flow

13.2.6.2 Available test data (simulations, radiation testing, in-flight)

RoRA's effectiveness in Xilinx FPGAs was evaluated on some benchmark circuits by means of fault-injection experiments in the FPGA's configuration memory. The results exposed in reference [162] 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.

13.2.6.3 Added value (efficiency)

- RoRA can increase hardness to SEUs in SRAM FPGA designs by a factor up to 85 compared to a "standard" (without RoRA) 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, only additional automatic design steps.
- This technique helps mitigating upsets in the configuration memory (that can impair the existing TMR in the user flip-flops) and in the user logic.

13.2.6.4 Known issues (weaknesses, elements to be considered)

Performance penalty: ~22 %

The radiation tolerance improvement figures observed so far [162] vary up and down, depending on the actual functions implemented inside the FPGA.

The brief summary of known issues for reliability-oriented place and route algorithm are given in Table 13-8.

Table 13-8: Summary of key characteristics for reliability-oriented place and route algorithm

Abstraction level	Electronic system
Pros	No area penalty
Cons	Performance penalty: ~22 %
Mitigated effects	SEU
Suitable validation methods	Accelerated ground tests HW/SW fault injection
Automation tools	University di Torino RoRA and Veri-Place tools

13.2.7 Embedded processor protection

13.2.7.1 Description of the concept

13.2.7.1.1 Overview

The latest FPGA families embed hardwired processors which are sensitive to SETs, SEUs and SEFIs since these FPGAs are, as of today (2014), only implemented in commercial processes without any built-in protections against radiation effects. Several techniques are possible to mitigate radiation effects in the embedded processor function:

- Purely software-based approaches as what is presented in section 14. Those techniques generally imply little hardware overhead but modifications of the software.
- Spatial redundancy-based solutions involving multiple processors are presented at electronic system level in section 15.2.5. They have 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 [163].

Other parts of these "commercial" FPGAs (e.g. configuration memory or power up logic) that are also vulnerable to radiation effects that need, in most space application cases, additional mitigation (e.g. scrubbing of reconfiguration memory), as explained in the rest of Sections 10 and 12.

13.2.7.1.2 Software-based techniques

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

13.2.7.1.3 Spatial redundancy

Dual-Modular Redundancy such as Lockstep or DT2. (see Section 15.2.5).

13.2.7.1.4 Hybrid approach

This approach, presented in reference [163], mixes software and hardware modifications in order to achieve radiation tolerance. The architecture presented in Figure 13-14 presents the hardware modification part which consists in adding the I-IP module. This IP (Intellectual Property) core 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 [163]. It is important to ensure the robustness against radiation effects of the I-IP itself, using TMR or any other available mitigation techniques available to ensure enough reliability of this special IP core.

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

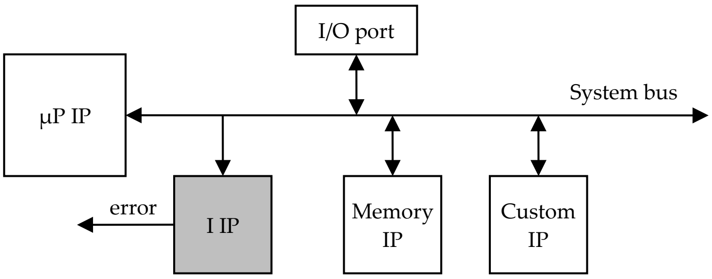


Figure 13-14: Hybrid architecture using a fault detection-oriented I-IP

13.2.7.2 Available test data (simulations, radiation testing, in-flight)

The hybrid technique was implemented on a Virtex-II Pro FPGA using the embedded PowerPC [163]. Both the processor and the I-IP core work at 100 MHz. The implementation of the I-IP module uses 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 100000 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.

13.2.7.3 Added value (efficiency)

- Mitigate SETs, SEUs and SEFIs
- This technique helps mitigating upsets in the configuration memory and in the user logic that ultimately have a negative effect in the embedded processor.

The brief summary of key characteristics for embedded processor protection is given in the Figure 13-9**.**

Table 13-9: Summary of key characteristics for embedded processor protection

Abstraction level	Circuit architecture
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

13.2.8 Partial reconfiguration or Scrubbing of configuration memory

13.2.8.1 Description of the concept

13.2.8.1.1 Overview

Spatial redundancy by itself is not sufficient to avoid radiation induced errors in SRAM-based FPGAs. Indeed, it allows rejecting transients in the combinatorial logic and upsets in registers (see sections 13.2.1 and 13.2.2). However, the configuration memory of SRAM-based FPGAs can be also sensitive to the effects of radiation, which can create a permanent malfunction of the circuit programmed inside the FPGA by changing, for example, the nature or performance of a logical function implemented in a LUT or the type of an IO port in use. In those cases when the configuration memory can be altered by radiation it is then very important to periodically reload the configuration bitstream of the FPGA in order to over-write the configuration bits with the good ones and to avoid the accumulation of faults in the configuration memory. This continuous loading of the bitstream is popularly called "scrubbing". Scrubbing, as explained in Xilinx Application Notes 138 and 151 [164], [165], allows a system to repair bit-flips in the configuration memory (including the memory cells that configure the LUT, the ones that control the routing and the CLB customization) 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 13-15, 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.

Due to the large sizes that the configuration memory can have compared to "user memory" (i.e. flip-flops and embedded memory cells) it is equally important, if not more, to protect against faults both in the configuration memory and in the user logic. As an example, the configuration memory for the Xilinx Virtex-6 family is about four to eight times larger than the user memory. It is important to notice that scrubbing is not sufficient to completely protect SRAM-based FPGAs from particle effects as it only avoids accumulation of faults in the configuration memory. Indeed, faults can occur between two scrubbing cycles and provoke errors in the application until the next refresh of the configuration memory. Moreover, scrubbing will not correct faults in user registers nor in embedded RAM. Consequently, it is important to apply additional mitigation techniques as a complement to scrubbing.

13.2.8.1.2 Full scrubbing

As explained in sections 13.2.1 and 13.2.2, 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.

13.2.8.1.3 Partial scrubbing

Large grain TMR (see section 13.2.3) 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 [166].

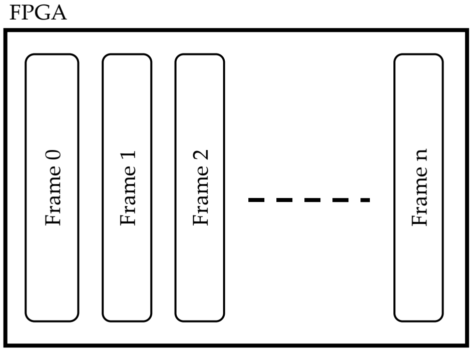


Figure 13-15: Organization of the configuration memory for the Xilinx Virtex family

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

Figure 13-16 illustrates a basic overview of an example of a possible implementation for an SEU correcting design by performing scrubbing. The memory storing the FPGA configuration is connected to the Virtex SelectMAP (a parallel interface used to configure and readback Xilinx FPGAs) interface through a configuration controller. This controller features a memory interface, a Cyclic Redundancy Check calculator and comparator (see section 12.2.1) and a finite state machine to control the operations.

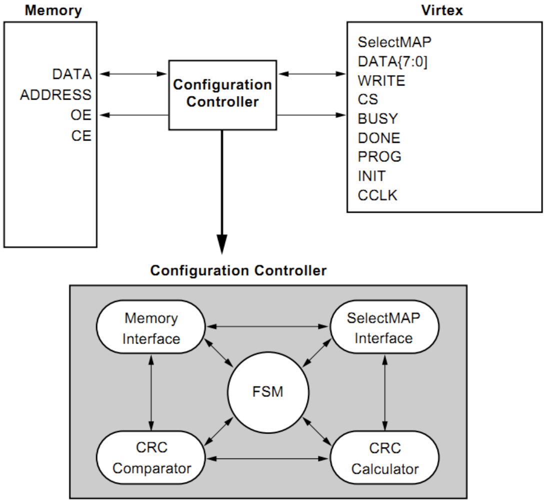


Figure 13-16: Simple configuration and SEU correction design

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 a dedicated scrubbing controller. The embedded processor hard core Power-PC or soft core Microblaze that can be available with some Xilinx FPGAs can be used as scrubbing controllers, but they are sensitive to radiation effects and it is therefore not recommended. 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 On-chip Peripheral Bus and the Embedded Development Kit tool can be used for that task.

13.2.8.1.4 Partial reconfiguration

As just explained in the "partial scrubbing" section 13.2.8.1.3, some SRAM-based FPGAs allow the user to perform a re-write of only a fraction of the reconfiguration bits. This can be done with different objectives. One objective can be to overwrite the bits of the configuration bitstream that may have been flipped by radiation with the good values (that have to remain safely stored in a memory device outside the FPGA), and then we would refer to this operation as "partial scrubbing".

But in addition to this strategy, the possibility of partially reconfiguring the FPGA can have other objectives, also linked to radiation effects mitigation. For example, if radiation has caused a permanent fault in a given area of the FPGA, and the user has been able to detect this, a possible mitigation technique could be to relocate the affected functions that were mapped in the faulty area to another area of the FPGA that free (not used) and fault-free. This strategy requires a dedicated partial reconfiguration controller, and logic to detect permanent-faults across used and unused areas of the FPGA. One example of such an strategy is "OLT(RE)^2"(On-Line on-demand Testing approach for permanent Radiation Effects in REconfigurable systems) [341], an on-line on-demand approach proposed by Bieleveld University to test permanent faults induced by radiations in reconfigurable systems used in space missions. OLT(RE)^2 exploits the partial dynamic reconfigurability mechanism offered by modern FPGAs to place special fault-detection test circuits [342] at runtime. The goal is to test unutilized areas of the FPGA fabric before using them, thus preventing functional modules of the reconfigurable system to be placed on faulty areas.

Dynamic partial reconfiguration can also be used to apply more or less amount of mitigation, depending on the known radiation environment conditions and/or how many radiation induced faults can be tolerated along the life of the space mission that the FPGA is serving. To achieve a reliable FPGA design, mitigation is applied according to the worst-case condition. The mitigation overheads (e.g. in performance, power consumption) during relaxed conditions can be optimised by not always applying mitigation for the worst case conditions. Adaptive mitigation in general and adaptive SEE mitigation in particular are introduced in [344] and [343].

13.2.8.2 Available test data (simulations, radiation testing, in-flight)

In reference [167], two versions of the Microblaze soft core processor, with and without BRAM scrubbing, but always using 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.

In reference [293], an internal ICAP configuration scrubber was implemented in a Virtex 4 FPGA and successfully demonstrated under high energy protons. The scrubber circuit was able to detect real-time failures in the bitstream and repair the bitstream when a single upset occurred within a frame. Both a standard non-triplicated scrubber and high reliable triplicated version of the scrubber were tested.

There are multiple publications summarising radiation test results that quantify the efficiency of scrubbing as mitigation, for example[335], as presented at RADECS 2001 for Virtex XQVR300.

Regarding dynamic partial reconfiguration mitigation techniques where permanent faults are detected and the functions relocated to a different unused area of the FPGA, experimental results have shown that OLT(RE)^2 may be applied to a large set of FPGA families and models, allowing faults both in physical wires and Programmable Interconnect Points (PIPs) to be detected, achieving a coverage rate of more than 98 % of the useable resources. Experiments carried out on a reconfigurable testbed (using Xilinx Virtex-4 FX100 FPGA) [340] demonstrated that the proposed approach is viable for space applications.

13.2.8.3 Added value (efficiency)

- Prevent SEU accumulation in the configuration memory.
- On recent Xilinx devices scrubbing can be achieved from inside the FPGA using the HardWare Internal Configuration Access Port (HWICAP), and an internal scrubbing controller, therefore not using an external processor for the scrubbing.
- The application is not interrupted.
- This technique helps mitigating upsets in the configuration memory but not in the user logic.
- Dynamic partial reconfiguration can also be used to mitigate radiation induced permanent faults caused by TID effects (combined with aging and wear out mechanisms). This could be particularly useful for non-rad hard FPGAs.

13.2.8.4 Known issues (weaknesses, elements to be considered)

- Partial reconfiguration and Scrubbing make use of an external controller to perform the new bitstream upload 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 user’s memories (e.g. BRAMs in Xilinx) nor in user’s flip-flops. A solution named BRAM TMR is recommended to cope with rad effects in embedded user memory (see section 13.2.4).
- Upsets occurring between two scrubbings can provoke errors. For this reason additional mitigation techniques such as TMR can be implemented in many cases as a complementary technique to scrubbing.
- Dynamic partial reconfiguration mitigation may involve having to store large amount of bitstreams, and maybe slow (generating, programming and running fault detection circuits before implementing the partial reconfiguration of the FPGA).
- Some permanent faults in some FPGA resources (e.g. user’s memory or DSP routing resources) may not be easy to detect.

The brief summary of key characteristics for a Scrubbing of configuration memory is given in the Table 13-10**.**

Table 13-10: Summary of key characteristics for scrubbing of configuration memory

Abstraction level	Electronic system
Pros	Restore good configuration bit values and avoid fault accumulation in the configuration memory. Mitigate permanent faults.
Cons	Can require an external controller and external memory to store good or alternative bitstreams
Mitigated effects	SEU, MBU/MCU, TID (combined with aging)
Suitable validation methods	Accelerated ground tests, fault injection

14 Software-implemented hardware fault tolerance

14.1 Overview

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. Mitigation techniques at this level imply modifications in the software used by the electronic system, although these modifications are not always suitable to all types of software (e.g. software which uses interrupts or dynamic memory allocation).

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 to Intellectual Property (IP) processors embedded in space ASICs or FPGAs, which either do not include any mitigation techniques for the radiation effects faults of concern or where not enough mitigation can be implemented in the hardware due to system requirements (e.g. power consumption or chip area occupation).

SIFT provides support by implementing an active time 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. In our context, instructions are understood as individual instructions or groups or blocks of instructions. Transients and upsets being the considered types of faults, redundancy is obtained by selectively duplicating 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.

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.

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 this section as well as in Section 15, can detect and recover from SETs occurring in the clock/reset lines.

A summary of mitigation techniques and the radiation effects they address is given in Table 14-1.

Table 14-1: Summary of effects versus mitigation techniques

Mitigation techniques		Radiation effects			
		SET	SEU	MBU	MCU
14.2.1	Redundancy at instruction level	X	X	X	X
14.2.2	Redundancy at task level	X	X	X	X
14.2.3	Redundancy at application level: using a hypervisor	X	X	X	X

14.2 Mitigation techniques

14.2.1 Redundancy at instruction level

14.2.1.1 Description of the concept

14.2.1.1.1 General

Temporal 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 (or an instruction block) n times and then comparing the results. A potential error occurring during one of the executions therefore would be detected. When n = 2 it is possible to detect faults, but not to correct them. In this case a third computation is used in order to determine the correct result. If n > 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 B3) and so on.

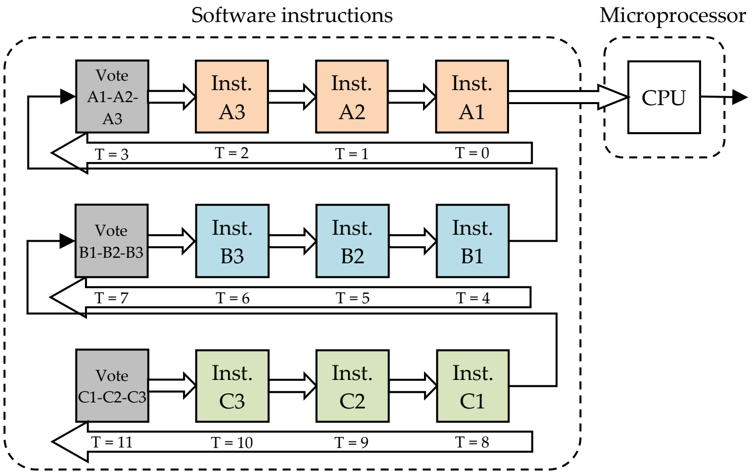


Figure 14-1: Temporal redundancy at instruction level

Temporal 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 is 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 are duplicated, so that both replicas R0 and R1 are updated.
- Arithmetic, logic and Boolean statements are replicated.
- All the data structures involved in read operations are checked for consistency by testing whether R0 and R1 match, after each read operation.

It is important that specific ordering of the instructions is 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 is disabled. The obtained executable code retains the needed redundant instructions, and preserves 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 is 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 is devoted to third-party code (software developed by someone else), 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, the particular care is placed in the consistency check function as rounding errors can apply. As a result, a threshold based acceptance test replaces 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 4.3.3.2.4) detection and recovery mechanisms.

14.2.1.1.2 Fault coverage:

SIFT techniques are able to detect up to 100 % of the Single Event Upsets affecting 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) cannot be detected.

14.2.1.1.3 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 use for data and execution flow faults.

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

- All the data structures in the original software are duplicated as explained before. 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 before.
- 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.

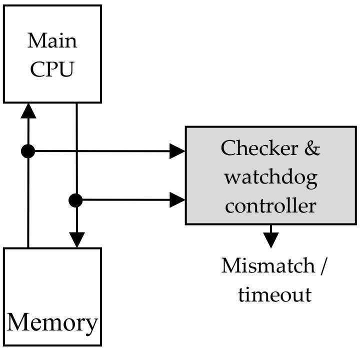


Figure 14-2: Optimized architecture for temporal redundancy applied at instruction level

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, see the fragment of C code reported in Figure 14-3.

```
#define N     100
int a[N];
int b[N];
int c[N];

void main( void )
{
  int   i;

  // a and b are initialized with input data

  for( i = 0; i < N; i++ )
  {
        c[i] = a[i]*b[i];
  }
}
```

Figure 14-3: Example of code

The code presented in Figure 14-3 implements the described before technique. All data structures (arrays and variables) are duplicated, and all the statements are duplicated. It is noticed that complex statements such as on line 11 of Figure 14-3 can contain read and write operations, and therefore the proper rules are 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" is 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 [192], [193], [194] and [195].

Examples:

a. Error Detection by Duplicated Instructions: the Error Detection by Duplicated Instructions (EDDI) approach developed by Stanford University [196], 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 on-board a satellite can be found in the "available test data" section 14.2.1.2.

b. Time-Triple Modular Redundancy: the Proton platform, by Space Micro, implements a technique, called Time Triple Modular Redundancy, combining spatial and temporal redundancy.

14.2.1.2 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 [197].

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 [198]:

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

14.2.1.3 Added value (efficiency)

Area overhead resulting by the use of the external checker and the watchdog is negligible when compared to other techniques like spatial redundancy.

14.2.1.4 Known issues (weaknesses, elements to be considered)

- Not compatible with third-party libraries, OS
- Errors during interrupt processing cannot be detectable
- Heavy software modifications
- Branching can render instruction level redundancy not possible

The brief summary of key characteristics for redundancy at instruction level is given in the Table 14-2.

Table 14-2: Summary of key characteristics for redundancy at instruction level

Abstraction level	Electronic system
Pros	Fault coverage: 100 % for data, >95 % for execution flow
Cons	Memory overhead and code size increase: >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

14.2.2 Redundancy at task level

14.2.2.1 Description of the concept

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

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

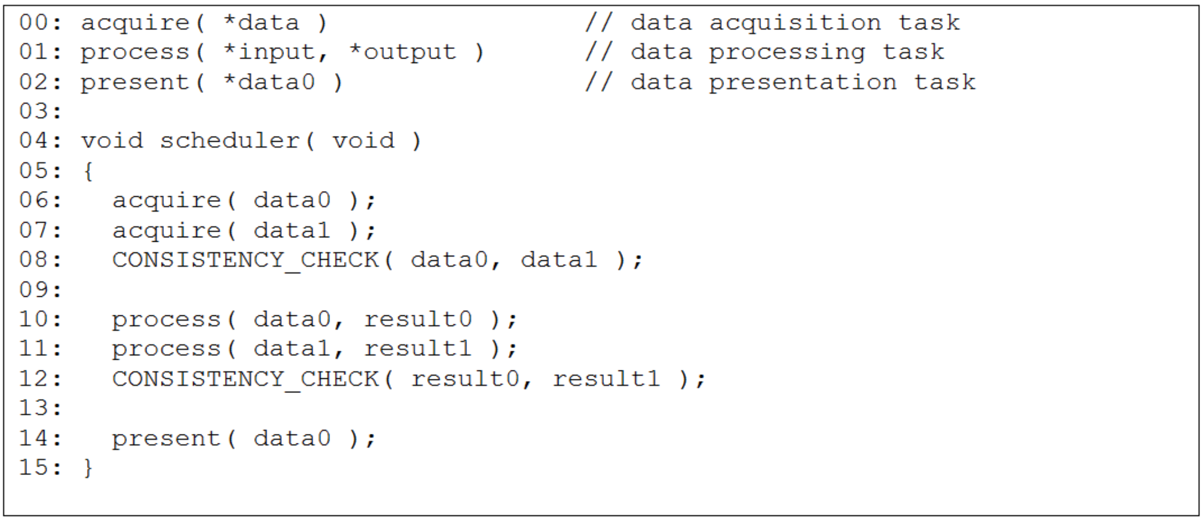
Redundancy is applied at task level, and consistency checks are inserted at task level, so that acquired data are compared before starting data processing, and produced results are compared before starting data presentation. A scheduler orchestrates the overall operation, as illustrated in Figure 14-5.

Task-level redundancy is potentially less expensive to implement than instruction-level redundancy, as modifications are applied at higher granularity 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 use 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 is 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 can propagate in the system for a longer period of time, and they can 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 is not 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 are 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 14-5).



```
acquire( *data )                 // data acquisition task
process( *input, *output )       // data processing task
present( *data0 )                // data presentation task

void scheduler( void )
{
  acquire( data0 );
  acquire( data1 );
  CONSISTENCY_CHECK( data0, data1 );

  process( data0, result0 );
  process( data1, result1 );
  CONSISTENCY_CHECK( result0, result1 );

  present( data0 );
}
```

Figure 14-5: Task-level redundancy

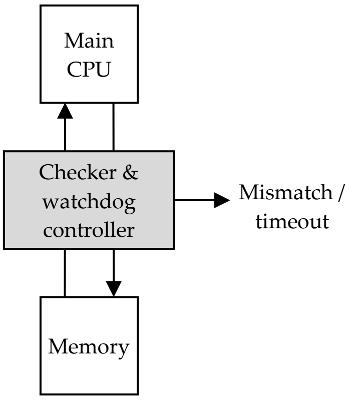


Figure 14-6: Architecture for temporal redundancy applied at task level

DMT (*Duplex Multiplexé dans le Temps*, i.e. duplex in time) is a CNES patented architecture [199], [200], [201], [202] aiming at, but not limited to, scientific missions and small satellites [203]. 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”.

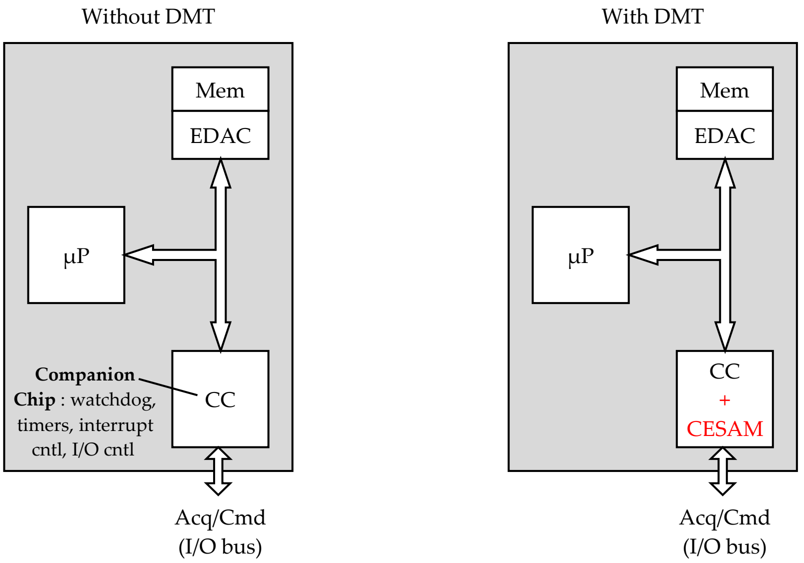


Figure 14-7: DMT architecture

In conventional space architecture, inputs are read from sensors during acquisition phase, then data are processed and commands to actuators can 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. Major results such as commands to actuators and other task's parameters 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 is 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, use the more time-consuming "backward recovery". During a recovery phase, no data exchange is used 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 is important to notice that the DMT architecture described in the present section maximise the software implementation; a new version, reusing the hardware function CLOPES (including an hardware comparator and an input-output controller) developed for DT2 architecture (see 15.2.5), allows to reduce the software impact of the fault protection, and to increase the reachable fault coverage.

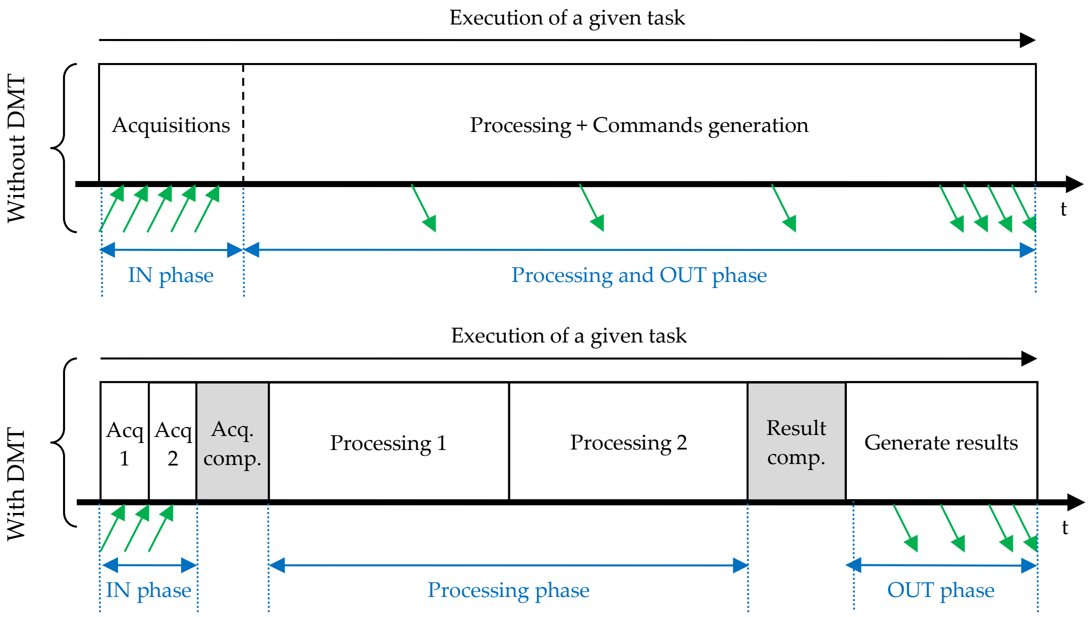


Figure 14-8: Scheduling and fault detection in DMT architecture

14.2.2.2 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 (section 5.9 and 5. 10 in [179]).

14.2.2.3 Added value (efficiency)

- Fault coverage: close to 100 %. Lock-stepping TMR [199] reaches 100 % fault coverage.

14.2.2.4 Known issues (weaknesses, elements to be considered)

- It needs software architecture modifications to differentiate IN/PROC/OUT phases (preferred optimised implementation, but not mandatory).
- In order to obtain a good level of fault coverage the instruction-level redundancy scheme can use the following:
  - CPU with an internal MMU
  - CPU board having a specific memory bridge.
- Third-party libraries, OS, hardware drivers are compatible with the instruction-level redundancy scheme.

The brief summary of key characteristics for redundancy at task level is given in the Table 14-3.

Table 14-3: Summary of key characteristics for redundancy at task level

Abstraction level	Electronic system
Pros	Fault coverage: close to 100 %
Cons	Code size increase 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

14.2.3 Redundancy at application level: using a hypervisor

14.2.3.1 Description of the concept

14.2.3.1.1 Overview

Whenever only one processor is used and in order to have redundancy for fault tolerance we decide to use more than one virtual machine, interrupts and an operating system of those virtual machines, then a possible solution can be found in hypervisor-based fault tolerance [204] as an example of redundancy at application level. Redundancy at application level is understood as a step higher in abstraction granularity when compared to task level: we are duplication an entire software programme or a large set of tasks.

The general idea consists in employing a special hypervisor tailored for space (i.e. to achieve fault tolerance and not to improve performance, as it is normally the goal of hypervisors for non-space applications) to implement two or more 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 (see 15.2.5.2.2), 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. Then the hypervisor or a support application takes the appropriate decisions as to mitigate the fault.

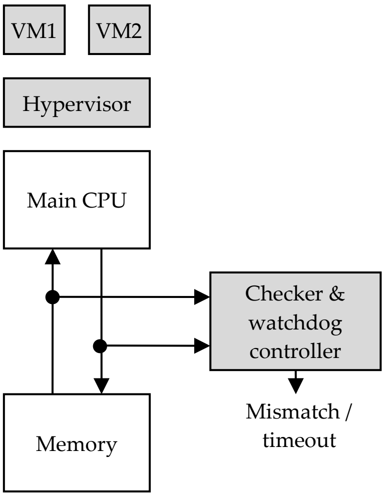


Figure 14-9: Time redundancy at application level

14.2.3.1.2 Example: Hypervisor-Based Fault Tolerance system based on LEON3 processor

Reference [205] presents an implementation of an Hypervisor-Based Fault Tolerance (HBFT) system based on the LEON3 processor and the XtratuM hypervisor [206]. 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 can 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.

14.2.3.2 Available test data (simulations, radiation testing, in-flight)

Reference [205] 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 by using a hypervisor system architecture) 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 %).

14.2.3.3 Added value (efficiency)

- Fault coverage: >96 %
- Software is not modified
- Compatible with third-party libraries, Operating Systems and interrupts

14.2.3.4 Known issues (weaknesses, elements to be considered)

Time overhead: ~2,5x (detection)

Memory overhead: >2x

The brief summary of key characteristics for redundancy at application level is given in the Table 14-4

Table 14-4: summary of key characteristics for redundancy at application level

Abstraction level	Electronic system
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

15
System architecture

15.1 Overview

Off-chip mitigation techniques refer to solutions aiming at reducing the effect of radiation on electronic devices that are implemented by the hardware and/or the software surrounding and connected to the device. For the mitigation implemented at software level this handbook has a specific dedicated Section 14, therefore this Section mainly concentrates in hardware-driven techniques, even if the cooperation of software is used in some cases. Several techniques and solutions are presented in this Section in order to mitigate a wide variety of radiation-induced effects.

Many “off-chip” mitigation techniques can sometimes also be implemented inside the FPGA or the ASIC, and therefore in some cases a more comprehensive description of the technique is given in other Sections of the handbook, while in this Section the technique is only briefly mentioned. For example, 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 many types of hazards (e.g. TID, SET, SEL, SEU or SEFI) but is not always effective against GCR and ions from Solar Particle Events (SPE) and protons.

External hardware protection and SEFI recovery 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 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 uses 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 uses three times the initial amount of hardware resources and provides fault detection and correction without time overhead.

A summary of mitigation techniques and the radiation effects they address is given in Table 15-1.

Table 15-1: Summary of mitigation techniques at electronic system level and the radiation effects they address

Mitigation techniques		Radiation effects			
		TID	SEL	SET	SEU
15.2.1	Shielding	X	X	X	X
15.2.2	Watchdog timers		X		X
15.2.3	Power cycling and reset		X		X
15.2.4	Latching current limiters		X		
15.2.5	Spatial Redundancy			X	X
15.2.5.2	Duplex architectures			X	X
15.2.5.2.2	Lockstep			X	X
15.2.5.2.3	Double duplex			X	X
15.2.5.2.4	Double Duplex Tolerant to Transients			X	X
15.2.5.3	Triple Modular Redundant system			X	X
15.2.6	Error Correcting Codes			X	X
15.2.7	Off-chip SET filters			X	

15.2 Mitigation techniques

15.2.1 Shielding

15.2.1.1 Description of the concept

A good introduction to radiation shielding can be found in Section 5 of ECSS-E-HB-10-12A.

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 [315]. 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. As explained in a space environment analysis performed for AXIOM [316], according to Fortescue et al. (2003) [315], the typical thickness of Al shielding in a spacecraft is between 2,5 mm and 3,8 mm which gives for the L1 orbit a radiation dose between 4,7 krad and 3,2 krad, as also reflected in Figure 15-1. For comparison, most commercial (not hardened) electronic parts start having problems above 2 krad. If we want to use semi-hard parts, TID are kept below 20 krad. This corresponds to a minimum shielding of 0,5 mm of Aluminum and is easily achievable even with appropriate design margins. Another comparison of the TID accumulated during a year for different Al shield thicknesses and different orbits is presented in Figure 15-2.

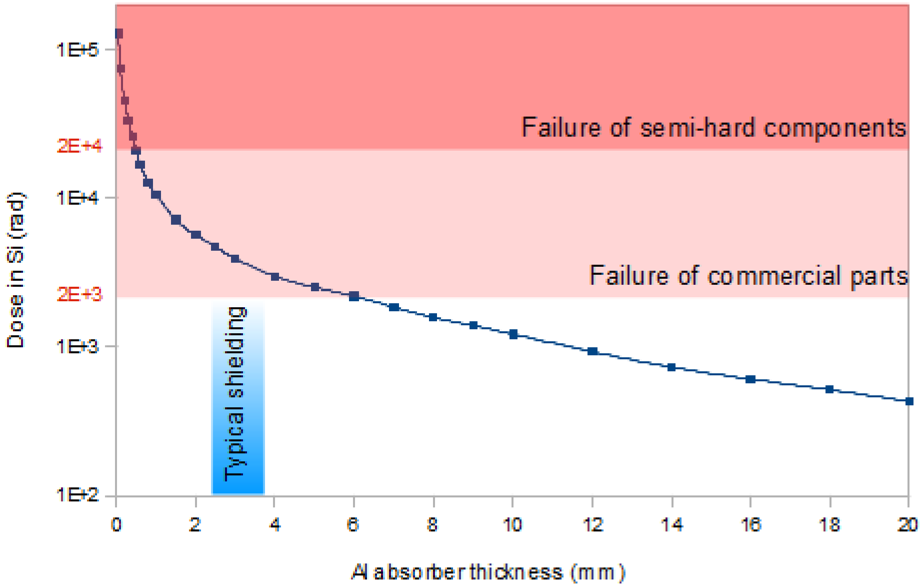


Figure 15-1: TID for the L1 orbit with indication of the typical shielding range and the failure regions of commercial and semi-hard components (after [315])

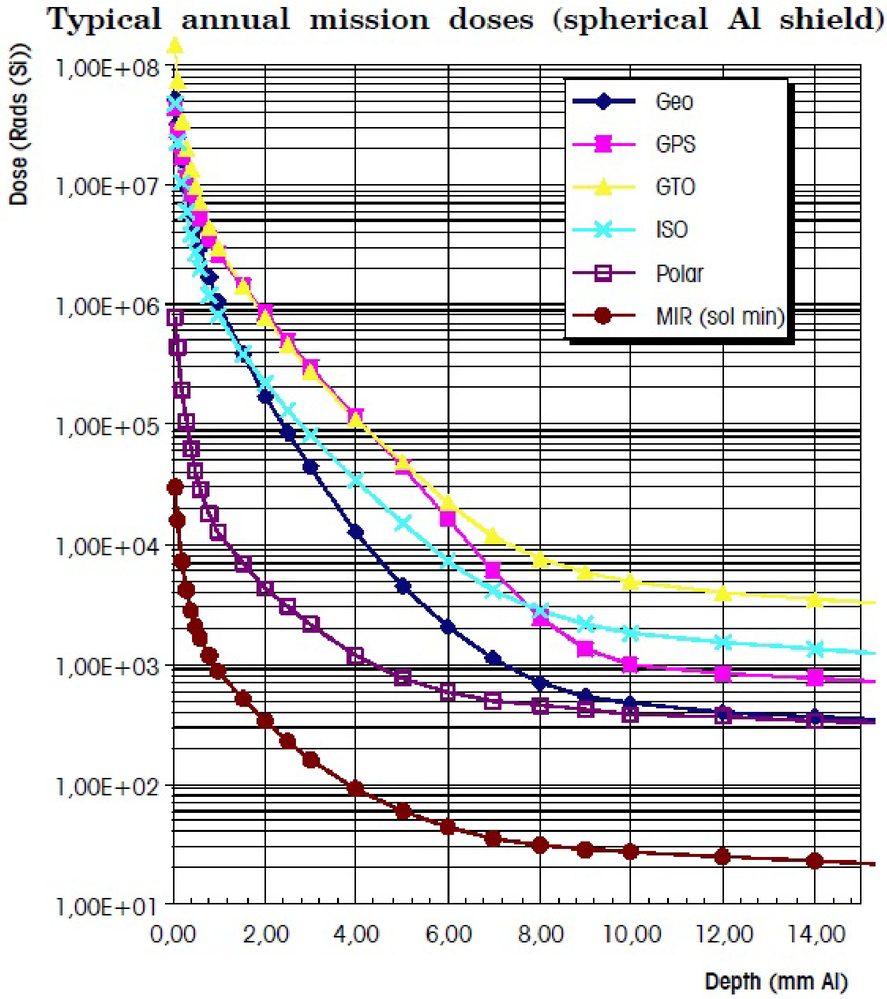


Figure 15-2: Typical annual mission doses (spherical Al shield) for various orbits, from ECSS-E-10-04A

Commonly used materials in satellites are:

- Aluminium (low/medium atomic number) for light shielding, some quantitative examples given in Figure 15-3 and Figure 15-4.
- 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.
- Tantalum.

15.2.1.2 Available test data (simulations, radiation testing, in-flight)

Figure 15-3 shows the contribution of the different environments (trapped electrons and protons, solar protons and the bremstrahlung) to the total dose. We can see in the figure that for the NASA ST5 mission the electrons dominate the TID environment up to 250 mils (1000 mils = 1 inch = 2,54 cm) of shielding and that they are nearly completely eliminated after 350 mils of shielding

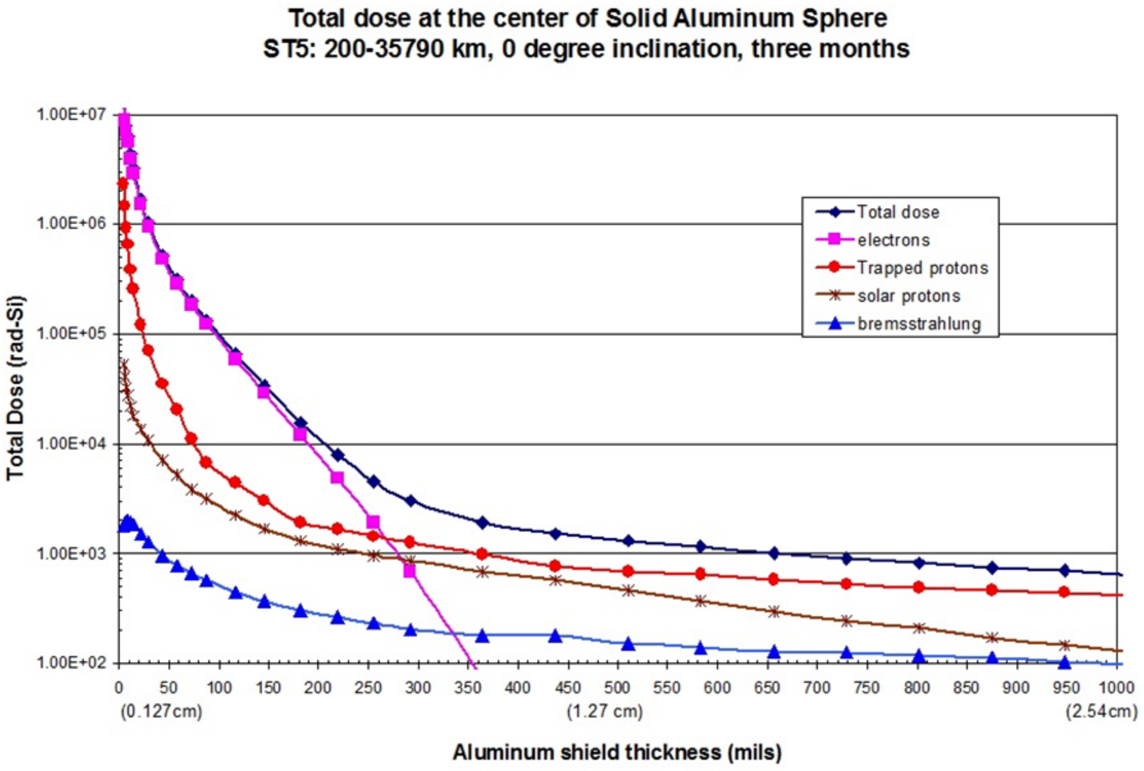


Figure 15-3: Example of a dose depth curve (C. Poivey, NSREC 2002 short course)

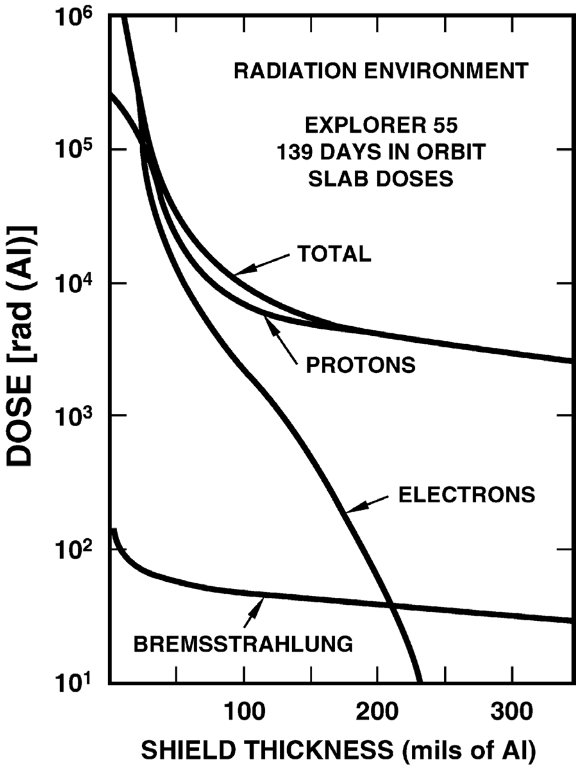


Figure 15-4: Figure Contributions of protons, electrons, and bremsstrahlung to total dose as a function of aluminum shielding. The data were taken after a 139-day exposure during the Explorer 55 space mission. (After [313])

- Reference [207] 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 [208]. The first conclusion is that with the considered shield distribution, shield thicknesses exceeds 0,8 mm. 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 [209]. Calculation results indicate that, for the radiation attenuation specified 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 used 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 [210]. 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 [211] 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 [212] describes the natural radiation environment inside spacecraft. 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.

15.2.1.3 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 produce secondary particles which are a potential threat to electronic devices. Reference [213] 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 %.

The brief summary of key characteristics for shielding is given in the Table 15-2.

Table 15-2: Summary of key characteristics for shielding

Abstraction level	Electronic System
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) Geant4 tools [280]: estimation of shielding requirements FASTRAD (performs optimum shielding analysis from 3D model of the system)

15.2.2 Watchdog timers

Electronic systems based on a processor device can suffer service interruption caused by a radiation induced SEFI. In such a case the system is able to recover a normal operating mode on its own. Off-chip watchdog timers can be used to monitor specific output signals of the processor IC, in order to periodically check that the expected outputs are there, and that there is no functional interrupt. If the expected output signal (or sequence of signals) indicates to the external watchdog that indeed there is unfortunately a functional anomaly, the rest of the system implements a recovery (mitigation) action on the IC, such as for example, a reset and or a power cycle that can eliminate persistent incorrect states in memory elements of the IC.

Watchdog timers and SEFI-recovery circuitry can also be integrated inside the ASIC or FPGA and thus have autonomous mitigation of these effects. Section 10 describes in more detail this technique.

15.2.3 Power cycling and reset

Removing completely the power source and turning it back on, also referred to as "power-cycling", can sometimes be the only way to eliminate the SEE-induced malfunction. Another type of softer reset can sometimes be adequate to eliminate the existing SEE condition.

15.2.4 Latching current limiters

15.2.4.1 Description of the concept

Latching Current Limiters (LCL) are active overload protections for power lines in satellites [216]. 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 Latch-up (SEL), they are critical 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 15-5, 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 is as short as possible (<10 μsec). Whenever the overload limitation is reached, the power MOSFET is switched off.

Another interesting feature shown on Figure 15-5 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.

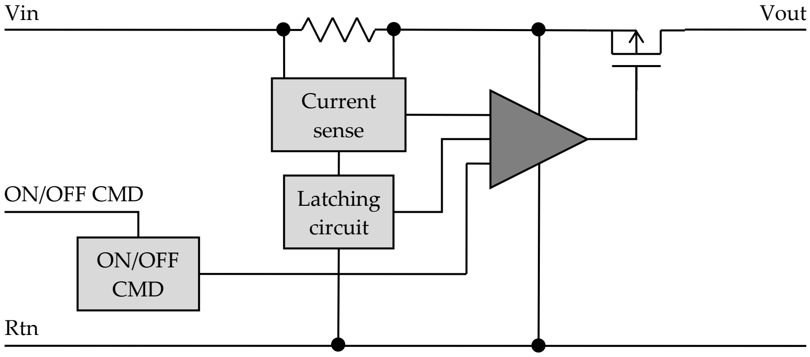


Figure 15-5: Block diagram of a LCL

MAXIM MAX892 circuit is used as current limiter for MYRIADE micro-satellite [279].

15.2.4.2 Available test data (simulations, radiation testing, in-flight)

- A study proved the LCL's efficiency to protect against SEL non radiation hardened circuits [217].
- 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) [218].

15.2.4.3 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.

15.2.4.4 Known issues (weaknesses, elements to be considered)

- The LCL is a critical safety element for the satellite and therefore it is important to pay special attention during selection of its parts to ensure that they meet the specified radiation immunity according to the mission.
- When setting the current threshold, the designer is to take into account the supply current increase caused by TID.

The brief summary of key characteristics for latching current limiters is given in the Table 15-3.

Table 15-3: Summary of key characteristics for latching current limiters

Abstraction level	Electronic system
Pros	Current overload protection
Cons	Area overhead: LCL circuitry
Mitigated effects	SEL
Suitable validation methods	Ground accelerated test

15.2.5 Spatial Redundancy

15.2.5.1 Overview

The concept of introducing redundant identical circuits working in parallel to then compare their outputs in order to see if a radiation effect has provoked an erroneous behaviour in any of the replicas and then discard the outputs (duplex architectures) or vote and select the good output (done in triple redundancy) was already explained in Section 10. This technique can be applied inside a single chip or can also be implemented across multiple chips and the support of auxiliary off-chip hardware and software. What follows is a revision of the duplex and triplication approaches when implemented with multiple chips, at what we call in this handbook the "electronic system level" or "off-chip" mitigation.

15.2.5.2 Duplex architectures

15.2.5.2.1 Description of the concept

The Bi-MR (Bi-Modular Redundancy), also called duplex architecture or dual-modular redundancy (DMR), is issued from the spatial redundancy concept present in section 11.2.1. It uses two replicas of a processing unit and compares the outputs to detect potential differences provoked by SEEs (Figure 15-6). Such an architecture is mainly a fail-stop architecture as it is able to detect faults but not to recover them.

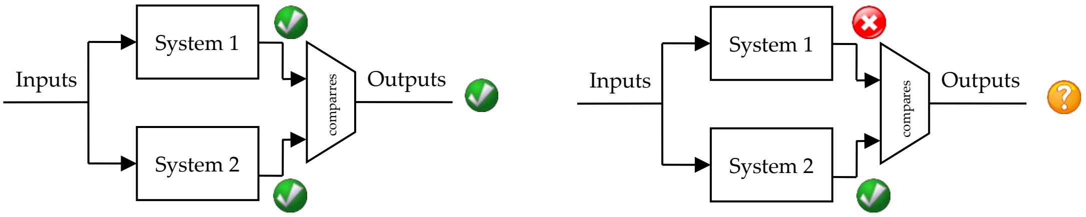


Figure 15-6: Block diagram of a duplex architecture

15.2.5.2.2 Lockstep

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 15-7). However, as the software running on each processor does not use any specific coding rules, both interrupts/traps and operating systems are supported.

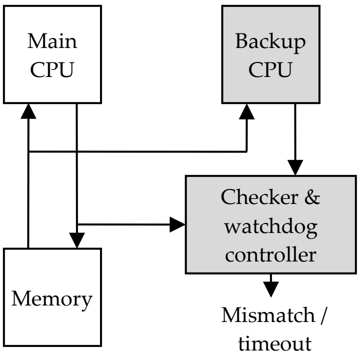


Figure 15-7: Lockstep architecture

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), it is preferable to configure cache memory in write-through mode if cache memory is used.

This topology is particularly suitable when two soft or hard CPU IP Cores are used. For example two PPC405 (hard IP) or two LEON3 (soft IP) in a Xilinx Virtex-4.

A Lockstep system has the following advantages:

- 100 % fault coverage (fault detection)
- Software is not modified
- 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 that a µP having the lockstepping capability is used (clock synchronisation or other mechanisms, full predictability, …), capability less and less compliant with deep sub-micron technologies. This technique was implemented on some µP such as the MICROCHIP ATMEL ERC32, Intel Pentium, Intel i960, IBM RH6000, IBM PowerPC750FX, ARM Cortex R family.

15.2.5.2.3 Double duplex

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 15-8). 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.

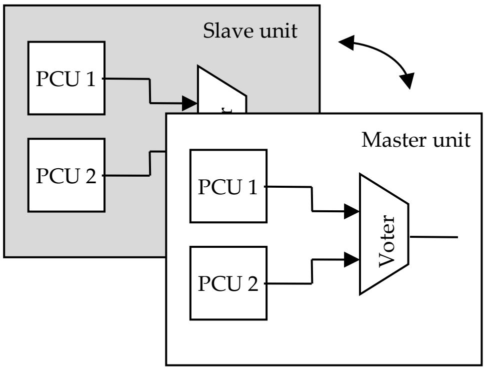


Figure 15-8: UCTM-C/D architecture

15.2.5.2.4 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 [199]. DT2 is a "structural mini-duplex":

- 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 used in DT2, they are implemented in an SEE-free ASIC or FPGA (Figure 15-9):

- CESAM, a simplified version of the DMT's CESAM (see section 14.2.1).
- 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 necessary between the two PUCs as each one has its own safe context storage inside its own memory to avoid fault propagation between channels.

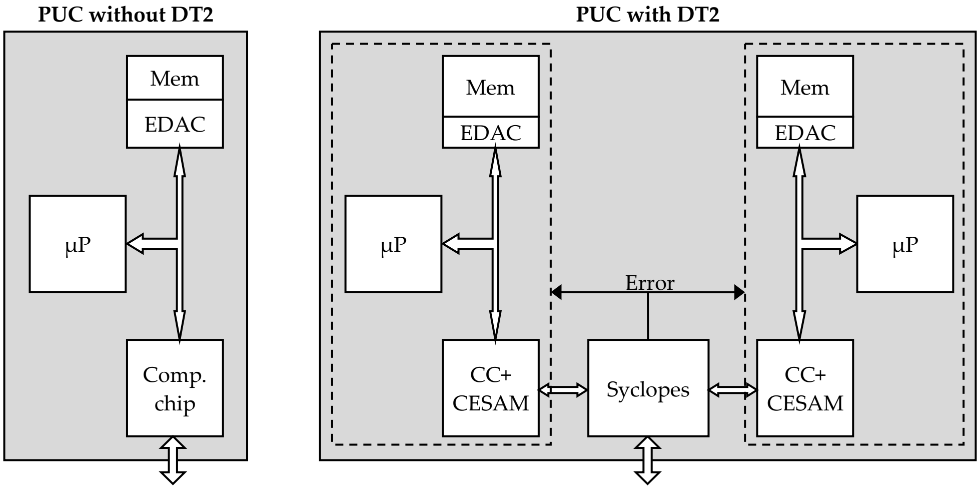


Figure 15-9: DT2 hardware architecture

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

15.2.5.2.5 Available test data (simulations, radiation testing, in-flight)

Reference [219] 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. 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.

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.

15.2.5.2.6 Added value (efficiency)

Fault coverage: >99 % if voter is radiation immune

15.2.5.2.7 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.

The brief summary of key characteristics for double duplex architecture is given in Table 15-4.

Table 15-4: Summary of key characteristics for double duplex architecture

Abstraction level	Electronic system
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

15.2.5.3 Triple Modular Redundant system

15.2.5.3.1 Description of the concept

Triple Modular Redundancy (TMR) applied at electronic system level is based on the same spatial redundancy concepts which are explained in more detail in section 11.2.1.3. In a TMR-based electronic system, hardware resources are triplicated in order to perform three identical tasks in parallel.

Redundancy at this level can vary from rather simple cases of redundant signals coming from the same chip (but different IO buffers inside the chip, as for example explained in the “global TMR” technique for FPGAs in 13.2.2) to cases where the whole chip is replicated in order to cope with faults.

Figure 15-10 illustrates a TMR system architecture embedding three identical microprocessors executing concurrently the same tasks (Task A at T=0, then Task B at T=1, and Task C at T=2). 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 15-11 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 “analogue comparator”. If one of the outputs is different from the two others, then the output is forced by the correct value.

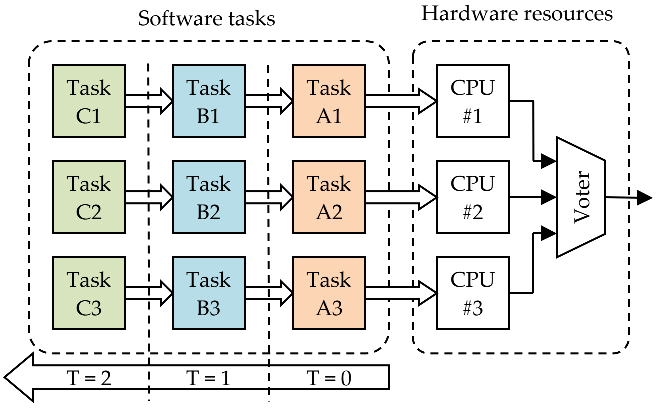


Figure 15-10: Triple Modular Redundancy

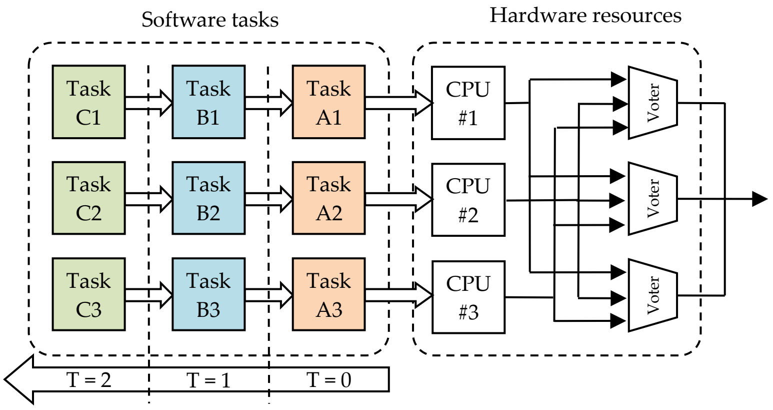


Figure 15-11: Full Triple Modular Redundancy

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 [220]. 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 (Microchip Atmel).
- The GUARDS architecture designed for critical applications such as rail, nuclear and space systems [221].
- 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 [222], [278].
- The SCS750 space-qualified board, developed by Maxwell technologies [223], 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).
- The Proton platform, by Space Micro, implements a technique combining spatial and temporal redundancy called Time Triple Modular Redundancy [198].

15.2.5.3.2 Available test data (simulations, radiation testing, in-flight)

Radiation test results for the SCS750 rev7 board [224]:

- 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 [198]:

- TID > 100 krad (Si) (orbit dependent)

- SEL (th) > 70 MeV*cm^2/mg
- SEU < 10-4 (orbit dependent)
- 100 % SEFI mitigation

15.2.5.3.3 Added value (efficiency)

TMR architecture grants almost a complete immunity to SET, SEU, MCU/MBU and SEFI.

15.2.5.3.4 Known issues (weaknesses, elements to be considered)

TMR system architecture has a weak point: the output comparator. The electronic system designer takes special care when implementing the voter or comparator of the outputs of the redundant devices in order to ensure that radiation effects on this element of the TMR architecture cannot invalidate the intended mitigation at system level. There are different ways to achieve this, one being for example using a rad hard FPGA for the voter part.

The brief summary of key characteristics for Triple Modular Redundant systems is given in the Table 15-5

Table 15-5: Summary of key characteristics for Triple Modular Redundant system

Abstraction level	Electronic system
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

15.2.6 Error Correcting Codes

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. Mitigation based on these codes can be implemented inside or outside the chip by a companion chip or a general purpose microprocessor. A comprehensive description is given in section 12.2.1.

15.2.7 Off-chip SET filters

If harmful SET pulses are expected at the outputs of the IC, SET filtering can be implemented outside the chip with dedicated pulse filtering buffer lines. This section will be expanded in future revisions of this handbook.

16
Validation methods

16.1 Introduction

It is important that applications intended to operate in harsh environment and critical applications (for example involving human lives) are validated with respect to how they will perform under radiation and to determine if they meet the constraints imposed by the final environment. While *real-life tests* provide accurate results, they also need long time experiments. Consequently, radiation ground 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.

In addition to fault injection techniques, where real radiation is emulated, different radiation sources and experiments can be used to validate the mitigation techniques. We could summarize the “real life” versus “ground accelerated” radiation environment characteristics as:

- Real-life environment (in flight or at ground): mixed particles species of broad energy spectra, combined effects (TID, DD and SEE), omnidirectional environment, actual particle rates/fluxes.
- Ground accelerated tests: single particle species, mono-energetic spectrum, individual effects, mono-directional environment, accelerated particle rates/fluxes.

16.2 Fault injection

Fault injection is defined as the deliberate insertion of faults into an operational system in order to observe its response [255]. Two main reasons can 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 (e.g. logical gates and memory cells) or complex functions (e.g. arithmetic or logical units and bus structures).
- 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 [256].

16.2.1 Fault injection at transistor level

16.2.1.1 Overview

Fault injection is an attractive technique for the evaluation of design characteristics such as reliability, safety and fault coverage [257]. Fault injection at transistor level done by simulation tools allows predicting SEE/TID sensitivity levels before performing radiation effects emulation by fault injection at other levels (gate, device or system), or accelerated tests and real-life experiments (with real radiation).

16.2.1.2 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. 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 find out the most vulnerable nodes of their transistors and to determine the minimum critical energy of charged particles. However this methodology involves important costs in terms of CPU computing power.

Examples of tools which were developed to model radiation effects in semiconductors and to allow performing SEE prediction of microelectronic circuits are:

- SEMM-2 is a state-of-the-art SEU simulation system, for both present and future CMOS technologies. Compared to SEMM-1, which was developed in the mid of the 80's for bipolar technologies, SEMM-2 has incorporated significant enhancements that render it an accurate SEU analysis tool suitable for basic research as well as for analyzing advanced CMOS [234].
- TIARA (Tool suIte for rAdiation Reliability Assessment) is a complete general-purpose simulation platform developed by STMicroelectronics to investigate the sensitivity of Radiation-Hardened-by-Design (RHBD) flips flops to heavy ions [301]. It allows accurate numerical evaluations of the sensitivity of microelectronic circuits in various radiation environments. TIARA is dynamically linked with SPICE solver (Eldo) and integrates a GDS parser to extract cell geometry data from the layout.
- MRED (Monte Carlo Radiative Energy Deposition) is essentially a framework for computing SEEs in semiconductors in which the component tool describing radiation interactions and transport in matter is a built-in, Monte Carlo, binary-collision code based on Geant4 [235], [236]
- DASIE (Detailed Analysis of Secondary Ion Effect) is the name of a code family dedicated to the SEE rate prediction. It has been developed to investigate SEE phenomena in SRAM and to predict the SEU and MCU and MBU rates. The SEE sensitivity can be calculated for SRAM devices with a limited set of technology parameters. The analytical method allows to quickly evaluating the SEU rate induced by proton, neutron and heavy ions but cannot deal with multiple upset events. MC DASIE fills this gap but the calculation time increases. DASIE can be considered as a generic method able with some further works in the future to investigate others SEE phenomena and other technologies [237].
- MUSCA SEP3 (Multi-Scales Single Event Phenomena Predictive Platform) aims at calculating both the SEE cross-section and SER, in the ground test and operational configurations. The approach consists in modelling the whole device, its local and global environment and the detailed characteristics of the radiation environment. This method constitutes a pragmatic approach dedicated to the neutron, proton and heavy ion radiation fields and can investigate Single and Multiple Events (SEU and MCU) in SRAM and Single Event Transients (SET) in CMOS technology [238].
- TFIT, SoCFIT: the TFIT software is a simulation tool for Cell Level Soft Error Analysis developed by IRoC (France) that predicts the failure rate (FIT) of cell designed on specific foundries' technologies. TFIT uses the foundry's process response model as technology input and spice

netlist and GDS2 as design input. Application for a cell are voltage, clock speed, presence of ECC and are user input through the GUI. SoCFIT uses the SER database of cells SER performances as technology input (output from TFIT) and the RTL/netlist as design input. An example of use of TFIT for 8T SRAM is given in reference [308].

- Accuro, rExplore and Roplace. These are tools developed by Robust Chip Inc. (USA) to, among other circuit reliability analysis, simulate and explore the SEE induced soft error rates and cross-sections in 2D and 3D circuit layout topologies. They have also automated the implementation of a layout methodology called LEAP (Layout Design through Error Aware Placement), developed with support of the Defense Threat Reduction Agency (DTRA), [336] and[337].

Other tool examples are: **Davinci** [258]**, Taurus** [259], **Athena/Atlas (Silvaco)** [260], **DESSIS** [261], **SPENVIS Geant4** tools (e.g. **GRAS**) [280] or **OMERE** [346]**.**

16.2.1.3 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 result is transient current pulse. Each circuit element (e.g. memory cell and logic gate) is simulated to determine the magnitude and the shape of the potential voltage transient that can 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 and Vdd. A current generator configured to reproduce the current pulse issued from physical level 2D/3D simulation is added to the DUT electrical model [302], [303]. Such simulations can be obtained from any commercial, freeware SPICE or analogue 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.

16.2.2 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 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 have been developed by various groups:
    - MEFISTO (LAAS-CNRS) [262], [263], [264], [265]
    - SEU Simulation Tool (ESA/U. Nebrija) [295]
    - ASSESS (Politecnico di Torino) [296]
- 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 [266]. The advantage of this method is that it is not intrusive. Indeed, both the simulation tool and the DUT model are left unchanged.
- Hardware-accelerated fault injection at gate level by using a reconfigurable FPGA platform where faulty-states can be introduced by partially reconfiguring the FPGA while the netlist inside

is receiving stimuli and while the outputs are being observed to see the effects of the faults. FT-UNSHADES and FLIPPER are examples of this type of fault-injection and analysis test systems. More details can be found in 16.2.3.3.

16.2.3 Fault injection at device level

16.2.3.1 Overview

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 involves developing the DUT, a board embedding the DUT and the tester.

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
- SRAM and Flash-based FPGAs

16.2.3.2 Fault injection in processors

16.2.3.2.1 Introduction

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.

This section presents the CEU (Code Emulated Upsets) method [267]. 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.

16.2.3.2.2 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. Such software simulated bit-flips is called CEU from now on. The piece of code able to provoke the CEU occurrence is called CEU code. The memory location in which the upset is injected is 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 flipped and "0" elsewhere).

c. Writing the corrupted value back to the CEU target location.

The only remaining step 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 performs 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 is 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.

16.2.3.2.3 Application error-rate prediction

The result of a fault injection, performed in 16.2.3.2 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:

$$\tau_{inj} = \frac{\#errors}{\#injected\ bit\ flips} \qquad (1)$$

τ_{inj} can also be interpreted as the average number of bit-flips needed 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 is defined as the average number of particles needed 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:

$$\sigma_{sta} = \frac{\#\ of\ observed\ bitfips}{fluency} \qquad (2)$$

Thus, the complete system error-rate is obtained by combining (1) and (2):

$$\sigma_{seu} = \tau_{inj} * \sigma_{sta} \qquad (3)$$

The main advantage of the CEU method relies on the fact that particle accelerator campaigns are done only once to obtain the static cross-section. A beam is not needed for the remaining part of the prediction. 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 [268], and the predicted results were close to the measures obtained from particle accelerator campaigns.

16.2.3.3 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 [269], while others modify the bitstream before downloading it in the device configuration memory or during download operations [160], as it is done with the **"FLIPPER"** tool [297], [270]. Although the fault-injection approaches permit to evaluate the effects of SEEs 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. There are fault injection and analysis tools like "**FT-UNSHADES"** (U. of Seville, Spain) [298], [299], [300], which have evolved in time to increase the fault injection speed and the flexibility to inject faults in both the configuration and the user's memory with unprecedented degrees of freedom, controllability and observability. This tool in particular can be used to emulate the SEE effects in both ASIC and FPGA netlists.

As an example, the CEU method devoted to processors, presented in section 16.2.3.2, can be adapted to reprogrammable FPGAs (whose configuration memory is based on SRAM or Flash technology) and are detailed in 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 as explained before for processors. However it is important that the FPGA architecture is compatible with the fault injection mechanism. 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.

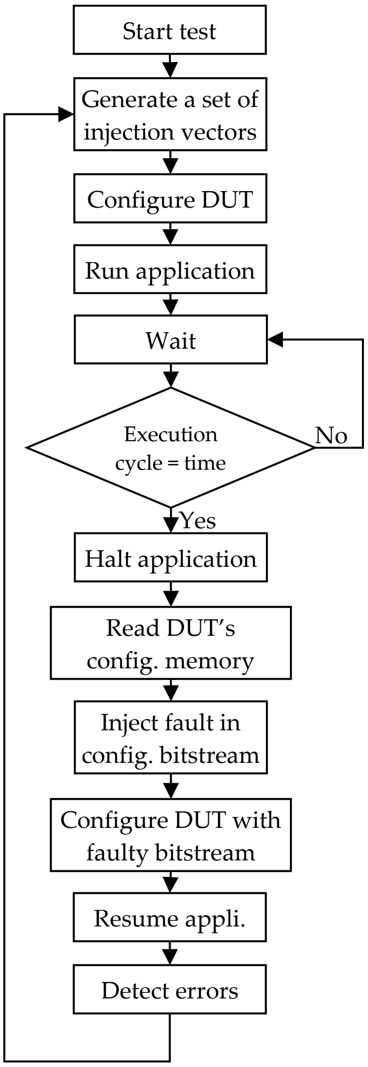

Start test
Generate a set of injection vectors
Configure DUT
Run application
Wait
Execution cycle = time
No
Yes
Halt application
Read DUT's config. memory
Inject fault in config. bitstream
Configure DUT with faulty bitstream
Resume appli.
Detect errors

Figure 16-1: Flow chart for fault injections in FPGAs

As depicted in Figure 16-1, 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 is 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 allows 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 to obtain the 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 [271].

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 targeted memory bit and its function in the application.

16.2.3.4 Analytical methods for predicting effects of soft errors on SRAM-based FPGAs

Although the fault-injection approaches (see section 16.2.3.4) 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 software programs able to elaborate the circuit netlist both at the post-synthesis and at the post-layout level. An analytical approach based on synthesis tools is proposed in [273], [274], [275].

In [273] 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 [274] 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 [275] 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 [276], [277]. The analysis is then coupled with a set of reliability constraints.

A complete software tool, **VERI-Place**, has been developed in [317] in which the circuit error rate estimated on a SRAM-based FPGA on the basis of the accumulation of SEUs within the configuration memory has been validated with respect to fault-injection.

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.

16.2.4 Fault injection at system level

A representative example of integrated design and fault-injection environment at system level is **DEPEND** [272]. 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 behaviour, repair schemes, and system software in detail.
- It simplifies modelling 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 behaviour 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 behaviour is evaluated. Faults are injected, repair schemes are initiated, and reports classifying faults' effects are generated during this process.

16.3 Real-life radiation tests

16.3.1 Overview

Real-life radiation tests consist in operating a target application IC in a natural radiation environment, that, in some cases can be its intended final operational environment. Different solutions are available depending on the considered environment and scope of the tests:

16.3.2 Tests on-board scientific satellites

Some projects accept applications devoted to study the behaviour of the radiation on circuits and their software if they have one. To mention a few examples: MPTB (Microelectronics and Photonics Testbed) [239], STRV (Space Technology Research Vehicles) [240] and [241], LWS-SET (Living With a Star – Space Environment Testbed) [242], NASA SEUXSE and MISSE SpaceCube experiments to test the radiation tolerance FPGA technology [318], or the CARMEN-2 CNES experiment on board JASON-2 [338].

16.3.3 On-board stratospheric balloons

On-board stratospheric balloons are able to operate in the stratosphere during long periods of time and at an altitude between 12 km and 45 km. 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 tons to altitudes of 40 km. A generic platform devoted to detect upsets in two successive technological generations of SRAMs is presented in reference [243]. Preliminary results obtained in commercial flights were successfully compared to those issued from a state-of-the-art predicting tool (The MUSCA SEP3 tool [238]).

16.3.4 Ground level tests

Ground level tests provide high flexibility capabilities because they are not tied by weight, volume and power consumption constraints as it can be the case for the two previously presented platforms. The long-term exposure to natural radiation can reveal valuable information about the sensitivity of the IC to TID and SEE effects, and how given mitigation techniques are working as expected or not. These type of tests can be conducted at **sea-level** or **in altitude** (to have an acceleration factor), but also **underground**, if we want to remove the atmospheric neutron contribution in favour of checking the influence of alpha particles from radioactive contaminants. An example of real life component qualification is the Rosetta experiments by Xilinx [244]. It consists of several hundreds of FPGAs being monitored to detect upsets in their configuration memories. These test-beds are installed at different altitudes, from -550 m to 2550 m, in the US and in France. Another example is the altitude and underground tests of CMOS 65 nm SRAM performed in the framework of a scientific collaboration between the "Altitude SEE Test European Platform" (ASTEP platform) and the "Laboratoire Souterrain de Modane" (LSM, joint CEA-CNRS research unit)[304].

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 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 or HW/SW fault injections are often preferred.

16.4 Ground accelerated radiation tests

16.4.1 Overview

Accelerated tests are performed in facilities, such as synchrotrons and linear accelerators which provide 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 to the ones found in space. However, the important parameter characterizing the interaction between a particle and matter being the LET for heavy ions, and energy for protons, particle accelerators are calibrated to provide particles having similar LETs and energies to those of particles present in the natural space environment.

16.4.2 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 test methods and guidelines used to do radiation tests of integrated circuits. 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 radiation test methods and guidelines

Standard reference	Standard name	Particle source	Type of radiation tests
ESCC 25100	SEE testing of integrated circuits and discrete semiconductors devoted to space applications	Protons Heavy ions	SEE
JEDEC JESD57	Test Procedures for the Management of Single-Event Effects in Semiconductor Devices from Heavy Ion Irradiation	Heavy ions	
ASTM F 1192	Standard Guide for the measurement of Single Event Phenomena (SEP) Induced by HI irradiation of Semiconductor Devices		

Standard reference	Standard name	Particle source	Type of radiation tests
JEDEC JESD89A	Measuring and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices	Alpha Neutrons	
ESCC 22900	Total Dose Steady-State Irradiation Test Method	Gamma	TID
MIL-STD-883/ 1019.4	Test Method Standard Microcircuits / Ionizing radiation (total dose) test procedure	Gamma	

16.4.3 SEE test methodology

16.4.3.1 Overview

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, ASICs, FPGAs and memory ICs.

16.4.3.2 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 16-2).

This test is used to obtain the static cross-section curve. This test flow represents in a way a worst 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, however, in this flow we are testing all memory elements of the device. The result of a static test characterizes the device itself, independently of the final application.

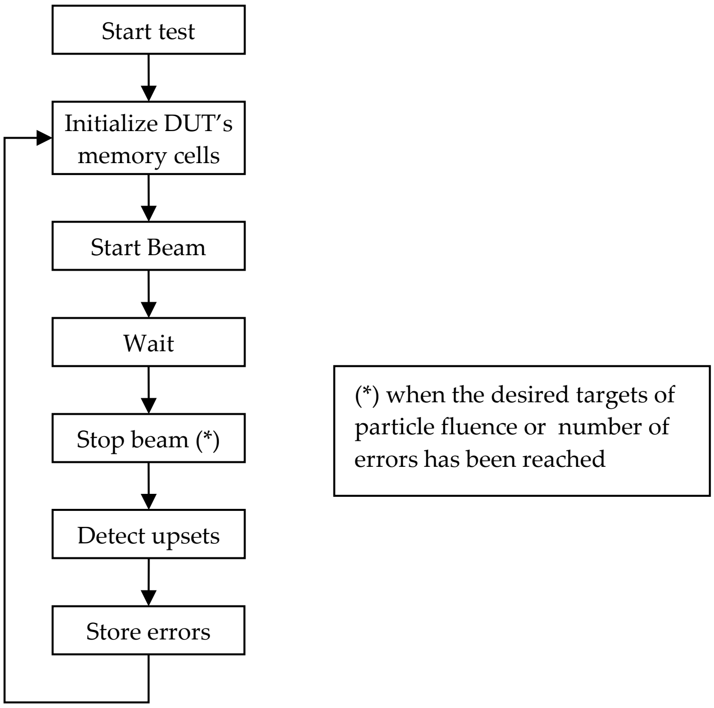

Start test
Initialize DUT's memory cells
Start Beam
Wait
Stop beam (*)
Detect upsets
Store errors
(*) when the desired targets of particle fluence or number of errors has been reached

Figure 16-2: Flow chart of a typical static test

16.4.3.3 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 16-3, this is performed by running the final application or specific benchmark programmes under beam until an error is detected on the application's outputs. Dynamic test is more complex than static test but it is recommended in order to detect all types of errors that can potentially appear in complex applications. The drawback of this strategy is that any change in the application can imply the need to perform a new test campaign.

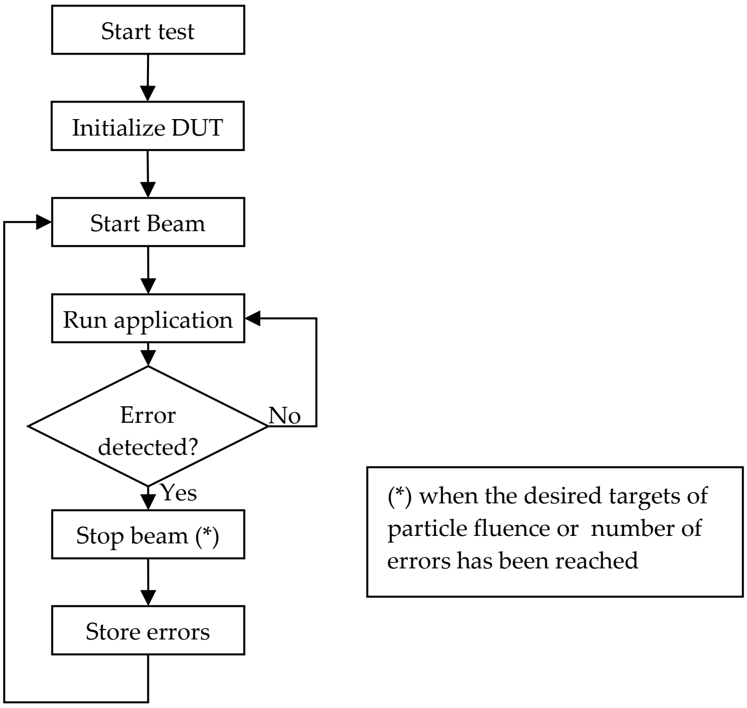
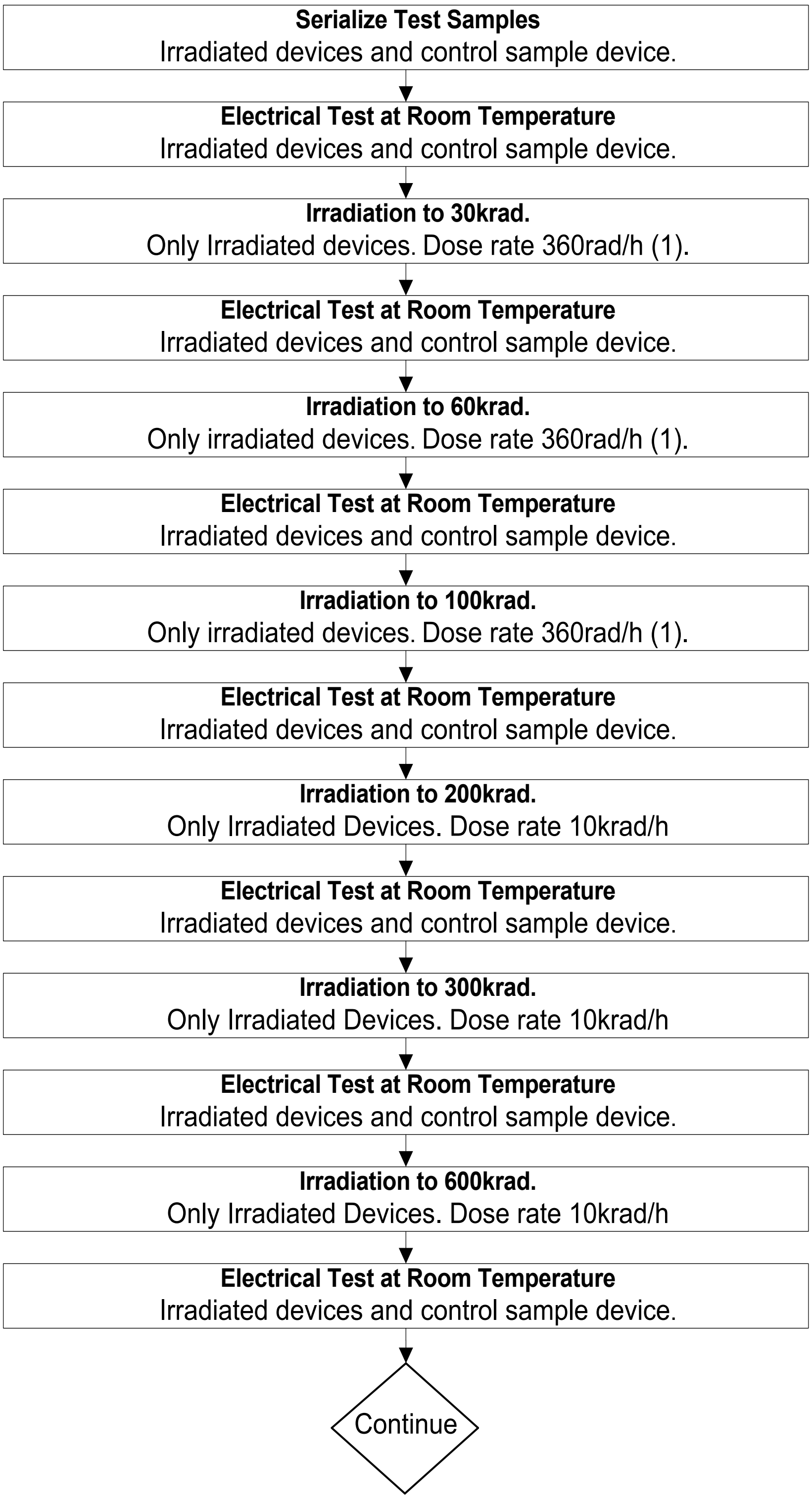


Figure 16-3: Flow chart for a typical dynamic test

16.4.4 TID test methodology

A real example of a TID proposed test flow of test vehicle to characterise the TID sensitivity of mixed-signal ASICs built on a 180 nm CMOS technology is presented in Figure 16-4. This flow illustrates the main steps and typical elements to be taken into consideration, such as the use of a control sample, the temperature, dose rates, irradiation levels or annealing time.


Serialize Test Samples
Irradiated devices and control sample device.
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 30krad.
Only Irradiated devices. Dose rate 360rad/h (1).
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 60krad.
Only irradiated devices. Dose rate 360rad/h (1).
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 100krad.
Only irradiated devices. Dose rate 360rad/h (1).
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 200krad.
Only Irradiated Devices. Dose rate 10krad/h
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 300krad.
Only Irradiated Devices. Dose rate 10krad/h
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Irradiation to 600krad.
Only Irradiated Devices. Dose rate 10krad/h
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Continue

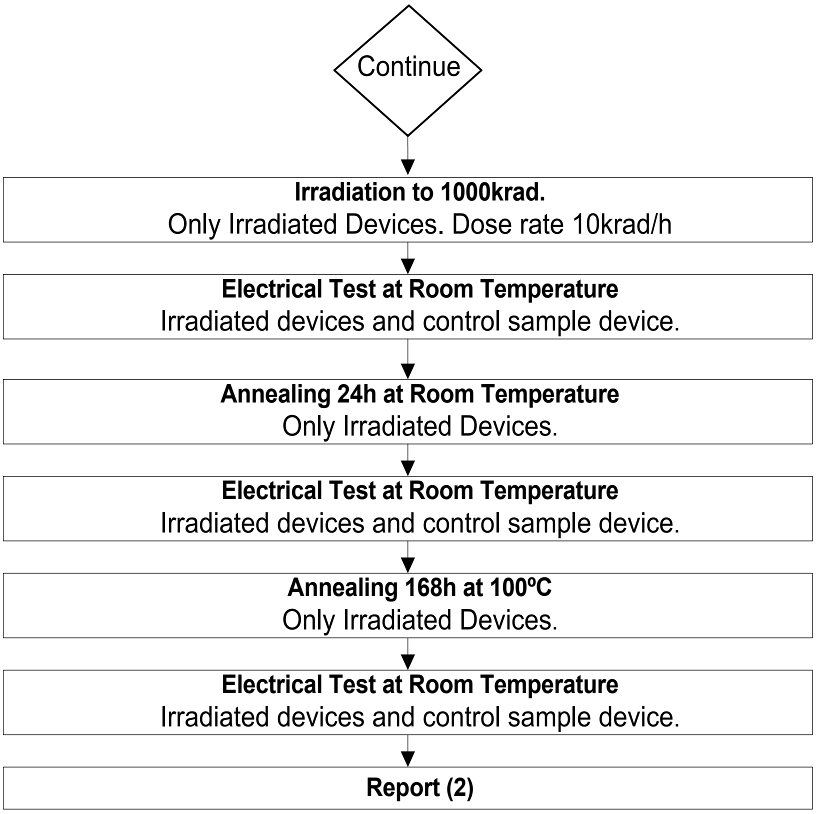

Continue
Irradiation to 1000krad.
Only Irradiated Devices. Dose rate 10krad/h
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Annealing 24h at Room Temperature
Only Irradiated Devices.
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Annealing 168h at 100ºC
Only Irradiated Devices.
Electrical Test at Room Temperature
Irradiated devices and control sample device.
Report (2)

Figure 16-4: Example of TID proposed test flow of test vehicle

16.4.5 TID and SEE test facilities

16.4.5.1 Overview

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 desired tests:

a. Total Ionizing Dose: for this kind of characterization, parameters are measured at different dose levels. Main used source for this is Cobalt 60. Proton accelerators are also suitable in some cases. The problem with protons is that they generate displacement damage at the same time and the dose rate cannot be easily lowered to low dose rate (<360 rad/h or lower) as recommended for all technologies containing bipolar elements. Cobalt 60 is so widely used because the yield of un-recombined electron-hole pairs is worst case compared to most space particles, there is usually no need for device delidding, and it is normally easier than running tests with particle accelerators. Cobalt 60 also usually permits a large range of dose rate possibilities.

b. Single Event Effect: on-line testing of the different device parameters and functionalities is performed. Particle accelerators are used either with protons or heavy ions.

c. Displacement Damage: parameters are measured at different particle fluencies corresponding to different displacement damage doses. Particle accelerators are used (electrons, protons and neutrons).

There are multiple radiation test facilities that are used by the space components industry, vendors and agencies. A nice international compendium of 66 irradiation test facilities was put together by RADECS 2011 organizers, was updated in RADECS 2015, and is available on-line [305]. A list of radiation test facilities can also be found under the www.escies.org radiation database.

16.4.5.2 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 Displacement damage contribution
Protons **(accelerator)**	High dose rate available Representative of some orbits	
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	

Particle accelerators have the advantage to provide high dose rates that allow to perform accelerated tests. However, for EEE components high dose rates are usually not recommended, especially for components embedding bipolar technology In addition such facilities are associated to a non-negligible cost. Moreover, protons can 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 [245].

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 MeV and 1,33 MeV, dose uniformity is ensured. Gamma sources (mainly Co60) are the most widely used facilities for TID testing. A non-exhaustive list of gamma ray test facilities is given in Table 16-3.

Table 16-3: Non-exhaustive list of worldwide Gamma ray facilities

Facility	Sources, dose rates
Cobham (former Aeroflex) RAD - USA	Co-60 and Cs-137, 1mrad(Si)/s to 100 rad(Si)/s
CNA - Spain	Co-60, 0,36 to 500 Gy(Si)/s
ESTEC - Netherlands	Co-60,0,4 rad(Si)/min to 150 rad(Si)/min
Fraunhofer Int - Germany	Co-60, 1µGy(Si)/s to Gy(Si)/s
JAEA - Japan	Co-60, 1Gy(Si)/h to 104Gy(Si)/h
UCL - Belgium	Co-60, 1,8krad(Si)/h to 80 rad(Si)/h

16.4.5.3 Single event effects

16.4.5.3.1 Overview

Single event effects are mainly studied using particle accelerators which are able to produce different types of beams such as heavy ions, protons or neutrons. 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 are placed in a vacuum chamber with cable feedthroughs.

Lists of accelerators available in Europe and the US classified by particle types and energy ranges are provided in the following subsections.

16.4.5.3.2 Heavy ions

A non-exhaustive list of heavy ion test facilities is given in Table 16-4.

Table 16-4: Non-exhaustive list of worldwide heavy-ion facilities

Facility	Energy
Berkeley - USA	32,5 MeV/amu
Brookhaven National Laboratory - USA	85 MeV/amu
CYCLONE UCL - Belgium	10 MeV/amu
GANIL - France	100 MeV/amu(*)
IPN - France	≤ 10 MeV/amu
JYFL - Finland	10 MeV/amu
LNL - Italy	≤ 10 MeV/amu
Texas A&M University - USA	15 and 25 and 40 MeV/amu
(*) amu = Atomic Mass Unit, 1 amu = 1,66054 x 10^{-27} kg	

16.4.5.3.3 Protons

Several facilities are available for device testing using protons. A non-exhaustive list is given in Table 16-5. 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 16-5: Non-exhaustive list of worldwide proton facilities

Facility	Energy
CPO - France	Up to 200 MeV
Crocker Nuclear Laboratory - USA	Up to 68 MeV
CYCLONE UCL - Belgium	Up to 70 MeV
GNPI - Russia	Up to 1 GeV
Indiana University - USA	Up to 200 MeV
IPN - France	Up to 20 MeV
JYFL - Finland	Up to 60 MeV
Lawrence Berkeley Laboratory - USA	Up to 55 MeV
PSI/OPTIS - Switzerland	Up to 63 MeV
PSI/PIF - Switzerland	Up to 250 MeV
SIRAD - Italy	Up to 28 MeV
Triumf - Canada	Up to 520 MeV

16.4.5.3.4 Neutrons

Neutron tests mainly concern avionic applications but start to be a major concern for all electronic equipment, even those operating at ground level. The JEDEC standard JESD89 [246] 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 16-5). However, the same standard explains how to reach data using quasi-mono-energetic neutron beams, which is available in Europe.

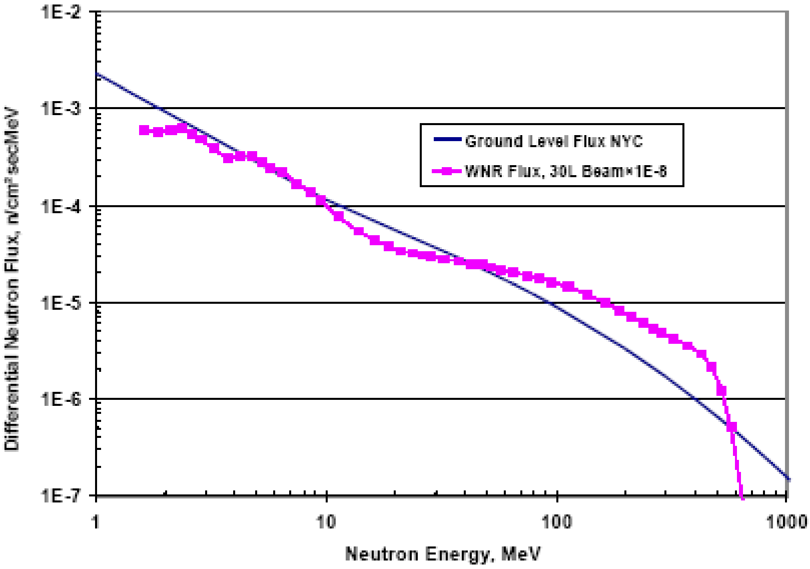


Figure 16-5: Neutron fluxes in NY City and at LANL

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.

16.4.5.3.5 SEE tests practical constraints and DUT preparation

Particle accelerators impose some constraints and it is important that the designers are aware of them 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 cannot meet the requirements in term of impedance or speed of some applications.
- In Heavy Ion tests one of the most important constraint is the limited ion energy and then the corresponding limited penetration depth of some tenth of µm which make the device lid removal mandatory in most cases, and the inherent risk to misinterpret the test results in case the penetration depth is not sufficient.
- Another consequence of vacuum is the temperature control issue. It is important to take into account that the only way the energy is dissipated, 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 decreases the LET threshold and increase the cross-section saturation [254]. 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 can be exposed to particles. Consequently it is important that special care is 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 is remotely controlled.
- Electrical noise can 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 [183] 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 MHz to 200 MHz. Therefore, it is important that the DUT is tested at the expected operational frequency whenever this is possible.
- It is very important to decide and control extremely well the DUT biasing levels, as tiny shifts in the voltage levels can result sometimes in large variations of the radiation effects being (or not) observed.

Depending on the nature of the used beam, the sample can be prepared in order to expose sensitive area of the die to the particles. It is the case for heavy ions and low energy protons (below 10 MeV) which involves opening the packages. This operation can be easily done for circuits having a metallic lid. Plastic and ceramic packages use mechanical or chemical processes to expose the die. Such attacks can have destructive consequences, in some cases leading to the rebonding of the chip.

If the DUT's die is mounted in a flip-chip package, then the penetration length of the particles is taken into account. Indeed, if the particle track length becomes too short, the observed device's sensitivity can be underestimated. In the worst case, the particles cannot even reach the active volumes and no effect is generated. A die thinning process is 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 have thickness variations across the surface. This induces LET variations from part to part of the device, and thus data is influenced.

16.4.6 Complementary SEE test strategies

16.4.6.1 Overview

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 crucial for the estimation of the circuit sensitivity on the final radiation environment, but it does not provide information such as instant of occurrence and location on the events that provoked the observed errors. Complementing explained test techniques in 16.4.5.2,16.4.5.3, there are a few other that are often used as well:

- Laser beam SEE tests
- Ion-Microbeam SEE tests
- Californium-252 and Americium-241 SEE tests

16.4.6.2 Laser beams SEE tests

Laser has been studied for years by different research groups to define its field of application with regard to particle accelerators. At the origin of laser testing comes the fact that although the basic mechanisms of the charge generation with a laser are different from the ones involved in the interaction of an ion with matter, the consequence is the same: the spatially and temporally localized generation of charges in Silicon which can lead to Single Event Effects.

A very useful source of information with examples of laser testing for radiation effects analysis are the RADLAS (RADiation Analysis LASer Facilities Day) thematic workshops with on-line repositories [306] or resulting in diverse IEEE scientific journal publications [307].

The main advantages of laser facilities are: [247][248]

- The flexibility: it has no radiation constraints nor need of vacuum,
- The spatially and temporally localized laser shots which allow the mappings of the sensitive locations or periods of time,
- The high penetration depth depending on the wavelength (hundreds of µm for a 1,06µm laser in a typical silicon substrate).

The key parameters are:

- The wavelength: the charge generation in silicon can be achieved either by single photon absorption, if the wavelength is less than 1,1 µm or by multi photons (especially two photons) absorption if the wavelength is greater than 1,1 µm. Single photon absorption has been widely studied and it is a mature way to do laser testing. Two photons absorption is a more recent way to do laser testing, based on nonlinear absorption of photons which has shown promising capabilities [249]. For single photon absorption, the wavelength has a direct influence on both:
    - — The spot size: it highly depends on the wavelength and the optical lens of the facility. The diffraction effect limits the minimum spot size achievable to roughly the wavelength.
    - — The penetration depth: the shorter the wavelength, the shorter the penetration depth. For a typical silicon substrate, a 1,06 µm laser has a penetration depth in silicon up to several hundreds of µm whereas at 780 nm it is only 10µm.
- The pulse duration: A broad range of pulse durations is achievable with laser sources: from femtosecond laser up to continuous laser.

<u>Front-side and Back-side laser tests</u>: [250][251]

There are two ways to perform laser tests: either from the front side of the device or through the back side. For integrated devices, it is highly recommended to perform laser tests from the back side since otherwise, on the front side, metal layers can mask some of the active layers. This has a consequence on the choice of the wavelength: for back-side laser tests, either the wavelength is chosen close to 1,1 µm so that the laser beam can cross the silicon die thickness before reaching the active layers or the silicon die undergoes thinning.

<u>Correlating laser energy/heavy ion LET and absolute cross-section determination</u>: [251]

The topic of the correlation between the laser energy and the heavy ion LET is not straightforward. In fact, due to its spot size limited by diffraction, a laser beam is more representative of a high energy heavy ion which track diameter can reach several µms rather than low and medium energy heavy ions which track sizes are commonly estimated to be less than 0,05 µm. This spot size effect makes the correlation between the laser energy and the heavy ion LET be different depending on the integration level of the Device Under Test. This effect also impacts the correlation between laser and heavy ion cross-sections. Therefore, it is important to both take care when trying to correlate laser energies and heavy ion LETs, and when extrapolating laser cross-sections to heavy ion equivalent ones especially on high integrated devices.

Ways to use a laser facility as a complementary tool to accelerators:

Besides the spot size effect which makes not straightforward the correlation with low/medium energy heavy ions, the laser tool has been demonstrated to be a very efficient tool complementary to accelerator facilities especially for:

- Assessing the sensitivity in a relative manner for different operating conditions [284] Screening the DUT, especially to detect latch-up sensitive devices [252],
- Injecting faults in given areas and at given timing, to sort out the different application failures and assess the efficiency of mitigations [253],
- Localizing sensitive areas [248].

There are multiple laser test facilities worldwide that can be used for SEE testing. A non-exhaustive list of laser test facilities is provided in Table 16-6

Table 16-6: Non-exhaustive list of worldwide laser test facilities

Facility	Laser type
CSL - Belgium	Nd-YAG, Excimer, CO_2, Ar, Solid state, He Cd,
AGIF – Suresnes, France	Pulsed Nd:YAG
NASA-JPL / CALTECH - USA	Pulsed near infrared – single photon
NRL - USA	Pulsed width 1ps, wavelength 590 nm
SPELS NRNU - Russia	Q-switched and DPSS picosecond Nd:YAG
USAL-LASER - Spain	Nd:YAG, Nd:V, CO_2, Ti-Zafire, He-Ne

16.4.6.3 Ion-Microbeam SEE tests

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 of high energy: 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. An example of how their microbeam was used to do SEE tests of commercial DSP components is given in [319]. In addition, but offering lower energy microbeams, the SIRAD-INFN Legnaro National Laboratory (LNL) in Padova, Italy, offers the possibility to conduct SEE microbeam testing, as it was done for commercial SDRAMs in the reference example of [320].

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 16-7.

Table 16-7: Summary of the characteristics of laser and microbeams

	Heavy Ion Beam	Laser	Heavy Ion Microbeam
Beam diameter on DUT	A few cm	Depends on the wavelength (down to roughly 1µm for a 1,06 µm laser)	Down to 1 µm
Track size	Depends on the energy - up to several µm at high energies and down to <0,05 µm at low energies		<0,05µm
Range	Range is several tenths of µm or more depending on the energy	Penetration depth depends on the chosen wavelength. It can be larger than hundreds of µm	up to several tenths of µm
Localization of sensitive areas	NO	YES	YES
Study of rare phenomena			
Cross-section determination	YES	Not easily	YES, but with special care if range is short

16.4.6.4 Californium-252 and Americium-241 SEE tests

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).

Californium-252 is an artificial radioactive element that spontaneously fissions into several fragments (Figure 16-6), alpha particles and neutrons. Fission fragments that represent only 3 % of the total amount of fission products are useful for SEE purpose.

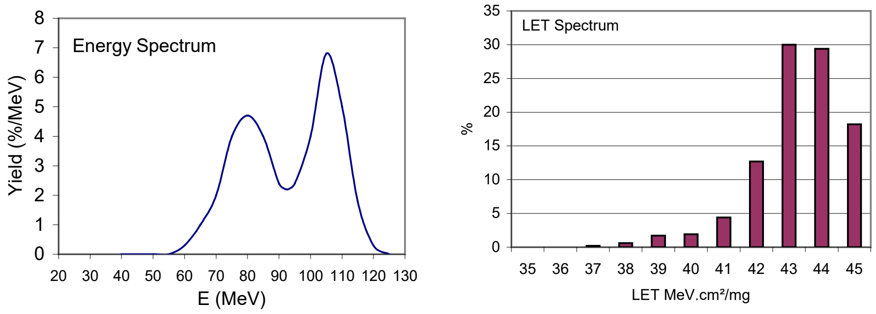


Figure 16-6: Californium-252 fragments energy spectrum (left) and LET spectrum (right)

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 43 MeV *cm^2/mg) allows inducing errors in devices and debugging test set-up before moving to the accelerator site.

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.

Annex A (informative) Vendor/institute-ready solutions that include mitigation or help to mitigate

There is a wide offer of ASIC and FPGA technology which either incorporates already one or more mitigation techniques against radiation effects, or that can help the IC user or developer to apply some mitigation. This technology is sometimes available through commercial suppliers or sometimes through research groups (universities or institutes).

This Annex A gives link to the list of some of the vendor-ready solutions or tools that are best known to the space ASIC and FPGA users and developer community. It is very important to understand that in many cases, the user would have to combine a vendor-ready technology with additional mitigation techniques or tools in order to get to the level of radiation hardness needed. Due to advances in technology and to the ever changing commercial landscape, some of these third party solutions will become obsolete or discontinued, while new ones become available.

Therefore, the summary of existing "vendor/institute-ready solutions" presented at the ESCIES website is a complement to this Handbook and cannot and does not aim to be exhaustive. To facilitate a timely update of the contents, the information is available as a downloadable document posted at the ESCIES web site: https://ESCIES.org

Bibliography

[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] W. E. Meyerhof, Elements of Nuclear Physics. New York: McGraw-Hill, 1967.

[6] 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.

[7] "Circumventing Radiation Effects By Logic Design: Cookbook", ESA contract 12495/97/NL/FM, Jul. 1999.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] S. Cristoloveanu S. S. Li, Electrical Characterization of Silicon-On-Insulator Materials and Devices. Springer, 1995.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] H. M. Manasevit W. I. Simpson, "Single-crystal silicon on a sapphire substrate”, Journal of Applied Physics, vol. 35, no. 4, p. 1349, 1964.

[22] 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.

[23] T. Sato, J. Iwamura, H. Tango, K. Doi, "CMOS/SOS VLSI technology”, Material Research Society Proceedings, vol. 33, p. 3, 1984.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] D. R. Alexander, "Transient ionizing radiation effects in devices and circuits", Nuclear Science, IEEE Transactions on , vol. 50, no. 3, p. 565, Jun. 2003.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.,

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] T. N. Bhar, R. J. Lambert, H. L. Hughes, "Electron trapping in Si implanted SlMOX", Electronics Letters, vol. 10, pp. 1026-1027, May 1998.

[56] 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.

[57] 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.

[58] 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.

[59] A. H. Johnston, "Scaling and Technology Issues for Soft Error Rates", 4th Annual Research Conference on Reliability, Stanford University, pp. 4-5, Oct. 2000.

[60] 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.

[61] 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.

[62] 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

[63] 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.

[64] 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

[65] 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.

[66] 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.

[67] D. R. Alexander, "Design issues for radiation tolerant microcircuits for space", Short Course of the Nuclear and Space Radiation Effects Conference (NSREC), Jul. 1996.

[68] 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.

[69] G. Anelli et al., "Total dose behaviour of submicron and deep submicron CMOS technologies", Workshop on Electronics for LHC Experiments, p. 139, 1997.

[70] 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.

[71] 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.

[72] 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.

[73] F. Faccio, "Design Hardening Methodologies for ASICs", in Radiation Effects on Embedded Systems, Springer, Ed. 2007.

[74] 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.

[75] 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.

[76] L. R. Rockett D. J. Kouba, "Radiation Hardened 150nm Standard Cell ASIC Design Library for Space Applications", Aerospace Conference, 2008 IEEE , Mar. 2008.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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

[85] 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

[86] Cobham (former Aeroflex) Gaisler. [Online]. http://www.gaisler.com/cms/index.php?option=com_content&task=view&id=194&Itemid=139

[87] Cobham (former Aeroflex). (2009, Nov.) Datasheet: UT0,6µCRH Commercial RadHard Gate Array Family. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/ut06crhsrh.pdf

[88] Cobham (former Aeroflex). (2009, Nov.) Advanced Data Sheet: UT0,25µHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/ut025asic.pdf

[89] Cobham (former Aeroflex). (2010, Aug.) Advanced Data Sheet: UT130nHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/UT130nmHBD.pdf

[90] Cobham (former Aeroflex). (2010, Jul.) Advanced Data Sheet: UT90nHBD Hardened-by-Design (HBD) Standard Cell. [Online]. http://www.aeroflex.com/ams/pagesproduct/datasheets/UT90nHBDdatasheet.pdf

[91] ATK, "Application Note for the 0,35µ Radiation Hardened Standard Cell Library", Jan. 2004.

[92] L. Dugoujon. (2010, Mar.) ST Microelectronics: DSM ASIC Technology & HSSL (KIPSAT). [Online]. http://microelectronics.esa.int/mpd2010/day2/DSM65nm.pdf

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] R. R. Troutman, Latchup in CMOS technology: the problem and its cure, Springer, Ed. 1986.

[99] A. Hastings, The Art of Analog Layout, 2nd ed., Prentice-Hall, Ed. New York, 2005,

[100] 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.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] 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.

[106] Q. Zhou K. Mohanram, "Transistor Sizing for Radiation Hardening", Proc. of 42nd IEEE IPRS, 2004.

[107] 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.

[108] 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.

[109] 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.

[110] 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.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

[115] 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.

[116] 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.

[117] 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.

[118] 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.

[119] 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.

[120] 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.

[121] 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.

[122] 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.

[123] 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.

[124] 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.

[125] 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.

[126] 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.

[127] 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.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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.

[136] 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.

[137] 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.

[138] 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.

[139] 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.

[140] 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.

[141] 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.

[142] 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.

[143] M. Nicolaidis, "Design for soft error mitigation", Device and Materials Reliability, IEEE Transactions on , vol. 5, no. 3, pp. 405-418, Sep. 2005.

[144] 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.

[145] 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.

[146] 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,

[147] 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.

[148] 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.

[149] D. G. Mavis P. H. Eaton, "Soft error rate mitigation techniques for modern microcircuits”, Reliability Physics Symposium Proceedings, 2002. 40th Annual , p. 216, 2002.

[150] 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.

[151] 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.

[152] 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.

[153] Actel, Application note AC128: Design Techniques for radiation-hardened FPGAs. http://www.microsemi.com/document-portal/doc_download/129913-ac128-design-techniques-for-radhard-fpgas-app-note

[154] 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.

[155] A. Manuzzato, "Single Event Effects on FPGAs, Phd”, 2009.

[156] Xilinx, Application note 197: Triple Module Redundancy Design Techniques for Virtex FPGAs. 2001.

[157] 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.

[158] 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.

[159] 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.

[160] 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.

[161] L. Sterpone, Electronics System Design Techniques for Safety Critical Applications, Springer, Ed. 2008.

[162] 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.

[163] 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.

[164] Xilinx, Application note 138: Virtex FPGA Series Configuration and Readback. 2005.

[165] Xilinx, Application note 151: Virtex Series Configuration Architecture User Guide. 2004.

[166] C. Carmichael, M. Caffrey, A. Salazar, "Correcting Single-Event Upset through Virtex Partial Reconfiguration", Xilinx Application Notes, XAPP216, 2000.

[167] 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.

[168] T. K. Moon, Error Correction Coding: Mathematical Methods and Algorithms. Wiley-Interscience, 2005.

[169] M. S. Liu, G. A. Shaw, J. Yue, "Fabrication of stabilized polysilicon resistors for SEU control", Patent United States Patent 5212108, May 18, 1993.

[170] 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.

[171] 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.

[172] 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.

[173] 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.

[174] L. Geppert, "A Static RAM Says Goodbye to Data Errors", IEEE Spectrum, Feb. 2004.

[175] 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.

[176] 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.

[177] L. R. Rockett, "An SEU-hardened CMOS data latch design", Nuclear Science, IEEE Transactions on, vol. 35, no. 6, pp. 1682-1687, Aug. 2002.,

[178] 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.

[179] 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.

[180] 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.

[181] 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.

[182] 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.

[183] 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.

[184] 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.

[185] 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.

[186] 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.

[187] 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.

[188] 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.

[189] 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.

[190] 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.

[191] 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.

[192] O. Golubeva, M. Rebaudengo, M. Sonza Reorda, M. Violante, Software-Implemented Hardware Fault Tolerance. Media, Springer Science+Business, 2006.

[193] 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.

[194] 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

[195] 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.

[196] 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.

[197] 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.

[198] Space Micro inc. - Space Electronics Division Products. [Online]. http://www.spacemicro.com/space_div/se_div.htm

[199] 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

[200] 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.

[201] 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.

[202] 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.

[203] M. Pignol, "COTS-based applications in space avionics", Design, Automation & Test in Europe Conference & Exhibition (DATE), 2010, pp. 1213-1219, 2010.

[204] T. C. Bressoud F. B. Schneider, "Hypervisor-based fault tolerance", ACM Transactions on Computer Systems, vol. 14, no. 1, pp. 80-107, 1996.

[205] 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.

[206] M. Masmano, I. Ripoll, A. Crespo, "XtratuM: a Hypervisor for Safety Critical Embedded Systems", Instituto de Informatica Industrial, Universidad Politecnica de Valencia.

[207] 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.

[208] E. C. Smith, "Effects of realistic satellite shielding on SEE rates ", Nuclear Science, IEEE Transactions on , vol. 41, no. 6, pp. 2396-2399, 1994.

[209] 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.

[210] 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.

[211] S. B. Guetersloh, C. Zeitlin, L. H. Heilbronn, J. Miller, "Effectiveness of shielding materials for dose reduction”, Aerospace Conference, 2006 IEEE , 2006.

[212] J. H. Adams, "The Natural Radiation Environment inside Spacecraft”, Nuclear Science, IEEE Transactions on, vol. 29, no. 6, p. 2095, Dec. 1982.

[213] 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.

[214] 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.

[215] 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.

[216] 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.

[217] 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.

[218] B. Johlander. (2004) ESCIES. [Online]. https://escies.org/GetFile?rsrcid=879

[219] 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.,

[220] 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.

[221] D. Powell, A Generic Fault-Tolerant Architecture for Real-Time Dependable Systems. Boston: Kluwer Academic Publishers, 2001.

[222] 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.

[223] 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.

[224] Maxwell Technologies. [Online]. http://about.maxwell.com/microelectronics/products/sbc/scs750.asp

[225] J. Baylis, Error Correcting Codes: A Mathematical Introduction. Boca Raton, FL: CRC Press, 1998.

[226] E. R. Berlekamp, Algebraic Coding Theory, Revised edition ed. Aegean Park Pr, 1984.

[227] F. J. MacWilliams N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland Mathematical Library, 1977.

[228] R. Schriebman, "Error Correcting Codes", Apr. 2006.

[229] E. R. Berlekamp, "Nonbinary BCH decoding", Information Theory, IEEE Transactions on, vol. 14, no. 2, pp. 242-242, Mar. 1968.

[230] S. B. Wicker V. K. E. Bhargava, Reed-Solomon codes and their applications, 1st ed. IEEE press, Piscataway, 1994.

[231] P. White A. Kisin, "Parallel RS Encoders and Decoders in SDRAM Memory for Space Applications", MAPLD Conference, 2003,

[232] G. Mitchell, "Investigation of Hamming, Reed-Solomon, and Turbo Forward Error Correcting Codes", Army Research Laboratory ARL-TR-4901, 2009.

[233] 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.

[234] H. H. K. Tang E. H. Cannon, "SEMM-2: a modeling system for single event upset analysis", Nuclear Science, IEEE Transactions on, vol. 51, no. 6, pp. 3342-3348, Dec. 2004.

[235] R. A. Weller, M. H. Mendenhall, R. A. Reed, R. D. Schrimpf, K. M. Warren, B. D. Sierawski, L. W. Massengill, "Monte Carlo Simulation of Single Event Effects", Nuclear Science, IEEE Transactions on, vol. 57, no. 4, pp. 1726-1746, Aug. 2010.

[236] R. A. Weller, R. A. Reed, K. M. Warren, M. H. Mendenhall, B. D. Sierawski, R. D. Schrimpf, L. W. Massengill, "General Framework for Single Event Effects Rate Prediction in Microelectronics", Nuclear Science, IEEE Transactions on, vol. 56, no. 6, pp. 3098-3108, Dec. 2009.

[237] G. Hubert, N. Buard, C. Weulersse, T. Carriere, M. C. Palau, J. M. Palau, D. Lambert, J. Baggio, F. Wrobel, F. Saigne, R. Gaillard, "A review of DASIE code family: contribution to SEU/MBU understanding", On-Line Testing Symposium, 2005. IOLTS 2005. 11th IEEE International, pp. 87-94, Jul. 2005.

[238] 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.

[239] 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.

[240] 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.

[241] 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.

[242] B. Sherman M. Cuviello, "NASA's LWS/SET technology experiment carrier", Aerospace Conference, 2003. Proceedings. 2003 IEEE , vol. 1, Mar. 2003.

[243] 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.

[244] 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.

[245] 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.

[246] JEDEC standard, Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices. JESD89, 2001.

[247] V. Pouget, D. Lewis, P. Fouillat, "Time-resolved scanning of integrated circuits with a pulsed laser: application to transient fault injection in an ADC", Instrumentation and Measurement, IEEE Transactions on, vol. 53, no. 4, pp. 1227-1231, Aug. 2004.

[248] F. Miller, N. Buard, G. Hubert, S. Alestra, G. Baudrillard, T. Carriere, R. Gaillard, J. M. Palau, F. Saigne, P. Fouillat, "Laser Mapping of SRAM Sensitive Cells: A Way to Obtain Input Parameters for DASIE Calculation Code", Nuclear Science, IEEE Transactions on, vol. 53, no. 4, pp. 1863-1870, Aug. 2006.

[249] D. McMorrow, W. T. Lotshaw, J. S. Melinger, S. Buchner, R. L. Pease, "Subbandgap laser-induced single event effects: carrier generation via two-photon absorption", Nuclear Science, IEEE Transactions on, vol. 49, no. 6, pp. 3002-3008, Dec. 2002.

[250] F. Darracq, H. Lapuyade, N. Buard, F. Mounsi, B. Foucher, P. Fouillat, M. C. Calvet, R. Dufayel, "Backside SEU laser testing for commercial off-the-shelf SRAMs", Nuclear Science, IEEE Transactions on, vol. 49, no. 6, pp. 2977-2983, Dec. 2002.

[251] F. Miller, N. Buard, T. Carriere, R. Dufayel, R. Gaillard, P. Poirot, J. M. Palau, B. Sagnes, P. Fouillat, "Effects of beam spot size on the correlation between laser and heavy ion SEU testing", Nuclear Science, IEEE Transactions on, vol. 51, no. 6, pp. 3708-3715, Dec. 2004,

[252] D. McMorrow, S. Buchner, M. Baze, B. Bartholet, R. Katz, M. O'Bryan, C. Poivey, K. A. LaBel, R. Ladbury, M. Maher, F. W. Sexton, "Laser-Induced Latchup Screening and Mitigation in CMOS Devices", Nuclear Science, IEEE Transactions on, vol. 53, no. 6, pp. 1819-1824, Aug. 2006.

[253] A. Bougerol, F. Miller, N. Guibbaud, R. Gaillard, F. Moliere, N. Buard, "Use of Laser to Explain Heavy Ion Induced SEFIs in SDRAMs", Nuclear Science, IEEE Transactions on, vol. 57, no. 1, pp. 272-278, Feb. 2010.

[254] A. H. Johnston T. F. Miyahira, "Latchup Test Considerations for Analog-to-Digital Converters", SEE symposium, Apr. 2000.

[255] 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.

[256] 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.

[257] D. K. Pradhan, Fault-Tolerant Computer System Design. Prentice Hall, 1994.

[258] "Davinci Three Dimensional Device Simulation Program Manual", Synopsys, 2003.

[259] "Taurus Process/Device User Manual", Synopsys, 2003.

[260] "Athena/Atlas User's Manual", Silvaco int, 1997.

[261] "DESSIS User's Manual", ISE release 6, vol. 4, 2000.

[262] 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.

[263] 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.

[264] 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.

[265] 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.

[266] 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.

[267] 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.

[268] 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,

[269] 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.

[270] 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.

[271] 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.

[272] 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.

[273] P. Sundararajan B. Blodget, "Estimation of mean time between failure caused by single event upset", Xilinx Application Notes, XAPP559, Jan. 2005.

[274] 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.

[275] 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.

[276] C. Carmichael, "Triple module redundancy design techniques for virtex FPGAs", Xilinx Application Notes, XAPP197, Nov. 2001.,

[277] "TMRTool User Guide", Xilinx User Guide, UG156.

[278] JAXA - REIMEI (INDEX) satellite. [Online]. http://www.jaxa.jp/projects/sat/index/index_e.html

[279] CNES MYRIADE satellite. [Online]. http://smsc.cnes.fr/MYRIADE/GP_plateforme.htm

[280] ESA Space Environment Information System (SPENVIS) Geant4 tools. [Online]. https://www.spenvis.oma.be/help/background/geant4/geant4.html

[281] B. Cooke, "Reed-Muller Error Correcting Codes", MIT Undergraduate Journal of Mathematics, pp. 21-26, 2006.

[282] 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.,

[283] 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.

[284] 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.

[285] J. R. Schwank, M. R. Shaneyfelt, B. L. Draper and P. E. Dodd, "BUSFET—A radiation-hardened SOI transistor", IEEE Trans. Nucl. Sci., vol. 46, no. 6, pp. 1809– 1816, Dec.1999.

[286] Jianjun Chen, Shuming Chen, "Novel Layout Technique for Single-Event Transient Mitigation Using Dummy Transistor", IEEE Trans. Dev. and Mat. Rel., vol. 13, no. 1, pp. 177-184, March 2013.

[287] S. Jagannathan, M. J. Gadlage, B. L. Bhuva, R. D. Schrimpf, B. Narasimham, J. Chetia, J. R. Ahlbin, and L. W. Massengill, "Independent measurement of SET pulse widths from N-hits and P-hits in 65-nm CMOS", *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, pp. 3386–3391, Dec. 2010.

[288] J. J. Chen, S. M. Chen, B. Liang, and B. W. Liu, "Simulation study of the layout technique for P-hit single-event transient mitigation via the sourceisolation", *IEEE Trans. Device Mater. Rel.*, vol. 12, no. 2, pp. 501–509, Jun. 2012.

[289] M. P. Baze, S. P. Buchner, and D. McMorrow, "A digital CMOS design technique for SEU hardening", *IEEE Trans. Nucl. Sci.*, vol. 47, no. 6, pp. 2603–2608, Dec. 2000.

[290] K. P. Rodbell, D. F. Heidel, J. A. Pellish, P. W. Marshall, H. H. K. Tang, C. E. Murray, K. A. LaBel, M. S. Gordon, K. G. Stawiasz, J. R. Schwank, M. D. Berg, H. S. Kim,M. R. Friendlich, A.M. Phan, and C.M. Seidleck, "32 and 45 nm radiation-hardened-by-design (RHBD) SOI latches", *IEEE Trans. Nucl. Sci.*, vol. 58, no. 6, pp. 2702–2710, Dec. 2011.

[291] J. J. Chen, S. M. Chen, B. Liang, B. Liu, and F. Liu, "Radiation hardened by design techniques to reduce single event transient pulse width based on the physical mechanism", *Microelectron. Reliab.*, vol. 52, no. 6, pp. 1227–1232, Jun. 2012.

[292] T. Roy, A. F.Witulski, R. D. Schrimpf, M. L. Alles, and L.W. Massengill, "Single event mechanisms in 90 nm triple-well CMOS devices", *IEEE Trans. Nucl. Sci.*, vol. 55, no. 6, pp. 2948–2956, Dec. 2008.,

[293] Jonathan Heiner, Nathan Collins, and Michael Wirthlin, "Fault Tolerant ICAP Controller for High-Reliable Internal Scrubbing", IEEE Aerospace Conference, March 2008.

[294] Neyer, A.; Wunderlich, R.; Heinen, S., " An all-digital PLL for satellite based navigation in 90 nm CMOS" , Circuits and Systems and TAISA Conference, 2009 NEWCAS-TAISA '09.

[295] SEUs Simulation Tool, Universidad de Nebrija and ESA; http://www.nebrija.es/~jmaestro/esa/sst.html

[296] C. Bernardeschi, L. Cassano, A. Domenici, and L. Sterpone, "ASSESS: A Simulator of Soft Errors in the Configuration Memory of SRAM-based FPGAs", In IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems Volume: 33, Issue: 9, Pages: 1342-1355, Sept. 2014

[297] "FLIPPER" fault injection tools for SRAM-based FPGAs, INAF/IASF, http://cosy.iasf-milano.inaf.it/flipper_index.htm

[298] "FT-UNSHADES" fault injection and analysis tool for ASIC and FPGA netlists, Escuela Superior de Ingenieros. Universidad de Sevilla, http://ftu.us.es/

[299] H. Guzmán-Miranda, J. N. Tombs, M. A. Aguirre, " FT-UNSHADES-uP: A platform for the analysis and optimal hardening of embedded systems in radiation environments", Escuela Superior de Ingenieros. Universidad de Sevilla, IEEE Industrial Electronics 2008

[300] Mogollón, Juan M., Guzmán Miranda, Hipólito, Nápoles Luengo, Javier, Aguirre M.A., "Metrics for the Measurement of the Quality of Stimuli in Radiation Testing Using Fast Hardware Emulation", IEEE Transactions on Nuclear Science. 2013. Vol. 60. Num. 4. Pag. 2450-2460.

[301] Roche, P.; STMicroelectron., Crolles, France ; Gasiot, G.; Autran, J.L.; Munteanu, D.; " Application of the TIARA Radiation Transport Tool to Single Event Effects Simulation", http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=23 (Volume:61, Issue: 3), Pag. 1498-1500.,

[302] A. Ammari, L. Anghel, R. Leveugle, C. Lazzari, R. Reis, " SET Fault Injection Methods in Analog Circuits: Case Study", TIMA, http://tima.imag.fr/alfa-nicron/documents/8set_fault.pdf

[303] Do, E.; Liberali, V.; Stabile, A.; Calligaro, C., " Layout-oriented simulation of non-destructive single event effects in CMOS IC blocks", Radiation and Its Effects on Components and Systems (RADECS), 2009.

[304] JL Autran, P Roche, S Sauze, G Gasiot, D Munteanu, P Loaiza, M Zampaolo, J Borel, "Altitude and underground real-time SER characterization of CMOS 65 nm SRAM", IEEE Transactions on Nuclear Science, 2009.

[305] Susana MARTÍN BARBERO , Stefan K. HÖFFGEN , Guy BERGER , Héctor GUERRERO, " COMPENDIUM OF INTERNATIONAL IRRADIATION TEST FACILITIES", presented and distributed at RADECS 2011, Seville, Spain. Available on-line: http://acdc.sav.us.es/cna/images/documentos/Irradiation%20Facilities%20Catalogue%20RADECS%202011.pdf

[306] RADLAS 2013, 4th Thematic Workshop on Laser Testing of Radiation Effects, Paris, France, http://www.ies.univ-montp2.fr/radlas2013/

[307] Stephen P. Buchner, Florent Miller, Vincent Pouget and Dale P. McMorrow, "Pulsed-Laser Testing for Single-Event Effects Investigations", IEEE Transactions on Nuclear Science, vol. 60, no. 3, June 2013.

[308] S. Yoshimoto, T. Amashita, D. Kozuwa, T. Takata, M. Yoshimura, Y. Matsunaga, H. Yasuura, H. Kawaguchi, and M. Yoshimoto, "Multiple-bit-upset and single-bit-upset resilient 8T SRAM bitcell layout with divided wordline structure", 2011 IEEE 17th International On-Line Testing Symposium.

[309] C. L. Chen and M. Y. Hsiao, “Error-correcting codes for semiconductor memory applications: a state-of-the-art review”, IBM Journal of Research and Development 28(2), 1984, pp. 124-134.

[310] M. Y. Hsiao "A Class of Optimal Minimum Odd-weight-column SEC-DED codes", IBM Journal of Reserach and Development, vol 14, pp. 395--301, 1970.

[311] S. Ghosh and P. D. Lincoln, “Low-Density Parity Check Codes for Error Correction in Nanoscale Memory”, SRI Computer Science Laboratory Technical Report, CSL-0703, 2007

[312] S. Liu, P. Reviriego, J.A. Maestro, "Efficient Majority Logic Fault Detection with Difference-Set Codes for Memory Applications", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 20, No 1, January 2012, pp. 148-156.

[313] R. A. Cliff, V. Danchenko, E. G. Stassinopoulos, M. Sing, G. J. Brucker, and R. S. Ohanian, “Prediction and measurement of radiation damage to CMOS devices on board spacecraft”, IEEE Trans. Nucl. Sci., vol. 23, no. 6, pp. 1781–1788, Dec. 1976.

[314] Fortescue, Peter, John Stark, and Graham Swinerd. Spacecraft systems engineering. 3rd ed. John Wiley and Sons, 2003.

[315] Kirill Tsytsura, " AXIOM: Advanced X-ray Imaging of the Magnetosphere", III. Space Environment, UCL DEPARTMENT OF SPACE & CLIMATE PHYSICS, MULLARD SPACE SCIENCE LABORATORY, http://www.mssl.ucl.ac.uk/~gbr/kirill/environment.html

[316] M. Desogus, L. Sterpone, D. Merodio Codinachs, "Validation of a tool for estimating the effects of soft-errors on modern SRAM-based FPGAs", 2014, IEEE 20th International On-line Testing Symposium, 2014, pp. 111-115

[317] SEUXSE and NASA MISSE SpaceCube experiments to test the radiation tolerance of Xilinx FPGA and on-board computer technology https://nepp.nasa.gov/mapld_2008/presentations/t/08%20-%20Blansett_Ethan_mapld08_pres_1.pdf

[318] http://www.nasa.gov/mission_pages/station/research/experiments/1314.html#description

[319] Menichelli, M.; Alpat, B.; Battiston, R.; Bizzarri, M.; Blasko, S.;Burger, J.; Caraffini, D.; Gil, E.C.; Dai, T.; Haller, C.; Kounine, A.; Maris, O.; Papi, A.; Plyaskine, V.; Schartd, D.; Simon, R.S.;Steuer, M., " SEE tests for commercial off-the-shelf DSPs to be used in a space experiment", Radiation Effects Data Workshop, 2001 IEEE

[320] Bertazzoni, S.; Di Giovenale, D.; Mongiardo, L.; Salmeri, M.;Mencattini, A.; Salsano, A.; Bisello, D.; Candelori, A.; Giubilato, Piero; Kaminski, A.; Nigro, M.; Rando, R.; Wyss, J.; Lora, S. , " TID and SEE characterization and damaging analysis of 256 Mbit COTS SDRAM for IBEM application", 8th European Conference on Radiation and Its Effects on Components and Systems, 2005. RADECS 2005.

[321] M. Lauriente, A. L. Vampola, "Spacecraft anomalies due to radiation environment in space”, NASDA/JAERI 2nd International Workshop on Radiation Effects of Semiconductor Devices for Space Applications, Tokyo, Japan, March 1996.

[322] Reviriego, P.; Maestro, Juan Antonio; Sanghyeon Baeg; ShiJie Wen; Wong, R. , " Protection of Memories Suffering MCUs Through the Selection of the Optimal Interleaving Distance", IEEE Transactions on Nuclear Science, Vol. 57, No 4(1), August 2010, pp. 2124-2128.

[323] Reviriego, P.; Bleakley, C.; Maestro, Juan Antonio; O'Donnell, Anne, “Offset DMR: A Low Overhead Soft Error Detection and Correction Technique for Transform-Based Convolution”, IEEE Transactions on Computers (Volume:60 , Issue: 10), Oct. 2011, pag. 1511-1516

[324] LEON2FT HDL IP Core, http://www.esa.int/Our_Activities/Space_Engineering_Technology/Microelectronics/LEON2-FT_-_HDL

[325] William A. Howes , “On-Orbit FPGA SEU Mitigation and Measurement Experiments on the Cibola Flight Experiment Satellite”, 2011, Brigham Young University ScholarsArchive, http://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=3473&context=etd

[326] Riaz Naseer, Jeff Draper, Younes Boulghassoul ; Sandeepan DasGupta, Art Witulski , “Critical Charge and SET Pulse Widths for Combinational Logic in Commercial 90nm CMOS Technology”, 2007, Great Lakes Symposium on VLSI (GLSVLSI), March 11–13, 2007, Stresa-Lago Maggiore, Italy; http://www.isi.edu/~draper/papers/glsvlsi07.pdf

[327] Single event transient mitigation and measurement in integrated circuits, by Actel Corporation, US7772874, Aug 2010

[328] Method and system for reducing glitch effects within combinational logic, by Honeywell International, Inc., US7193451 *, Mar 2007

[329] Rezgui et al.; "New Methodologies for SET Characterization and Mitigation in Flash-Based FPGAs"; Publication Year: 2007; Nuclear Science, IEEE Transactions on; vol. 54 , Issue: 6 , Part: 1; pp. 2512-2524.

[330] Zhengfeng Huang , “A high performance SEU-tolerant latch for nanoscale CMOS technology“, Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014

[331] Melanie D. Berg, Hak S. Kim, Kenneth A. LaBel, Anthony D. Phan, Christina M. Seidlick, “An Analysis of Heavy-Ion Single Event Effects for a Variety of Finite State-Machine Mitigation Strategies”, MAPLD 2014 , NASA Technical Reports Server (NTRS), http://ntrs.nasa.gov/search.jsp?R=20140008975

[332] Microsemi RTAX-S/SL and RTAX-DSP Radiation-Tolerant FPGAs (Data Sheet) http://www.actel.com/documents/RTAXS_DS.pdf

[333] Particle Test of Xilinx Virtex-II FPGA using XTMR Mitigation Technique, Saab Ericsson Space & ESA, QCA Final Presentation Day 8, January 2007 https://escies.org/download/webDocumentFile?id=5483

[334] Application-Like Radiation Test of XTMR & FTMR Mitigation Techniques for Xilinx Virtex-II FPGA, Saab Ericsson Space & ESA, Nov 2004 https://escies.org/download/webDocumentFile?id=888

[335] F. Sturesson, S. Mattsson, C. Carmichael, R. Harhoe-Ssrensen, “Heavy Ion Characterization of SEU Mitigation Methods for the Virtex FPGA”, RADECS 2001

[336] Accuro, rExplore and Roplace tools by RobustChip http://www.robustchip.com

[337] Lilja, K. ; Bounasser, M. ; Wen, S. J. ; Wong, R , “Single-Event Performance and Layout Optimization of Flip-Flops in a 28-nm Bulk Technology”, Nuclear Science, IEEE Transactions on (Volume:60, Issue: 4), Aug. 2013

[338] CARMEN-2 experiment on-board JASON satellite. https://jason.cnes.fr/en/JASON2/carmen2.htm

[339] D. G. Mavis, P. H. Eaton, M. D. Sibley, R. C. Lacoe, E. J. Smith, and K. A. Avery , “Multiple Bit Upsets and Error Mitigation in Ultra-Deep Submicron SRAMS”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 55, NO. 6, DECEMBER 2008

[340] Hagemeyer, J.; Hilgenstein, A.; Jungewelter, D.; Cozzi, D.; Felicetti, C.; Rueckert, U.; Korf, S.; Koester, M.; Margaglia, F.; Porrmann, M.; Dittmann, F.; Ditze, M.; Harris, J.; Sterpone, L.; Ilstad, J., "A scalable platform for run-time reconfigurable satellite payload processing”, in *Adaptive Hardware and Systems (AHS), 2012 NASA/ESA Conference on* , vol., no., pp.9-16, 25-28 June 2012

[341] Cassano, Luca; Cozzi, Dario; Korf, Sebastian; Hagemeyer, Jens; Porrmann, Mario; Sterpone, Luca, "On-line testing of permanent radiation effects in reconfigurable systems”, in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013* , vol., no., pp.717-720, 18-22 March 2013

[342] Sorrenti, D.; Cozzi, D.; Korf, S.; Cassano, L.; Hagemeyer, J.; Porrmann, M.; Bernardeschi, C., "Exploiting dynamic partial reconfiguration for on-line on-demand testing of permanent faults in reconfigurable systems”, in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2014 IEEE International Symposium on* , vol., no., pp.203-208, 1-3 Oct. 2014

[343] R. Glein, B. Schmidt, F. Rittner, J. Teich, and D. Ziener, “A Self-Adaptive SEU Mitigation System for FPGAs with an Internal Block RAM Radiation Particle Sensor”, in IEEE 22nd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2014, pp. 251–258

[344] A. Jacobs, G. Cieslewski, A. D. George, A. Gordon-Ross, and H. Lam, “Reconfigurable Fault Tolerance: A Comprehensive Framework for Reliable and Adaptive FPGA-Based Space Computing”, ACM Trans. Reconfigurable Technol. Syst., vol. 5, no. 4, pp. 21:1–21:30, Dec. 2012.

[345] W. A.. Kolasinski, J. B. Blake, J. K. Anthony, W. E. Price, and E. C. Smith, “Simulation of cosmic-ray induced soft errors and latchup in integrated circuit computer memories”, *IEEE Trans. Nucl. Sci.*, vol. 26, pp. 5087–5091, Dec. 1979

[346] **OMERE** (Outil de Modélisation de l'Environnement Radiatif Externe), http://www.trad.fr/OMERE-Software.html