Die approbierte Originalversion dieser Dissertation ist in der Hauptbibliothek der Technischen Universität Wien aufgestellt und zugänglich.
http://www.ub.tuwien.ac.at

TU UB WIEN Universitätsbibliothek

The approved original version of this thesis is available at the main library of the Vienna University of Technology.
http://www.ub.tuwien.ac.at/eng

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Design of Custom ASIC for Radiation Experiments to Study Single Event Effects

PhD THESIS

zur Erlangung des akademischen Grades

Doktor/in der technischen Wissenschaften

eingereicht von

Varadan Savulimedu Veeravalli
Matrikelnummer 1127877

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Dr.techn. Andreas STEININGER

Diese Dissertation haben begutachtet:

(Prof. Dr. Cecilia Metra) (Prof. Dr. Milos Krstic)

Wien, 12.10.2017

(Varadan Savulimedu Veeravalli)

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Design of Custom ASIC for Radiation Experiments to Study Single Event Effects

PhD THESIS

submitted in partial fulfillment of the requirements for the degree of

Doktor/in der technischen Wissenschaften

by

Varadan Savulimedu Veeravalli
Registration Number 1127877

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Ao.Univ.Prof. Dr.techn. Andreas STEININGER

The dissertation has been reviewed by:

(Prof. Dr. Cecilia Metra)

(Prof. Dr. Milos Krstic)

Wien, 12.10.2017

(Varadan Savulimedu Veeravalli)

Erklärung zur Verfassung der Arbeit

Varadan Savulimedu Veeravalli
Treitlstrasse, 3, 2nd Floor, E182/2

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

(Ort, Datum) (Unterschrift Verfasser)

Acknowledgements

First and foremost I would like to express my deepest appreciation to Prof. Andreas Steininger and Prof. Ulrich Schmid for presenting me the opportunity to work in the FATAL project that laid the foundation for this thesis.

Without Prof. Andreas Steininger's guidance, patience and encouragement this dissertation would not have been possible. He provided me the opportunity to work with different international groups to have a deeper understanding about radiation effects in digital circuits. I am grateful for his relentless support in overcoming numerous obstacles that I have been facing through my research.

I would like to thank my colleagues from the Embedded Computing Systems group, Jakob, Alexander, Rameez, Thomas, Robert, and Martin who took part in my activities from long research discussions to spicy luncheons. A special thanks goes to Florian for helping me translate my abstract from English to German. I would like to pay my gratitude to technical staff Karl Malle and Heinz Deinhart for their support. I would especially like to thank the department secretary Traude Sommer for her support and efforts in teaching me German.

I would also like to thank Dr. Cecilia Metra and Dr. Milos Kristic for taking their valuable time to be on my committee.

Last but not the least I would like to acknowledge my wife Nityaa for her continuous support throughout this thesis. She stood by me through thick and thin and I would have never achieved this milestone in my life without her persisting motivation and hard work.

I will never be able to thank everyone enough for making my life at the institute very comfortable and at the same time keeping me sane. I will always cherish the memories I made with you all.

Dedication

To my wife Nityaa and my children Vaishali and Vishwa without whom this thesis would have been complete three years earlier

Abstract

Technology scaling has made the transistors increasingly susceptible to radiation particle strikes. As a consequence, particles with lower energy – which are substantially more frequent – can already cause non-destructive single event effects in CMOS circuits. Understanding them is not very straightforward, as there are so many parameters involved along with these effects, like radiation particle strikes' strength, target circuit, path of propagation, and surrounding environment. Our goal in this thesis is to study these effects in digital CMOS circuits and aid construction of efficient radiation tolerant circuits. Firstly, the effectiveness of the existing radiation hardening techniques to particle hits in digital CMOS circuits has been mainly studied in this thesis (under a given set of environmental conditions). We explicitly analyze how the performance of two selected radiation hardening techniques, namely transistor sizing and stack separation, when exposed to particle hits varies with temperature and supply voltage.

We present design aims and concepts as well as implementation results of a digital ASIC that is dedicated as a target for long-term irradiation experiments. Its sole purpose is to study susceptibility to radiation as well as propagation of radiation effects, and aid in understanding the same. The infrastructure should be able to record the SETs, in spite of the need of being tolerant to particle strikes in itself that cannot be avoided in some types of radiation experiments. The problem of devising a suitable infrastructure lies in the partly contradictory requirements, like constrained area, radiation tolerance and good resolution of the location and propagation path of particle hits. This was a major challenge in our thesis.

To analyze *single-event-transient* (SET) sensitivity in digital CMOS circuits we propose an on-chip measurement architecture for various target circuit blocks. We also propose an architecture that allows tracing, generation and propagation of SETs in the Sklansky adder and inverter tree. Our measurement architectures are based on non-rad-hard counters namely, linear feedback shift registers and Muller pipeline based up/down counters. The design evaluation is done by means of comprehensive fault injection experiments, which are based on detailed Spice models of the target circuits in conjunction with a standard double-exponential current injection model for single-event transients (SET). We show that the infrastructure is resilient against double faults, as well as many triple and even higher-multiplicity faults. Together with a probabilistic analysis and fault dictionary we can conclude that the proposed architectures will indeed sustain significant target hit rates, without exceeding the resilience bound of the measurement infrastructure.

Finally to measure SET pulsewidths in any digital circuit a unique on-chip measurement infrastructure is proposed. Unlike the known oscilloscope-based methods, our approach is all-digital: SET durations are measured by the SET-gated counting of pulses generated by a high-frequency ring oscillator, and stored in an up/down-counter array organized in a ring. We carefully elaborate a comprehensive concept for making our infrastructure SEU tolerant, again with the main challenge being to attain a sufficiently high probability of recording useful hits in the target before exhausting the SEU tolerance of the infrastructure. Our key contribution here concerns the protection of the counter array: Rather than resorting to radiation hardening or explicit triple modular redundancy (TMR), we save area by using a novel redundant duplex counter architecture: For a small number of recorded SETs, our architecture implicitly implements TMR, albeit in a way that degrades gracefully for larger numbers of recorded SETs.

We have presented the measurement infrastructure and a detailed pre-fabrication analysis of the circuits hosted in the digital ASIC. We sketch our respective solutions for the on-chip transmission architecture and present the resulting area distribution of the final ASIC layout which has been performed for an industrial 65nm bulk CMOS process. We also show how we optimized the layout for the purpose of our experiments and present all relevant implementation details. The datasheet of the ASIC that is of paramount importance is presented in great detail. Moreover, an overview of the experimental setup is presented and some specific details are highlighted.

Kurzfassung

Die ständig voranschreitende Verkleinerung der Strukturbreiten integrierter digitaler Schaltungen macht die verwendeten Transistoren zunehmend anfällig für Strahlungseffekte. Das führt dazu, dass bereits Partikel mit geringer Energie, die wesentlich häufiger auftreten, transiente Fehler (engl. Single-Event-Transient - SET) in CMOS Schaltungen verursachen können. Da dabei der Einfluss vieler verschiedener Parameter, wie die Stärke des auftreffenden Partikels, der betroffene Schaltungsteil sowie der Ausbreitungspfad und die unmittelbare Umgebung des Einschlagortes, eine Rolle spielt, sind diese Effekte schwierig zu analysieren und charakterisieren. Das Ziel dieser Arbeit ist es, diese Strahlungseffekte in der CMOS Technologie zu untersuchen, um so die Entwicklung von effizienten strahlungsresistenten Schaltungen zu ermöglichen. Zunächst wird die Effektivität existierender Methoden zur Strahlungshärtung (unter gegebenen Umweltbedingungen) evaluiert. Hierbei konzentrieren wir uns auf die Analyse der Fragestellung, in welchem Ausmaß die Temperatur bzw. die Versorungspannung Einfluss auf die Wirksamkeit zweier bestimmter Methoden hat, nämlich “Transistor Sizing” und “Stack Separation”.

Weiters präsentieren wir Designziele und Konzepte, sowie Resultate aus der Implementierung eines digitalen ASICs, der für Langzeitstrahlungsmessungen entwickelt wurde. Dieser Chip soll dazu dienen, die Empfindlichkeit für, und die Ausbreitung von Strahlungseffekten zu untersuchen und besser zu verstehen. Die Messinfrastruktur muss in der Lage sein, SETs aufzuzeichnen und dabei aber selbst ein gewisses Maß an SET-Toleranz aufweisen, was bei Messungen dieser Art grundsätzlich nicht vermeidbar ist. Eine der größten Herausforderung dieser Arbeit war die Konzipierung dieser Infrastruktur. Dabei sind nämlich teilweise gegensätzliche Anforderungen, wie die eingeschränkte Chipfläche, gute Strahlungstoleranz, sowie eine möglichst gute Auflösung für die Erfassung des Einschlagortes und des Ausbreitungspfads eines auftreffenden Partikels, zu berücksichtigen.

Um die Empfindlichkeit von CMOS Schaltungen für SETs zu analysieren, schlagen wir eine auf den Chip integrierte Messeinrichtung vor, die es ermöglicht verschiedene Zielschaltungen zu untersuchen. Darüberhinaus stellen wir eine Architektur vor, die in der Lage ist die Erzeugung und Ausbreitung von SETs in Sklansky Addieren und Invertiererbäumen zu verfolgen. Den Kern unserer Messarchitekturen stellen nicht-strahlungsharte Zähler dar. Im speziellen kommen Linear Feedback Shift Register und auf Muller-Pipelines basierende Vor-/Rückwärtszähler zum Einsatz. Die Evaluierung des Designs erfolgt durch umfassende Fehlerinjektionsexperiemente, basierend auf detaillierten Spice Modellen der untersuchten Schal-

tung sowie des Standard doppelt exponentiellen Strompulsmodells für SETs. Mit diesen Untersuchungen können wir zeigen, dass unsere Messinfrastruktur robust gegen sämtliche Doppelfehler sowie etliche Dreifach- und Mehrfachfehler ist. Zusammen mit einer ergänzenden statischen Analyse kommen wir zu dem Schluss, dass die vorgestellte Architektur tatsächlich mit beträchtlichen Partikeleinschlagsraten umgehen kann, ohne dabei das Leistungsvermögen der Messinfrastruktur zu überschreiten.

Für die Messung der Pulsbreite von SETs in beliebigen digitalen Schaltungen stellen wir ebenfalls eine entsprechende Messeinrichtung vor. Im Gegensatz zu Methoden die auf Oszilloskopmessungen beruhen, ist unser Ansatz vollständig digital: Die SET-Dauer wird dabei durch SET-maskiertes Zählen von Pulsen, die von einem hochfrequenten Ringoszillator generiert werden, ermittelt. Die Ergebnisse werden in einem, als Ring organisierten, Array von Vor-/Rückwärtszählern gespeichert. Wir erarbeiten ein umfassendes Konzept um unsere Infrastruktur gegen SETs zu schützen, die sich in Speicherelementen manifestieren, wobei auch hier der Fokus darauf liegt, eine ausreichend hohe Wahrscheinlichkeit für das Auftreten eines SETs zu erreichen, ohne dabei die Toleranz der Messinfrastruktur zu überschreiten. Unser Hauptbeitrag konzentriert sich dabei auf den Schutz des Zählerarrays: Anstatt auf Strahlungshärtung oder explizite Dreifachredundanz (engl. Triple Modular Redundancy – TMR) zurückgreifen zu müssen, sparen wir Chipfläche durch eine neuartige Duplexzählerarchitektur. Für eine niedrige Anzahl an SETs implementiert unser Ansatz implizit ein TMR System, wobei dieses bei steigender Anzahl von SETs sogenanntes „graceful degradation“ Verhalten aufweist.

In der Arbeit präsentieren wir die komplette Messinfrastruktur, sowie detaillierte Vorproduktionsanalysen der enthaltenen Schaltungen. Weiter skizzieren wir unsere Lösungen für die auf dem Chip integrierte Übertragungsarchitektur und zeigen die resultierende Chipflächenverteilung des finalen ASIC-Layouts für einen industriellen 65nm Fertigungsprozess. Wir diskutieren ebenfalls die vorgenommenen Optimierungen, die angewendet wurden, um das Chiplayout auf die Anforderungen der Experimente anzupassen und dokumentieren alle relevanten Implementierungsdetails. Das Datenblatt des ASICs ist dabei von besonderer Wichtigkeit. Abschließend präsentieren wir einen Überblick über den Aufbau des Experiments, wobei einige wichtige Details besonders hervorgehoben werden.

Contents

List of Figures **xvii**

List of Tables **xxi**

1 Introduction **1**
1.1 Motivation . . . 2
1.1.1 SET Model . . . 3
1.1.2 Soft Error Rate . . . 3
1.1.2.1 SET Generation . . . 4
1.1.2.2 SET Propagation . . . 5
1.1.2.3 SET Masking . . . 6
1.1.3 Radiation Hardening Mechanisms . . . 7
1.2 Scope . . . 8
1.3 List of Key Contributions . . . 9
1.3.1 Design of Novel Radiation Hardening Mechanisms . . . 10
1.3.2 Innovative Measurement Infrastructure SET Sensitivity . . . 10
1.3.3 Novel Measurement Infrastructure for SET Propagation . . . 11
1.3.4 Unique Measurement Infrastructure for SET Pulse widths . . . 11
1.3.5 Design of Radiation Target ASIC . . . 12
1.4 Outline and Methodology . . . 12

2 SET Injection Mechanisms **15**
2.1 Background . . . 16
2.1.1 3D models . . . 17
2.1.2 Spice model . . . 18
2.1.2.1 Double Exponential Current Model . . . 20
2.1.2.2 Improved Current Model . . . 22
2.2 SET Simulation Model . . . 23
2.2.1 3D TCAD model . . . 24
2.2.2 Spice Model . . . 26
2.3 Spice Model Study - C-element Example . . . 29
2.3.1 Muller C-Element . . . 29
2.3.2 Variation Analysis . . . 32
2.3.3 Ramifications . . . 33
2.4 Simulation Setup for SET Analysis . . . 33

3 Radiation Hardening Mechanisms **35**
3.1 Background . . . 35
3.1.1 Device-level Hardening . . . 36
3.1.2 Circuit-level Hardening . . . 37
3.1.3 System-level Hardening . . . 38
3.2 Proposed Radiation Hardening Mechanisms for Muller C-Element . 39
3.2.1 Radiation Hardening by Sizing . . . 39
3.2.2 Dual Interlocked Storage Cell Mechanism . . . 40
3.2.3 Radiation Hardening by Separation Mechanism . . . 41
3.2.4 Summary . . . 41
3.3 Combinational Circuits . . . 42
3.3.1 SET Analysis – XOR gate . . . 43
3.3.2 Radiation Hardening Mechanisms . . . 44
3.3.2.1 Radiation-Hardening by Gate Sizing . . . 44
3.3.2.2 Defect-Tolerant Logic . . . 46
3.3.2.3 Analog Voter . . . 48
3.3.2.4 Radiation Hardening by Separation Mechanism . . 48
3.3.2.5 Code Word State Preserving (CWSP) Element . . 50
3.3.3 Summary . . . 52
3.4 Performance under VT Variations . . . 53
3.4.1 Target Circuits . . . 53
3.4.1.1 Sizing Requirements for Rad-Hard Sizing Mechanism . . . 54
3.4.2 Setup for VT Variation Experiments . . . 55
3.4.3 SET Experiments with VT variations . . . 57
3.4.3.1 Transistor Sizing Mechanism . . . 57
3.4.3.2 Stack-Separation Mechanism . . . 60
3.4.4 Summary . . . 67
3.5 Sequential Circuits . . . 69
3.5.1 Background . . . 70
3.5.1.1 Linear Feedback Shift Register . . . 70
3.5.1.2 Parallel-In Serial-Out . . . 71
3.5.2 Proposed Rad-hard Mechanisms . . . 72
3.5.2.1 Radiation Hardening by Sizing for the LFSR . . . 73
3.5.2.2 Hardware Redundancy for the LFSR . . . 73
3.5.2.3 Time Redundancy for the LFSR . . . 75
3.5.2.4 Radiation Tolerance by Separation for the LFSR . 75
3.5.2.5 Radiation Tolerance using DICE for the LFSR . . 76
3.5.2.6 Hardening by Sizing for the PISO . . . 77
3.5.2.7 Radiation Tolerance by Separation for the PISO . 77
3.5.2.8 Radiation Tolerance using DICE for the PISO . . . 77
3.5.2.9 Time Redundancy for the PISO . . . 77
3.5.3 Summary . . . 77

4 Sensitivity and Spatial Distribution of SETs **81**
4.1 Target Architecture . . . 83
4.1.1 Inverter . . . 83
4.1.1.1 Inverter Chain . . . 83
4.1.2 NAND-NOR Logic . . . 84
4.1.2.1 NAND gate . . . 84
4.1.2.2 NOR gate . . . 85
4.1.2.3 NAND NOR Tree . . . 86
4.1.3 Sequential Circuits . . . 87
4.1.3.1 Flip-Flop . . . 87
4.1.3.2 Flip-Flop Chain . . . 88
4.1.4 Asynchronous Circuits . . . 89
4.1.4.1 Muller C-element . . . 89
4.1.4.2 Muller Pipeline . . . 90
4.1.5 XOR gate . . . 91
4.1.5.1 XNOR Tree . . . 92
4.1.6 Summary . . . 93
4.2 Measurement Architecture – Semi-Static Mode . . . 94
4.2.1 Architecture A . . . 95
4.2.2 Architecture B . . . 96
4.2.3 Architecture C . . . 96
4.2.3.1 Up/Down Counter . . . 96
4.2.4 Architecture D . . . 98
4.2.5 Architecture E . . . 98
4.2.6 Architecture F . . . 100
4.2.7 Architecture G . . . 101
4.3 Evaluation and Analysis - Semi-Static Mode . . . 101
4.3.1 Overhead Analysis . . . 102
4.3.2 Analysis Setup . . . 103
4.3.3 LFSR Counter Evaluation . . . 103
4.3.4 Up/Down Counter Evaluation . . . 105
4.3.5 Fault Dictionary . . . 106
4.3.6 SET Simulations . . . 109
4.4 Probabilistic Analysis . . . 110
4.5 High Speed Measurement Architecture . . . 115
4.5.1 SET Analysis . . . 117
4.5.2 Hardware-Overhead Analysis . . . 118
4.6 Summary . . . 120

5 Propagation of SETs **121**
5.1 Sklansky Adder . . . 121
5.1.1 Background . . . 121
5.1.2 Architecture Description . . . 122
5.1.3 Measurement Architecture . . . 124

5.1.3.1 Data Collection in the Carry Propagation Path . . 125
5.1.3.2 Overall Measurement Infrastructure 125
5.2 Inverter Tree 127
5.2.1 Measurement Architecture 127
5.2.1.1 Static Mode 127
5.2.1.2 Dynamic Mode 129
5.3 SET Analysis – Sklansky Adder 131
5.3.1 Identification of the most sensitive adder state 132
5.3.2 SET Injection Experiments in the 16-bit Adder 132
5.3.3 Fault Dictionary 135
5.3.4 SETs in the Counters 139
5.4 SET Analysis – Inverter Tree 140
5.4.1 Static Mode 140
5.4.2 Dynamic Mode 144
5.5 Summary 146

6 Pulsewidth Measurement of SETs 151
6.1 Background 152
6.2 Measurement Infrastructure Requirements 153
6.3 Baseline SET Pulse-width Measurement Architecture 154
6.3.1 Principle 154
6.3.2 Design space 154
6.3.3 Switch placement 155
6.3.4 Radiation tolerance 157
6.3.5 SET Analysis 158
6.3.5.1 Verification for other target circuits 161
6.4 Measurement Infrastructure for Multiple SETs 163
6.5 Multiple SET Architecture – Improvement of Counter Array 166
6.5.1 Counter array implementation 166
6.5.2 Attaining Fault Tolerance 166
6.5.2.1 Guiding principles 166
6.5.2.2 Protecting the address counter 167
6.5.2.3 Protecting the counter array 168
6.5.2.4 Initialization and read-out 170
6.5.3 Resulting architecture 171
6.5.4 Multiple Event Transients Analysis 172
6.6 Algorithm for pulse width extraction from the read-outs 174
6.7 Fault Dictionary 176
6.8 Probabilistic Analysis 180
6.8.1 Computing P_{fail} for at most 3 target SETs 183
6.8.2 Computing P_{fail} for more than 3 target SETs 185
6.9 Discussion of our Analysis Results 187
6.10 Summary 189

7 Target FRad ASIC 191

7.1 On-Chip Data Transmission Architecture . . . 192
7.1.1 Application Requirements . . . 192
7.1.2 Operation of PISO . . . 193
7.1.3 Architecture Options . . . 194
7.1.3.1 Single PISO – Measurement Infrastructure . . . 195
7.1.3.2 Single PISO – Multiple Measurement Infrastructure 196
7.1.4 Summary . . . 197
7.2 ASIC Architecture . . . 199
7.2.1 FRad Overview . . . 199
7.2.2 Requirements . . . 199
7.2.3 Specifications . . . 200
7.2.3.1 SET Sensitivity . . . 201
7.2.3.2 SET Propagation . . . 201
7.2.3.3 PISO . . . 202
7.3 ASIC Layout and Implementation details . . . 203
7.3.1 ASIC Floorplan . . . 203
7.3.2 Layout and Placement . . . 205
7.4 ASIC Functional Behavior . . . 213
7.4.1 Reset . . . 213
7.4.1.1 Verification of Reset . . . 213
7.4.2 Programming . . . 215
7.4.2.1 Verification . . . 215
7.5 ASIC – SET Experiments . . . 217
7.5.1 30-bit PISO . . . 220
7.5.2 84-bit PISO . . . 220
7.5.3 110-bit PISO . . . 221
7.5.4 75-bit PISO . . . 221
7.6 Data Transmission from ASIC to PC . . . 222
7.6.1 Gateway . . . 222
7.6.2 Operation of Gateway . . . 223
7.6.3 Requirements . . . 223
7.6.4 Concept . . . 224

8 Conclusions and Future Work 227
8.1 Summary of Key Contributions . . . 227
8.1.1 SET Modeling . . . 227
8.1.2 Design of Novel Radiation Hardening Mechanisms . . . 228
8.1.3 Innovative Measurement Infrastructure SET Sensitivity . . . 229
8.1.4 Novel Measurement Infrastructure for SET Propagation . . . 230
8.1.5 Novel Measurement Infrastructure for SET Pulsewidths . . . 231
8.1.6 Design of FRad Chip . . . 231
8.2 Outlook . . . 232
8.2.1 Fabrication of the ASIC . . . 233
8.2.2 Gateway FPGA Setup . . . 233

8.2.3 Radiation Experiments on Microbeam and Reactor 234
8.2.4 Technology Variations 234
8.2.5 Other Single Event Effects 234
8.2.6 Spice Modeling 235

Bibliography **237**

A Appendix A **253**
A.1 FRad Chip Pin Description 253
A.2 ASIC Signal Description 257
A.2.1 Clock 257
A.2.2 Reset 258
A.2.3 Input Data Signals 259
A.2.4 Input Control Signals 260
A.2.5 Data Output Signals 260

List of Figures

2.1 Inverter with Double Exponential Current Source 21
2.2 Simulation of an Inverter with Double Exponential Current Model . . . 21
2.3 Improved Current Model 22
2.4 Simulation of an Inverter with Improved Current Model 23
2.5 TCAD 3D Structure of an Inverter (Cutting Plane through NMOS) . . . 24
2.6 Test Chip Schematics for Calibration and Validation of the 3D Model and the Spice Model 25
2.7 Measured SET Voltage Pulses (Inverter) under Heavy-Ion (^{197}Au, 946MeV) Irradiation [129]: SETs for a) Low (0), b) High (1) Inputs 26
2.8 Length of SET vs. Exponential Peak Current I_0 28
2.9 Muller C-element (a) Symbol, (b) Logical equivalent 29
2.10 Conventional Pull-up Pull-down Muller C-element 30
2.11 Van Berkel Muller C-element 30
2.12 Weak Feedback Muller C-element 31
2.13 Inverter based Muller C-element 31
2.14 Simulation results 32

3.1 DICE Cell Based Muller C-element 40
3.2 Radiation Hardened Muller C-element using Separation Mechanism . . 41
3.3 Transistor level Schematic of Cross Coupled XOR gate 43
3.4 Gate Level Schematic of IAO XOR gate 43
3.5 Simulation of SET hits in CC XOR gate 44
3.6 Simulation of SET hits in IAO XOR gate 45
3.7 SET Simulations of Rad-Hard CC XOR Gate 45
3.8 Defect-Tolerant Inverter 46
3.9 Simulation of SETs in Defect-tolerant Inverter 47
3.10 Analog Voter with Comparator 47
3.11 SET Simulation of XOR gate with Analog Voter1 48
3.12 Radiation Hardening by Separation Mechanism 49
3.13 Simulation of SETs for Radiation Tolerant XOR gate 51
3.14 CWSP CC XOR gate 51
3.16 Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA 58
3.17 Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=450fC, Tr=10ps, Tf=160ps, I=3mA 59

3.18 Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=300fC, Tr=10ps, Tf=110ps, I=3mA 61
3.19 Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA 62
3.20 Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA 63
3.21 Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=160ps, I=3mA 64
3.22 Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=160ps, I=3mA 65
3.23 Results of voltage and temperature variation experiments for Stack Separation with Q=300fC, Tr=10ps, Tf=110ps, I=3mA 66
3.24 Results of voltage and temperature variation experiments for Stack Separation with Q=300fC, Tr=10ps, Tf=110ps, I=3mA 67
3.25 32-bit LFSR 70
3.26 4-bit Parallel-in, Serial-out Shift Register 71
3.27 Schematics of TMR LFSR Counter 73
3.28 Schematics of the Digital Voter 74
3.29 Schematics of TMR Flip-Flops 74
3.30 Schematics of TMR XNOR Gate 75
3.31 Transistor level Schematics of DICE Latch 76
3.32 Control Logic of the PISO 77

4.1 (a) Transistor Level Schematic of Inverter, (b) Symbol of Inverter 83
4.2 Logic Diagram of Inverter Chain 84
4.3 (a) Transistor Level Schematic of NAND, (b) Symbol of NAND gate . . 85
4.4 (a) Transistor Level Schematic of NOR, (b) Symbol of NOR gate 85
4.5 Logic Diagram of NAND/NOR Tree 87
4.6 (a)Transistor Level Schematic of D-Flip-Flop, (b) Symbol of D-Flip-Flop 88
4.7 Logic Diagram of Flip-Flop Chain 89
4.8 Logic Diagram of Muller Pipeline 90
4.9 (a) Transmission gate based XOR, (b) Symbol of XOR gate 91
4.10 Logic Diagram of XNOR Tree 92
4.11 Measurement Architecture A 96
4.12 Measurement Architecture B 96
4.13 Measurement Architecture C 97
4.14 Schematic of (a) Muller C-element with Reset (rst), (b) Muller C-element with Set (set) and (c) Up/Down Counter 97
4.15 Measurement Architecture D 98
4.16 Measurement Architecture E 99
4.17 Measurement Architecture F 100
4.18 Measurement Architecture G 101
4.19 Simulation of the DUTs under exposure 110
4.20 Simulation of the Up/Down Counters under exposure 111
4.21 Simulation of the LFSR Counter 1 112

4.22 Simulation of the LFSR Counter 2 . . . 113
4.23 Measurement Setup for Dynamic Mode . . . 116
4.24 Schematic of Weak-Feedback (a) Muller C-element with Reset (rst), (b) Muller C-element with Set (set) and (c) Up/Down Counter . . . 116
4.25 Simulation of the pipeline with target circuit under exposure . . . 118
4.26 Simulation of the pipeline with reference circuit under exposure . . . 118
4.27 Simulation of the pipeline with target and reference circuit under exposure 119

5.1 Gate Level Schematic of Sklansky Adder Cells . . . 123
5.2 Architecture of 16-bit Sklansky Adder . . . 123
5.3 Measurement Architecture for SET Propagation in the 16-bit Sklansky Tree Adder . . . 126
5.4 Measurement Architecture for the Static Inverter Tree . . . 128
5.5 Measurement Architecture for the Inverter Tree – Dynamic Mode . . . 130
5.6 SET Analysis of Sklansky Adder . . . 133
5.7 SET Analysis of Sklansky Adder . . . 133
5.8 Counter L_8 - SET Analysis of Sklansky Adder . . . 134
5.9 Counter L_{14} - SET Analysis of Sklansky Adder . . . 134
5.10 Counter L_6 - SET Analysis of Sklansky Adder . . . 134

6.1 Baseline Architecture to Measure SET Lengths . . . 156
6.2 Length of SETs in a D Flip-Flop . . . 163
6.3 Architecture to Measure Multiple SET Lengths . . . 165
6.4 Pulse width Measurement Architecture for Multiple SETs . . . 171
6.5 Simulation results for the SETs injected in the target circuit . . . 173
6.6 Simulation Results: Detail view of a SET in the target and a single SET in the grounded counter A_1 . . . 175

7.1 Simulation of 4-bit PISO . . . 194
7.2 4-bit PISO Timing diagram . . . 195
7.3 Block diagram of 4:1 MUX . . . 196
7.4 ASIC Floorplan . . . 204
7.5 Muller C-element Layout . . . 206
7.6 Muller C-element with “set” Layout . . . 206
7.7 Muller C-element with “reset” Layout . . . 207
7.8 Inverter Chain Layout . . . 207
7.9 Nand Nor Tree Layout . . . 207
7.10 Inverter Tree Layout . . . 208
7.11 Black Cell Layout . . . 208
7.12 Gray Cell Layout . . . 209
7.13 Half Adder Layout . . . 209
7.14 Sklansky Adder Layout . . . 210
7.15 Up/Down Counter Layout . . . 210
7.16 32-bit LFSR Layout . . . 211
7.17 30-bit PISO Layout . . . 211

7.18 84-bit PISO Layout 211
7.19 ASIC layout with Targets, Measurements and PISO circuits 212
7.20 Behavior of the Counters (read out from 84-bit PISO) after Reset 214
7.21 Behavior of the Counters (read out from 30-bit PISO) after Reset 214
7.22 Behavior of the Counters (read out from 84-bit PISO) after Programming 10 Transitions 216
7.23 Behavior of the Counters (read out from 30-bit PISO) after Programming 10 Transitions 216
7.24 SETs in the Target Circuit read out by the 30-bit PISO 218
7.25 SETs in the Target Circuit read out by the 84-bit PISO 218
7.26 SETs in the Sklansky Adder read out by the 110-bit PISO 219
7.27 SET in the Inverter Tree read out by the 75-bit PISO 219
7.28 Interface Architecture 222
7.29 Timeline of our Architecture Setup 224

List of Tables

2.1 Truth Table of Muller C-Element 30

3.1 Comparison of Radiation Hardening Mechanisms for Muller C-element 42
3.2 Comparison of Different Fault-Tolerant Mechanisms 52
3.3 Required sizing for different choices of current pulse parameters, all with a charge of 450fC 54
3.4 Required sizing for different choices of current pulse parameters, all with a charge of 300fC 55
3.5 Comparison of Different Radiation-Tolerance Mechanisms 78
3.6 Comparison of Different Fault-Tolerant Mechanisms 79

4.1 Truth Table of Inverter 84
4.2 Truth Table of NAND gate 84
4.3 Truth Table of NOR gate 86
4.4 Truth Table of D-Flip-Flop 88
4.5 Truth Table of XOR gate 91
4.6 Number of Transistors for Different Architectures 102
4.7 Hardware Overhead Analysis for Measurement Setup 103
4.8 Operation of the LFSR Counter in No-Fault Scenario 104
4.9 LFSR Counter – SETs in XNOR Gates & Flip-Flops 105
4.10 Fault Analysis of the Up/Down Counter 107
4.11 Fault Dictionary 108
4.12 Hardware Overhead Analysis 119

5.1 Fault Coverage of the Static Inverter Tree Architecture 128
5.2 Fault coverage of the proposed architecture (symmetric cases for which identical arguments apply are shown in parentheses) 131
5.3 Fault Dictionary for Sklansky Adder 136
5.4 Fault Dictionary for Sklansky Adder 137
5.5 Fault Dictionary for Sklansky Adder 138
5.6 Fault Dictionary 142
5.7 Fault Dictionary 143
5.8 Fault Dictionary for Inverter Tree 147
5.9 Fault Dictionary for Inverter Tree 148
5.10 Fault Dictionary for Inverter Tree 149

6.1 Recording capabilities (vs. reference count) of Architectures I–IV for different charges injected in an inverter 159
6.2 Architecture (II) & (IV) – Measurement Statistics – Q_{SET}=1.06pC . . . 161
6.3 Sequence of addressing in the counter array 169
6.4 Fault Dictionary for SETs in the Target Circuit 178
6.5 Fault Dictionary (excerpt): SEUs in the Up/Down Counters 179
6.6 Values for $P_{fail}(k)$ for $N = 14$ and different values of C, k. 185

7.1 SET Sensitivity Architectures 201
7.2 SET Propagation Architecture 202
7.3 Leaf Cells with die area 205

A.1 FRad Pin List 254
A.2 FRad Pin List 255
A.3 FRad Pin List 256
A.4 MUX and CUT combination 260

CHAPTER 1

Introduction

Economic progress and technical advancement of the commercial semiconductor industry in the 1960s completely changed the way electronic components were purviewed [127]. This technology advent created a resilient components market for design against radiation. Since then, radiation tolerant components are widely used only in areas such as satellites, spacecrafts (abundance of radiation particles in space), nuclear power stations (sensors), military aircraft's (against atmospheric particles) and nuclear weapons. Typically to harden the circuits against radiation insulating substrates, redundancy, hardened latches, etc. are employed. The aggressive expansion of the consumer and business markets in the 90s has dramatically affected the development of radiation resilient hardware, which was only a tiny fraction of the commercial market [127].

Currently in the nano age shrinking feature sizes are the key to the progress in VLSI technology with respect to clock speed, dynamic power, integration density etc. However, this increases the susceptibility to faults (due to their smaller geometries and critical charge [133, 63, 75]), ultimately making radiation effects very relevant for commercial circuits. It is also argued in the literature [16, 133, 50, 34, 15] that, while with older technologies (130nm and above) radiation-induced transient errors used to be relevant for aerospace applications only, now with recent technologies, they are becoming an issue even for earth-bound applications, making the need for efficient radiation hardening mechanisms a pertinent problem that is not only restricted to specific safety-relevant functions but may also apply to future commodity circuits. Previously, the type of faults being dealt with in commercial semiconductor components were aging [30, 88, 91], electric wear-out [79, 31], stuck-at faults [116, 22, 115], stuck-open faults [96, 67, 99, 121] and manufacturing defects [118, 139, 83]. There is a huge body of work to rely upon when it comes to these "classic" sources of errors, but, for radiation-induced errors, which are increasingly dominating the failure rate of deep sub-micron VLSI circuits [75, 16], there is comparatively very little available.

Our main concern in the thesis are radiation-induced errors, collectively termed *single-event effects* (SEEs) in literature. Technology scaling has increased the im-

portance of these errors in digital circuits, furthermore, it has increased the requirement for SEE studies. SEEs occur when the active area of a VLSI circuit is hit by ionizing particles (or even by neutrons, which typically result from heavy ion interactions with nitrogen or oxygen atoms in the atmosphere). There are two types of SEEs namely destructive and non-destructive ones. As opposed to permanent (destructive) SEEs such as latch-up, threshold voltage shifts and burn-outs in power semiconductors [113, 40, 128], the primary concern in modern VLSI circuits are non-destructive SEEs. The errors resulting from non-destructive SEEs are not permanent but rather transient (i.e., can be corrected).

Consequently a systematic study of radiation effects on a given VLSI circuit is no more an exotic task of some space engineer, but a necessity even for everyday products, and novel, cost-effective radiation tolerance methods need to be developed. In order to be able to build efficient radiation tolerant hardware, one must have a good understanding of SEEs. The hardware that needs to be hardened should be exposed to radiation and the effects must be observed. This would provide us an insight on the vulnerabilities of the hardware. Performing the same process for standard logic gates would help us build any hardware that can be protected against radiation. Our thesis aids in building a solid knowledge on SEEs in digital circuits, that would enable anyone with basic knowledge of semiconductor physics to build efficient radiation hardened circuits.

1.1 Motivation

There are three types of non-destructive SEEs in digital circuits:

- ⋆ Single Event Transients (SETs)
- ⋆ Single Event Upsets (SEUs)
- ⋆ Single Event Functional Interrupts (SEFIs)

When an energized particle strikes the silicon, it transfers its energy by creating free electron-hole pairs, resulting in a dense ionized layer in the region of impact. This ionization in turn generates a transient current pulse that can cause an upset when interpreted as a signal in the circuit [156]. If the current induced by the particle strike is high enough the ON-transistor cannot balance it and a voltage change at the node will occur causing a SET. If the SET manifested in the combinational circuit propagates to a sequential circuit or a storage cell then it could lead to an SEU (also called “soft error”). Unfortunately, SEUs may also occur if a transistor within the storage element is affected by a particle strike. A soft error which would cause a temporary loss of device functionality in a detectable way, but would not require power cycling of the device to restore operability is called as SEFI. If the voltage on the struck node is recovered by the current feed through the ON-transistor no SET will be observed. In this thesis we focus only on SETs and SEUs in digital circuits.

1.1.1 SET Model

In order to trigger these effects in a digital circuit we need to either build an elaborate device level model, or a simple model that only considers the circuit architecture (transistor placement). Previously SET models were built only for space applications, mainly to construct radiation mitigating components. Recent trends in electronics such as technology scaling require us to build SET models not only to construct rad-hard components but to understand charge distribution, SET generation, SET propagation, etc, in digital circuits. A device level model typically consumes a lot of time in executing a simple simulation on a larger circuit to describe the SEEs (as it takes into account technology parameters, parasitic load, etc.,), hence is impractical to use. In contrast, the simple model (that does not take into consideration the technology parameters or parasitic load) completes a simulation of million gates in hours, but does not model the SEEs accurately. This raises the need for a model that accurately describes the SEEs in digital circuits.

Robust circuit design – in particular, for critical applications in space and aerospace, needs models that accurately describe SET/SEU generation and propagation in modern VLSI technology, yet are easy and efficient to use at early design stages: Such models both allow to assess the radiation tolerance of different architectural designs and hardening techniques and to estimate the final soft-error rate of a circuit. Moreover, to elaborate more efficient, cheaper solutions for radiation mitigation, the propagation and masking of SETs must be precisely understood.

Modeling radiation effects both on the analog and on the digital level have their own challenges, like:

- How does a circuit's susceptibility to radiation depend on its own activity (rate of ongoing transitions during exposure)?
- How to precisely represent the charge deposition caused by the particle impact in an analog simulation?

1.1.2 Soft Error Rate

Soft error rate (SER) is the rate at which SEUs occur in a digital circuit. The three primary reasons for the increase in SERs in digital circuits over the years are:

- increased circuit complexity results in more hit targets
- decreasing feature sizes and supply voltages decrease the electrical charge used for representing information, which makes it more likely for a particle hit to create an SEE
- increasing clock frequencies increase the probability that an SET generated in combinational logic gates gets latched and hence causes an SEU.

To compute the SER of a given chip, simulation [50, 90, 136, 16], probabilistic analysis [32, 90, 110, 119, 133, 130] as well as validating measurements[142, 61,

74, 65, 32, 63, 75, 17, 50, 54] have been used. Obviously, such SER results allow the assessment of technology scaling [50, 75, 43, 63, 133]. The total SER per chip has increased dramatically [50, 16] due to increasing chip complexity. Although technology improvements (*silicon on insulator* (SOI), *metal-insulator-metal* (MIM) caps etc.) [123, 93] are very effective for mitigating SEEs, they are not sufficient to maintain acceptable SERs. Moreover, they are considered too expensive [16] for replacing bulk technology in general, and there are also reports of unexpected effects like SET pulse broadening during propagation [44].

Most of the studies so far have focused on a single inverter cell or a memory/array of flip-flops to calculate SERs, while the effect of radiation on and its propagation in more complex circuit structures have hardly ever been investigated. Particles with higher energy can cause errors in digital circuits that are quite visible, whilst particles with lower energy that are substantially more frequent – can cause errors in VLSI circuits that may either get masked or propagate. Obviously this competition between propagation and masking is crucial for whether an SET finally becomes activated as an SEU. In order to assess the SER of a circuit, one must address the following effects:

1.1.2.1 SET Generation

It is important to understand the SEU generation process. There exists an ample amount of literature on the topic (see e.g. [64, 20, 17, 93, 101, 95]) that deals with experimental SET measurements. Suitably designed radiation targets (usually long inverter chains) are exposed to accelerated radiation tests (using neutron [111] or heavy-ion[18, 41, 20, 45, 160, 44, 105, 106, 14, 12, 3, 51] beams) and/or laser-based failure injection [18, 102, 107, 45, 43, 44]. The resulting SETs are measured using several different approaches: Besides indirect approaches based on SER measurements [18, 25, 61, 65, 64], which use the correlation between SET pulse-width and the *linear energy transfer* (LET) of specific heavy-ions, there are several different approaches for digital on-line measurement of SET pulse-widths using variable delay latches [20, 41] or self-triggered inverter + latch chains [160, 107, 105, 111, 17]. A few papers also report on analog measurements of SET pulse-widths by directly connecting a real-time oscilloscope [44, 43, 45, 33].

Based on the above reported results, we can conclude that one can estimate the SER in an experimental ASIC, which is exposed to radiation, over time. However, the SET generation process used in the literature in general raises a few questions such as:

- Is the SER data provided by the target circuits valid for the fabricated ASIC with rad-hard components? (even if the whole ASIC is exposed to radiation, any SETs within the rad-hard components are mitigated)
  - In order to accurately compute SER data of an ASIC we must use only non rad-hard components in the ASIC.

- Is there SER data for complex structures such as adders or parity logic available?
  - There exists SER data only for simple structures such as inverter chains or memory cells in the literature. Therefore, we must create a framework to provide this data.
- Is there enough SER data on complex structures calibrated from ambient radiation?
  - Most of the SER data is calibrated from prolonged experiments on focused radiation and not from ambient radiation. Hence, monitoring architectures that can withstand ambient radiation and provide reliable SER data must be constructed.

1.1.2.2 SET Propagation

The *propagation* of an SET is not simply linear; forks will multiply SETs, so a single transient may end up in numerous upsets. The problematic issue with SET propagation is that a single SET may cause multiple upsets in general, a phenomenon called as “charge sharing”, which can lead to effects like SET pulse quenching [4] and double-pulse generation [3]. First its impact may be so large (as compared with the transistor features) that it affects more than one transistor in the first place. Even if it should initially hit only one transistor, the deposited charge can spread to other junctions, again affecting multiple locations. And finally even a single SET may multiply itself by the fan-out of the affected output. All those cases have the potential of defeating error detection/correction provisions and other fault tolerance strategies that are usually dimensioned for single faults only. Therefore it is vital to study these effects.

For deep sub-micron technologies, the actual spreading of the charge, its conversion into an SET, as well as the propagation of the latter in the circuit (including parasitic channels) is not fully understood. Therefore an understanding of how SETs propagate in combinational logic is vital. However, there are a set of questions posed by SET propagation such as:

(i) Which SETs successfully propagate to the output in a circuit? What are the other factors that influence this other than the strength of the charge induced in the circuit by radiation particles?

(ii) Does an SET successfully propagate in a fork in all the paths or only in few paths (and decays in the rest)?

(iii) While analysing SET propagation to obsere a "worst case", are there any steps taken to avoid SET masking?

Accordingly, not all SETs actually cause a functional fault of the affected circuit; a significant share will be masked [32, 119] before causing an SEU. In this context,

the SET length (i.e. the width of the voltage pulse originating from the injected charge) plays a crucial role: Obviously a short pulse has a higher potential of being masked than a long one. This is why an assessment of SET lengths is instrumental for:

(i) Devising accurate models that relate particle characteristics (energy, angle, location of hit, etc.) and SET pulsewidths, and

(ii) Studying SET propagation throughout a digital circuit (how does SET length increase/decrease?).

1.1.2.3 SET Masking

With respect to *masking* usually 3 mechanisms are distinguished [84, 133]:

(a) *Electrical masking* is concerned with analog effects that weaken the SET amplitude or width to the point where it is no more recognized at a subsequent input;

(b) *Logical masking* considers whether the SET occurred in a logically sensitized path (an AND gate with one input at LOW will mask an SET on the other input); and

(c) *Temporal masking* expresses the property of a storage element to ignore the state of its input during certain phases (consider a latch in hold state, e.g.).

An accurate analysis of logical masking requires an exhaustive classification of all sensitive paths in a given combinational logic [119]. Such an explicit modeling is of course expensive (in [39], it is shown that computing the most reliability-critical path is NP-hard); alternative approaches rely on fault injection [7, 74] and probabilistic modeling [32, 110].

In synchronous circuits, SETs originating from combinational logic can only lead to SEUs if they propagate to the flip-flops and arrive there within their setup and hold time. Temporal masking is very effective if the latter are small relative to the clock cycle [75, 133, 32, 110, 119, 34]. However, due to ever decreasing time margins , this assumption does no longer hold true, and the problem is further exacerbated by SETs hitting the clock drivers [130].

In asynchronous circuits temporal masking effects are very different. To be precise, temporal masking is tightly intertwined with logical masking here: The ability of an asynchronous circuit like a Muller C-element to memorize a SET-transition on some input depends on its other input(s). In reasonably regular structures, like bundled data or delay insensitive asynchronous pipelined architectures, there are ways to analyze temporal masking similar to synchronous circuits [102, 80]. In general, however, an accurate analysis of temporal masking in asynchronous systems requires an exhaustive classification of all paths involved in the completion detection process and hence explicit modeling.

Logical masking and temporal masking can be explored in a relatively systematic way, and on a high level of abstraction, for a given circuit. Electrical masking, in contrast, depends on many details, such as output loads, routing, or parasitics. Therefore an experiment is the appropriate choice to study it.

Ultimately, physical experiments in which the circuit is exposed to actual radiation clearly provide the most accurate and realistic study on generation and propagation of SETs, but these are expensive in terms of provision of a suitable target chip, and in terms of having a suitable radiation facility available. This is a non-trivial task, since tracing the short SET pulses cannot simply be performed at pins via external equipment alone, but requires sophisticated on-chip infrastructure.

1.1.3 Radiation Hardening Mechanisms

The study of radiation effects as well as the assessment of the hardening methods within the device under test, in principle, can be done in physical experiments. These, however, require access to expensive radiation sources and the experimental conditions that are often hard to precisely control. Radiation hardening mechanisms in general are designed for applications that do not concur with typical voltage and room temperature and has to be tested for varying voltages and temperatures.

For the current technologies (90nm and lower) voltage and temperature variations have also become a major concern in ground based applications. Even when provided with a perfectly stable voltage at the supply pins, a chip's internal logic will finally experience variations in the supply voltage due to the voltage drops that changing currents cause on parasitic resistances and inductances in the supply rails [120]. In the same way temperature will vary all over the chip and over time due to varying heat dissipation at the chip's different function units [94]. It is well understood that voltage and temperature have a significant impact on propagation delays, so normally the concern is the impact of those variations on the attainable computing performance [23, 71, 58]. Therefore, any radiation hardened circuit built in the current technologies has to undergo tests for these variations.

As a consequence, efficient techniques for attaining radiation hardness assurance are receiving increasing interest for both,

- Ground bound applications to prevent new technology nodes from exhibiting perceivable transient failure rates
- Space applications to allow leveraging the performance gain offered by those new technologies while still keeping SEU rates within acceptable limits.

As a matter of fact, radiation hardening mechanisms incur area and performance penalties, and without strict optimization they can easily spoil the benefits of using smaller feature sizes. It is therefore crucial to carefully tailor them to the specific needs, rather than just "over-designing" them. Some of the open questions in this aspect are:

1. How does the SET sensitivity of a circuit (quantitatively) vary with supply voltage and temperature?

2. How do the radiation hardening mechanisms presented in the literature perform under those variations?

3. How much do they need to be enhanced to attain the desired level of radiation hardening under worst conditions, as compared with the best case?

This insight will not only globally provide us a feeling for how sensitive radiation hardening mechanisms are to those variations, it will also, more specifically, allow us to judge the additional cost of allowing a wider range of operating temperature or supply voltage variations for a given circuit.

1.2 Scope

The ultimate vision of our work (i.e., TU Vienna's FATAL project (Fault-tolerant Asynchronous Logic) supported by the Austrian Science Fund (FWF) under project number P21694) is to come up with a reasonably accurate high-level model for SETs/SEUs, allowing us to faithfully predict upset rates and vulnerabilities in a design and thus incorporate the appropriate degree of protection. In this context our aim is to design an ASIC and expose it to radiation. We plan to use two types of radiation sources:

- ⋆ A micro-beam that allows a precise control of time and location of particle impact (typically for one specific particle type per experiment campaign), and

- ⋆ An atomic reactor that provides a more realistic mix of particle types, however, without precise control of timing and location; here the whole chip is exposed to radiation without interruption throughout the whole measurement campaign.

The target ASIC will be equipped with a number of target circuits; simple ones like inverters and flip-flops for comparison with existing work, but also more complex ones like incrementer and basic asynchronous circuits like a Muller C-element. As a part of the analysis we will measure the length of SETs, SET sensitivity of different target circuits, SET propagation, spatial distribution, etc., in order to have a reference for validating our models. To obtain the desired information (detailed tracing of SET generation and propagation) we need to augment the target circuits with on-chip infrastructure that comprises circuits for capturing and pre-processing radiation effects [149]. For various reasons this measurement infrastructure must be on-chip, but as it is therefore exposed to radiation as well (in the reactor experiments), it must be radiation hardened, and its area be confined to the bare minimum. The infrastructure should be able to reasonably infer the location of the SET and thereby provide the SET sensitivity of each target circuit for a particular LET and

also help us estimate the soft error rate in the ASIC. After all, our results are only meaningful, if we can rely on the read-outs.

Furthermore to measure the pulse-width of the SETs we need a fully digital measurement infrastructure, since the analog amplifiers used in [68] are too large to be employed in more complex architectures. In addition, although analog measurements provide detailed pulse shapes, measuring digital SET pulsewidths still requires the choice of appropriate voltage thresholds. By contrast, this happens naturally and automatically in an all-digital setting. It is important that the measurement infrastructure thus built be able to reliably record pulse-widths of multiple consecutive SETs.

In order to transmit the SET data from the measurement circuits we employ a transmission architecture. This transmission architecture must be hardened in order to avoid loss of data during transmission. The target ASIC that hosts the target, the measurement and the transmission circuits needs to be validated before fabrication to make sure that the infrastructure is capable of recording and transmitting the SET data while being exposed to radiation. In order to perform the validation we need to mimic the radiation particle strike in a simulation using the SET models available in the literature.

Finally we need to implement a standard interface for transfer of the measurement data on this ASIC to a host PC. The reason behind this interface is that we will not be able to move a PC sufficiently close to the radiation environment where the target ASIC will be located. Therefore, we have to insert an intermediate dedicated interface that would form a gateway between target ASIC and host PC. Its task will be to collect the data from the target ASIC via a very lean custom interface and upload them to the host PC via a standard interface.

Ultimately this thesis aims to provide a platform for analyzing the SET generation, SET sensitivity, SET propagation, SET distribution and SET pulse-widths in digital circuits. So far in the literature all these effects were analyzed individually, no researcher has built an infrastructure that combinedly analyzes these SEEs in digital circuits.

1.3 List of Key Contributions

The global aim of this thesis is the design of a radiation target ASIC to perform a comprehensive investigation of SETs in digital circuits. The challenges we face to thoroughly study SETs and their effects in the current technologies are:

(i) Selection of target circuits to efficiently analyze SETs

(ii) Radiation protection of the measurement infrastructure against SETs

Therefore to collect useful SET data from the targets the ASIC must fulfill certain basic requirements:

a Restrict to a strict digital implementation to avoid complex analog structures in the ASIC.

b Provide appropriate radiation protection to the infrastructure to be able to record correct SET measurement data.

c The infrastructure should be able to record SETs precisely.

d Continuously capture SETs in the targets and store an array of measurement values in the measurement infrastructure. The stored data must be transmitted without any error to the PC

e Place as many target and measurement infrastructure blocks as possible in the die area of the ASIC to analyze diverse SET effects. The measurement infrastructure competes with the target circuits for die area, and hence, it must be kept as lean as possible, in spite of the need of being tolerant to particle hits in itself that cannot be avoided in ambient radiation experiments. If they occupy too much die area then the probability of a SET in the target circuit becomes low.

To analyse particle strikes in digital circuits we used a SET model following a combined approach:

Step 1: Expose a sample circuit to physical radiation to understand SET pulsewidth and shape [68]

Step 2: Calibrate TCAD models to accurately compute the SET shape and length [69]

Step 3: We tweaked the parameters of the Spice model (double exponential current model [93, 119]) to make sure that the results are aligned with results from TCAD model

1.3.1 Design of Novel Radiation Hardening Mechanisms

We radiation hardened some of the circuits of interest (Muller C-element, flip-flops, combinational gates) against particle strikes using the mitigation techniques presented in the literature under a given set of environmental conditions. We also improved the radiaiton hardening mechanism for the given circuits such that they perform correctly under voltage and temperature variations.

1.3.2 Innovative Measurement Infrastructure SET Sensitivity

To support experiments in uncontrollable standard radiation environments, we developed a purely digital measurement infrastructure [149, 148] that allows the long-term monitoring of statistical SET generation properties. We proposed radiation targets like Muller C-elements and elastic pipelines as well as standard combinational gates and flip-flops with an elaborate on-chip measurement infrastructure to understand sensitivity and spatial distribution of SETs. Major architectural challenges result from the fact that the latter must operate reliably under the same radiation conditions the target circuits are exposed to, without wasting precious die area

for a rad-hard design. A measurement architecture based on multiple non-rad-hard counters is used, which we show to be resilient against double faults, as well as many triple and even higher-multiplicity faults. The design evaluation is done by means of comprehensive fault injection experiments, and probabilistic analysis of the sustainable particle flow rates, based on a detailed area analysis and experimental cross-section data.

1.3.3 Novel Measurement Infrastructure for SET Propagation

A measurement architecture that allows us to trace generation and propagation of SETs in combinational target circuit is proposed. The problem of devising a suitable on-chip measurement infrastructure lies in the partly contradictory requirements, like constrained area, radiation tolerance and good resolution of the location and propagation path of particle hits. Our proposed architectures are based on linear feedback shift registers and asynchronous up/down counters that can be used as lean and robust counter implementations. The former provide a very robust means for obtaining an absolute count of SETs, the latter can (as they provide relative counts only) be kept very small even in case of dynamic operation of the target, and can hence be placed in a sufficient degree of redundancy to allow a posteriori error correction. These counters are attached at selected locations within the target circuits, and we show by means of a simulation study as well as a fault dictionary (allows us to identify all single and double SET occurrences in both the targets as well as counters) these architectures indeed fulfill our expectations.

1.3.4 Unique Measurement Infrastructure for SET Pulse widths

Design and analysis of an all-digital on-chip measurement infrastructure, which facilitates long-term monitoring of single event transient durations in digital VLSI circuits exposed to uncontrollable radiation is presented. SET durations are measured by the SET-gated counting of pulses generated by a high-frequency ring oscillator, and stored in a single-event upset tolerant up/down-counter array organized in a ring. Rather than using radiation hardening or explicit triple modular redundancy, we use a novel redundant duplex counter architecture here. For a small number of recorded SETs, our architecture implicitly implements TMR, albeit in a way that degrades gracefully for larger numbers of recorded SETs. Besides standard functional and timing verification, we use Spice-based SET injection for verifying the effectiveness of our SEU-tolerant architecture, and some cross section-based probabilistic analysis for confirming that our measurement infrastructure indeed achieves its purpose.

1.3.5 Design of Radiation Target ASIC

Design aims and concepts as well as implementation results of a digital ASIC are presented, which is dedicated as a target for radiation experiments. It carries various target and measurement circuit blocks mentioned earlier. The resulting area distribution of the final ASIC layout for an industrial 65nm bulk CMOS process is presented in here. We also presented the optimized layout of the target, measurement circuits and PISO for the purpose of our experiments and present all relevant implementation details. The data transmission setup from the ASIC to PC via FPGA is provided. ASIC validation is elucidated in great detail.

1.4 Outline and Methodology

Our thesis is structured in different chapters that are to some extent stand alone parts, which paves a more efficient way for the reader to navigate to the chapters that he/she is interested in without going over the whole document.

Chapter 2 provides an overview of the existing SET injection mechanisms. It comprises of the different circuit level SET injection models and the device level TCAD model typically used to create transient faults in the circuits. A brief analysis on the relevant SET injection models with a sample circuit is presented. Finally the generic simulation setup used for SET analysis throughout the thesis is presented.

Chapter 3 presents a brief introduction of the different hardening mechanisms in the literature, and some of them are explained in great detail. Radiation hardened asynchronous, combinational and sequential circuits are presented. Performance of some of the radiation hardened circuits is analyzed under voltage and temperature variations, while being exposed to radiation in simulations.

Chapter 4 deals with sensitivity to/spatial distribution of SETs in digital circuits. The target circuits used by us to analyze the SET sensitivity in semi-static and dynamic mode are presented. Multiple measurement architectures (that record SET data) for the targets are presented and the pros/cons are discussed in detail. We briefly evaluate the architectures by means of SET simulations. Based on the SET analysis a fault dictionary is generated. We also present a probabilistic analysis to validate out architecture.

Chapter 5 proposes novel targets that can shed light on SET propagation in digital circuits. Unique measurement architectures are proposed for each target. A thorough SET analysis is presented which justifies the chosen architecture. A fault dictionary is created based on the post simulation SET data, which validates the architecture.

Chapter 6 discusses the unique measurement infrastructure designed for recording SET pulse lengths. The gradual development of the infrastructure from recording single SETs to multiple SETs is elucidated. We also describe the provisions taken to protect the infrastructure against SETs (that may lead to corruption of the collected SET data). We perform an SET analysis on the infrastructure to verify its operation. Based on the analysis we provide a fault dictionary that would help us to

decipher the correct SET data. A probabilistic analysis is presented that validates the chosen measurement infrastructure.

Chapter 7 primarily deals with the radiation target ASIC (termed as "FRad chip"). A brief overview of the data transmission architecture (different options) used in the ASIC is presented. We also provide a brief SET analysis for the on-chip transmission architecture. The process of data transmission from ASIC to PC is explained in great detail and summarized. The FRad ASIC is validated by means of SET injection campaigns with all the targets, measurement architectures and PISO in place.

Chapter 8 concludes the findings of this thesis. It also presents the essence of the work and discusses the directions for this work in future research.

CHAPTER 2

SET Injection Mechanisms

Most often it is impractical to subject a circuit to radiation in order to study SETs, hence we need SET models. Previously SET models were built only for space applications, mainly to construct radiation mitigating components. Recent trends in electronics requires us to build SET models not only to construct rad-hard components but to understand charge distribution, SET generation, SET propagation, etc, in digital circuits. Therefore, it is desirable to have good models available that faithfully predict the manifestation of the particle hit as an SET as well as its propagation and masking within the device under test.

One of the best ways to understand SETs is to implement the digital circuits in an ASIC along with sense amplifiers (to monitor SEEs) in all the nodes of the circuit under test and expose the whole setup to radiation [69]. To understand elementary circuits, like inverters, NAND gate, etc. this will be extremely effective. But to understand the SEEs in a circuit of 100 gates, it is not feasible for the reasons listed below:

- Will blow up the required number of sensor amplifiers; as we need to monitor the input, the output and the internal nodes. It is not feasible to build an mixed-signal ASIC with that many amplifiers, as it consumes too much core/pad area.
- Radiation hardened sensor amplifiers are needed to analyze SETs in ambient radiation
- Longer radiation exposure times are required to perform the analysis.
- Extremely complicated/huge external instrumentation (scope, channels, storage, etc.) required to retrieve the data from the amplifiers

Therefore, the above approach can be used to understand SETs in elementary gates. With the knowledge obtained from this approach we can construct effective SET simulation models, thereby building cost-effective monitoring architecture for candidate target circuits.

Our motivation behind the usage of SET models is listed below:

- To choose appropriate target circuits that would help us understand SEEs
- To evaluate the measurement architectures and validate the data provided by them on the particle strikes in the targets.
- To inspect the effectiveness of the radiation hardened architectures in the literature and build efficient mitigation mechanisms for the relevant components employed in the ASIC
- Ultimately, help us build an ASIC that can provide all the information about SEEs when exposed to radiation

At the pre-fabrication phase we inject SETs on all the target and measurement circuits to ensure the collection of useful data when exposed to radiation.

2.1 Background

Over the years a number of SET simulation models that model radiation particle strikes have been proposed in the literature and our survey revealed three potential SET injection mechanisms to mimic particle strikes in a digital circuit:

1. 3D model
2. *Spice model* - analog transistor level model
3. temporary signal inversion in a digital model

3D models basically take into consideration the physical structure of the *device under test* (DUT), angle of particle impact, region of impact, flux, etc. They physically model the charge collection and the decay of the current pulse precisely. In general 3D models are used to understand the SET generation process of a particle strike in a single transistor of a gate in a certain technology. Several finite element-based simulation tools like DAVINCI [36, 37, 119], DESSIS [74, 33, 77, 13], NanoTCAD [93, 105], Synopsis SDevice [4, 3], ACCURO [85] and Cadence Sentaurus-Device [53] have been employed for this purpose, also in mixed-mode simulations with Spice models. Apart from "regular" SET generation [35, 93, 119], physical simulations and experiments also revealed irregular phenomena [51, 12, 3]. Note that 3D modeling usually suffers from the unavailability of technology-related data like doping profiles, which are (at best) compensated by calibrating the models, by e.g. using transistor models from manufacturer's process design kits [13]. But, there are established precise ways of modeling the particle impact e.g. using ACCURO [85] RCI toolset.

To describe the actual generation of SETs, as well as SET propagation along a chain of gates, analytic [95, 26, 72, 77] or *Spice models* [122, 36, 18, 74, 32, 93] are used. A *Spice model* takes into consideration just the transistor level model of the

DUT, it doesn't require the physical model of the DUT to trigger an SET like the 3D model. The usual approaches basically inject a current with a given rise time and decay time. With this model we can control the charge induced in the DUT and the decay time for the induced charge. Note that the SET pulses generated by the *Spice model* depend very much on operating conditions like supply voltage, temperature, load, driving strength etc.[36, 38, 74, 119, 93, 77, 43, 44]. There are established ways of precisely modeling circuit behavior, but precisely modeling particle impact using *Spice model* is an unsolved problem.

In this section we will discuss briefly some of the 3D models and the spice models listed in the literature.

2.1.1 3D models

Different approaches have been proposed in the literature to model soft errors using the Synopsys TCAD 3D device simulator.

To evaluate a system under realistic faults and conditions, a simulation methodology was proposed by Kalbarczyk et al. [74]. The approach is to derive fault models and conduct fault-injection studies at different levels of system abstraction (transistor-level, circuit-level, chip-level and system-level). The primary fault model is obtained by simulating the transistor-level effect of radiation particle strikes. The resulting current bursts create the first-level fault dictionary and are used in the circuit level simulation. The resulting outputs are recorded in the fault dictionary and can be used to analyze the impact of transients at the higher simulation levels, i.e., the chip level and the system level. This approach is extremely helpful for users to observe the effect in the system level, as a cause of a fault in the transistor.

Ramanarayanan et al. [119] proposed a tool to model SETs in the device level. Three different tools were used to model soft errors: the *Monte-Carlo n-particle* (MCNP) toolset for n-si interactions [131]; the *Transport of Ions in Matter* (TRIM) toolset for charge deposition [165], and the Synopsys TCAD Davinci 3D device simulator for charge collection. They found that the charge collection process is weakly dependent on voltage, substrate bias, and angle. Using this tool they calibrate the SER for *device under test* (DUT) and compare it with the SER rate calculated using HSPICE circuit simulations.

Mavis et al. [93] proposed a new circuit level charge collection model, that accounts for the interaction of circuit voltage response with the device physics boundary conditions driving carrier transport dynamics. They illustrate the shortcomings of the Spice model in their paper, as negative voltage is observed at the output of the DUT when a current pulse is injected at the output node. They substantiate their analysis by injecting an SET using a 3D device physics model. Overall they elucidate that the most efficient SET simulation model is integrating the 3D model with the Spice model.

Saremi et al. [126] proposed a model to understand the time response of an inverter to ionizing particles based on physical equations. They derived the model by solving the current equations in three distinct time segments of the voltage tran-

sient. The model is validated by comparing the 3D-TCAD simulations with varying parameters.

Lu et al. [87] present the single event effect of a SRAM using mixed mode simulation of heavy ion based on TCAD in a 40nm process. They observed that the longer the distance from the center of the drain is, the smaller the charge is, the larger the incident angle is, the more easily a particle strike leads to the SEU. They propose the RC simplified mixed-mode simulation and compare it with the 3D-TCAD simulation. It shows that the model can accurately predict the anti single event effect capability, which can provide theoretical basis and data support for the anti radiation and reinforcement of nano-devices.

All of the above approaches provide an accurate way of modeling an SET, but the simulations are time consuming. To model an SET in a circuit of 1K gates using the TCAD model would take months to complete and is quite impractical. To model SETs in elementary combinational gates it is quite reasonable to use 3D-TCAD model; but for larger circuits its not ideal and hence, spice model seems to be the more appropriate choice.

2.1.2 Spice model

A number of Spice analog models have been proposed in literature over the years, which model radiation hits via current injection, and are hence compatible with critical charge (Q_{crit}) models.

For example, Roche et al. [124] modeled the Q_{crit} as a sum of capacitance and conduction component as shown in eqn. 2.1.

$$Q_{crit} = C_N V_{DD} + I_{DP} T_F \tag{2.1}$$

In eqn. 2.1; C_N is the equivalent capacitance of the struck node, V_{DD} the supply voltage, I_{DP} the maximum current of the ON transistor, and T_F the cell flipping time. The capacitance and conductance components do contribute to the Q_{crit}, but it is overestimated by the eqn. 2.1, because the flipping threshold of an inverter is less than V_{DD} (say, $V_{DD}/2$ for perfectly matched NMOS and PMOS). Furthermore the conductance term in eqn. 2.1 considers only the peak values of the current, which is not realistic.

The above issues are addressed to some extent by Xu et al. [159] w.r.t an SRAM cell. They simplified the critical charge model to be dependent on the capacitor, voltage change, transistor drive current and the duration of the disturbance, as shown in eqn. 2.2.

$$Q_{crit} = \int_0^{V_{trip}} C_N dV + \eta I_P T_{pulse} \tag{2.2}$$

In eqn. 2.2; V_{trip} is the static tripping point of the SRAM cell, η is a correction factor, I_P is the driving current of the affected transistor, and T_{pulse} is the duration of the particle-induced current pulse. The critical charge eqn. 2.2 provides a better estimation of the capacitance; by increasing the source/drain junction capacitance

and the addition of a backend MIM capacitor. Even though the critical charge models the capacitance better, it fails to incorporate the dynamics of voltage transient at the struck node, the quantitative description of I_P, and the contributions of different transistors that constitute the cell. Hence, the effectiveness of the estimation of Q_{crit} under process induced variability becomes limited.

Zhang et al. [162] proposed an analytical technique to estimate the Q_{crit} of an SRAM cell in terms of transistor parameters and injected current's amplitude and duration. Unlike the previous model, this model considers the dynamic response to a particle strike. The only pitfall with this model is that they model the noise source using a rectangular current pulse instead of an exponential one.

When an α-particle or a heavy ion generated by a neutron strike crosses a pn-junction, a funneling process occurs as described by Hseih et al. [70] (charge collection by drift is the dominating phenomenon here). Hellebrand et al. [66] proposed a refined circuit-level model that takes into consideration the charge collected by drift, thereby allowing a variable voltage across the pn-junction. They claim that many SET models do not consider the charge collected by drift and thus do not take into account the varying voltage across the pn-junction. They take the double-exponential model as an example and show that it does not consider varying voltage while generating SETs. Ultimately, they built a current model that calculates the drift current of the particle hit. With the help of the simulations they prove that the refined model reveals twice as many critical effects as the traditional current model.

Velamala et al. [152] proposed a probability model that examines the propagation of the SET at any node to the output of a circuit. Using the double-exponential model to create the SETs they study how the sensitivity to SETs changes with CMOS technology scaling.

Gili et al. [55] presented an SET propagation model that can be used to categorize the propagation likelihood of a given signal. They derived some analytical descriptions for SET pulses in terms of their width and height. The formulas obtained are generic, and they claim that models based on these formulas show a good prediction of pulse propagation. The authors extended this model for being incorporated in CAD tools, to automatically determine the reliability of CMOS ICs against SET effects in [56].

Rohani et al. [125] used the double-exponential model as the base to develop an analytical based pulse determination technique which they validated by pulse determination technique from laser experiments.

Wrobel et al. [158] used an accurate model based on simulation of atmospheric neutron induced transient currents in a 90nm drain electrode, through a detailed diffusion model. They used Monte-Carlo tools to conduct this study. They replaced the transient currents with currents based on double-exponential law. The three parameters of the double-exponential model; rise time, fall time and collected charge are only known approximately and are not accurate. Hence, the authors focused only on the shape of the transient pulse in order to make sure that the double-exponential model is as realistic as possible. Their simulations revealed that the current shape has a small influence on the SEU cross-section and SER. They also proved that they

need only two parameters, namely charge collected and the maximum time. The authors conclude that the double-exponential current shape is acceptable to simulate the transient current induced by ionization particles. In [157] they confirm this finding, and they propose to replace the rising time parameter with one fifth of the falling time parameter.

Hamad et al. [59] proposed a methodology to abstract, model and analyze SET propagation at both transistor and gate level. They modeled SET at gate level by utilizing transistor level characterization libraries. They identified the vulnerable nodes and injected SETs at the same, while they also analyzed SET propagation for each injected SET. They claimed that the new gate-level characterization libraries can accurately analyze SET propagation and estimate the soft error rate at RTL level.

Buard et al. [112] propose a methodology that uses a combination of Monte-Carlo-based selection of nuclear reactions, simulation of the carriers transport in the device and spice simulation. They propose a piecewise linear current model that mimics particle strikes in devices. They created a set of currents that would mimic particle strikes to test latchup and burnouts in digital circuits.

Most proposed models agree in the qualitative definition, but differ in essential quantitative aspects [73]. So far the most agreed model to mimic the actual charge deposition mechanism of a particle strike uses double exponential currents [109, 13, 53, 136].

2.1.2.1 Double Exponential Current Model

An analytical model is proposed by Messenger et al. [95] to produce logic upset in the DUT. To inject SET in a transistor of the target, they connect a current source to the source of the transistor such that it generates a double-exponential current pulse according to Eq. (2.3) [95, 155]:

$$I_P(t) = I_0(e^{-t/T_\alpha} - e^{-t/T_\beta}) \tag{2.3}$$

Herein, I_P denotes the transient current pulse, I_0 the peak current of the two exponential terms, T_α the decay time (fall time) of the current pulse, and T_β the time constant for initially establishing the ion track (rise time). Calculations reveal that the total charge Q_P of such a pulse is

$$Q_P(t) = \int_0^\infty I_P(t)\,dt = I_0(T_\alpha - T_\beta), \tag{2.4}$$

At the instance of the strike, the 'OFF' NMOS transistor is turned 'ON' for the short duration of the transient pulse, creating a temporary path from V_{DD} to ground. Therefore the ground current at the time of the particle strike, consists of I_d and the node current since the output capacitance discharges through the NMOS to change the state of the output from logic 1 to 0. Similarly, a particle striking the PMOS, turns it 'ON' for the duration of the particle strike, creating a short circuit path between V_{DD} and ground. However in this case if the 'ON' current produced by

the particle strike is strong enough, then the drain current I_d is used to charge the output capacitance to change the output of the circuit from logic 0 to 1. Therefore, it is observed that whenever a particle strike occurs, there is a conduction path created between V_{DD} and ground giving rise to short circuit current.

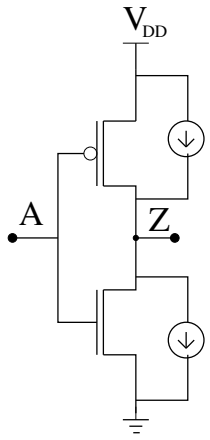


Figure 2.1: Inverter with Double Exponential Current Source

To understand the current model better we injected SETs in the inverter. We injected SETs in the PMOS and NMOS of the inverter at two different time intervals. To inject an SET in the PMOS we connected the current source to the VDD and the output node of the inverter, such that the direction of current is to the inverter from VDD as shown in Fig. 2.1. Similarly, to inject an SET in the NMOS we connected the current source to the GND and the output node of the inverter, such that the direction of current is from the inverter to the GND as shown in Fig. 2.1.

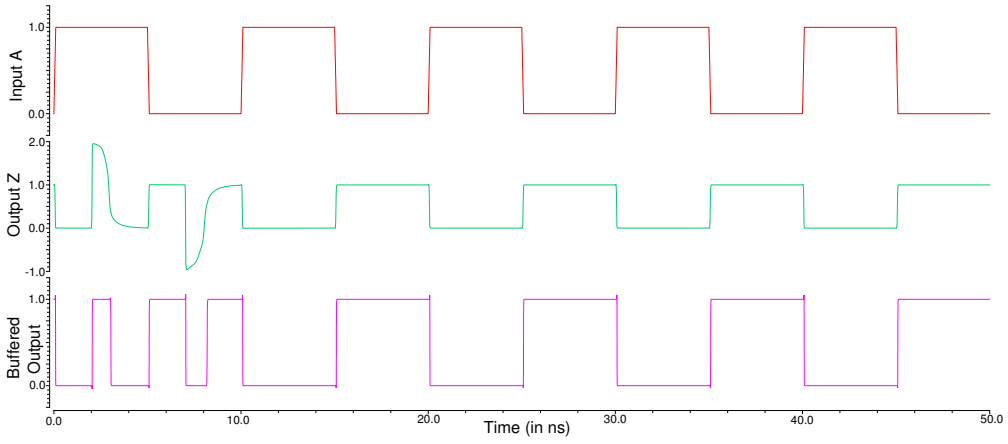


Figure 2.2: Simulation of an Inverter with Double Exponential Current Model

We built the inverter under study using a commercially available UMC 90nm CMOS kit in the Cadence environment. The simulation was conducted using Cadence Spectre simulator and HSPICE simulator at a room temperature. To inject an

SET in the inverter with a critical charge of 450fC we used the following parameters for the current pulse: the rise time constant as 10ps, the decay time constant 100ps and the current injected as 5mA. The output waveform of the inverter with all the relevant nodes is presented in the Fig. 2.2. We can notice that the SET injected in the PMOS of the inverter overshoots the VDD (1.0V) and the SET injected in the NMOS goes below GND (0V) in the second row of the waveform shown in Fig. 2.2. We can also observe the buffered output of the inverter in the third row of the waveform (refer Fig. 2.2). The waveform of the SET mimics the particle strike, but is not perfect as the circuit does not have the parasitic resistance and capacitance included. Furthermore, it overshoots above VDD and goes below 0V, which is the artefact of the current model. Although the current model has some shortcomings, it is a suitable *Spice model* available in the literature to analyze SETs in digital circuits.

2.1.2.2 Improved Current Model

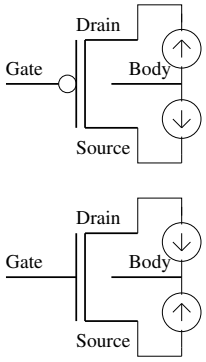


Figure 2.3: Improved Current Model

Kleinosowski et al. [76] proposed a method of modeling SETs in a logic gate using two separate current sources inserted at the source and drain. They claim that they improve the method of analyzing soft errors that arise in a logic circuit. Their current waveforms have a double exponential shape and can be independently adjusted. For simulating an NMOS transistor, the first current source directs current from the source terminal to the body and the second current source directs current from the drain terminal to the body, as shown in the Fig. 2.3. Similarly for simulating a PMOS transistor, the first current source directs current from the body terminal to the source terminal and the second current source directs current from the body to the drain terminal, as shown in the Fig. 2.3. The equation governing this current model is the same as the one used by the double exponential current model Eq. 2.3.

We injected SETs in the PMOS and NMOS of the inverter using this current model to understand the model better, as shown in Fig. 2.4. We used the same parameters used in Sec. 2.1.2.1 for all the sources in this current model. From the conducted simulation we concluded the following:

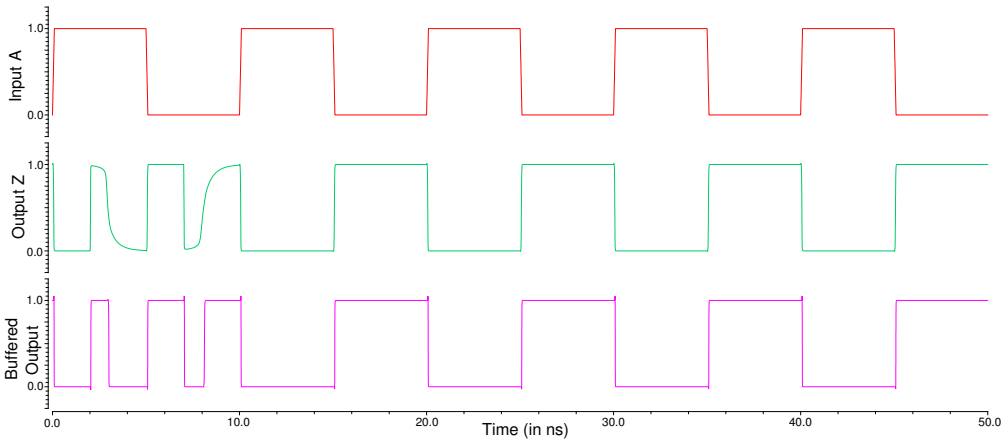


Figure 2.4: Simulation of an Inverter with Improved Current Model

- Unlike the double exponential current model, the inverter output when the PMOS is injected with an SET using this model does not overshoot VDD.
- Similarly, when the NMOS is injected with an SET using this model, the output of the inverter does not go below GND like the double exponential current model.
- One of the prime advantage of this model is that we can target a particular transistor in a circuit to create an upset, while the double exponential model can only concentrate on the nodes

Hence, this model is slightly better than the double exponential current model as it does not overshoot or undershoot. Apart from this we do not see any other advantage of using this model, and hence to analyze a particle strike in the circuit it would be sufficient to use double exponential current model. This way we can avoid using two current sources to trigger a single particle strike.

2.2 SET Simulation Model

Modeling a particle strike is quite complicated. There are three important constraints that we have to take into consideration while modeling a particle strike:

- The radiation source
- Transport of the charge in the device
- Charge collection in the device

For example, when a cosmic particle such as a neutron or proton strikes an ASIC, it produces several simultaneous charge fragments in different directions. It is quite vital to calculate the charge produced by all these fragments. We should also consider the nuclear reaction these particles could create upon impact within the ASIC.

Generally, the charge created by the particle strike would produce electron-hole pairs in the device. These electron-hole pairs would undergo a random walk until they are collected by the device junctions. Since a typical track has millions of electron-hole pairs it would take a very long time to calibrate the random walk. To calculate the charge collection, we need to input parameters such as collecting junctions, depletion region, funnel region, oxide layers, contacts, etc. Hence, to model a particle strike we need to establish a mechanism that stores the time of arrival of these particles, and the evolution of the same.

In modeling the SETs one must perform a circuit analysis of the current pulses at all the nodes. It is important to not only calculate the charge collected at each node, but also the temporal evolution. To perform this we need to know the expected current pulse at the p-n junctions; which could be achieved using device level simulations. Hence, a 3D model was built for this purpose by Hofbauer et al. [129].

2.2.1 3D TCAD model

Like in [74, 93, 13, 119], Hofbauer et al. [129] use 3D device simulations for calibrating and validating the *Spice model*. Relying on 3D TCAD models of the elementary circuits that are derived from the detailed floorplan of a circuit in UMC $90nm$ technology, these simulations allowed them to accurately determine their behavior under heavy-ion radiation: More technically, the charge generation along the ion track in the silicon is modeled with the SRIM-TRIM nuclear code simulation software [165]. The resulting charge generation profile is then used as an input for the Synopsis TCAD device simulator, which can compute accurate SET current and voltage pulses. As a typical example, Fig. 2.5 shows the 3D TCAD model of a single inverter structure. In order to reduce the necessary number of mesh points, the metal connections are not included in the 3D model but rather considered using proper boundary conditions. This does not adversely affect the quality of the simulation results, but saves a lot of simulation time.

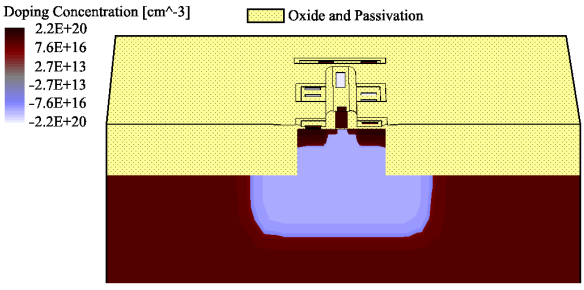


Figure 2.5: TCAD 3D Structure of an Inverter (Cutting Plane through NMOS) [129]

Unfortunately, accurate 3D device simulation also needs technology-related information, like doping profiles and well depths: The SET generation process is very sensitive to those parameters. Since such information is usually only known to the

manufacturer (and typically not disclosed to customers), the need arose to also calibrate and validate the 3D TCAD model. Rather than using transistor models provided in the manufacturer's *process design kits* (PDK), as done in [13], which are of questionable use for accurately calibrating the complex SET generation process, they conducted carefully controlled SET measurements [129] at the micro-beam radiation facility at the GSI [141] in Darmstadt (Germany) for this purpose.

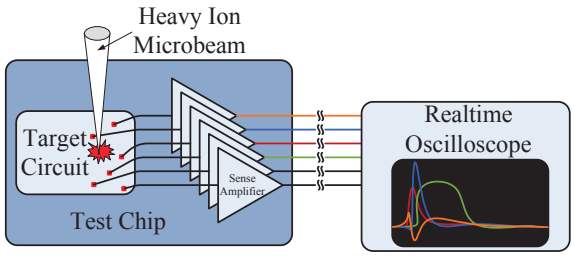


Figure 2.6: Test Chip Schematics for Calibration and Validation of the 3D Model and the Spice Model [129]

In the micro-beam facility they could carefully focus the radiation in the ASIC at sub-μm level and deposit ions, with well-known energy level, at any location of the chip. For this purpose they custom built an ASIC in 90 nm UMC CMOS technology, that hosts target circuits (inverter chains and Muller C-elements) with very high-speed analog sense amplifiers, as shown in Fig. 2.6. The SET voltage pulses generated by the target circuits upon an ion hit (which is detected by a channeltron at the microprobe facility) are low-intrusively captured by these sense amplifiers and finally recorded by an external real-time oscilloscope.

For the inverter chain target circuit, they measured typical voltage pulses as shown in Fig. 2.7 for different impact positions of the ions. It is important to mention that the resulting SETs do not only depend on the impact position of the ion but also on the state of the circuit: For the two different inverter input levels, quite different behavior could be observed [129]: *full-width half-maximum* (fwhm) pulse widths of up to $\sim$1.6 ns for a low (0) input level, and up to $\sim$800 ps for a high (1) input level were observed, with very small rise times.

Finally, calibration of the technology-dependent model parameters of the 3D TCAD models was done by means of offline comparison of the SET voltage pulses predicted by the 3D device simulations and the actual SET voltage pulses recorded in our experiments. Their efforts resulted in 3D TCAD models predictions that match the experimental data sufficiently well, such that we could use the predicted collected amount of charge in the source contacts of the transistors for calibrating the Spice model as described in Sec. 2.2.2. Note that due to the very long simulation times of the complex 3D device simulations and the huge amount of data recorded in their experiments, they are still refining the calibration. In fact, to increase the confidence in the 3D TCAD model, they are conducting additional measurement

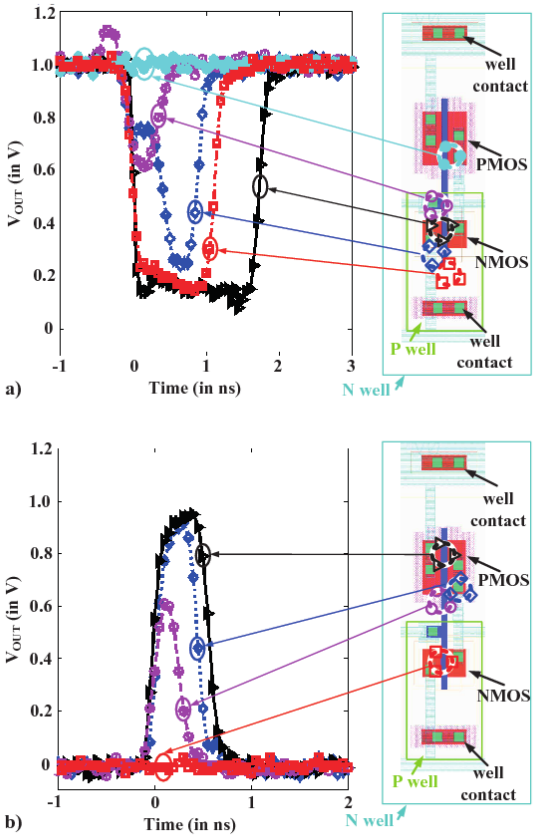


Figure 2.7: Measured SET Voltage Pulses (Inverter) under Heavy-Ion (^{197}Au, 946MeV) Irradiation [129]: SETs for a) Low (0), b) High (1) Inputs

campaigns at the GSI microbeam facility, e.g., using heavy-ions with different energies.

To accurately re-engineer the technology-dependent parameters for the 3D-TCAD model by means of calibration is impractical, as there will always be room for refining the parameters. Therefore, instead of finely refining the technology parameters it is enough to approximately calibrate the technology parameters. They could infer from the 3D TCAD models that the amount of collected charge strongly depends on the impact position of the ion. Approximately 300 fC to 350 fC are collected by the source contact for worst case scenarios, resulting in SETs which are capable to propagate. The corresponding rise times of the SET voltage pulses at the output of the simulated inverter are in the range of 10 ps to 70 ps.

2.2.2 Spice Model

We have already established that physical radiation experiments are difficult and expensive; and 3D simulations are complicated and time consuming; the cost efficient

and less complicated way to study the effects of radiation in a larger circuit is by using the Spice simulations. So, injecting a current pulse with double exponential shape has become the method of choice for emulating a radiation particle strike and the charge of this pulse is considered characteristic for the deposited particle energy.

Based on the data recorded from the radiation experiments and the calibrated 3D model we would tweak the *Spice model* to recreate the particle strike in the transistor level. The current model that we propose to use for this purpose is the double exponential current model governed by the eqn. 2.3. The double exponential model, however, has three degrees of freedom, namely rise time, fall time and peak current, and there is no clear agreement in the literature on their actual choice. Eqn. 2.3 provides the transient current pulse, whereas the peak current of the SET (I_{peak}) is given by eqn. 2.5

$$I_{peak} = I_0\Big(e^{\frac{T_\beta \log(T_\beta/T_\alpha)}{T_\alpha - T_\beta}} - e^{\frac{T_\alpha \log(T_\beta/T_\alpha)}{T_\alpha - T_\beta}}\Big). \tag{2.5}$$

We executed a number of initial simulations using an inverter chain as our target circuit for calibrating the parameters I_0, T_α and T_β. Our goal was to determine a parameter setting which leads to SET voltage pulses (resp. critical charges Q_{crit}) that mimic the ones measured in real-time micro beam experiments as faithfully as possible [68, 69]. Recall that the measured SET voltage pulse lengths ranged up to 800 ps (resp. 1.6 ns) for logic high inverter input (resp. low input), with Q_{crit} in the range of 300-350 fC. We varied the current model parameters I_0, T_α and T_β until both (a) $Q_{crit} = Q_P$ according to Eq. (2.4) and (b) the SET voltage pulse lengths predicted by Spice matched reasonably well.

The modified current model for the gold particle had two parameters as constant the rise time (10 ps) and the critical charge (300fC). We varied the fall time and the peak currents for the same Q_{crit}, to match the SET length of the voltage pulses observed at the output in the 3D model.

In order to get some basic understanding of the transformation of an analog current pulse in an inverter to a digital voltage pulse at the output, Fig. 2.8 plots the length of the SET voltage pulse observed at the output of the buffer (inverter has a buffer as load) over I_0, for fixed[1] $T_\alpha = 100$ ps and $T_\beta = 10$ ps; this results in a peak current of $I_{peak} = 0.78 I_0$ according to Eq. (2.5). There is already a digitally visible SET with a length of 125 ps for $I_0 = 1$ mA, while for I_0 between 2 mA and 10 mA the length of the observed digital SET grows (approximately logarithmically) from 540 ps to 1.4 ns. For $I_0 = 3.33$ mA, (a) Eq. (2.4) reveals an injected charge of about $Q_P = 300$ fC, matching our Q_{crit}, and (b) Fig. 2.8 reveals an SET voltage pulse length of 800 ps that is also in the right order of magnitude.

Indeed, fine-tuning of the model parameters provided us with maximum SET voltage pulses of 800 ps for a high inverter input, which nicely matches the measurement results. For a low inverter input, the maximum SET duration we could

[1]The simple dependence in Fig. 2.8 would not hold if the timing parameters T_α, T_β were also varied.

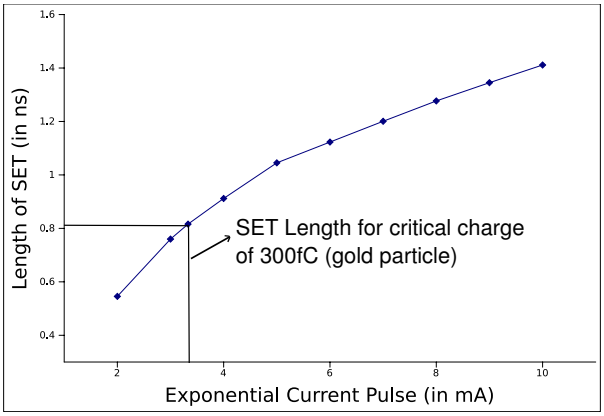


Figure 2.8: Length of SET vs. Exponential Peak Current I_0

generate with our choice of model parameters is 980 ps, which somewhat underestimates our longest measured SET durations. We conjecture that this is, in part, an artefact of the lack of parasitic capacitance in the *Spice model* of the target circuits taken from UMC's PDK. It may also be a sign of the need of some structural improvement of the double exponential current model (cp. [32, 93]), however.

It must be noted here that there are inherent fundamental differences between 3D TCAD model and *Spice model* that render a *perfect* matching of the pulse shape ultimately impossible: The *Spice model* shall represent the complex charge deposition (and collection) process, which is apart from the characteristics of the particle impact as such determined by various and highly non-linear "current paths", by a single current source with a more or less pre-determined current shape, which provides only a few parameters for tuning. When applying such a substantially simplified model to (purposely) abstract away details, one cannot expect a perfect representation of reality. The 3D TCAD model, on the other hand, is much more powerful in this respect, but its high computational complexity makes it practically impossible to also incorporate the entire relevant "context" of the hit transistor in the circuitry (which, however, determines the transformation of the current pulse into a voltage pulse and its propagation).

The single-source double exponential current model employed in our *Spice model* represents the current state-of-the-art, which has been considered a suitable trade-off between tractable complexity and sufficient accuracy in most of the related research work. For compatibility with this research, and also due to lacking alternatives, we simply had to accept the artefacts mentioned above. However, part of our envisioned future work in this area will be devoted to alternative *Spice models*, which provide better modeling accuracy with still acceptable complexity.

2.3 Spice Model Study - C-element Example

We investigate the impact of the chosen *Spice Model* on the Muller C-element. To this end we study the charge required to flip the state of the Muller C-element, while varying rise and fall time. The double exponential current model has too many degrees of freedom, i.e., we can vary the parameters and still generate the same critical charge. In here we will investigate the dependence of the effect of the particle strike for a given critical charge on the shape of a SET. We would like to analyze the behavior of this *Spice model* on the C-element without the 3D TCAD model data or radiation data to guide it.

2.3.1 Muller C-Element

Muller C-element or Muller C-gate is a state holding element originally designed by Muller [104]. It is one of the fundamental building blocks in the design of self-timed circuits. It has two inputs ('a' and 'b') and one output ('z'). The operation of a Muller C-element can be viewed as a (combinational) AND for transitions. Figure 2.9 shows the symbol as well as an implementation of the Muller C-element based on NAND gates. The output of the C-element will remain high (low), if both the inputs are high (low). If the inputs differ then the previous output state is retained. The behavior of the output of the C-element is better explained by the Boolean equation. 2.6. The truth table is presented in Table. 2.1.

$$z = z_{prev} \bullet a + z_{prev} \bullet b + a \bullet b \tag{2.6}$$

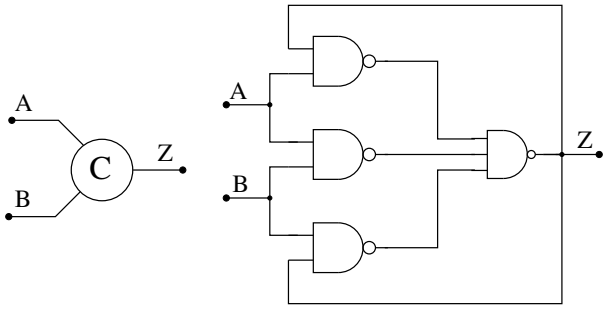


Figure 2.9: Muller C-element (a) Symbol, (b) Logical equivalent

There are different implementations for the Muller C-element namely: static, dynamic and gate-level. Compared to static implementations, dynamic implementation is quite economical; but suffers from excessive static power consumption [143]. Mostly static implementations are preferred because the information stored in the C-element is available for unbounded periods. Our focus is more towards static implementation because they are less complex, have reduced power, transition, and propagation delays.

Over the years different implementations for the C-element were proposed [144, 138, 145, 92, 161, 21, 132], of which we chose to investigate the following:

Table 2.1: Truth Table of Muller C-Element

A	B	Z	mode
0	0	0	transparent
1	0	0	hold
0	1	0	hold
1	1	1	transparent
1	0	1	hold
0	1	1	hold

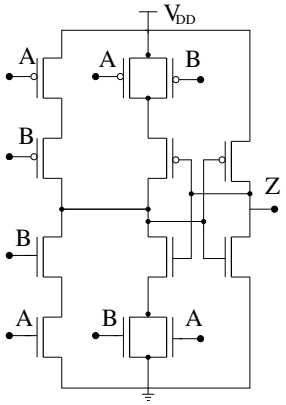


Figure 2.10: Conventional Pull-up Pull-down Muller C-element

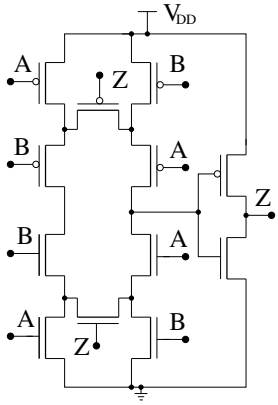


Figure 2.11: Van Berkel Muller C-element

- A conventional pull-up pull-down CMOS implementation introduced by Sutherland et al. [138] is presented in Figure. 2.10. This implementation does not impose any restrictions on the sizes of the transistors, i.e, it is ratioless.

- A CMOS implementation introduced by Van Berkel et al. [145] is presented in Figure. 2.11. The output state of the circuit is maintained through a feedback conducting path of three transistors in the pull-up tree or the pull-down tree. Similar to Sutherland's circuit, this circuit is also ratioless.

- A CMOS implementation utilizing an inverter latch proposed by Martin et al. [92] is presented in Figure. 2.12. The circuit suffers from a driver conflict problem at node Z', which is mitigated by choosing minimum-size transistors for the feed-back inverter [132]. For a proper operation, certain size ratios must be imposed on the transistors.

- A Minority voter based C-element is presented in Figure. 2.13. This circuit uses four inverters and it suffers from high static short circuit current.

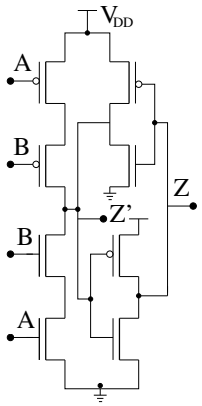


Figure 2.12: Weak Feedback Muller C-element

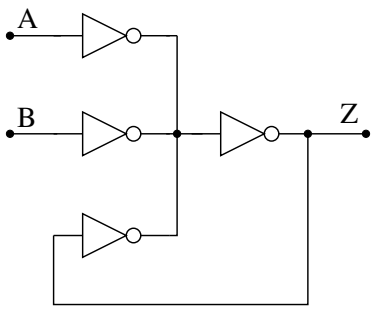


Figure 2.13: Inverter based Muller C-element

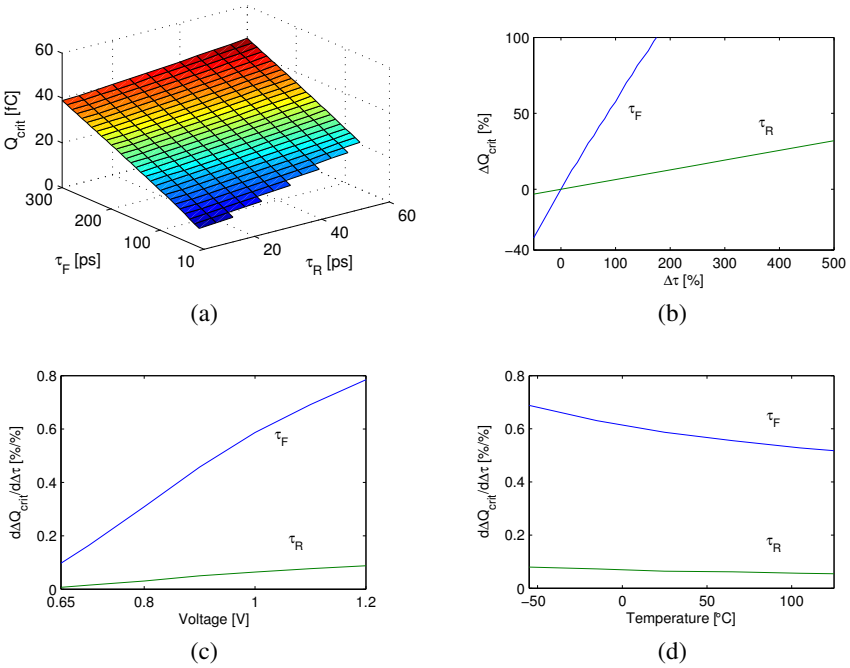


Figure 2.14: Simulation results

2.3.2 Variation Analysis

We performed a campaign of HSPICE simulations on a Van Berkel C-element designed in UMC $90nm$ bulk CMOS with transistor sizing conforming to [132]. According to the aim of our study we varied the T_β and T_α constants from 5 to $60ps$ and from 10 to $300ps$ respectively. For each combination of T values, I_0 was varied to find the smallest current that caused an SEU, thus finding the critical charge. As can be seen in Fig. 2.14a, there is indeed a dependency of Q_{crit} on the two τ parameters.

Figure 2.14b shows two vertical cuts through this 3D-plot, along the nominal values of $T_\beta = 10ps$ and $T_\alpha = 100ps$, respectively. One can see that the dependence is almost perfectly linear for both parameters. Note that we have used relative scales for the x- and y-axis now to better indicate by how many percent Q_{crit} changes if one T is varied by some percentage. The influence in terms of $\%$ change of Q_{crit} per $\%$ variation of T is about 0.064 for T_β, and about 0.59 for T_α.

In a next step we have investigated, how this derivative, in turn, depends on voltage and temperature. Figure 2.14c shows the derivatives of graphs such as that in Figure 2.14b when the voltage is varied from $0.65V$ to $1.2V$, keeping the temperature constant at $25°C$. Again, all values are normalized to the nominal pulse and the corresponding Q_{crit}. Here it is visible that higher supply voltage causes a more pronounced dependence of Q_{crit} on both T values. Figure 2.14d shows the same for varying temperature between $-55°C$ and $125°C$ at a constant voltage of $1V$. Here the variation is relatively insignificant.

2.3.3 Ramifications

Our results clearly indicate that the deposited charge is not the only characteristic parameter of an SET pulse, as often (implicitly) assumed in the literature. The effect of an SET also noticeably depends on its rise and fall time constants. More specifically, short rise and fall times make the pulse more effective, with the choice of the fall time having a much more pronounced impact (when using the nominal values $10ps$/$100ps$ as a starting point). This is important to know, as in experimental studies pulses of very different shapes have been observed [129]. Having no "one-size-fits-all" solution for the simulation model at hand, we are forced to apply pulses of various shapes in our simulations as well, if we want to cover all real-world scenarios. We also found that voltage and temperature not only directly impact the critical charge (this is known, see [146]) but also its dependence on the rise and fall time. For lower voltage, e.g., the choice of T becomes less relevant.

2.4 Simulation Setup for SET Analysis

The default simulation setup that we will use for SET analysis in the rest of the thesis is presented below:

- To perform the SET analysis in all the target/measurement/PISO circuits in the Cadence environment we use this default setup, if not mentioned otherwise.
- Simulations are conducted using either HSPICE [1] or Spectre simulators.
- The double exponential current model is used to inject SETs in the circuits under test. The setup for the current model are as follows:
  - The rise time constant is always set to 10ps
  - The fall time constant is varied from 60ps to 110ps
  - The current pulse I_0 is varied from 2mA to 8mA
- Simulations are conducted for room temperature (27^{o}C)

We chose the current parameters to inject critical charges ranging from 100fC to 800fC in all the devices under test.

CHAPTER 3

Radiation Hardening Mechanisms

The fundamental part of our research is to investigate the effects of radiation particle strikes in CMOS circuits, as well as their propagation. So, we build an ASIC to analyze SETs/SEUs in different types of combinational (NAND, NOR, Muller-C elements, etc.) and sequential elements (Flip-flop chains, Muller pipeline, etc.), we require measurement infrastructure that is resilient as it will be exposed to the same radiation source as the target circuits in some settings. After all, our results are only meaningful, if we can rely on the read-outs. For this purpose we wanted to construct radiation hardened measurement infrastructure for our target circuits.

Considering that newer technology nodes are becoming increasingly susceptible to radiation effects, the efficient hardening of sequential and combinational logic in general, is becoming a relevant problem that is not only restricted to specific safety-relevant functions but may apply to future commodity circuits as well. With this background in mind the analysis presented here can be viewed as a relevant contribution that goes well beyond the scope of our needs.

Many solutions have been proposed over the years regarding both, the modeling of the effect of radiation particle hits as well as their mitigation on technology level, circuit level or system level. Unfortunately, these existing models and circuits are often targeted to different fault assumptions, technologies and application demands – a clear and common picture viewing those from a common perspective is missing. It is therefore not easy for someone without profound experience in the field to identify the appropriate solution for his/her problem. For this purpose we wanted to analyze the available mechanisms and check if there is any appropriate (in terms of actual radiation tolerance and area overhead) mechanism available in the literature.

3.1 Background

There has been a lot of research devoted to radiation-hardened circuit design approaches for combinational and sequential circuits. Several papers report on experimental studies in hardened combinational circuits [52, 164] and radiation hardened

memories [57, 2]. Radiation hardening mechanisms can be categorized as follows: system level [57], circuit level [164, 154] and device level [47, 62, 140].

3.1.1 Device-level Hardening

These techniques involve a fundamental change of or enhancement to the fabrication process to increase the particle energy threshold that can create an SEU [35, 28]. They mainly intend to minimize and mitigate the effect of a particle strike in a device by either using a specific technology process or adding some extensions to the existing technology process. For example, *silicon-on-insulator* (SOI) process has proven to be inherently less susceptible to SEUs than a bulk-CMOS process [114]. The SOI technology is characterized by placing a thin layer of silicon on the top of an insulator during the manufacturing process, which also helps to protect the bulk from charged particles, thereby reducing any SETs. The main drawback of this technology is the fabrication cost.

Usage of the p-well on p-substrate as an effective protection barrier was established by Fu et al. [47]. They have shown that the higher doping of the p-well at the surface reduces the charge collection by funneling and the doping gradient relative to the substrate doping reflects the charge collected by diffusion from the substrate. Both funneling and diffusion charge collection mechanisms have significantly reduced the SER.

A quadruple well structure to isolate the particle strike inside the well was proposed by Hayden et al. [62] to improve the SER. They use a diode isolated array to provide protection against aplha particle events. A junction under this array cuts off alpha particle funneling tails and reduces the charge collected at the storage node after an SER event.

An epitaxial layer on a substrate with a high carrier concentration, or the formation of buried barrier layers using high energy ion implantation is proposed by Takai et al. [140] to protect the DRAM from soft errors. They found that the epitaxial layer is quite effective in reducing SER, but a retrograde well structure with double buried p+ layers was found to be more effective for the soft-error immunity.

There are other ways of hardening such as: shielding the package against radiation (to reduce the exposure of the bare device), usage of rugged SRAMs instead of DRAMs, etc.

Even though these techniques are very effective in reducing SEU sensitivity, we do not pursue them for the following reasons:

(i) Costs incurred by these techniques from a process and materials standpoint might be excessive for mainstream applications.

(ii) Our goal is to analyze SEEs to build better circuits in standard technologies for radiation environment, hence, modifying the process or using non-standard technology is not an option.

3.1.2 Circuit-level Hardening

These approaches are extremely attractive as they let us use standard bulk-CMOS process. The basic principle behind these hardening mechanisms [164, 154] is:

- Employ robust circuit design methodologies that reduce the sensitivity of the final design to SEUs
- Increase the critical charge of the circuit by inserting elements like resistors and capacitors to slow the propagation of voltage transisents

Sizing the transistors to withstand the charge created by the particle strike is a transistor level hardening mechanism proposed by Zhou et al. [164, 163]. They use the brute force circuit level hardening mechanism that would work for any technology node. The required size depends on many factors like charge deposited in the node, drive strength of the gate and original node capacitance.

The *Dual Interlocked storage CEll* (DICE) design proposed by Calin et al. [29] achieves immunity to radiation-induced SEUs. For combinational circuits, a *delay filtering* (DF) mechanism [101] can completely eliminate SET pulses shorter than a critical width. Combining those, a DF-DICE storage element [108] is made tolerant not only to upsets within the storage cells but also to transients on every input signal. The DICE structure mainly utilizes two conventional cross-coupled inverters, connected by two bi-directional feedback inverters. The four nodes of the inverters store the data as two pairs of complementary values (i.e., 1010 or 0101). The logic state of each of the four nodes of the cell is controlled by two adjacent nodes in the feedback. The two nodes on each diagonal do not depend on one another, this dual node feedback control helps achieve immunity to upsets.

A partial duplication approach to provide immunity against soft errors is presented by Mohanram et al. [100]. They selectively target the most susceptible nodes and duplicate the specific circuitry.

A novel circuit level SEU hardening technique for high speed SiGe HBT Logic circuit is proposed by Mukherjee et al. [103]. They reduced the SEU vulnerability of a novel low-voltage high-speed SiGe latch by implementing an additional storage cell redundancy block to achieve the required decoupling.

Garg et al. [52] proposed a novel radiation tolerant CMOS standard cell library that is effective in implementing radiation hardened digital circuits. They exploit the fact that at any given point of time in a gate only PMOS or NMOS transistors are vulnerable. The output driven by the PMOS transistors of a radiation tolerant gate is generated by the PMOS transistors alone and it drives PMOS transistors only. In other words they separate the PMOS and the NMOS transistors in a gate and divide the output into two separate signals, that way any SET in the PMOS would be compensated by the NMOS and vice versa. We tested their design and found that the gates provide an extremely high degree of radiation tolerance. The radiation tolerant logic gates consume a lot more transistors compared to the standard logic gates. For example; a normal inverter consumes two transistors, but, a radiation tolerant inverter consumes six transistors. We performed Cadence Spectre

simulations on the radiation hardened inverter by injecting SETs using the double exponential current model. From the executed simulations we observed that this mechanism provides radiation tolerance for critical charges greater than 500 fC and upto 950 fC.

A redundancy based circuit-level principle for making combinational cells tolerant against single permanent faults and manufacturing defects is proposed in [10]. They provide tolerance by replacing each transistor with four transistors connected in series or in parallel depending on the circuit architecture. They were also able to implement simple fault-tolerant combinational blocks like MUXes and decoders based on their principle.

Overall the mechanisms presented above were proposed for different technology nodes and their hardening capability with UMC $90nm$ bulk CMOS technology must be validated before employing any of the same.

3.1.3 System-level Hardening

The system level hardening mechanisms [57] usually rely on fault-detection or fault-tolerance or redundancy mechanisms that either detect or correct the effects of SEUs. Error detection and correction mechanisms are widely used in memories to provide immunity against SEUs, but are not much useful in protecting combinational and sequential circuits as they consume too much die area.

Neumann et al. [153] proposed the *triple-modular redundancy* (TMR) that uses three identical instances of the same system operating in parallel, and whose results are later processed by a voting system to produce a single output. If any one of the three instances fails, the other two can mask the fault. However, if the voter fails then the complete system will fail. To eliminate this weakness, a triplicated voting mechanism is sometimes used [89]. This strategy only works up to the point where a single, final decision is mandatory, leaving the final voter always unprotected. In order to reduce the visibility of the voter we could increase the number of identical instances (*n-modular redundancy*(NMR)) and spatially reduce the probability of the voter (we relatively reduce the area of the voter) being hit and increase the immunity of the system.

Anghel et al. [9] proposed the usage of *Code Word State Preserving* (CWSP) elements instead of using full hardware redundancy to provide SET immunity. They generate the redundant information by combining self-checking design with time redundancy. If a transient pulse changes an input code word into a non-code word, the output state produced by the last valid code word is preserved. The scheme relies on duplication of signals, which is more efficient than TMR.

A better mechanism for single as well as multiple faults (for NMR schemes) by employing an analog voter built from inverters and an analog comparator is proposed by Lisboa et al. [86]; to show that digital voters are ineffective in a NMR system for multiple upsets. The rationale is that in the analog world an SEU in a single gate can be viewed as noise, which is an everyday problem in this domain. The inverter outputs are shorted together to form one input to the comparator, the

other input is a reference voltage. Askari et al. [11] proposed a redundancy-based fault-tolerance method to design an analog mean voter. The voter selects its output based on the mean of its analog input signals.

Repetition of computations in ways that allow errors to be detected is the basic philosophy behind time redundancy mechanisms [8, 81]. We execute the same operation with the same inputs in the hardware at three different time intervals and ultimately all the results are compared. If there are any errors they will be detected in the results. The basic concept of this form of time redundancy is that the same hardware is used multiple times in differing ways such that comparison of the results obtained at the two times will allow error detection. There are many ways of performing this operation such as: recomputing with shifted operands, recomputing with swapped operands, recomputing with alternating logic, etc. All these different operations are used to detect permanent faults in the hardware.

Ideally these hardening mechanisms should work for any technology node as they are system level mechanisms, but neither of them are explicitly implemented for providing radiation tolerance. Hence, they must be validated before we put to use in our ASIC.

3.2 Proposed Radiation Hardening Mechanisms for Muller C-Element

A particle strike in the C-element could corrupt the stored data; to avoid such a loss we had to build a radiation-hardened C-element. The chosen radiation hardened design should not only protect the C-element against SETs but must also be area efficient. We explored radiation hardening options in both system and circuit level and chose three ways of providing radiation tolerance:

1. Radiation Hardening by sizing mechanism [164]
2. Dual Interlocked Storage Cell (DICE) mechanism [29]
3. PMOS and NMOS Separation Mechanism [52]

3.2.1 Radiation Hardening by Sizing

The weak-feedback C-element is chosen as the target circuit, as it is the most area-efficient (uses only 8 transistors) of all the three transistor based C-element designs. To inject SETs in the C-element we use the setup proposed in Sec. 2.4. Generally, NMOS is more vulnerable than PMOS as the Q_{crit} of the NMOS is less than the PMOS. Hence, if a circuit can withstand an SET in the NMOS then it would be able to withstand SETs in the PMOS; assuming the (W/L) size of the PMOS is either same or more than the NMOS.

We gradually increased the (W/L) size of the NMOS at the output node to withstand the injected charge, while maintaining the sizing constraints imposed on

the C-element. Our aim is to make sure that the C-element withstands a maximum Q_{crit} of 500 fC. As a first step we conducted multiple simulations to appropriately size the C-element to withstand the particle strike of 100 fC. In the next steps we gradually increased the injected charge in increments of 50 fC to a maximum of 500 fC. The (W/L) size of the transistor was gradually increased to withstand the particle strikes and the appropriate size was validated using Spectre simulations. The minimum (W/L) sizing required for the weak-feedback C-element to withstand a particle strike of 500 fC turned out to be 14 times the original W/L.

3.2.2 Dual Interlocked Storage Cell Mechanism

Our aim is to use the DICE principle to provide tolerance to the weak-feedback C-element. Note that this principle was originally adapted only for latches and flip-flops; the authors didn't propose this mechanism for a C-element. Hence, we had to adapt this principle for the C-element. In order to do so we chose the weak-feedback Muller C-element as that structure uses a guard gate and two inverters. We replicated the guard gates of the C-element, as shown in Figure. 3.1. Similarly we also replicated the two inverters and constructed it such that two of the diagonal inverters have higher drive strength compared to the other two inverters.

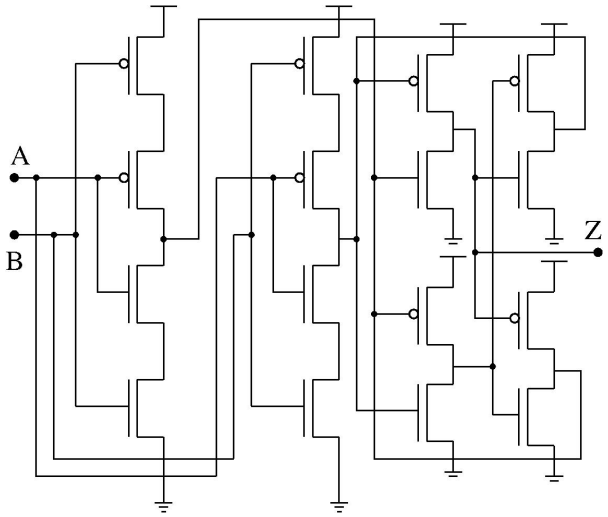


Figure 3.1: DICE Cell Based Muller C-element

The DICE structure as it is did not perform as expected for the UMC $90nm$ bulk CMOS technology. Note, that it was proposed initially for a different technology. In order to ensure the operation (provide immunity) of the DICE cell we re-sized the whole structure, which turned out to be an overkill. Therefore, we decided to re-size parts of the structure to provide immunity for 500 fC critical charge; in particular we re-sized the strong inverters. But, the C-element was not quite stable after the re-sizing of just the strong inverters, hence, we re-sized the guard gates to make the C-element stable. In essence we increased the (W/L) size of the guard gates and

the strong inverters by 1.5 and 4, such that they could withstand particle strikes of 500 fC.

3.2.3 Radiation Hardening by Separation Mechanism

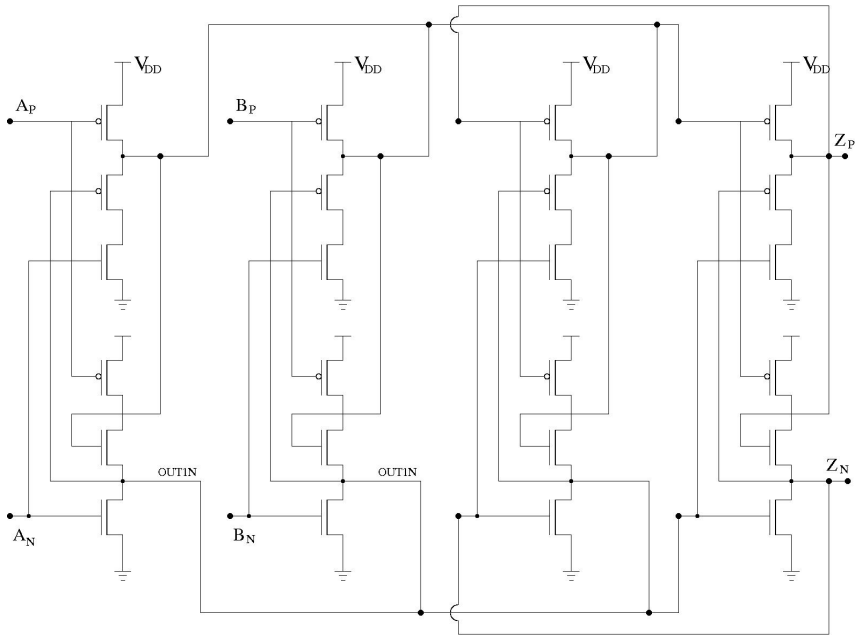


Figure 3.2: Radiation Hardened Muller C-element using Separation Mechanism

To build a radiation tolerant C-element using the separation mechanism proposed by Garg et al. [52], we cannot use any of the transistor level implementations of the C-element. We can either use the logic gate based C-element implementation or the inverter based C-element implementation. The logic gate based implementation consumes a higher number of gates compared to the inverter based implementation, hence, consumes more die area. Therefore, we chose to use the inverter based implementation to build the radiation hardened C-element as presented in Fig. 3.2. We executed simulations (using the setup presented in Sec. 2.4) in the C-element by injecting SETs of charges ranging from 100 fC to 950 fC, and concluded that the C-element is indeed radiation tolerant.

3.2.4 Summary

Overall we have adapted and investigated three radiation hardening mechanisms for the Muller C-element, all of which provide radiation tolerance up to a charge of 500 fC. As we would like to use the most area efficient radiation hardening mechanism, we calculated the area equivalent of the three approaches which is presented in Table. 3.1. The area equivalent is calculated based on the transistors and (W/L) sizing, not based on the layouts of the approaches.

Table 3.1: Comparison of Radiation Hardening Mechanisms for Muller C-element

Components	No. of Trans.	(W/L) Sizing	Area Equiv.
Non Rad-Hard	8	1	8
Rad-Hard Sizing	8	14	112
DICE Cell	16	Multi-sizing	32
Rad-Hard Separation	24	1	24

From Table. 3.1 we can observe that the sizing mechanism consumes higher area compared to the other mechanisms. The most area efficient mechanism is the Muller C-element with inverters, but it has a higher static current and routing complexity. The DICE cell based mechanism avoids the drawbacks imposed by the separation mechanisms and still has a relatively low area equivalent. Based on this we concluded that any particle strikes of charge $\leq$ 500 fC can be mitigated more efficiently using the DICE mechanism, and for particle strikes $\geq$ 500 fC we can use the separation mechanism.

3.3 Combinational Circuits

Most circuit-level hardening techniques to date have focused only on memories [2], latches and flip-flops. There is a significant amount of research done in protecting the memory arrays and the latch elements, and comparatively there is very little research available relevant to combinational circuits. Moreover, for current and future technologies, the impact of soft errors on combinational elements is now receiving significant attention. In $45nm$ technology node, a majority of the observed soft failures will be related to SET events that occur in logic blocks [15, 97]. Hence, it is critically important to develop effective techniques to analyze and quantify the impact of soft errors on combinational logic circuits. Furthermore, voter circuits are often the residual single point of failure in system-level fault tolerance solutions, which causes a specific interest in making the related, combinational circuits radiation tolerant. Our aim here is to evaluate the potential of the existent fault-tolerance and radiation-hardening mechanisms to provide immunity (for a particle strike with a charge of 500fC) for an XOR (Exclusive-OR) gate built using UMC $90nm$ bulk CMOS technology. The reason behind using the XOR gate as a target is because it is one of the pivotal gates in building measurement counters.

The XOR is a very basic gate, specifically for asynchronous circuits where it forms the logical OR for transitions. Moreover it is fundamental in parity checking circuits. One of the most crucial activities to be performed by our SEE monitoring architecture is to detect the differences between two signals, for which we require an XOR gate. Besides, an XOR gate has a very different internal structure, compared

to the NAND/NOR gates (the internal structure is not complicated for these gates). We have chosen two types of XOR gates as our targets:

1. Cross-Coupled (CC) XOR gate constructed using inverters and pass transistors as shown in Figure. 3.3, and

2. Invert-AND-OR (IAO) XOR gate, constructed using standard gates as shown in Figure. 3.4. This gate is a standard expansion of the XOR function ($Z = A \bullet \overline{B} + B \bullet \overline{A}$).

Before we validate the state-of-the-art mechanisms for tolerance against SETs, we need to analyze the behavior of the XOR gate when exposed to radiation. We injected SETs in the XOR gate using the state-of-the-art SET injection current model, to examine their behavior under exposure.

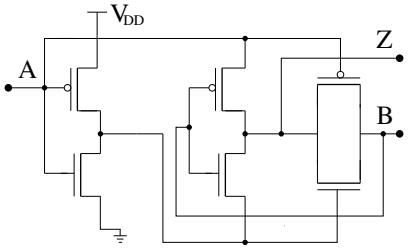


Figure 3.3: Transistor level Schematic of Cross Coupled XOR gate

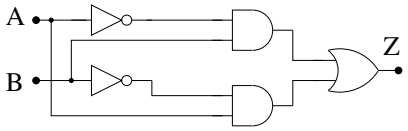


Figure 3.4: Gate Level Schematic of IAO XOR gate

3.3.1 SET Analysis – XOR gate

We injected SETs in the CC XOR gate using the setup presented in Sec. 2.4. We monitored the output of the inverters and the transmission gate, to help us trigger SETs at the NMOS (PMOS) when the node output is 1 (0). The SET simulations for both the NMOS and PMOS transistors are shown in Figure. 3.5. The waveforms are self explanatory.

For the IAO implementation of the XOR gate, we injected SETs at the outputs of both the AND gates and the OR gate at different time intervals. In Figure. 3.6 we present the SET simulations of the IAO XOR gate for both NMOS and PMOS transistors. The waveforms of the input signals (A,B) and output signal (Z) are presented in Figure. 3.6 (first three rows). The output of XOR gate with SET hits in the AND gates ($A \bullet \overline{B}$ and $\overline{A} \bullet B$) are presented in rows 4 (refer "SET in AND1"

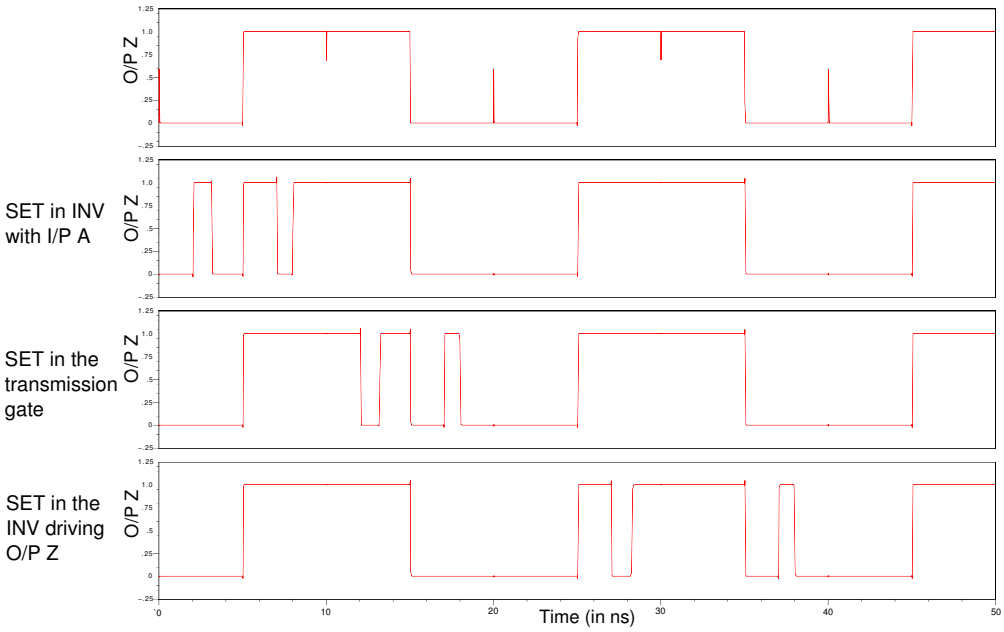


Figure 3.5: Simulation of SET hits in CC XOR gate

of Fig. 3.6) and 5 (refer "SET in AND2" of Fig. 3.6). Note, that we do not present the output of the AND gates in the waveform, rather we show the effect of the SETs triggered in the same on the XOR gates' output. Similar, the effects of SETs in the OR gates are presented in the last row. We can observe that the SETs we triggered in the AND and OR gates successfully propagated to the output of the XOR gate. We will use the same set of tests to validate the radiation hardening mechanisms built for the XOR gates.

3.3.2 Radiation Hardening Mechanisms

To justify confidence in the readouts collected by the measurement infrastructure on our experimental ASIC, we require tolerance against double faults. We can employ any of the methods presented in Section. 3.1 to achieve this. However, to find out (i) which method actually withstands double faults (the original papers are focused on single faults) and (ii) which is the most efficient solution for our chip, we will perform extensive fault simulation studies using the setup introduced in Sec. 2.4. For the functional principle of the respective methods please refer to Sec. 3.1.

3.3.2.1 Radiation-Hardening by Gate Sizing

As a first attempt we used gate sizing to protect the CC XOR gate against SEUs. In our simulation we triggered SETs at all circuit nodes (refer Fig. 3.7). To harden the gate we increased the (W/L) of the transistors in the XOR gate (not the buffer) gradually, by increasing W while keeping L constant. For a gate with $8 * (W/L)$ we can observe that the pulse width of the SETs is already reduced but still visible.

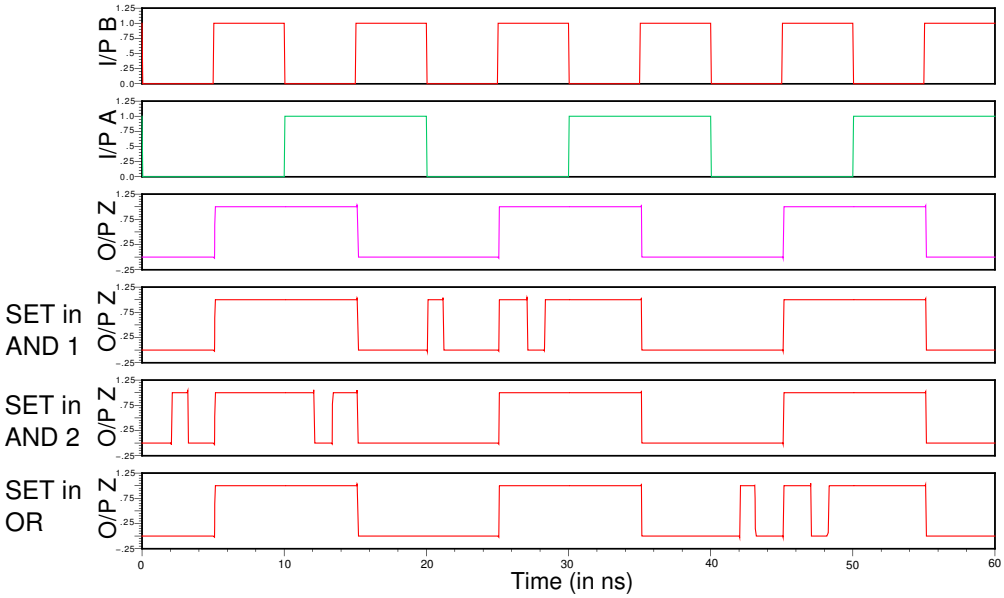


Figure 3.6: Simulation of SET hits in IAO XOR gate

Eventually we observed that for a CC XOR gate with $14 * (W/L)$ we can mitigate all SETs at the buffered output (refer Fig. 3.7), although the unbuffered output still shows minor spikes. This indicates that we are right at the borderline with the sizing, confirming that the solution is safe. This also nicely matches our results from Sec. 3.2 for the Muller C-element.

Similarly, for the IAO XOR gate we found an 8-fold increase of (W/L) necessary for mitigating all SETs.

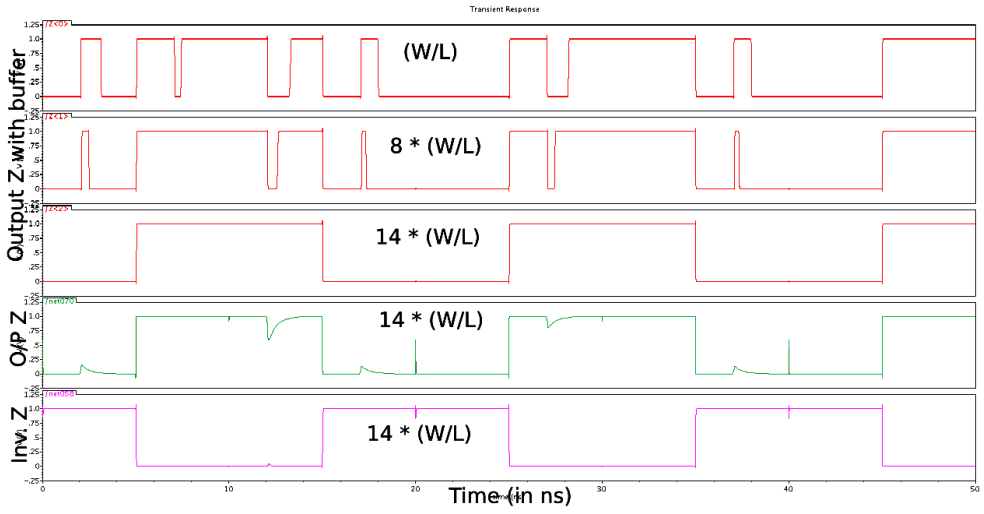


Figure 3.7: SET Simulations of Rad-Hard CC XOR Gate

3.3.2.2 Defect-Tolerant Logic

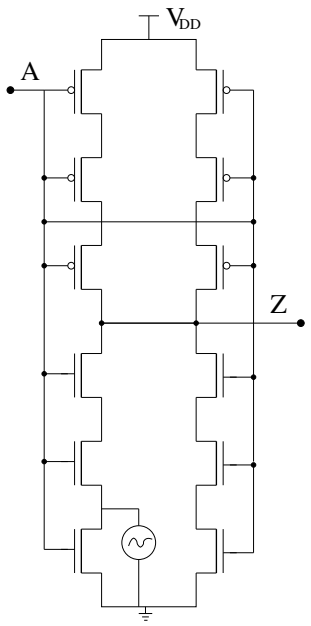


Figure 3.8: Defect-Tolerant Inverter

Anghel et al. proposed an architecture that can tolerate defects and permanent faults in the logic gates [10]. We wanted to verify if the architecture is immune to soft errors as well and if so its application in building an XOR gate. For this purpose we built an inverter based on their architecture, as shown in Figure. 3.8.

To validate the inverter's immunity against soft errors we injected SETs into all circuit nodes. Figure. 3.9 illustrates some of the results. For an input as given in row 1, row 2 shows the output of the inverter in the fault free case, which serves as a reference for its correct behavior. SET hits at the bottom (top) NMOS (PMOS) transistor of the inverter are presented in row 3. Finally, row 4 illustrates the output behavior for SET hits at the NMOS (PMOS) near the output. In both the cases we can observe that the circuit is not radiation-tolerant. We also injected SETs in the transistors in the middle, and found out that the circuit is not radiation tolerant (we do not present the results in the figure).

The SET analysis reflects that the original purpose of this circuit is rather *defect* tolerance. In order to radiation harden the circuit, we had to increase the (W/L) size of all transistors by 16 times. This is slightly more than for the non-tolerant inverter, however, yields a solution that is both radiation tolerant as well as defect tolerant. Our focus is towards radiation tolerance and not defect tolerance, hence we do not pursue this mechanism. Furthermore, we do not build an XOR gate using this approach either.

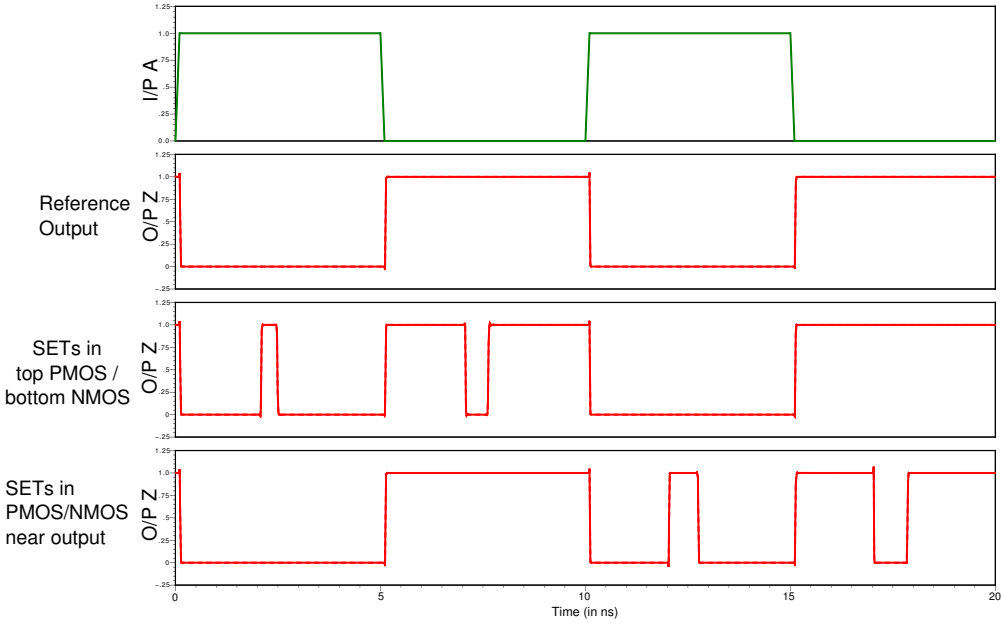


Figure 3.9: Simulation of SETs in Defect-tolerant Inverter

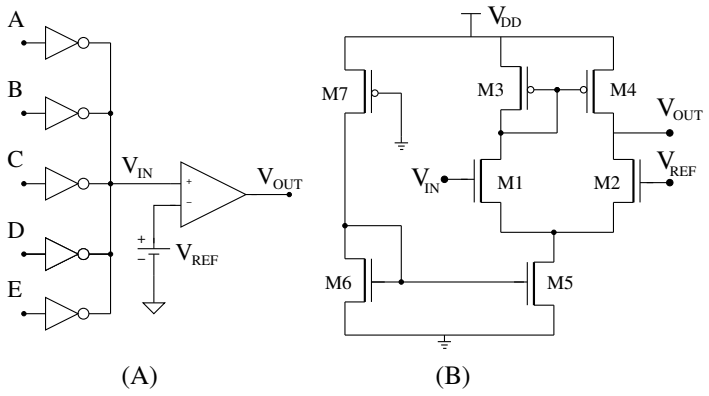


Figure 3.10: Analog Voter with Comparator

3.3.2.3 Analog Voter

Following the approach of Lisboa et al. [86] we constructed a radiation tolerant XOR gate based on replicated (unprotected) CC-XOR gates feeding an analog voter with inverters and an analog comparator as shown in Figure. 3.10. Initial simulations revealed that to sufficiently outweigh the influence of one failing replica in the analog sum and thus attain radiation tolerance we had to use 5-fold redundancy instead of TMR for the XORs (not shown in Figure. 3.10) sourcing the inverters and for the inverter structure.

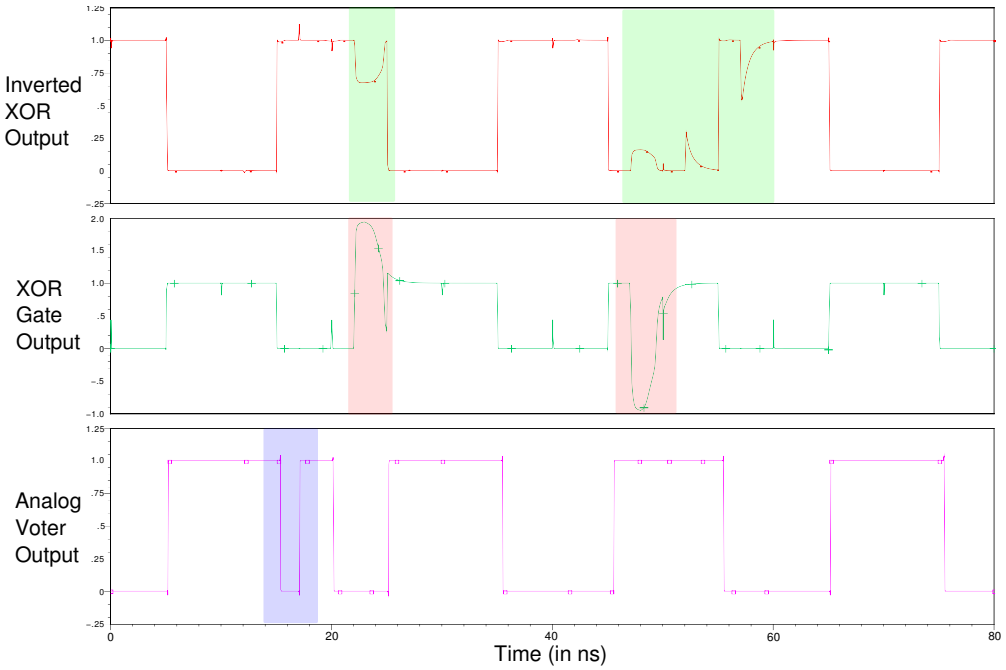
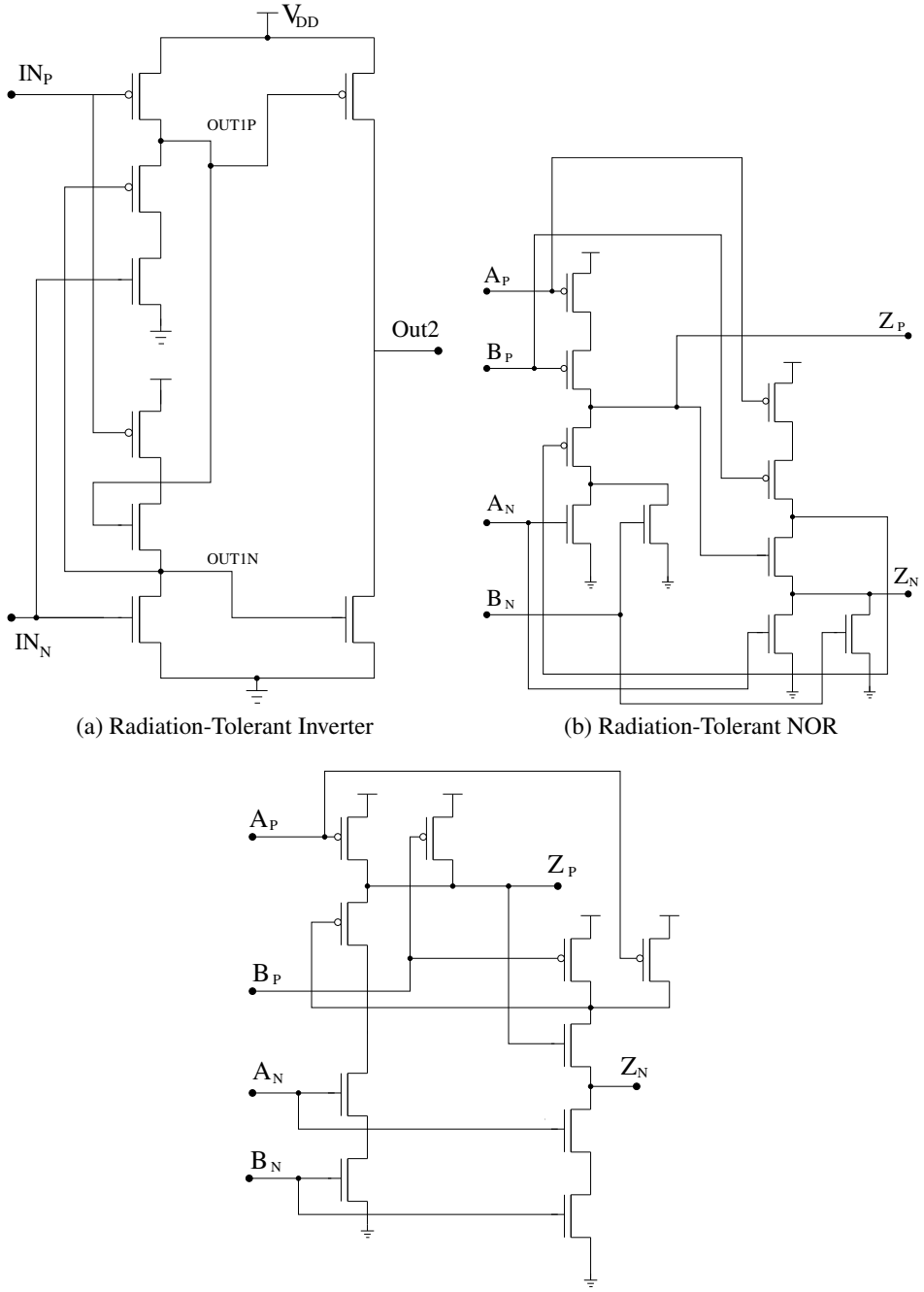


Figure 3.11: SET Simulation of XOR gate with Analog Voter

We injected SETs in all the nodes of the XOR gates, the inverters and the comparator. Figure. 3.11 illustrates some results, namely the output of one of the inverters (row 1) and the XOR gates (row 2), each when being subjected to an SET. The output of the comparator when exposed to particle strike is presented in row3. We observe that all the SETs originating from the XOR gate and the inverter are mitigated, but one of the SETs within the comparator is not mitigated. In conclusion, the circuit is not fully radiation tolerant, however, its weakness is limited to a very small spot. This can be avoided again by appropriate sizing. However, since sizing is a very intricate issue for the analog comparator (see [86]) we did not further pursue that.

3.3.2.4 Radiation Hardening by Separation Mechanism

We constructed a radiation-tolerant XOR gate inspired from the architecture presented by Garg et al. [52]. Notice that this approach does not work for the CC XOR



(a) Radiation-Tolerant Inverter

(b) Radiation-Tolerant NOR

(c) Radiaiton-Tolerant NAND

Figure 3.12: Radiation Hardening by Separation Mechanism

as it is not applicable to transmission gates. So we went for an IAO-based implementation. We built the XOR gate using the NAND, NOR and inverter, and their radiation tolerant implementations are presented in Fig. 3.12.

We injected SETs in all nodes of the XOR gate and observed that the output of the XOR gate (last row) is not affected by any of the particle strikes (simulation results presented in Figure. 3.13). The injected SETs with their locations as presented in the Fig. 3.13 are listed below:

- ***Row 1***: SETs in the NMOS of the inverter driving one of the input signals
- ***Row 2***: SETs in the PMOS of the inverter driving one of the input signals
- ***Row 3***: SETs in the NMOS of the NAND gate
- ***Row 4***: SETs in the PMOS of the NAND gate
- ***Row 5***: SETs in the NMOS of the NOR gate
- ***Row 6***: SETs in the PMOS of the NOR gate

From the simulations we can observe that none of the SETs created any impact in the output of the XOR gate. Overall we can conclude that this circuit can indeed mitigate all SETs. Even with minimum transistor sizing SETs with charge greater than 950fC turned out to be necessary to create an upset, which is nearly double the value we applied to the other schemes. Also note that interfacing this logic to the normal gates is simple (refer Fig. 3.12 (a)).

3.3.2.5 Code Word State Preserving (CWSP) Element

Recalling that by using CWSP as proposed in Anghel et al. [9] we cannot achieve radiation tolerance for the output node, we constructed a CC XOR gate as follows (Fig. 3.14): We built the input inverter in a CWSP style. Furthermore we use an extra CWSP inverter for the B input (as we have to supply an inverted input to B), which not only protects the input as such but also the inverter driving the XOR output. So we do not have to use CWSP for the latter. CWSP is not applicable to the transmission gate.

As expected, our simulations showed that any SET occurring at the output of the CWSP CC XOR gate cannot be mitigated by the architecture itself. In order to provide immunity against particle hits in all the nodes we had to increase the size of transistors by 22, 18 and 14 times (W/L), depending on the position (we did not need to re-size the transistors of the delay elements). This mechanism is worse than radiation hardening by sizing mechanism. Hence, we decided not to proceed further with this mechanism, therefore, we did not implement the IAO XOR gate using the same.

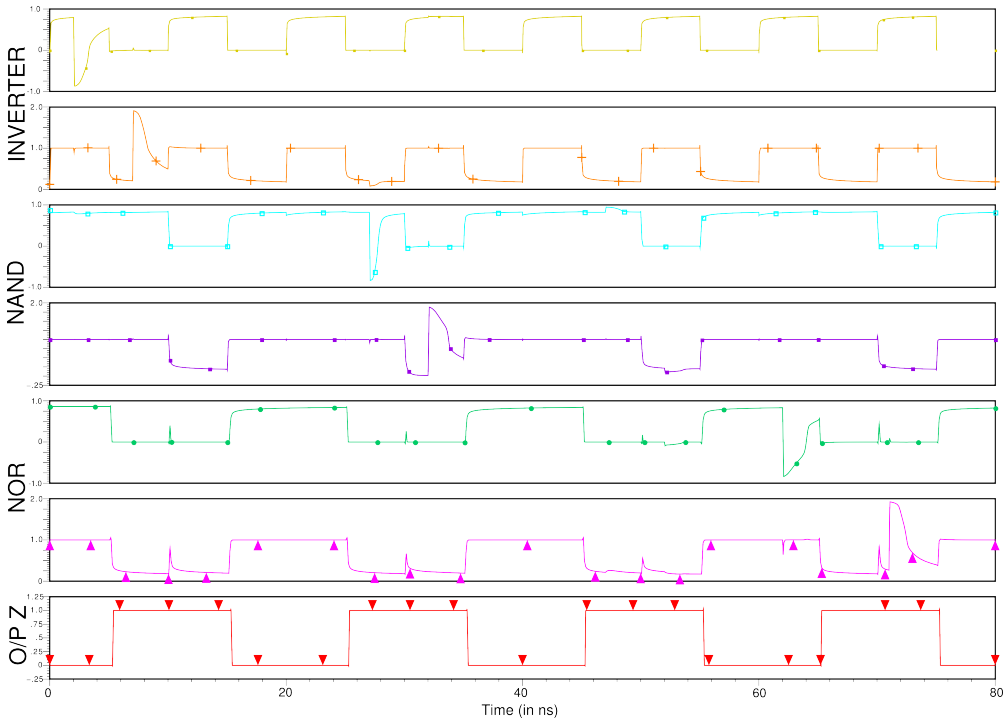


Figure 3.13: Simulation of SETs for Radiation Tolerant XOR gate

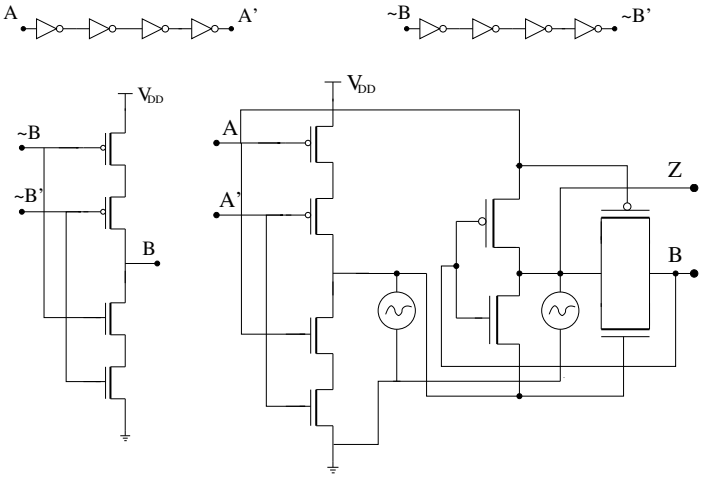


Figure 3.14: CWSP CC XOR gate

3.3.3 Summary

Our simulation-based analysis and optimization has yielded a set of circuit implementations that are finally (with one exception) all sufficiently radiation-tolerant (for $Q < 450fC$) for our envisioned on-chip measurement circuits. To identify the most efficient ones, we will compare those circuits with respect to their area overhead. Since the latter significantly depends on routing, original (i.e. unscaled) W/L ratio, technology and many other factors, it is difficult to provide accurate figures here. Therefore we simply use the number of transistors multiplied by the required scaling factor as a first estimate.

Table 3.2: Comparison of Different Fault-Tolerant Mechanisms

Target	Approach	Section	No. of Trans.	(W/L) Sizing	Area Equiv.
Inverter	Sizing	3.3.2.1	2	*14	28
	Defect Tolerant Logic	3.3.2.2	12	*16	192
	Separation	3.3.2.4	6	*1	6
XOR	Sizing	3.3.2.1	6	*14	84
	Separation	3.3.2.4	60	*1	60
	CWSP-XOR	3.3.2.5	28	*1/ *14/ *18	216
	5-MR XOR with Analog Voter	3.3.2.3	47	cf. Lisboa [86]	91

Table. 3.2 clearly shows that radiation hardening by transistor sizing is superior to the defect tolerant logic for the inverter implementation. Due to its prohibitive overhead the latter is not further considered for the XOR implementation; it might only be beneficial for cases where permanent faults need to be tolerated as well. Among the XOR implementations CWSP is definitely the most inefficient choice, requiring the highest area and yielding a relatively complex circuit (recall Figure. 3.14). The remaining techniques all seem to exhibit acceptable overhead. In the voter based design the analog comparator with its need for an analog reference voltage is problematic.

The separation approach appears to be most efficient in terms of area, however this is misleading: It requires a very high number of transistors and complex routing which is not considered in this table. Still it provides very high robustness even for up to 950fC, so it is a viable choice. The conventional radiation hardening by sizing represents an efficient and well proven solution. It involves the lowest risk in terms of routing and circuit complexity, and since in our experiments we do not expect particles with more than 450fC, it seems to be the best choice.

At this point it is also interesting to think about the circuits' robustness against coincident faults: Radiation hardening relies on increasing the individual node capacitances, through which the circuit naturally withstands coincident faults at sev-

eral nodes. The same applies to those parts of the other circuits that we improved by re-sizing. The separation approach, in turn, is robust through the strict separation of N- and P-stacks: As the only threat is switching off a currently conducting stack, it does not matter how many coincident impacts actually contributed to this effect. In the CSWP-XOR all inputs are protected individually and can hence withstand coincident SETs, while the internal nodes benefit from the re-sizing. The only problematic circuit with respect to coincident hits seems to be the analog voter, whose structure implies weaknesses when multiple inputs are hit. We have performed comprehensive simulations for double-fault scenarios, which gave good confirmation for the above statements.

3.4 Performance under VT Variations

The effectiveness of the radiation hardening mechanisms chosen for the circuits to mitigate particle hits has so far been studied mainly under nominal voltage and room temperature. We would like to explicitly analyze the performance of two selected radiation hardening techniques (namely transistor sizing and stack separation) under temperature and voltage variations.

We would like to know how the radiation hardening techniques perform under those variations, and how much they need to be enhanced to still attain the desired level of radiation tolerance under worst conditions, as compared with the best case. This insight will not only globally provide us a feeling for how sensitive radiation tolerance mechanisms are to those variations, it will also, more specifically, allow us to judge the additional cost of allowing a wider range of operating temperature or supply voltage variations for a given circuit. To this end we will subject an inverter hardened by the respective method to simulation based SET injection using the current model from Sec. 2.4.

We decided to use a simple inverter circuit to test these techniques. As we are going to conduct tests in varying voltages, temperatures and particle charge; we would like to keep the simulation complexity simple. Increasing number of nodes will increase the complexity of the analysis and, hence, we chose the smallest circuit.

3.4.1 Target Circuits

The radiation tolerant inverter based on the stack-separation mechanism was already presented in Figure. 3.12. Note that it will always generate two outputs (“OUT1P” for the P-stack and “OUT1N” for the N-stack). For the conversion to single rail at the circuit output, these outputs are connected to the PMOS and NMOS transistors of a normal inverter as illustrated in the right part of Figure. 3.12. As explained in Section. 3.3.2.4 no sizing constraints need to be considered, so the standard sizing can be used for this rad-hard mechanism. In contrast, the radiation hardening by sizing requires the transistor sizes to be increased, while at the same time the mobility ratios between PMOS and NMOS should also be considered.

Table 3.3: Required sizing for different choices of current pulse parameters, all with a charge of 450fC

Rise Time (T_β)	Fall Time (T_α)	Peak Current (I_0)	Required (W/L) Sizing
10ps	110ps	4.5mA	32
10ps	130ps	3.75mA	27.8
10ps	160ps	3mA	23.28
10ps	210ps	2.25mA	18.4
10ps	260ps	1.8mA	15.2
10ps	310ps	1.5mA	13
10ps	460ps	1mA	9

3.4.1.1 Sizing Requirements for Rad-Hard Sizing Mechanism

For analyzing the impact of the pulse shapes we executed a set of simulation in Cadence Spectre to determine the required sizings (at nominal voltage and 25°C) for various choices of the SET current pulse parameters like current and fall time. In a first campaign we varied peak current and fall time in such a way that, according to eqn. 2.3, the injected charge always amounted to 450 fC (recall Sec. 2.4 that we generally fixed the rise time to 10ps). Although the injected charge was thus constant, we observed significant differences in the resulting SET length, and accordingly the amount of sizing required to make the inverter rad-hard varied. We will later discuss the changing SET lengths in Section. 3.4.2, for now we will focus on the required sizings that are shown in Table 3.3.

We can notice that for a fall time of 110ps and 4.5mA the required sizing to make the inverter rad-hard is 32, while for a fall-time of 460ps and 1mA current it is just 9. From comparisons with preliminary radiation experiments [129] we already know that this significant difference is at least partly an artefact of the state-of-the-art SET current injection model. Since we do not have a better model available, we randomly choose two different parameter sets from the Table 3.3 (along with the respective sizing) in order to make sure that our predictions for the *voltage and temperature* (VT) variations hold:

- T_β =10ps, T_α = 110ps, I_0 = 4.5mA
- T_β =10ps, T_α = 160ps, I_0 = 3mA

We performed the same analysis for sets of fall time and peak current resembling a charge of 300fC. The results are presented in Table 3.4. Again we can observe a significant difference in the required sizing, ranging from 22.2 (110ps/3mA) to 9 (310ps/1mA). Like before, we decided to choose two parameter sets:

- T_β =10ps, T_α = 110ps, I_0 = 3mA

Table 3.4: Required sizing for different choices of current pulse parameters, all with a charge of 300fC

Rise Time (T_β)	Fall Time (T_α)	Peak Current (I_0)	Required (W/L) Sizing
10ps	110ps	3mA	22.2
10ps	130ps	2.5mA	19.2
10ps	160ps	2mA	16.2
10ps	176.67ps	1.8mA	14.8
10ps	210ps	1.5mA	12.8
10ps	260ps	1.2mA	10.56
10ps	310ps	1mA	9

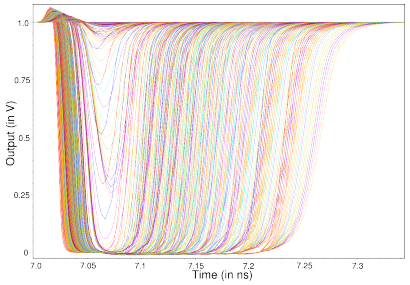
- T_β =10ps, T_α = 160ps, I_0 = 2mA

3.4.2 Setup for VT Variation Experiments

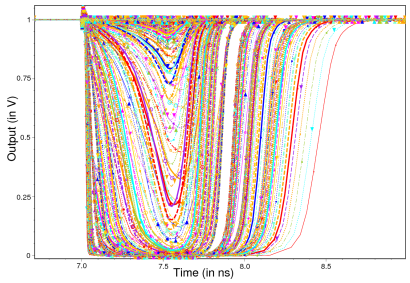
We do not use the generic setup presented in Sec. 2.4 for this simulation campaign. For the VT variation experiments we decided to vary the supply voltage (V_{DD}) from 0.65V to 1.2V with a step size of 25mV (nominal voltage is 1.0V). When going below 0.65V the PMOS transistor will be unable to pull-up in sufficient time. We tried to make the step size small enough to see all relevant details, while still keeping the number of points reasonable in the interest of simulation time. Similarly we decided to vary the temperature from -55°C to 175°C, with a step size of 10°C. So, we finally ended up with a VT space comprising 552 points. As mentioned above we did the analysis for two charges (450fC and 300fC) with two different fall times and peak currents each. So for each radiation hardening mechanism we ran through the whole VT space for the following four different particle characteristics:

- T_β =10ps; T_α = 110ps; I_0 = 3mA; Q_{crit}=300fC
- T_β =10ps; T_α = 160ps; I_0 = 2mA; Q_{crit}=300fC
- T_β =10ps; T_α = 110ps; I_0 = 4.5mA; Q_{crit}=450fC
- T_β =10ps; T_α = 160ps; I_0 = 3mA; Q_{crit}=450fC

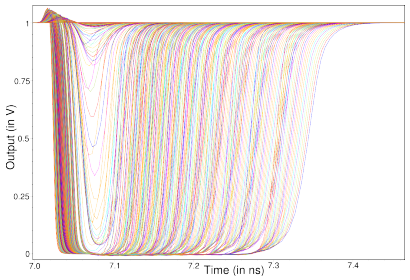
Figure. 3.15 shows those 4 different cases for each of the two hardening mechanisms. In each subfigure the 552 different SET shapes resulting from the different choices of voltage and temperature are overlaid, giving a cumulated view.



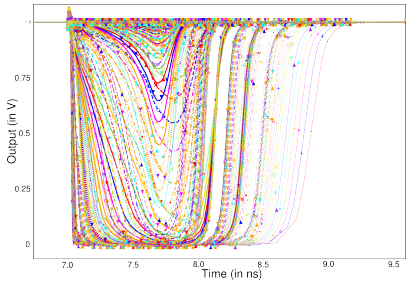
(a) Rad-Hard Sizing (Tr=10ps, Tf=110ps, I=4.5mA)



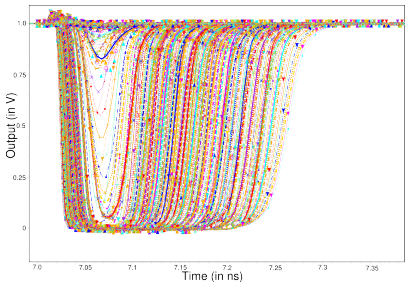
(b) Stack-Separation (Tr=10ps, Tf=110ps, I=4.5mA)



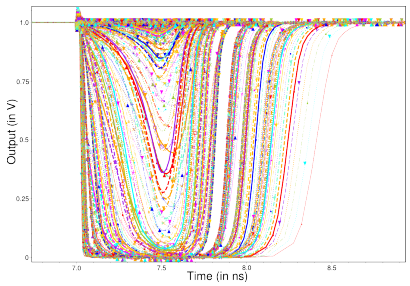
(c) Rad-Hard Sizing (Tr=10ps, Tf=160ps, I=3mA)



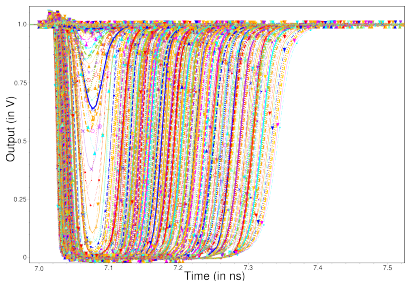
(d) Stack-Separation (Tr=10ps, Tf=160ps, I=3mA)



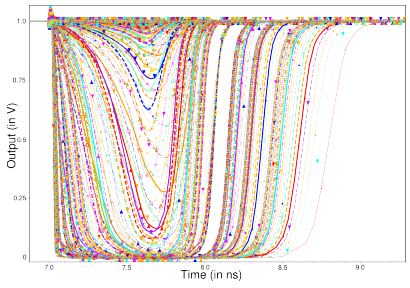
(e) Rad-Hard Sizing (Tr=10ps, Tf=110ps, I=3mA)



(f) Stack-Separation (Tr=10ps, Tf=110ps, I=3mA)



(g) Rad-Hard Sizing (Tr=10ps, Tf=160ps, I=2mA)



(h) Stack-Separation (Tr=10ps, Tf=160ps, I=2mA)

Figure 3.15: Effect of voltage and temperature variations on radiation hardening mechanisms for Q_{crit} 450 fC (a...d), and 300 fC in (e...h)

3.4.3 SET Experiments with VT variations

Before we present and elucidate the outcomes of our simulated particle hits for the mechanisms, we would like to discuss the facts that will remain common to all experiments:

- All the simulation data presented were not observed directly at the output of the device under test (DUT), i.e. the rad-hard inverter, but rather at the output of a (non rad-hard) buffer that is connected to the DUT's output. This buffer not only presents a realistic load to the DUT, it also gives a natural judgment of which SET is large enough to be perceived by a connected load and which not.
- However, a judgment of the SET "severity" at the buffer output must be made. Our solution here is to consider only those SETs problematic that have full swing, which in our case of the regular output being constantly at logic HI, means they must reach down to 0V. For the other SETs we assume they will be electrically masked by a subsequent stage. This is a somewhat deliberate decision, but, as we will see later, since the observed trends are continuous anyway, the particular choice of the threshold does not change the conclusions we make.
- For the full swing SETs we will display histograms showing how their length evolves with temperature and voltage. We measure this length at 800mV.
- For the non-critical SETs it does not make sense to display a length. Therefore we rather show the observed waveforms, such that the reader is free to make an interpretation.

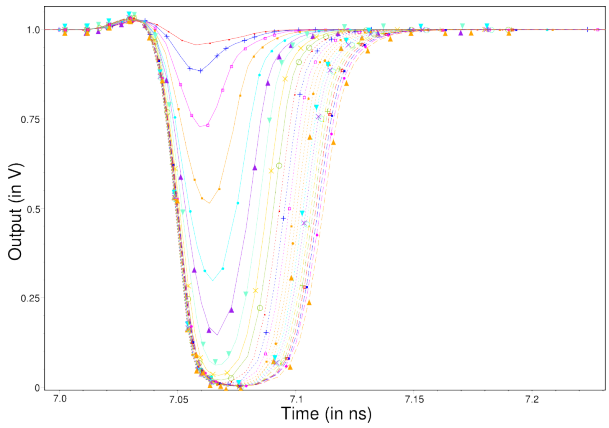
3.4.3.1 Transistor Sizing Mechanism

We will start our presentation of the simulation data for the radiation hardening by sizing with the two scenarios for the 450fC particle strikes, and in a next step present the results for 300fC.

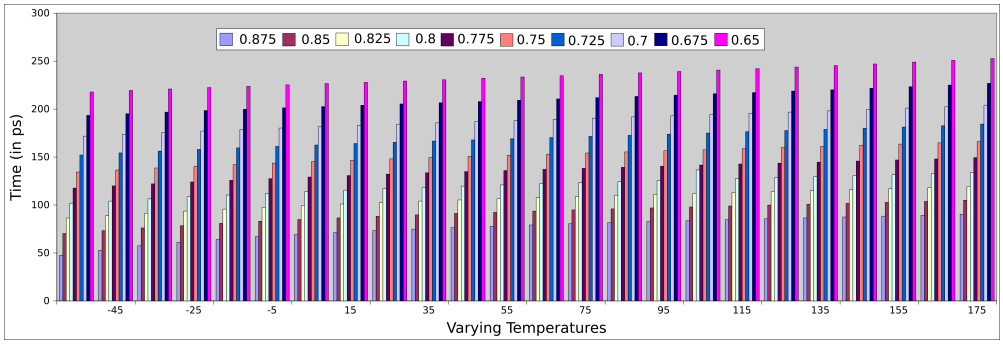
For 450fC

For the particle strike with T_β=10ps, T_α=110ps and I_0=4.5mA we can observe the following behavior under voltage and temperature variation:

- For voltages above nominal (1V) no SET effects were observed.
- When decreasing the supply voltage below 1V, voltage drops become visible (see Figure. 3.16(a)). Those do, however, not reach full swing until the supply voltage is decreased below 900mV (and the worst case temperature of 175°C assumed).
- Going further down from 0.875V to 0.65V we observe SET pulses reaching all the way down to 0V. A bar diagram showing their length over voltage and temperature is given in Figure. 3.16(b).



(a) SET pulse shapes with V_{DD}=0.9V



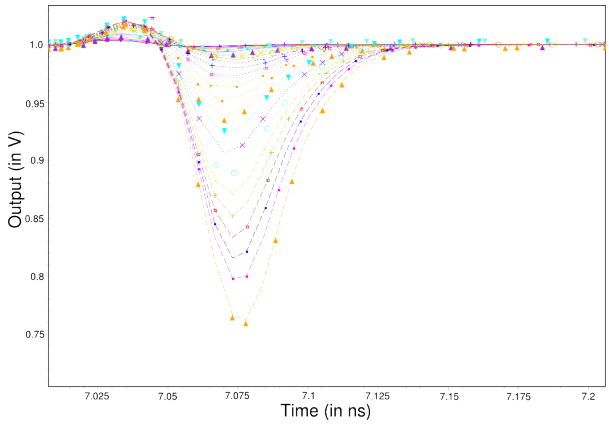
(b) SET length over temperature and V_{DD}

Figure 3.16: Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA

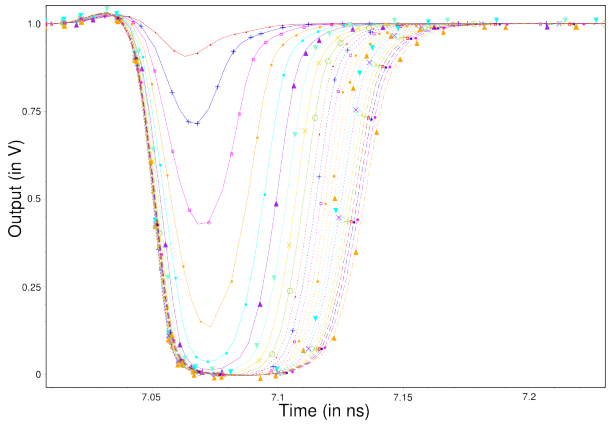
- This diagram shows that the SET length increases monotonically as the supply voltage decreases from 875mV to 650mV.
- We can further observe that SET length increases monotonically with rising temperature. This effect, however, is not very pronounced.
- The maximum length of SET for the rad-hard sizing mechanism is approximately 250ps in the worst case corner of 650mV and 175°C.
- The behavior under voltage and temperature variations is continuous, i.e. the SET pulses gradually reach 0V and then their pulse length exhibits a monotonic and gradual increase.

In the next step we will investigate whether we observe the same pattern for the 450fC particle strike with different fall time (T_β=10ps, T_α=160ps and I_0=3mA). The results are shown in Figure. 3.17. They allow the following observations:

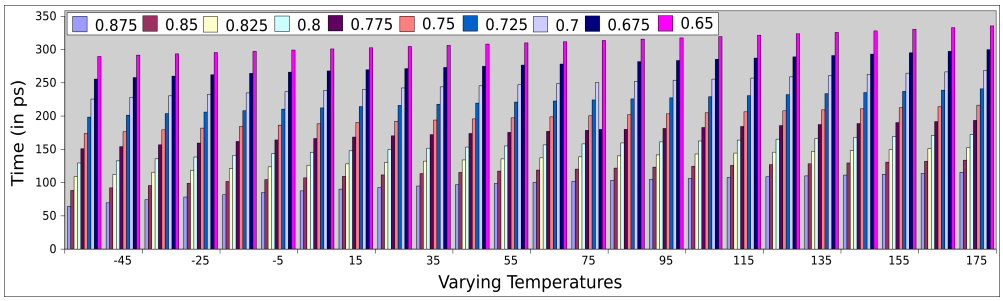
- Similar to the particle strike with T_α = 110ps, there are no visible SET effects for supply voltages above the nominal voltage (1V).



(a) SET pulse shapes with V_{DD}=0.95V



(b) SET pulse shapes with V_{DD}=0.9V



(c) SET length over temperature and V_{DD}

Figure 3.17: Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=450fC, Tr=10ps, Tf=160ps, I=3mA

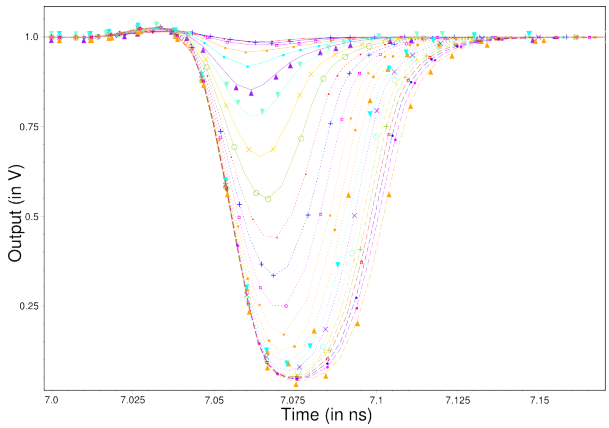
- Like before, spikes not reaching down to 0V can be observed in the supply voltage range from 1V down to 900mV (175°C). More specifically we can see in Figure. 3.17(a) that for 950mV supply voltage not a single spike goes down even below 0.750V (i.e. over the whole temperature range), while, as shown in Figure. 3.17(b), for 900mV supply voltage the spikes nearly touch the 0V mark already.
- Compared to the previous experiment (with T_α = 110ps) the observed SET pulses are generally longer (This is the reason why we did not choose one of the even higher fall times listed in Table 3.3; as it would have caused an even more severe effect, thus distracting from the actual message).
- For the range of V_{DD} = [0.875 ... 0.650]V we again observe SET pulses going down to 0V. Their length over voltage and temperature is shown in the bar diagram in Figure. 3.17(c).
- Like before the SET length monotonically increases with falling supply voltage.
- SETs become longer with rising temperature, but again this dependence is not very pronounced.
- In the worst case corner (650mV and 175°C) we observe an SET of length 330ps.
- Like before the behavior is continuous and monotonic under the applied voltage and temperature variations.

In comparison with the first experiment we can conclude that all trends have stayed the same. The only notable difference is the increased SET length that we observe for a higher fall time of the current pulse.

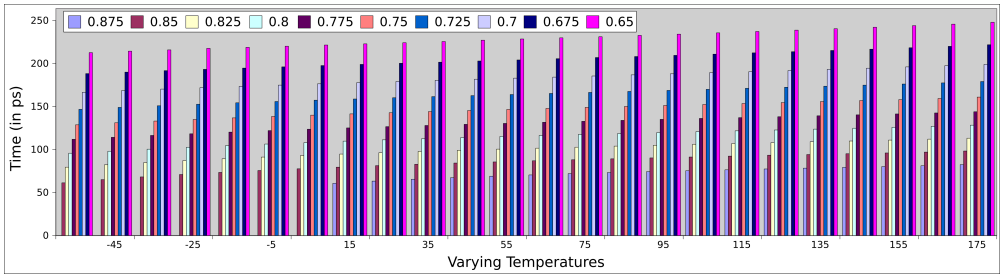
For 300fC
Considering this relatively small impact of the fall time on the experimental results we restrict the investigations with 300fC charge to a single parameter set, namely T_β=10ps, T_α=110ps, I_0=3mA, in the following. The results are summarized in Figure. 3.18. In general they confirm the observations we made for 450fC with the key difference that the observed pulse lengths are somewhat shorter now and do not reach 250ps in the worst case.

3.4.3.2 Stack-Separation Mechanism

Having completed the investigation of the radiation hardening by sizing, we will now turn to the analysis of the stack separation mechanism under voltage and temperature variations. Again we will start with a charge of 450fC and then continue with 300fC.
For 450fC



(a) SET pulse shapes with V_{DD}=0.9V

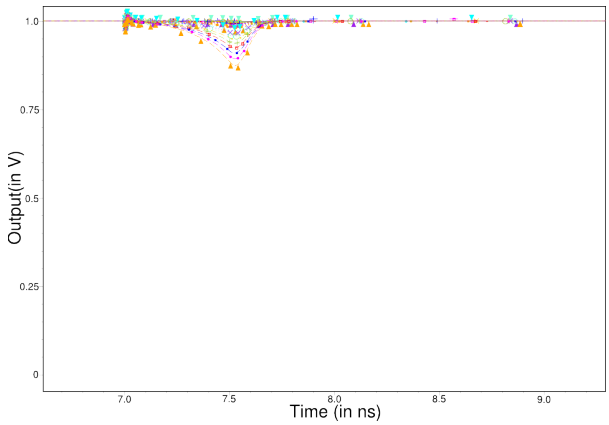


(b) SET length over temperature and V_{DD}

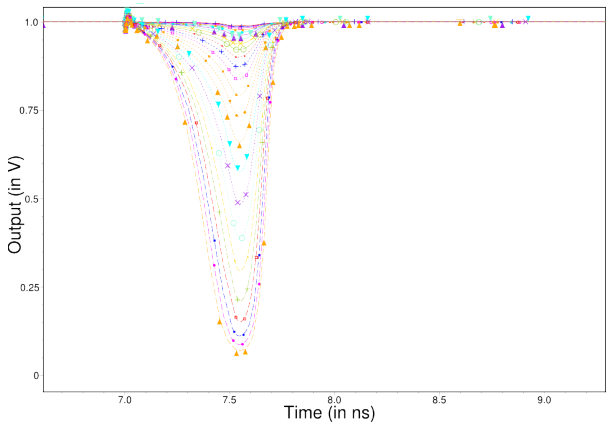
Figure 3.18: Results of voltage and temperature variation experiments for Rad-Hard Sizing with Q=300fC, Tr=10ps, Tf=110ps, I=3mA

For a parameter set of T_β=10ps, T_α=110ps and I_0=4.5mA we observe the following behavior (see Figure. 3.19, 3.20):

- No visible SET effects for V_{DD} above nominal (1V).
- The supply voltage must be reduced down to 750mV to observe full swing SETs, even for the worst case temperature of 175°C. Figs. 3.19(a) and (b) illustrate for the examples of 850mV and 800mV, respectively, that the spikes never go down to 0V for higher V_{DD}. Figure. 3.20(a) shows the borderline case of 750mV. Here the spikes reach down to a few μV.
- In the range from 725mV down to 650mV we observe full SET pulses, whose length is shown in Figure. 3.20(b) over voltage and temperature.
- In this bar graph we observe a monotonic increase of SET pulse length with falling supply voltage.
- The temperature dependence is relatively pronounced now and relies on the supply voltage: For a supply voltage of 0.725V increasing temperature also increases the SET length, while for lower supply voltages (0.65V, 0.675V)



(a) SET pulse shapes with V_{DD}=0.85V



(b) SET pulse shapes with V_{DD}=0.8V

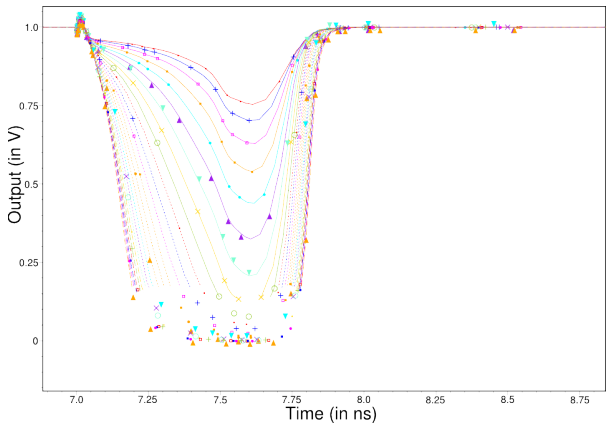
Figure 3.19: Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA

the SET length becomes shorter with rising temperature. The borderline case is near 0.7V where there seems to be no significant dependence of SET length on temperature. Notice that in general the curve becomes flat for high temperatures, while the temperature effect is much higher in the range below approx. 65°C.

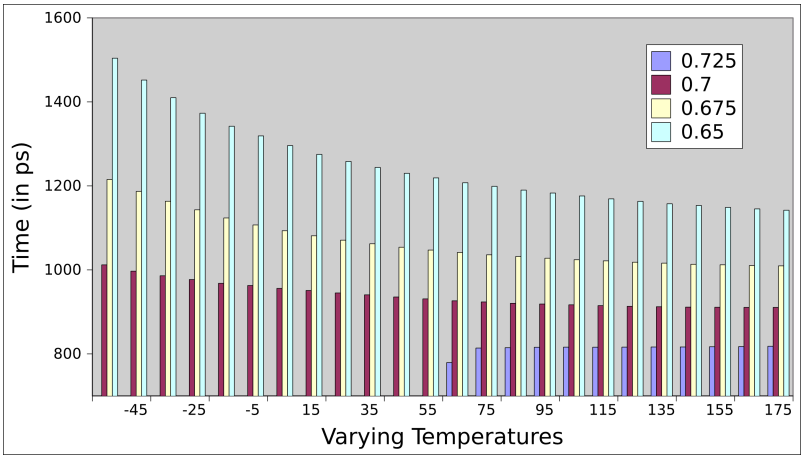
- The temperature influence is so pronounced that with a supply voltage of 725mV the SET spikes do not even reach full swing for temperatures below 65°C, while they do above this value.

- The maximum length of SET for this mechanism turned out to be 1500ps, with the worst case corner being at 650mV and -55°C.

- The behavior of the stack separation mechanism is non-continuous under voltage and temperature variations: Once spikes reach full swing, their length be-



(a) SET pulse shapes with V_{DD}=0.75V



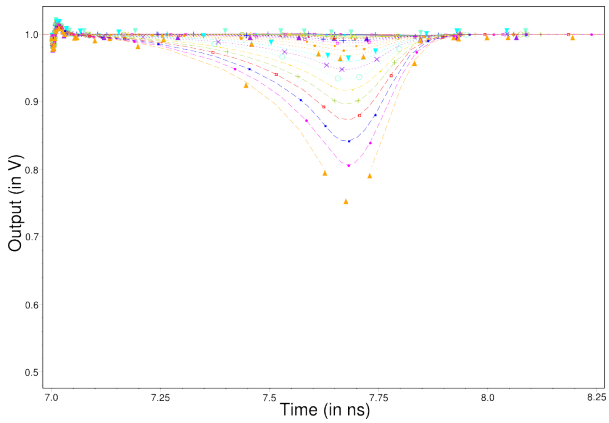
(b) SET length over temperature and V_{DD}

Figure 3.20: Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=110ps, I=4.5mA

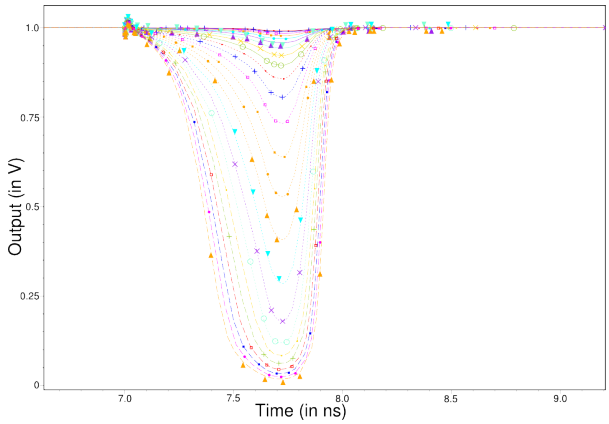
comes considerable; in our case we did not observe pulses shorter than 750ps (observe in Figure. 3.20(b) that the y-scale starts at 700ps rather than 0ps).

Next we will explain the simulation results for the alternative 450fC particle strike, namely with T_{β}=10ps, T_{α}=160ps and I_0=3mA:

- No SET effects observed above the nominal voltage (1V).
- Like in the previous case we observe spikes that do not touch the 0V mark for supply voltages down to 750mV (actually this time we have several full swing SETs at 750mV). Figs. 3.21(a), (b) and Fig. 3.22 (a) show the pulse shapes we obtained over the full temperature range for supply voltages of 850mV, 800mV and 750mV, respectively.



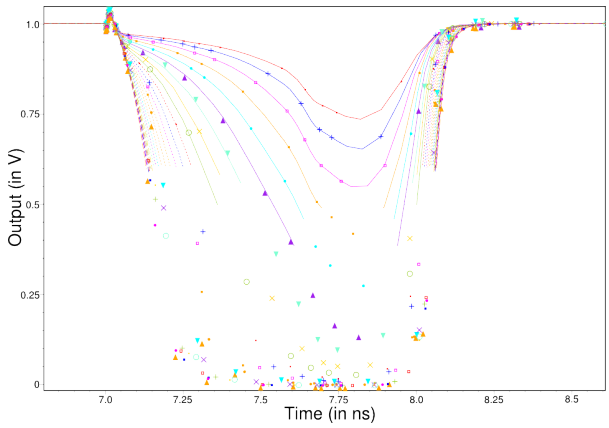
(a) SET pulse shapes with V_{DD}=0.85V



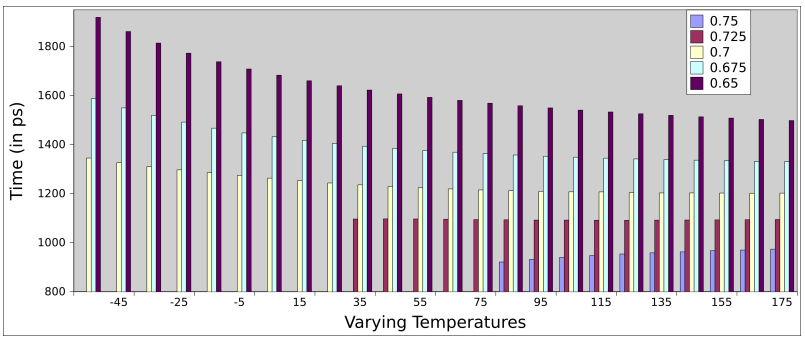
(b) SET pulse shapes with V_{DD}=0.8V

Figure 3.21: Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=160ps, I=3mA

- The bar graph of the SET lengths obtained in the voltage range from 750mV down to 650mV is shown in Figure. 3.22(b). Here we observe an increasing SET length as V_{DD} goes down.
- The temperature dependence is essentially the same as in the previous case: For low supply voltages (0.65V, 0.675V) we observe a decrease of SET length over temperature, while we see a very pronounced increase of SET length for supply voltages of 0.750V and 0.725V. Like before the dependence is stronger for lower temperatures, while the curve flattens towards higher temperatures.
- We observe two cases where temperature is decisive for whether an SET pulse reached full swing: for 750mV temperature must be above 75°C, and for 725mV it must be at least 35°C.
- In general, the observed SETs are longer than those observed in the previous experiment (with shorter fall time) for comparable conditions.



(a) SET pulse shapes with V_{DD}=0.75V



(b) SET length over temperature and V_{DD}

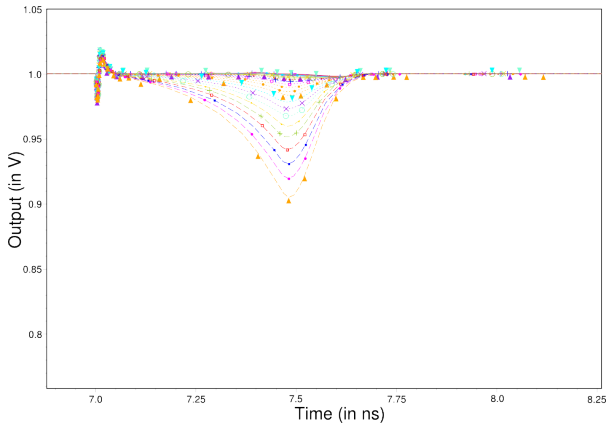
Figure 3.22: Results of voltage and temperature variation experiments for Stack Separation with Q=450fC, Tr=10ps, Tf=160ps, I=3mA

- The maximum length of SET for this mechanism is 1925ps, with the worst case corner at 650mV and -55°C.
- Like before we observe non-continuous behavior: Once the SET pulses reach full swing, their length becomes considerable. There is no gradual transition incorporating short SET pulses.

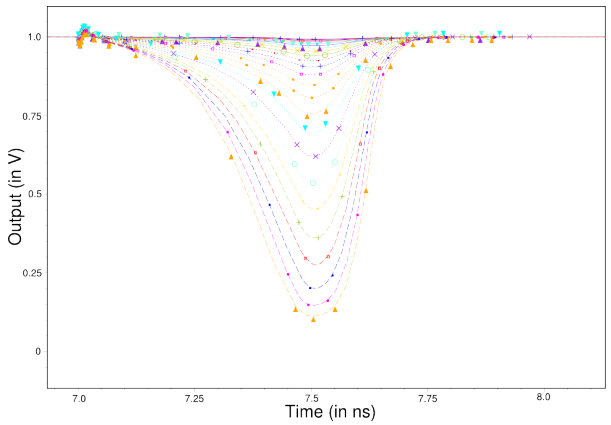
For 300fC

Since, apart from a general increase of pulse length, we did not observe any significant differences for the higher fall time, we will again restrict our analysis for 300fC charge to one parameter set only, namely T_{β}=10ps, T_{α}=110ps, I_0=3mA. The results are shown in Figure. 3.23 and have the following characteristics:

- With supply voltages above nominal no SET effects are observed.
- The SET pulses do not reach full swing for a V_{DD} down to 750mV. Figs. 3.23(a), (b) and Fig. 3.24(a) show the observed waveforms for supply voltages of 850mV, 800mV and 750mV, respectively.



(a) SET pulse shapes with V_{DD}=0.85V



(b) SET pulse shapes with V_{DD}=0.8V

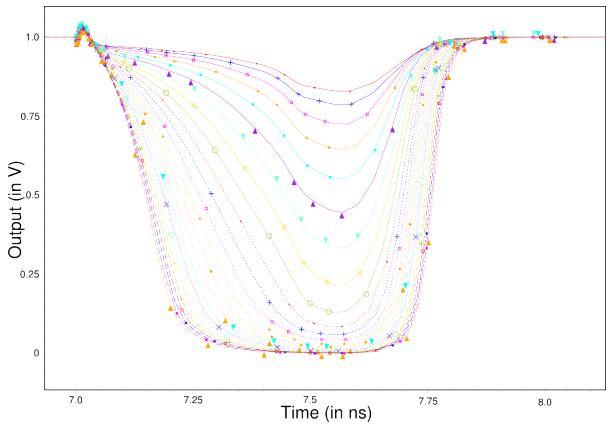
Figure 3.23: Results of voltage and temperature variation experiments for Stack Separation with Q=300fC, Tr=10ps, Tf=110ps, I=3mA

- Starting from 725mV down to 650mV we observe full swing pulses. The bar graph in Figure. 3.24(b) indicates that their length increases as V_{DD} decreases.

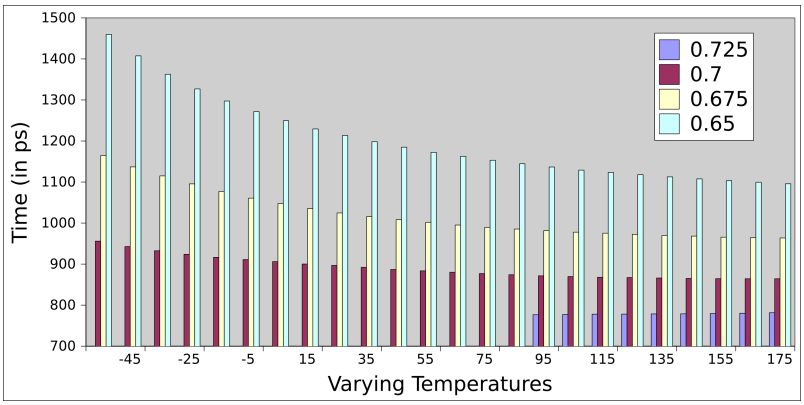
- The temperature dependence is again the same as we observed with the higher charge: For 0.700V the influence of temperature is insignificant, while for lower (higher) voltages pulse length decreases (increases) with rising temperature. This temperature dependence is more pronounced for lower temperatures.

- For a supply voltage of 725mV we observe a borderline temperature of 95°C below which no full swing pulse is observed.

- The maximum length of SET is 1460ps, with the worst case corner at 650mV and -55°C .



(a) SET pulse shapes with V_{DD}=0.75V



(b) SET length over temperature and V_{DD}

Figure 3.24: Results of voltage and temperature variation experiments for Stack Separation with Q=300fC, Tr=10ps, Tf=110ps, I=3mA

- Again the behavior is non-continuous; once we observe a full-swing SET its length is larger than 750ps.

3.4.4 Summary

Our simulation experiments have shown interesting general trends as well as differences between the two mechanisms under investigation:

- There is a dependence of SET susceptibility on voltage and temperature for both investigated mechanisms. For supply voltages above 900mV both mechanisms were reliable. As V_{DD} drops further both of them finally failed at some point.

- In all cases lower supply voltage decreased the performance of the hardening mechanisms. This expected behavior could be observed either by the increasing SET pulse length (under otherwise constant conditions) or, in case

the SET pulses did not reach full swing, by an increasing pulse amplitude. For the rad-hard sizing the pulse length increased approximately by [7.08 ... 9.56]ps per 10mV decrease of the supply voltage (value depending on the charge and fall time). For the stack separation this gradient was nearly 10 times higher, namely [61 ... 77]ps per 10mV.

- As expected, there is a general trend that higher temperature decreases the performance of the hardening mechanisms, which we again observed by longer SETs or higher pulse amplitudes. While this is completely true for the radiation hardening by sizing, our experiments also revealed a counter-intuitive behavior of the stack separation mechanism: For low supply voltage (0.65V, 0.70V) the performance decreases towards lower temperatures. Therefore the worst case corner of this mechanism is at -55°C and 0.65V, and not, as expected and confirmed for the case of the rad-hard sizing at 175°C and 0.65V.
- For rad-hard sizing the pulse length increased by [0.13 ... 0.18]ps per °C, which is relatively insignificant. For stack separation the gradient turned out to depend heavily on temperature. On average we observed a value of [0.911 ... 1.13]ps per °C, respectively, which is again 10 times higher than the former.
- Our experiments with different charges showed that higher charge causes more severe effects (i.e. longer SETs in our measurements). This is as expected. However, it is interesting to observe in Figs. 3.16...3.18 that the fall time has a more significant impact on the SET length than the charge.
- The simulation runs using different pulse parameters for the same charge revealed that the pulse parameters do matter: Longer fall time leads to longer pulses. We can conclude from this that (a) precise modeling of a particle hit in the simulation is important (not only the deposited charge is relevant, for its conversion into a current pulse the impedances that determine the shape need to be carefully considered), and (b) the length of the current pulse is more important than its height (which may serve as a first input for a refined model).
- In general, stack separation exhibited reliable operation over a wider range of conditions: While for rad hard sizing the first full swing pulses were observed at 875mV, stack separation worked reliably down to 750mV.
- Rad hard sizing works relatively robust and predictable: Exceeding the limits will cause small pulses that gradually increase as the violation gets larger. The maximum SET lengths we observed were 330ps (for 450fC) and 248ps (for 300fC).
- The behavior of stack separation under voltage and temperature variations is not so linear: Once the mechanism's limits are exhausted, it will fail miserably, i.e. instantly cause an SET with significant length. The shortest observed SET length was 750ps, which is much higher than the longest one observed for the rad hard sizing. It ranged up to 1.95ns.

- In order to cover the worst case corner with the rad hard sizing mechanism, the sizing must be increased to 108 for 450fC (or 72 for 300fC). This is more than another 3 times increase compared to the sizing for nominal voltage and room temperature. Compared to the original (unprotected) circuit this is a huge increase, so it really pays to strictly cut down the range of operating conditions to the minimum.

- In contrast, there is no such up-scaling possible for the stack separation method.

Overall the stack separation mechanism turned out to be much more cost efficient: It proved to operate reliably down to 750mV with the original sizing. In some experiments we did in another context (Sec. 3.3.2.4), we found out that it can handle charges up to 950fC. So as long as one can guarantee to remain within these operational conditions, it is certainly the better choice. However, there is no easy way of enhancing this mechanism for higher charges or a wider range of voltages and temperature. As soon as these limits are exceeded it tends to fail instantly, producing pulses of significant length. Also, its temperature behavior becomes quite non-regular for lower supply voltages.

The rad hard sizing is certainly more expensive, but it can be scaled for a wider range of conditions. Moreover, it fails gradually, producing short pulses whose length continuously increases with the severity of the violation. However, in order to cover the worst case corner of $V_{DD} = 650mV$ and T=175°C, it requires a sizing of 108, which is about 36 times the area of the stack separation method. This significant overhead might be invested in providing a more stable environment for the latter, instead.

We can conclude from our analysis that for radiation environment where we could have extreme voltages and temperatures; employing radiation hardening by sizing mechanism is futile, whereas usage of separation mechanism is fruitful. Therefore, we propose to use the separation mechanism to radiation harden the combinational gates.

3.5 Sequential Circuits

The two core sequential elements for our radiation target ASIC infrastructure are the Linear Feedback Shift Register (LFSR) and the Parallel In Serial Out (PISO) shift register. Both the LFSR and the PISO are based on a chain of registers. The LFSRs are mainly used as counters for counting normal transitions and SETs. All these data recorded by the counters is extremely important and has to be protected, as corrupted data would lead us to false interpretations. In order to avoid corruption of the data we would have to radiation harden the LFSR counter.

The PISOs are mainly used in the ASIC to reduce the number of output pins and use a smaller package. They are basically used to serially transfer the counter values to the host computer. The data transferred by the PISO needs to be protected as any data corrupted during transmission to the host computer would record an incorrect

SET hit, which would lead to incorrect ramifications. Hence, we need to protect the data within the PISO.

3.5.1 Background

3.5.1.1 Linear Feedback Shift Register

An LFSR is a synchronous shift register with XOR or XNOR gates forming selected feedbacks [42], which produces a deterministic and periodic pseudo-random counting sequence. It is heavily used in practice for generating CRC checksums and pseudo-random bit strings. Compared to conventional binary counters [6], an LFSR reduces the amount of required logic and minimizes routing complexity. This is beneficial for us, as it makes the counter cheaper and less prone to particle impacts. The disadvantage is that the count sequence is not the normal binary increment sequence, but as the sequence is deterministic, conversion is straightforward. As will become clear below, this will even work for our advantage.

An LFSR with n flip-flops can implement a $2^n - 1$ state counter [42, 5]. The choice of the polynomial used should ensure $2^n - 1$ states, with no repeated states; such a polynomial is known as 'primitive', or maximal-length polynomial [5]. Good design practice demands a reset that provides start-up in a known condition. In our case a low at the RST input resets the count value to 0. Two circuit structures can be used to implement a given polynomial, namely, the many-to-one design and the one-to-many design. We chose a one-to-many design based on XNOR gates, since the associated count sequence involves many bit changes per step, which is beneficial for our purpose (This choice will be substantiated later in Sec. 4.3.3).

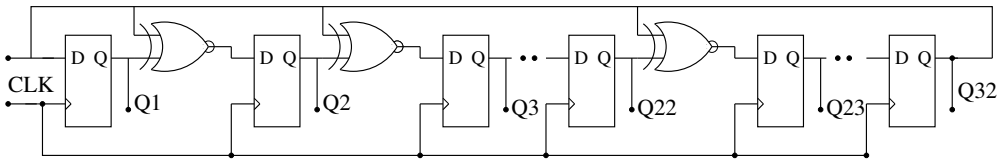


Figure 3.25: 32-bit LFSR

The block diagram of the 32-bit LFSR is shown in Figure. 3.25. The reason behind the necessity of a 32-bit LFSR will be substantiated in Sec. 4.2. The 32-degree polynomial we use for our design is $x^{32} + x^{22} + x^2 + x + 1$. With each rising clock edge the 32-bit LFSR will step to the next state, thus cycling through a sequence of about 4.2 billion different values. The LFSR counter was built using D flip-flops (employing transmission gates) with asynchronous reset and XNOR gates. We built the transistor level schematic of the LFSR counter in UMC $90nm$ technology in Cadence. The (W/L) sizing of the NMOS transistor we used for building the XNOR, the inverters and the transmission gates is (250nm/80nm).

In order to examine its native susceptibility to particle hits we injected SETs into each of the XNOR gates and flip-flops of the LFSR counter independently. We used the setup presented in Sec. 2.4 to generate sufficiently strong current pulses in the

LFSR, i.e., digitally visible, SETs. Overall, we observed that the initial difference created by the SETs in the LFSR counter, when compared to the faultless scenario, is very small (which is not unexpected since we injected a single SET), but after the next clock transition the impact created by this small difference is witnessed as billions of skipped transitions (refer Sec. 4.3.3 for detailed information). Due to our careful selection of the LFSR polynomial and its one-to-many implementation, we can indeed generalize this observation: A single bit flip in any LFSR cell will always exhibit a much larger and hence easily detectable effect in the actual count sequence [42], which finally justifies our decision to use an LFSR counter.

3.5.1.2 Parallel-In Serial-Out

A PISO converts data from a parallel format to serial format. By parallel format we mean that the data bits are present simultaneously on individual wires, one for each data bit as shown in Figure 3.26. By serial format we mean that the data bits are presented sequentially in time on a signal wire as in the case of 'Z'. The logic diagram shown in Figure 3.26 illustrates the principle at the example of a 4-bit PISO.

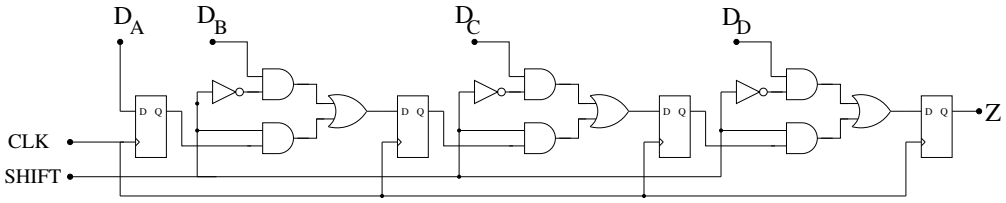


Figure 3.26: 4-bit Parallel-in, Serial-out Shift Register

It comprises three stages that can be replicated for the number of parallel inputs required ($n - 1$ stages for an n bit PISO). D_A, D_B, D_C and D_D are the parallel inputs, where D_A is the most significant bit and D_D is the least significant bit. One stage of the PISO consists of a D flip-flop for storage and a multiplexer (AND-OR structure) that allows switching between two modes of operation under the control of the signal SHIFT. In *load* mode (SHIFT = low) data from the parallel inputs $D_A...D_D$ will be captured with the rising edge of CLK. In *shift* mode the bits of this data word will be shifted out serially at the output Z (MSB first) with every rising edge of CLK.

In our ASIC we use a 84-bit PISO, built with the same technology as the one presented above. The parallel inputs are connected to diverse counters and LFSRs inside the chip, while the control signals CLK and SHIFT as well as the output are connected to pins. Since in a useful operation the parallel load precedes the shift mode, a dedicated reset is not required. Like with the LFSR we have again performed fault injection by means of HSPICE simulations to identify the weak points of the unprotected circuit.

We found out that half of the SETs injected in the flip-flops were masked and the remaining SETs propagated successfully to the output of the flip-flop. The overall effects of particle strike in the PISO are listed below:

- PISO is dormant or inactive:
  - The "CLK" signal is inactive, hence any SET within the flip-flop will not be converted to SEU and would disappear.
  - Any SET in the control logic could trigger the PISO to sample data. Even though it samples the data, the data will be available only for the period when the SET is active. Furthermore, the "CLK" signal is inactive, hence data would not be sampled. Hence, all the SETs triggered in the control logic has no effect in the PISO
- PISO is active:
  - We observed that when the "CLK" signal is active then some of the SETs in the FF will be converted into an SEU and shifted out. Hence, the flip-flops must be protected against SETs during read-out
  - We also observed that the control logic of the PISO is extremely sensitive to SETs, as it could change the PISOs operation to sampling data instead of shifting. This could make the control logic feed wrong data to one of the flip-flops in the PISO.

We concluded from these observations that the most sensitive part of the PISO is the control logic and then the flip-flops. We must provide a proper tolerance to the PISO in order to avoid incorrect data transferred out of the ASIC.

3.5.2 Proposed Rad-hard Mechanisms

Protecting the LFSRs, the PISO, and any other sequential logic in general is becoming a relevant problem not only for safety applications alone, but may also apply to future commercial circuits; as the newer technology nodes are growing increasingly susceptible to radiation effects. In this section we will explore different methods for attaining radiation tolerance on the system, and the circuit level. The PISO is comprised of registers and some combinational elements just like the LFSR, so we can essentially use the same mechanisms used for the LFSR for its protection. However, as outlined above, the most crucial part of the PISO is the control architecture, whose protection is therefore vital. This puts a different focus on the selection than in the LFSR case.

In principle we can distinguish four different robustness levels for our counter and PISO:

Level a Detection of one or more errors in the counter: This prevents us from using erroneous results; we can safely discard them, but they are lost.

Level b Mitigation of a single SET: A single SET at a time will not upset the count, so we can still use the result. Further SETs occurring after the previous ones have been mitigated, can also be handled.

Level c Mitigation of multiple SETs at different points: Multiple SETs occurring at different components (whose scope needs to be specified later) at the same time do not corrupt the count.

Level d Mitigation of multiple SETs without restrictions: Multiple SETs occurring at the same time, even on the same component, do not corrupt the count. The probability of this kind of a multiple upset is, however, very low.

3.5.2.1 Radiation Hardening by Sizing for the LFSR

To obtain the required sizing we injected SETs into all sub-circuits (flip-flops, XOR gates) and gradually increased their sizing until they were able to withstand the simulated particle hits. As a result, we had to increase the (W/L) sizes by 10 for the flip-flop and by 14 for the XNOR gate. As this larger sizing globally increases all critical charges, an LFSR with these radiation hardened components can withstand both single and multiple upsets of 450fC without limitations on temporal or spatial coincidence (level (d)).

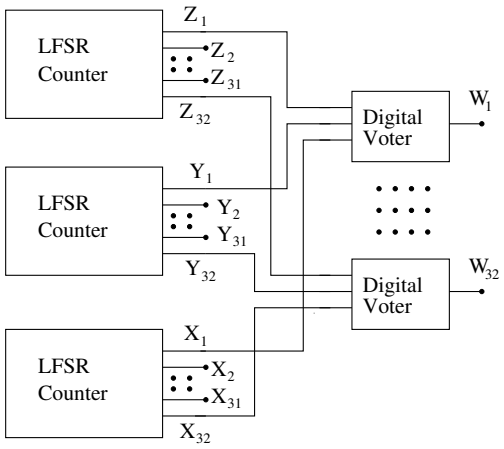


Figure 3.27: Schematics of TMR LFSR Counter

3.5.2.2 Hardware Redundancy for the LFSR

We compared two different approaches for the LFSR using TMR. As a first approach we use three LFSRs as shown in Figure. 3.27 and employ a voting on their outputs when we read them out. We do not triplicate the voter, as we need a single output. The total overhead caused by this approach to a normal LFSR is the two extra LFSRs plus 32 digital voters, one per output bit. The digital voter circuit used for the TMR is shown in Figure. 3.28. The characteristic properties of this approach are:

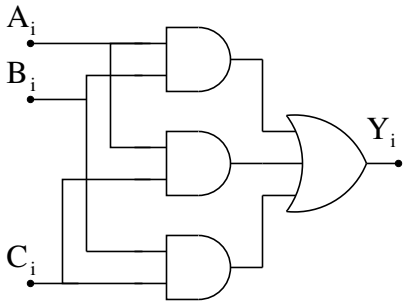


Figure 3.28: Schematics of the Digital Voter

- All single and even all multiple faults will be mitigated, as long as they only affect one single instance of the LFSR (level (c)). However, the voting will fail even for single errors in two or more instances of the LFSR.

- All (single and multiple) transient faults in the voter are mitigated, as long as they are not effective during the (relatively short) readout interval (we assume a stateless implementation of the voter). In the latter case, however, there is the risk of reading an erroneous result.

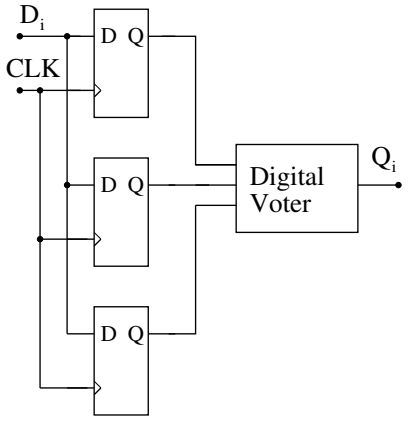


Figure 3.29: Schematics of TMR Flip-Flops

As a second approach we use the voted flip-flop states not only for readout but also for the shifting during the normal operation of the LFSR. In other words, we replaced all flip-flops of the LFSR with a "TMR set" comprised of three flip-flops and a voter circuit as shown in Figure. 3.29. In addition, we replaced all XNOR gates of the counter with three XNORs and a voter circuit as shown in Figure. 3.30. The total overhead caused by this approach to a normal LFSR counter is two extra LFSR counters and 35 digital voters (the 32 from before plus 3 extra for the XNORs).

This yields the following characteristic properties:

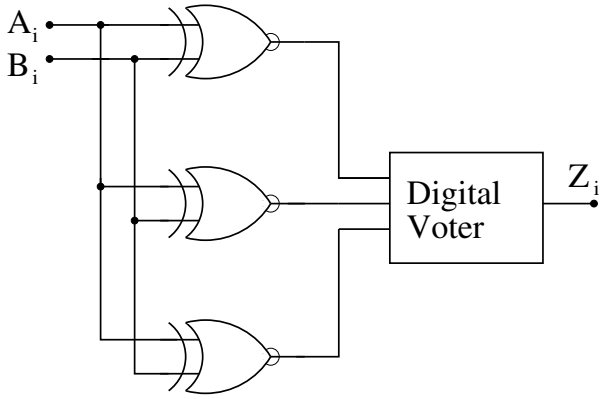


Figure 3.30: Schematics of TMR XNOR Gate

- All single and multiple transient faults in the flip-flops and XNOR gates can be mitigated, as long as they do not affect more than one TMR set within the same clock cycle (level (c)).
- Any transient fault in the voter will make the counter generate a faulty value.

In the second architecture the voter could as well be triplicated, as its outputs feed a triplicated structure (XOR, flip-flop) anyway. However, one of the three voter outputs would still need to be selected as the LFSR output, and a fault in this very voter would still invalidate the result. Therefore we preferred to apply the approach from Section 3.5.2.1 and sized the (W/L) ratio of the digital voter as required.

By using a radiation hardened voter we can provide radiation tolerance for the LFSR up to the desired extent in both architectures. At this point the second architecture becomes preferable: Recall that while the residual risk is a multiple SET within one TMR set within one clock cycle in both cases, the TMR set is considerably smaller in the second approach (granularity of register vs. granularity of whole LFSR).

3.5.2.3 Time Redundancy for the LFSR

Time redundancy is based on performing the same operation multiple times and comparing the results. Albeit being very efficient, this principle implies that repeating an operation always leads to the same result. Unfortunately this is not true for the LFSR: Due to its pronounced stateful behavior, repeating a counting step or sequence obviously yields different results, so a comparison does not make sense.

3.5.2.4 Radiation Tolerance by Separation for the LFSR

The radiation-tolerant CMOS standard cell library proposed by Garg et al. [52] can be used to provide protection to the LFSR. We require three standard cells (i.e, inverter, NAND and NOR gate) to realize a flip-flop and an XNOR gate. The NAND and the inverter standard cells (refer Fig. 3.12) are available in the literature [52].

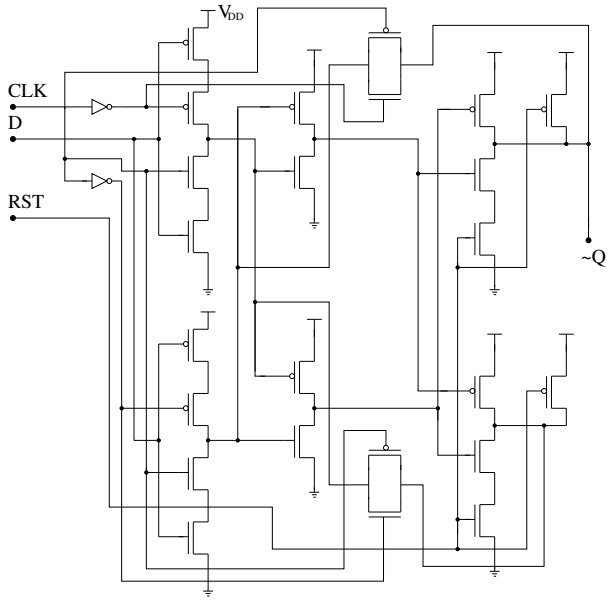


Figure 3.31: Transistor level Schematics of DICE Latch

Based on the same principle we built a NOR gate (refer to Fig. 3.12). Unlike the rest of the architectures studied so far, an LFSR architecture built from these primitives proved to be able to tolerate particle hits of 950fC even with the original (W/L) sizing. The only multiple upsets it cannot tolerate are those affecting both an NMOS and a PMOS of the same sub-circuit at the same time. The radiation tolerant XNOR gate requires 56 transistors and the flip-flop requires 134 transistors. Unfortunately, the routing complexity of the circuits built according to this principle is very high.

3.5.2.5 Radiation Tolerance using DICE for the LFSR

Transient faults in the flip-flops of the LFSR counter can be mitigated using *Dual Interlocked Storage Cell* (DICE) elements proposed by Calin et al. [29]. According to our requirement we modified the original DICE flip-flop architecture by adding a clock and a reset, similar to [108]. However, we didn't have to use *delay filtering* in the inputs of the flip-flops, as all the components of the counter will be radiation-hardened and thus supply correct inputs.

The custom DICE latch constructed for our LFSR counter utilizing the control signals "CLK" and "RST" is shown in Figure. 3.31(a). Since the DICE flip-flop did not tolerate the injected SETs with the original sizing, we had to increase the W/L. By means of our simulated SET injections we found the following values: inverters, guard gate and transmission gate 2x; NAND gate driving the output of the latch 4x. A radiation hardened LFSR counter constructed with DICE elements will use 32 DICE flip-flops and three XNOR gates. For hardening the XNOR gates we sized them to withstand a particle hit of charge 450fC. As an alternative we also applied the approach proposed by Garg, et al., [52].

3.5.2.6 Hardening by Sizing for the PISO

We can provide radiation tolerance by sizing the flip-flops as already explained in Section. 3.5.2.1. Concerning the combinational logic we transformed the logic function shown in Figure. 3.26 into a more efficient equivalent form built from NAND gates only (see Figure. 3.32). The (W/L) size of those had to be increased by 14 until they were able to withstand the particle hits in our Spice simulations.

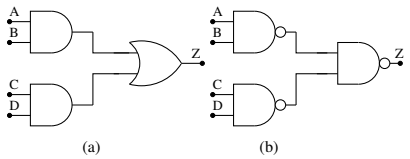


Figure 3.32: Control Logic of the PISO

3.5.2.7 Radiation Tolerance by Separation for the PISO

Since our PISO implementation comprises the same logic elements as the LFSR, namely flip-flops and NAND gates, we can use the same circuits as shown in Section. 3.5.2.4.

3.5.2.8 Radiation Tolerance using DICE for the PISO

Radiation tolerance can also be achieved by using the DICE approach for the flip-flops as outlined in Section. 3.5.2.5 but without reset. For the control logic we can use hardening by sizing (refer Section. 3.5.2.6) or stack separation (refer Section. 3.5.2.7).

3.5.2.9 Time Redundancy for the PISO

One operation cycle of the PISO involves capturing a value from the LFSR and shifting it out serially over a pin. While the PISO is still a fundamentally sequential element and the re-execution of a single step within its operation cycle does not yield the same result (recall the discussion from Section. 3.5.2.3), the re-execution of the whole operation cycle does so, provided the LFSR value did not change. As a consequence of this insight, we can establish time redundancy for our PISO by simply performing two complete read cycles and comparing the results. In case of mismatch we can execute a third read cycle and perform voting. This does not incur any area or speed penalty; the price is simply a prolongation of the transmission interval.

3.5.3 Summary

Table 3.5 and Table 3.6 give an overview of the different ways of providing radiation tolerance for both the LFSR counter and the PISO that we have discussed in the two

Table 3.5: Comparison of Different Radiation-Tolerance Mechanisms

Components	No. of Trans.	(W/L) Sizing	Area Equiv.	Radiation Tolerance Level
LFSR Counter				
Flip-Flops	25	1	824	a
XNOR	8	1		
Counter	824	1		
LFSR Counter using TMR (Approach A)				
Flip-Flops	25	1	8232	a, b
XNOR	8	1		
Voter	30	6		
Counter	3432	M		
		M:multi-sizing		
LFSR Counter using TMR (Approach B)				
Flip-Flops	25	1	8772	a, b
XNOR	8	1		
Voter	30	30		
Counter	3522	M		
Radiation-Hardening by sizing for LFSR counter				
Flip-Flops	25	10	8336	a, b, c, d
XNOR	8	14		
Counter	824	M		
Radiation-Hardening on circuit level for LFSR counter				
Flip-Flops	134	1	4468	a, b, c
XNOR	60	1		
Counter	4468	1		
LFSR counter w DICE FFs and sized XNOR				
DICE Flip-Flops	62	M	4816	a, b, c
XNOR	8	14		
Counter	2008	M		
LFSR counter w DICE FFs and circuit level XNOR				
DICE Flip-Flops	62	M	4660	a, b, c
XNOR	60	1		
Counter	2164	M		

Table 3.6: Comparison of Different Fault-Tolerant Mechanisms

Components	No. of Trans.	(W/L) Sizing	Area Equiv.	Radiation Tolerance Level
8-bit PISO				
Flip-Flops	18	1	262	a
NAND	4	1		
PISO	262	1		
8-bit PISO: Hardening by sizing				
Flip-Flops	18	10	3020	a,b,c,d
NAND	4	14		
PISO	262	M		
8-bit PISO: Stack separation				
Flip-Flops	80	1	970	a,b,c
NAND	10	1		
PISO	970	1		
8-bit PISO: DICE FFs and sized combinational logic				
Flip-Flops	54	M	2372	a,b,c
NAND	4	14		
PISO	586	M		
8-bit PISO: DICE FFs and stack separated combinational logic				
Flip-Flops	54	M	1222	a,b,c
NAND	10	1		
PISO	736	M		
8-bit PISO: Time Redundancy				
Flip-Flops	18	1	262	a,b,c,d
NAND	4	1		
PISO	262	1		

previous sections. Here we not only consider the attained level of radiation tolerance, but also an area equivalent computed from the number of transistors weighted with their respective (W/L) sizing. In order to also have some rough indication on the wiring complexity, we use the (unweighted) number of transistors as a measure here.

Overall we can see that the TMR is the least efficient approach for the LFSR counter as it consumes much area while providing relatively little radiation tolerance. The stack separation mechanism appears to be more efficient for both, LFSR and PISO, but it uses a large number of transistors, which transforms into a very high routing complexity. Recalling, however, that it can withstand charges up to 950fC, it may be the best option, if protection against higher charges is required, which is not the case here. Radiation hardening by sizing seems to be the safest solution in both the cases, but consumes very much area. In the case of our LFSR counter we are rather willing to accept the risk of having to discard results in the extremely rare cases of coincident particle hits, so we favor the solution based on the DICE flip-flops – after all it only consumes half the area compared to (W/L) sizing alone. While making this definite decision for the counter, we leave the final choice among the two variants (stack separation and hardening by sizing) concerning the XNOR gate for the layout analysis as both of them have the same area equivalent.

In the case of the PISO we prefer to use either DICE with stack separated combinational logic or time redundancy mechanism. We chose these two safe solutions in consideration of the fact that the PISO forms the important bridge between our chip and the outside world. However, should it turn out after the layout that we are short of die area with our design, we still have the option to go for time redundancy and accept the increase in transmission time. This will be decided in Chapter. 7.

CHAPTER 4

Sensitivity and Spatial Distribution of SETs

Our goal is to understand the sensitivity of digital logic gates to SETs. Exposing the logic gates to radiation would provide us the information, but it is quite expensive and at the same time impractical to build ASICs just to understand the SET sensitivity[1]. Sensitivity to SETs can be quantified by the minimum charge required to flip the polarity of the gate. Each and every logic gate has its own structure and therefore none of the logic gates have the same parasitic resistance and capacitance. The critical charge varies from one gate to another, therefore, the minimum charge required to create an upset in each and every gate is not the same. We can exploit the SET sensitivity concept to also analyze the spatial distribution and thereby estimate the soft error rate.

To be more precise the most sensitive gate would be the inverter, as the parasitic capacitance and resistance load would be the least compared to other logic gates. But, an inverter with a higher drive strength ("16") will have more parasitic load than a NAND or a NOR gate with a drive strength of "1"[2]. It is hard to classify the most sensitive gate when we take higher drive strengths into consideration, hence to keep it simple as a first step we deal with logic gates with same drive strength ("1").

The challenges in choosing the target architectures to understand SET sensitivity are listed as follows:

1. Maintain the same drive strength for all the logic gates

    a) It is important to study the dependence of SET sensitivity for different drive strengths, but, in order to accurately estimate the soft error rate of the FRad Chip it is important to use gates of same drive strength

[1] Monitoring the SET behavior by connecting the inputs and outputs of the logic gates directly to the IO pads of the ASIC, will only accomodate less number of targets in the ASIC.

[2] Note that as the drive strength varies the parasitic capacitive load associated with the gate also varies.

   b) As a part of future work we will build more ASICs to understand the dependence of SET sensitivity with varying drive strengths

2. Classify which gates are susceptible to SETs for a particle strike in a particular energy spectrum

   a) We must categorize the energy spectrum in terms of critical charge

   b) The amount of energy must be increased in steps of 10fC (will be helpful in classifying the sensitivity of the gates within a resolution of 10fC).

3. We need to choose efficient target architectures that are elementary and/or frequently used in practice.

   a) We should be able to explore the behavior of the target both in dynamic and static mode; i.e., we need the option of exercising/stimulating the targets

   b) To be more realistic (w.r.t loading), the targets should note be just standard logic gates, but also structures that are frequently used in the semiconductor industry

The target circuits we chose are listed below:

- Inverter
  - Inverter Chain
- NAND-NOR Logic
  - NAND gate
  - NOR gate
  - NAND-NOR tree
- Sequential circuits
  - Flip-Flop
  - Flip-Flop Chain
- Asynchronous circuits
  - Muller C-element
  - Muller Pipeline
- XOR gate
  - XNOR tree

All these architectures receive a dynamic stimuli at the inputs with a frequency of 100MHz. Note, that the measurement architecture used should be able to differentiate the events caused by SETs and normal stimuli. To measure the SET events we need to build a special architecture. Moreover these events must be precisely recorded. Note that the measurement architecture need not have to indicate which transistor got hit in the target, but it must be able to notify which target got hit. The measurement architecture can be radiation hardened or non radiation hardened, but it should be able to deliver useful data about the target circuits. Hence, it should either be immune to particle strikes or isolate the radiation behavior within itself. Using radiation hardened architectures would consume too much die area, hence, usage of non radiation hardened architectures is favored if possible to have more information about SETs.

4.1 Target Architecture

4.1.1 Inverter

Inverters are the most basic and simple elements in CMOS and thus the preferred radiation targets in the existing literature. Incorporating inverters in our study is not only relevant in practice, but also allows us to compare our results to literature. For a given transistor sizing, they are also the fastest CMOS circuits, thus potentially vulnerable to even very short SETs. The structure of the inverter with an input A and output Z is shown in Fig. 4.1. The output Z of inverter is LOW if the input A of the inverter is HIGH, and viceversa. The truth table of the inverter is shown in Table. 4.1.

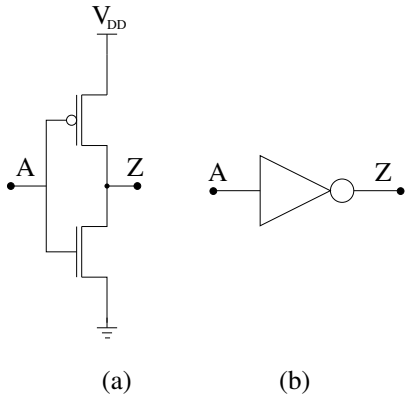


Figure 4.1: (a) Transistor Level Schematic of Inverter, (b) Symbol of Inverter

4.1.1.1 Inverter Chain

In order to have a reasonably large target area and a rich testbed for investigating propagation effects, we provide a chain of 17 inverters, as shown in Fig. 4.2 (in fact,

Table 4.1: Truth Table of Inverter

A	Z
0	1
1	0

multiple instances thereof).

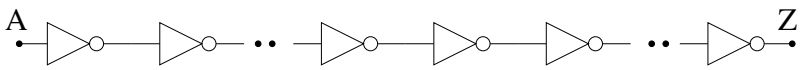


Figure 4.2: Logic Diagram of Inverter Chain

We chose the inverter chain as the target to check if the SETs injected in the first inverter propagates all the way to the output. This could help us study masking effects in detail. We can also analyze what amount of energy or charge should the particle strike generate in order to make a visible SET in the output of the chain. To do so, we injected SETs in the output nodes of each and every inverter. From the SET analysis we found out that the minimum charge required to create an upset in the output of first inverter got masked before it reached the output of the target. It was therefore necessary to inject an SET with a sufficiently large charge in the first inverter to ensure that the SET propagated all the way to the output. In essence this target could help us understand the propagation effects of the inverter chain.

4.1.2 NAND-NOR Logic

4.1.2.1 NAND gate

The NAND gate otherwise known as a negative-AND gate is a logic gate which produces an output that is false only if all its inputs are true. The structure of a NAND gate with two inputs A,B and output Z is shown in Fig. 4.3. A LOW in the output Z of the NAND gate is possible only if both the inputs A and B of the NAND gate are HIGH. If either of the inputs are LOW or both the inputs are LOW then the output will remain HIGH. The truth table of the NAND gate is shown in Table. 4.2.

Table 4.2: Truth Table of NAND gate

A	B	Z
0	0	1
0	1	1
1	0	1
1	1	0

We injected SETs in the output node of the NAND gate to analyse the effects of particle strikes in the PMOS and NMOS of the NAND gate. From the analysis we

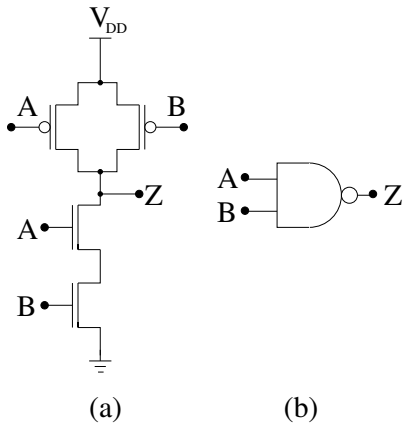


Figure 4.3: (a) Transistor Level Schematic of NAND, (b) Symbol of NAND gate

observed that the PMOS is immune to SETs in the first three states mentioned in the Table 4.2 and we could only create an upset in the NAND gate by injecting SETs in the NMOS. Similarly, we observed the viceversa for the last state presented in Table 4.2.

4.1.2.2 NOR gate

The NOR gate is a logic gate which produces an output that is true only if all its inputs are false. The structure of a NOR gate with two inputs A,B and output Z is shown in Fig. 4.4. A HIGH in the output Z of the NOR gate is possible only if both the inputs A and B of the NOR gate are LOW. If either of the inputs are HIGH or both the inputs are HIGH then the output will remain LOW. The truth table of the NOR gate is shown in Table. 4.3.

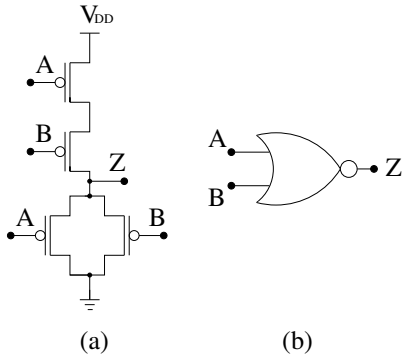


Figure 4.4: (a) Transistor Level Schematic of NOR, (b) Symbol of NOR gate

We injected SETs in all the nodes of the NOR gates to analyse the effects when exposed to radiation. SET analysis revealed that the PMOS is immune to SETs for the first logic state presented in the Table 4.3 and we could steer an upset in the NOR

gate by injecting an SET in the NMOS. For all the remaining states we observed the viceversa, i.e., the NMOS is immune to SETs and the PMOS is vulnerable.

Table 4.3: Truth Table of NOR gate

A	B	Z
0	0	1
0	1	0
1	0	0
1	1	0

4.1.2.3 NAND NOR Tree

NAND trees have always been a topic of interest in terms of testing and SETs. NAND and NOR implementations are slightly more complex than inverters and therefore exhibit different phenomena. One is the availability of two inputs, which allows us to form a tree structure. Another one is the possibility of logical masking of errors.

We have 64 NAND gates in the first stage that are all driven by a single input signal, which allows us to jointly stimulate activity with minimal overhead. The outputs of the NAND gates fan-in as inputs for NOR gates and so on, yielding a tree with 127 gates in total, see Fig. 4.5. The tree has 7 levels, hence in the fault-free case the output will be the inverse of the input.

Note that if the 64 NAND gates are driven by separate inputs then in total we will need 128 input signals. It is impractical to use 128 pins in the FRad Chip for just one target, therefore, we decided to drive all the signals of the tree with one input signal.

We injected SETs in all the nodes of the tree. From the analysis we observed the following:

- Of all the SETs injected in the first stage of the tree only the stronger SETs propagate to the output of the tree, while the weaker SETs are masked.
- The SETs injected in the NMOS of the NAND gates in the first stage of the tree did not propagate and were masked. The SET in the output of the NAND gate will flip from “HI” to “LO”. The NOR gate receives one input as “LO” (SET) and the other as “HI”. Hence, the SET will be masked.
- The SETs injected in the PMOS of the NAND gates in the first stage of the tree propagated all the way to the output of the tree. The SET in the output of NAND gate will flip from “LO” to “HI”. The NOR gate will receive one input as “LO” and the other as “HI” (SET). Hence, the SET propagates to the NOR in the second stage and then so on to the output of the tree.
- Similarly, such scenarios were observed for the gates in all the stages, except for the last stage of the tree.

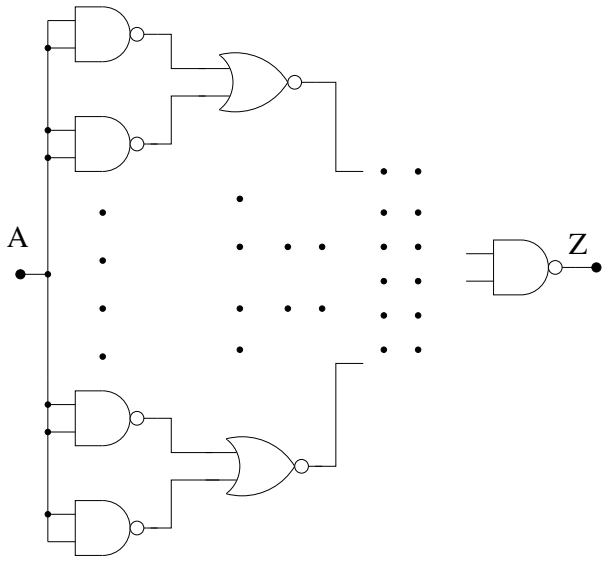


Figure 4.5: Logic Diagram of NAND/NOR Tree

This tree could help us understand the propagation of SETs within NAND and NOR gates. As we have both the elementary gates and the tree as targets, we could compare and classify which energy level of SETs would propagate and which would not. When we expose it to radiation using a micro-beam we know which gate we are targeting, therefore, we have no need to monitor all the nodes.

In order to locate the exact gate with upset when exposed to radiation in a reactor, we need to monitor all the nodes of the target. If we monitor each and every node then the measurement architecture will consume a lot more die area. As a consequence we decided to just measure the SET sensitivity of the tree.

4.1.3 Sequential Circuits

4.1.3.1 Flip-Flop

Flip-flops are the fundamental building blocks of virtually every synchronous design. We chose the flip-flop as our target to understand effects of particle strike on basic sequential circuit and storage elements. Flip-flops are edge-triggered meaning the output changes only on a single type of clock edge. Of the different flip-flops in the literature, we chose the D-type flip-flop also known as data or delay flip-flop, for our purpose. The transistor level schematic and the truth table of the D-flip-flop as shown in Fig. 4.6 and Table. 4.4. The flip-flop basically captures the value of the data input (D) at the rising edge of the clock input (CLK). The captured value is the output Q. The previous value of the output is restored, when the data input (D) changes while the clock edge is not rising. The flip-flop can be interpreted as memory cell.

We injected SETs in all the nodes of the flip-flop to understand the effects when exposed to radiation. The analysis revealed that some of the SETs injected were

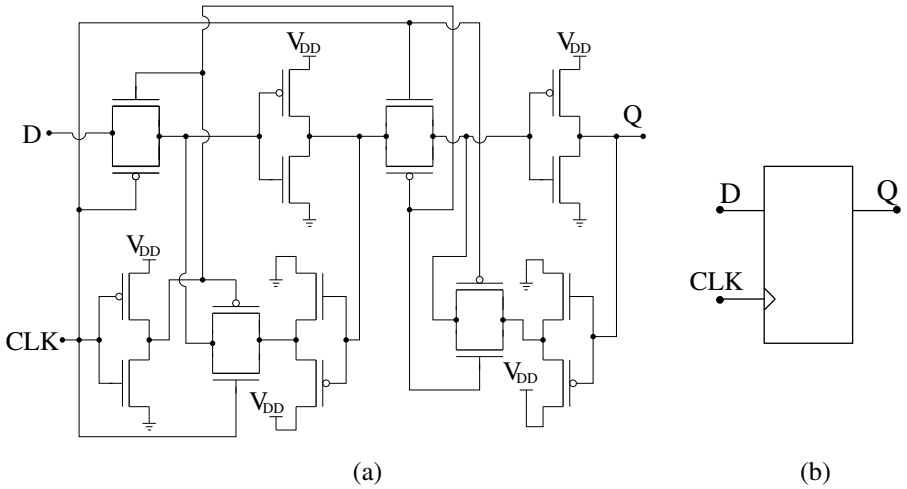


Figure 4.6: (a)Transistor Level Schematic of D-Flip-Flop, (b) Symbol of D-Flip-Flop

masked, and some had some transient effects, while some of them changed to SEU. We observed that the relevance of the particle strike in the flip-flop also depends on the state of the flip-flop. If we trigger the SET during the rising edge of the CLK input, the SET would be converted to an SEU.

Table 4.4: Truth Table of D-Flip-Flop

CLK	D	Q
Rising Edge	0	0
Rising Edge	1	1
Non-rising	X	Q_{prev}

4.1.3.2 Flip-Flop Chain

Like inverters, they have received much attention in radiation-related research in the past, which allows us to compare our results against existing data. This type of architecture is used as a design for testing technique referred as scan chain. As shown in Fig. 4.7, we provide a chain of 33 edge-triggered master-slave D-flip-flops, which are implemented using transmission gates and inverters. Note that all the flip-flop outputs are reset to "0" when the ASIC is reset. When there is a transition in the input of the first flip-flop in the chain, then the data output is transmitted to the next flip-flop, and so on. The measurement architecture will observe 32 "0"s for the first 32 clock cycles and in the 33rd clock cycle it will receive the first data bit from the target.

Similar to the other targets we injected SETs in all the nodes of the chain. From the analysis we observed the following:

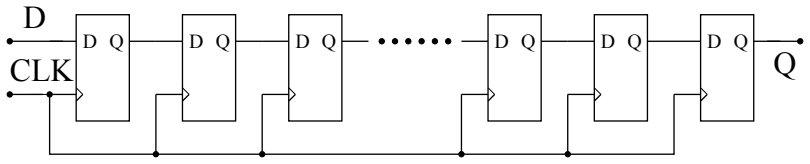


Figure 4.7: Logic Diagram of Flip-Flop Chain

- Once the SET is latched and converted to SEU, this SET propagates to the next flip-flop and so on.
- The probability of a particle strike hitting two different flip-flops at two different positions such that the SEU is masked, before if reaches the output of the chain, is extremely low.
- Location of the position of the SEUs in the flip-flops for some particle strikes could be detected after post-processing the data. It is not detected for all the SEUs, this is because we know the transitions in the Flip-flop and the count sequence in the measurement architecture. But, to accurately recover the location of the SEU we need an infrastructure that records data in different flip-flops.

Taking all these observed analysis into consideration we decided to come up with a monitoring architecture that can count all the SEUs occurring in the target, but not the location of the SEU.

4.1.4 Asynchronous Circuits

4.1.4.1 Muller C-element

The Muller C-element (the three transistor level implementations) is explained in great detail in Sec. 2.3.1. We proposed to use it as a target to understand the effect of SETs in asynchronous circuits. The SET analysis for the Muller C-element is presented in Sec. 2.3. We use all the three implementations as targets, as each one of them has different number of nodes, structure and parasitic load. Note that when the inputs of the C-element differ the previous output is restored and this property makes the SET analysis complicated. We observed the following behavior from the analysis:

- The injected SET flipped the C-elements' state (C-element experienced an SEU), i.e. its output Z immediately and had a lasting impact until a new pattern is applied (changing the inputs)
- The SET injected does not have an immediate effect on the output Z, but when applying the next set of patterns, the output makes an unexpected, lasting change. A particular behavior coined as "SEU*". For further details refer [147].

4.1.4.2 Muller Pipeline

An elastic pipeline is built from Muller C-elements (refer Sec. 2.3.1 for background) and inverters as shown in Fig. 4.8. Three different elastic pipeline implementations will be used as target circuits:

1. Elastic pipeline based on Van Berkel C-element
2. Elastic pipeline based on the C-element using an inverter latch
3. Elastic pipeline based on the Conventional pull-up pull-down C-element

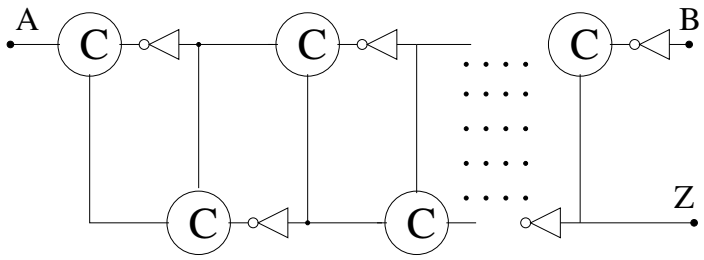


Figure 4.8: Logic Diagram of Muller Pipeline

The elastic pipeline in Fig. 4.8 is essentially a FIFO buffer for signal transitions that is often used in handshake-based circuits. The C-elements in the pipeline propagate the signals in a carefully controlled way that maintains the integrity of each wave [132, 135]. The speed of signal propagation is determined by the actual delays of the circuit.

The Muller pipeline works as follows: The first transition supplied by the left-hand environment via input A will eventually reach the output Z at the right-hand environment. If the right-hand environment does not respond via input B to the pending transition, the pipeline will eventually fill up. Note that the pipeline could also provide an acknowledgment output to the left-hand environment for indicating a full pipeline; the source should stop generating transitions at input A in this case. Since pipeline read and write operations are well-coordinated in our case, we can omit this additional output.

The most interesting property of the circuit is that it is delay-insensitive, i.e., it works correctly regardless of wire and gate delays. Since many asynchronous designs are based on elastic pipelines, its behavior in the presence of radiation effects (SET generation, propagation and latching) is of utmost relevance. Beyond being an attractive target the elastic pipelines are also useful as measurement counters.

We injected SETs in all the nodes of the pipeline, of which some of the SETs were masked. The SETs triggered were dependent on the state of the C-element. Example: Consider a C-element (C1) driving another C-element (C2), meaning the output of C1 is input to C2. Assume the two inputs of C2 are "1" changing the output of C2 to "1". Triggering an SET in C1's output changing the level from "1" to "0", would not have any effect on the output of C2, hence, the SET is masked.

Our SET analysis revealed that the manifestation of particle strike in the pipeline depends primarily on the state of the C-elements in the pipeline [137].

4.1.5 XOR gate

XOR gate implements an exclusive OR for the input transitions. It is frequently used for parity computation, binary addition, and subtraction in digital logic. The transistor level schematic of the transmission gate based XOR gate with two inputs A, B and output Z, along with the symbol is shown in Fig. 4.9. A HIGH in the output Z of the XOR gate is possible only if one of the inputs is LOW. If both the inputs of the gate are LOW or HIGH, then the output will remain LOW. The truth table of the XOR gate is presented in Table. 4.5.

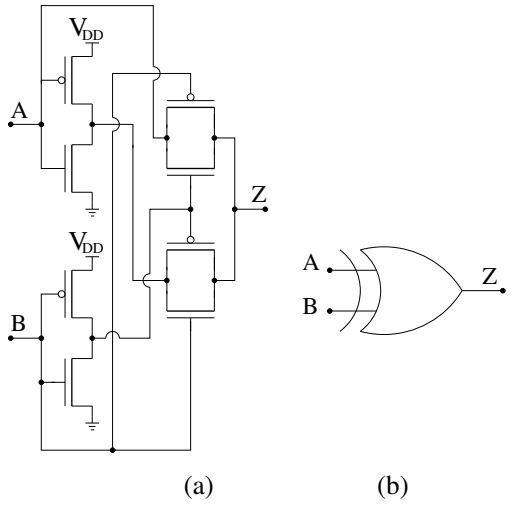


Figure 4.9: (a) Transmission gate based XOR, (b) Symbol of XOR gate

We injected SETs in all the nodes of the XOR gate. Note that we could not inject SETs specifically in the transmission logic, we could only inject it in the nodes to create an upset in the gate. From the SET analysis we observed that the NMOS is immune while in the first and last states presented in the Table 4.5 and to create an upset in the XOR gate we could only inject SETs in the PMOS. Similarly, we observed the vice versa for the second and third states of the Table 4.5.

Table 4.5: Truth Table of XOR gate

A	B	Z
0	0	0
0	1	1
1	0	1
1	1	0

4.1.5.1 XNOR Tree

The XNOR gate forms the equivalent of the logical OR for transitions, another very basic functionality in asynchronous circuits and also fundamental for parity checking circuits. Compared to NAND/NOR gates, it has a very different internal structure. We employ an XNOR gate implementation based on a CMOS transmission gate (shown in Fig. 4.9) with inverter.

Similar to the NAND/NOR tree it uses a 7 level tree structure, starting with 64 gates in the first level and 32 gates in the next level and so on 1 gate in the last level. The tree is constructed with 127 gates in total. It is apparent from Fig. 4.10 that two outputs of XNOR gates fan-in to an XNOR gate at the next level. Having 128 different inputs for all the 64 XOR gates would be impractical, therefore, we connected the inputs of the 64 XNOR gates in the first stage to a single input. Due to the XNOR function all gates will therefore, independently from this input, present a logic 1 at their outputs, and the tree output will transiently go to low only in case of an SET somewhere in the tree. As we will see, this behavior is very convenient for our purposes.

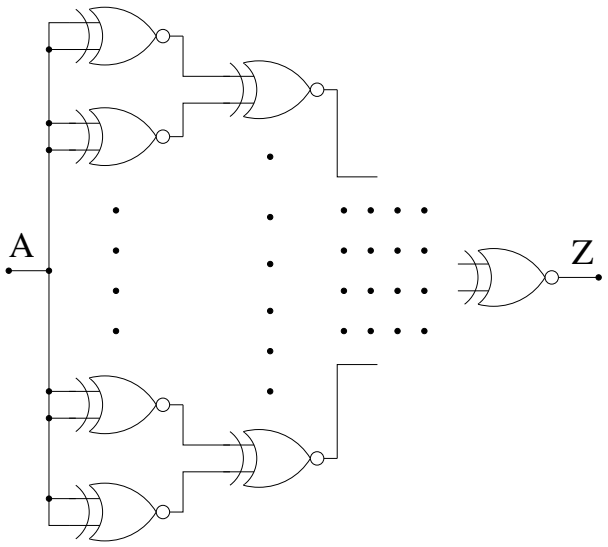


Figure 4.10: Logic Diagram of XNOR Tree

We injected SETs in the tree to check if the SET injected in the first level of the tree propagates all the way to the output. The SET analysis revealed the following:

- The XNOR tree is immune to all the SETs in the PMOS
- SET in the NMOS of the XNOR gate in the first stage flips the output data of the XNOR gate to “LO”. In the second stage the XNOR gate receives two inputs “LO” (SET) and “HI” and the delivers an output “LO” and so on. The output of the XNOR tree delivers an output “LO”.

- SET injected with the minimum charge required to flip the output of the XNOR gate in the first stage of the tree does not propagate all the way to the output of the tree, instead, the pulse faded before it reached the output.
- Precise location of the SET will not be possible to detect unless we monitor all the nodes of the tree. We are interested in the sensitivity of the SETs, therefore, will only monitor the output node of the tree.
- The XNOR tree will not report any transitions in the output unless there is a particle strike in any of the gates of the tree.

4.1.6 Summary

Overall from the above analysis we can conclude the following:

- Each and every circuit has a unique behavior and therefore, a measurement architecture that suits the need of the target would be needed.
- Total number of inputs needed for the target circuits are listed below:
  - Combinational gates require two inputs
  - Flip-flops (chain) require three inputs (data, clock, and reset)
  - Muller pipeline, Inverter chain, tree structures require only one input
- From the SET analysis in the NAND, NOR and XOR we can observe that:
  - When one input is low and the other is high: NMOS is vulnerable in the NAND and XOR gate, while PMOS is vulnerable in the NOR gate.
  - When both the inputs are low: NMOS is vulnerable in the NAND and NOR gate, while PMOS is vulnerable in the XOR.
  - When both the inputs are high: PMOS is vulnerable in the NAND, XOR and NOR gate.
- The behavior of the flip-flop and C-element are unique

It is quite complex to build measurement architecture specific to the behavior of each and every circuit. Furthermore, using separate input pins to steer data in the combinational circuit occupies input pads that could be used for outputs.

Just like we shorted the inputs of the tree structure we decided to short the inputs of the NAND, NOR, XOR, and C-element. Furthermore we decided to steer a single input to all our target circuits except the sequential circuits. For the sequential circuits we will feed that input as the data signal.

The effect of shorting the inputs in the targets are listed below:

- Both the NAND and NOR gates acts as a inverter. In other words inverter with different parasitic loads.

- XOR gates' outputs remains low at all times.
- Muller C-element acts as a buffer. When the inputs differ the C-element restores its previous stored state in the output. That property is lost when we shorted the inputs

With this alteration to the targets we can quantify that the behavior of the circuits has been modified (i.e., the targets will either act as an inverter or a buffer) to suit our needs but the circuit structure is still intact. Therefore, the need not build separate measurement architectures for each and every target is nullified. We can use a common measurement architecture for all the targets except the XOR and XNOR tree. We can build a very simple architecture for the XOR and the XNOR tree, as the outputs will be constant unless there is a particle strike in the same.

4.2 Measurement Architecture – Semi-Static Mode

The measurement architecture must facilitate the continuous monitoring and recording of all occurring SETs, at the level of digital signals, in statistical long-term experiments. To get as much information as possible from a radiation experiment, as many nodes in our target circuits (also called as DUT) as possible must be monitored simultaneously. As the pool of target circuits is quite large (discussed in Sec. 4.1), we need to choose an appropriate measurement architecture such that all the target and measurement architecture fit in one ASIC, ideally there will be multiple instances of each. Please note that our goal is to make sure the ASIC is core limited and not pad limited, i.e., we would like to use all the die area of the ASIC to get as much SET data as possible. Note, that the number of monitored nodes is limited by the available die area and the number of pins, therefore our measurement architecture should be robust and efficient,

We have 11 targets just to analyze the sensitivity of the SETs and will have more targets to analyze the other SEEs. Therefore, having one separate input per target is a luxury we cannot afford, so we decided to have only one input pin driving all the data inputs of the targets involved in analyzing the SET sensitivity. Note, that the flip-flops would still need the "CLK" input other than the data input. Moreover, the modifications we made to the targets to reduce its complexity worked to our advantage in here.

Besides the target circuits we should also make sure that the number of output pins of the monitoring architecture is within the limit. Taking that into consideration we chose to build the measurement architecture with digital counters. The quality of the measurements provided by the counters would not be the same as with analog amplifiers [68], but the data provided by the counters would be sufficient to analyze the sensitivity of the targets.

We want to investigate SET generation in our DUTs both in static and in dynamic mode. For the latter, we provide a common data signal that can be used to collectively stimulate switching activity. Recall that the XNOR tree has the beneficial property of exhibiting activity at its output only in case of a particle strike.

Therefore, it is sufficient to use a simple incrementer for counting SETs here. Unfortunately, not all our other DUTs exhibit this nice behavior. Since the generation of the stimuli is under our control, however, we can easily provide a correct reference signal for comparison/subtraction purposes.

Considering that we are not interested in the exact *temporal* matching of the behaviors of DUT and reference, but rather in matching their signal traces, a more appropriate solution is an up/down counter, with the DUT output feeding one input and the reference signal feeding the other one. Obviously, we cannot use a synchronous up/down counter, since SETs would not adhere to setup/hold constraints and hence cause metastability. Moreover, in order to catch even short SETs, our counters should be as fast and sensitive as possible. Fortunately, there is a nice and area efficient way of building an asynchronous up/down counter for transitions that is based on an elastic pipeline.

Alternatively, we may use an incrementer as well to count the transitions performed by the DUT during a measurement period. However, in this case, we will see the sum of transitions due to the SETs in the DUT plus those due to the regular DUT switching activity. As the stimuli applied to the DUT are under our full control, we can subtract the latter a posteriori; the incrementer must accommodate a much larger count value, though.

Being on-chip, the measurement circuitry will be exposed to radiation just like the DUTs and hence has to operate properly in the presence of particle hits. Recall that the FRad Chip is not primarily designed for being used under micro-beam irradiation, but rather with any radiation source. Instead of resorting to the radiation hardening mechanisms presented in Chapter 3[3], we decided not to protect the counters. Considering that both proposed types of counters resemble interesting target structures by themselves (namely, a flip-flop chain as well as an elastic pipeline), we decided *not* to mask particle hits in these circuits but rather to let them occur: This effectively turns the on-chip measurement infrastructure into an additional radiation target.

Keeping these requirements as the base criteria, we constructed a set of measurement architectures for the DUTs to record the SETs.

4.2.1 Architecture A

The generation of stimuli in the DUT is under our control, so, we can easily provide a correct reference signal for comparison. This can be accomplished by using a simple wire (instead of a wire we can also use a buffer), since all the DUTs except the XNOR tree exhibit a behavior equivalent to that of a wire. Any mismatch between the DUT and the reference signal can be extracted by an XOR gate, whose output is fed to the SET measurement counter as shown in Fig. 4.11. The only pitfall here is that the XOR tends to produce glitches in case of a non-zero skew between DUT and reference, thus leading to potentially spurious counts.

[3] All of those mechanisms cause high overheads, thus rendering a pretty large share of the die area unusable for additional DUTs

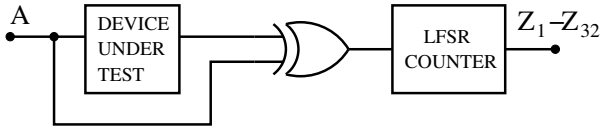


Figure 4.11: Measurement Architecture A

4.2.2 Architecture B

We tried to improve architecture A by adding another DUT instead of a reference signal to avoid a non-zero skew, as shown in Fig. 4.12. This architecture is better than the previous one. It still produces some glitches in the XOR gate. Unfortunately, to make sure that this architecture works we need to do an exact temporal matching of the DUTs. It is nearly impossible to make sure that both the DUTs produce signals such that there are no glitches seen in the XOR gate. Hence, we decided not to pursue this architecture.

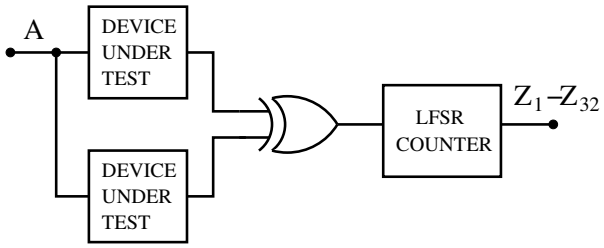


Figure 4.12: Measurement Architecture B

4.2.3 Architecture C

While analyzing architecture B we realized that we are more interested in matching the signal traces than the temporal matching and hence decided to use two counters and eliminate the XOR gate as shown in Fig. 4.13. Our counter should be able to detect even the shortest SETs, thus it should be fast and sensitive. We chose to employ the asynchronous up/down counter in here (refer Sec. 4.1.4.2). The only problem with this architecture is that, if any of the counters gets hit then we cannot be sure whether the targets or the counters got hit by the particle strike. Therefore, we cannot recover from a single fault in the up/down counters; unless they are radiation hardened. If we radiation harden the counters we can reasonably be sure if there was an SET in the target. The only problem would be that we cannot recover from the DUTs each getting hit by particles once (as the counters are reset in such a scenario).

4.2.3.1 Up/Down Counter

The construction of the up/down counters is similar to the Muller pipeline [138], which has been explained in Sec. 4.1.4.2. We could build the up/down counters

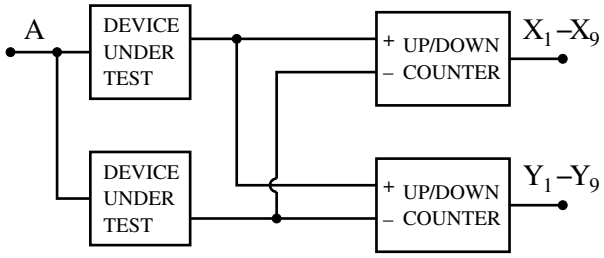


Figure 4.13: Measurement Architecture C

using one of the three implementations of the C-element presented in Sec. 2.3.1. After a careful analysis we chose to implement our SET up/down counters as a 9-stage pipeline made up of Van-Berkel Muller C-elements [138]. Note that our counter should be able to count both up and down. To enable the capability of counting down we preset the pipeline to a value of 5 upon reset. In order to fulfill this, we need to add extra transistors (with appropriate sizing) to the C-elements as shown in Fig. 4.14 (a) and (b).

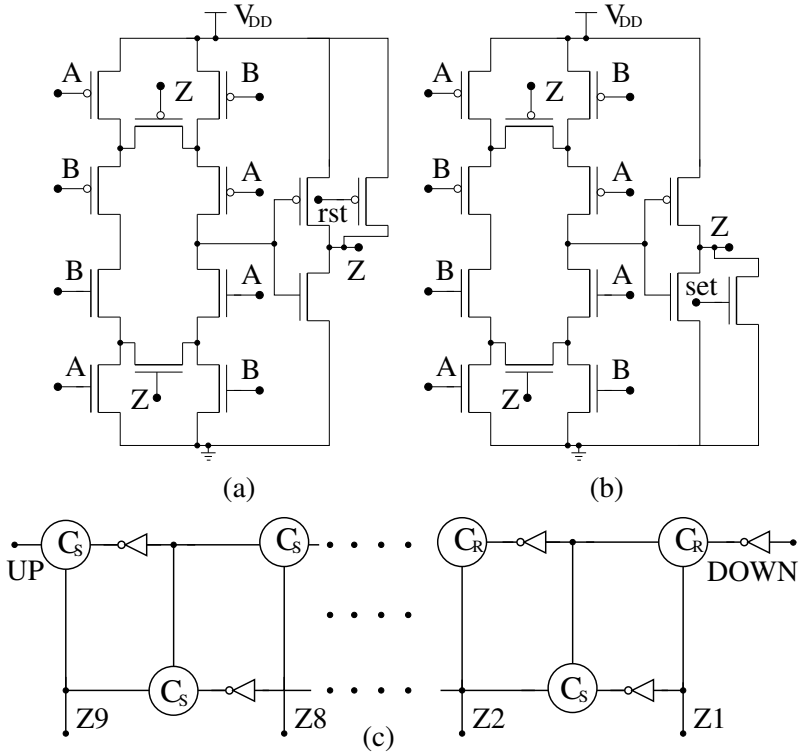


Figure 4.14: Schematic of (a) Muller C-element with Reset (rst), (b) Muller C-element with Set (set) and (c) Up/Down Counter

The up/down counter utilizing the two versions of the C-elements (with "set" and "rst") and inverters is shown in Fig. 4.14 (c). The outputs $Z_1 - Z_5$ are preset

to 1, while $Z_6 - Z_9$ are preset to 0; all bottom-row C-elements are initialized to 0. A transition on *UP* will add to the transitions already present in the pipeline, while a transition at *DOWN* will remove one transition from the pipe, thus decreasing the count.

4.2.4 Architecture D

We extended architecture C as shown in Fig. 4.15. Note that now we employ three targets and three up/down counters. Some of the features of the architecture are:

- The targets are connected such that any SET in one of the targets could be easily detected as long as the counters are not hit.
- Any two SETs in the targets such that one SET in one of the targets and the second SET in the other, can also be easily detected as long as the counters are not hit. Note, that if any of the counters get hit then all the data is lost.
  - To avoid such a scenario we radiation harden the counters.
- If all the three targets get hit exactly once then we would have no information of particle strikes in the targets.

To make sure this architecture delivers SET data we could radiation harden one of the targets, at the cost of reducing the target to measurement area ratio.

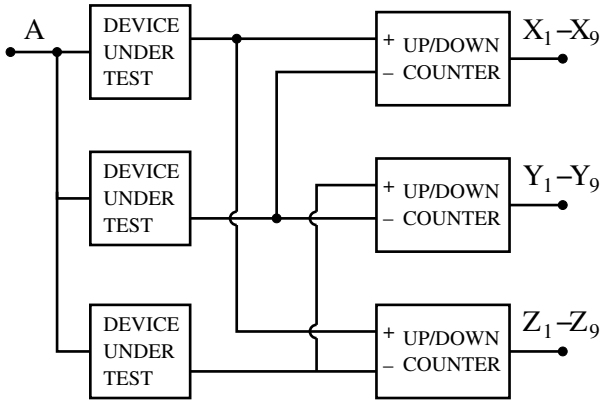


Figure 4.15: Measurement Architecture D

4.2.5 Architecture E

All the architectures we have discussed so far employ either synchronous or asynchornous counters. We learnt from architectures C/D that the up/down counter erases any SET recorded in it; if it has SET transition both in its “up” and “down” input. We also learnt from the architectures A/B that the synchronous (LFSR) counters also records the glitches in the XOR gate. Therefore, if we remove the XOR gate then we could avoid the glitches and face the following problems:

- We will record all (both SET and normal) the transitions from the target in the LFSR counter.
- We could only record transitions from one target with one counter

In the current architecture we decided to combine both the synchronous (record both normal transitions and SETs in the LFSR counter) and asynchronous counter (combine the up/down counters with the LFSR counters such that it can help us recover from SETs that erase up/down counters data). The challenge here is to find a clever arrangement that allows us to distinguish between errors that occurred in the original target circuit and those in the counters. To this end, we use the following three strategies:

- For our SET counters, we employ an LFSR, the benefit being that the counting sequence in a (carefully chosen) LFSR always involves multiple bit changes per count. Hence, a single bit flip caused by an SEU will lead to a dramatic change in the count sequence that is easily recognizable by an a posteriori analysis.
- To make sure that we have a correct copy of the count available even in case of a counter hit, we use duplication. Since, thanks to using an LFSR counter, we can identify the corrupted value, there is no need to go for triplication.
- For the difference counter, we cannot rely on recognizing erroneous counts. Duplication just allows us error detection but not recovery. A viable alternative is using an up/down counter in combination with an LFSR counter (which must be quite wide then, of course). This will not only allow recovery of the correct count, but will also provide diversity that might turn out very beneficial in a radiation environment.

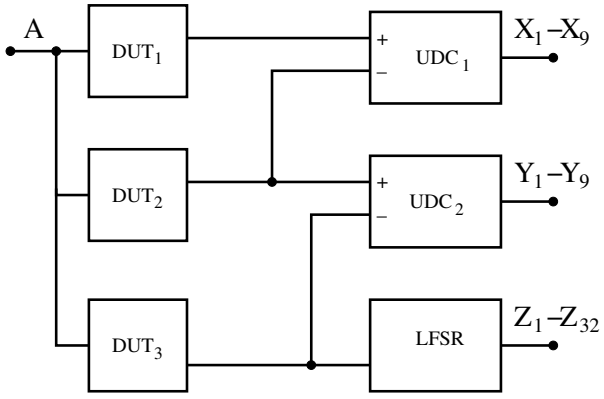


Figure 4.16: Measurement Architecture E

The architecture presented in Fig. 4.16, employs three DUTs of the same type, that would be mutually used as reference. The behavior of DUTs as observed by the counters are listed as follows:

- SETs in DUT_1 are observed only by UDC_1 with an "UP" count
- SETs in DUT_2 are observed by both UDC_1 and UDC_2, former with a "DOWN" count and later with an "UP" count
- SETs in DUT_3 are observed by both UDC_2 and LFSR, former with a "DOWN" count

Except for DUT_1 all the other DUTs have their transitions recorded in two counters. Therefore, any particle strike in UDC_1 does not provide any information about SETs in DUT_1. Our architecture clearly fails to recover all the the single faults. Hence, we need to modify this architecture to make sure that all single and double faults are definitely recovered.

4.2.6 Architecture F

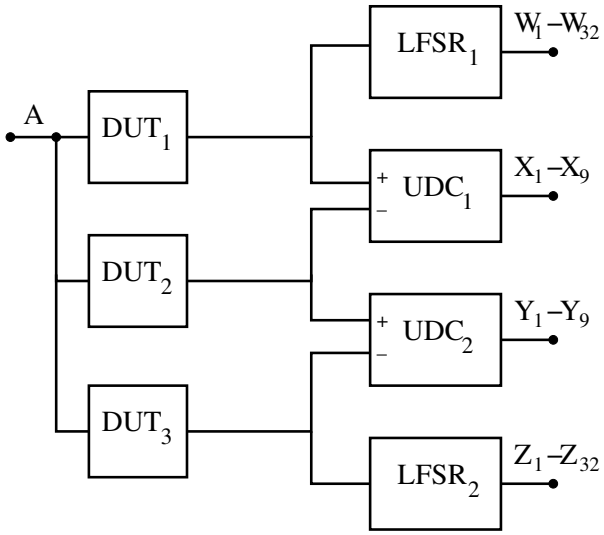


Figure 4.17: Measurement Architecture F

Measurement architecture F which is a slight modification to architecture E is presented in Fig. 4.17. It comprises three DUTs of the same type, which we mutually use as a reference. For example, the behavior of DUT_2 is observed by the two up/down counters UDC_1 and UDC_2. Note that these counters have different references (DUT_1 and DUT_3, respectively) and use different polarity (UDC_1 counting down and UDC_2 counting up on output transitions of DUT_2). In principle, this architecture allows us to tolerate any of the two up/down counters becoming faulty. However, as we cannot be sure to safely recognize every SEU of an up/down counter, it may (in rare cases) happen that we end up with two counts indicating different numbers of SETs, which without additional information are both plausible.

For DUT_1, we use a different strategy: Its behavior is observed by both UDC_1 (counting up) and an LFSR counter. The benefit here is that, as motivated above, we

can trust to recognize any faulty behavior of the latter. So in case the LFSR counter indicates a plausible number of SET occurrences in the target, we can simply trust it, while otherwise we still have the result of UDC_1 as a backup. Here we need a 32-bit LFSR for reasonably long measurement periods without wrap-around (42 seconds for a 100MHz input data stimulus), which we consider necessary for a safe recognition of counter hits. Finally, we use the same strategy for DUT_3.

Given the relatively low hit rate (according to Sec. 4.4, we will tune measurement period and radiation intensity to experience only a few hits per period), our general strategy in interpreting an observed scenario is to assume the lowest possible number of hits that could have led to the given observation. Considering, e.g., that UDC_1 counts up for failures in DUT_1 while it counts down for those in DUT_2, one might argue that SET observations may cancel out each other. This is, however, not the case, since we have redundant information in UDC_2 and the LFSR counter. With this combined information, it is possible to accurately identify every single hit, all double hits in both the target and the measurement circuits, and even many multiple hits correctly (for details see Sec. 4.3.5). Backed up by the probabilistic calculations in Sec. 4.4, we are convinced that our architecture represents an excellent choice with respect to the combined criteria of area efficiency, fault tolerance, diagnosability and diversity. Overall, it clearly surpasses the more evident solutions using three LFSR counters or three up/down counters.

4.2.7 Architecture G

For the XNOR tree, we simply use two LFSR counters in parallel, as shown in Fig. 4.18. Although we expect only few hits per DUT in a measurement period on average (see Sec. 4.4), we decided to go for a 16-bit LFSR (for details see below) in order to retain a sufficiently long counting sequence; this makes the recognition of incorrect counts more reliable. By using two LFSR counters, we make sure that we have a correct count available in case one LFSR has been hit.

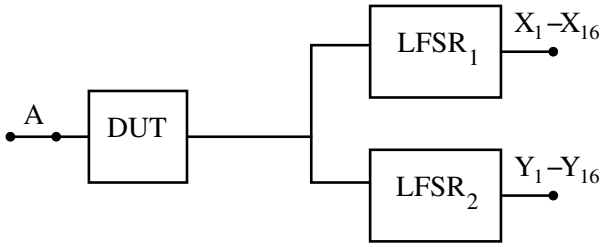


Figure 4.18: Measurement Architecture G

4.3 Evaluation and Analysis - Semi-Static Mode

The goal of this section is to provide an overview and some results of our prefabrication analysis of the proposed measurement architectures. Apart from area

considerations, our primary concern is an evaluation of the resilience against particle hits.

4.3.1 Overhead Analysis

Table 4.6 lists the total number of transistors required by the different target circuits described in Sec. 4.1 and the SET counters introduced in Sec. 4.2.

Table 4.6: Number of Transistors for Different Architectures

Architecture	Total No. of Transistors
Inverter	2
NAND	4
NOR	4
XOR	8
Flip-Flop	18
Muller C-Element	12
17-Inverter Chain	34
33-Flip-Flop Chain	594
128-input NAND-NOR Tree	508
128-input XNOR Tree	1016
35 C-element Van-Berkel elastic pipeline	490
35 C-element Weak-Feedback elastic pipeline	350
35 C-element Conventional elastic pipeline	490
16-bit LFSR Counter	440
32-bit LFSR Counter	856
9-bit up/down Counter	187

The measurement architecture utilizes three instances of each target circuit, with two 32-bit LFSR counters and two up/down counters. The exception to this is the XNOR tree target, one instance of which is monitored by two 16-bit LFSR counters. The resulting area consumption and the overhead incurred by the measurement circuits over the target circuits are given in Table 4.7. Note that the only substantial overhead incurred by the measurement setup occurs for the combinational gates and the inverter chains, which is due to the small size of the target. For the other target circuits, the measurement overhead is very reasonable. On average, the measurement circuitry consumes 19% more area than the target circuits. Given that our SET counters can also be seen as additional target circuits in our architecture, the overhead is acceptable.

Table 4.7: Hardware Overhead Analysis for Measurement Setup

Architecture	No. of Trans. for Target Circuits	No. of Trans. for Measurement Circuits	Overhead Factor (Target Circuit as base)
Inverter	6	2086	347.67
NAND	12	2086	173.83
NOR	12	2086	173.83
XOR	24	2086	86.92
Flip-Flop	54	2086	38.63
Muller C-Element	36	2086	57.94
Inverter Chain	102	2086	20.451
Flip-Flop Chain	1782	2086	1.171
NAND-NOR Tree	1524	2086	1.369
XNOR Tree	3048	880	0.289
Elastic Pipeline	1330	2086	1.568
All	7786	9224	1.185

4.3.2 Analysis Setup

The primary tool for the analysis of our measurement circuits' resilience against particle hits is simulation-based fault injection, using appropriate Spice models as described in Sec. 2.1.2.1. To get confidence in our architecture, we injected faults in each and every gate of each SET counter and analyzed the resulting behavior of the circuit.

We used release 6.1.6 of the Cadence Virtuoso Front-end to Back-end design environment to create the schematics of our circuits. They were all designed using UMC 90nm NMOS and PMOS device models. We chose custom W/L (width/length) ratios for the NMOS transistors, while the W/L ratios of the PMOS transistors were chosen based on the structure of the corresponding circuit. The Spice netlists were extracted from the respective Cadence schematics.

We performed all our analog simulations using HSPICE Version D-2010, using the following setup: To generate switching activity in the circuits, we toggled the data input every 5ns. After 10ns, we triggered the set and reset signals of the counters for about 40ns, which initializes the LFSR counter to 0 and the up/down counters to 5. At specifically selected times during normal operation, we triggered SETs by injecting a current pulse in the Spice netlist (refer to Sec. 2.4).

4.3.3 LFSR Counter Evaluation

The regular operation of the 32-bit LFSR is illustrated in Table. 4.8: With each rising clock edge, the counting proceeds by one step; the 32-bit LFSR will step

through a sequence of about 4.2 billion different values. A low at the RST input resets the count value to 0.

Table 4.8: Operation of the LFSR Counter in No-Fault Scenario

Time	LFSR Count	Actual Count
0-10ns	4194310	1
10-50ns	0	0
50-60ns	4194310	1
60-70ns	12582922	2
70-80ns	29360146	3
80-90ns	62914594	4
90-100ns	130023490	5
100-110ns	264241282	6

For our fault-tolerance analysis, we injected faults in each of the XNOR gates and flip-flops independently. Selected results are listed below (see also Table 4.9):

- Injection of an SET causing a bit flip from 1 to 0 in the XNOR gate tapped between Q_1 and Q_2 (please refer to Figure 3.25) at 75ns: Here the benefit of using an LFSR for counting becomes apparent. While only one bit of the output actually changes due to the SET, the related change in the counting sequence is drastic and hence easily recognizable: According to Table 4.8 the value following 29360146 should be 62914594, but here it is 29360144, effectively causing a huge jump in the counter sequence (see rightmost column).

- Injection of a fault causing bit flip from 0 to 1 in the XNOR gate tapped between Q_{22} and Q_{23} at 75ns: The injected SET caused the counter to skip 2.7 billion steps approximately, as shown in Table 4.9.

- Injection of the fault in the XNOR gate tapped between Q_2 and Q_3 at 80ns: The injected fault in XNOR gate created a bit flip of 1 from 0. The value following 29360146 should be 62914594 as per Table 4.8, but it is 62914592, causing the counter to skip 2.4 billion steps approximately.

- Injection of an SET causing a bit flip from 0 to 1 in the flip-flop with output Q_{15} at 80ns: This increased the LFSR count by 2^{15} and the actual count by 1.64 billion steps approximately. Again this is easy to detect.

- Injection of an SET causing a bit flip from 0 to 1 in the flip-flop with output Q_{16} at 80ns: It caused the counter to jump 162 million steps approximately.

Note that instead of the 15^{th} flip-flop if the particle strikes the 16^{th} flip-flop the number of skipped transitions is reduced tenfold. Overall, this confirms that a single bit flip in the LFSR counter is witnessed as billions of skipped transitions, making

Table 4.9: LFSR Counter – SETs in XNOR Gates & Flip-Flops

Time	LFSR Count	Actual Count
XNOR gate tapped between Q_{22} and Q_{23}		
60-70ns	12582922	2
70-75ns	29360146	3
75-80ns	2176843794	2782524433
80-90ns	58720293	2782524434
90-100ns	121634892	2782524435
XNOR gate tapped between Q_1 and Q_2		
60-70ns	12582922	2
70-75ns	29360146	3
75-80ns	29360144	2325803548
80-90ns	62914598	2325803549
90-100ns	130023498	2325803550
XNOR gate tapped between Q_2 and Q_3		
60-70ns	12582922	2
70-80ns	29360146	3
80-90ns	62914592	2449044163
90-100ns	130023494	2449044164
Flip-Flop with output Q_{15}		
60-70ns	12582922	2
70-80ns	29360146	3
80-90ns	62947362	1647004572
90-100ns	130089026	1647004573
Flip-Flop with output Q_{16}		
60-70ns	12582922	2
70-80ns	29360146	3
80-90ns	62980130	162967025
90-100ns	130154562	162967026

it an attractive candidate as an SET counter. Due to our careful selection of the LFSR polynomial, its one-to-many implementation (see Sec. 3.5.1.1), and backed up by numerous further experiments, we can indeed generalize this observation: A single bit flip in any LFSR cell will always infer a much larger and hence easily detectable effect in the actual count, which finally justifies our decision to use an LFSR counter.

4.3.4 Up/Down Counter Evaluation

In our analysis, SETs were injected into all C-elements and inverters to evaluate the resulting behavior of the up/down counter introduced in Sec. 4.2.3.1. Recall that the up/down counters are initialized to a count of 5, represented by 111110000 on

$Z_9 \ldots Z_1$ in Fig. 4.14.(c). Table 4.10 lists some of the scenarios obtained (e.g. at 75ns and 105ns):

A fault injected at 130 ns in the C-element that drives the output Z_8, e.g., changed the outputs Z_6, Z_7 and Z_8 to 1. There were also many instances when the fault injected at the same node in a different time interval just changed the output Z_8 temporarily to 1 (for one step) and switched back to 0.

- Fault injected at 105 ns in the Muller-C gate with RST signal that drives output Z_5: resulted in the count reduced by 1.
- Injection of fault in the Muller-C gate with RST signal that drives output Z_4 at 105 ns: changed the outputs of both Z_4 and Z_5 to 0, yielding a count of 3.
- Fault injected at 75 ns in the Muller-C gate which is located between outputs Z_4 and Z_5: changed the output Z_5 to 0.
- Injection of fault in the Muller-C gate which is located between Z_6 and Z_7 at 75 ns: changed the output Z_6 to 1
- Fault injected at 130 ns in the Muller-C gate with SET signal that drives output Z_8: changed the outputs of Z_6, Z_7 and Z_8 to 1.
- Fault injected at 130 ns in the Muller-C gate with SET signal that drives output Z_7: changed the outputs of Z_6 and Z_7 to 1.

Overall, we observe that the effect of an SET in an up/down counter is dependent on the location and the direction of the resulting bit flip. Unlike in the LFSR case, the initial effect of the fault is not "amplified", such that a particle hit in the up/down counter cannot easily be distinguished from a regular counting step caused by an SET in the associated target. This confirms that some kind of replication is indeed mandatory for using these counters in our measurement architecture.

4.3.5 Fault Dictionary

We have created a comprehensive fault dictionary for our measurement architecture, which associates every fault scenario (single or multiple SET hit(s) in counters and targets) with its "syndrome", i.e., the set (U_1, U_2, L_1, L_2) of resulting readouts on the up/down counters UDC_1 and UDC_2, as well as the $LFSR_1$ and $LFSR_2$. Used in the reverse direction, this dictionary allows us to infer from an observed syndrome the fault scenario that caused it, with, e.g., (U_1, L_2, D_2) indicating that UDC_1, $LFSR_2$ and DUT_2 have been affected by an SET. This mapping, unfortunately, is not bijective, as different multiple-fault scenarios may map to the same syndrome. We use two strategies to handle this issue: (1) By carefully choosing the measurement period (see Sec. 4.4), we can safely neglect the probability of experiencing many SET hits within one period (i.e., before reading out and re-initializing the counters). This allows us to ignore fault scenarios involving more than, e.g., 4 SETs in our dictionary. The same reasoning supports our strategy (2), namely, associating an

Table 4.10: Fault Analysis of the Up/Down Counter

Time	Up/Down Count	Actual Count
C-element (with set) between the outputs Z_4 and Z_5		
65-70ns	111110000	5
70-75ns	000001111	5
75-80ns	1111**0**0000	**4**
80-85ns	0000**1**1111	**4**
C-element (with rst) at output Z_5		
95-100ns	111110000	5
100-105ns	000001111	5
105-110ns	1111**0**0000	**4**
110-115ns	0000**1**1111	**4**
Muller-C gate with RST at output Z_4		
95-100ns	111110000	5
100-105ns	000001111	5
105-110ns	111000000	3
110-115ns	000111111	3
Muller-C gate between the outputs Z_6 and Z_7 Y_6 and Y_7		
65-70ns	111110000	5
70-75ns	000001111	5
75-80ns	111111000	6
80-85ns	000000111	6
C-element (with set) at output Z_8		
120-125ns	111110000	5
125-130ns	000001111	5
130-135ns	00000**000**1	**8**
135-140ns	11111**111**0	**8**
Muller-C gate with SET at output Z_7		
120-125ns	111110000	5
125-130ns	000001111	5
130-135ns	000000011	7
135-140ns	111111100	7

observed syndrome with the scenario that involves the lowest number of faults, as it is far more probable to occur than other matching scenarios that might exist. Of course, however, this can lead to misinterpretation in rare cases.

Table 4.11 shows an excerpt of our fault dictionary. Herein "*" and "X" both indicate an incorrect counter value, with the latter being recognizable as an error and the former not. "$\surd$" indicates that the expected LFSR value for the fault free case is read, "+" stands for a correctly incremented LFSR value.

Table 4.11: Fault Dictionary

Observed Syndrome				Location of Faults	
U_1	U_2	L_1	L_2	Actual Location	Interpretation
No Fault Scenario					
5	5	$\surd$	$\surd$	$---$	$---$
Single Fault Scenario					
6	5	+	$\surd$	D_1	D_1
4	6	$\surd$	$\surd$	D_2	D_2
5	4	$\surd$	+	D_3	D_3
*	5	$\surd$	$\surd$	U_1	U_1
5	*	$\surd$	$\surd$	U_2	U_2
5	5	X	$\surd$	L_1	L_1
5	5	$\surd$	X	L_2	L_2
Double Faults Scenario					
Location of all faults traceable					
Problematic Triple Fault Scenarios					
*	5	X	$\surd$	(U_1 , L_1 , D_1)	(U_1 , L_1)
*	*	$\surd$	$\surd$	(U_1 , U_2 , D_2)	(U_1 , U_2)
5	*	$\surd$	X	(U_2 , L_2 , D_3)	(U_2 , L_2)
Problematic Quadruple Fault Scenarios					
*	*	+	$\surd$	(D_1 , D_2 , U_2 , U_1)	(D_1 , U_2 , U_1)
6	*	+	X	(D_1 , D_3 , U_2 , L_2)	(D_1 , U_2 , L_2)
*	*	X	$\surd$	(D_1 , U_1 , U_2 , L_1)	(U_1 , U_2 , L_1)
*	6	X	$\surd$	(D_1 , D_2 , U_1 , L_1)	(U_1 , D_2 , L_1)
5	*	X	$\surd$	(D_1 , D_2 , U_2 , L_2)	(D_1 , U_2 , L_2)
*	5	X	X	(D_1 , U_1 , L_1 , L_2)	(U_1 , L_2 , L_1)
*	*	$\surd$	+	(D_2 , D_3 , U_1 , U_2)	(D_3 , U_2 , U_1)
*	5	$\surd$	X	(D_2 , D_3 , U_1 , L_2)	(L_2 , U_1)
4	*	$\surd$	X	(D_2 , D_3 , U_2 , L_2)	(D_2 , U_2 , L_2)
*	*	X	$\surd$	(D_2 , U_1 , U_2 , L_1)	(U_1 , U_2 , L_1)
*	*	$\surd$	X	(D_2 , U_1 , U_2 , L_2)	(U_1 , U_2 , L_2)
*	*	$\surd$	X	(D_3 , U_1 , U_2 , L_2)	(U_1 , U_2 , L_2)
5	*	X	X	(D_3 , U_2 , L_1 , L_2)	(U_2 , L_1 , L_2)

We will provide a short description of the observed scenarios below:

- Single fault scenario: *Particle strike in DUT_3* – SET injected in DUT_3 at $t + \delta t_2$, the resulting failure can be noticed both in UDC_2 (count decreased by one) and the LFSR2 (one extra step).
- Double fault scenario: *Particle strikes in $LFSR_1$ and UDC_2* – When SETs are injected in both the up/down counters independently at different $t + \delta t$, the effect of the SETs are noticed in the respective counters themselves (please refer to Sec. 4.3.4 and 4.3.3 for the effects of SETs in the counters). As the $LFSR_2$ has no SETs recorded in it we can clear DUT_3 and $LFSR_2$ of any fault, thereby isolating the faulty block as UDC_2. As UDC_1 has no SETs recorded in it, we can conclude that there is no SET recorded in DUT_1 and therefore isolate the fault to $LFSR_1$.
- Triple fault scenario: *Particle strikes in DUT_1, UDC_1 and $LFSR_1$* – When SETs are injected in the DUT, the up/down counter and the LFSR counter independently at different $t + \delta t$, the effect of the SETs are noticed in the respective counters. Note that any SET in DUT_1 will be recorded in $LFSR_1$ and UDC_1. Further SETs in $LFSR_1$ and UDC_1 would corrupt any SET data of DUT_1 recorded by the same. As we cannot recover SET data about all the three blocks we called these as the problematic scenarios.

It turns out that our architecture facilitates correct identification of the hit circuit for all single faults. The same is true for all double faults (not shown for brevity). Furthermore, most of the triple faults and even quadruple faults are correctly identified; the few problematic cases that lead to a wrong interpretation are shown in the table. In the case when all four counters are hit, we do not have any useful information left, of course.

4.3.6 SET Simulations

To give a brief overview of the SET analysis performed to validate our architectures, we present an example considering an inverter chain as the DUT, using the measurement architecture from Fig. 4.17. We injected SETs in all the three target circuits DUT_1, DUT_2, DUT_3 at different times, observable at the outputs of the DUTs as shown in Fig. 4.19: An SET is injected at 87ns in DUT_1, at 117ns in DUT_2 and at 147ns in DUT_3. The effect of these SETs in the DUTs, the up/down counters and the LFSR counters can be inferred from Figures 4.19, 4.20, 4.21 and 4.22.

More specifically, the effect of the SET injected at 87ns can be observed in UDC_1 (refer to signals X_1-X_9 of the UDC in Fig. 4.20) and in $LFSR_1$ (refer to Fig. 4.21). The effect of the fault injected at 117ns in DUT_2 can be observed in UDC_1 and UDC_2 (refer to signals X_1-X_9 and Y_1-Y_9 in Fig. 4.20). Similarly, the fault injected at 147ns in DUT_3 can be observed in UDC_2 (refer to signals Y_1-Y_9 in Fig. 4.20) and in $LFSR_2$ (refer to Fig. 4.22). One notices that, at 190ns, the SETs injected in the target circuits canceled the counts of UDC_1 and UDC_2, thus bringing

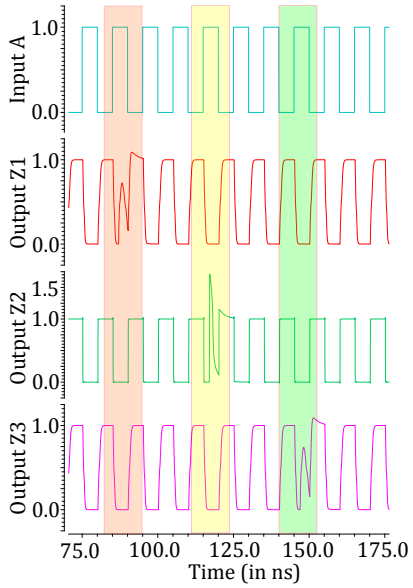


Figure 4.19: Simulation of the DUTs under exposure

them back to the initial state. However, the effect of the SETs in DUT_1 and DUT_3 is still observable in $LFSR_1$ and $LFSR_2$, respectively.

More specifically, assuming that these were the only three SETs observed in this target circuit during the measurement period of 40s, we will observe no change in the UDCs and one extra count in both the LFSRs at the end of the measurement period. From these values, we can infer that the faults did not occur in $LFSR_1$ or $LFSR_2$: If a fault occurred in the LFSR, then there would not be just one extra count but millions of extra counts. From the LFSR's values we can thus infer that the fault occurred in the target circuits DUT_2 & DUT_3 and thus explain the SET's effect in the UDCs: Based on their values, we deduce that the SET in DUT_1 canceled the effect of SETs created by DUT_2 and DUT_3 in the UDCs. This is how we determined the corresponding entry in the fault dictionary in Table. 4.11.

Our fault dictionary has been validated by means of numerous simulated SET injections (up to seven at a time) into various locations, using the same process as explained above. We are hence convinced that the chosen measurement architecture will indeed work as expected.

4.4 Probabilistic Analysis

Given the non-negligible number of transistors I_M of the measurement circuitry M as compared to the number of transistors I_T of the target circuitry T in Table 4.7 in Sec. 4.3 on one hand, and the ability of M to tolerate just a double hit for sure[4]

[4]Given that M can also tolerate many triple and even higher-order faults, this is a very conservative assumption.

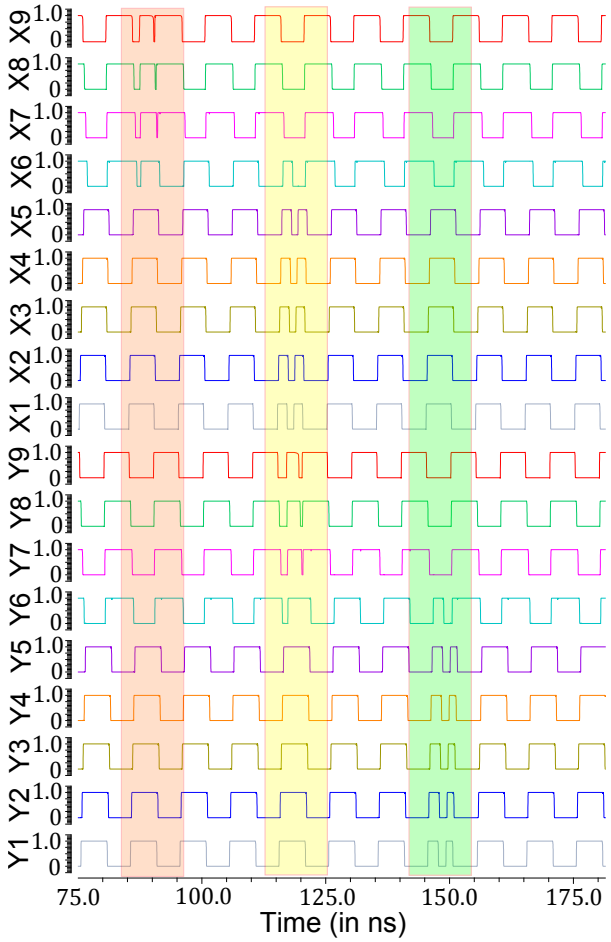


Figure 4.20: Simulation of the Up/Down Counters under exposure

on the other hand, the question about feasible measurement periods $\Delta = \Delta(\phi)$ for a given particle flux ϕ (in particles per $\mu m^2 \cdot s$) arises: Δ must be chosen small enough such that, with reasonably high probability, there are at most two hits in M during Δ; we call such a measurement period *safe*. At the same time, with reasonably high probability, two consecutive hits in T should occur within some P safe measurement periods sufficiently often, in order to get statistically meaningful data on the SET generation process.

A gross estimate of Δ and P can be determined using cross section data. Although such an estimate necessarily ignores the fact that target and measurement circuitry have very different structure and topology, it provides meaningful results due to the fact that we do not rely on SEU cross sections but rather on SET cross sections: Whereas it is known that memory elements like flip-flops are more susceptible to radiation than combinational logic, this is primarily a consequence of the fact that SETs in combinational logic are relatively unlikely to be latched. Consequently, they do not as easily lead to an SEU as SETs resulting from a direct hit of a

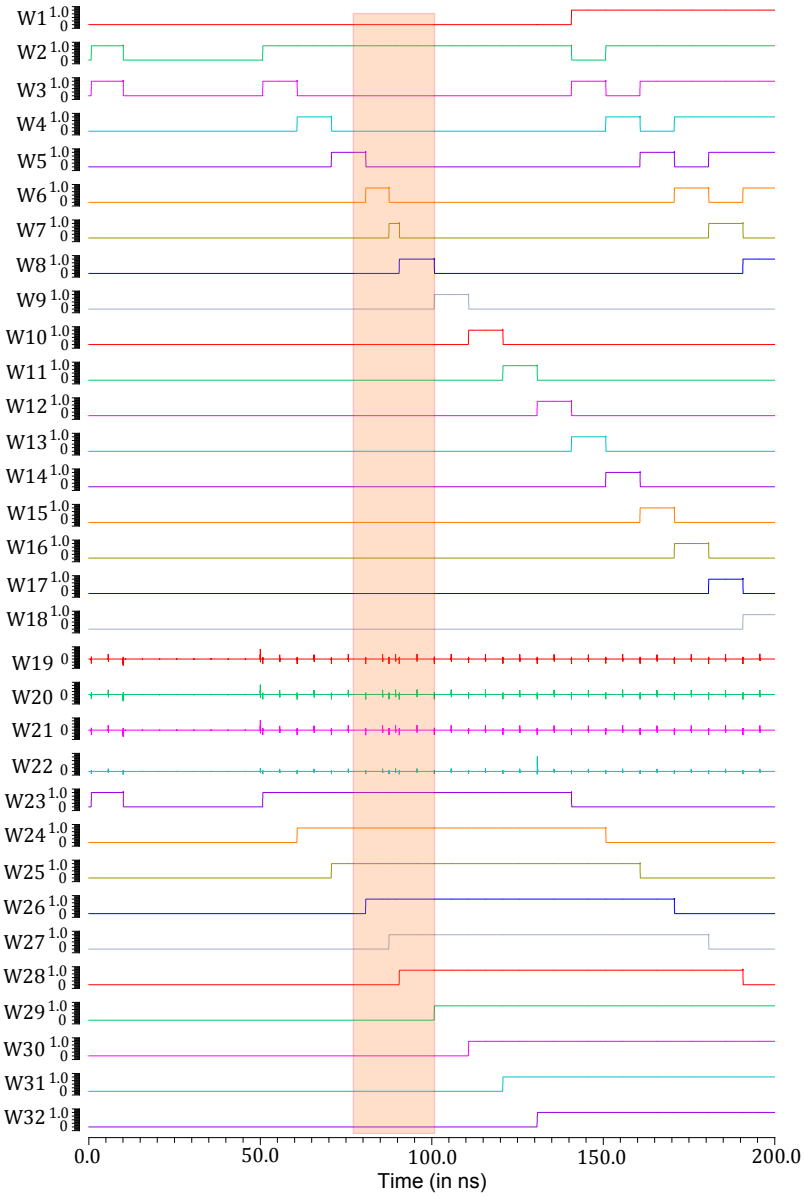


Figure 4.21: Simulation of the LFSR Counter 1

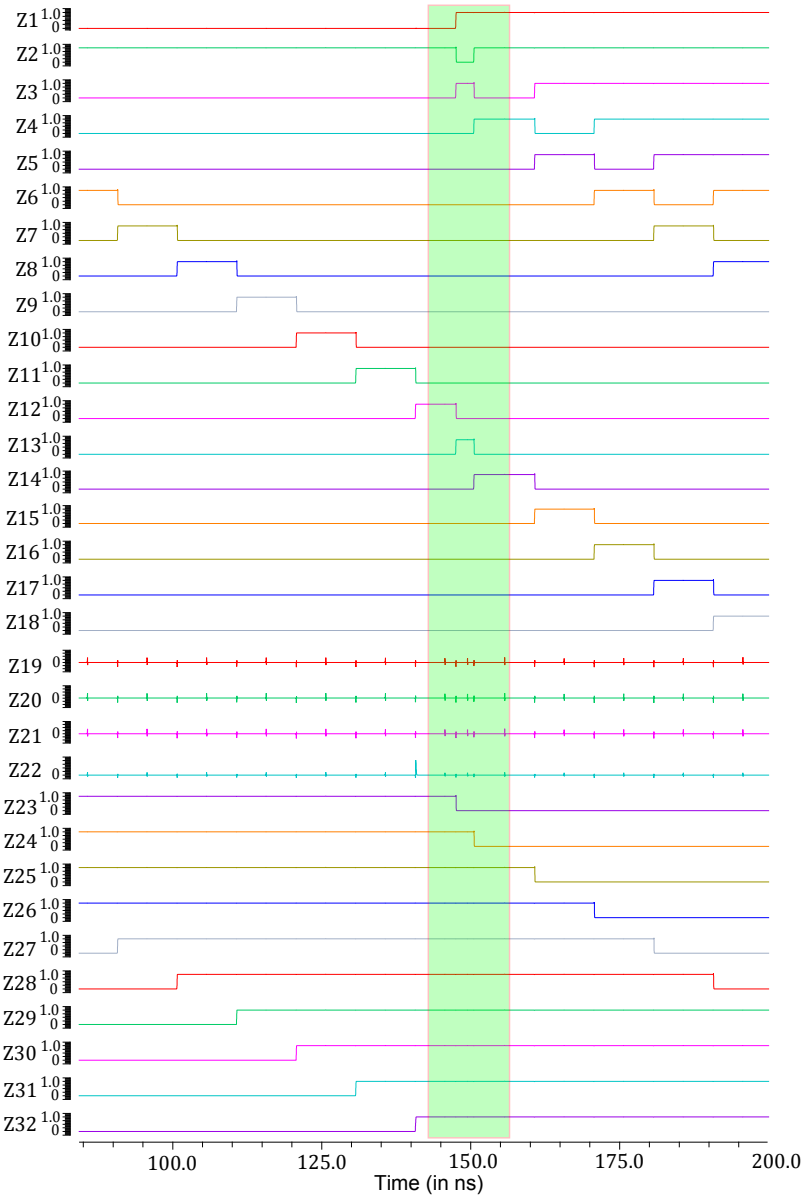


Figure 4.22: Simulation of the LFSR Counter 2

flip-flop. By contrast, the SET generation process is the same both in combinational logic and in flip-flops.

Our radiation experiments for validating the 3D model provided a (saturated) SET cross section γ of about $\gamma = 5\ \mu m^2$ for our 90 nm ASIC technology, which matches the figures given in the literature [106]. The cross section expresses that a total fluence of 1 particle per γ results in 1 SET per device of interest (in our case, per transistor) on average. Trivial calculations based on expected values reveal that if we choose $\phi\Delta = \frac{1}{\gamma I_M}$, we get one hit in M during Δ on average. Since Δ should be chosen large enough to fully exploit M's double-hit resilience, but should only rarely lead to triple hits, we choose

$$\Delta = \frac{C}{\gamma\phi I_M},$$

for some constant $0 < C \leq 2$, which leads to $E[H_M] = C$ hits in M on average. For arbitrary distributions of the number of hits H_M in a single measurement period in M, Markov's inequality $P\{H_M \geq h\} \leq E[H_M]/h$ reveals a triple-hit probability of $p = P\{H_M \geq 3\} \leq C/3$; it can be made sufficiently small by choosing C sufficiently small. As this results in a geometric distribution of safe measurement periods, we can expect an average of $P_M = 1/p \geq 3/C$ consecutive safe measurement periods.

On the other hand, the average number of hits in T during Δ is CI_T/I_M, so we can expect one hit on average in T after

$$P = \frac{I_M}{CI_T} \tag{4.1}$$

measurement periods; note that they eat up a total time of $P\Delta = \frac{1}{\gamma\phi I_T}$.

To see a hit in T before the measurement is affected by a triple hit in M on average, we should have something like $P \leq P_M$, which is guaranteed if $\frac{I_M}{I_T} \leq 3$. This is a very conservative estimate, however. To obtain the actual probability of failure P_{fail}, i.e., of an unsafe measurement period within two consecutive target hits, we will assume that the number of hits in M and T follow a compound Poisson distribution with the same average hit rate per $\mu m \cdot s$. This implies a rate $\lambda_M = C$ per measurement period in M, and $\lambda_T = CI_T/I_M$ in T.

Recalling the geometric distribution of safe measurement periods with parameter p and the fact that the probability of no target hit within k measurement periods is $e^{-\lambda_T k} = e^{-C_T k}$, where we used the abbreviation $C_T = CI_T/I_M$, we find

$$P_{fail} \;=\; \sum_{k\geq 0} p(1-p)^k e^{-C_T k} = \frac{p}{1-\frac{1-p}{e^{C_T}}} = \frac{pe^{C_T}}{e^{C_T} - 1 + p}.$$

Since the Poisson distribution of H_M implies $p = P\{H_M \geq 3\} = 1 - (1 + C +$

$C^2/2)e^{-C} = 1-(1+C')e^{-C}$ with $C' = C + C^2/2$, we thus easily obtain

$$\begin{aligned} P_{fail} &= \frac{\big(1-(1+C')e^{-C}\big)e^{C_T}}{e^{C_T}-(1+C')e^{-C}} = \frac{1-(1+C')e^{-C}}{1-(1+C')e^{-C-C_T}} \\ &= \frac{1-(1+C+\frac{C^2}{2})e^{-C}}{1-(1+C+\frac{C^2}{2})e^{-C(\frac{I_M+I_T}{I_M})}} \end{aligned} \tag{4.2}$$

Expression (6.12) for P_{fail} can be made as small as desired by choosing $C \in (0, 2]$ sufficiently small, for all reasonable ratios I_T/I_M. For example, for $I_T = I_M/2$, which is more than reasonable for all target circuits except for the inverter chain according to Table 4.7, we obtain $P_{fail} < 0.01$ for $C = 0.2$. For the inverter chain, Table 4.7 reveals $I_T = I_M/20$, which yields $P_{fail} < 0.1$ for $C = 0.2$. Note that, according to (6.6), $C = 0.2$ leads to $P = 5$ measurement periods between two target hits on average. Given the quite conservative assumptions underlying our probabilistic analysis, we can hence finally conclude that our measurement architecture is indeed excellently suited for collecting statistically meaningful long-term data.

4.5 High Speed Measurement Architecture

The targets we have discussed so far operate at a frequency of 100 MHz. In this section we would like to analyze the SET behavior of targets that operate at a minimum frequency of 1 GHz.

With a target circuit in static mode, every transition at the output indicates an SET caused by a particle hit and can hence be easily recorded by a counter. In dynamic operation, however, we need to distinguish transitions caused by the regular operation from those caused by particle hits. A suitable solution already outlined in Sec. 4.2.3 is the use of a *golden reference*, an identical instance of the target circuit that provides a reference for the transitions due to regular operation. By means of a difference counter we can then identify the number of extra (or missing) transitions due to particle hits. Since SETs are extremely short (a few 100ps) we need a very fast counter to reliably recognize them. For the purpose here, we want our target to operate at a very high frequency to keep the transistors "in transition" during a high proportion of time relative to the stable state. This again requires a fast difference counter. In addition to that the counter must mitigate the radiation that the connected targets are to be exposed to. Note that with a synchronous circuit we have a risk of meta-stability issues when operating at a very high frequency, hence we must opt to an asynchronous circuit. Therefore, the target and measurement counter we choose should be able to operate in a very high speed and provide reliable SET data.

Taking into consideration the requirements we decided to use a counter and target that is based on a Muller pipeline. Fig. 4.23 shows our test setup: It is centered around an asynchronous up/down counter [49, 48] that is constructed solely from Muller C-elements and inverters. All C-elements are internally realized as in the

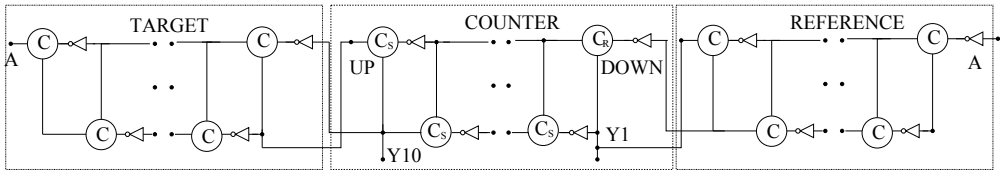


Figure 4.23: Measurement Setup for Dynamic Mode

weak-feedback implementation from [132], with the only difference that we added one NMOS or PMOS transistor at the output of the gate, to initialize the C-elements to 0 or 1 as shown in Fig. 4.24. We are using a 10-bit up/down counter in the setup and the Muller pipelines are also of the same length as the counter. Unlike, the other architectures we explained previously in Sec. 4.2.3.1 we initialize this up/down counter to a value of 2 (to avoid reading from an empty FIFO in case of a higher number of down transitions).

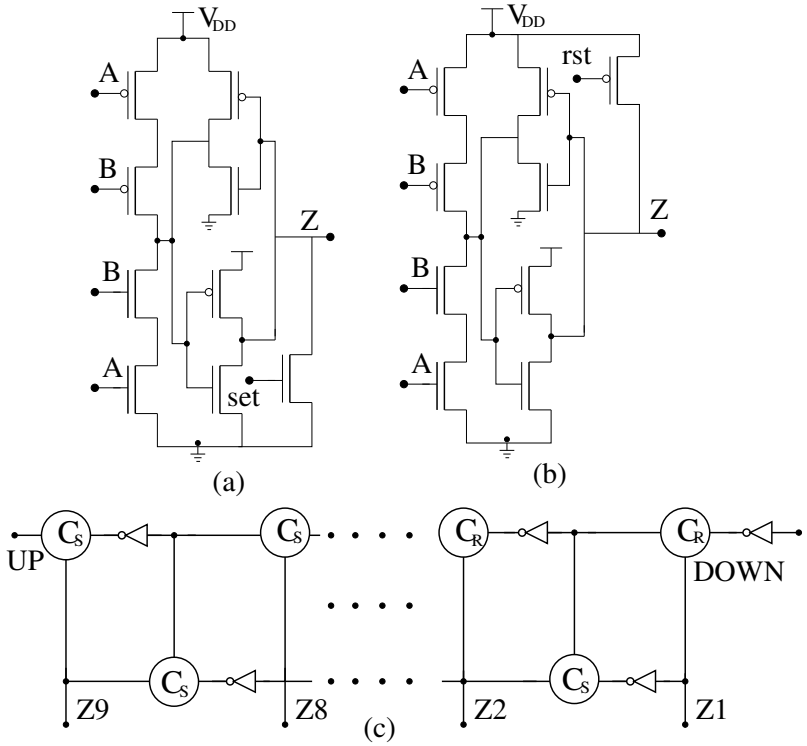


Figure 4.24: Schematic of Weak-Feedback (a) Muller C-element with Reset (rst), (b) Muller C-element with Set (set) and (c) Up/Down Counter

In our measurement setup we use an elastic pipeline as target circuit and connect it along with an identical reference to the counter as shown in Fig 4.23. All the C-elements in the architectrure utilize the weak-feedback implementation. The output of the target circuit and the reference are connected to the “UP” and “DOWN” inputs of the up/down counter. We were able to operate the non radiation-hardened

measurement setup in a very high frequency ($>$ 1GHz). The effects of particle strike in the setup are listed below:

- Particle hits in both the target and the reference would nullify the transitions in the counter.
- Particle strikes in the counter will let the counter reset to spurious counts.

In order to avoid this we decided to protect the counter and the reference from particle strikes by radiation hardening them using the mechanisms presented in Sec. 3.2.

After hardening the circuit we could reliably monitor the SETs in the target. The delay of a non radiation hardened C-element and inverter are less than the radiation hardened ones. Therefore, the target and reference circuit will have different logic delays. But, now the frequency of operation of the setup must be adjusted to avoid filling the pipeline of the target circuit. The frequency of operation of the setup after hardening the counter and the reference circuit will reduce significantly.

4.5.1 SET Analysis

We performed analog level simulations by injecting SETs in the measurement setup (presented in Sec. 4.5) to study the behavior of the same when exposed to radiation. Before conducting our SET analysis we wanted to calibrate the operational frequency of our setup. From the analog simulations we were able to determine that the typical frequency in which we can operate the setup safely without having any temporal issue is 3GHz. This is the operational frequency for the non-radiation hardened setup. The SET analysis performed on the original setup without any added radiation tolerance, is presented in Figures. 4.25, 4.26, and 4.27.

We have already observed the effects of particle strikes in the up/down counter (refer Sec. 4.3.4). An SET was injected in the target circuit at 87ns as shown in Fig. 4.25, as a result the count of the up/down counters increased by 1. Similarly an SET was injected at 47ns in the reference circuit as shown in in Fig. 4.26, as a result the count decreased by 1. Any SET in one of the target or reference circuit is visible in the counter. In the next step we injected two SETs in the setup as shown in Fig. 4.27, one in the reference circuit at 47ns and the other 87ns in the target circuit. In the end the two SETs reset the counter value to its original at 88ns.

The above analysis reaffirms the following facts:

- Radiation tolerance is required for the counter: Without it the counter can reset to spurious counts, thus providing us with no usable data about SETs.
- Reference circuit needs to be radiation hardened to avoid loss of SET data in the target circuit

We used two types of radiation hardening mechanisms to provide tolerance to the counter and the reference: 1) DICE implementation and 2) hardening by separation. The implementations for Muller C-element and the inverter are discussed in great detail in Chapter. 3. Unfortunately, the required circuit enhancements to

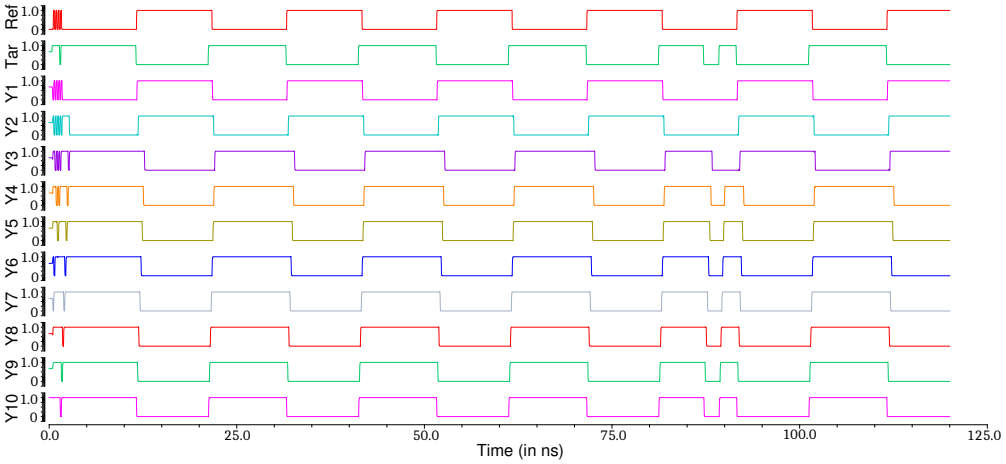


Figure 4.25: Simulation of the pipeline with target circuit under exposure

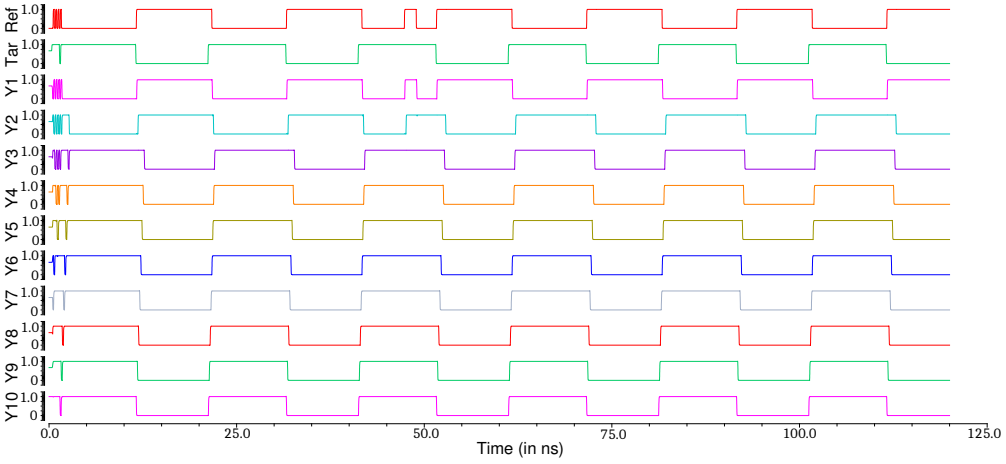


Figure 4.26: Simulation of the pipeline with reference circuit under exposure

provide tolerance decreased the speed of the counter, i.e., it reduced the frequency of operation. The maximum frequency achievable for the radiation hardened setup without forming bubbles in the pipeline is 1GHz. Although this counteracts our original goal of having the counter as fast as possible, the attainable speed is still sufficient to understand SET behavior in high speed circuits.

4.5.2 Hardware-Overhead Analysis

While finally all extensions yielded a sufficient degree of radiation tolerance, they differ in their area overhead and hence efficiency. Note that our up/down counter utilizes 19 Muller C-elements with "set" & "rst" transistors and 19 inverters. We provide a hardware overhead analysis for both the rad-hard mechanisms based on the required number of transistors for the enhanced counter, as well as an area estimate (area equiv.) based on the number of transistors weighed by their sizing.

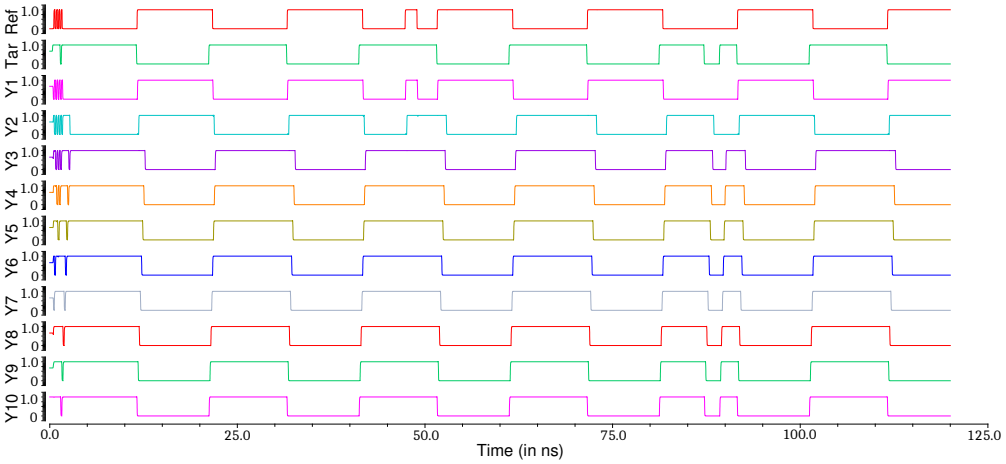


Figure 4.27: Simulation of the pipeline with target and reference circuit under exposure

Table 4.12: Hardware Overhead Analysis

Protection of	Applied Mechanism		No. of trans	W/L Sizing	Area Equivalent
	C-Element	Inverter			
Counter	DICE	Separation	475	M	779
Counter	Separation	Separation	627	1	627
Counter + Reference	DICE	Separation	931	M	1539
Counter + Reference	Separation	Separation	1235	1	1235

During the analysis we should consider that with increasing number of transistors per circuit the amount of routing overhead increases exponentially, and not linearly. The separation mechanism even though it requires a lower number of transistors the layout overhead is quite high. From the Table. 4.12 we can infer that the DICE mechanism seems to be most area efficient, as it uses a moderate number of transistors and the routing overhead is low, even though some of the transistors are larger than the basic transistors used by us in general.

However, the hardening by separation mechanism was able to provide radiation tolerance for particle strikes of a critical charge of 900fC even with the original sizing. So the designer can choose between a more efficient and lean or a very robust and bulk circuit. For our analysis we are concentrating more towards heavy ions, chromium particles and alpha particles so we opt for the more efficient and lean circuit using the DICE mechanism.

4.6 Summary

We presented our choice of target circuits and on-chip measurement architecture to analyse SET sensitivity in digital circuits, along with the results of the pre-fabrication analysis. Key challenges resolved by our measurement infrastructure are presented below:

- distinguishing SETs from normal switching activity of the target circuits,
- providing reliable SET data acquisition in spite of radiation hits in the measurement infrastructure, and
- leaving as much of the die area available for the target circuits as possible.

Rather than employing a rad-hard design, our infrastructure considers the measurement circuitry as additional target circuits, and hence allows to tolerate hits in the former by an architectural design that supports reliable fault detection based on a fault dictionary. Our measurement infrastructure has been evaluated by means of elaborate SET-injection experiments based on double exponential current model. We also presented the probabilistic analysis that allowed us to conclude that the infrastructure indeed serves its purpose in delivering useful SET data.

CHAPTER 5

Propagation of SETs

Our main focus is to trace the generation and propagation of SETs in a combinational circuit placed in the *FRad Chip*. We have already built architectures to study the SET sensitivity in different types of target circuits. Now, we would like to choose target circuits such that they could give us specific information about SET propagation. The chosen target should be able to propagate the SET to at-least three gates in its path, and we should also be able to predict and trace the same without any hassle. In essence the targets should have the following characterestics listed below:

- Simple – in order to be practically tractable
- Realistic – to yield results of practical value
- Symmetric – to allow for comparisons among paths
- Include forks – to observe SET multiplication
- Allow static and dynamic operation, to study the difference

The two targets that are chosen based on the above requirements and which would definitely propagate an SET are: Sklansky Adder and Inverter Tree. We will motivate the chosen targets in the next few sections. We have chosen two totally different target structures, and to be able to trace the propagation path of the SET we need custom measurement architectures for each of them.

5.1 Sklansky Adder

5.1.1 Background

For many processing operations from counting to multiplication to filtering, addition is the basis. Adder circuits have been of great interest to digital system designers, and an extensive, almost endless, assortment of adder architectures serving

different speed/area requirements can be found in the literature [60]. Some of them include ripple carry, carry lookahead, carry increment [166], carry select [19], carry skip [82], Brent-Kung [24], Kogge-Stone [78] and Sklansky (conditional sum) [134] adders.

The simplest design of these adders is the ripple-carry adder in which the carry-out of one bit is connected as the carry-in to the next. Due to this chain structure the carry-out influences the carry in all subsequent bits. We are interested in the adders that do not compute slowly (when one needs to add many bits), hence our focus is more towards carry look ahead adders.

All the fast adders look ahead to predict the carry-out of a multi-bit group. Long adders use multiple levels of lookahead structures for even more speed. For wide adders the delay of carry lookahead adders is primarily dominated by the delay of passing the carry through the lookahead stages. This delay can be reduced by looking ahead across the lookahead blocks. In general, one can construct a multi-level tree of lookahead structures to achieve a delay that grows with $logN$ (with N being the adder's bit width). There are many ways to build the lookahead tree that offers tradeoff among

- The amount of wiring between the stages,
- The number of logic gates,
- The maximum fanout on each gate, and
- The number of stages of logic.

The three fundamental carry propagation logic tree adders that are of interest to us are the Brent-Kung, Sklansky and Kogge-Stone architecture. Each of these architectures offer a different tradeoff between delay, area, and wiring complexity. The Brent-Kung adder has the fewest wires and minimum logic depth. Its drawback is that it has $(2(log_2N) - 1)$ stages. In contrast, the Kogge-Stone adder has just log_2N stages, but it has long wires to be routed between stages. Finally, the Sklansky adder also comes along with log_2N stages and without requiring that much routing, but at the expense of fanouts that double at each level. Patil et al. [117] compared some of the carry propagation adders and concluded that the Sklansky adder topology is the most energy efficient compared to the other adders in the $90nm$ technology that we were targeting initially.

5.1.2 Architecture Description

Before explaining the Sklansky tree adder we would like to explain some basic terminology about its constituent components. They are:

1. Bitwise *Propagate* (P) and *Generate* (G) cells,
2. Group PG cells, and

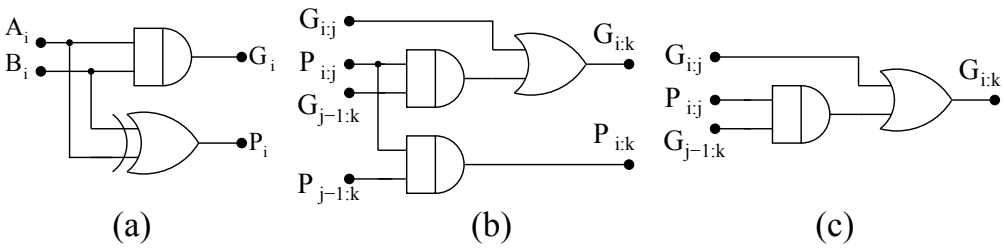


Figure 5.1: Gate Level Schematic of Sklansky Adder Cells

3. Sum XORs.

The bitwise PG cells are computed using the basic inputs of the adder circuit. Generate is computed as $G_i = A_i * B_i$ and propagate is computed as $P_i = A_i \oplus B_i$. In essence both the cells together are nothing but a half adder circuit as shown in Fig. 5.1(a). The bitwise PG cells serve as inputs to the group PG cells. The group PG cell has the upper inputs (i.e. those that handle the most significant bits) coming from $i : j$ and the lower inputs (those that handle the least significant bits) coming from $j - 1 : k$ (with $i > j > k$), to form an output of $i : k$ (see Fig. 5.1 (b,c)).

There are two types of group cells: the gray and the black cells (please refer to [27] for more explanation). Gray cells only compute $G_{i:j}$ as shown in Fig. 5.1(b), while the black cells compute both $G_{i:j}$ and $P_{i:j}$ as shown in Fig. 5.1(c). Black cells are used when the cell output drives the upper input of another group PG cell, while the gray cell will be used when the output drives the lower inputs or sum XORs. Please note that the output of the black cell drives the inputs of the gray cell, but never vice versa.

The outputs of the group PG cells and the bitwise propagate cells together drive the sum XORs to compute the adder's output. The sum is computed as $S_i = P_i \oplus G_{i-1:0}$.

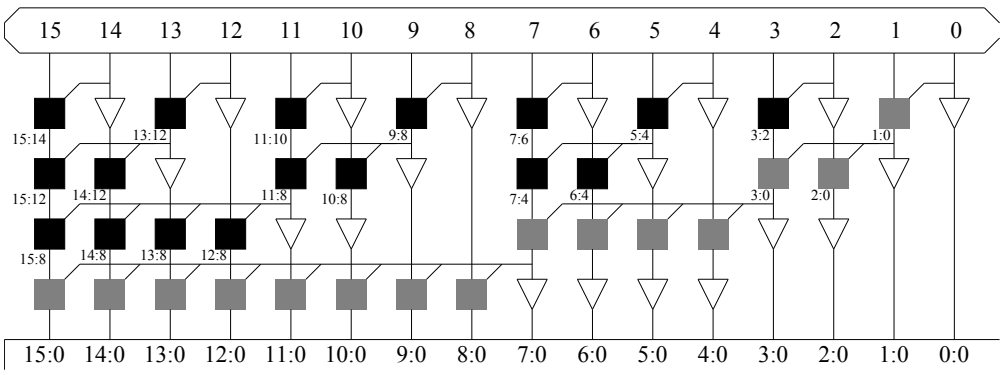


Figure 5.2: Architecture of 16-bit Sklansky Adder

The carry architecture (Group PG cell logic) of the 16-bit Sklansky adders is presented in Fig. 5.2. One can see that the architecture uses gray cells, black cells and buffers. Buffers are inserted to decouple the capacitive load from the critical

path, which is of importance only to the wide adders. For our case this is not crucial so we will disregard the buffers in our implementation later on.

Please note that the Sklansky tree adder reduces the delay to ($log_2 N$) stages by computing intermediate prefixes along with the large group prefixes. However, this comes at the expense of fanouts that double at each level: The gates fan out to (8,4,2,1) respectively (Please note the gray blocks in Fig. 5.2). These high fanouts cause poor performance on wide adders unless the gates are appropriately sized or the critical signals are buffered before being used for the intermediate prefixes.

Note that we do not fully exploit the potential of the Sklansky adder architecture; we rather use it as a platform to exemplify how the basic gates we already investigated in isolation in previous work behave in a larger context.

5.1.3 Measurement Architecture

Our main focus is to monitor the SET generation and propagation in the Sklansky tree adder, especially in the carry chain. We plan to subject this circuit to radiation in well controlled experiments, both in a nuclear reactor as well as in a micro-beam. We will operate the adder as an incrementer, i.e. adding 1 to the current output each cycle. In this way we can easily move the counter to any desired value by virtue of only a few input signals (thus saving precious pins on the ASIC). In order to collect the number and location of upsets due to particle impacts, we must augment our target circuits with a suitable measurement infrastructure. In case of the Sklansky tree adder this means placing some kind of counters at selected locations. The selection of type and locations of these counters is the key to efficiently monitor SET propagation. To make best use of the experiments the measurement infrastructure must fulfill the requirements presented in Sec. 1.3 and the ones presented below:

(R1): By evaluating the collected counts from adder and monitoring counters it must be possible to reason about location and propagation of the SET. In the ideal case we have a counter in every node of the adder. We will have to decide which of these we can omit in the interest of saving area, thus fulfilling (Req. 1.3 e).

(R2): Being located on the target chip, the counters are as well subjected to the radiation. Therefore it is mandatory that an upset of the counter value can be recognized in the read-out. As will be outlined below, an LFSR is well suited for this purpose. Alternatively the counter can be radiation hardened.

(R3): If a counter value is lost, it shall still be possible (at least in most cases) to interpret the observed hits on the adder – there must be sufficient redundancy in the measurement infrastructure. Consequently we must not reduce the number of counters to the bare minimum (as implied by (Req. 1.3 e)), and we must leverage a priori knowledge as much as possible.

5.1.3.1 Data Collection in the Carry Propagation Path

While the sum logic is essentially the same in all different adder types, the carry propagation logic is the most characteristic and crucial part of the adder architecture. Any bit flip caused by an SET at any point of the carry propagation path can spread throughout the whole adder. Recall that this is one of the reasons why we chose to use a carry look ahead adder as a target in the first place.

There are a lot of carry propagation paths in the 16-bit adder (Figs. 5.2 and 5.3), but the one marked in red is the longest and hence the critical path of the 16-bit adder. Also note that all the cells in the critical path are gray cells. Our aim here is to monitor the generation and propagation of SETs in this critical path. For monitoring the critical path it is sufficient to monitor the output nodes of half adder H_1 and gray cells G_1, G_3, G_7, G_{15} and G_{16}. In accordance with requirement (Req. 1.3 c) we added 5-bit LFSR counters to all these nodes to monitor the SET activity.

With these counters in place we can easily identify where the SETs were generated and how they propagated in the critical path, thus satisfying (Req. 1.3 e). Please note that, being constrained by (Req. 1.3 e), we can only identify the SETs in particular blocks at the critical path, not all of them. The monitoring architecture for these blocks in the critical path is shown in Fig. 5.3 (counters $L_1 ... L_5$ on the top, as well as L_6 at the bottom right).

The question that arises here is what would be the consequence of SETs within the counters, and whether radiation hardened counters are necessary for proper operation of this architecture (recall (R2), (R3)). This will be discussed in more detail in Sec. 5.3.

5.1.3.2 Overall Measurement Infrastructure

To also study SETs in blocks (i.e. half adders, gray cells, black cells) that are not part of the critical path, we have to extend the infrastructure by further counters. Considering the area constraint imposed by (Req. 1.3 e) we decided not to add counters in all the critical nodes, but only at the output of the XOR gates, which is nothing but the "SUM LOGIC" block. The resulting architecture is presented in Fig. 5.3 (counters $L_7 ... L_{22}$ on the right). We used 5-bit LFSR counters here as well (Req. 1.3 c).

The question whether a radiation hardened architecture is necessary for proper operation (R4) applies here as well. Another question that arises for this architecture is, whether the picture provided by the available counters will be sufficient to analyse both SET generation and propagation in all the blocks (R1), (R3). It is safe to say that having the counters just at the outputs will be sufficient to analyze the *generation* of the SETs in all the blocks. It remains to be analyzed whether we will be able to make a valid prediction of SET *propagation* by just using these counters. This issue will be treated in Sec. 5.3.

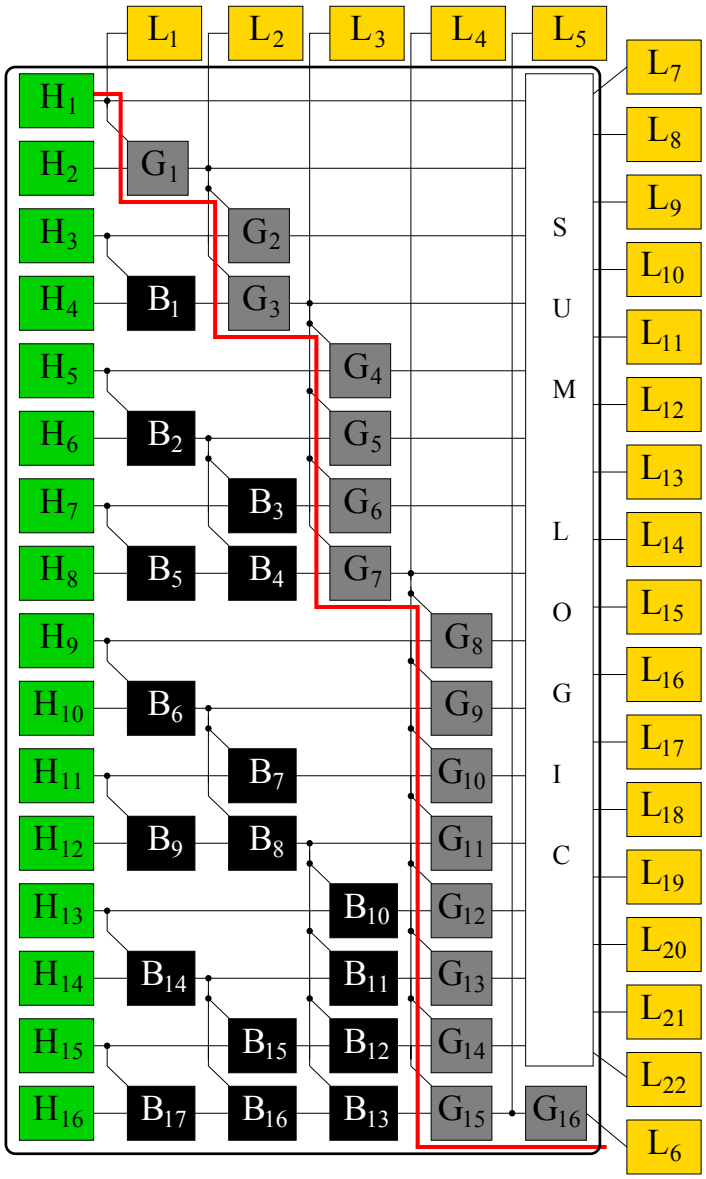


Figure 5.3: Measurement Architecture for SET Propagation in the 16-bit Sklansky Tree Adder: Half adders are denoted by H, black cells by B, grey cells by G, and LFSRs by L.

5.2 Inverter Tree

Considering the characterestics mentioned before, we decided to use a 4-stage inverter tree as our target. As shown in Fig. 5.5, the first stage (root) has just one inverter, while the second stage has two inverters, the third has four inverters and the last stage has eight inverters, resulting in a total of 15 gates. In the figure the inverters are labeled as I_1, I_2,..., I_{14}, I_{15}.

Inverters are the most fundamental, yet simple gates in CMOS, so they will allow us very detailed analysis and results of general interest. As inverters do not perform logical masking, we can rely on continuously having all paths sensitized – so electrical masking will be the only masking effect observed in this circuit. The tree structure includes many forks, thus allowing us to observe fault multiplication, while at the same time also exhibiting a depth of 4 stages for studying attenuation/amplification of the electrical pulses. The symmetry of the structure introduces some redundancy that we will leverage in the measurement architecture (see subsequent sections). The downside is that the inverter has a very small footprint (recall that we wanted to have a large target area), but using 15 inverters in the tree partly compensates for this. From a practical view the tree structure is advantageous for operating in the dynamic mode: there is only one input that needs to be supplied, while a detailed observation is possible on the 8 outputs.

5.2.1 Measurement Architecture

Our aim is to provide a clever architecture that does not need to rely on any rad-hard counters to provide protection against SETs. We use redundant components which are not expensive and at the same time area efficient. We will use both the counters that we have introduced earlier. Generally we will, due to its smaller footprint, prefer the asynchronous *up/down counter* (UDC), wherever we can reduce the observation to a comparison of transition counts. Should we need an absolute reference count, we will use the LSFR. The latter also has the advantage of an inherent error detection. All the LFSR counters used in our architecture are labeled as L_1, L_2, L_3, ..., L_{15} and the up/down counters are labeled as U_1, U_2,..., U_{18}, U_{19}.

5.2.1.1 Static Mode

In the static mode, there will be no activity in the inverter tree. If there is any activity in the tree at all, then it would be because of a particle strike in the tree. To record the SETs and also trace the path of the inverter tree we need to add counters in each and every output of the inverter. As we have 15 inverters in the tree, we would have to employ 15 counters to trace the path of the SET. We need not use up/down counters as the circuit is quite straightforward, hence we can do fine just with the 5-bit LFSR. The measurement architecture employed to monitor SET propagation in the inverter tree in static mode is presented in Fig. 5.4.

The architecture might look very simple, but it provides a more elaborate way to trace the SET propagation. One might think that the SET in the origin inverter

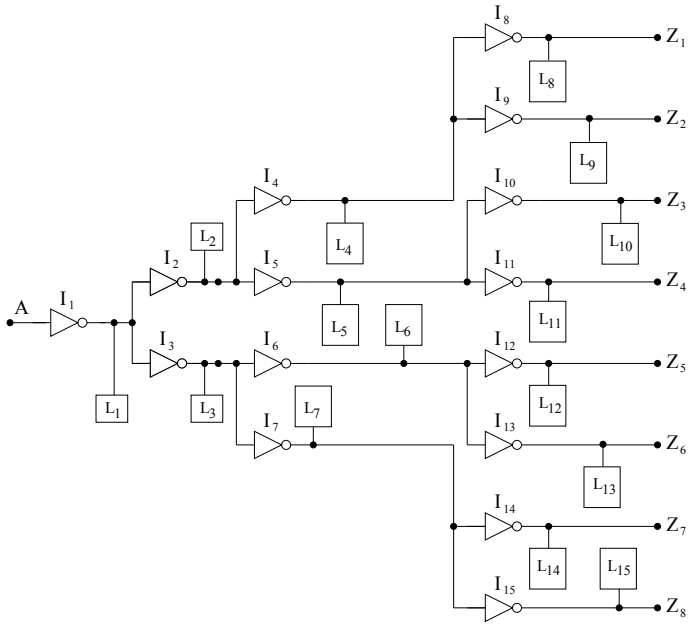


Figure 5.4: Measurement Architecture for the Static Inverter Tree

Table 5.1: Fault Coverage of the Static Inverter Tree Architecture

Fault in circuit	detectable by
I_1	$L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8, L_9, L_{10}, L_{11}, L_{12}, L_{13}, L_{14}, L_{15}$
I_2	$L_2, L_4, L_5, L_8, L_9, L_{10}, L_{11}$
I_3	$L_3, L_6, L_7, L_{12}, L_{13}, L_{14}, L_{15}$
I_4	L_4, L_8, L_9
I_5	L_5, L_{10}, L_{11}
I_6	L_6, L_{12}, L_{13}
I_7	L_7, L_{14}, L_{15}
I_8	L_8
I_9	L_9
I_{10}	L_{10}
I_{11}	L_{11}
I_{12}	L_{12}
I_{13}	L_{13}
I_{14}	L_{14}
I_{15}	L_{15}

is monitored only by one counter, and any SET in the counter might inhibit any usable data for the origin inverter, but it is not true. Note that if the SET propagates to the next stage and so on, it will be recorded in all the subsequent counters in the tree. Hence, we can conclude that the origin inverter has the highest amount of fault coverage, while the inverters in the last stage have the least amount of coverage. The fault coverage for the architecture is presented in Table 5.1.

From Table 5.1 we can observe that the SET injected in the inverter located in the first stage was recorded by all the 15 counters, while the inverters in the second stage have only 7 counters that record the SETs. Furthermore, the inverters in the last stage have only one counter that records their SETs.

Finally, the SET propagation in the inverter tree can be recorded safely using this architecture as we have redundant counters recording the same in the forks. We do not have enough redundancy in the fourth stage, and moreover particle strikes in the last stage do not provide sufficient data about SET propagation. Therefore, we are fine with not having any redundancy for the counters in the last stage. We will elaborate more on the architectures' efficiency in Sec. 5.4.1

5.2.1.2 Dynamic Mode

We can nicely exploit the symmetry of our tree structure with the UDCs: By connecting the up and down inputs to different inverter outputs (within the same level of depth, of course), the observed difference will always be zero in the fault-free case (which is why we can come along with a relatively small count range), and it will give us insight into fault occurrences, as well as fault masking, respectively, within one of the associated inverters. This principle works very well for the third and fourth stage of the tree where we have a sufficient number of gates available within the same stage.

Let us start the explanation of the architecture with the third stage: Here every inverter output is observed by 3 UDCs, all of which will record every SET affecting it. Should, in addition to the inverter, one UDC fail as well, we still have two correct counts available. While the failure of the inverter plus two of its associated UDCs already exceed our target of tolerating two SETs per observation period, we still have to consider the case of two UDCs being hit while the inverter operates correctly. So let us select two arbitrary UDCs. If we choose the two that do not share the same inverter output as an input, then we simply have two single faults that can be easily detected by the respective two remaining, fault-free UDCs at every connected node. If the UDCs share the same node for one of their inputs, then their respective other input will be connected to different nodes, for which the UDC fault again represents just a single fault and is hence covered. At these locations the faulty UDCs can be identified, and so the remaining, third UDC can still be identified even at the shared node, and its count be used. To implement this strategy we need 6 UDCs for the third stage, as shown in Fig. 5.5.

For the fourth stage of the inverter tree we decided to use a similar strategy. Here we carefully chose a combination of UDCs such that we could provide three counters per inverter while at the same time taking care not to form "clusters", so at

least one UDC would reach into another quadruple of nodes. For example, notice the counters U_8, U_9 and U_{10} in the Fig. 5.5. One can notice the UDC, U_{10} connected to both Z_1 and Z_5. Similarly notice the UDCs U_{12}, U_{13}, and U_{15}.

For the stages 1 and 2 the situation is different, as we do not have a sufficient number of nodes available. Here we have to employ additional LFSRs to attain the desired radiation tolerance (recall that the UDC does not provide error detection capabilities, while the LFSR does). More specifically we use one LFSR for stage 1 and 2 for stage 2, i.e. one per inverter output. For stage 2 we have one UDC and one LFSR per node (see Fig. 5.5), which is again sufficient for reliable operation under up to 2 faults: An SET within the LFSR can be detected by the LFSRs inherent capabilities. As we know that in the fault free case all LFSR counts must be equal ($L1 = L2 = L3$), it is straightforward to recover a lost L_2 from L_3 and vice versa. Should both be lost, we can rely that no fault has occurred in an inverter, by our double-fault assumption; and we have U_1 for an additional check.

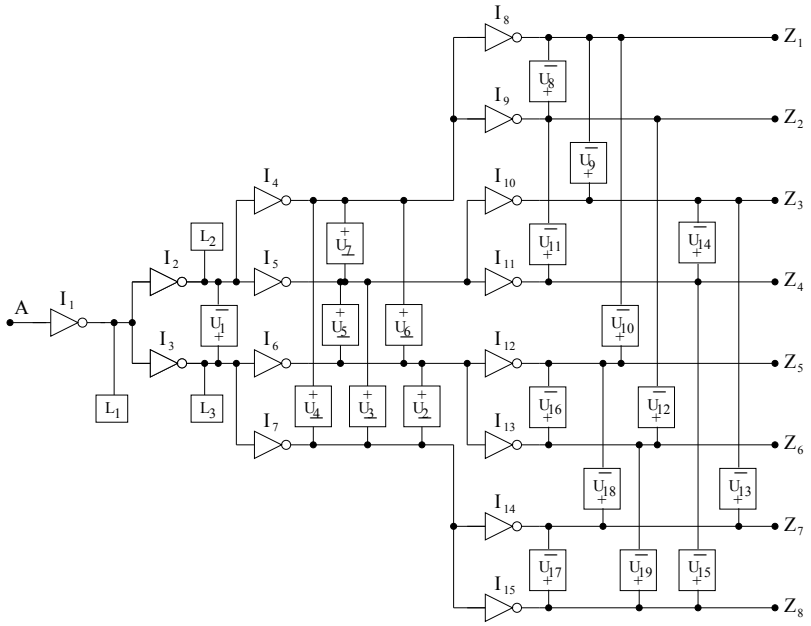


Figure 5.5: Measurement Architecture for the Inverter Tree – Dynamic Mode

In the first stage we only have one counter, which is obviously not sufficient to withstand double faults, like one affecting both the inverter and the LFSR. Here we must resort to the availability of correct LFSR counts from stage 2 (and this explains why we did not simply use 3 UDCs in that stage). This is illustrated in Table 5.2, where for each inverter it is shown in which counter an SET hit of it will be reflected.

As can be seen in the table, we have sufficient coverage for all circuits – it even looks like we have overdone the redundancy. Recall, however, that we want to monitor fault masking, so we cannot assume that a transition, once entering the chain, will actually propagate all the way through it. Therefore, as an additional require-

Table 5.2: Fault coverage of the proposed architecture (symmetric cases for which identical arguments apply are shown in parentheses)

Fault in circuit	detectable by
I_1	$\mathbf{L_1}$, L_2, L_3
L_1	$\mathbf{L_1}$, L_2, L_3
I_2 (I_3)	$\mathbf{L_2}$, $\mathbf{U_1}$, U_3, U_4, U_5, U_6, U_{10}, U_{12}, U_{13}, U_{15}
L_2 (L_3)	$\mathbf{L_2}$, $\mathbf{L_3}$, $\mathbf{U_1}$, L_1
U_1	$\mathbf{L_2}$, $\mathbf{L_3}$
I_4 (I_5...I_7)	$\mathbf{U_4}$, $\mathbf{U_6}$, $\mathbf{U_7}$, U_9, U_{10}, U_{11}, U_{12}
U_2 (U_3...U_7)	$\mathbf{U_3}$, $\mathbf{U_4}$, $\mathbf{U_5}$, $\mathbf{U_6}$
I_8 (I_9...I_{15})	$\mathbf{U_8}$, $\mathbf{U_9}$, $\mathbf{U_{10}}$
U_8 (U_9...U_{19})	$\mathbf{U_9}$, $\mathbf{U_{10}}$, $\mathbf{U_{11}}$, $\mathbf{U_{12}}$

ment, we need a consistent view of counter values within each stage, i.e. without the support of information from the adjacent stages. Only then we can reliably make conclusions on faults that have popped up or vanished since the previous stage.

Recall that the discussion of radiation tolerance capabilities above has always been carefully limited to information available within the stage under consideration, and the entries in bold font in Table 5.2 illustrate that there is always enough "local" information. The only exception is stage 1, where we had to partly rely on counts from stage 2. This fact will compromise the analysis of fault masking by stage 1. However, we felt that adding a complete LFSR just for redundancy purposes is too costly (in terms of area) for just having one single inverter (I_1) included in this analysis.

Overall our design has 22 counters, namely 19 UDCs and 3 LFSRs.

5.3 SET Analysis – Sklansky Adder

The primary purpose of the SET injection experiments presented in this section is to validate that the proposed architecture indeed allows us to capture and identify all SET occurrences by virtue of the available LFSR readouts, as demanded in requirements (Req. 1.3 c), (R1), (R2) & (R3). A first problem here is the interleaving of potential SET events with events generated by the normal operation of the adder. We have two basic choices to solve this problem:

- Allow such an interleaving, increase the width of the counters to capture both types of events, and subtract the counts due to normal activity (known from fault free analysis) afterwards, or

- Operate the adder in the static mode to avoid the events caused by normal operation. In that case the counters record SET related events only.

From the view of (Req. 1.3 e) the second option is clearly preferable. The problem here, however, is to identify a representative state of the adder in which to apply the SETs. In the physical experiments with the chip we can simply plan for multiple runs, each starting with a different state of the adder. For the purpose of our validation here, we want to check the worst scenario only (for the sake of saving simulation time), and conclude that more benign scenarios will be handled by our architecture as well. In order to identify this worst case scenario, we performed preliminary simulations with a 2-bit Sklansky adder.

5.3.1 Identification of the most sensitive adder state

We constructed a 2-bit Sklansky adder by reducing the 16-bit architecture from Fig. 5.2 to bits 0 and 1. Similarly we reduced the measurement architecture from Fig. 5.3 to 2 bit. The worst case for the measurement infrastructure is the one where a single SET becomes effective in many places. This happens when masking effects are at their minimum.

From the three masking effects known in the literature, *temporal masking* does not apply here, as we have a purely combinational circuit. We minimize *electrical masking* by applying SETs of significant charge that cannot simply get filtered by parasitic RC elements. Furthermore we took care to trigger the SETs at those points in time where they actually can become effective, i.e., we created particle strikes to hit the open transistors. To reduce *logical masking* to the minimum we applied SETs in all possible (static) states of the adder, striving to identify the one that showed the most significant effect. Note that in the physical experiments with the chip, the aim will of course be different: Rather than artificially reducing all masking effects, the crucial issue will be to study the extent of those very masking effects in practice, and in this way identify sensitive locations and paths on the one hand and robust ones on the other hand. However, at that time we must be able to rely on the chosen measurement architecture.

Overall we were able to observe SET propagation in all states, and there were a couple of sequences that showed better propagation of SETs; i.e. the length of the SETs pulse never degraded as the SETs propagated, while the other sequences did show some amount of degradation. One of those sequences that exhibited the lowest degree of masking had its inputs (A, B, C_{IN}) stuck at (1, 0, 0) to generate a carry of 0 and sum of 1. This sequence successfully propagated the SETs especially in the carry chain of the 2-bit adder. Therefore we decided to use an equivalent input pattern for our analysis of the 16-bit adder.

5.3.2 SET Injection Experiments in the 16-bit Adder

In a first campaign we injected SETs in each of the blocks of the critical path (as described in Sec. 5.1.3.1) sequentially (every 12ns) to see their vulnerability against SETs.

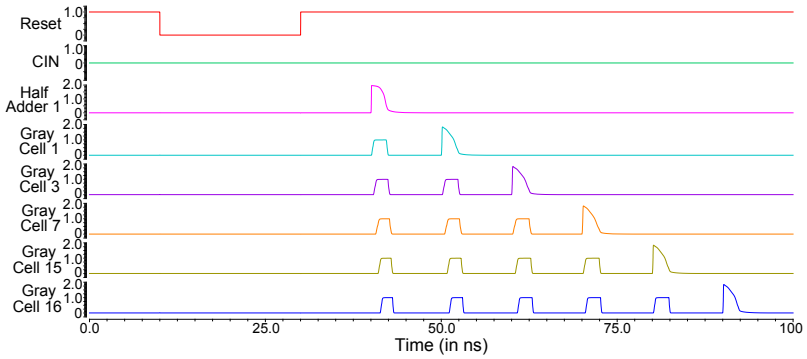


Figure 5.6: SET Analysis of Sklansky Adder

As can be seen in Fig. 5.6 (topmost traces) the SET injected in H_1 propagated to all subsequent blocks, i.e. G_1, G_3, G_7, G_{15} and G_{16}. Similarly the SET injected in G_1 propagated to G_3, G_7, G_{15} and G_{16}, and so on – each injected SET propagated to all downstream blocks as well as directly to the respective outputs. The traces of Fig. 5.7 (Z_1... Z_{16}) show the outputs of the "SUM LOGIC". A first conclusion from this observation is that, as expected, a single SET can indeed cause multiple output bits to flip.

This kind of propagation behavior, however, primarily depends upon the inputs fed to these blocks. In this sense the observation also confirms our choice of the most sensitive adder state from Sec. 5.3.1.

We can hence expect this choice to work fine in general with our 16-bit adder, also for SETs affecting blocks that are not in the critical path.

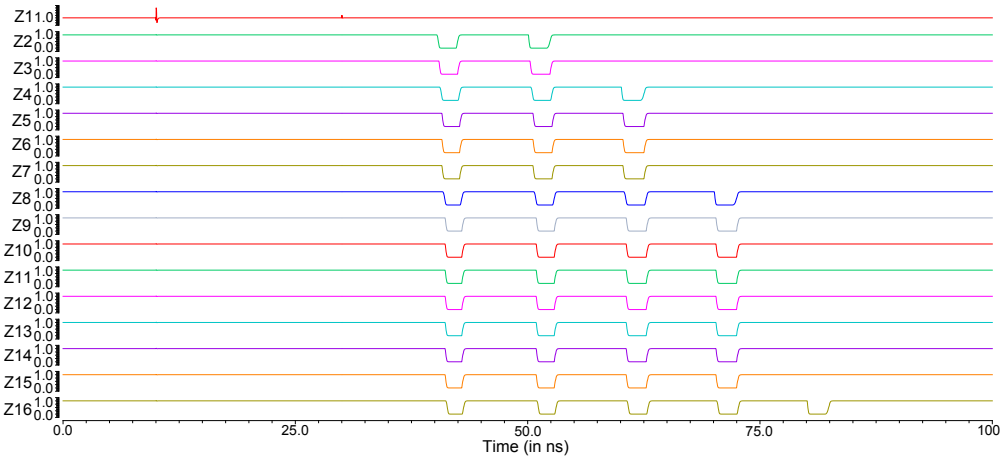


Figure 5.7: SET Analysis of Sklanksy Adder

Note that since the SET in any of the blocks in the origin or intermediate places of the critical path propagates, it will be recorded in all downstream counters. So the SET in H_1 will be observed in all the counters L_1...L_6. Similarly an SET in G_1 will be observed in counters L_2...L_6, and so on. At the end of our simulation mea-

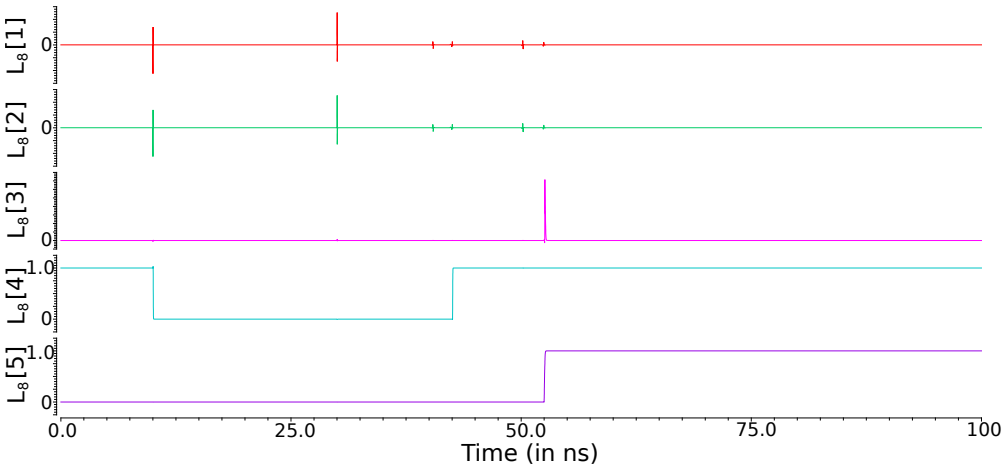


Figure 5.8: Counter L_8 - SET Analysis of Sklanksy Adder

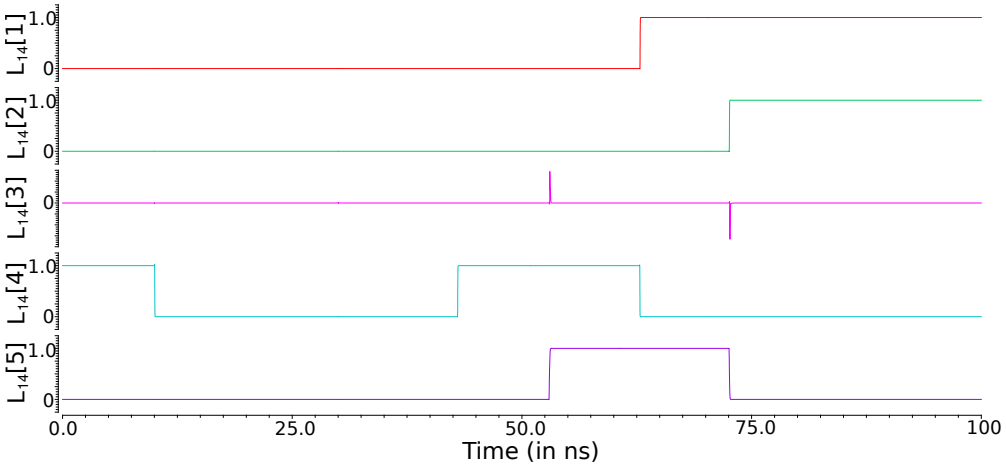


Figure 5.9: Counter L_{14} - SET Analysis of Sklanksy Adder

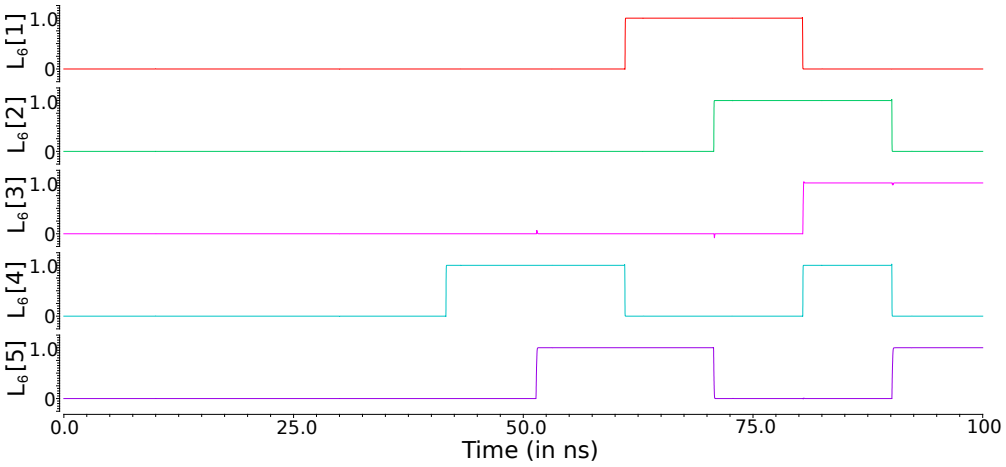


Figure 5.10: Counter L_6 - SET Analysis of Sklanksy Adder

surement the counts seen in L_1, L_2, L_3, L_4, L_5, L_6 is 1, 2, 3, 4, 5 ,6. This exemplifies the kind of data we will have available at the end of our radiation experiments, and from these data we will need to figure out the SET locations.

Notice that, due to the fact that we connected counters to internal nodes as well as to the outputs, and due to the propagation, we have redundant indications available for one SET. For example an SET in G_3 can be observed in seventeen counters (L_3-L_6, L_{10}-L_{22}) and an SET in G_7 can be observed in ten counters (L_4-L_6, L_{14}-L_{22}). In a similar fashion we can see that all of the blocks in which we injected SETs have redundant indications. This confirms that our measurement architecture meets requirement (R5).

To better elucidate the SET propagations and the type of data collected by the counters we present some of the counters' data (L_6, L_8, L_{14}). The counter L_6 records gray cell 16's SET data. Similarly, L_8 & L_{14} records the SET data of Sum Logic Z_2 & Z_8. We can observe from Fig. 5.10 that the counter L_6 records six SETs as expected (refer to Fig. 5.6 for the number of SET transitions in gray cell 16). Similarly, we can observe from Fig. 5.8 (Fig. 5.9) that the counter L_8 (L_{14}) records two (four) SET transitions as expected (refer to Fig. 5.7 for the number of SET transitions in the Sum Logic). We can hence conclude from the above observation and SET experiments that the counters do record the SET data properly.

Even in the case where an SET does not fully propagate we will, due to this redundancy, be able to say where the SET originated and we will also be able to trace the exact location in a similar fashion as explained above. To simplify the process of retracing the SETs we came up with a fault dictionary which will be the subject of Sec. 5.3.3.

A second simulation campaign was conducted to verify and validate the effectiveness of the monitoring architecture. In here we injected SETs, again at different time instants, in all the blocks of the 16-bit adder, including those that are not part of the critical path. The objective of this analysis was to check whether the SETs propagate or not (the same sequence of inputs that was used in the critical path is used here again). The result of this analysis turned out to be positive, and at the same time helped us build an elaborate fault dictionary for our architecture.

5.3.3 Fault Dictionary

The fault dictionary for the 16-bit adder is presented in Tables 5.3, 5.4, and 5.5. It uses the same notation as Fig. 5.3.

The columns $L_1 ... L_{22}$ indicate the counter values observed for a certain SET location that is indicated in column "Actual Location". When the counter does not record any transitions its value is indicated as $\surd$. When a SET transition is recorded the count is indicated as $+$. We call the array of these counter values in a line a *syndrome* of the SET location. Most of the blocks in the adder have their unique syndromes, however, since we do not have counters at each and every node, the syndromes for several SET locations coincide. For each SET location the column

Table 5.3: Fault Dictionary for Sklansky Adder

Observed Syndrome																							Location of Faults	
L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	L_{16}	L_{17}	L_{18}	L_{19}	L_{20}	L_{21}	L_{22}	Actual Location	Interpretation
No Fault Scenario																							
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	– – –	– – –
Single Fault Scenario																							
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	H_1	H_1
√	√	+	+	+	+	√	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	H_2	H_2
√	√	√	+	+	+	√	√	+	+	+	+	+	+	+	+	+	+	+	+	+	+	H_3	H_3
√	√	√	√	+	+	√	√	√	+	+	+	+	+	+	+	+	+	+	+	+	+	H_4	H_4
√	√	√	√	√	+	√	√	√	√	+	+	+	+	+	+	+	+	+	+	+	+	H_5	H_5
√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	+	+	+	H_6	H_6, B_2
√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	+	+	H_7	H_7
√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	+	H_8	H_8
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	H_9	H_9
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	H_{10}	H_{10}, B_6
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	H_{11}	H_{11}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	H_{12}	H_{12}, B_8, B_9
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	H_{13}	H_{13}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	H_{14}	H_{14}, B_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	H_{15}	H_{15}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	H_{16}	H_{16}

Table 5.4: Fault Dictionary for Sklansky Adder

Observed Syndrome																						Location of Faults	
L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	L_{16}	L_{17}	L_{18}	L_{19}	L_{20}	L_{21}	L_{22}	Actual Location	Interpretation
√	+	+	+	+	+	√	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	G_1	G_1
√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	√	√	√	√	√	√	G_2	G_2
√	√	+	+	+	+	√	√	+	+	+	+	+	+	+	+	+	+	+	+	+	+	G_3	G_3, B_1
√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	√	√	√	√	G_4	G_4
√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	√	√	√	G_5	G_5
√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	√	+	G_6	G_6, B_3
√	√	√	√	+	+	√	√	√	√	√	√	√	+	√	+	+	+	+	+	+	+	G_7	G_7
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	G_8	G_8
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	G_9	G_9
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	G_{10}	G_{10}, B_7
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	G_{11}	G_{11}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	G_{12}	G_{12}, B_{10}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	G_{13}	G_{13}, B_{11}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	G_{14}	G_{14}, B_{12}, B_{15}
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	G_{15}	G_{15}, B_{13}, B_{16}, B_{17}
√	√	√	√	√	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	G_{16}	G_{16}

Table 5.5: Fault Dictionary for Sklansky Adder

Observed Syndrome																						Location of Faults	
L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	L_{16}	L_{17}	L_{18}	L_{19}	L_{20}	L_{21}	L_{22}	Actual Location	Interpretation
√	√	+	+	+	+	√	√	√	+	+	+	+	+	+	+	+	+	+	+	+	+	B_1	G_3, B_1
√	√	√	+	+	+	√	√	√	√	√	+	+	+	+	+	+	+	+	+	+	+	B_2	H_6, B_2
√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	√	+	B_3	G_6, B_3
√	√	√	+	+	+	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	+	B_4	B_4, B_5
√	√	√	+	+	+	√	√	√	√	√	√	√	+	+	+	+	+	+	+	+	+	B_5	B_4, B_5
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	+	+	+	+	+	+	+	B_6	H_{10}, B_6
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	B_7	G_{10}, B_7
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	B_8	H_{12}, B_8, B_9
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	+	+	+	+	+	B_9	H_{12}, B_8, B_9
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	B_{10}	G_{12}, B_{10}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	B_{11}	G_{13}, B_{11}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	B_{12}	G_{14}, B_{12}, B_{15}
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	B_{13}	$G_{15}, B_{13}, B_{16}, B_{17}$
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	+	B_{14}	H_{14}, B_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	B_{15}	G_{14}, B_{12}, B_{15}
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	B_{16}	$G_{15}, B_{13}, B_{16}, B_{17}$
√	√	√	√	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	B_{17}	$G_{15}, B_{13}, B_{16}, B_{17}$

"Interpretation" indicates all possible interpretations, i.e. the correct one as well as other locations with the same syndrome.

We can, e.g., notice that H_6 and B_2 share the same syndrome. This is because any SET in the half adder H_6 will propagate to the black cell B_2 and we do not have any counters in the intermediate node, hence we cannot differentiate the SETs in these blocks. Similar circumstances arise for the blocks (H_{10}, B_6); (H_{14}, B_{14}) and (H_{12}, B_8, B_9).

Similarly, the gray cells and the black cells share syndromes. Gray cell (G_3) and black cell (B_1), e.g., share the same syndrome. This is because any signal in B_1 will only propagate to G_3 and not to any other node. Hence SETs in either of these blocks cannot be differentiated. There is one scenario where even four blocks share the same syndrome, namely the four blocks in the most significant bit of the adder (please note the three black cells and one gray cell in Fig. 5.7).

We can conclude from our preliminary analysis of SETs that this fault dictionary can reasonably predict the SET generation and propagation process for the 16-bit adder. There are some limitations in terms of SET locations that share the same syndrome. These cases are, however, relatively infrequent, and furthermore the blocks that share the syndrome are always next to each other. So it is not a significant setback for our measurement infrastructure and hence a reasonable compromise considering the area constraints imposed by requirement (Req. 1.3 e).

5.3.4 SETs in the Counters

It remains to be investigated whether the redundancy of our architecture allows us to stay with unprotected LFSRs, or we will have to employ radiation hardening to handle the case of SETs hitting an LFSR.

In the first place, we may safely assume that a particle hit in the LFSR will never[1] go unnoticed, since due to the chosen LFSR structure single-bit upsets, as expected to be caused by SETs, will lead to implausible jumps in the count sequence. However, even if the failure is detected, the respective counter value will be lost. In order not to loose too many experimental results, we do not want to be forced to discard the whole observation in every such case.

A look into the fault dictionary can help us answer this question: First of all, every single counter upset alone yields a unique syndrome (not shown in Tables 5.3, 5.4, 5.5); e.g., the "no fault scenario" with a + in the respective counter's column creates a unique syndrome. The situation with a counter upset occurring in the same observation period as an SET in a target block is more intricate, however. As an example consider the cases of (a) an SET in the actual location H_4 and (b) an SET in the actual location H_5. Those can be distinguished by means of counter value L_9 only. Should this counter value get corrupted through another particle hit, this distinction will not be possible any more. More generally, of the 49 blocks there are 15 for which, due to the same reason, no unique interpretation will be possible if a certain counter value is lost. However, the probability of this to happen

[1] at least with negligible probability

is sufficiently low: There are 22 LFSR counters, 16 half adders, 16 gray cells and 17 black cells. For the critical scenario we need to have a particle hit in one of the 15 target cells (H_4 or H_5 in the above example) and in the single corresponding counter (L_9). We can safely assume this to be a rare case, and hence having to discard that one readout will not perceivably reduce the number of valid experimental readouts in practice. Hence, we decided to use non-radhard LFSR counters in the interest of having more area available for target circuits.

5.4 SET Analysis – Inverter Tree

The purpose of the SET injection experiments presented in this section is to verify, by means of simulation, that the proposed architecture indeed works up to our expectations. We also performed experiments on varying the charge from 50fC - 450fC. All the SETs (with charges higher than 150fC) injected in the first, second and third stages of the inverter tree propagated to the last stage. Some injected SETs (charges lower than 150fC) did not propagate all the way to the output node, showing no record of SETs in some of the counters. This indicates that some kind of masking indeed occurred[2].

5.4.1 Static Mode

We conducted a series of experiments where we injected SETs in the architecture as follows:

- SET was injected in only one inverter or counter – location of the origin of the fault was traceable
- SETs were injected in either two inverters, or two counters or one inverter $\&$ one counter at different time intervals – location of the origin of the fault was still traceable for most of the scenarios
- SETs were injected in three component of the inverter tree – exact location of the origin of the fault may not be traceable

Based on the design analysis presented in Sec. 5.2.1, and supported by the SET injection experiments we created a fault dictionary that would provide us an immediate mapping from a set of observed counter values to the location(s) of the SET(s) that caused it. Accordingly, our dictionary (shown in Tables 5.6, 5.7) has two columns, namely "observed syndrome" and "location of faults". The columns L_1, L_2, ... , L_{14}, L_{15} indicate the individual values of the counters observed for a particular particle strike that is indicated in column "location of faults". When there are no transitions recorded by the counter or when the counter is not affected by any particle strike, it is indicated as $\surd$. When an SET transition is recorded by the LFSR

[2]It still needs to be verified that this masking actually always occurs in the inverters and not only in the counters, or that those undesired cases can be identified

it is indicated as $+$, and two SET transitions recorded by the LFSR is indicated as $++$.

We present two scenarios in Table 5.6: no-faults, and single fault. When there are no SET hits in the target or the measurement circuits, then the counters will not record all SETs. This is our base case. Table 5.7 presents the double fault scenario. For the single fault scenario all SETs in the inverters are presented in the table. We do not present any data about the single faults in LFSR as it is quite obvious. Note that the presented syndromes correspond to the successful propagation of SETs, i.e. without masking.

Let us take into consideration the SET in I_1. If this SET successfully made it through stage 3 but then became too small to be recognized by the fourth stage, then it would just be recorded by the counters L_1, L_2, L_3, L_4, L_5, L_6, and L_7, while the counters in the last stage (L_8...L_{15}) would not show any effect. Based on this syndrome we would be able to say what happened exactly in this scenario. Overall we can conclude that all the single faults in any component would result in unique syndromes.

For the double fault scenario, we determined the syndromes for all combinations of SET hits in the architecture, but presenting all the 435 combinations of faults in the table costs too much space, hence we only present a few important scenarios in Table 5.7. The most important observation here is that the faults affecting the target inverters (including double faults within itself) again yielded unique syndromes. Some of the double faults within the combination of the counters and the targets may not be correctly interpreted.

To illustrate the proposed architecture, let us look at a few examples:

- We can observe from the scenarios (I_8, L_8) and (L_8) that the same counter is affected by the SETs. Hence, we cannot distinguish a double fault from a single fault. There are eight such scenarios.

- For the double fault scenario (I_4, I_8) we can observe that (L_4, L_8, L_9) counters record the SETs. Also note that the L_8 counter recorded two SET transitions. Note that if the SET in the inverter I_4 is weak and it may not fully propagate in the fork, while partially propagating to L_9 and not to L_8. Then this double fault scenario would be classified as a single fault scenario I_4.

- Take into consideration the scenario (I_1, L_1): we can notice that all the counters record the SETs, and since the counter L_1 is corrupted we could also classify this scenario as (I_2, I_3, L_1)

From the above illustrations we can conclude that weaker SETs would be a problem for our architecture to locate the origin of fault and trace the path of SET propagation. We can also conclude that some double faults can be classified as single faults, while some can be classified as triple faults. The real question that arises in here is the probability of an SET occuring in the target circuit and the subsequent counter that monitors the SET in the target. Note that this is quite improbable if we scramble the measurement counters in the architecture.

Table 5.6: Fault Dictionary

Observed Syndrome															Location of Faults
L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	
No Fault Scenario															
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	− − −
Single Fault Scenario															
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	I_1
√	+	√	+	+	√	√	+	+	+	+	√	√	√	√	I_2
√	√	+	√	√	+	+	√	√	√	√	+	+	+	+	I_3
√	√	√	+	√	√	√	+	+	√	√	√	√	√	√	I_4
√	√	√	√	+	√	√	√	√	+	+	√	√	√	√	I_5
√	√	√	√	√	+	√	√	√	√	√	+	+	√	√	I_6
√	√	√	√	√	√	+	√	√	√	√	√	√	+	+	I_7
√	√	√	√	√	√	√	+	√	√	√	√	√	√	√	I_8
√	√	√	√	√	√	√	√	+	√	√	√	√	√	√	I_9
√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	I_{10}
√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	I_{11}
√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	I_{12}
√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	I_{13}
√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	I_{15}

Table 5.7: Fault Dictionary

Observed Syndrome															Location of Faults
L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	
Double Fault Scenario															
+	++	+	++	++	+	+	++	++	++	++	+	+	+	+	I_1, I_2
+	+	+	++	+	+	+	++	++	+	+	+	+	+	+	I_1, I_4
+	+	+	+	+	++	+	+	+	+	+	++	++	+	+	I_1, I_6
√	+	+	+	+	+	+	+	+	+	+	+	+	+	+	I_2, I_3
√	+	√	+	+	+	√	+	+	+	+	+	+	√	√	I_2, I_6
√	√	+	+	√	+	+	+	+	√	√	+	+	+	+	I_3, I_4
√	√	+	√	√	+	++	√	√	√	√	+	+	++	++	I_3, I_7
√	√	+	√	√	+	+	√	√	+	√	+	+	+	+	I_3, I_{10}
√	√	+	√	√	+	+	√	√	+	+	+	+	+	+	I_3, I_{11}
√	√	√	+	√	√	√	++	+	√	√	√	√	√	√	I_4, I_8
√	√	√	+	√	√	√	+	++	√	√	√	√	√	√	I_4, I_9
√	√	√	√	+	√	√	√	√	++	+	√	√	√	√	I_5, I_{10}
√	√	√	√	+	√	√	√	√	+	++	√	√	√	√	I_5, I_{11}
√	√	√	√	+	√	√	√	√	+	+	+	√	√	√	I_5, I_{12}
√	√	√	√	+	√	√	√	√	+	+	√	+	√	√	I_5, I_{13}
√	√	√	√	√	+	√	√	√	√	√	++	+	√	√	I_6, I_{12}
√	√	√	√	√	+	√	√	√	√	√	+	++	√	√	I_6, I_{13}
√	√	√	√	√	+	√	√	√	√	√	+	+	+	√	I_6, I_{14}
√	√	√	√	√	+	√	√	√	√	√	+	+	√	+	I_6, I_{15}
√	√	√	√	√	√	+	√	√	√	√	√	√	++	+	I_7, I_{14}
√	√	√	√	√	√	+	√	√	√	√	√	√	+	++	I_7, I_{15}
√	√	√	√	√	√	√	+	+	√	√	√	√	√	√	I_8, I_9
√	√	√	√	√	√	√	√	+	√	+	√	√	√	√	I_9, I_{11}
√	√	√	√	√	√	√	√	√	+	+	√	√	√	√	I_{10}, I_{11}
√	√	√	√	√	√	√	√	√	√	+	√	√	√	+	I_{11}, I_{15}
√	√	√	√	√	√	√	√	√	√	√	+	√	+	√	I_{12}, I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	+	+	√	I_{13}, I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	I_{14}, I_{15}

Ultimately, we can conclude from the observations and the fault dictionary provided in Tables 5.6 and 5.7 that the proposed architecture works fine for both single and double fault scenarios, for which it can locate the origin of the fault.

We did not include triple fault scenarios in our analysis in here. Our preliminary observation from the SET injection experiments is that we can reliably detect the occurrence of all triple faults. Furthermore, we do not expect to have triple faults within a single read out such that we have no usable data from this architecture.

5.4.2 Dynamic Mode

In the dynamic mode we will steer activity in the input at a frequency of 100MHz. Hence, the output states of the inverter will keep toggling "low" and "high"; instead of being "low" or "high" throughout the experiment.

In the first set of experiments we injected only one SET per component (that includes 22 counters and 15 inverters) at a time. As expected, we were able to locate the origin of fault with the help of counters in these scenarios. We also injected two SETs, in the the whole architecture covering a variety of cases like double faults within the same component, faults in two different counters, or in two different inverters, and faults in one counter and one inverter at the same time. In all those cases we could verify the anticipated behavior. Not surprisingly, for triple faults we could not identify the origin of the SET in all cases.

Based on the design analysis presented in Sec. 5.2.1, and supported by the SET injection experiments from Sec. 5.4 we created a fault dictionary to provide us an immediate mapping from a set of observed counter values (called "syndrome" again) to the location(s) of the SET(s) that caused it. Accordingly, our dictionary (shown in Table 5.8) has two columns, namely "observed syndrome" and "location of faults". The columns L_1, L_2, ... , U_{18}, U_{19} indicate the individual values of the counters observed for a particular particle strike that is indicated in column "location of faults". When there are no transitions recorded by the counter or when the counter is not affected by any particle strike, this is indicated as $\surd$. When an SET transition is recorded by the LFSR it is indicated as $+$ (to simplify the explanation we refer to the static mode of operation here), and the SETs recorded by the UDCs are indicated as $+/-$ (i.e., an up or down transition).

In the Tables 5.8, 5.9 and 5.10 we consider three scenarios : no-faults, single fault and double faults. When there are no SET hits in the target or the measurement circuits, then the counters will not record any SETs. This is our reference case.

For the single fault scenario all SETs in the inverters are presented in the table. Please note that the presented syndromes correspond to the successful propagation of SETs, i.e. without masking. In case of masking an SET will not be recorded any more in a later stage. As an example, let us consider an SET in I_3. If successfully propagated the syndrome is as presented in the table.

However, if this SET successfully made it through stage 3 but then became too small to be recognized by the fourth stage, then it would just be recorded by the counters L_3, U_1, U_3, U_4, U_5, and U_6, while the counters of the last stage (U_8...U_{19})

would not show any effect. Based on this (new) syndrome we would be able to say what happened exactly in this scenario, and of course we can extend the table accordingly, which is not done here for the sake of brevity. For the same reason the table does not show the syndromes for faults in the counters either, as their coverage within our architecture has already been discussed in Section 5.2.1. Overall, in the context of elaborating the fault dictionary, we found good confirmation that all single faults in any component result in unique syndromes and are hence straight forward to identify. Interestingly, all these syndromes differ in at least three counters. This led us to the conclusion that any SET in one target circuit and one counter will also yield a unique syndrome (as long as only double faults are considered).

To continue with the double fault scenario, we calibrated the syndromes for all combinations of SET hits in the target circuits in an identical fashion, but due to space restrictions we only present a few important scenarios in Tables 5.9 and 5.10. The most important observation here is that every combination (in total 120) of faults affecting the target inverters (including double faults within itself) again yielded a unique syndrome.

To illustrate the beauty of the proposed architecture, let us look at a few examples:

- From the scenarios (I_2, I_4) and (I_2, I_5) in the table. 5.9 we can observe that some counters are equally affected by both of these SET effects. However, we can notice differences in U_3, U_4, U_5, U_6, U_7, U_9, U_{10}, U_{11}, U_{12}, U_{13}, U_{15}, which all show non-matching effects. This demonstrates the advantage of using the up/down counters in conjunction with the symmetry of the tree structure.

- A similarly argument holds for the scenarios (I_4, I_8) and (I_4, I_9) shown in the table: we can observe that again some counters equally record both these SETs, and again the syndromes clearly differ, this time in U_8, U_9, U_{10}, U_{11}, U_{12}. We can observe the same for (I_7, I_{14}) and (I_7, I_{15}).

- Taking a look at the scenario for (I_8, U_8), we can observe that the SETs will be recorded only in the counters U_9, and U_{10}, as U_8 is faulty and has to be discarded. From the down transitions in both U_9, and U_{10} we can still correctly conclude that the fault occurred in I_8, thereby confirming that another fault occurred in U_8.

- The common observation from the scenarios (I_8, I_{12}), (I_9, I_{11}), (I_{10}, I_{11}), (I_{11}, I_{15}), (I_{12}, I_{14}), (I_{13}, I_{15}) and (I_{14}, I_{15}) is that they all have four different counters recording the SETs, but not more than four. At the same time one can also observe that there are variations shown by at-least three counters in each scenario with respect to the other scenarios.

Overall we can conclude from the observations and the fault dictionary provided in Tables 5.8, 5.9, and 5.10 that the proposed architecture works fine for both single and double fault scenarios, for which it can also locate the origin of the fault.

We did not include triple fault scenarios in our analysis so far, as they are beyond our fault hypothesis (recall that we can adjust the read-out periods to the flux accordingly to make multiple faults reasonably improbable during that interval). Still it is interesting to observe how our architecture actually behaves under triple faults. Our observation is that we can reliably detect the occurrence of all triple faults. The identification of their location, however, is not possible any more – there will be two or more possible interpretations (i.e. matching syndromes for different locations). For example, faults in I_8, U_8, U_9 show the same syndrome as those in U_8, U_9, U_{10}.

5.5 Summary

We presented the target and the measurement architectures chosen for understanding SET propagation effects in digital circuits. We validated the infrastructure by means of SET injection experiments using the state-of-the-art current model. Our simulations confirmed that single SETs in the target will be observed by multiple counters at multiple locations. We have also systematically developed a fault dictionary, which evidently proves that this infrastructure allows us to handle and identify all expected fault scenarios, including those where a counter is affected.

Table 5.8: Fault Dictionary for Inverter Tree

Observed Syndrome																						Fault Location
L_1	L_2	L_3	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}	U_{19}	
No Fault Scenario																						
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	− − −
Single Fault Scenario																						
+	+	+	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	I_1
√	+	√	−	√	+	+	+	+	√	√	√	−	√	−	−	√	−	√	√	√	√	I_2
√	√	+	+	√	−	−	−	−	√	√	√	+	√	+	+	√	+	√	√	√	√	I_3
√	√	√	√	√	√	+	√	+	+	√	−	−	−	−	√	√	√	√	√	√	√	I_4
√	√	√	√	√	+	√	+	√	−	√	+	√	+	√	−	√	−	√	√	√	√	I_5
√	√	√	√	+	√	√	−	−	√	√	√	+	√	+	√	√	√	√	√	−	−	I_6
√	√	√	√	−	−	−	√	√	√	√	√	√	√	√	+	√	+	√	√	+	+	I_7
√	√	√	√	√	√	√	√	√	√	−	−	−	√	√	√	√	√	√	√	√	√	I_8
√	√	√	√	√	√	√	√	√	√	+	√	√	−	−	√	√	√	√	√	√	√	I_9
√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	−	−	√	√	√	√	√	I_{10}
√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	+	−	√	√	√	√	I_{11}
√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	√	√	−	√	−	√	I_{12}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	+	√	√	−	I_{13}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	√	−	+	√	I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	+	√	+	I_{15}

Table 5.9: Fault Dictionary for Inverter Tree

Observed Syndrome																			Fault Location
L_1	L_2	L_3	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}	U_{19}	
Double Fault Scenario																						
+	+2	+	−	√	+	+	+	+	√	√	√	−	√	−	−	√	−	√	√	√	√	I_1, I_2
+	+	+	√	√	√	+	√	+	+	√	−	−	−	−	√	√	√	√	√	√	√	I_1, I_4
+	+	+	√	√	+	√	+	√	−	√	+	√	+	√	−	√	−	√	√	√	√	I_1, I_5
+	+	+	√	+	√	√	−	−	√	√	√	+	√	+	√	√	√	√	√	−	−	I_1, I_6
√	+	√	−	√	+	+2	+	+2	+	√	√	−	−2	−	√	√	−	√	√	√	√	I_2, I_4
√	+	√	−	√	+2	+	+2	+	−	√	+	−	+	−	−2	√	−2	√	√	√	√	I_2, I_5
√	+	+	+	+	−	−	−2	−2	√	√	√	+2	√	+2	+	√	+	√	√	−	−	I_3, I_6
√	√	+	+	−	−2	−2	−	−	√	√	√	+	√	+	+2	√	+2	√	√	+	+	I_3, I_7
√	√	+	+	√	−	−	−	−	√	−	−	√	√	+	+	√	+	√	√	√	√	I_3, I_8
√	√	+	+	√	−	−	−	−	√	+	√	+	−	√	+	√	+	√	√	√	√	I_3, I_9
√	√	√	√	√	√	+	√	+	+	−	−2	−	−	√	√	√	√	√	√	√	√	I_4, I_8
√	√	√	√	√	√	√	+	+	+	−	−	−2	−2	√	√	√	√	√	√	√	√	I_4, I_9
√	√	√	√	√	+	√	+	−	√	+	√	+	√	−	√	√	√	√	√	√	√	I_5, I_{10}
√	√	√	√	√	+	√	+	√	−	√	+	√	+	√	−	√	−	√	√	√	√	I_5, I_{11}
√	√	√	√	√	+	√	+	√	−	√	+	√	+2	√	−	+	−2	√	√	√	√	I_5, I_{12}
√	√	√	√	√	+	√	+	√	−	√	+	√	+	√	−	√	−	√	√	−	√	I_5, I_{13}

Table 5.10: Fault Dictionary for Inverter Tree

Observed Syndrome																						Fault Location
L_1	L_2	L_3	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}	U_{19}	
Double Fault Scenario																						
√	√	√	√	+	√	√	−	−	√	√	√	+2	√	+	√	√	√	−	√	−2	−	I_6, I_{12}
√	√	√	√	+	√	√	−	−	√	√	√	+	√	+2	√	√	√	+	√	−	−2	I_6, I_{13}
√	√	√	√	+	√	√	−	−	√	√	√	+	√	+	+	√	√	√	−	√	−	I_6, I_{14}
√	√	√	√	+	√	√	−	−	√	√	√	+	√	+	√	√	+	√	+	−	√	I_6, I_{15}
√	√	√	√	−	−	−	√	√	√	√	√	√	√	√	+2	√	+	√	−	+2	+	I_7, I_{14}
√	√	√	√	−	−	−	√	√	√	√	√	√	√	√	+	√	+2	√	+	+	+2	I_7, I_{15}
√	√	√	√	√	√	√	√	√	√	√	−	−	−	−	√	√	√	√	√	√	√	I_8, I_9
√	√	√	√	√	√	√	√	√	√	−	−	√	√	√	√	√	√	−	√	−	√	I_8, I_{12}
√	√	√	√	√	√	√	√	√	√	+	√	√	√	−	√	+	−	√	√	√	√	I_9, I_{11}
√	√	√	√	√	√	√	√	√	√	+	√	√	−	−	√	√	+	√	+	√	+	I_9, I_{15}
√	√	√	√	√	√	√	√	√	√	√	+	√	+	√	−	√	−	√	√	√	√	I_{10}, I_{11}
√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	+	√	√	+	√	+	I_{11}, I_{15}
√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	+	√	√	−	−	√	√	I_{12}, I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	+	√	√	+	−	+	−	I_{13}, I_{14}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	√	+	+	+	√	√	I_{13}, I_{15}
√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	+	√	+	√	√	+	+	I_{14}, I_{15}

CHAPTER 6

Pulsewidth Measurement of SETs

The objective of this chapter is to measure the pulsewidth of a particle strike in a digital circuit when exposed to an uncontrollable radiation. In other words we need to record the SET pulse duration for different target circuits. In order to do so, the measurement architecture we propose should start measuring the pulsewidth from the point of impact (measurement should begin when the target is hit by a particle strike) until the decay of the charge (measurement should stop when the energy created by the particle is depleted). As we are targeting a purely digital ASIC we cannot host any analog sense amplifiers to accurately measure the SET duration, hence must come up with a creative way to do the same in the digital domain. Note that the infrastructure that we are building should be immune to particle strikes, else it would be recording erroneous data. Similar to our previous measurement architectures we prefer using a non rad-hard infrastructure for recording pulse widths. Still, choosing the target circuit is of extreme significance in here, hence they must satisfy the basic requirements given below:

- Simple – We need not use complicated circuits such as adders, multipliers, etc., as targets; because they do have a higher logic delay which could mask the SETs. Therefore we must use simple targets such as the basic combinational and sequential circuits.
- Capacitive Load – For benchmarking all the basic gates we must make sure they all have the same capacitive load.
- Static operation – As a first step we are interested in gathering information about the SET pulsewidth in the targets when they are in the static mode, hence we will not apply stimuli in the input of the targets. The inputs would either be connected to power or ground.

Based on the above requirements we chose to use the standard logic gates, D Flip-flop and Muller C-element with unit load as our target circuits. Now, the real challenge in here is to build an infrastructure that converts the analog pulse shape into a digital pulse and help us compute the approximate SET duration.

6.1 Background

Over the past years, quite some research has been dedicated to SET pulsewidth measurement in digital circuits, see e.g. [148] for an overview. Among the reported results there are several approaches for the on-chip measurement of SET pulse widths. Nicolaidis et al. [111] proposed a circuit that measures the duration of SETs at the outputs of logic gates by using a chain of cell copies, in which each copy is monitored by a latch. This circuit could be used to characterize a cell library.

Eaton et al. [41] developed a new SET test structure based on a variable temporal latch. The structure they built is capable of passing or filtering SET events generated in external combinational logic of a pre-programmed width. This technique allows them to measure the width of an SET event by incrementally increasing the pulsewidth "filter" until they transition from passing the transient to completely blocking the event. They do not rely on any external probing techniques and they are the first to measure SET pulsewidths using standard CMOS gates in a deep submicron process. Benedetto et al. [20] proposed an extension to [41] to determine the distribution of SET pulse widths created by particles with a given *linear energy transfer* (LET) value.

Baze et al. [17] built an architecture for characterizing SETs in logic gates. It employs a low pass filter using a guard gate that controls the minimum SET pulse width, combined with an asynchronous latch that captures and records SETs. Narasimham et al. [107] proposed a self-triggered structure for measuring SET pulse width for a 1.5μm process in increments of one inverter delay and conducted laser based injections. Yanagawa et al. [160] extended this approach by developing an on-chip self-triggering flip-flop to measure the SET pulse widths and applied it for heavy-ion-induced SET pulse measurements. Using this latter measurement architecture, Narasimham et al. [105] investigated the distribution of SET pulse widths produced by heavy ions in $130nm$ and $90nm$ CMOS technologies.

The common factor in all these approaches is a fairly complex measurement architecture for capturing and recording SETs. Unlike these approaches, our solution needs to:

a Be area efficient (to retain as much of the available die area as possible for radiation target circuits)

b Be radiation tolerant (as it is exposed to the same radiation as the target circuits)

c Provide a reasonable resolution for SET lengths in the 1 ns-range.

In [151] we proposed a suitable, purely digital infrastructure for measuring SET pulse widths in logic gates. We validated our infrastructure with SET injection experiments and provided radiation tolerance to the counters using redundancy. The limitation of the infrastructure, however, is that the counters must be read out before the next SET occurs; otherwise no usable data about the pulse widths will finally be read out. In [150], we extended the infrastructure to record multiple SETs. In

this architecture, however, the counters we used do not have any protection against radiation, making them vulnerable to even a single SEU. Our goal is to augment the architecture in an efficient way to make the counters SEU-tolerant.

6.2 Measurement Infrastructure Requirements

The envisioned scenario is that of long-term monitoring experiments, with the ASIC being permanently exposed to irradiation, and the results being periodically read out by a host device (that is protected from radiation). Our aim is to build an on-chip measurement infrastructure that allows collecting as much information as possible on SET pulse widths seen on a given node of our target circuit under radiation. In more detail, this breaks down into the requirements that have already been presented in Sec. 1.3:

Req. 1.3 (b) Efficient use of recordings: SEU-tolerant measurement infrastructure

Req. 1.3 (c) High-quality measurements: good temporal resolution

Req. 1.3 (d) Efficient use of exposure time: continuous recording

Req. 1.3 (e) Efficient use of area: lean infrastructure

One immediate consequence of Requirements (a), (b) and (e) is that we need a fully digital implementation. While the setup based on analog amplifiers as presented in [68] allows for a very detailed post-processing of the pulse shapes, those amplifiers consume a large area and are very sensitive to radiation. So, while they are very useful for microbeam experiments, they are not applicable for our purpose.

Another consequence of (e) is that traditional radiation hardening by sizing is not an option for attaining (b). While it provides high robustness, the area penalty it incurs for a $90nm$ design is prohibitive for our purpose, leaving hardly any space for the actual target cells and a negligible probability for these being hit. Moreover, its speed limitations would severely impair the achievable time resolution. Therefore, we are looking into alternative approaches like in [149, 148].

In general, we observe an inherent trade-off between Requirements (b) and (e): Measures for increasing the infrastructure's SEU-tolerance typically also increase its area. For a given average number of SETs we want to observe in the target, we have a corresponding average number of SEUs in the measurement infrastructure, where the proportionality factor is essentially the area ratio of the measurement infrastructure versus the target. Consequently, the larger the infrastructure gets (even if for the sake of SEU-tolerance), the higher the demands on its SEU-tolerance level. So it may well turn out that a smaller solution with a lower degree of SEU-tolerance is better than a more elaborate one. Finding a good trade-off here and carefully leveraging all available redundancy will be one focus of our further analysis.

In fact, there is also a contradiction between (d) and (e), as the on-chip storage implied by (d) impairs (e) by increasing the area.

A related trade-off in the context of "efficient use of results" concerns the discarding of SET recordings: Clearly we want to collect valid results only. Considering the statistic nature of radiation parameters, however, this will not be fully possible in practice: There is always a non-zero probability for an excessive number of SEUs in the measurement infrastructure that cannot be corrected or at least detected with an affordable amount of redundancy. However, the residual erroneous SET recordings resulting from such cases must be kept reasonably close to zero. This calls for good *error detection* capabilities in the infrastructure, and for a strategy "discard in case of doubt".

At the same time, we do not want to unnecessarily discard precious read-outs, so we also need *error correction* capabilities. This demands for a higher degree of redundancy and hence collides with Requirement (e). Still, error correction capabilities may be a clever investment in terms of (d). And like above there may be rare adverse multiple error scenarios in which the correction may produce erroneous results (due to assuming a different, more probable scenario that may have created the observed effect). A strict "discard in case of doubt" policy may be too rigorous here by unnecessarily reducing the number of samples.

Finding a good solution here is a highly non-trivial problem that will be addressed in the further analysis as well.

6.3 Baseline SET Pulse-width Measurement Architecture

6.3.1 Principle

The basic architecture of our circuit is shown in Fig. 6.1. Its key components are (1) a *ring oscillator* formed by an inverter loop, (2) a *switch* that closes the loop (and hence enables oscillation) for the duration of the SET, and (3) a *counter* that records the number of pulses produced during that window. By multiplying the counter value with the oscillator period (which is determined in a calibration phase), SET pulsewidths can be measured.

6.3.2 Design space

Within this architectural concept, our design space comprises the following choices:

1. **Number of stages in the ring oscillator:** Obviously, the oscillator (refer Fig. 6.1) period limits the temporal resolution of our measurement, so the frequency must be high. At the same time, however, the counter's maximum speed needs to be considered, otherwise pulses will be lost. Consequently, the number of ring oscillator stages must be carefully tuned to the capabilities of the chosen counter.

2. **Counter implementation:** Following the above argument, a very fast counter is required. The choices we consider comprise LFSRs and Up/Down counters.

3. **Switch placement:** There are several options for placing the switch within the ring oscillator (relative to the tap for the counter). An appropriate choice is crucial for a fast and stable operation of the circuit. In addition to the switch required for controlling the oscillation loop, another switch may be employed to ensure a fast detaching of the counter from the ring oscillator. The options we consider are shown in Figure 6.1; they will be explained and motivated below.

4. **Radiation tolerance method:** Recall that the whole test chip, and hence also our measurement infrastructure, is intended to be operated in an ambient radiation environment during the experiments. This requirement considerably impacts all our design choices. For example, the resulting choice needs to protect the counter values from SEUs, which has a significant impact on suitable counter implementations.

6.3.3 Switch placement

We assume an active-low target circuit output, i.e., nominal high output with a negative SET pulse in case of a particle hit. This output directly controls the select input s of our switch, where $s = 0$ closes the loop. Of course, the dual case of an active-high output can be easily covered with an inverted polarity of the switch control (i.e., close switch for $s = 1$). Preliminary simulations showed that the floating output of a simple switch (transmission gate) causes problems in the open state. Therefore, we efficiently implemented the switch from a multiplexer that uses transmission gates, which either closes the loop or outputs low when the loop is open.

From the numerous options for placing the switch that we tried out, Figure 6.1 shows four options that we consider to be representative:

- **Architecture (I):** Our preliminary analysis showed that with two switches in place, it takes a ring of 5 inverters to reduce the ring oscillator frequency to the point where it can be safely accommodated by the up/down counters. Hence, we employed two switches in the loop, one (S_1) right after the counter, and another one (S_2) with a distance of three inverters in the loop from (S_1). The switches placements allow fast and reliable control of the ring oscillator, however, SETs in the two inverters of the forward path will unduly increment the count.

- **Architecture (II):** The structure is essentially the same as in (I), but the counter now taps the loop directly after the switch. The two switches employed in the loop are placed such that, one (S_1) is placed right before the counter, and another one (S_2) is placed at the opposite end of the loop. More

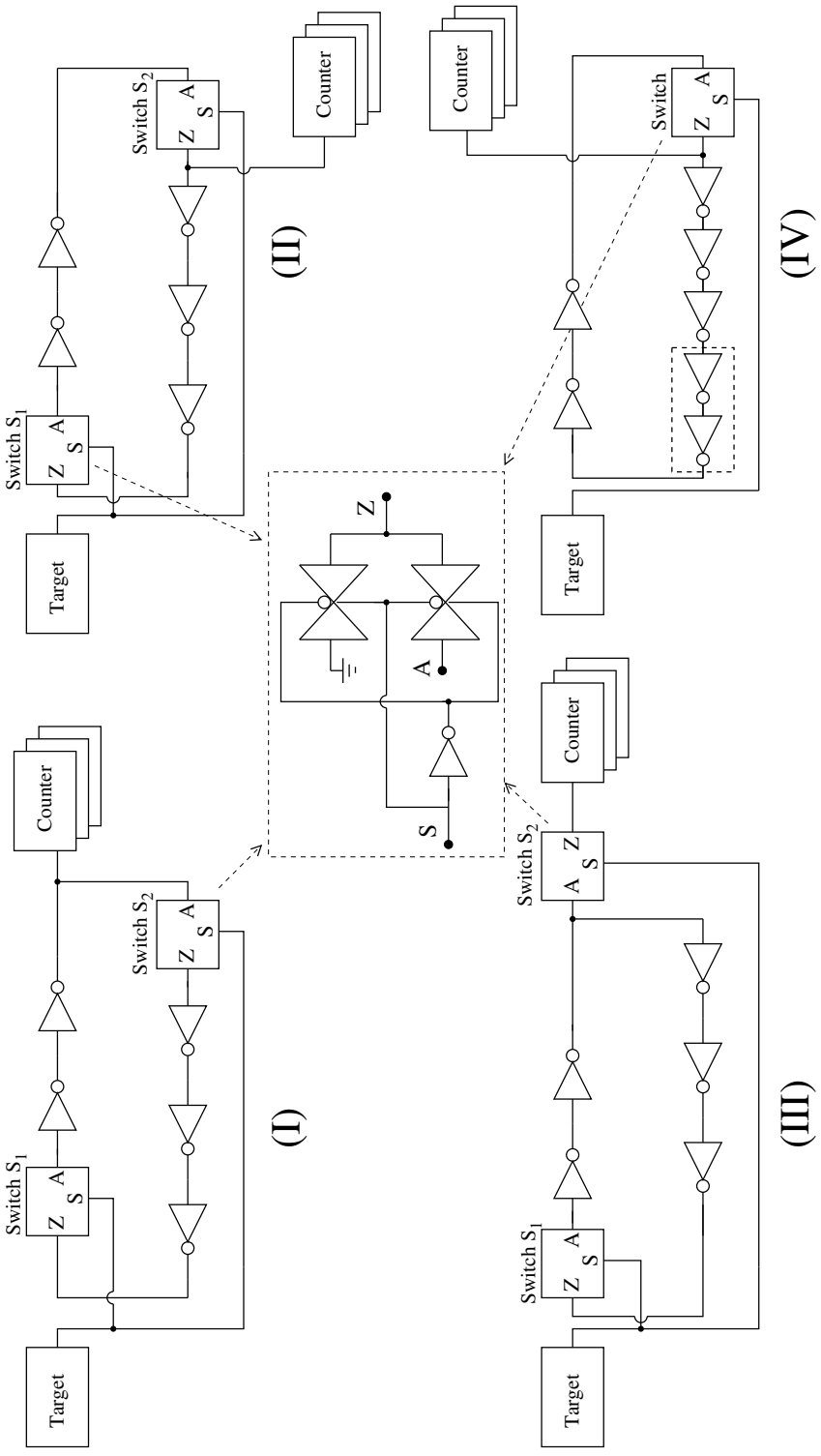


Figure 6.1: Baseline Architecture to Measure SET Lengths

specifically, S_2 is placed such that an even number of inverters is between its output and the input of S_1. The switch masks SETs in the forward inverters as well.

- **Architecture (III):** We employed two switches, of which only one ($S1$) is used to break the loop, while the other (S_2) is dedicated to detach the counter from the loop. Compared to II we moved the second switch out of the loop, thereby masking potential SETs in the loop from the counter.

- **Architecture (IV):** Only one switch is employed in this architecture. We already know that with two switches in place, it takes a ring of 5 inverters to reduce the oscillator frequency to safely record the data in the counters. Hence, we must adjust the frequency for the current architecture by adjusting the inverters in the oscillator. Compared to II, the left switch is removed, so a single switch now serves both purposes, namely breaking the inverter loop and disconnecting the counter. We have to conduct extensive simulations in this architecture to verify whether a single switch is enough to control the operation of the loop with sufficient temporal precision and signal integrity.

6.3.4 Radiation tolerance

In our experiments, the particle flux can be controlled such that we only need to care about single SETs per device (within a measurement interval, after which the measurement data are read out anyway). Our measurement circuit hence needs to tolerate single faults only.

As already mentioned, attaining radiation tolerance by sizing (i.e., radiation hardening)—as it is usually employed in other applications—is not an option, as it severely degrades switching speeds: High temporal resolution and hence high speed is among the most important properties of our circuit. Hence, we must rely on architectural means for achieving fault-tolerance.

The most critical component is the *counter*, no matter which implementation we finally choose: Due to its large internal state, it is particularly prone to SEUs; hence, in our first solution we triplicate it and read out all the instances to avoid the need for a rad-hard voter.

For the *inverters* forming the ring oscillator loop, we can distinguish two cases:

- During the active time (loop closed during an SET caused by a hit in the target circuit), all inverters are sensitive in principle; a concurrent hit of an inverter is sufficiently improbable due to our single-fault assumption, however. But, it is of immense interest to us to know such a probability of particle strike (refer Sec. 6.8 for probability analysis).

- During the idle time (loop open), an SET originating from a particle hit in an inverter may lead to an unwanted increase of the counter, provided there is a path from the inverter output to the counter even when the switches are open. By inspection of Figure 6.1, we can identify two “critical” inverters

(the ones on top) in Architecture I, while the careful switch placement effectively blocks all such SETs from the counter in all other cases. Note that the probability of such a scenario can be made flimsy by reducing the radiation exposure time to the ASIC. Moreover, the critical area of the inverters is very small, and hence, no need for further fault-tolerance measures.

Similarly, there is no need to protect any of the two *switches* either: They comprise 6 transistors only, of which only 2 are sensitive during the idle time.

6.3.5 SET Analysis

The goal of this section is to provide a brief analysis on all the measurement architectures presented above. We will test all the baseline architectures to verify which one of them is the best suited for our purpose. Based on this outcome the best architecture would be chosen and used for recording *multiple-event transients* (METs).

We evaluate the different design options using the setup presented in Sec. 2.4. All our simulation experiments were conducted using HSPICE and Cadence Spectre simulators. Our aim is to evaluate which combination of architecture and counter performs best, and our criteria are (a) temporal resolution[1] and (b) faithful recording of the actual oscillations of the ring oscillator (which we manually count in the simulation output for reference) in the counter.

The combinations of 4 architectures and 3 counters (one LFSR and two Muller pipelines MP_1 resp. MP_2 with weak-feedback resp. Van-Berkel Muller C-element) considered are listed in Table. 6.1. Using an inverter as the target circuit, the number of oscillator periods recorded in the counter (vs. their actual number) for different injected charges (hence pulsewidths) is shown. In preliminary simulation runs (without SET injection), we found out that a ring oscillator with 3 inverters in the loop is too fast for the counter, so we need at least 5. In Architecture (IV), we even needed 7 in order to compensate for the lacking switch. As a next step, we performed the SET injection experiments. We varied τ_F to attain charges in the range from 90fC to 1.06pC, which we identified as realistic and useful, while we kept the τ_R and I_0 as constant. For example, to achieve an injected charge of 90fC, we chose the parameters τ_R = 10ps, τ_F = 100ps and I_0 = 1mA. The entries in Table 6.1 show the counts recorded by the different counters in the 4 architectures, for different injected charges (Q_{SET}), together with the reference (in parenthesis). Note that the reference count changes with the architecture and counter implementation, since loop delays (inverters plus switches) as well as counter input characteristics (load) impact the frequency of the ring oscillator.

Architecture (I): LFSR and MP_2 work reliably, with the latter yielding a higher oscillation frequency and hence a better resolution (approx. 100ps) than MP_1. By contrast, MP_1 fails from τ_F=400ps onwards, as it does not faithfully count all tran-

[1]Of course, temporal resolution can only be judged in detail after physical design, but our pre-layout simulations still give us a good first indication.

Table 6.1: Recording capabilities (vs. reference count) of Architectures I–IV for different charges injected in an inverter

SET	Architectures											
Q_{SET}	(I)			(II)			(III)			(IV)		
in fC	LFSR	MP_1	MP_2	LFSR	MP_1	MP_2	LFSR	MP_1	MP_2	LFSR	MP_1	MP_2
MP_1: Weak Feedback Muller Pipeline; MP_2: Van Berkel Muller Pipeline												
Target : Inverter												
90	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)
190	2(2)	2(2)	2(2)	2(2)	2(2)	2(2)	2(1.75)	2(2)	2(2)	2(2)	2(2)	2(2)
290	2(2.5)	3(3)	3(3)	3(2.6)	2(3)	3(3)	2(2.25)	3(3)	3(3)	2(2.5)	2(3)	3(3)
390	3(3)	3(4)	4(4)	3(3.4)	3(4)	4(4)	3(3)	3(3.7)	4(4)	3(3.25)	3(4)	4(4)
490	4(4)	4(4.7)	5(5)	4(4)	4(5)	5(5)	4(4)	3(4.5)	5(5)	4(4)	3(5)	5(5)
590	4(4.5)	4(5.2)	6(5.6)	5(5)	4(5.5)	6(5.5)	4(4.5)	4(5.2)	5(5.3)	5(4.6)	3(5.5)	6(6))
690	5(5)	5(6)	6(6)	6(5.7)	4(6.5)	6(6.25)	5(5)	5(6)	6(6)	5(5.3)	4(6.5)	7(7))
790	6(6)	5(7)	7(7)	6(6.4)	5(7)	7(7.25)	6(5.6)	5(7)	7(7)	6(6)	4(7.2)	7(7.25)
890	6(6.4)	6(8)	8(8)	7(7)	6(8)	8(8)	6(6.25)	6(7.5)	8(7.7)	7(6.6)	5(8)	8(8.3)
990	7(7)	6(8.7)	9(9)	8(8)	6(8.75)	9(9)	7(7)	6(8.4)	8(8.5)	7(7.4)	5(9)	9(9.2)
1060	7(7.5)	7(9)	9(9)	8(8.4)	6(9.5)	10(9.5)	7(7.4)	7(9)	9(9)	8(8)	5(9.4)	10(9.6)

sitions. This is because the sizing requirements [132] make the weak-feedback implementation too slow.

Architecture (II): As for Architecture (I), the LFSR and MP_2 perform correctly, while MP_1 again fails. Notice, however, that there are more reference oscillations, which means that this architecture is faster than Architecture (I).

Architecture (III): The behavior of the different counters is essentially the same as above. Surprisingly, taking one switch out of the loop did not raise the oscillation frequency; the behavior is more like in Architecture (I).

Architecture (IV): Recall that we have only one switch and two extra inverters, which yields about the same speed as with the other architectures. Under these conditions, LFSR and MP_2 again work fine, while MP_1 fails.

Our first general conclusion from these experiments is that MP_1 keeps failing in all architectures, as it is too slow. So we discarded it. Second, MP_2 yields the highest oscillation frequency and hence the best resolution in all architectures; apparently it creates a smaller load on the ring oscillator than the LFSR. Also, MP_2 proved to capture shorter pulses than the LFSR, and we could observe that it works reliably even for low voltage swing (not shown here), which is not the case for the LFSR. Finally, recall that, in contrast to the LFSR, the MP allows half-cycle resolution – a considerable benefit for our purpose. The benefit of the LFSR is its higher area efficiency, its better scalability towards large count values (exponential in the number of stages, rather than linear, as for the MP), as well as its error detection capability due to its "irregular" counting sequence. In our application, however, we do not actually leverage those benefits, as we have relatively small counts and a triplicated counter anyway. These arguments clearly made us decide for MP_2.

Our analysis revealed that the choice of the architecture does not have much influence; as expected, the speed is primarily limited by the counter implementation. Still, Architecture (II) and (IV) are the most attractive candidates, as they are the fastest. Both the architectures have some pros and cons:

- One of the advantages that Architecture (IV) has over (II) is the number of inverters: should it turn out during the post-layout simulations that the counter can handle a faster oscillation as well (due to usage of an improved technology, or a reduced amount of capacitive loading), and the loop can hence be speeded up by removing two inverters, then reducing the number of inverters in the ring from 7 to 5 (Architecture (IV)) seems to be the safer option compared to going from 5 down to 3 (Architecture (II)), as the latter might suffer from lower frequency stability. One might also argue that the parasitic parameters added in Architecture (II) should provide enough frequency stability.

- Architecture (II) has an advantage over (IV) in terms of radiation tolerance: should the switch of Architecture (IV) close with a particle strike in it, then any residual signal in the oscillator could be recorded in the counter corrupting the SET data. Architecture (II) does not suffer from a similar effect make it better than (IV).

Taking these arguments into consideration, we could prefer Architecture (II) over Architecture (IV) as the frequency stability issue is not as critical as corrupted SET data. But, the final choice can be made only after verifiying these two architectures for some more target circuits.

6.3.5.1 Verification for other target circuits

The exploration of the design space presented so far has been restricted to inverters as the target circuit. This is reasonable, since the inverter is the fastest component in CMOS, and hence represents a worst case for SET measurement. Still, it is mandatory to verify our choices also for our other radiation target circuits. In the sequel, we will therefore extend our analysis to the following targets: NAND gate, Muller C-Element, and D-Flip-Flop. Since we expect longer SETs on those targets, we have extended MP_2 from a 10-bit UDC to a 40-bit UDC for this analysis.

Furthermore, recall that the chosen polarity of the switch control restricted our analysis to SETs in the NMOS so far. Using the alternative (inverted) switch control, we can also verify the ability of our approach to observe SETs in (selected) PMOS transistors as well. For a complete picture, however, still both polarities of the switch control must be provided for.

Table 6.2: Architecture (II) & (IV) – Measurement Statistics – Q_{SET}=1.06pC

Target Circuit	Architecture	Hit Transistor	Length of SET
NAND	(II)	NMOS	13(13)
	(IV)	NMOS	13(13)
Muller C-Element	(IV)	PMOS	8(8)
		NMOS	10(10)
	(II)	PMOS	8(8)
		NMOS	10(10)
D Flip-flop	(IV)	PMOS	23(23)
		NMOS	9(9)
	(II)	PMOS	23(24)
		NMOS	9(10)

Using the Architectures (IV) & (II) and the 3 target circuits mentioned above, we executed the same set of simulations with the same injected charges as listed in Table. 6.2. The outcome of the simulations perfectly matched our expectations. As an example, Table. 6.2 shows the outcome for a Q_{SET} of 1060fC (recall that this used to be the most critical case):

- For the **NAND** gate, we shorted both inputs to ground, hence we can observe only a high-to-low transition on the output (i.e., only a particle strike in an NMOS transistor), like before for the inverter target. As Table. 6.2 indicates, the SET resulting from the particle strike, however, is more pronounced here than for the inverter (13 vs. 10 cycles). Also, the count value perfectly

matches the reference, which confirms the proper operation of our approach for this target. With both the architectures we recorded the same pulse-widths.

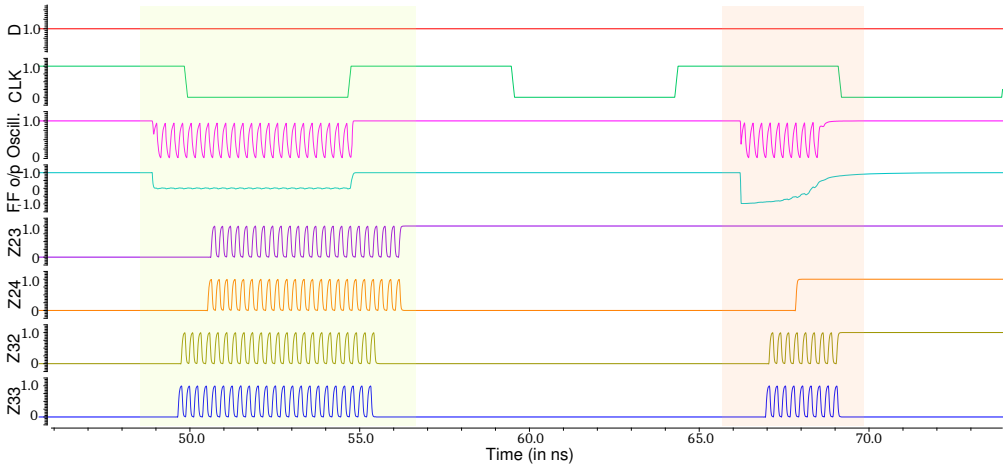
- For a Van-Berkel **Muller C-element** (MCE) as a target, both inputs were shorted to ground to obtain a high output (the MCE is inverting, cf. Figure 6.1). In this setting we can, like before, observe a particle strike in the NMOS of the output inverter as a negative pulse at the output. In addition, however, a particle hit in one of the PMOS transistors forming the P-stack also creates a negative pulse at the output. This has been confirmed by our simulations, albeit the generated SETs were weaker than NMOS SETs. Again, the count value nicely matched the reference count. Moreover, in case of the NMOS, the result (10 cycles) favorably matches that from the inverter target, which makes sense, considering that, ultimately, the target was again essentially an inverter here. Note that both the architectures showed the same effect even for the MCE.

- Finally, when using a conventional **D flip-flop** as a target, we connected the D input to the positive supply, while toggling CLK at a frequency of 100MHz. In this setting, the output Q is refreshed to high with every rising edge of CLK, where it remains during fault-free operation. First, we simulated a particle strike in the NMOS of the slave latch, i.e., directly at the output of the flip-flop. The resulting SET had a length of 10 cycles (refer to Fig. 6.2), which is comparable to the case of the inverter target again.

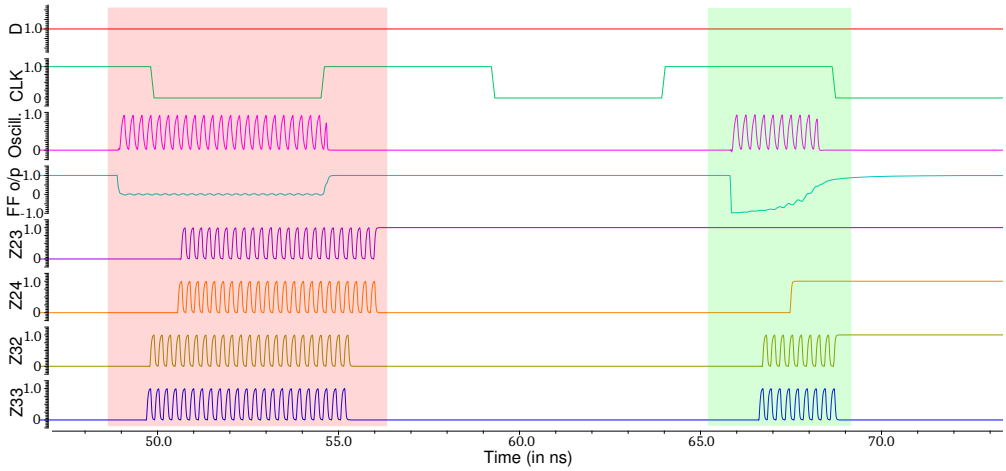
  Second, an SET was created by hitting the output inverter of the master latch, with the current source connected over the PMOS transistor. In this setting, an SET occurring right at the rising edge of CLK has the highest impact, as it creates an SEU that lasts for a complete clock period before being overwritten. In this case, however, our count value necessarily represents the clock period rather than the actual SET length. The more interesting observation here was that the SEU occurred irrespective of the applied charge. SETs in the master latch that occur after the rising CLK propagate to the output, as long as the slave is transparent (i.e., while CLK is high). They do not cause an SEU, however. Finally, if the SET in the master latch occurs right at the falling edge of CLK, it is captured by the slave, causing an SEU that lasts for half a clock period.

  Note that in Architecture (II) we can observe that there are variations in the pulsewidths w.r.t the number of transitions generated by the oscillator. Architecture (II) generates 24 transitions in the PMOS but only 23 of them are recorded by it, while Architecture (IV) generates 23 transitions and records 23. Similarly even for the NMOS, Architecture (II) reduces the number of recorded transitions by one. The reason the 24th transition is not recorded is because it was weaker than the others, hence disappeared during propagation.

Even though the transitions differ for both the architectures, they both show the same number of recorded pulsewidths. Overall, the analysis of our measurement



(a) Architecture (IV)



(b) Architecture (II)

Figure 6.2: Length of SETs in a D Flip-Flop

infrastructure confirmed that both the architectures are suitable for all our radiation target circuits: In most of the cases, the counter values matched the reference counts, and the results are plausible when compared with those observed for the inverter target. Taking into consideration the radiation tolerance we decided to opt for Architecture (II) instead of (IV).

6.4 Measurement Infrastructure for Multiple SETs

The architectures proposed above can only monitor a single SET in the DUT. If there is more than one SET in the baseline measurement architecture, then the counters will count on top of the previous count, thereby delivering spurious data. To avoid this; we *either* have to read out the counters after one SET and reset, *or* we have to disable the connection to the oscillator after one SET.

Instead of doing any of the above we decided to expand the current architecture such that it can record multiple SETs in the DUT. We have carefully selected the given architecture from several candidate solutions, as outlined in Sec. 6.3; to be precise we chose architecture II (refer Sec. 6.3.5 for the reason behind the choice) from the solutions presented. The use of 5 inverters in the ring, together with the switch delays, yields a frequency that is high enough to allow for sufficient resolution, while still being properly counted by the LFSR. The ability to collect an array of measurements is implemented by sequentially stepping through an array of counters, one per SET. Note that one SET is recorded by three counters, except the seventh SET; thereby employing 19 counters in total. The major additions we made to this architecture other than the counters to record METs are:

- **3-bit LFSR**: It implements a pointer to the counter that is currently active as shown in Fig. 6.3. With the falling edge of an SET (to simplify the explanation we assume the SET to be a HI pulse; however, the circuit can easily be adapted to work for a LO pulse on a normally HI signal as well) we increment the pointer to disconnect the current counter, thus conserving its value, and make the next one ready for the SET to come. The reason behind using the LFSR as the pointer is to ensure that any SET in the 3-bit LFSR does not visibly change the pointer to the counters that previously recorded SET data, thereby overwriting already recorded data.

- **Decoder**: A standard decoder is used (to ensure an efficient gateway from the oscillator to the counters) for converting the 3-bit counter addresses produced into one-hot-encoding, which is required by the *de-mux* that actually routes the SET-gated oscillator pulses to the appropriate counter. Since these circuits are purely combinational and hence not prone to SEUs, there is no need for replication here. The *de-mux* employed is shown in Fig. 6.3 . We employed a 8:1 de-mux as it is controlled by the 3 bits generated by the 3-bit LFSR. Note that the 3-bit LFSR has only seven counts, therefore, to avoid unconnected data bits in the architecture the eighth data bit is connected to a dummy signal.

- **3-input NAND**: Note that the concept behind the architecture is to store the width of the first six individual SETs in separate counters with redundancy, while the next and the subsequent SETs will be recorded by a single counter. This feature is enforced by the NAND gate. That is, as soon as the pointer reaches the last cell in the array (note that, due to the irregular count sequence of the LFSR, this is not “111” but “001” in our implementation) the NAND output freezes the pointer.

- **Switch for Pointer**: As show in Fig. 6.3 we can observe that the 3-bit LFSR is connected to the target using a switch. This switch is controlled by the NAND gate that paralyses the pointer. Note that if the NAND output is LO the pointer will be connected to the target, else the input of the pointer is grounded. Any further SETs in the target after the pointer is grounded will

not change the gateway in the de-mux, hence will be recorded in the same counter.

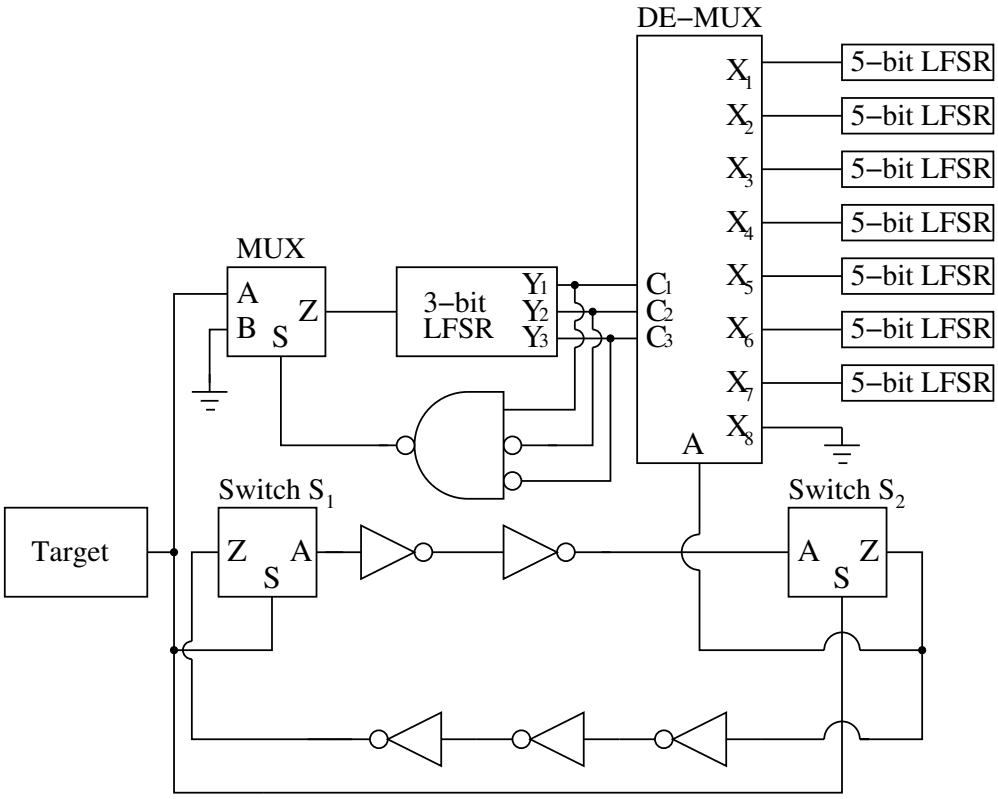


Figure 6.3: Architecture to Measure Multiple SET Lengths

This circuit can easily be changed to increase or decrease the length of the array, as demanded by the application. Furthermore, we could as well have X2 count the width of the (single) 6th SET, and discard all further SETs completely, by a few modifications in our architecture. However, the given solution allows us to identify an overflow of our array and take appropriate measures (changing the environment parameters or the read-out interval, e.g.). A further extension might be to use the NAND output ("S" terminal of MUX in Fig. 6.3) to indicate that the array is nearly full, and thus request a readout by the host. We prefer a (maximum-length) LFSR over a conventional binary counter for several reasons:

- Its implementation requires fewer combinational gates, thus saving area.
- We do not rely on the regular count sequence; anyway it is straightforward to transform the observed state into a count value.
- Within its irregular counting sequence, a bit flip in one of its flip flop cells (caused by an SET in itself rather than the target circuit) will lead to a huge

jump. Since we have provided a count range of 31 while we expect SETs to last for 6 cycles at most, we can easily identify single bit flips by a plausibility check. The drawback of using the LFSR is that one state is sticky and can therefore not be used in the count sequence. This is, however, not very relevant in our case.

6.5 Multiple SET Architecture – Improvement of Counter Array

Note that the architecture presented previously uses three counters for recording one single SET in the DUT. As such we use 19 LFSRs for the architecture, which consumes a lot of silicon area. In here our aim is to reduce the number of counters employed to record the SETs and at the same time use three counters to provide redundancy, for this we chose the up/down counters.

6.5.1 Counter array implementation

In order to maintain a list of pulse width measurement results, we implement an array of counters. An address pointer is used to sequentially select the next free counter once an SET measurement is finished. More specifically, we have a "one hot" address counter that is incremented with the trailing edge of an SET such that it already points to the next free counter once the next SET arrives at the target. Since the interval between SETs is quite large (much larger than seconds on average), the propagation delay of this address counter is uncritical; however, it must be fast enough to recognize short SETs at all, otherwise it would fail to increment. Our current architecture provides an array of $n = 7$ counters $A_0, \ldots, A_{n-1}$, refered to as *absolute counters*, which allow to record up to 7 target SET durations (refer Fig. 6.4).

6.5.2 Attaining Fault Tolerance

6.5.2.1 Guiding principles

While the architecture sketched above already nicely fulfills Req. 1.3 (c)–(e), fault tolerance, as demanded in Req. 1.3 (b), still requires special consideration. After all, being located on the same die, the measurement infrastructure will be exposed to the same level of radiation as the target. Before going into detail with the respective provisions we propose for the individual blocks, let us present the guiding principles we applied in their design:

1. We expect SETs with a width of approximately 1ns to hit the target with a rate of less than one per 10s (see Sec. 6.8). This means that the switches will be closed with a duty cycle of less than $1 : 10^{10}$; in other words the architecture will be in the idle state most of the time. Therefore, it is extremely unlikely

that we will see an SET hit the architecture while the switches are closed – that would be a very near coincident double hit, first in the target and then in the measurement infrastructure. We can hence safely neglect this case. As a consequence, we can assume our infrastructure works properly during the oscillation phase of the ring oscillator, *unless* it is suffering from an SEU in at least one of its sequential elements. In other words, we need not be concerned with SETs in the combinational logic of our infrastructure, but we do need to care for SEUs.

2. As already outlined in Sec. 6.2, the probability to experience an SEU in the infrastructure is significantly higher than seeing an SET in the target. This is simply because the area of the infrastructure is much larger. Consequently, the target of our fault-tolerance strategy will be to tolerate at least a single SEU in the infrastructure (in the sense that still valid results are maintained), and (as far as possible) detect all double SEUs (in the sense that the results are known to be no more trustworthy and hence discarded). We believe this represents a good trade-off between feasibility of implementing fault tolerance with reasonable area overhead (Req. 1.3(e) and still obtaining a sufficient percentage of useful readouts Req. 1.3(b)).

6.5.2.2 Protecting the address counter

As already pointed out, the speed of the address counter is not critical. Therefore, we implement it as a 3-bit LFSR, which yields the most area efficient solution for indexing an array of 7 SET counters. In particular, we have chosen a one-to-many implementation of the polynomial $x^3 + x^2 + 1$. This maximum-length polynomial cycles through 7 states, while the state 111, as usual, is sticky and is therefore avoided.

Being a highly sequential element, the address counter is particularly prone to SEUs and therefore requires specific protection. One way of attaining this would be implementing a larger count range and actually exploiting only a subset of the code set then. This would allow plausibility checking, as outlined in Sec. 3.5.1.1, 4.3.3. However, in the sense of Req. 1.3(b) it is paramount to our approach to avoid losing results due to an incorrect indexing in the array (thus either pointing to a non-existing counter index, or directing the pulses from a new measurement into a counter that already contains a previous result). Since this plausibility-based kind of protection is not reliable enough for our purpose, we use TMR instead: We decided to triplicate the 3-bit LFSR and add a voter [98] that is, as usual, able to mask one faulty 3-bit input word. In addition, we have provided our voter with the capability of detecting a mismatch in all three input words and consistently set a triplicated *voter error flag* in this case.

Consequently, the residual risk are two SEUs affecting two replicas of the LFSR in exactly the same way, thereby making the voter believe that those matching erroneous LFSR values are the correct one. Assuming that all replicas are affected by SEUs with the same probability, and that all erroneous states of the LFSR are

equally likely, we have a proportion of $2/3 \cdot 1/7 \approx 10\%$ of all feasible double SEUs in the triplicated LFSR structure[2] that create this undesired scenario. Besides this quite small probability of critical double SEUs in the LFSRs, we also get additional detection capabilities by using

- the voter error flags, and
- the SET recordings stored (can detect pointer errors) in the counter array

6.5.2.3 Protecting the counter array

We have already motivated why we implement the counter as an up/down counter (UDC) based on an elastic pipeline (refer Sec. 4.2.3.1), and we have already argued that it needs specific protection (refer Sec. 4.3.4). In principle, we could protect it by triplication as well. However, given that this counter, with its depth of 10 entries and its less area efficient implementation occupies a significantly larger area than the address counter, and that we have an array of such counters, we simply cannot afford triplication in view of the discussion given in the context of Req. 1.3(a).

As already motivated, radiation hardening by sizing does not work for our purpose (due to the area overhead), so we have to employ some form of redundancy to protect our counter values. Our aim is single-error correction and double-error detection, for both of which we need at least 3 instances of the counter value.

Since the decision to use Muller pipelines as counters allows us a very convenient implementation of up/down counters (UDCs), we can implement a *gracefully degrading* TMR architecture by means of a novel duplex approach. Denoting by $j \in \{1, \ldots, n\}$ the j-th target SET that is to be recorded, let $L(j) \in \{0, \ldots, n-1\}$ be the corresponding LFSR output. Let X_{i+1} be the de-mux output that is activated when the voter provides the address word $i \in \{0, \ldots, n-1\}$, which implies that the j-th SET is routed to $X_{L(j)+1}$. For example, for our 3-bit LFSR, which has the output sequence $0, 2, 6, 5, 3, 4, 1$, the third target SET will be output at $X_{L(3)+1} = X_7$ as $L(3) = 6$.

Our redundant counter architecture for the counter array $A_0, \ldots, A_{n-1}$ is organized as follows: Let $\pi(i)$ be any permutation of $\{0, \ldots, n-1\}$, which says that $X_{\pi(i)+1}$ is routed to the absolute counter A_i.

- $X_{\pi(i)+1}$ of the de-mux is fed directly to the "up" input of a UDC that has its "down" input grounded, which takes over the role of A_i.
- The same $X_{\pi(i)+1}$ is fed to another UDC D_i that is shared with $X_{\pi(i-1)+1}$, whereby $X_{\pi(i)+1}$ counts up and $X_{\pi(i-1)+1}$ counts down. As it effectively counts the difference $A_i - A_{i-1}$, it is called a *difference counter*. This is the first redundant instance for A_i.
- The same $X_{\pi(i)+1}$ is fed to the "down" input of yet another UDC that is shared with $X_{\pi(i+1)+1}$, hence $X_{\pi(i)+1}$ counts down and $X_{\pi(i+1)+1}$ counts up. As it

[2]Note that the probability of such double SEUs to occur at all is already very low

effectively counts $A_{i+1} - A_i$, it is nothing else but the difference counter D_{i+1}. This completes the symmetry and represents the second redundant instance.

- At the border indices $i = 0$ and $i = n - 1$, we simply wrap around, i.e., $D_0 = A_0 - A_{n-1}$. Consequently, one difference counter is embedded between each neighboring pair of absolute counters (in particular, $D_i = A_i - A_{i-1}$ is embedded between A_{i-1} and A_i), such that we have a strict alternation of absolute and difference counters. Due to the wrap-around, the counter array can be viewed as a ring.

To illustrate how this works in principle, let us consider an example: Assume that an SEU has occurred in the difference counter D_3 shared between A_2 and A_3. We can easily identify that the absolute counters A_2 and A_3 hold correct values: For example, for verifying A_3, we have two additional values $D_4 = A_4 - A_3$ and A_4, which are both correct. Subtracting the latter confirms the value stored in A_3. So if the difference $A_3 - A_2$ is not consistent with the value of D_3, the latter must be erroneous. For a complete treatment of all possible cases, see the fault dictionary in Sec. 6.7 and the analysis in Sec. 6.5.4.

Unfortunately, however, there is also another reason for inconsistent values in the related counters A_i, D_i and D_{i+1}: Since the SET pulse and the ring oscillator clock are unrelated, the SET-gating might cut short the last oscillator pulse. In this case, it may happen that e.g. A_i records this last pulse, whereas D_i does not. In the worst case, the range of consistent values for D_{i+1} could hence be as large as $A_{i+1} - A_i - 1 \leq D_{i+1} \leq A_{i+1} - A_i + 1$. To reduce this range, our architecture makes sure (by a proper layout) that D_{i+1} never (down-) counts a pulse that is not also (up-) counted in A_i and D_i. Thanks to this restriction, two absolute counters A_j, A_{j+1} only need to be considered *consistent* if $A_{j+1} - A_j \leq D_{j+1} \leq A_{j+1} - A_j + 1$.

Table 6.3: Sequence of addressing in the counter array

Number j of target SET	De-mux output activated	addressed counters
1	X_1	D_0, A_0, D_1
2	X_3	D_2, A_2, D_3
3	X_7	D_4, A_4, D_5
4	X_6	D_6, A_6, D_0
5	X_4	D_1, A_1, D_2
6	X_5	D_3, A_3, D_4
7	X_2	D_5, A_5, D_6

The permutation $\pi(i)$, which we did not specify further up to now, allows some further optimization. In particular, we choose $\pi(i)$ to be such that $L(i) + 1 = \pi(2i \mod n)$. For our 3-bit LFSR, this results in the assignment of the de-mux outputs $X_{\pi(i)+1}$ to A_i as shown in Table. 6.3. This choice of π ensures that the recorded

target SETs are stored in the absolute counters in the following order:

$$A_0, A_2, A_4, A_6, A_1, A_3, A_5 \tag{6.1}$$

In the case of at most 3 target SETs[3], one observes that there is an absolute counter $A_{2i+1} = 0$ between any two non-zero A_{2i} and $A_{2(i+1)}$ (for $i \in \{0, \ldots, 2\}$). Consequently, every non-zero absolute counter A_{2i} *exclusively* utilizes the two difference counters D_{2i} and D_{2i+1} for also storing its count. Obviously, this is equivalent to TMR. Whereas we lose the TMR equivalence when more than 3 target SETs occur, this does not mean that we also lose all SEU-tolerance properties: We will prove later on that the architecture can tolerate all single SEUs and detect all remaining double-SEUs for sure (as well as many multiple SEUs) even in this case. Consequently, our duplex architecture, which needs only $2n$ UDCs to store n values, can indeed be viewed as a gracefully degrading TMR architecture. Had we simply duplicated each counter in the traditional "duplication and comparison" style, we could only detect single SEUs, and never perform any correction — with the same number of counters.

6.5.2.4 Initialization and read-out

The operation of our architecture will be partitioned in a sequence of consecutive *measurement periods*. At the beginning of every measurement period, all LFSRs will be set to their initial value $L(1)$, which is 0 for our 3-bit LFSR. Every LFSR's associated voter error-flag is also cleared.

Whereas all absolute counters are just initialized to 0, determining proper initial values for the difference counters requires more care. Because of Requirement (3), we do not want to double the size of the difference counters, which would be necessary for matching the counting range of the absolute counters in both positive and negative direction. Fortunately, proper initialization allows us to use the same UDCs also for the D_i's: For each difference counter D_i, we know from the addressing sequence (6.1) whether the first count will be (u) upward or (d) downward. Accordingly, we initialize $D_i := 2$ in the former case, and $D_i := 8$ otherwise. Note that we do not use 0 resp. 10 here, to allow some margin for the subsequent counting that goes into the "wrong" direction. Obviously, one has to subtract the correct initial value before using a difference counter's value for consistency checking later on. Whereas this strategy limits the permissible counting range to 8 for (u) and to 2 plus previous down-count for (d), it will work for typical SET durations (and could of course be extended by using longer UDCs in general).

At the end of a measurement period, all absolute and difference counter values as well as all LFSR outputs and voter error flags are read-out for post-processing.

[3]The probabilistic analysis in Sec. 6.8 will reveal that it is extremely unlikely to observe more than 3 target SETs under reasonable radiation conditions. Consequently, we do not foresee any provisions for handling an overrun of the counter array, which would again only increase the area of the measurement infrastructure.

6.5.3 Resulting architecture

The architecture resulting from the considerations given above is shown in Fig. 6.4.

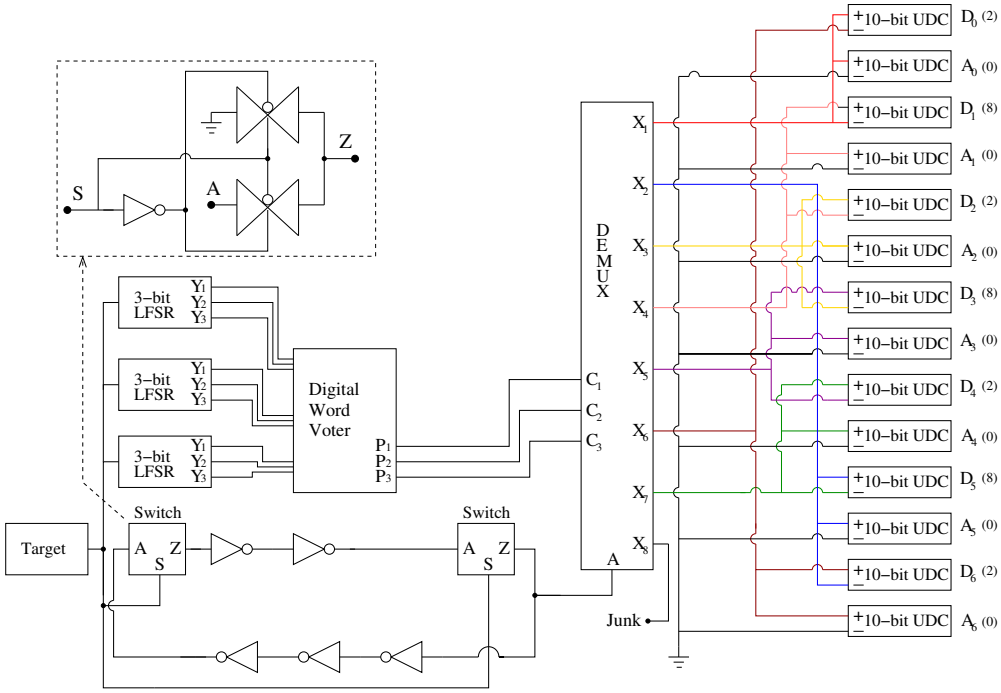


Figure 6.4: Pulse width Measurement Architecture for Multiple SETs

It is apparent that the SET pulse is fed into several units, namely, the two switches as well as the three LFSRs. Given that this a very short pulse, we must also consider the case of a marginal pulse width (or height) that is recognized by only some of the units, and ignored by others.

First, a diverging behavior of the switches for a marginal SET does not create problems due to the serial arrangement of the switches that results in an AND behavior. As the switch is definitely faster than the LFSR, however, we need to consider the case that the switch closes but the LFSR does not increment the address when it opens again. This might cause the currently addressed counters to sum up the duration of the current (very short) SET pulse and the next SET pulse. However, by tuning the reaction time of the UDC to that of the LFSR in the design, we can ensure that such a short pulse is not counted even if it manages to close the switch. In this sense, the LFSR speed limits determine the smallest SET pulse width that can be detected.

The remaining problem is a different perception of the marginal SET pulse among the LFSRs. In this case, one or two of the LFSRs will increment while the other(s) do(es) not. This will make the voter decide for the majority, which still produces a valid behavior. However, the LFSRs are now out of sync and the SEU-

tolerance capability of the TMR arrangement is exhausted. Again, such cases can be made very rare by carefully matching the timing behavior of the LFSRs.

Finally, we have the ring oscillator output being fed into one absolute and two difference counters in parallel. Again here one may experience diverging behavior in case of short SETs that produce marginal outputs of the ring oscillator (in fact one may see such behavior even for longer SETs, namely when the opening of the switch cuts the current output pulse down to marginal size). Albeit we can build on a good matching between the UDCs (here it turns out beneficial that they are all the same circuit), we may still experience related counts that differ by ± 1 due to this effect[4]. As already discussed, this inconsistency can be limited to 1 count by making the path to the "down" input slower than those to the "up" input and to the absolute counter; the remaining uncertainty needs to be considered when performing counter consistency checking, however.

6.5.4 Multiple Event Transients Analysis

A brief analysis would be conducted to verify the radiation tolerance and measurement capabilities of the whole setup. We built a transistor-level design of the proposed infrastructure (presented in Sec. 6.5) in UMC $90nm$ bulk CMOS technology and verified it with extensive simulation runs to make sure it (a) properly and reliably records SETs with the desired resolution and (b) provides the desired radiation tolerance. We can show a small selection of our results here only, namely those that illustrate the concept.

The overview of the waveforms observed when applying a sequence of 6 SETs to our target circuit (inverter) is presented in Fig. 6.5 (note that these SETs have different charges ranging from 100fC to 1pC): The oscillator's output, which is also the input of the de-mux (trace:"A"); the outputs of the digital word voter (traces 1-3: "P_1, P_2, P_3") and the outputs of the de-mux (traces 4-9: "X_1, X_3, X_7, X_6, X_4, X_5"); they are arranged in the LFSR counting order "$X_1 \rightarrow X_3 \rightarrow X_7 \rightarrow X_6 \rightarrow X_4 \rightarrow X_5 \rightarrow X_2$". At the input of the de-mux, we can observe how the ring oscillator is briefly activated with each SET. Fig. 6.5 shows how the pulse trains seen at the oscillator output are nicely distributed to the counters, by separating each and every SET at the output of de-mux. It also shows how the counters take turn in recording the SET durations.

We do not display how transitions are recorded within the counters due to space restrictions. However, Fig. 6.6 shows an example of how the traces of de-mux output X_4 are recorded by counter A_1. It shows the signal traces at the individual Muller C-elements that constitute the UDC. This illustrates and confirms that A_1 is able to record all the oscillator pulses, and of course we have verified that all the other counters are fast enough to capture the oscillator pulses as well. Note that this is a schematic simulation, after synthesis and routing it may turn out that further tuning is necessary, as wire delays are quite significant. Furthermore, Fig. 6.6

[4] A skew larger than one clock period will not occur in a reasonable physical design, so we can rightfully expect the difference among all replicas to be at most ± 1.

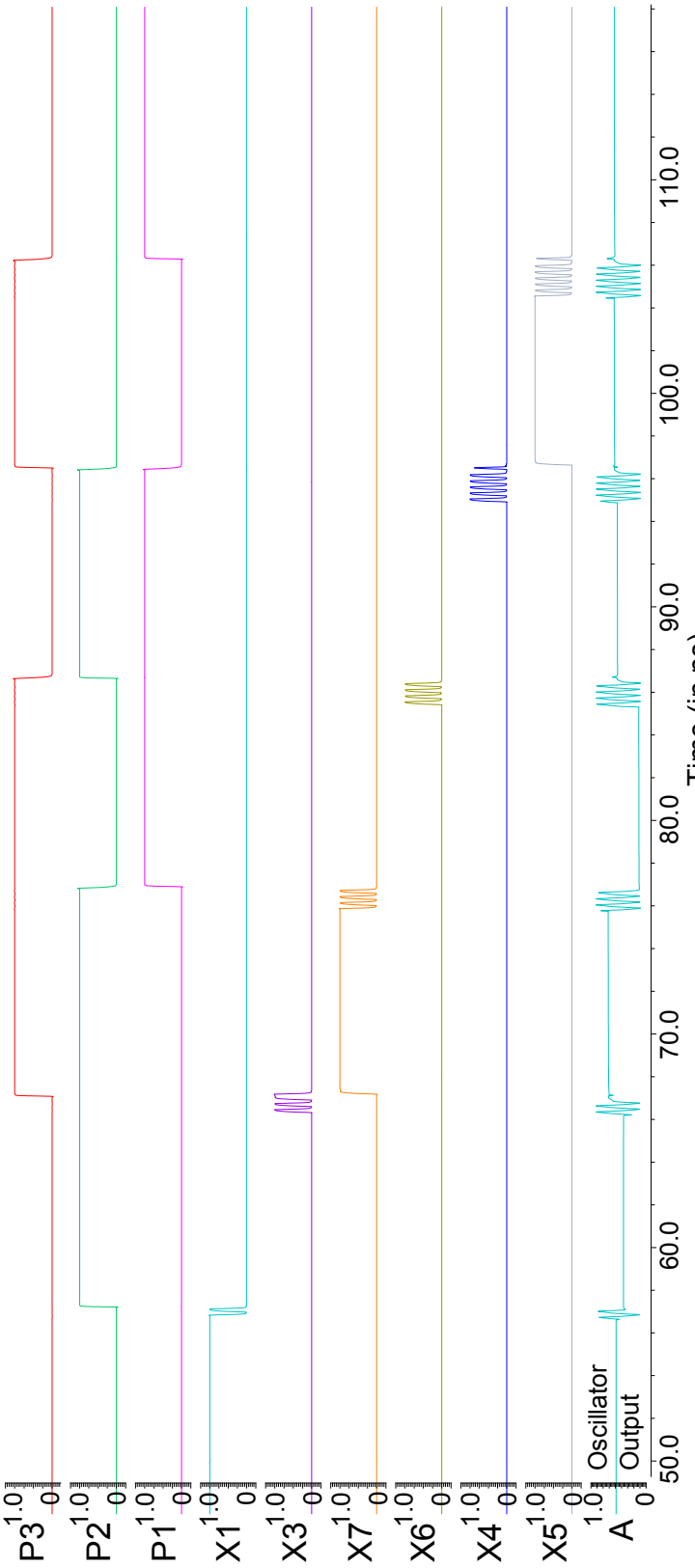


Figure 6.5: Simulation results for the SETs injected in the target circuit

shows how the UDC reacts to a particle hit in itself: In the case shown, $A_1(6)$ and $A_1(7)$ flip to HI as a result of the SET, and hence the count increases by two. As already explained, the correct value of the counter can be recovered by means of the neighboring difference counters, though.

6.6 Algorithm for pulse width extraction from the read-outs

In the sense of Requirement (4), we strive to leverage each and every information we have available for detecting and correcting the recorded counts. In particular, after read-out, we have obtained all absolute and difference counts, as well as the triplicated voter error flags and LFSR outputs, from the end of the measurement period available for SEU correction/detection. Furthermore, we build on the following knowledge about the SEU-tolerance properties of our architecture and the experiment setup, which will be established in Sec. 6.8:

- In reasonable radiation environments, SEUs are rare events (eq. (6.5)). Double SEUs are much less likely than single SEUs, and higher order SEUs have, in comparison, negligible probability. So in determining the root cause of an observed read-out, we will always apply the explanation with the lowest number of SEUs, and consider possible others as sufficiently unlikely to be neglected. This of course causes an uncertainty in our statistics, but this uncertainty is typically low, and in the absence of further information, this is the best we can do.
- We can reliably detect and even correct all single SEUs, both in any counter TMR structure (Lemma 3) and in the entire counter architecture (Lemma 5). Moreover, we can detect all double SEUs except consistent double hits of adjacent counters, which are erroneously corrected as a single hit of the remaining counter.
- In the LFSR TMR structure, we can reliably detect and even correct all single SEUs (Lemma 3). By means of the additional replicated voter error flags, we can also reliably detect all double SEUs in the LFSRs.
- We can detect many higher-order SEUs, but do not leverage this ability in our calculations and pessimistically just rely on the fact that they are sufficiently rare (Lemma 4 and 6).

This leads us to the following strategy for processing our read-outs:

1. Check for a LFSR double hit. If found, discard the whole read-out and exit with an error.
2. For all difference counters, remove the offset resulting from the non-zero initialization.

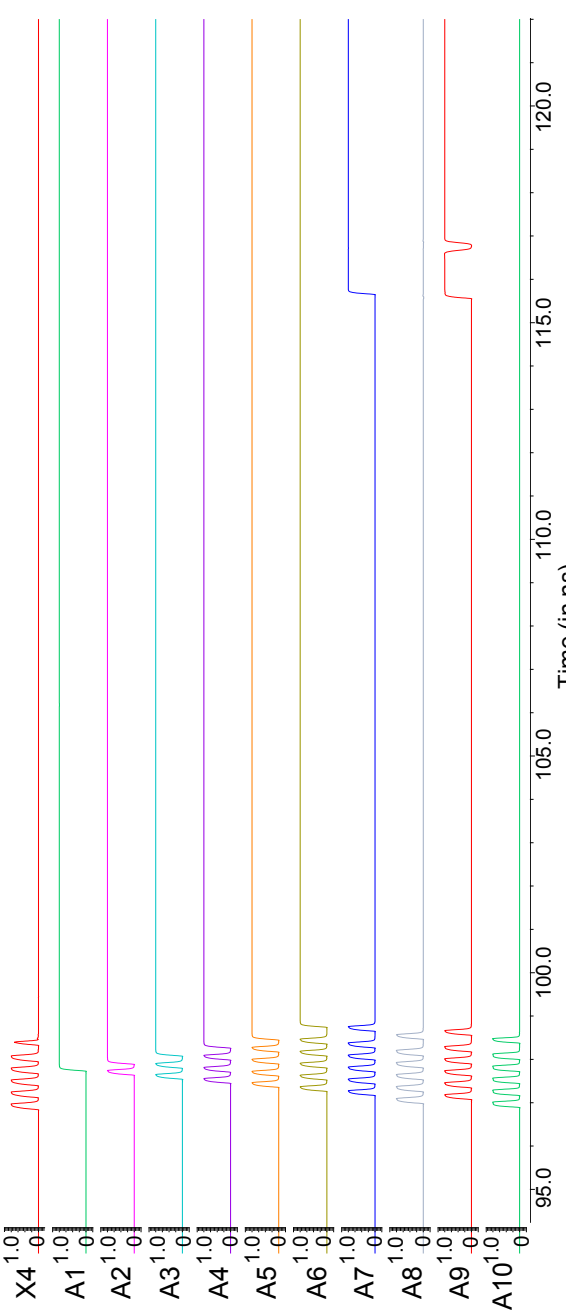


Figure 6.6: Simulation Results: Detail view of a SET in the target and a single SET in the grounded counter A_1

3. Determine the index given by the majority of the LFSRs, which can be assumed to be correct. Check whether the absolute counter entries at that index and all higher ones (which should not have been filled) show a count of zero. If this is not the case in at most two absolute counters, set them to 0; in case of more non-zero absolute counters discard the whole read-out and exit with an error.

4. For all difference counters, check whether they are consistent according to our definition. Mark all inconsistent counters and thus obtain a *syndrome*.

5. If there are no inconsistent counters, exit successfully (with the SET durations contained in the absolute counters).

6. Try to find an explanation for the syndrome by a single SEU in the measurement infrastructure (the associated syndromes can be pre-computed and thus easily recognized). If such an explanation can be found, correct the single counter and exit successfully.

7. For the remaining cases, a double or higher-order SEU must have occurred in the measurement infrastructure that may or may not be correctable. Depending on the outcome, exit successfully or with an error.

6.7 Fault Dictionary

We created a *fault dictionary* for our infrastructure, which associates every fault scenario (single or multiple SET-induced bit flips in the counters, depending on the number of recorded target SETs) with the set (A_0, A_1, ... A_6, D_0, D_1, ... D_6) of resulting read-outs of the up/down counters. This dictionary allows the SEU correction algorithm to infer from an observed read-out the SEU scenario that probably caused it. This inference is based on the most probable explanation of a read-out, i.e., the one assuming the lowest number of SEUs and SETs. As an example, the fault-free recording of a single SET in the target could as well be caused from a triple fault in the counter array (D_0, A_0, D_1), which is, however, very unlikely. At the same time, as this example shows, there are multi-SEU scenarios for which a "simpler" explanation exists and which will hence be misinterpreted. This shows the limitation of the approach with respect to SEU multiplicity. Of course, our redundancy concept makes sure that all scenarios that are within our single/double fault hypothesis are correctly covered (in fact, there are many scenarios that exceed the hypothesis but are still correctly interpreted, as no simpler explanation happens to exist).

Table 6.4 shows our fault dictionary for SETs triggered in the target circuit alone, i.e., correct SET recordings. Herein "$\surd$" indicates that the expected value for the fault-free case is read, "$+$ or $-$" stands for a correctly incremented/decremented UDC value, and "$+/-$" for the value of a counter that has been correctly incremented and decremented as well. It reveals how the counters increment or decre-

ment in the course of the fault-free recording of target SETs. Recall that the unconventional indexing sequence of the counters is due to the use of an LFSR instead of a binary counter.

Table 6.5 presents the fault dictionary for SEUs in up/down counters. It has been validated by means of numerous SET injection simulations (up to twelve at a time) into various locations. Note that we are only discussing the possibilities of single, double and triple faults in the *counters* here; target SETs are not explicitly considered. We can distinguish the following cases:

1. *Single-SEU scenario*: If there has been a fault in any one of the counters, it can be easily traced back to the affected counter, as outlined above already: The two neighboring counters provide sufficient diagnostic information for that purpose.

2. *Double-SEU scenario*: In the worst case, there could be consistent SEUs in two up/down counters, which then contain consistent (but erroneous) values; let us use A_2 and D_3 as an example. We could explain this either correctly, or by assuming A_2 to be correct and blaming D_2 and D_3 to have suffered from an SEU. It is exactly this type of scenario where we need extra information (as e.g. provided by the voter error flags in the case of the LFSRs) to take the right decision. Similarly, if the SEUs occur in the counters D_0, A_0 or in D_0, D_1, we would have to deliver the same conclusions. This is one of the limitations of the TMR arrangement of the counters.

   In all the other cases, where the double-SEU is not consistent, we can accurately locate the affected counters.

3. *Triple fault scenario*: In the best case scenario, we can have three different SEUs in counters associated with three different target SETs. Using the same arguments as above, we can recover all values in that case. We can also have a double-SEU scenario for one target SET and a single-SEU scenario for another target SET. This would allow detection of the double fault and recovery from the single fault. In the worst case, we can have three SEUs in all the three counters that record the same target SET, like A_0, D_0 and D_1, for example. In principle this means that we cannot even be sure to detect this fault, as the erroneous values might be consistent. The residual risk of misinterpretation is low enough to be accepted as a residual error in our statistics, however.

In order to avoid facing the above worst case scenarios already for single particle hits that affect multiple transistors, we can scramble the physical location of the counters on the die such that no two counters that record the same SET are adjacent to each other. However, multiple independent SETs may still produce a worst case scenario. If the number of SETs is generally too high, we can reduce the radiation exposure time and read out the data more frequently.

Table 6.4: Fault Dictionary for SETs in the Target Circuit

Observed Syndrome														Active counter	No. of Faults	Address ptr 3-bit LFSR		
A_0	A_1	A_2	A_3	A_4	A_5	A_6	D_0	D_1	D_2	D_3	D_4	D_5	D_6	–	–	L_3	L_2	L_1
No Fault Scenario																		
√	√	√	√	√	√	√	√	√	√	√	√	√	√	–	–	0	0	0
Fault Scenario																		
+	√	√	√	√	√	√	+	−	√	√	√	√	√	X_1	1	0	0	0
+	√	+	√	√	√	√	+	−	+	−	√	√	√	X_3	2	0	1	0
+	√	+	√	+	√	√	+	−	+	−	+	−	√	X_7	3	1	1	0
+	√	+	√	+	√	+	+/−	−	+	−	+	−	+	X_6	4	1	0	1
+	+	+	√	+	√	+	+/−	−/+	+/−	−	+	−	+	X_4	5	0	1	1
+	+	+	+	+	√	+	+/−	−/+	+/−	−/+	+/−	−	+	X_5	6	1	0	0
+	+	+	+	+	+	+	+/−	−/+	+/−	−/+	+/−	−/+	+/−	X_2	7	0	0	1

Table 6.5: Fault Dictionary (excerpt): SEUs in the Up/Down Counters

Observed Syndrome														Location of Fault	
														Actual Location	Interpretation
A_0	A_1	A_2	A_3	A_4	A_5	A_6	D_0	D_1	D_2	D_3	D_4	D_5	D_6	–	–
No Fault Scenario															
√	√	√	√	√	√	√	√	√	√	√	√	√	√	–	–
Single Fault Scenario															
X	√	√	√	√	√	√	√	√	√	√	√	√	√	A_0	A_0
√	√	√	√	√	√	√	X	√	√	√	√	√	√	D_0	D_0
√	√	X	√	√	√	√	√	√	√	√	√	√	√	A_2	A_2
√	√	√	√	√	√	√	√	√	X	√	√	√	√	D_2	D_2
√	√	√	X	√	√	√	√	√	√	√	√	√	√	A_3	A_3
√	√	√	√	√	√	√	√	√	√	X	√	√	√	D_3	D_3
Double Fault Scenario															
X	X	√	√	√	√	√	√	√	√	√	√	√	√	A_0, A_1	A_0, A_1
√	X	X	√	√	√	√	√	√	√	√	√	√	√	A_1, A_2	A_1, A_2
X	√	X	√	√	√	√	√	√	√	√	√	√	√	A_0, A_2	A_0, A_2
√	√	√	√	√	√	√	√	X	√	√	X	√	√	D_1, D_4	D_1, D_4
X	√	√	√	√	√	√	X	√	√	√	√	√	√	A_0, D_0	any two of $\{A_0, D_0, D_1\}$
√	X	√	√	√	√	√	√	X	√	√	√	√	√	A_1, D_1	any two of $\{A_1, D_1, D_2\}$
√	√	√	√	√	X	√	√	√	√	√	√	√	X	A_5, D_6	any two of $\{A_5, D_5, D_6\}$
√	√	√	X	√	√	√	√	√	√	X	√	√	√	A_3, D_3	any two of $\{A_3, D_3, D_4\}$
Triple Fault Scenario															
X	X	X	√	√	√	√	√	√	√	√	√	√	√	A_0, A_1, A_2	A_0, A_1, A_2
√	√	√	√	√	√	√	X	X	X	√	√	√	√	D_0, D_1, D_2	D_0, D_1, D_2
X	√	√	√	√	√	√	X	X	√	√	√	√	√	A_0, D_0, D_1	A_0, D_0, D_1, T(F_1)
√	X	√	√	√	√	√	√	X	X	√	√	√	√	A_1, D_1, D_2	A_1, D_1, D_2, T(F_5)
√	√	√	√	√	√	X	X	√	√	√	√	√	X	A_6, D_6, D_0	A_6, D_6, D_0, T(F_4)

6.8 Probabilistic Analysis

Given the considerably larger number of transistors of the measurement circuitry as compared to the number of transistors of the target circuitry on the one hand, and the ability of the measurement infrastructure to tolerate only a certain number of counter hits on the other hand, the question about feasible measurement periods $\Delta = \Delta(\phi)$ for a given *particle flux* ϕ (in particles per $\mu m^2 \cdot s$) arises: Δ must be chosen small enough such that, with reasonably high probability, there are only tolerable hits in in the measurement circuitry during Δ; we call such a measurement period *safe*. At the same time, with reasonably high probability, there should be at least one hit in the target circuitry within some W measurement periods, in order to get meaningful SET duration measurements within reasonable time at all. Given ϕ, this effectively defines a range of suitable values for Δ. In this section, we will show that this range is not empty (albeit W may be large; it may hence take quite some time until meaningful SET data is gathered). This confirms that our measurement architecture reasonably achieves its purpose.

The suitable range of values for Δ can be estimated by using cross section data. The lower limit of this range is determined via the *SET cross section* γ (in μm^2) applied to the target circuitry. The SET cross section expresses that a total fluence of 1 particle per γ results in 1 SET per device of interest on average. Radiation experiments reported in [148] established a (saturated, i.e., asymptotic w.r.t. increasing linear energy transfer values of the particles) per-transistor SET cross section γ of about $5\ \mu m^2$ for our 90 nm ASIC technology, which also matches the figures given in the literature [106]. Trivial calculations based on expected values reveal that if, given ϕ, we choose Δ large enough such that

$$\phi\Delta = \frac{x/I_T}{\gamma}, \tag{6.2}$$

$x \geq 1$ transistors will be hit (and hence produce an SET) in a target circuit consisting of I_T transistors during Δ on average.

For the upper bound of the suitable range for Δ, we need the *SEU cross section* γ_M of our counters (which are implemented by Muller pipelines) resp. γ_L of our LFSRs; it characterizes single-event upsets that actually change a counter's resp. LFSR's value. We estimate γ_L via the SET cross section γ by setting $\gamma_L = I_L\gamma = 330\ \mu m^2$, where $I_L = 66$ is the number of transistors in a single 3-bit LFSR.

Whereas we could do the same for estimating the SEU cross section of our counters, this would lead to an overly pessimistic value for γ_M: Each of our 10-bit counters consists of $I_M = 288$ transistors, but not every SET, i.e., a hit in any transistor, actually changes the counter's value. And indeed, γ_M depends on many factors, including the implementation of the Muller C Gates, their interconnect in the pipeline structure, the current counter value, and even whether the counter is currently changing (dynamic mode) or in hold mode (static mode). For more accurate predictions, γ_M needs to be determined explicitly. Fortunately, appropriate simulation experiments for our 10-bit counters were performed in [137]. According to [Table IV][137], their (saturated) SEU cross section is $\gamma_M = 350\ \mu m^2$; note that

it occurs in static mode, where the counters are much more vulnerable to SEUs than in dynamic mode.

Since γ_L is very similar to γ_M, in what follows, we will use the cross section γ_M for both counters and LFSRs for simplicity. Using a similar reasoning as above reveals that, given ϕ and the number of counters N, if we choose Δ small enough such that

$$\phi\Delta = \frac{y/N}{\gamma_M}, \tag{6.3}$$

$y \geq 1$ counters will be hit (and hence change their count) in the measurement circuitry during Δ on average.

Since Δ should be chosen large enough to fully exploit the measurement infrastructure's SEU resilience, albeit without leading to excessively many SEUs, we choose

$$\Delta = \frac{C}{N\gamma_M\phi}, \tag{6.4}$$

for some constant $C > 0$. Obviously, this leads to $\lambda_M := C$ counter hits in the measurement architecture during Δ on average. Note carefully that C is the only parameter that can be chosen freely to tune the probability of success/failure of our measurement architecture for a given particle flux ϕ.

On the other hand, for the same ϕ, the average number x of SETs generated in T during the above Δ evaluates to $x = \lambda_T := \frac{CI_T\gamma}{N\gamma_M}$, as can be checked by plugging in (6.4) into (6.2).

Clearly, our architecture fails in a measurement period if both (i) $k > 0$ SETs are generated in the target circuitry and (ii) the measurement period is not safe: In this case, our measurement architecture faces more counter and LFSR hits than it can tolerate, such that at least one of the recorded SET durations is erroneous. Let $P_{fail}(k)$, which implicitly depends on Δ and hence on C, be the conditional probability that (ii) happens in case of (i). Note carefully that we do not assume here that we can reliably detect an unsafe measurement period.

For the subsequent calculation of $P_{fail}(k)$ and all related quantities, we will assume that the number of hits in (i) all the counters, (ii) the LFSR TMR structure, and (iii) the target architecture during a single measurement period follow independent joint spatial-temporal Poisson distributions with rates (i) $\lambda_A = C$, (ii) $\lambda_L = 3C/N$ and (iii) $\lambda_T = \frac{CI_T\gamma}{N\gamma_M} = C\rho$, respectively. The value for λ_L follows from λ_A and the fact that the single LFSR and single counter cross sections have been assumed to be the same (γ_M), and that we have 3 LFSRs in our TMR structure. The constant

$$\rho = \frac{I_T\gamma}{N\gamma_M}$$

can be seen as the ratio of the SET sensitivity of the entire target circuit over the SEU sensitivity of the entire counter architecture. For our particular implementation, $\rho = I_T/980$ (with $I_T = 2$ for an inverter target, for example) is typically very small.

As our measurement infrastructure provides different levels of SEU-tolerance in the case of at most 3 target SETs (where we essentially have independent TMR

counter structures for every recorded SET data) vs. more than 3 target SETs (where we can essentially tolerate only single and many double SEUs), we will compute $P_{fail}(k)$ for these two cases separately in Section 6.8.1 ($P_{fail}(k)$, $1 \leq k \leq 3$) and Section 6.8.2 ($P_{fail}(> 3)$).

Before that, however, we will determine the probability P_k that one observes $k \geq 0$ target SETs in a measurement period. Under our assumptions, we have

$$P_k = \frac{\lambda_T^k}{k!} e^{-\lambda_T} = \frac{(C\rho)^k}{k!} e^{-C\rho} \approx \frac{(C\rho)^k}{k!}(1 - C\rho), \tag{6.5}$$

where the last approximation holds for small $C\rho$ due to $e^x = 1 + x + O(x^2)$ for $x \to 0$. It is apparent that P_k goes down very rapidly with k in this case. Hence, we will rarely see more than a few target SETs in a measurement period for $\rho = I_T/980$ (unless I_T is also large).

Moreover, as the expected time between two SETs is exponentially distributed with mean $1/\lambda_T$, we can expect one SET in the target circuitry on average within

$$W = \frac{1}{C\rho} \tag{6.6}$$

measurement periods; they eat up a total time of $P\Delta = \frac{1}{\phi I_T \gamma}$. Again, for our value of $\rho = I_T/980$, this W will be quite large for any reasonable choice of C (albeit every measurement period itself may be quite short in case of large ϕ or I_T).

Finally, we compute the probability P_{succ} that at least one SET occurs during a safe measurement period. As target SETs and counter SEUs are independent under our assumptions, we immediately get the following Lemma 1:

Lemma 1 (Success probability)**.** *The probability that at least one SET occurs during a safe measurement period is*

$$\begin{aligned} P_{succ} &= \sum_{k \geq 1} (1 - P_{fail}(k)) P_k \qquad (6.7) \\ &\geq \sum_{k=1}^{3} (1 - P_{fail}(k)) \frac{(C\rho)^k}{k!} e^{-C\rho} + \Big(1 - \sum_{k=0}^{3} \frac{(C\rho)^k}{k!} e^{-C\rho}\Big)(1 - P_{fail}(> 3)). \end{aligned}$$

Note that there is an optimal choice for C, given ρ and N, which maximizes P_{succ}.

It is apparent from the Taylor series expansion of e^x at $x = 0$ that, for small $C\rho$, the contribution of the term involving the second sum to P_{succ} is only $O((C\rho)^4/4!)$ and hence quite negligible. Actually, P_{succ} is mainly determined by the term $k = 1$ in the first sum here, which eventually reveals that $P_{succ} \approx (1 - P_{fail}(1))C\rho$.

Clearly, in our setting, the number of measurement periods until the first safe one witnessing at least one SET is geometrically distributed with success probability P_{succ}. It follows that the average number of measurement periods until success is just $1/P_{succ}$. For small $C\rho$, we thus obtain the following Lemma 2:

Lemma 2 (Average duration until successful SET recording)**.** *The average time until a safe measurement period with at least one target SET occurs is*

$$\frac{1}{P_{succ}} \approx \frac{1}{C\rho(1 - P_{fail}(1))} = \frac{W}{1 - P_{fail}(1)}. \tag{6.8}$$

Note that (6.8) is of course consistent with (6.6). Their relation also shows that, for small $C\rho$ and reasonably small $P_{fail}(1)$, the main reason for a non-successful measurement period is just the absence of any target SET, rather than an unsafe measurement period. So despite the fact that we cannot be sure to detect an unsafe measurement period (in the case of excessively many counter hits), we can be sure that the probability of reading out erroneous SET durations in a measurement period with k target SETs is at most $1 - P_{fail}(k)$.

6.8.1 Computing P_{fail} for at most 3 target SETs

Recall that our measurement architecture with $N = 2n$ counters consists of n *absolute* counters A_j, $0 \leq j < n$, with a *difference counter* $D_{j+1} = A_{j+1} - A_j$ placed between A_j and A_{j+1}, which are all arranged in a ring (with increasing indices in clockwise direction). We will consider the "abstract" ring of the n absolute counters only, where we implicitly index arithmetic $\mod n$ for elements in the index set $\{0, \ldots, n-1\}$. Herein, D_n refers to the "hidden" difference counter D_0 between A_{n-1} and A_0 (which counts up with A_0 and counts down with A_{n-1}).

We say that two consecutive absolute counters A_j, A_{j+1} are *consistent*, if $A_{j+1} - A_j \leq D_{j+1} \leq A_{j+1} - A_j + 1$. The uncertainty by one count results from the possibility of the (one-sided[5]) inconsistent recording of the last oscillator pulse in different counters. We call a double hit of two adjacent counters consistent, if they leave the corresponding absolute counters consistent. Note that the probability of a consistent double hit is considerably less than the probability of a standard (i.e., not necessarily consistent) double hit: As consistent hits must be such that the altered count values (say, D_i and A_{i-1}) match (within 1 count) the (unaltered) value of A_i, this leaves only at most $2S$ possible altered pairs of counter values, where S is the smallest positive or negative counting range of any involved counter: There are at most $S + 1$ possible pairs minus the original pair that match exactly, which must be doubled due to the possible difference of 1 count. As each pair occurs with a probability of $1/S^2$, a consistent double hit occurs at most with the unconstrained double-hit probability times a factor of $2/S$.

In the case of at most $k = 3$ target SETs, as well as in the case of our LFSRs, which is exactly analogous, the counters D_i, A_i, and D_{i+1} associated with counting the target SET associated with index i effectively implement a TMR structure. For a safe measurement period, neither the TMR LFSR structure nor any of the k TMR counter structures may suffer from hits that cannot be tolerated. In order to compute $P_{fail}(k)$, we will rely on the following Lemma 3:

[5]Recall that our architecture ensures that e.g. D_i never (down-)counts a pulse that is not also (up-)counted in A_{i-1} and D_{i-1}.

Lemma 3 (Bad TMR counter hits)**.** *Let i be the index of an absolute counter A_i such that both $A_{i-1} = 0$ and $A_{i+1} = 0$ at the end of a single measurement period. Then, we can recover one (or more) hits in any single counter among D_i, A_i, and D_{i+1}. Except for consistent double hits of adjacent counters (which are erroneously corrected as a single hit of the remaining counter), we can reliably detect all double hits that cannot be tolerated.*

Proof. Assuming that at most two SEUs have occurred during the measurement period, we have the following exhaustive cases:

(a) If neither A_{i-1}, A_i nor A_i, A_{i+1} are inconsistent, there was no single or double hit.

(b) There are two adjacent counters A_ℓ, A_r with $i \leq r + 1 = \ell \leq i + 1$, such that D_ℓ is the only inconsistent difference counter. Without loss of generality (the other case is symmetric), assume that $r = i - 1$ and $\ell = i$; note that $A_{i-1} = 0$ here. Unfortunately, it is impossible to distinguish whether (i) D_i suffered from single hit, (ii) A_i, D_{i+1} experienced a consistent double hit. Since a single hit is of course much more likely than a consistent double hit, our requirement of guaranteed single-hit tolerance forces us to always assume (i) and thus to re-set $D_i := A_i - A_{i-1}$. Note carefully, though, that this convention makes it impossible to reliably detect the consistent double hit (ii) here.

(c) Both A_{i-1}, A_i and A_i, A_{i+1} are inconsistent, so both the difference counters D_i and D_{i+1} are inconsistent. If these difference counters point to the same consistent correction value $A_{i+1} - D_{i+1} = D_i + A_{i-1}$ (within at most one count) for A_i, we know that the latter suffered from a single (or double) hit. Otherwise, however, it is impossible to distinguish whether the actual hits occurred in (i) A_i, D_{i+1}, (ii) D_{i+1}, D_i or (iii) A_i, D_i. Hence, we cannot correct such a double hit, but we can reliably detect it.

Since the above cases are exhaustive, the proof of Lemma 3 is completed. □

For computing a lower bound for the probability of a safe measurement period for k target SETs, we use the fact that the k TMR counter structures and the LFSR TMR structure are completely disjoint. Due to our assumptions, SEUs occur independently with rate $\lambda_L = 3C/N$ in every single TMR structure in this case. Since each can tolerate at least a single hit according to Lemma 3, the probability of successful TMR operation is at least

$$P^{TMR} \geq \left(1 + \frac{3C}{N}\right) e^{-3C/N}. \tag{6.9}$$

Since we have k independent TMR counter structures plus the LFSR TMR structure, we end up with the following Lemma 4:

Lemma 4 ($P_{fail}(k)$ for $1 \leq k \leq 3$)**.** *The probability of a non-safe measurement period for* $1 \leq k \leq 3$ *is*

$$P_{fail}(k) \leq 1 - \left(\left(1 + \frac{3C}{N}\right)e^{-3C/N}\right)^{k+1}. \tag{6.10}$$

Obviously, $P_{fail}(k)$ can be made as small as desired by choosing $C \in (0, 2]$ sufficiently small. Table 6.6 provides $P_{fail}(k)$ for $N = 14$ and different values of C and k, which reveal that our architecture works very well for reasonable choices of C.

$P_{fail}(k)$	$k = 1$	$k = 2$	$k = 3$
$C = 0.2$	0.0018	0.0027	0.0036
$C = 1.0$	0.039	0.058	0.077
$C = 1.5$	0.082	0.12	0.157

Table 6.6: Values for $P_{fail}(k)$ for $N = 14$ and different values of C, k.

6.8.2 Computing P_{fail} for more than 3 target SETs

In this last subsection, we also compute $P_{fail}(> 3)$. For a safe measurement period, neither the LFSR TMR structure nor the entire counter structure may suffer from hits that cannot be tolerated. For the latter, we rely on the following Lemma 5:

Lemma 5 (Bad counter hits)**.** *For* $N = 2n \geq 10$*, our measurement architecture involving* N *counters can tolerate all single and double hits in a single measurement period, except some of those that hit different counters that are separated by strictly less than 4 non-hit counters. Except for consistent double hits of adjacent counters (which are erroneously corrected as a single hit of the remaining adjacent counter), it can reliably detect all double hits that cannot be tolerated.*

Proof. As there are at most two counter hits and $n \geq 5$ as $N \geq 10$, there must be a maximal block of at least 2 consecutive absolute counters $A_\ell, \ldots, A_r$ with $l < r$ where all difference counters in between, i.e., D_{j+1} for $\ell \leq j < r$, are consistent in the sense that $A_{j+1} - A_j \leq D_{j+1} \leq A_{j+1} - A_j + 1$. We have the following exhaustive cases for ℓ and r:

(a) If $r = \ell$, there was no single or double hit.

(b) $r + 1 = \ell$, i.e., B consists of all absolute counters and there is no one left between r and ℓ. As $r \neq \ell$, D_ℓ must be the only inconsistent difference counter. However, it is impossible to distinguish whether (i) D_ℓ suffered from single hit, (ii) A_ℓ, $D_{\ell+1}$ experienced a consistent double hit or (iii) A_r, D_r did so. Since a single hit is of course much more likely than a consistent double hit, our requirement of guaranteed single-hit tolerance forces us to

always assume (i) and thus to re-set $D_\ell := A_\ell - A_r$. Note carefully that this convention makes it impossible to reliably detect the consistent double hits (ii) and (iii) in our architecture.

(c) $r + 2 = \ell$, i.e., there is exactly one absolute counter A_m with $m = r + 1$ not in B between r and ℓ. As before, since B could not be extended further, the difference counters D_ℓ and D_m must be inconsistent. If these counters point to the same consistent correction value $A_\ell - D_\ell = D_m + A_r$, within at most one count, for A_m, we know that the latter suffered from a single (or double) hit. Otherwise, however, it is impossible to distinguish whether the actual hits occurred in (i) A_m, D_ℓ, (ii) D_ℓ, D_m or (iii) A_m, D_m. Hence, we cannot correct such a double hit, but we can reliably detect it.

(d) If $r + 3 = \ell$, then there are exactly 2 absolute counters A_m, A_{m+1} with $m = r + 1$ not in B in between r and ℓ. As in case (c), D_ℓ and D_m must be inconsistent. Unfortunately, we cannot distinguish whether (i) A_m, A_{m+1} or else (ii) D_ℓ, D_m have been hit. Note that, in case (i), the hits must be such that D_{m+1} is consistent, which makes it less likely than case (ii), by a similar argument as in (a). Nevertheless, we cannot reliably correct but only detect this double hit.

(e) Otherwise, there are at least 3 absolute counters A_m, A_{m+1} and A_{m+1} with $m = r+1$ not in B between r and ℓ. We can correct the double hit here, as we have sufficiently many equations to disambiguate between the two possible hit cases (i) A_m, A_{m+2} or else (ii) D_ℓ, D_m that are analog to (i) and (ii) in case (d).

As the above cases are exhaustive, this completes the proof of Lemma 5. □

We proceed with computing a (conservative) bound for the probability P^N that two hits that occur independently and uniformly among $N = 2n \geq 10$ counters can be tolerated. We use the Boltzmann-Maxwell statistics (that is compatible with our Poisson process), where each of the overall N^2 different possibilities to place 2 indistinguishable balls (hits) into N boxes (counters) is equally likely. For the first hit, we have N different counters to select from. For the second hit, Lemma 5 tells us that we must spare 4 counters before and after the first hit one to rule out some double hits that we cannot tolerate, which gives us $N(N-9)/2$ different double-hit scenarios affecting different counters that can be tolerated for sure. Since we can also tolerate double hits of one and the same counter, we can add these N scenarios, which gives us $N(N-7)/2$ tolerable double-hit scenarios overall. The number of all possible double-hit scenarios without restriction is $\binom{N+1}{2}$, i.e., the number of 2-sequences from $\{1, \ldots, N\}$ with repetitions allowed. Consequently, we obtain

$$P^N \geq \frac{N(N-7)}{(N+1)N} = \frac{N-7}{N+1}. \tag{6.11}$$

Lemma 5 showed that our counter architecture can tolerate all single hits as well as a fraction of $(N-7)/(N+1)$ of all double hits according to (6.11). Recalling

that a safe measurement period also requires the LFSR TMR to suffer from at most a single hit, which happens with probability P^{TMR} given in (6.9), we get the following uniform upper bound $P_{fail}(k) \leq P_{fail}(> 3)$, which holds for any feasible number $3 < k \leq n$ of recorded target SETs:

Lemma 6 ($P_{fail}(> 3)$)**.** *The probability of a non-safe measurement period for $k > 3$ is upper bounded by*

$$\begin{aligned} P_{fail}(> 3) &:= 1 - \Big(1 + \lambda_M + \frac{\lambda_M^2(N-7)}{2(N+1)}\Big)e^{-\lambda_M} \cdot P^{TMR} \\ &= 1 - \Big(1 + C + \frac{C^2(N-7)}{2(N+1)}\Big)\Big(1 + \frac{3C}{N}\Big)e^{-C(1+3/N)} \end{aligned} \quad (6.12)$$

$P_{fail}(> 3)$ can again be made as small as desired by choosing $C \in (0, 2]$ sufficiently small. For example, for $C = 0.2$ resp. $C = 1.0$, we obtain $P_{fail}(> 3) \approx 0.01$ resp. $P_{fail}(> 3) \approx 0.2$.

It is worth noting, though, that even a non-negligible P_{fail} is acceptable here: Besides the fact that it it very unlikely to ever observe more than 3 target SETs for reasonable choices of C, our analysis and hence our bound is very conservative: In reality, our architecture also tolerates many scenarios where more than double counter hits occur, and detects even more.

6.9 Discussion of our Analysis Results

Based on the results of the probabilistic analysis, we can validate several of the decisions we made in the design of our measurement architecture, and finally justify that it indeed serves its purpose.

By plugging in the upper bounds for $P_{fail}(k)$ given in Lemma 4 and $P_{fail}(> 3)$ given in Lemma 6 in Lemmas 1 and 2, the probability P_{succ} of seeing at least one SET in a safe measurement period and the average number $1/P_{succ}$ of measurement periods until a safe one with some target SET hits is encountered can be computed. First, it turns out that P_{succ} is primarily determined by ρ, the ratio of the SET cross section of the entire target circuit over the SEU cross section of the entire counter architecture: As $P_{succ} \approx (1 - P_{fail}(1))C\rho$ for small ρ, even $P_{fail}(1) = 0$ would not lead to a value of P_{succ} larger than $C\rho$, which is $C/490$ for an inverter target (for some $C \in (0, 2]$). This illustrates the importance of keeping the infrastructure area as low as possible (Requirement 3 in Section 6.2) for keeping the average number $1/P_{succ}$ of measurement periods until observing the first useful target SET recording small. Our duplex-like architecture clearly surpasses a conventional TMR protection of the counter array in this regard.

Unlike standard duplication and comparison of individual counters, however, our architecture is (more than) single SEU-tolerant and can detect all the remaining double hits for sure, in addition to many multiple SEUs. Column $k = 1$ in Table 6.6 hence reveals very small values for $P_{fail}(1)$ for reasonable choices of C. As a consequence, erroneous SET recordings due to non-safe measurement periods

would be rare even when our architecture provided no additional SEU detection capabilities. By contrast, as hits in the counters are much more likely than in the target, $P_{fail}(1)$ for the standard duplex architecture would be close to 1; useful SET recordings would hence be rare. In this light, our SEU-tolerant redundant counter architecture appears close to optimal.

The low value of P_{succ} also makes it very unlikely to see more than three SETs per measurement period. As a consequence, the TMR-like behavior provided by our counter architecture will be guaranteed in almost all cases. Still, we can handle up to 7 target SETs per measurement period, albeit with a reduced level of SEU-tolerance. Note that Lemma 5, which underlies the derivation of $P_{fail}(> 3)$, holds only if we have $n \geq 5$ absolute counters (i.e., at least $N = 10$ counters overall). Given that an m-bit full-length LFSR has a count sequence of length $2^m - 1$, our choice of $m = 3$ and hence $n = 7$ is the smallest feasible one (unless we decide to go with part of the count sequence only, thus realizing $n = 5$, e.g.).

We conclude our discussion of the implications of our analysis by pointing out some additional issues that result from the flexibility of our architecture, which can be exploited in several different ways:

- When using the (unmodified) circuit in microbeam experiments, we can be sure to have hits in the target only. Up to $n = 7$ target SETs can be reliably recorded here. Note carefully that the SEU-tolerance of the measurement infrastructure will never be triggered to become active.

- By minor modifications of the measurement infrastructure, we can connect multiple targets to a single counter array in such a way that we leave a distance of 4 in between them: After a first recording in A_i, we continue with A_{i+2}, thus again obtaining a TMR-like behavior by leaving A_{i+1} at zero. Further SETs are then written to A_{i+1} and A_{i+3}. The minimum ring size here is 8, so we would need to extend n from 7 to 15 (by moving from a 3-bit LFSR to a 4-bit one and increasing the demultiplexer accordingly) in order to connect 3 targets in parallel: As the indexes assigned to each target are fixed, we can still associate each entry with the target that produced it.

- To increase the likelihood of observing target SETs, we could logically OR multiple targets. This effectively increases I_T and hence ρ, which also leads to a higher number of target SETs in a single measurement period and hence a better utilization of our counter array. However, we cannot associate a given SET recording with some particular target anymore.

- The very simple and modular structure of the UDC makes it easy to adapt the depth of the UDCs to the expected maximum count, which depends both on the ring oscillator frequency and the LET value of the ionizing particles.

6.10 Summary

We have presented a measurement infrastructure that records multiple SET pulsewidths in digital circuits. We also analyzed the implementation options for building an all-digital, radiation-tolerant circuit for measuring SET pulsewidths using analog simulation. The speed of the counter proved to be the limiting factor, a fast up-counter based on a Muller Pipeline in conjunction with carefully placed switches in the oscillators feedback loop was found superior over all alternative solutions. The major design challenge has been the exposure of both the target and the measurement infrastructure to the same radiation environment. The intended operation of our architecture has been verified by means of SET injection experiments that led us to build a comprehensive fault dictionary. We also introduced a probabilistic analysis which showed that, for a given particle flux, a suitable duration of the measurement period can be found by which at the same time (a) a sufficiently high probability of at least one target hit can be achieved while (b) the measurement period is still safe. We can hence claim that our measurement architecture indeed fulfills its purpose.

CHAPTER 7

Target FRad ASIC

The primary objective of this chapter is the design of the radiation target digital ASIC, which includes the on-chip data transmission architecture. We adequately explain the design of the ASIC step by step from the concepts to the fabrication phase in great detail. This chapter amalgamates the designs presented in Chapters 4 and 5, i.e., all the measurement infrastructures designed for understanding SET sensitivity and SET propagation will be implemented in this ASIC. The measurement architecture used in these infrastructures must facilitate the intermediate monitoring and recording of all SETs in the target circuits, at the level of digital signals in long term experiments.

To get as much SET data as possible from a radiation experiment, as many nodes in our target circuits as possible must be monitored simultaneously. To analyze the SET data recorded by the counters, we need to communicate all the data from the ASIC to the PC. If we feed all these counter data directly to the output pads, then we will not be able to use all the planned infrastructure in a single ASIC. As mentioned before we are interested in continuously monitoring the targets with the counters, and the reason behind the usage of counters is to collect data for post processing. On-chip pre-processing is used to reconcile these requirements:

- We extract SET occurrences out of the possibly superposed dynamic operation of the DUTs as early as possible.
- Since we are not interested in the precise time of occurrence of SETs in statistical analysis, it suffices to just count the number of SETs in consecutive measurement periods, at the end of which the counts will be transferred to some off-chip data recording unit and be reset.
- To save pins, the data transfer will be performed serially using *parallel-in serial-out* (PISO) circuit.

7.1 On-Chip Data Transmission Architecture

Each measurement infrastructure has around 30-bits, 75-bits, 84-bits or 110-bits of data to be transferred for post processing. If we employ one pin for each bit, then our ASIC would become pad limited; but by employing a PISO on-chip to seed the data out of the counters via a single output pin our ASIC has attained a good balance between usage of pins and area. The basic principle behind the PISO is presented in Sec. 3.5.1.2.

7.1.1 Application Requirements

It is worth mentioning that some of the radiation sources we envision for our physical experiments with the chip (atomic reactor, e.g.) do not allow to control location or time of radiation particle impact. This means that:

(i) we must expect particles hitting the measurement infrastructure and PISOs

(ii) we cannot restrict radiation to the measurement phase only, SETs will rather occur during data readout as well.

To counteract (ii) we keep the data transmission intervals much shorter than the measurement period; this can essentially be done by a proper arrangement of particle rate/energy, number and width of LFSRs as well as readout clock. In addition we have to keep in mind that all protection measures we implement for the PISO will tend to slow down its operation, thus reducing the applicable readout clock. (i) is the reason why we need to incorporate radiation tolerance in PISO. In addition, it is important to keep the area of the PISOs as small as possible, for two reasons: Firstly, smaller area means lower probability of a particle hit; and secondly target circuits and infrastructure compete for the same die area – by keeping the infrastructure small we can afford more area for target circuits.

In principle we can distinguish four different robustness levels for our counter and PISO, refer to Sec. 3.5. In order to be able to rely on the collected experimental data, we must take care to consider errors on the target circuits only in our statistics, not those on the counters or PISO. In principle, even *level (a)* in the list presented in Sec. 3.5 fulfills this requirement. However, as SET occurrences on the target are expected to be relatively rare, we are interested in not losing too many of them by having to discard results. After all, considering its relative area, we have to expect a noticeable number of hits in the counter as well. We can also infer the same from the probabilistic analysis presented in Chapter 4 (Over long term measurement periods we will observe a considerable number of upsets in the target circuits and the probability of upsets in the measurement circuits is higher than that for the target circuits) and Chapter 6 (the probability of an upset in the infrastrcuture is higher than the target). To attain *level (b)*, the counters therefore need to exhibit radiation tolerance as well. Multiple upsets in the counter, however are expected to be rare; hence, it would be sufficient to just recognize them.

Interestingly counters and PISO have substantially different requirements for radiation tolerance, due to the nature of their operation. The counters are initialized at the start of a measurement period, and they have to maintain a correct count value throughout the complete measurement period until their values have been captured into the PISO in the subsequent readout phase. The PISO has one control logic per stage, so the area of the combinational logic is about the same as that of the flip-flop. The PISO is only activated for the data transfer after the measurement period. During this short phase it will be operated in a highly dynamic fashion (recall that we want to keep the readout period short, so we will apply the highest possible clock). Therefore bit flips of the flip-flops are very unlikely relative to SETs in the combinational logic. The effect of a particle hit is different in the flip-flops and the control logic:

- A single upset in a flip-flop will cause the transmitted count value to be wrong by one bit, and this is reliably recognized by plausibility checking.
- An SET in the combinational multiplexers, on the other hand, has the potential of causing more global problems with the process of parallel loading and shifting of data, thus leading to unpredictable behavior.

In summary the control logic of the PISO requires more attention than the flip-flop.

7.1.2 Operation of PISO

Each and every measurement circuit will have 30, 75, 84 or 110 binary outputs, and a suitably designed PISO circuit must be used to enable serial data transmission via one single output pin. The operation of the PISO is illustrated using a 4-bit PISO presented in Fig. 3.26. Every stage (except the very first one) consists of a D flip-flop for storage and an AND-OR selector required for selecting parallel load vs. shift-out: The PISO register, formed by the D-flip flops, is loaded in parallel upon a clock transition when *SHIFT* is low, and is shifted out serially with every clock cycle after setting *SHIFT* to high. In general, these elements can be replicated for the number of stages required, i.e., the 4-bit can be expanded to 30-bit PISO by adding 26 flip-flops and AND-OR selectors.

The simulation of a 4-bit PISO in three different time intervals from the ASIC perspective is presented in Fig. 7.1. This waveform would help us understand the operation of the PISO better. The figure shows all the relevant signals of the PISO. One can notice that the clock is toggling even while the reset is performed. It can also be observed that the last data "D_3" comes out first and the first data "D_0" comes out last. The last data is repeatedly latched with every extra clock cycle (more clocks than required for the PISO) until there is an activity in the shift/reset.

Three of the most crucial control signals of a PISO are the clock (CLK), the reset (RST) and the shift (SHIFT), and their sequence of operation is of extreme importance. Some facts of the control signals are listed as follows:

(i) The shift signal may remain "low" or "high" while the PISO is reset.

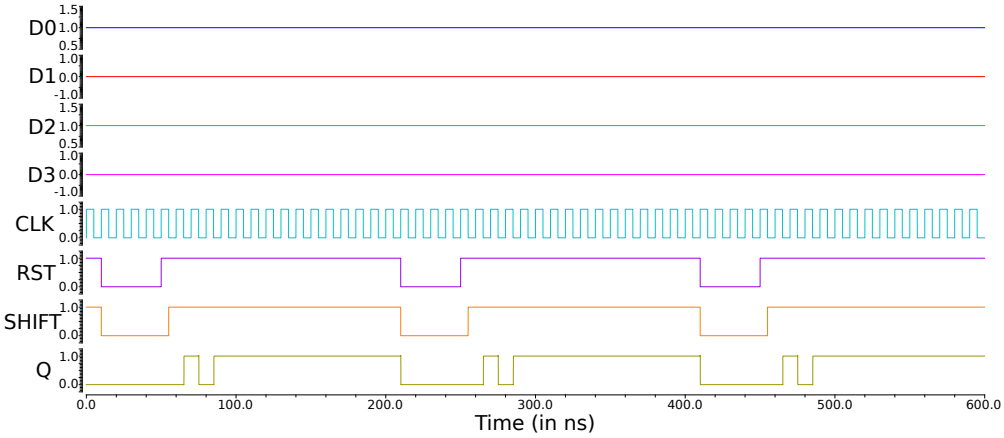


Figure 7.1: Simulation of 4-bit PISO

(ii) To allow data loading into the PISO after initializing it, if the shift signal is "high" then it must be steered to "low" (refer (a) in the Fig. 7.2).

(iii) The clock signal must toggle before the shift signal is set to "high".

(iv) When the clock signal is "high" then the shift signal is steered to "low" and remains "low" when the clock is "low" (refer (b) in the time diagram). There must be a delay of t_1 between both the clock (steered to "high") and shift (steered to "low") signals to avoid timing violations as indicated in Fig. 7.2.

(v) When the clock signal is "high" after a delay of t_2 the shift signal is steered to "high" to avoid any metastability within the PISO (refer (c) in the timing diagram)

(vi) The actual data transfer takes place with the negative edge of the clock signal and when the shift signal is "high".

(vii) Ideally after transmitting the data the clock must be stopped to avoid dynamic power consumption.

There is no other means of verifying the data of the measurement counters in the ASIC. One can only validate the operation of the counters using the PISO, and hence, the operation of PISO must be thoroughly understood.

7.1.3 Architecture Options

To accomodate multiple targets and measurement infrastructures within the ASIC, we proposed multiple implementations of the PISO:

1. Usage of a single PISO for one measurement infrastructure
2. Usage of a shared PISO for multiple measurement infrastructures

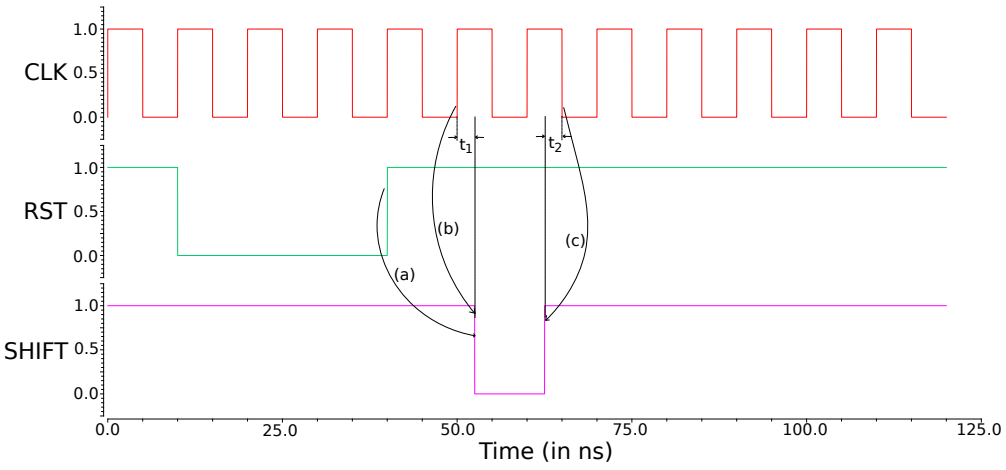


Figure 7.2: 4-bit PISO Timing diagram

(a) Non rad-hard architecture

(b) Partial rad-hard architecture – protection provided for the multiplexors

(c) Rad-hard architecture

The process of determining the most area-efficient tradeoff involves building and analyzing all these PISO structures. The largest PISO in the ASIC is 110-bit wide. Ideally, to transmit the data from the ASIC to outside environment (termed as "transmission delay") would take approximately 115*T_{clk}, where T_{clk} is the clock delay.

7.1.3.1 Single PISO – Measurement Infrastructure

We connect the output data bits of the counters of a single measurement infrastructure directly to the parallel input ports of the PISO.
Benefits – The amount of time consumed to transfer all the counter data from the ASIC is equivalent to the time consumed by the largest PISO to transfer the data to the PC.
Pitfalls – Any SET/SEU in the PISO during the read-out (only when exposed to ambient radiation) will have incorrect data transmitted to the PC.

To avoid erroneous data transmission we provide tolerance to the PISO using the rad-hard mechanisms (dice, rad-hard by sizing, rad-hard by separation,etc.) presented in Sec. 3.5.2.6, 3.5.2.7, 3.5.2.8. All the options presented increase the area of the PISO at least five-fold, thereby reducing the die area for the target and measurement circuits. Hence, we chose to use time redundancy instead to provide tolerance.

Time redundancy basically involves executing the same operation with the same inputs in "n" different time intervals and in the end voting on the output received in all the "n" different time intervals. Of course, there is a risk of the voter being hit

by an SET with this mechanism. In our case the voting is done in the PC, hence this is a perfect alternative for our ASIC.

In our case we transmit the data from the ASIC using the PISOs at three different time intervals (t_0, $t_0 + \Delta t$, $t_0 + 2\Delta t$) to the PC. Note that the probability of a fault occuring at the same location in all the three different time intervals is negligible. Therefore, we can reasonably be sure that this mechanism would provide enough tolerance for the data in the counters.
Benefits – Any data loss due to an SET in the PISO can be recovered without any hassle, as we have three readouts of the same data.
Pitfalls – The read-out time of the ASIC has increased three fold when operating in time redundancy.

7.1.3.2 Single PISO – Multiple Measurement Infrastructure

A *multiplexor* (MUX) is employed to reduce the number of PISOs in the ASIC, i.e., in the place of four PISOs we employ one PISO using 4:1 MUXes. The MUX basically combines the data outputs of four similar measurement infrastructures (A_0, B_0, C_0, and D_0) to a single PISO input (Z_0), where the data connected to the PISO is chosen by the two select bits (S_0 and S_1) of the MUX.

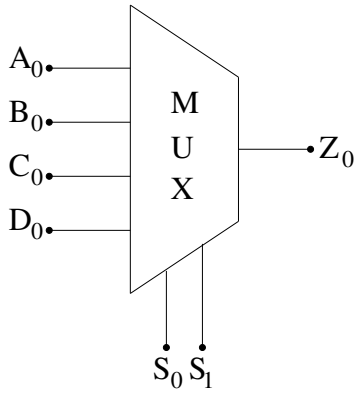


Figure 7.3: Block diagram of 4:1 MUX

For an n-bit measurement infrastructure (where "n" denotes the total number of data bits of all the counters) we would need "n" MUXes to successfully implement this transmission structure.
Benefits - It enables us to use a lot more measurement infrastructures in the ASIC thereby utilizing all the die area.
Pitfalls - The transmission delay of the ASIC is quadrupled, when four measurement architectures employ a single PISO.

Radiation-Hardening – Any SET within the MUX or the PISO could transfer false data to the PC. To avoid such a scenario, we provide tolerance using some of the classic mechanisms. All these mechanisms in the literature increase the die

area at least by 5 times compared to a normal PISO, refer Table. 3.6 for details. The goal behind the usage of MUXes with PISO is to reduce the die area and hardening them defeats their purpose.

Partial Radiation-Hardening – Instead of hardening both the PISO and the MUXes; we decided to harden the MUXes alone using hardening by sizing mechanism. As a result the die area of the MUX increased 22 times, which is almost equivalent to the die area of one non rad-hard PISO. From this analysis we can conclude that even partially hardening the transmission architecture is expensive in terms of area.

Non Radiation-Hardening – Instead of hardening the architectures in space we decided to let it be as is and use time redundancy to provide tolerance. The principle behind this mechanism is the same as mentioned before; we read the data from the PISO at three different time intervals. Any SET/SEU within the PISO or MUXes can be resolved with this mechanism in place.
Benefits - It enables us to use a lot more measurement infrastructures in the ASIC thereby utilizing all the die area.
Pitfalls - Transmission delay is increased to twelve times the delay of the largest PISO, when four measurement architectures employ a single PISO.

7.1.4 Summary

The actual design of the PISO used in the ASIC is complicated by two facts:

(i) Being on-chip, the PISO must be protected against radiation effects as long as it holds relevant data; which is during transmission.

(ii) Read out ($T_{readout} < T_{radiationtime}$) must be fast to minimize the risk of having a counter change (due to an SET) while being read.

$T_{readout}$ – Read out delay of the ASIC.
$T_{radaition}$ – The amount of time the ASIC is exposed to radiation before a read-out is performed.

We concluded to solve (i) and (ii), by employing temporal redundancy instead of triplicating the PISO or opting for a rad-hard implementation - that would both cause high area overhead and still not solve the second issue. Now the remaining question is which architecture to employ: (a) Single PISO per infrastructure or (b) Shared PISO per four infrastructures.

Comparison of the two architectures are listed below:

- Read-out delay
  - Employing a MUX to use multiple infrastructures, strains $T_{readout}$ of the ASIC.

  - A state machine that would automatically operate the MUXes and transfer all the relevant data of the PISO can be constructed. Hence, we may not select the measurement architectures manually, but instead operate the ASIC systematically for architecture (b).
  - The data transmission delay of the architecture (b) is estimated to be five times that of (a), when taking into account the delay of all the MUXes for switching between the different measurement infrastructures.

- No. of pins required
  - Architecture (a) requires one output pin per PISO, hence it will use four output pins for four measurement architectures.
  - Architecture (b) requires only one output pin for four measurement architectures. But, it requires two input pins for selecting the measurement architectures using the MUXes. Note that all the MUXes can use the same inputs for selection.

- Die area
  - Architecture (a) consumes area of four PISOs for four measurement architectures.
  - Architecture (b) consumes one PISO for four measurement architecture, and the number of MUXes employed depends on the width of the PISO. Typically the area of the MUXes and the routing is equivalent to area of one PISO. So, architecture (b) consumes half the area consumed by architecture (a)

The choice of the architecture is complicated by the facts listed below:

- Ideally, while operating the ASIC at 100MHz, we should be able to conduct 90 tests over an hour (where for each test: $T_{radiation}$ would be estimated at 40s, and $T_{readout}$ for architecture (a) less than 10us and (b) less than 50us). This read out delay is still reasonable for (a) and (b).

- Assuming the particle rate in the radiation chamber is very high and to have usable data, we perform read outs quite often; then $T_{radiation}$ would be reduced, and the $T_{readout}$ remains the same. Especially, this could be the case in ambient radiation where we may have to perform read outs for every fifty or hundred transitions in the ASIC to have usable SET data. We already know that the $T_{readout}$ of architecture (b) is higher than (a). There is a very high probability that in this case of architecture (a) $T_{radiation} = T_{readout}$, then for architecture (b) $T_{radiation} < T_{readout}$.

Considering the particle rate and to keep the read out delay low we decided to use architecture (a) instead of (b); even though (b) would provide us with a lot more SET data than (a).

7.2 ASIC Architecture

The custom architectures that can analyse SET sensitivity, SET propagation, and SET distribution were initially designed in UMC $90nm$ bulk CMOS technology. However, we plan to host all these architectures in the "FRad Chip" after redesigning them in UMC $65nm$ bulk CMOS technology. As we know that the critical charge of a transistor in $65nm$ is lower than that of a $90nm$, thereby, we can conclude that a transistor designed in $65nm$ is more vulnerable to SETs compared to one in $90nm$. Therefore, one can expect that the measurement infrastructure designed in $90nm$ CMOS technology would function properly in $65nm$. But, in order to be reasonably sure we must verify the functionality of these architectures in $65nm$; i.e., we must conduct functional simulation and SET injection simulation in these architectures in $65nm$ technology.

7.2.1 FRad Overview

The radiation target ASIC hosts a set of target, measurement and data transmission architectures to analyse SEEs, furthermore, to have relevant results:

* Targets that are both elementary and frequently used in practice were selected

* The targets are stimulated to understand state/frequency dependence of SEEs

Taking these into consideration a set of target circuits that were presented in Chapters 4 – 5 were used in the ASIC. We elaborated previously that we employ a measurement architecture that does not need to rely on any rad-hard counters to provide protection against SETs. Ultimately, by leveraging parts of our measurement infrastructure, we also have asynchronous Up/Down counters (UDCs) (which are essentially Muller pipelines) and LFSRs available as targets.

Note that we did not implement the architectures that were presented in Chapter 6 in this ASIC. In the first fabrication run we decided to only implement the architectures to measure sensitivity and propagation becasue this is our test ASIC. We want to validate if the architectures indeed work to our expectations. When the ASIC successfully passes this phase of testing, we will initiate the second fabrication run in which we will also include architectures to measure the pulsewidhts of an SET.

7.2.2 Requirements

The basic requirements of the "FRad Chip" have been presented in Sec. 1.3. Requirements (other than the ones presented in Sec. 1.3) to which the targets and measurement architectures must adhere to are presented in the Chapters 4& 5.

As the requirements are already elaborated we will directly focus on the intricate part of our ASIC that is the layout. The layout of our ASIC is complicated by the need to separate the target, the measurement and the data transmission circuits; to be able to focus the ion beam on the targets without any hassle in a controlled radiation

experiment. Therefore, instead of using an automatic place and route tool to create the layout of the digital ASIC, we decided to use a snap together custom cell layout.

7.2.3 Specifications

→ ***Manufacturing Technology***: UMC L65LL a 65nm generation CMOS process technology based on P-sub structure with 10 layers of copper metal and low-K dielectrics is employed. This technology is specifically for low power consumption application such as handheld product design.

→ ***Standard Cell Library***: UMK65LSCLLMVBBR tapless standard cell library based on UMC's 65nm Low-K low leakage RVT process is used. Using only metal one within the cell layout, this library offers 216 cell types and the total cells amount to 1088 with multiple drive strengths included in each cell type. Supporting most metal options in UMC, UMK65LSCLLMVBBR is applied with voltage ranging from 0.9 V to 1.32 V.

→ ***IO Library***: The L65LL BOAC in-line IO library that offers a wide range of functional and performance options for IOs. This IO library allows users to modify the IO slew rate and driving strength of silicon by changing the logic state of slew rate and strength control pins, which minimizes the effort of designers in obtaining the optimal electrical solution. The library is divided into group of 1.8V/2.5V/3.3V CMOS IO cells.

→ ***Bondpad pitch***: This is the centre distance between two adjacent bond pads and for our ASIC we chose it as 80um.

→ ***ASIC area***: The area of the typical mini@sic offered by IMEC through special MPW (multi-project-wafer) prototyping conditions is 1875um X 1875um.

→ ***Total number of pads in ASIC***: 84

→ ***Pads per side of the ASIC***: 21

→ ***Supply pins for core logic***: 6

→ ***Supply pins for IOs***: 6

→ ***Ground pins for IOs/core***: 12

→ ***ASIC input pins***: 16

→ ***ASIC output pins***: 44

→ ***Core power supply***: 1.08V (min), 1.2V (typical), 1.32V (max)

→ ***IO power supply***: 2.25V (min), 2.5V (typical), 2.75V (max)

→ ***Dimensions of the IO, supply and ground pads***: 88.8um (height) X 60um (width)

→ ***Dimensions of the corner pads***: 88.8um X 88.8um

→ ***Operation frequency of the data and clock signals***: 100MHz (maximum)

→ ***Typical operating temperature of the ASIC***: -40^{o}C (min), 25^{o}C (typical), 125^{o}C (max)

7.2.3.1 SET Sensitivity

The set of target circuits we chose to understand SET generation and sensitivity in this ASIC are listed in Table. 7.1. We also used elementary combinational (inverter, NAND, NOR, XOR, Muller C-element) and sequential (D-flip-flop) elements as targets. We combined the basic standard logic gates with a 4:1 MUX. Similarly, the C-elements and flip-flops with different drive strenghts were combined using a 4:1 MUX. We used two different measurement architectures to monitor SEEs in these targets: (1) uses two LFSRs and two UDCS (refer architecture F in Chapter. 4) and (2) three UDCs (refer architecture D in Chapter. 4). We aim to verify the probability of two SETs occurring in the three-UDC architecture in such a way that no useful data is recoverable. Finally, we also want to verify the reliability of the combined LFSR/UDC architecture which we deem more efficient.

Table 7.1: SET Sensitivity Architectures

Target Circuits	Measurement Circuits	PISO
Inverter Chain	2 32-bit LFSRs & 2 UDCs	84-bit
	3 UDCS	30-bit
NAND-NOR Tree	2 32-bit LFSRs & 2 UDCs	84-bit
	3 UDCS	30-bit
Flip-Flop Chain	2 32-bit LFSRs & 2 UDCs	84-bit
	3 UDCS	30-bit
Elastic Pipeline	2 32-bit LFSRs & 2 UDCs	84-bit
	3 UDCS	30-bit
4:1 MUX	2 32-bit LFSRs & 2 UDCs	84-bit
	3 UDCS	30-bit

7.2.3.2 SET Propagation

To monitor SET generation and propagation in the ASIC we chose the Sklansky adder and inverter tree as targets. Having activity in the Sklansky adder will make the operation itself complicated, on top of that monitoring SETs in the same would be infeasible. Hence, we decided to operate the Sklansky adder in static mode, in a state where all carry outputs are likely to fire in case of an SET. We basically employed 5-bit LFSRs at the outputs of the adder and at the outputs of the gray

cells in the critical path. In order to collect the number and location of upsets due to particle impacts in the critical path and also study SETs in blocks (i.e., half adders, gray cells, black cells) that are not part of the critical path we augmented our target with 22 5-bit LFSRs. It is safe to say that having the counters just at the outputs will be sufficient to analyze the *generation* of the SETs in all the blocks.

Like with the Sklansky adder we again chose to operate the inverter tree in static mode to simplify the infrastructure for monitoring SET propagation. However, we need to factor in fault masking, so we cannot assume that a transition, once entering the chain, will actually propagate all the way through it. Therefore, we need a consistent view of counter values within each stage, i.e. without the support of information from the adjacent stages. Only then we can reliably make conclusions on faults that have popped up or vanished since the previous stage. Keeping this in mind we added counters, more specifically 5-bit LFSRs, in all output nodes of the inverter in the tree. In total we used 15 LFSRs to monitor SET propagation.

In order to have a clearer picture of SET generation and propagation we also used a 5-stage D-flip-flop chain and 3 stage Muller pipeline as targets. To analyse SET propagation we monitored the outputs of all the flip-flops in the chain. We connected the data signal of the chain to ground and operated the clock at nominal frequency, thereby propagating any upset to the next stage. In the pipeline we monitored the outputs of all the C-elements and the inverters. We didn't ground any of the input signals in the pipeline, to allow monitoring SETs in the pipeline in three different modes: full, empty and half-full. In a controlled environment we can extract far better SET data from these two targets, compared to the others. Furthermore, with this SET data we could better analyse the data recorded by the other flip-flop chains and pipelines. Therefore, to monitor the SETs we added 5-bit LFSRs in the critical nodes of these targets (refer Table. 7.2 for the number of LFSRs).

Table 7.2: SET Propagation Architecture

Target Circuits	Measurement Circuits (5-bit LFSRs)	PISO
5-stage flip-flop chain	5	25-bit
3-stage Muller pipeline	11	55-bit
Sklansky Adder	22	110-bit
Inverter tree	15	75-bit

7.2.3.3 PISO

We have different flavors of architectures and each flavor requires a unique PISO for data transmission, as shown in Table 7.1, 7.2. From the table we can interpret that the measurement infrastructure that uses two 32-bit LFSRs and two 10-bit UDCs

has their data transmitted using 84-bit PISO. Note, that we have several instances of the same architecture in the ASIC, and for all those architectures we use the same length of PISO. In total we have used 44 PISOs in the ASIC:

* 25-bit PISO - 1
* 55-bit PISO - 1
* 75-bit PISO - 3
* 110-bit PISO - 3
* 30-bit PISO - 18
* 84-bit PISO - 18

The list of structures presented so far are the components that are employed in the ASIC, and we basically provide an overview of the same and their purpose.

7.3 ASIC Layout and Implementation details

We constructed the transistor level schematics of all our targets, measurement counters and data transmission circuits in UMC $65nm$ LL bulk CMOS technology using Cadence Virtuoso (Version IC6.1.6). We used the schematics from the standard cell library (refer Sec. 7.2.3) to create leaf cells of complex structures in transistor level. The standard cell library does not have asynchronous elements included in it. So, we custom built and characterized a transistor level schematic of Van Berkel Muller C-element using the PMOS and NMOS provided by the technology library. We also configured the C-element to have the "set" (steer the output of the C-element to low) and "reset" (steer the output of the C-element to high) capabilities to construct the up/down counters. The correct functional operation was verified, first for each of the circuits individually and then for the whole infrastructure using Cadence Spectre and HSPICE.

7.3.1 ASIC Floorplan

Floor planning is the most fundamental step in ASIC physical design. In this stage we basically decide the following: Die size, core size of the chip, and I/O pad's location. Some details on the placement of the I/O pads are listed below:

→ All the I/O pads used have the same height, hence must be properly placed such that I/O pad power rings of all the pads are connected with each other.

→ Generally I/O pads are not placed in the corner of the chip and we use corner cells that fill the gap and provide I/O pad power ring connectivity.

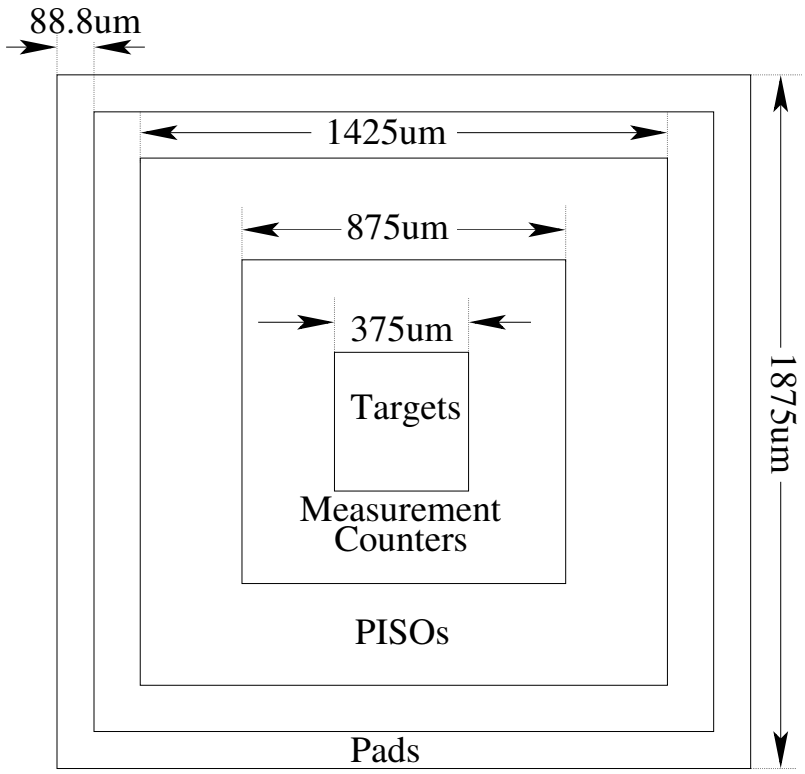


Figure 7.4: ASIC Floorplan

→ Filler cells are used in between I/O pads to maintain a reasonable bondpad pitch. Similar to corner cells they fill the void and provide I/O pad power ring connectivity.

The I/O pad placement of the ASIC is presented in Fig. 7.4. Note that we cannot use an automated place and route tool to build our ASIC, rather we have to do a manual layout, as we have very specific constraints in the placement of the circuits. Specifically, we decided to place the target circuits in the center and surround it by measurement circuits which are in turn surrounded by PISO, as shown in Fig. 7.4. The actual area allocated by us for the different structures in the ASIC are listed below:

→ Targets: 375um x 375um

→ Measurement Counters: 875um x 875um - 375um x 375um

→ PISOs: 1425um x 1425um - 875um x 875um

→ BondPads: 88.8um x 88.8um

Table 7.3: Leaf Cells with die area

Circuit	Area (in um2)	No. of Instances	Total Area (in um2)
Inverter Chain	39.1	24	938.4
Nand-Nor Tree	193.24	24	4637.76
Elastic Pipeline	309.31	24	7423.44
Flip-Flop Chain	142.58	24	3421.92
Sklansky Adder	4495.63	3	13486.89
Inverter Tree	47.48	3	142.44
Inverter	2-11	6	12-66
NAND	2-11	6	12-66
NOR	2-11	6	12-66
XOR	2-11	6	12-66
Vanberkel Muller C-Element	13.13	6	78.78
D-Flip-flop	2-11	6	12-66
32-bit LFSR	1792.84	36	64542.24
5-bit LFSR	119.34	111	13246.74
10-bit Up/Down Counter	671.78	90	60460.2
84-bit PISO	6758.48	18	121652.64
110-bit PISO	9629.56	3	28888.68
75-bit PISO	6782.1	3	20346.3
30-bit PISO	1812.46	18	32624.28
Target			30459.63
Measurement			138249.18
Transmission			203511.9

7.3.2 Layout and Placement

Considering that our initial outset was to dedicate as much area as possible for the target cells, it is interesting to observe the area consumption of the different blocks, as given in Table 7.3. We allocated 140625 um^2 area for the targets, but they consume only 30459.63 um^2 (excluding the routing area). Note that for the basic gates we do not provide this info in detail, as it is guarded by an NDA, hence we only give a range. The leaf cells of the characterized C-element is presented in Fig. 7.5. The leaf cell of C-element configured with the "set" and "reset" signals is presented in Fig. 7.6 & 7.7. Please note that we presented the layouts of some of the circuits, to have a basic understanding about the layout and routing complexity of the structure.

We performed a snap together cell layout for all of them, some of which were quite straightforward (inverter chain, Muller pipeline, flip-flop chain, etc.), while other were a little complex (nand-nor-tree, inverter tree, etc.). The inverter chain

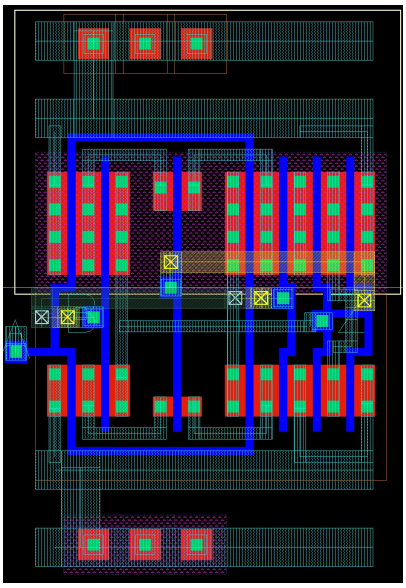


Figure 7.5: Muller C-element Layout

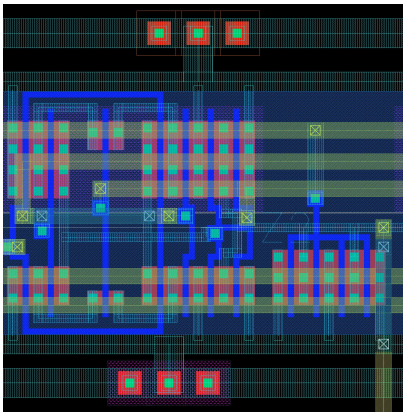


Figure 7.6: Muller C-element with “set” Layout

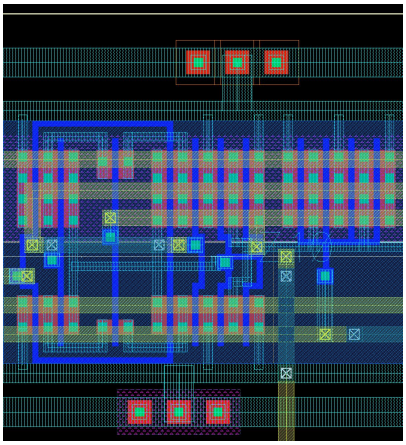


Figure 7.7: Muller C-element with “reset” Layout

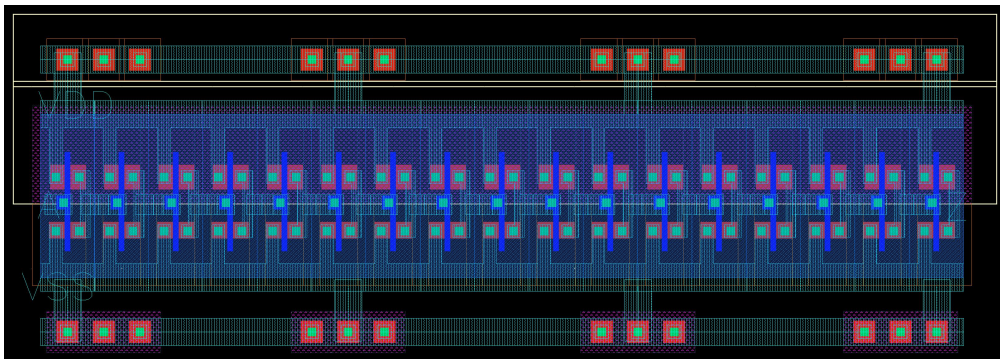


Figure 7.8: Inverter Chain Layout

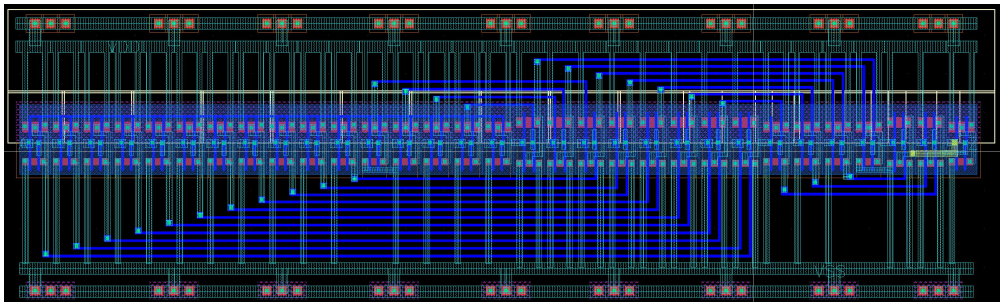


Figure 7.9: Nand Nor Tree Layout

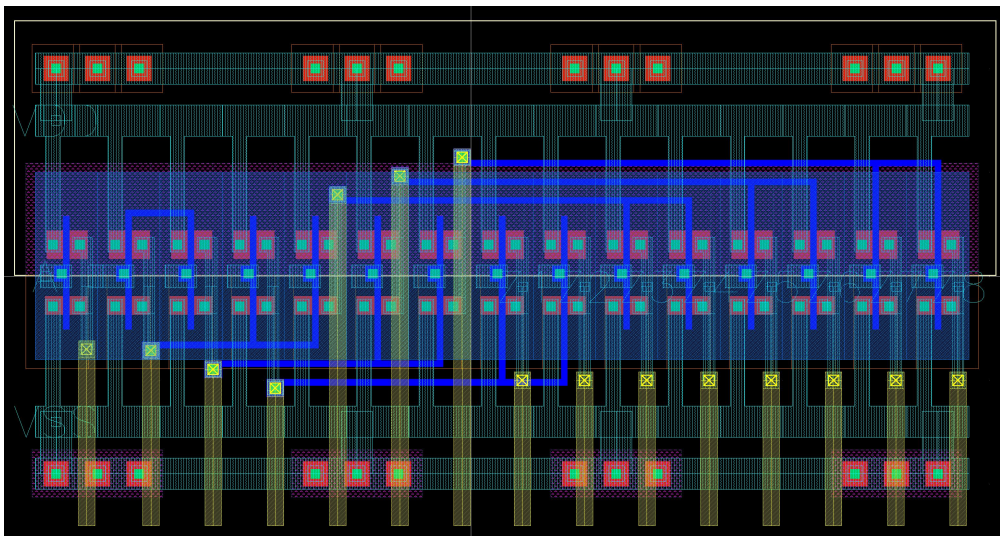


Figure 7.10: Inverter Tree Layout

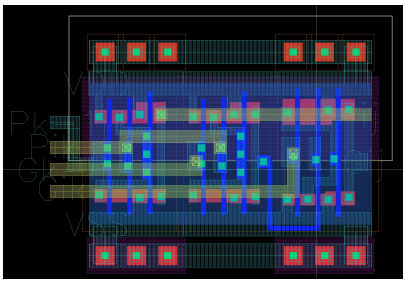


Figure 7.11: Black cell Layout

presented in Fig. 7.8 shows that the layout is quite simple. There is no routing needed as the first inverters' output snap to the second inverters' input in the chain and so on. From Fig. 7.9 we can observe that even though we created a snap together cell layout of the NAND and NOR; the routing of the outputs of the first stage of NAND to the next stage of NOR is a little complex. Similarly, we can also observe from Fig. 7.10 the routing complexity between the inverters.

There are also some circuit blocks such as Sklansky adder and PISOs that require a lot more effort in placement of leaf cells let alone routing. The Sklansky adder uses components such as gray cells, black cells and half adders. We created the leaf cells of these basic components (refer Fig. 7.11, 7.12, 7.13), not shown in the Table 7.3. Using these leaf cells we created a snap together cell layout of the Sklansky adder as shown in Fig. 7.14. The routing complexity for this adder is higher than the other targets, and thereby the area consumed by it is linear with the routing complexity. We used two different metal layers for horizontal routing and vertical routing. We do not use the same metal layer for both horizontal routing and

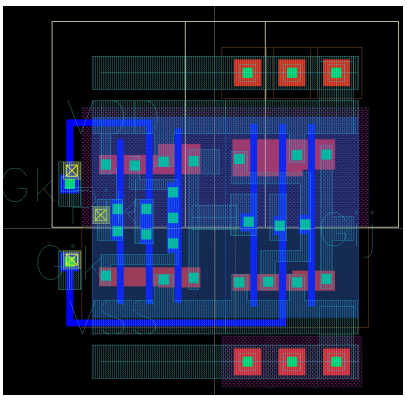


Figure 7.12: Gray Cell Layout

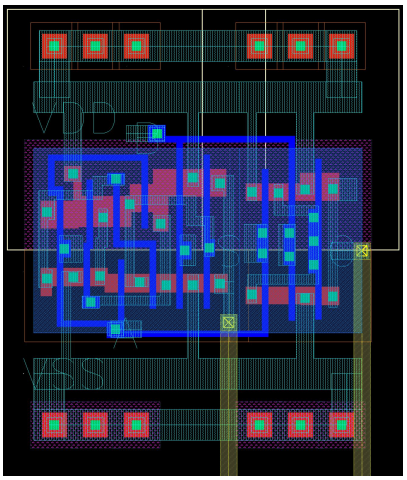


Figure 7.13: Half Adder Layout

veritcal routing within a block to avoid short circuits.

We use different lengths of PISO in our ASIC. As a first step we created a leaf cell with one MUX and flip-flop and using this instance we create a snap together cell layout of the PISO. The largest PISO in our ASIC is 110-bit PISO. If we created such a layout using 110 instances, then we would end up with a very long PISO. To avoid such an scenario we split the snap together cells into pieces of 10 or 20 instances per row, and create multiple rows for a PISO. In the case of 30-bit PISO (refer Fig. 7.17) we created a row of 10 instances and ended up with three rows. From the Figs. 7.15 , 7.16, 7.17 & 7.18 we can observe the efforts taken in terms of routing the signals from the measurement counters to PISO.

We can conclude that creating these leaf cells is not very straightforward and it takes a lot of effort and insight in constructing one. We conducted DRC (*Design Rule Check*) and LVS (*Layout Versus Schematic*) tests on all these leaf cells using

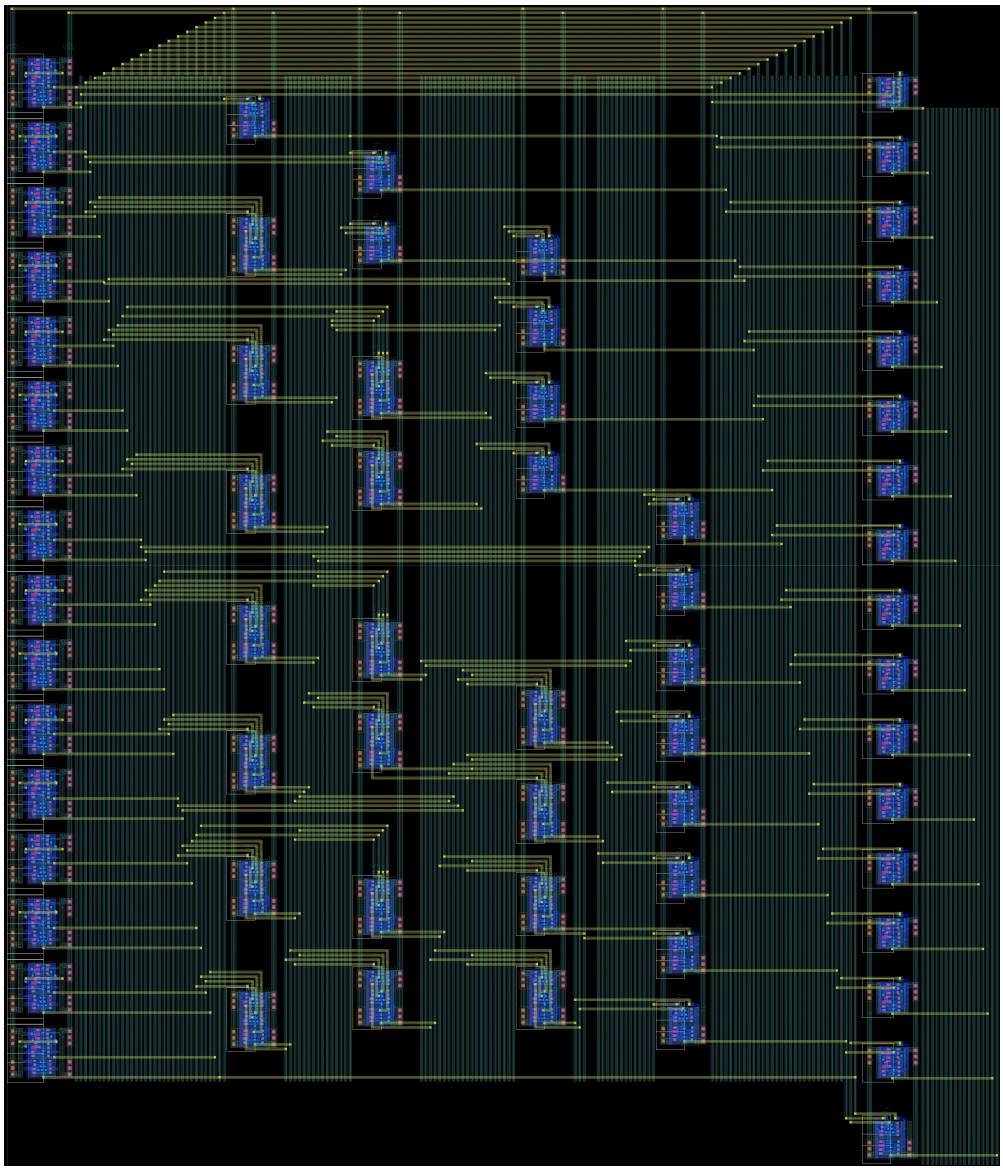


Figure 7.14: Sklansky Adder Layout

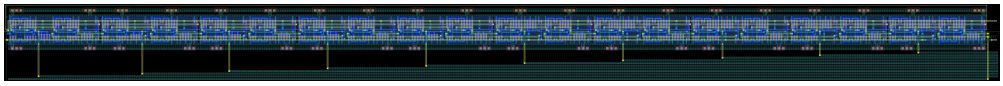


Figure 7.15: Up/Down Counter Layout

Figure 7.16: 32-bit LFSR layout

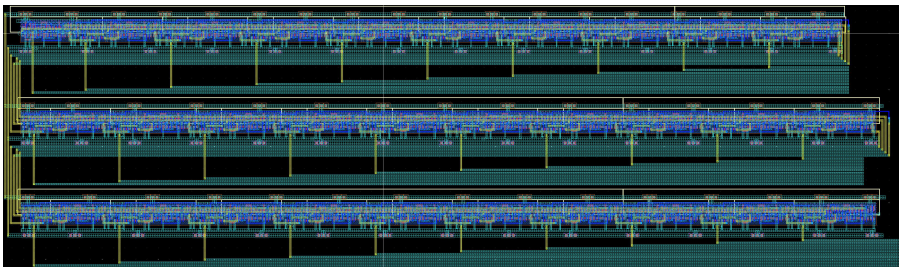


Figure 7.17: 30-bit PISO layout

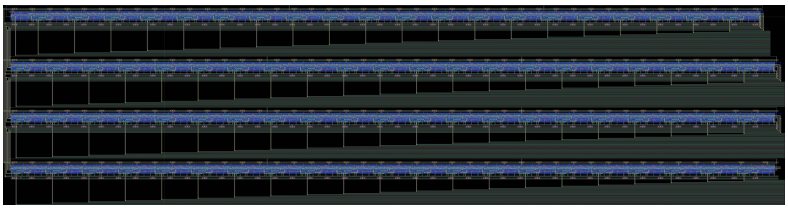


Figure 7.18: 84-bit PISO layout

Cadence Assura. Upon successful completion of these tests, we extracted the netlist using Assura and verified the functionality of the same using Cadence Spectre.

After verification we started the placement of all these cells in the ASIC. We placed the leaf cells of the target within the square shown in Fig. 7.4. Later, we placed the measurement counters on the ASIC. We placed them such that the counters are nearer to the targets, thereby reducing the routing overhead between them. Similarly, we placed the PISOs next to the counters. After successfully placing all the cells we manually did the routing between them. After completing the routing between all these cells we routed the output and input signals to the respective pads as discussed in Sec. A.1.

We added a couple of recognizers in the ASIC:

1. An alluminium ring around the target was added to recognize the location of the same.

2. Two logos as shown in Fig. 7.19 were added to know the orientation of the ASIC after fabrication.

In Fig. 7.19, it can be seen that the targets, measurement counters and finally PISOs are each surrounded by concentric yellow squares, which is *METAL layer*

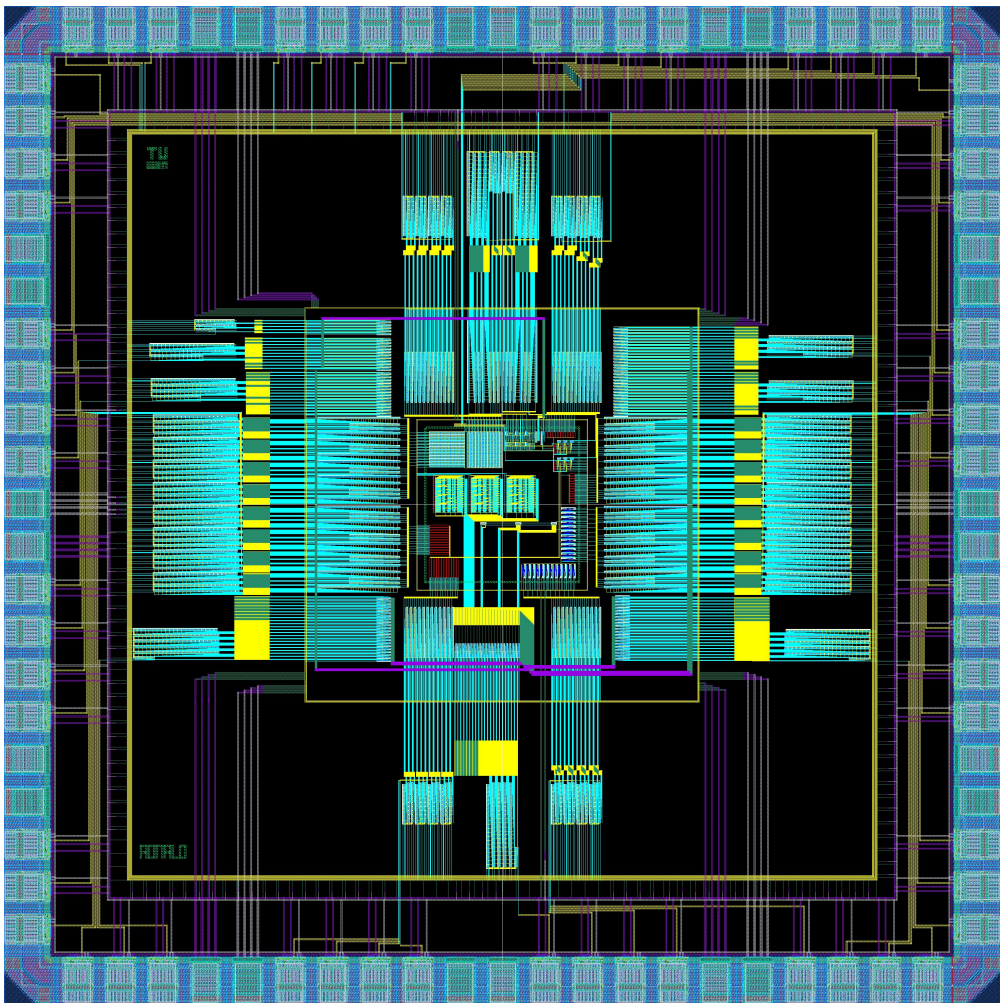


Figure 7.19: ASIC layout with Targets, Measurements and PISO circuits

2. This arrangement will be useful for experiments with well controlled radiation, like the micro beam, as it allows us to focus the radiation to the target circuits only while keeping the infrastructure and PISO free from SETs. Alternatively, to test the infrastructure's radiation tolerance, the latter can be specifically exposed to the radiation.

We can also observe from the figure that there is a lot of die area available for more targets, but there aren't enough pads. Also refering to the last three rows of the Table. 7.3, we can conclude that our actual target area is about 30kμm^2 which accounts for $8,18\%$ of the occupied die area. While the counters (representing secondary targets) account for 138kμm^2 or $37,14\%$ and the data transmission structures for 204kμm^2 $(54,68\%)$. This indicates that (a) with a rad-hard infrastructure the proportion of target area would have become much lower and hence marginal, and (b) the use of the counters as additional target is a substantial improvement.

7.4 ASIC Functional Behavior

The ASIC pin details and the signal description are presented in Appendix A. The functional behavior of the ASIC can be explained in two states of operation:

1. Reset - ASIC is initialized
2. Programming - Data is steered in the target circuits

7.4.1 Reset

After powering the ASIC "on" we initialize it. Initialization is performed by the reset signals:

- CNT-SET is steered to active "high": It initializes some of the C-elements to "high" in the Up/down counters
- TAR-CNT-RST is steered to active "low": It resets the LFSR counters and some of the C-elements in the Up/down counters to "low". It also resets all the flip-flops used as targets to "low".
- PISO RST is steered to active "low": It reset all the PISOs to "low".

When we initialize the ASIC basically all the LFSRs, Up/Down counters and PISOs are reset. All the LFSRs must output "0", and the Up/down counters must output "1111100000". If any of these values are not observed after reset then the ASIC is not properly initialized.

7.4.1.1 Verification of Reset

To verify if the ASIC is properly initialized we could read the data out of the counters using the PISO. Data transfer in the PISO takes place with the falling edge of the clock. Data sampling takes place only if the PISO SHIFT signal is "low". The "CLK" signal in the Fig. 7.20 refers to PISO CLK84 and the "CLK" signal in the Fig. 7.21 refers to PISO CLK30. For further details about the signal refer Chapter A.

We conducted the Spectre simulations on the ASIC to verify if it is properly initialized. We initialized the ASIC with the reset signals. Without steering any activity in the targets, we read the data out of the counters using the PISO. To start the read-out we activate the SHIFT signal of the PISO and, after 10ns, we started transmitting the data from the measurement circuits by stimulating the clock signal of the PISO at a frequency of 100MHz.

All the data read out of the PISOs are listed below:

→ Data read out of the 110-bit PISO is "110'b0". From the Table 7.2 we know that the 110-bit PISO receives its input from 22 5-bit LFSRs. This shows that all the 22 5-bit LFSRs got initialized to "5'b0".

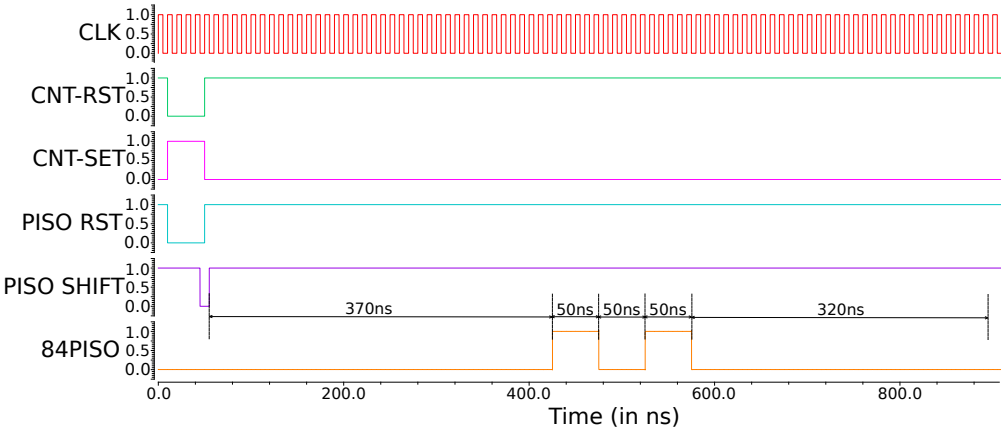


Figure 7.20: Behavior of the Counters (read out from 84-bit PISO) after Reset

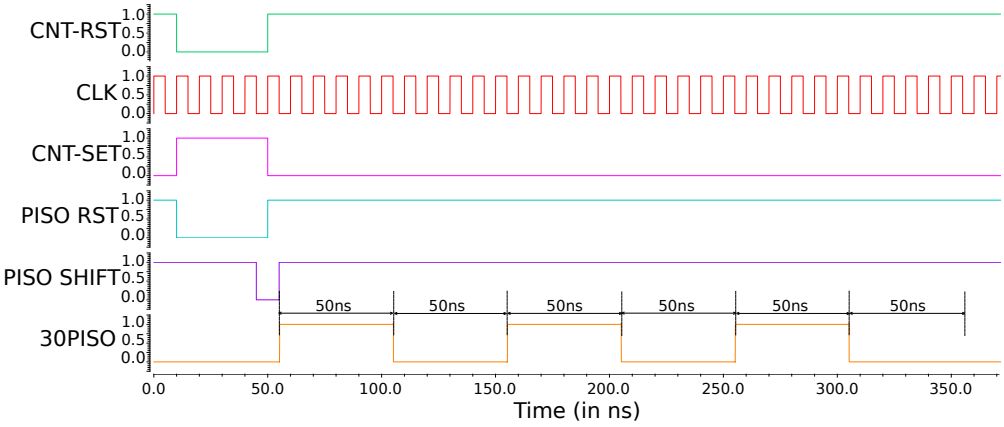


Figure 7.21: Behavior of the Counters (read out from 30-bit PISO) after Reset

- Similarly, data read out of 75-bit PISO, 55-bit PISO, and 25-bit PISO turned out to be “75’b0”, “55’b0” and “25’b0”. From the Table 7.2 we can decipher that all these PISOs receive their inputs from the 5-bit LFSRs. This shows that all the 5-bit LFSRs got initialized to “5’b0”.

→ The data transmitted by the 84-bit PISO after reset is presented in Fig. 7.20. One can observe that the first 37 bits are “0” (marked as 370ns in the figure), the next 15 bits are “111110000011111”, and the remaining 32 bits are “0”. From Table 7.1 we can interpret that the PISO receives its data from 2 32-bit LFSRs and 2 10-bit UDCs. The first 32 bits from the PISO represents the 32-bit LFSR, the next 20 bits represents the 2 10-bit UDCs and the remaining 32 bits represent the second 32-bit LFSR. Hence, based on this decomposition we can infer that the data read out from the two 32-bit LFSRs as “32’b0” and the two up/down counters as “1111100000”.

→ Similarly, the data transmitted from the 30-bit PISO after reset is presented in Fig. 7.21. We can observe that the data read out by the PISO is "5'b1, 5'b0, 5'b1, 5'b0, 5'b1, 5'b0". We can perceive from the Table 7.1 that the PISO receieves its input from 3 10-bit UDCs. Therefore we can infer from this that all the up/down counters output "10'b1111100000".

From these observations we can confirm that (i.e., the data read out from the PISOs) the ASIC is properly initialized.

7.4.2 Programming

During the programming phase we steer data signals into the different target circuits to analyse the effect of SEEs when these targets are stimulated. After the ASIC is properly initialized, we must further initialize the select signals TAR-SEL0 and TAR-SEL1 (refer Table. A.4 for further details) of the 4:1 MUX to chose the desired basic gate. Next, we stimulate the inverter chain, nand-nor-tree, flip-flop chain, the combinational gates and the flip-flops using the data (TAR-A-D) and the clock (TAR-CLK) signals. We stimulated TAR-CLK and TAR-A-D at a frequency of 100MHz to emulate the measurement period. Similarly we stimulated the Muller pipeline using the TAR-READ and TAR-WRITE signals at a frequency of 100MHz to emulate the measurement period.

After 40s we stop the stimulation of activity in the targets, to avoid the LFSR counters wrapping around to "0". Note that in 40s there are four billion transitions stimulated in the targets. After the activity is stopped in the targets, we start the read out. When the counter values are read out we should typically observe 4 billion counts in the LFSR and "1111100000" in the Up/down counters. We won't see any transitions in the 5-bit LFSR.

7.4.2.1 Verification

To verify if the ASIC is properly programmed we should read the counter data out of the ASIC after stimulating four billion transitions in the targets. After reading all the counter data we finally reset the whole ASIC and start over with a new initialization.

We conducted the Spectre simulations on the ASIC to verify its functionality. We initialize all the signals in the ASIC, furthermore, we stimulate ten transitions in the targets. The data read out of the counters using the PISOs are listed below:

→ Data read out of the 110-bit PISO is "110'b0". We can conclude from this that there is no activity in the 5-bit LFSRs. Moreover only if there is a particle strike in the Sklansky adder then only there will be activity recorded in the LFSRs.

- Similarly, data read out of 75-bit PISO, 55-bit PISO, and 25-bit PISO turned out to be "75'b0", "55'b0" and "25'b0". Therefore we can infer

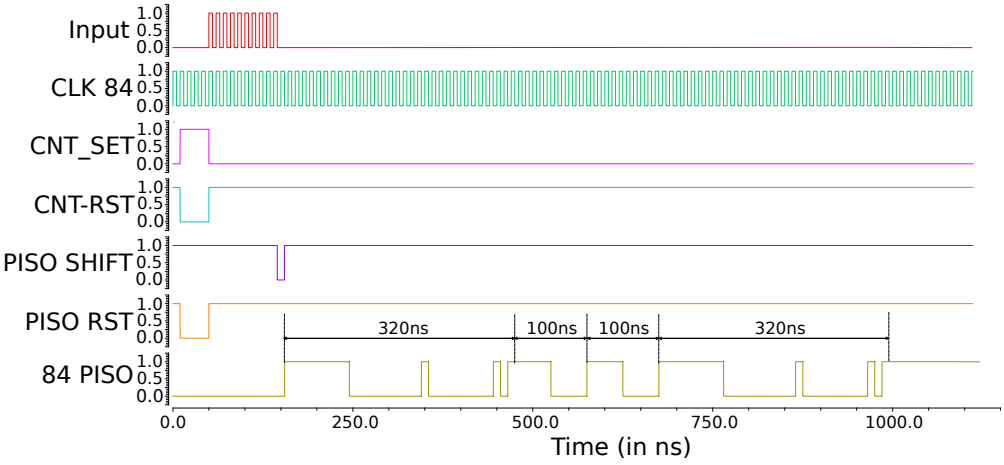


Figure 7.22: Behavior of the Counters (read out from 84-bit PISO) after Programming 10 Transitions

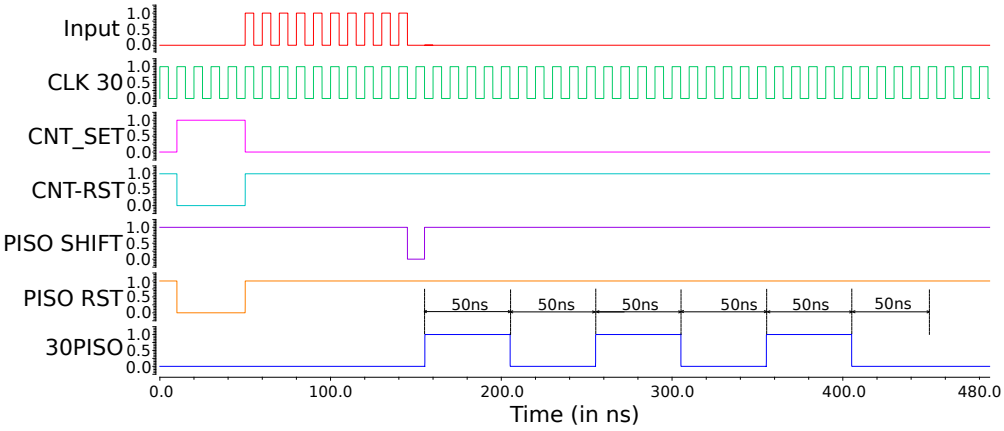


Figure 7.23: Behavior of the Counters (read out from 30-bit PISO) after Programming 10 Transitions

from this data that there has been no particle strike in the targets or the associated measurement counters (5-bit LFSRs).

→ The data transmitted from the 84-bit PISO after programming is presented in Fig. 7.22. We know that the first 32 bits read out of the PISO is from a 32-bit LFSR, and the next 20 bits are of the two UDCs and the last 32 bits are from another 32-bit LFSR. One can observe the following data recorded by the counters from the figure:

- $LFSR_1$ – "11111111100000000001000000000101"
- UDC_1 – "1111100000"
- UDC_2 – "1111100000"
- $LFSR_2$ – "11111111100000000001000000000101"

After deciphering the LFSRs' data we can conclude that ten transitions are recorded by the same. Furthermore, as there are no inconsistencies in the UDCs' data we can conclude that there were no SETs in the associated targets or UDCs.

→ Similarly, the data transmitted from the 30-bit PISO after programming is presented in Fig. 7.23. We know that the first 10 bits read out of the PISO is from one UDC, the next 10 bits read out is from a second UDC, and the last 10 bits are from the third UDC. One can observe the following data recorded by the counters from the figure:

- UDC_1 – "1111100000"
- UDC_2 – "1111100000"
- UDC_3 – "1111100000"

We can conclude from these data there has been no particle strikes in the targets or UDCs.

Overall from all these observations we can confirm that the ASIC is functioning properly.

7.5 ASIC – SET Experiments

For the verification of the SET tolerance of the infrastructure we could build on simulation results we had available for a 90nm technology already. The remaining task here was to verify that these results still hold for the chosen 65nm technology as well. Our extensive simulations have revealed that the architectural principles we chose are indeed technology independent.

We conducted Spectre simulations on the ASIC while injecting SETs on some of the target circuits within the ASIC. As a first step we initialized all the signals

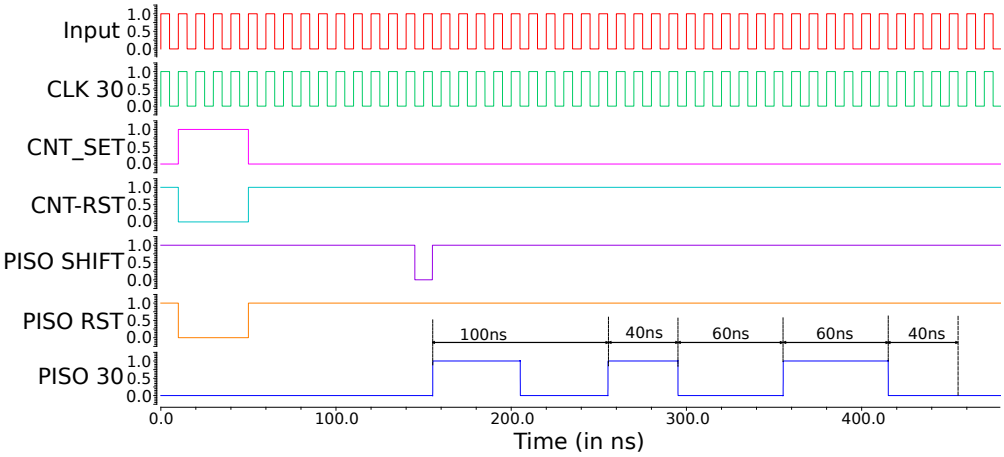


Figure 7.24: SETs in the Target Circuit read out by the 30-bit PISO

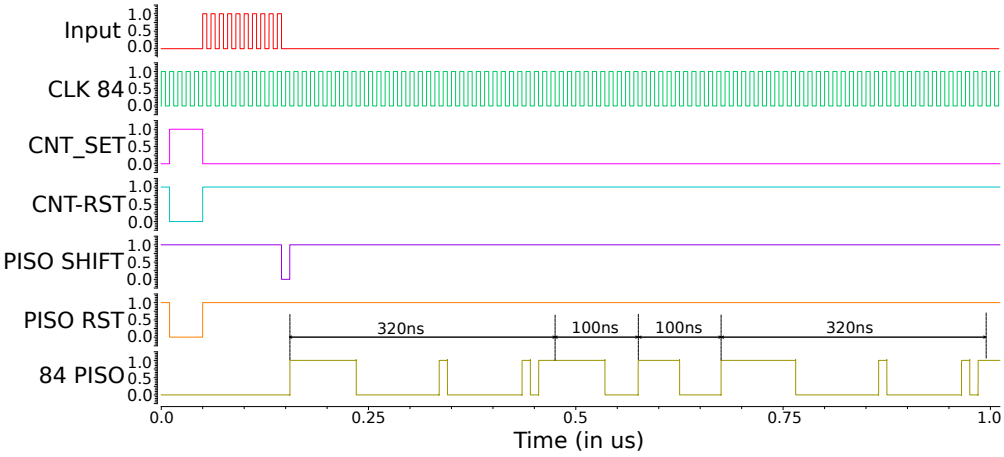


Figure 7.25: SETs in the Target Circuit read out by the 84-bit PISO

in the ASIC. Following that, we stimulated ten transitions (interval of 100ns) in the targets, during some of which we inject SETs. Note that some of the SETs are injected at the same timeline, while the others were injected at a different time. In any case all the SETs were injected subsequently after the ASIC initialization and before the completion of ten data transitions, and their charge was 450fC. The target circuits and the corresponding time of SET hits are listed below[1]:

→ SET was injected in one of the instances of the inverter chain connected to 2 32-bit LFSRs and 2 10-bit UDCs, at 72ns. The data in these counters were read out using the PISO. The outcome of the simulation is presented in Fig. 7.25.

[1] we will elucidate on the counter values later

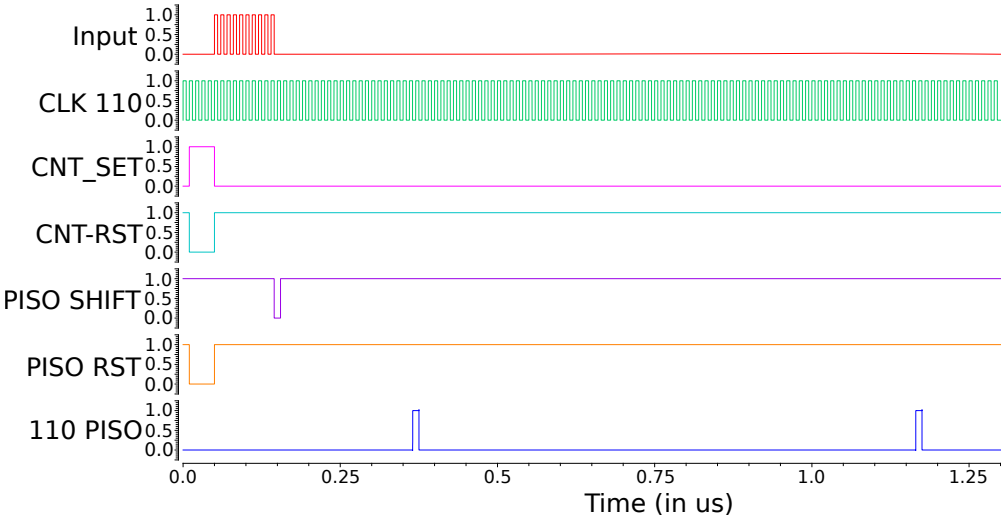


Figure 7.26: SETs in the Sklansky Adder read out by the 110-bit PISO

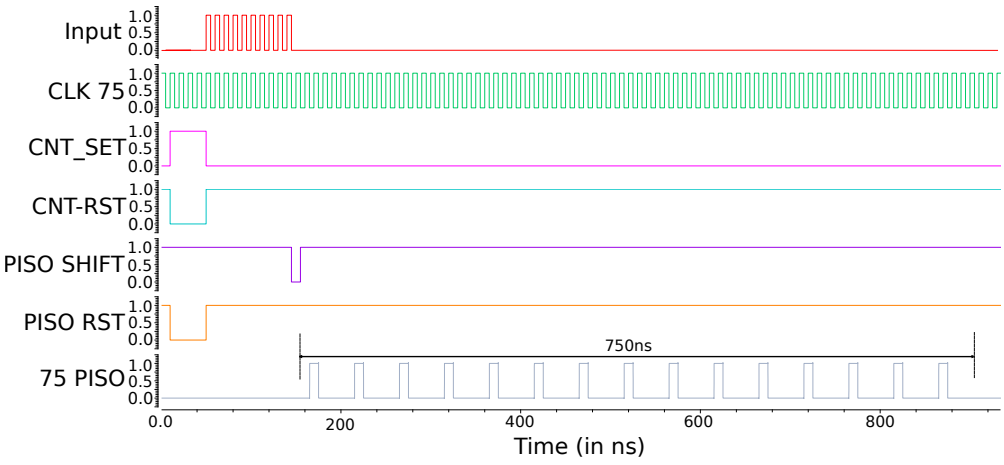


Figure 7.27: SET in the Inverter Tree read out by the 75-bit PISO

→ SET was injected in one of the instances of the inverter chain connected to 3 10-bit UDCs, at 72ns. The data in the counters were read out using 30-bit PISO. The outcome of the simulation is presented in Fig. 7.24.

→ SET was injected in one of the cells of the Sklansky Adder, at 92ns. Some of the internal nodes and all the output nodes of the adder are monitored using 22 5-bit LFSRs. The data of the counters are read out using 110-bit PISO. The outcome of the simulation is presented in Fig. 7.26.

→ SET was injected in origin inverter of the inverter tree connected to 15 5-bit LFSRs, at 82ns. The data of the counters are read out using 75-bit PISO. The outcome of the simulation is presented in Fig. 7.27.

Note, that we did not inject SETs in the measurement counters. Our aim is to verify whether:

(a) the SETs injected in the targets are successfully recorded by the counters

(b) the recorded data is successfully transmitted by the PISO

We can only observe the SET effects in the target indirectly by means of reading the data from the counters through the PISO.

7.5.1 30-bit PISO

From Fig. 7.24 we can observe the data read out by the PISO from the up/down counters. We can notice none of the counters show the same data:

- UDC_1 – "1111110000"
- UDC_2 – "1111000000"
- UDC_3 – "1111100000".

From these data we can conclude that there has been a "up" count in UDC_1 and "down" count in UDC_2. Based on this observation, we can further interpret (the most likely scenario) that the SET was triggered in the instance of the inverter chain connected to the "up" count of UDC_1 and "down" count of UDC_2.

7.5.2 84-bit PISO

We can observe the data read out by the 84-bit PISO from the LFSRs and up/down counters in the Fig. 7.25. The data percevied from the counters are as follows:

- $LFSR_1$ – "111111110000000000100000000001011"
- UDC_1 – "1111110000"
- UDC_2 – "1111100000"

- $LFSR_2$ – "11111111100000000001000000000101".

From this data we can conclude that there has been one extra transition recorded by $LFSR_1$ and one "up" count in UDC_1. This observation is consistent with the syndrome observed for "single fault scenario" in Table. 4.11. Based on the table we can interpret (the most likely scenario) this as a fault in the inverter chain instance that is connected to the "up" count of UDC_1 and $LFSR_1$.

7.5.3 110-bit PISO

: The input setting used by us for the Sklansky adder is as follows: A_{2i+1}, B_{2i+1} are initialized to "1" and A_{2i}, B_{2i} are initialized to "0"; where i ranges from 0 to 8. This setting is handwired in the layout. We routed the inputs of A_{2i+1} and B_{2i+1} to VDD. Similarly, the inputs of A_{2i} and B_{2i} are routed to VSS. Ideally all the LFSRs must show "0"; any data in the LFSR indicates that there has been a particle strike either in the target or in the counters. We can observe the data read out by the 110-bit PISO from the 5-bit LFSRs in Fig. 7.26. The data read out by the PISO is listed below for clarity:

- $LFSR_2$ – "00010"
- $LFSR_{17}$ – "00010"
- All the other LFSRs show "0"

From, the data we can conclude that the SET occured in the target node that is monitored by both the counters $LFSR_2$ and $LFSR_{17}$. Furthermore, we can interpret that the gray cell driving the output Z_{17} and the sum logic of the adder is the point where the SET is triggered. Hence, we can conclude that any SET in the adder will successfully propagate to the output.

7.5.4 75-bit PISO

We can observe the data read out by the 75-bit PISO from the 5-bit LFSRs in Fig. 7.27. The data percevied from all the 5-bit LFSRs are the same, which is "00010". From this data we can conclude that there has been an SET in the inverter tree that is recorded by all the 5-bit LFSRs. This observation is consistent with the syndrome observed for "single fault scenario" in Table. 5.6. Based on the table we can interpret that the SET occurred in the origin inverter of the tree. Note, that an SET in the origin inverter successfully propagated to all the other inverters in the tree and is recorded in all the LFSRs. Finally, we can conclude that this infrastructure will not only be able to record SETs, but will also trace the SET generation and propagation; when exposed to radiation.

We can conclude from all these observations that this ASIC will be able to provide useful data about SET generation and propagation in a radiation environment. Also note that exhaustive test is infeasible in this ASIC because we do not have any

test structures embedded in the same to verify the functionality of each and every target/measurement circuitry.

7.6 Data Transmission from ASIC to PC

The ultimate goal of our experiments is to collect statistical data for impact and effect of particles on the various target circuits. In order to attain sound statistics, we need to collect a high number of SEUs. In our experiments we use a flux of about 500 particles/second[2], which accounts to 20000 particles over the 40 second observation interval. Due to several mitigation and masking effects, however, only a fraction of those will eventually cause an upset in out target. Based on experiences from preliminary experiments we estimate that we will not see more than four upsets per target circuit in the worst case. As a consequence we need to plan for long-term experiments (many hours of continuous exposure), and we need to take special care to have a high yield of experimental data, i.e. avoid having to discard many results for whatever reason.

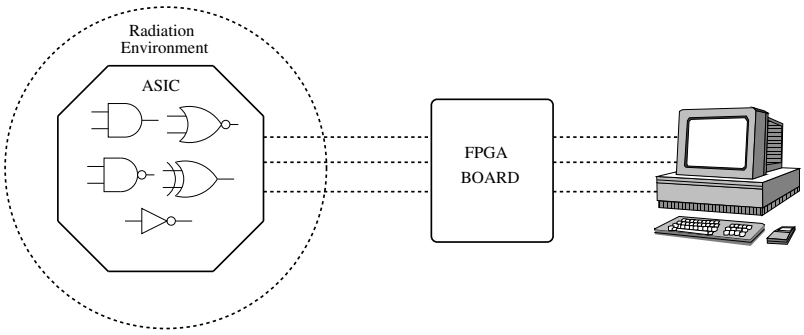


Figure 7.28: Interface Architecture

7.6.1 Gateway

Figure 7.28 shows the basic block diagram of the entire setup with our gateway component sitting right in the interface path between “FRad Chip” and host PC. The target chip will be in the radiation environment during the experiments, while the gateway will be relatively close, but not exposed to radiation. The host PC will be in a remote location, in further distance from the target. Since small read-out times are desirable, the data has to be shifted out of the ASIC very quickly. These requirements enforce the selection of the gateway. The gateway should satisfy the needs of the ASIC and one back end protocol for the not time critical PC transmission. The gateway (envisoned FPGA) then has to act as a protocol converter from

[2]Higher particle flux would be possible, in principle, but would (a) increase the risk of permanent damage and (b) make it impossible to separate the impacts into “single” events

a fast and custom interface to a slow, standard interface. Furthermore it also needs to compensate their bandwidth difference by buffering all data. The gateway basically provides the necessary data and control signals to initialize and program the ASIC. Furthermore, it also reads the data out of the measurement counters through the PISOs in the ASIC.

7.6.2 Operation of Gateway

The ASIC runs through one measurement cycle and then transmits its data to the gateway. The ASIC/gateway transmission time is also called the read-out time and has to be kept very low. Following the completion of the transfer the next measurement cycle starts in the ASIC. During the next measurement cycle the gateway transfers the data to the PC. The gateway/PC transmission can be slow but must be completed before the subsequent measurement cycle in the ASIC is completed. The PC finally waits for an incoming stream of data from the gateway and stores the same in a file.

The data stored by the PC contains the syndromes perceived from all the counters, which includes the SET data of the targets and the counters. In the next step the data has to be split up and the syndromes are evaluated. For syndrome evaluation the fault dictionary developed for all the architectures will come into use. With the help of the fault dictioanry we can classify the SET occurrences and a meaning can be given to each syndrome. This way we could build the knowledge of single event effects in the targets and measurement circuits.

The actual construction of the prototype is described in [46].

7.6.3 Requirements

Before coming up with an architectural concept for our gateway[3] we first need to state the requirements:

- In the reactor experiments we can neither switch off the radiation at the end of the observation period, nor predict the time and location of the particle strike. Therefore, there is a possibility for the counter values to change during readout. Since, the fault tolerance of our measurement and communication infrastructure on the “FRad” chip is not perfect, it may experience SEUs during data transfer to the gateway. Hence, the readout process must provide a high level of fault tolerance.

- For the same reason the readout process must be much shorter than the observation period. Only then we can regard the risk of experiencing an SEU during readout as a relatively insignificant “error effect” in our statistics, rather than a systematic distortion.

[3] for clarity we will call the gateway as the FPGA from here on

- The overall (net) number of bits to be transferred per observation period is 2687, available in chunks of 84 bits, 30 bits, etc. Redundant information for framing, data protection etc. is not considered and will add to this amount.
- As experiment time is relatively expensive and limited, we do not want to be forced to discard data because of errors in the transmission from the "FRad" chip to the host PC. Therefore the whole data path, including the FPGA itself as well as the datapath between FPGA and host PC, although not exposed to radiation, needs to be protected against (accidental) faults.
- The cabling of the target chip in the radiation source is difficult and expensive, as it has to cross the shielding provisions. Therefore the number of signal lines must be kept small.

7.6.4 Concept

Our proposed solution for the FRad/FPGA interface is a clocked serial data transfer just like in the scan chain used for testing: The individual counter values are serially transferred to the FPGA and stored. In this transfer the full control (activation of serial mode, clocking) lies with the FPGA. To speed up the transfer we must perform all the transfer (data from all the PISOs) in parallel.

Our strategy for attaining fault tolerance is repeatedly reading and transmitting the counter values. In this way, if a counter value should flip just while being read, or if a transient fault should occur during transmission, we can still attain a correct value by means of voting. Due to the expected low rate of SEUs in the targets and low probability of transients in the communication, protection against single faults is sufficient. For the FPGA/host interface we continue this strategy in a consequent manner: The three copies of the counter values are individually stored in the FPGA, and they are individually transferred to the host, where the voting is finally performed. This effectively protects the storage within the gateway as well.

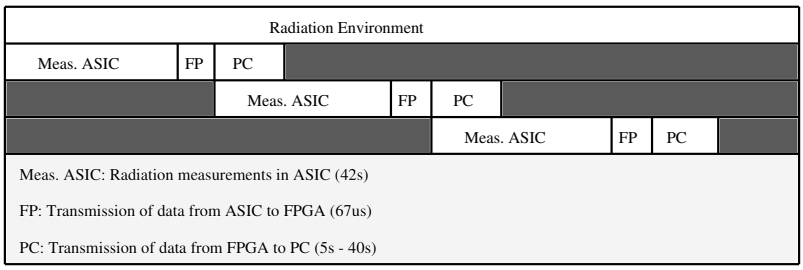


Figure 7.29: Timeline of our Architecture Setup

We have foreseen this storage capability to provide buffering between the two interfaces with their different requirements: The FRad/FPGA interface must be simple and fast, while the FPGA/host interface is more complex but has uncritical performance. Notice in figure 7.29 that we perform the replication on block

level rather than on bit level, i.e. we transfer the complete data block once, and then re-transmit it two more times. The benefit of doing so is that the counter values are copied into the PISO each time again, and due to the relatively large delay between these individual transmissions, any transient fault that might have affected one block transmission, will have decayed already when the second one starts.

As a consequence of this triplication of data, we need to transfer and store 8061 bits. When clocking the PISO with 100MHz the longest[4] transfer time amounts to (the maximum time taken by the largest PISO to transfer the data) 4μs, which is indeed much shorter than the observation period. The selection of an appropriate chip (FPGA) for implementing the gateway component is presented in [46].

[4]Since we have data words of 110, 84, 75, 55, 30 and 25 bit

CHAPTER 8

Conclusions and Future Work

This chapter basically summarizes the work that is incorporated in this thesis. In here we will present our key contributions in the same systematic order as they were presented in this thesis. Finally, we will take a look at the future research directions that could not be addressed in the scope of this thesis.

8.1 Summary of Key Contributions

The aim of our thesis was to design a radiation target ASIC to perform a comprehensive investigation of SETs in digital circuits. We will now summarize the work we did to achieve the same in this research study.

8.1.1 SET Modeling

The need to analyze SETs in digital circuits in turn created the requirement to find an efficient way of injecting the SETs in digital circuits – to understand the digital circuits' behavior to radiation effects. Especially in our case, we had to analyze how the SET data of the target circuits is interpreted by the measurement circuits. After a thorough literature review, we chose the double exponential current model to analyze SETs, as it is the only model that accurately mimics the particle strike in both qualitative and quantitative manner.

Relevant Publications

1. R. Najvirt, V. S. Veeravalli, and A. Steininger, "Particle Strikes in C-Gates: Relevance of SET Shapes", in Proceedings of 2nd Workshop on Manufacturable and Dependable Multicore Architectures at Nanoscale, Avignon; 2013; 4 pages

2. L. Anghel, V. S. Veeravalli, D. Alexandrescu, A. Steininger, K. Schneider, E. Costenaro, "Single Event Effects in Muller C-Elements and Asynchronous

Circuits Over a Wide Energy Spectrum", in Proceedings of IEEE Workshop on Silicon Errors in Logic - System Effects (SELSE 10), Stanford University, USA, 2014; 6 pages

3. A. Steininger, V. S. Veeravalli, D. Alexandrescu, E. Costenaro, L. Anghel; "Exploring the State Dependent SET Sensitivity of Asynchronous Logic - The Muller-Pipeline Example", in Proceedings of 32nd IEEE International Conference on Computer Design (ICCD), Seoul, Korea; 2014, pp. 61-67.

4. V. S. Veeravalli and A. Steininger, "Can we trust SET Injection Models?", in MEDIAN Finale Workshop on Manufacturable and Dependable Multicore Architectures at Nanoscale, Tallinn, Estonia, 2015, 6 pages.

5. V. S. Veeravalli and A. Steininger, "Study of a delayed single-event effect in the Muller C-element", 2016 21th IEEE European Test Symposium (ETS), Amsterdam, 2016, pp. 1-2.

8.1.2 Design of Novel Radiation Hardening Mechanisms

The idea of accurately monitoring SETs in the targets fueled the study of radiation hardening mechanisms. Our perspective was to build measurement counters and PISOs that are resilient to SETs. This encouraged us to evaluate the radiation hardening mechanisms in the literature. Some of the mechanisms were not compatible and some of them had to be improved to be able to perform as intended.

Ultimately, we constructed a radiation hardened Muller C-element to build resilient up/down counters. We also built radiation hardened PISOs and LFSRs. Finally, to be able to use the PISO for multiple measurement architectures we decided to construct resilient MUXes, and for this we tested the resilience of two state-of-the-art mechanisms under extreme temperatures and voltages, while injecting SETs.

Based on these evaluations and analysis we conclude that:

- To construct resilient combinational circuits the stack separation mechanism is preferred.

- For radiation hardened Muller C-element – the DICE mechanism is the best solution for $Q_{crit} \leq 500fC$ and stack separation mechanism is the best for $Q_{crit} > 500fC$

- The DICE mechanism turned out to be the best choice in constructing radiation hardened flip-flops.

Relevant Publications

1. V. S. Veeravalli and A. Steininger, "Efficient Radiation-Hardening of a Muller C-Element" 2012 Single Event Effects Symposium (SEE 2012), San Diego, USA.

2. V. S. Veeravalli and A. Steininger, "Radiation-tolerant combinational gates - an implementation based comparison," IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Tallinn, 2012, pp. 115-120.

3. V. S. Veeravalli and A. Steininger, "Performance of radiation hardening techniques under voltage and temperature variations," IEEE Aerospace Conference, Big Sky, MT, 2013, pp. 1-12.

8.1.3 Innovative Measurement Infrastructure SET Sensitivity

We have proposed a choice of target circuits and an on-chip measurement architecture along with the results of the pre-fabrication analysis. Key challenges have been: (i) distinguishing SETs from normal switching activity of the target circuits, (ii) providing reliable SET data acquisition in spite of radiation hits in the measurement infrastructure, and (iii) leaving as much of the die area available for the target circuits as possible. Rather than employing radiation hardened counters, our architecture considers the measurement circuitry as additional target circuits, and hence allows to tolerate hits in the former by an architectural design that supports reliable fault detection based on a fault dictionary. Fault-injection experiments based on detailed *Spice models* and some probabilistic analysis have been used for a comprehensive design validation, which is *the* major step along the road towards the final FRad Chip.

We also investigated how the susceptibility of a circuit (particularly an asynchronous one) to SETs is influenced by its activity. To this end we injected SETs in the pipeline during different degrees of activity. We faced a similar problem here – distinguishing transitions caused by the regular activity from those caused by particle hits. Our solution is to employ a difference counter that receives one input from the target and the other from an identical circuit serving as a fault free reference. We have provided an efficient implementation of this infrastructure, based on Muller C-elements and have shown how it can be effectively protected against SETs.

Relevant Publications

1. V. S. Veeravalli, A. Steininger, "Monitoring Single Event Transient Effects in Dynamic Mode", in "1st Workshop on Manufacturable and Dependable Multicore Architectures at Nanoscale (MEDIAN 2012)", 51 - 54.

2. V. S. Veeravalli, T. Polzer, A. Steininger and U. Schmid, "Architecture and Design Analysis of a Digital Single-Event Transient/Upset Measurement Chip", 15th Euromicro Conference on Digital System Design, Izmir, 2012, pp. 8-17. (**Best Paper Award**)

3. V. S. Veeravalli, T. Polzer, U. Schmid, A. Steininger, M. Hofbauer, K. Schweiger, H. Dietrich, K. S. Hornstein, H. Zimmermann, K. O. Voss, B. Merk, and M.

Hajek, “An infrastructure for accurate characterization of single-event transients in digital circuits”, Journal of Microprocessors and Microsystems, 37, 8 (November 2013), 772-791.

8.1.4 Novel Measurement Infrastructure for SET Propagation

We have presented our architecture for a target design that allows studying the propagation and electrical masking of SETs in combinational logic. For the actual target we propose: (i) a four-stage inverter tree, which is simple and generic, but still provides all the features required for our study, and (ii) a Sklansky adder, not only because arithmetic blocks are very common, but also because it exhibits both a chain structure to study propagation as well as different fanouts. The measurement infrastructure of the targets are listed below:

- Sklansky Adder - We have proposed the provision of LFSR based counters at selected locations.
- Static Inverter Tree - We have employed LFSR counters at the output of all the inverters in the tree.
- Inverter Tree with activity in the input – We chiefly used asynchronous up/down counters (as they represent a very efficient and elegant solution to our needs) and in some selected locations we augmented the tree with LFSR based counters.

We have elaborated a measurement architecture that can safely tolerate double faults by its inherent redundancy, thus saving the need for costly radiation hardening. We have systematically developed a fault dictionary, giving evidence that this infrastructure will allow us to handle and identify all expected fault scenarios, including those where a counter is affected. Our preliminary SET injection experiments based on simulations using *Spice modeling* have confirmed that single SETs will create errors at multiple locations.

From these experiments, we were able to identify the most sensitive input pattern with respect to fault propagation for the Sklansky adder. Note that these infrastructures would not only allow us to study the targets in static mode, but also in dynamic mode (for inverter tree), since we expect interesting insights from that.

Relevant Publications

1. V. S. Veeravalli and A. Steininger, “Architecture for monitoring SET propagation in 16-bit Sklansky adder”, IEEE Fifteenth International Symposium on Quality Electronic Design, Santa Clara, CA, 2014, pp. 412-419.
2. V. S. Veeravalli and A. Steininger, “Diagnosis of SET Propagation in Combinational Logic under Dynamic Operation”, in IEEE Workshop on Silicon Errors in Logic - System Effects (SELSE 10), Stanford University, USA, 2014, 6 pages.

8.1.5 Novel Measurement Infrastructure for SET Pulsewidths

We presented design and analysis of a fully digital infrastructure for measuring SET durations, which is versatile enough to be adapted to many different experimental settings. The major design challenge has been the exposure of both the target and the measurement infrastructure to the same radiation environment. Besides minimizing its area, the measurement infrastructure must be made as SEU-tolerant as possible in order to maximize the number of safe measurement periods (where the target is hit and the associated recording can be read out correctly, i.e., before an excessive number of hits also occured in the measurement infrastructure). We outlined the measures by which we succeeded to establish this balance. In addition, we had to address further requirements like good temporal resolution. The intended operation of our measurement infrastructure has been verified by means of SET injection experiments, which also led to a comprehensive fault dictionary. Some probabilistic analysis showed that, for a given particle flux, a suitable duration of the measurement period can be found by which at the same time (a) a sufficiently high probability of at least one target hit can be achieved while (b) the measurement period is still safe. We can hence claim that our measurement infrastructure indeed fulfills its purpose.

Relevant Publications

1. V. S. Veeravalli and A. Steininger, “Long term on-chip monitoring of SET pulsewidths in a fully digital ASIC”, in 22nd Austrian Workshop on Microelectronics (Austrochip), Graz, 2014, pp. 1-6.

2. V. S. Veeravalli, A. Steininger and U. Schmid, “Measuring SET pulsewidths in logic gates using digital infrastructure”, in Fifteenth International Symposium on Quality Electronic Design, Santa Clara, CA, 2014, pp. 236-242.

3. V. S. Veeravalli and A. Steininger, “Reliable and Continuous Measurement of SET Pulse Widths”, in 2015 Euromicro Conference on Digital System Design, Funchal, 2015, pp. 181-188.

4. V. S. Veeravalli, A. Steininger and U. Schmid, “A Versatile Architecture for Long-Term Monitoring of Single-Event Transient Durations”, Journal of Microprocessors and Microsystems, 2017, ISSN 0141-9331.

8.1.6 Design of FRad Chip

We have motivated the need for better understanding the generation and propagation of SETs in new VLSI technologies. To contribute to this aim, we have desiged a VLSI chip for physical radiation experiments that will carry both, basic circuit blocks serving as the actual targets, and measurement infrastructure.

We have presented design rationale and implementation details of the *FRad Chip* for radiation experiments. Our post-layout analysis of the area distribution

among those blocks confirms that it was necessary and also useful to employ the redundant architecture for protecting the on-chip measurement infrastructure, instead of the traditional methods like sizing or TMR. To support experiments with well controlled radiation sources (micro beam) we have taken care in the layout to concentrate the target blocks in the center, with counters and PISOs forming concentric rings around them.

Relevant Publications

1. V. S. Veeravalli and A. Steininger, "Design and Physical Implementation of a Target ASIC for SET Experiments", 2016 Euromicro Conference on Digital System Design (DSD), Limassol, 2016, pp. 694-697.

8.2 Outlook

The main goal of this thesis has been to understand the radiation effects in digital circuits, especially single event transients. The list of questions that would linger anyone that has read the thesis are:

- Have the radiation effects been completely studied in this thesis?
  - We have studied some of the radiation effects such as SET sensitivity, SET generation, SET propagation, SET spatial distribution and SEUs in this thesis.
  - The effects such as SEBs, SEFIs, Latchups, etc., are out of scope of this thesis and hence are not covered in here.
- Is this all there is to know about radiation effects?
  - Radiation effects is a very wide topic and since the 60s researchers have been trying to understand their behavior in electronics components built for space, reactors, etc. But, with technology advent the radiation effects study has become neccessary even for commercial circuits.
  - In this thesis we cover only the basic radiation effects, which is a very small portion.
- Are the chosen target circuits enough to understand the behavior of any digital circuit in existence when exposed to radiaiton?
  - In this thesis we were able to cover only a handful of targets. Based on the data percevied from these targets we could reasonably understand the effects of SETs and SEUs in digital circuits. Furthermore, the collected SET data could estimate the impact of SETs in some digital circuits, but not all of them.

  - For example we haven't covered targets such as mutipliers, DLL, memory, etc. Understanding the behavior of SETs in these specific circuits, from the SET data collected by the *FRad Chip*, is out of scope of this thesis.

- Is the theoretical and simulation based analysis enough to understand raditaion effects in any environment?
  - No, it is not enough. Note, that to understand the effects of a certain radiation environment we must expose our *FRad Chip* to the same.
  - Of course if we have the parameters available for the radiation environment, we can conduct some SET simulation studies for cross checking the data from the radiation experiments.

- Can we build radiation tolerant components based on the data provided by the circuits presented in this thesis?
  - Yes, we can construct radiation tolerant components based on the data provided in this thesis. Note, that the data provided in this thesis is only for $90nm$ technology. If we want to build radiation hardened components in a different technology (especially newer technologies such as $45nm$, $28nm$, $12nm$, etc.), then we must test the same for proper functional operation.

Even though we did our best to cover as much as possible in the field of *single event effects*, a bunch of topics could not be investigated within the horizon of this thesis and are hence reserved for future work. The following topics will be covered in the future work.

8.2.1 Fabrication of the ASIC

We are in the process of running post layout simulations to verify the functionality of the *FRad Chip* (in $65nm$ UMC bulk CMOS technology). Once the verfication is complete, we will send it for fabrication through the mini@sic program conducted by EUROPRACTICE IC service. We estimate to have our ASIC fabricated in the *Multi Project Wafer* (MPW) run scheduled for October 2017.

8.2.2 Gateway FPGA Setup

The data transfer from an experimental chip (that is subjected to radiation) to a host PC requires considerable care, in order to be sufficiently reliable. The idea is to use the controller FPGA as the gateway[1]. Our future plan is of course to test the fabricated *FRad Chip* for its functionality with this gateway and later use the same in the radiation experiments. At that point our concepts and implementation will have to prove their value in real life measurements.

[1]We have already reported this in Chapter. 7 and sketched its architecture

8.2.3 Radiation Experiments on Microbeam and Reactor

Our future work will encompass performing the intended radiation experiments on our chip. Based on their results we will be able to quantify the actual masking effects and elaborate a much more detailed model of the SET generation and propagation process (considering many different particle energies, angles of incidence etc. along with their respective relative probabilities). This in turn will allow us to devise a set of efficient SET mitigation schemes for the target blocks from which a designer can choose the one appropriate for a given purpose.

Once we receive the fabricated ASIC we plan to expose the whole setup to radiation in the Atomic reactor hosted by TU Wien. We have also written a beam-time proposal to conduct radiation experiments in 2018 at GSI Darmstadt with the help of MAT collaboration.

8.2.4 Technology Variations

We did not consider multiple drive strengths in this ASIC. We built the targets and other circuits for a single drive strength. As a part of future work we must consider utilizing multiple drive strengths to reasonably understand the single event effects with drive strenght varitions. Furthermore, we must test the circuits in different technologies such as $45nm$, $28nm$, etc., to understand the radiation effects better. This will also help us build better mitigation mechanisms.

All these technology variation analysis raises another question: “Is technology scaling necessary for components exposed to radiation?”. Research has to be done in this end, to check if we must really use newer technologies, to devise components that are built to mitigate radiation effects.

8.2.5 Other Single Event Effects

We must take a deeper look into these effects in the future:

- Single Event Latchups - These are the latch-ups caused by a single event upset. They might not occur just in the power rails, they can also happen at any place where the required parasitic structure exists. One must create this effect in CMOS and check if it is possible to avoid using non-tradiational latch-up tolerant circuitry.

- Single Event Burnouts - This type of effect usually occurs in space in power MOSFETs. But, now these effects can be seen in CMOS PWM controllers and CMOS driver circuits. We must investigate the effect in CMOS and find an effective unconventional solution to mitigate them.

- Single Event Functional Interrupts - It is important to model this effect to understand it better and if possible create a solution that does not require power reset. This type of effect could paralyse a system and hence has to be dealt with.

8.2.6 Spice Modeling

We have identified some discrepanices in the state-of-the-art double exponential current model and have also discussed them. It is enough to use this model to understand transient effects in digital circuits.

Our aim really is to check if it is possible to construct a Spice model that can deliver the SET data (shape, pulse width and peaks) proided by the 3D TCAD model. Is it possible to recreate "the SET effect a 3D model creates in the layout" with "a Spice model in the extracted netlist"? This is also the ultimate goal of the FWF sponsored project EASET at TU Wien.

To achieve this we at first decided to explore the discrepancies in the state-of-the-art current models which led us to discover a new type of single event upset in the Muller C-element.

We are still actively in the process of devising a spice model that can actually mimic a particle strike without any discrepancies.

Bibliography

[1] H. Abrishami, S. Hatami, and M. Pedram. Characterization and design of sequential circuit elements to combat soft error. In *IEEE International Conference on Computer Design (ICCD) 2008.*, pages 194 –199, oct. 2008.

[2] G. R. Agrawal, L. W. Massengill, and K. Gulati. A Proposed SEU Tolerant Dynamic Random Access Memory (DRAM) Cell. *IEEE Transactions on Nuclear Science*, 41(6):2035–2042, Dec. 1994.

[3] J. R. Ahlbin, T. D. Loveless, D. R. Ball, B. L. Bhuva, A. F. Witulski, L. W. Massengill, and M. J. Gadlage. Double-pulse-single-event transients in combinational logic. In *IEEE International Reliability Physics Symposium (IRPS)*, pages 3C.5.1 – 3C.5.6, April 2011.

[4] J. R. Ahlbin, L. W. Massengill, B. L. Bhuva, B. Narasimham, M. J. Gadlage, and P. H. Eaton. Single-event transient pulse quenching in advanced cmos logic circuits. *IEEE Transactions on Nuclear Science*, 56(6):3050 –3056, Dec. 2009.

[5] A. Ahmad, N. K. Nanda, and K. Garg. Critical role of primitive polynomials in an lfsr based testing technique. *Electronics Letters*, 24(15):953 –955, Jul 1988.

[6] A. Ajane, P. M. Furth, E. E. Johnson, and R. L. Subramanyam. Comparison of binary and lfsr counters and efficient lfsr decoding algorithm. In *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1 –4, Aug. 2011.

[7] A. Ammari, K. Hadjiat, and R. Leveugle. Combined fault classification and error propagation analysis to refine rt-level dependability evaluation. *Electronic Testing*, 21(4):365–376, 2005.

[8] D. A. Anderson. *Design of Self-checking Digital Networks Using Coding Techniques*. PhD thesis, Champaign, IL, USA, 1971. AAI7212065.

[9] L. Anghel, D. Alexandrescu, and M. Nicolaidis. Evaluation of a Soft Error Tolerance Technique Based on Time and/or Space Redundancy. In *Proc. 13th Symposium on Integrated Circuits and Systems Design*, pages 237–242, 2000.

[10] L. Anghel and M. Nicolaidis. Defects Tolerant Logic Gates for Unreliable Future Nanotechnologies. In *Proc. 9th International Work Conference on Artificial Neural Networks*, pages 422–429, 2007.

[11] S. Askari, B. Dwivedi, A. Saeed, and M. Nourani. Scalable Mean Voting Mechanism for Fault Tolerant Analog Circuits. In *Proc. 4th International Design and Test Workshop*, pages 1–6, Nov. 2009.

[12] N. M. Atkinson, J. R. Ahlbin, A. F. Witulski, N. J. Gaspard, W. T. Holman, B. L. Bhuva, E. X. Zhang, C. Li, and L. W. Massengill. Effect of transistor density and charge sharing on single-event transients in 90-nm bulk CMOS. *IEEE Transactions on Nuclear Science*, 58(6):2578 –2584, Dec. 2011.

[13] M. A. Bajura, Y. Boulghassoul, R. Naseer, S. Dasgupta, A. F. Witulski, J. Sondeen, S. D. Stansberry, J. Draper, L. W. Massengill, and J. N. Damoulakis. Models and algorithmic limits for an ecc-based approach to hardening sub-100-nm srams. *IEEE Trans. Nuclear Science*, 54(4):935–945, 2007.

[14] A. Balasubramanian, B. Narasimham, B. L. Bhuva, L. W. Massengill, P. H. Eaton, M. Sibley, and D. Mavis. Implications of total dose on single-event transient (set) pulse width measurement techniques. *IEEE Transactions on Nuclear Science*, 55(6):3336 –3341, Dec. 2008.

[15] R. Baumann. Soft errors in advanced computer systems. *Design & Test of Computers, IEEE*, 22(3):258–266, May-June 2005.

[16] R. C. Baumann. Radiation-induced soft errors in advanced semiconductor technologies. *IEEE Transactions on Device and Materials Reliability*, 5(3):305–316, Sept. 2005.

[17] M. P. Baze, J. Wert, J. W. Clement, M. G. Hubert, A. Witulski, O. A. Amusan, L. Massengill, and D. McMorrow. Propagating SET characterization technique for digital CMOS libraries. *IEEE Transactions on Nuclear Science*, 53(6):3472–3478, Dec. 2006.

[18] M.P. Baze and S.P. Buchner. Attenuation of single event induced pulses in CMOS combinational logic. *IEEE Transactions on Nuclear Science*, 44(6):2217–2223, Dec 1997.

[19] O. J. Bedrij. Carry-select adder. *IRE Transactions on Electronic Computers*, EC-11(3):340 –346, june 1962.

[20] J.M. Benedetto, P.H. Eaton, D.G. Mavis, M. Gadlage, and T. Turflinger. Variation of digital SET pulse widths and the implications for single event hardening of advanced CMOS processes. *IEEE Transactions on Nuclear Science*, 52(6):2114–2119, Dec. 2005.

[21] H. K O Berge, A. Hasanbegovic, and S. Aunet. Muller c-elements based on minority-3 functions for ultra low voltage supplies. In *Design and Diagnostics of Electronic Circuits Systems (DDECS), 2011 IEEE 14th International Symposium on*, pages 195–200, April 2011.

[22] B. B. Bhattacharya, B. Gupta, S. Sarkar, and A. K. Choudhury. Testable design of rmc networks with universal tests for detecting stuck-at and bridging faults. *IEE Proceedings E - Computers and Digital Techniques*, 132(3):155–162, May 1985.

[23] Keith A. Bowman, James W. Tschanz, Nam Sung Kim, Janice C. Lee, Chris B. Wilkerson, Shih-Lien L. Lu, Tanay Karnik, and Vivek K. De. Energy-efficient and metastability -immune resilient circuits for dynamic variation tolerance. *IEEE Journal of Solid-State Circuits*, 44(1):49 – 63, jan. 2009.

[24] R.P. Brent and H.T. Kung. A regular layout for parallel adders. *IEEE Transactions on Computers*, C-31(3):260 –264, March 1982.

[25] S. Buchner, M. Baze, D. Brown, D. McMorrow, and J. Melinger. Comparison of error rates in combinational and sequential logic. *IEEE Transactions on Nuclear Science*, 44(6):2209–2216, Dec 1997.

[26] Martin G. Buehler and Richard A. Allen. An analytical method for predicting CMOS SRAM upsets with application to asymmetrical memory cells. *IEEE Transactions on Nuclear Science*, 33(6):1637–1641, Dec. 1986.

[27] N. Burgess. Accelerated carry-skip adders with low hardware cost. In *The Thirty-Fifth Asilomar Conference on Signals, Systems and Computers*, volume 1, pages 852 –856 vol.1, nov. 2001.

[28] James S. Cable, Eugene F. Lyons, Michael A. Stuber, and Mark L. Burgener. Radiation-hardened silicon-on-insulator cmos device, and method of making the same, 03 2003.

[29] T. Calin, M. Nicolaidis, and R. Velazco. Upset Hardened Memory Design for Submicron CMOS Technology. *IEEE Transactions on Nuclear Science*, 43(6):2874–2878, Dec. 1996.

[30] V. S. Chirde and U. Jadhav. Design of a multiplier with adaptive hold logic (ahl) circuit to reduce aging effects. In *Computer, Communication and Control (IC4), 2015 International Conference on*, pages 1–5, Sept 2015.

[31] G. S. Choi and R. K. Iyer. Wear-out simulation environment for vlsi designs. In *Fault-Tolerant Computing, 1993. FTCS-23. Digest of Papers., The Twenty-Third International Symposium on*, pages 320–329, June 1993.

[32] K.A. Clark, A.A. Ross, H.H. Loomis, T.R. Weatherford, D.J. Fouts, S.P. Buchner, and D. McMorrow. Modeling single-event effects in a complex digital device. *IEEE Transactions on Nuclear Science*, 50(6):2069–2080, Dec. 2003.

[33] T. Colladant, O. Flament, A. L'Hoir, V. Ferlet-Cavrois, C. D'Hose, and J. du Port de Potcharra. Study of transient current induced by heavy-ion in nmos/soi transistors. *IEEE Transactions on Nuclear Science*, 49(6):2957 – 2964, dec 2002.

[34] A. Dixit and A. Wood. The impact of new technology on soft error rates. In *Proc. IEEE International Reliability Physics Symposium (IRPS'11)*, pages 5B.4.1 –5B.4.7, april 2011.

[35] P.E. Dodd and L.W. Massengill. Basic mechanisms and modeling of single-event upset in digital microelectronics. *IEEE Transactions on Nuclear Science*, 50(3):583 – 602, june 2003.

[36] P.E. Dodd and F.W. Sexton. Critical charge concepts for CMOS SRAMs. *IEEE Transactions on Nuclear Science*, 42(6):1764–1771, Dec 1995.

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

[38] Shlomi Dolev. Possible and impossible self-stabilizing digital clock synchronization in general graphs. Technical Report 96–06, Department of Mathematics and Computer Science Ben-Gurion University, Beer-Sheva, Israel, August 1996.

[39] Shlomi Dolev and Yinnon Haviv. Self-stabilizing microprocessors, analyzing and overcoming soft-errors. *IEEE Transactions on Computers*, 55(4):385–399, April 2006.

[40] Clive Dyer and David Rodgers. Effects on spacecraft & aircraft electronics. In *Proceedings ESA Workshop on Space Weather*, ESA WPP-155, pages 17–27, Nordwijk, The Netherlands, nov 1998. ESA.

[41] P. Eaton, J. Benedetto, D. Mavis, K. Avery, M. Sibley, M. Gadlage, and T. Turflinger. Single event transient pulsewidth measurements using a variable temporal latch technique. *IEEE Transactions on Nuclear Science*, 51(6):3365–3368, Dec. 2004.

[42] B. Elspas. The theory of autonomous linear sequential networks. *Circuit Theory, IRE Transactions on*, 6(1):45 – 60, mar 1959.

[43] V. Ferlet-Cavrois, P. Paillet, M. Gaillardin, D. Lambert, J. Baggio, J. R. Schwank, G. Vizkelethy, M. R. Shaneyfelt, K. Hirose, E. W. Blackmore,

O. Faynot, C. Jahan, and L. Tosti. Statistical analysis of the charge collected in SOI and bulk devices under heavy Ion and proton irradiation—implications for digital SETs. *IEEE Transactions on Nuclear Science*, 53(6):3242–3252, Dec. 2006.

[44] V. Ferlet-Cavrois, P. Paillet, D. McMorrow, N. Fel, J. Baggio, S. Girard, O. Duhamel, J.S. Melinger, M. Gaillardin, J.R. Schwank, P.E. Dodd, M.R. Shaneyfelt, and J.A. Felix. New insights into single event transient propagation in chains of inverters—evidence for propagation-induced pulse broadening. *IEEE Transactions on Nuclear Science*, 54(6):2338–2346, Dec. 2007.

[45] V. Ferlet-Cavrois, P. Paillet, D. McMorrow, A. Torres, M. Gaillardin, J.S. Melinger, A.R. Knudson, A.B. Campbell, J.R. Schwank, G. Vizkelethy, M.R. Shaneyfelt, K. Hirose, O. Faynot, C. Jahan, and L. Tosti. Direct measurement of transient pulses induced by laser and heavy ion irradiation in deca-nanometer devices. *IEEE Transactions on Nuclear Science*, 52(6):2104–2113, Dec. 2005.

[46] Bernhard Fritz. Verification of the frad radiation target chip and its experiment setup. Master's thesis, Technische Universität Wien, Institut für Technische Informatik, Treitlstr. 3/3/182-2, 1040 Vienna, Austria, 2017.

[47] Sai-Wai Fu, A.M. Mohsen, and 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*, 32(1):49–54, Jan 1985.

[48] G. Fuchs and A. Steininger. VLSI Implementation of a Distributed Algorithm for Fault-Tolerant Clock Generation. *Journal of Electrical and Computer Engineering*, 2011.

[49] Matthias Fuegger, Ulrich Schmid, Gottfried Fuchs, and Gerald Kempf. Fault-Tolerant Distributed Clock Generation in VLSI Systems-on-Chip. In *Proceedings of the Sixth European Dependable Computing Conference (EDCC-6)*, pages 87–96. IEEE Computer Society Press, October 2006.

[50] M. J. Gadlage, P. H. Eaton, J. M. Benedetto, M. Carts, V. Zhu, and T. L. Turflinger. Digital device error rate trends in advanced CMOS technologies. *IEEE Transactions on Nuclear Science*, 53(6):3466–3471, Dec. 2006.

[51] M.J. Gadlage, J.R. Ahlbin, B. Narasimham, B.L. Bhuva, L.W. Massengill, and R.D. Schrimpf. Single-event transient measurements in nMOS and pMOS transistors in a 65-nm bulk CMOS technology at elevated temperatures. *IEEE Transactions on Device and Materials Reliability*, 11(1):179–186, march 2011.

[52] R. Garg and S.P. Khatri. A Novel, Highly SEU Tolerant Digital Circuit Design Approach. In *IEEE International Conference on Computer Design*, pages 14–20, Oct. 2008.

[53] R. Garg and S.P. Khatri. 3d simulation and analysis of the radiation tolerance of voltage scaled digital circuit. In *Proceedings IEEE International Conference on Computer Design (ICCD'09)*, pages 498 –504, oct. 2009.

[54] G. Gasiot, P. Roche, and P. Flatresse. Comparison of multiple cell upset response of BULK and SOI 130nm technologies in the terrestrial environment. In *Proceedings IEEE International Reliability Physics Symposium (IRPS'08)*, pages 192–194, 27 2008-May 1 2008.

[55] X. Gili, S. Barcelo, S. Barcelo, S.A. Bota, and J. Segura. Analytical modeling of single event transients propagation in combinational logic gates. In *Radiation and Its Effects on Components and Systems (RADECS), 2011 12th European Conference on*, pages 408–411, Sept 2011.

[56] X. Gili, S. Barcelo, S.A. Bota, and J. Segura. Analytical modeling of single event transients propagation in combinational logic gates. *Nuclear Science, IEEE Transactions on*, 59(4):971–979, Aug 2012.

[57] B. Gill, M. Nicolaidis, F. Wolff, C. Papachristou, and S. Garverick. An Efficient BICS Design for SEUs Detection and Correction in Semiconductor Memories. In *Proceedings of the Conference on Design, Automation and Test in Europe*, volume 1, pages 592–597, March 2005.

[58] M.S. Gupta, J.A. Rivers, P. Bose, Gu-Yeon Wei, and D. Brooks. Tribeca: Design for pvt variations with local recovery and fine-grained adaptation. In *Microarchitecture, 2009. MICRO-42. 42nd Annual IEEE/ACM International Symposium on*, pages 435 –446, dec. 2009.

[59] G.B. Hamad, S.R. Hasan, O.A. Mohamed, and Y. Savaria. Modeling, analyzing, and abstracting single event transient propagation at gate level. In *Circuits and Systems (MWSCAS), 2014 IEEE 57th International Midwest Symposium on*, pages 515–518, Aug 2014.

[60] D. Harris and I. Sutherland. Logical effort of carry propagate adders. In *the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers*, volume 1, pages 873 – 878, nov. 2003.

[61] K. Joe Hass, Jody W. Gambles, Bill Walker, and Mike Zampaglione. Mitigating single event upsets from combinational logic. In *Proceedings of the 7th NASA Symposium on VLSI Design*, pages 4.1.1–4.1.10, oct 1998.

[62] J.D. Hayden, R.C. Taft, P. Kenkare, C. Mazure, C. Gunderson, B.-Y. Nguyen, M. Woo, C. Lage, B.J. Roman, S. Radhakrishna, R. Subrahmanyan, A. R. Sitaram, P. Pelley, J-H Lin, K. Kemp, and H. Kirsch. A quadruple well,

quadruple polysilicon bicmos process for fast 16 mb sram's. *Electron Devices, IEEE Transactions on*, 41(12):2318–2325, Dec 1994.

[63] P. Hazucha, T. Karnik, J. Maiz, S. Walstra, B. Bloechel, J. Tschanz, G. Dermer, S. Hareland, P. Armstrong, and S. Borkar. Neutron soft error rate measurements in a 90-nm CMOS process and scaling trends in SRAM from 0.25-um to 90-nm generation. In *Technical Digest IEEE International Electron Devices Meeting (IEDM'03)*, pages 21.5.1–21.5.4, Dec. 2003.

[64] P. Hazucha and C. Sevenson. Optimized test circuits for ser characterization of a manufacturing process. *Solid-State Circuits, IEEE Journal of*, 35(2):142 –148, feb 2000.

[65] P. Hazucha and C. Svensson. Cosmic ray neutron multiple-upset measurements in a 0.6-um CMOS process. *IEEE Transactions on Nuclear Science*, 47(6):2595–2602, Dec 2000.

[66] S. Hellebrand, C.G. Zoellin, S. Ludwig, T. Coym, and B. Straube. A refined electrical model for particle strikes and its impact on seu prediction. In *Defect and Fault-Tolerance in VLSI Systems, 2007. DFT '07. 22nd IEEE International Symposium on*, pages 50–58, Sept 2007.

[67] Y. Higami, K. K. Saluja, H. Takahashi, S. y. Kobayashi, and Y. Takamatsu. Increasing defect coverage by generating test vectors for stuck-open faults. In *2008 17th Asian Test Symposium*, pages 97–102, Nov 2008.

[68] Michael Hofbauer, Kurt Schweiger, Horst Dietrich, Horst Zimmermann, Kay-Obbe Voss, Bruno Merk, Ulrich Schmid, and Andreas Steininger. Pulse shape measurements by on-chip sense amplifiers of single event transients propagating through a 90 nm bulk CMOS inverter chain. *IEEE Transactions on Nuclear Science*, 59(6):2778–2784, December 2012.

[69] Michael Hofbauer, Kurt Schweiger, Horst Zimmermann, Ulrich Giesen, Frank Langner, Ulrich Schmid, and Andreas Steininger. Supply voltage dependent on-chip single event transient pulseshape measurements in 90 nm bulk CMOS under alpha irradiation. *IEEE Transactions on Nuclear Science*, 60(4):2640–2646, August 2013.

[70] C.M. Hsieh, P.C. Murley, and R.R. O'Brien. A field-funneling effect on the collection of alpha-particle-generated carriers in silicon devices. *Electron Device Letters, IEEE*, 2(4):103–105, April 1981.

[71] M. Ikeda, K. Ishii, T. Sogabe, and K. Asada. Datapath delay distributions for data/instruction against pvt variations in 90nm cmos. In *Electronics, Circuits and Systems, 2007. ICECS 2007. 14th IEEE International Conference on*, pages 154 –157, dec. 2007.

[72] R. C. Jaeger, R. M. Fox, and S. E. Diehl. Analytic expressions for the critical charge in CMOS static RAM cells. *IEEE Transactions on Nuclear Science*, 30(6):4616–4619, Dec. 1983.

[73] S.M. Jahinuzzaman, M. Sharifkhani, and M. Sachdev. An analytical model for soft error critical charge of nanometric srams. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 17(9):1187 –1195, sept. 2009.

[74] Z. Kalbarczyk, R.K. Iyer, G.L. Ries, J.U. Patel, M.S. Lee, and Y. Xiao. Hierarchical simulation approach to accurate fault modeling for system dependability evaluation. *IEEE Transactions on Software Engineering*, 25(5):619–632, Sep/Oct 1999.

[75] T. Karnik, P. Hazucha, and J. Patel. Characterization of soft errors caused by single event upsets in CMOS processes. *IEEE Transactions on Dependable and Secure Computing*, 1(2):128–143, April-June 2004.

[76] A.J. Kleinosowski, P.J. Oldiges, P.M. Solomon, and R.Q. Williams. Method for soft error modeling with double current pulse, December 2009. US Patent 7,627,840.

[77] D.. Kobayashi, H.. Saito, and K.. Hirose. Estimation of single event transient voltage pulses in VLSI circuits from heavy-ion-induced transient currents measured in a single mosfet. *IEEE Transactions on Nuclear Science*, 54(4):1037–1041, Aug. 2007.

[78] P. M. Kogge and H. S. Stone. A parallel algorithm for the efficient solution of a general class of recurrence equations. *IEEE Transactions on Computers*, C-22(8):786 –793, Aug. 1973.

[79] I. Koren and Z. Koren. Defect tolerance in VLSI circuits: Techniques and yield analysis. *Proceedings of the IEEE*, 86(9):1819–1838, Sep 1998.

[80] Weidong Kuang, Enjun Xiao, C.M. Ibarra, and Peiyi Zhao. Design asynchronous circuits for soft error tolerance. In *Proceedings IEEE International Conference on Integrated Circuit Design and Technology (ICICDT'07).*, pages 1–5, 30 2007-June 1 2007.

[81] Parag K. Lala, editor. *Self-checking and Fault-tolerant Digital Design*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2001.

[82] M. Lehman and N. Burla. Skip techniques for high-speed carry-propagation in binary arithmetic units. *IRE Transactions on Electronic Computers*, EC-10(4):691 –698, dec. 1961.

[83] Xiaolei Li, A. Strojwas, A. Swecker, and L. Milor. A study of defect propagation/growth for vlsi manufacturing yield impact prediction. In *Semiconductor Manufacturing Conference Proceedings, 1997 IEEE International Symposium on*, pages E31–E34, Oct 1997.

[84] P. Liden, P. Dahlgren, R. Johansson, and J. Karlsson. On latching probability of particle induced transients in combinational networks. In *Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., Twenty-Fourth International Symposium on*, pages 340–349, 1994.

[85] K. Lilja, M. Bounasser, S. J. Wen, R. Wong, J. Holst, N. Gaspard, S. Jagannathan, D. Loveless, and B. Bhuva. Single-event performance and layout optimization of flip-flops in a 28-nm bulk technology. *IEEE Transactions on Nuclear Science*, 60(4):2782–2788, Aug 2013.

[86] C. A. L. Lisboa, E. Schuler, and Luigi Carro. Going Beyond TMR for Protection Against Multiple Faults. In *Proc. 18th Symposium on Integrated Circuits and Systems Design*, pages 80–85, Sept. 2005.

[87] Z. Lu and W. Zhou. Analysis of single event effect on sram based on tcad simulation. In *2015 8th International Symposium on Computational Intelligence and Design (ISCID)*, volume 1, pages 588–591, Dec 2015.

[88] H. Luo and M. Nourani. Aging and leakage tradeoff in vlsi circuits. In *2015 10th International Design Test Symposium (IDT)*, pages 106–111, Dec 2015.

[89] R.E. Lyons and W. Vanderkulk. The use of triple-modular redundancy to improve computer reliability. *IBM Journal of Research and Development*, 6(2):200–209, April 1962.

[90] Atul Maheshwari, Israel Koren, and Wayne Burleson. Accurate estimation of Soft Error Rate (SER) in VLSI circuits. In *Proceedings of the 2004 IEEE Int. Symposium on Defect and Fault Tolerance in VLSI Systems*, pages 377–385, October 2004.

[91] M. Mounir Mahmoud, N. Soin, and H. A. H. Fahmy. Design framework to overcome aging degradation of the 16 nm vlsi technology circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(5):691–703, May 2014.

[92] A. J. Martin. *Formal program transformations for VLSI circuit synthesis*, pages 59–80. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1990.

[93] D.G. Mavis and P.H. Eaton. SEU and SET modeling and mitigation in deep submicron technologies. In *Proceedings 45th Annual IEEE International Reliability physics symposium*, pages 293–305, April 2007.

[94] R. McGowen, C.A. Poirier, C. Bostak, J. Ignowski, M. Millican, W.H. Parks, and S. Naffziger. Power and temperature control on a 90-nm itanium family processor. *Solid-State Circuits, IEEE Journal of*, 41(1):229 – 237, jan. 2006.

[95] G. C. Messenger. Collection of charge on junction nodes from ion tracks. *IEEE Transactions on Nuclear Science*, 29(6):2024–2031, Dec. 1982.

[96] S. D. Millman and E. J. McCluskey. Detecting stuck-open faults with stuck-at test sets. In *Custom Integrated Circuits Conference, 1989., Proceedings of the IEEE 1989*, pages 22.3/1–22.3/4, May 1989.

[97] S. Mitra, T. Karnik, N. Seifert, and Ming Zhang. Logic Soft Errors in sub-65nm Technologies Design and CAD Challenges. In *Proc. 42nd Annual Design Automation Conference*, pages 2–4, June 2005.

[98] S. Mitra and E.J. McCluskey. Word-voter: a new voter design for triple modular redundant systems. In *VLSI Test Symposium, 2000. Proceedings. 18th IEEE*, pages 465–470, 2000.

[99] E. K. Moghaddam and S. Hessabi. An on-line bist technique for stuck-open fault detection in cmos circuits. In *Digital System Design Architectures, Methods and Tools, 2007. DSD 2007. 10th Euromicro Conference on*, pages 619–625, Aug 2007.

[100] K. Mohanram and N.A. Touba. Partial error masking to reduce soft error failure rate in logic circuits. In *Defect and Fault Tolerance in VLSI Systems, 2003. Proceedings. 18th IEEE International Symposium on*, pages 433–440, Nov 2003.

[101] P. Mongkolkachit and B. Bhuva. Design Technique for Mitigation of Alpha-Particle-Induced Single-Event Transients in Combinational Logic. *IEEE Transactions on Device and Materials Reliability*, 3(3):89–92, Sept. 2003.

[102] Y. Monnet, M. Renaudin, and R. Leveugle. Designing resistant circuits against malicious faults injection using asynchronous logic. *IEEE Transactions on Computers*, 55(9):1104–1115, Sept. 2006.

[103] T.S. Mukherjee, A.K. Sutton, K.T. Kornegay, R. Krithivasan, J.D. Cressler, Guofu Niu, and P.W. Marshall. A novel circuit-level seu hardening technique for high-speed sige hbt logic circuits. *Nuclear Science, IEEE Transactions on*, 54(6):2086–2091, Dec 2007.

[104] D.E. Muller and W.S. Bartky. A theory of asynchronous circuits. In *Theory of Switching, Proc. Int'l Symp.*, pages 204–243, 1959.

[105] 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, and P.H. Eaton. Characterization of digital single event transient pulse-widths in 130-nm and 90-nm CMOS technologies. *IEEE Transactions on Nuclear Science*, 54(6):2506–2511, Dec. 2007.

[106] B. Narasimham, M.J. Gadlage, B.L. Bhuva, R.D. Schrimpf, L.W. Massengill, W.T. Holman, A.F. Witulski, and K.F. Galloway. Test circuit for measuring pulse widths of single-event transients causing soft errors. In *Proceedings IEEE International Conference on Microelectronic Test Structures (ICMTS'08)*, pages 142–146, March 2008.

[107] B. Narasimham, V. Ramachandran, B. L. Bhuva, R. D. Schrimpf, A. F. Witulski, W. T. Holman, L. W. Massengill, J. D. Black, W. H. Robinson, and D. McMorrow. On-chip characterization of single-event transient pulsewidths. *IEEE Transactions on Device and Materials Reliability*, 6(4):542–549, Dec. 2006.

[108] R. Naseer and J. Draper. DF-DICE: A Scalable Solution for Soft Error Tolerant Circuit Design. In *Proc. IEEE International Symposium on Circuits and Systems*, page 4, May 2006.

[109] E.H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F.L. Kastensmidt. Using Bulk Built-in Current Sensors to Detect Soft Errors. *IEEE Micro*, 26(5):10–18, Sept.-Oct. 2006.

[110] H.T. Nguyen, Y. Yagil, N. Seifert, and M. Reitsma. Chip-level soft error estimation method. *IEEE Transactions on Device and Materials Reliability*, 5(3):365–381, Sept. 2005.

[111] M. Nicolaidis and R. Perez. Measuring the width of transient pulses induced by ionising radiation. *Proceedings 41st Annual IEEE International Reliability Physics Symposium*, pages 56–59, March-4 April 2003.

[112] Michael Nicolaidis. *Soft Errors in Modern Electronic Systems*. Springer Publishing Company, Incorporated, 1st edition, 2010.

[113] Eugene Normand. Single-event effects in avionics. *IEEE Transactions on Nuclear Science*, 43(2):461–474, Apr 1996.

[114] P. Oldiges, K. Bernstein, D. Heidel, B. Klaasen, E. Cannon, R. Dennard, H. Tang, M. Ieong, and H. S. P. Wong. Soft error rate scaling for emerging soi technology options. In *VLSI Technology, 2002. Digest of Technical Papers. 2002 Symposium on*, pages 46–47, June 2002.

[115] A. Pal and B. Bhattacharya. Syndrome-testable logic design using dstl arrays for detecting stuck-at and bridging faults. *IEE Proceedings E - Computers and Digital Techniques*, 132(5):251–256, September 1985.

[116] J. H. Patel and L. Y. Fung. Concurrent error detection in alu's by recomputing with shifted operands. *IEEE Transactions on Computers*, C-31(7):589–595, July 1982.

[117] D. Patil, O. Azizi, M. Horowitz, R. Ho, and R. Ananthraman. Robust energy-efficient adder topologies. In *Computer Arithmetic, 2007. ARITH '07. 18th IEEE Symposium on*, pages 16 –28, june 2007.

[118] A. S. Priya. Defect-aware methodology for low-power scan-based vlsi testing. In *2015 Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG)*, pages 234–238, Dec 2015.

[119] R. Ramanarayanan, V. S. Degalahal, R. Krishnan, J. Kim, V. Narayanan, Y. Xie, M. J. Irwin, and K. Unlu. Modeling soft errors at the device and logic levels for combinational circuits. *IEEE Transactions on Dependable and Secure Computing*, 6(3):202–216, July 2009.

[120] Vijay Janapa Reddi, Svilen Kanev, Wonyoung Kim, Simone Campanoni, Michael D. Smith, Wei Gu-Yeon, and David Brooks. Voltage noise in production processors. *IEEE Micro*, pages 20 – 28, jan. 2011.

[121] M. K. Reddy and S. M. Reddy. Detecting fet stuck-open faults in cmos latches and flip-flops. *IEEE Design Test of Computers*, 3(5):17–26, Oct 1986.

[122] G.L. Ries, G.S. Choi, and R.K. Iyer. Device-level transient fault modeling. In *Proceedings Twenty-Fourth International Symposium on Fault-Tolerant Computing (FTCS-24)*, pages 86–94, Jun 1994.

[123] P. Roche and G. Gasiot. Impacts of front-end and middle-end process modifications on terrestrial soft error rate. *IEEE Transactions on Device and Materials Reliability*, 5(3):382–396, Sept. 2005.

[124] P. Roche, J.M. Palau, G. Bruguier, C. Tavernier, R. Ecoffet, and J. Gasiot. Determination of key parameters for seu occurrence using 3-d full cell sram simulations. *Nuclear Science, IEEE Transactions on*, 46(6):1354 –1362, dec. 1999.

[125] A. Rohani, H.G. Kerkhoff, E. Costenaro, and D. Alexandrescu. Pulse-length determination techniques in the rectangular single event transient fault model. In *Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS XIII), 2013 International Conference on*, pages 213–218, July 2013.

[126] M. Saremi, A. Privat, H. J. Barnaby, and L. T. Clark. Physically based predictive model for single event transients in cmos gates. *IEEE Transactions on Electron Devices*, 63(6):2248–2254, June 2016.

[127] R.D. Schrimpf and D.M. Fleetwood. *Radiation Effects and Soft Errors in Integrated Circuits and Electronic Devices*. International journal of high speed electronics and systems. World Scientific Pub., 2004.

[128] J.R. Schwank, M.R. Shaneyfelt, P. Paillet, D.E. Beutler, V. Ferlet-Cavrois, B.L. Draper, R.A. Loemaker, P.E. Dodd, and F.W. Sexton. Optimum laboratory radiation source for hardness assurance testing. *IEEE Transactions on Nuclear Science*, 48(6):2152–2157, Dec 2001.

[129] K. Schweiger, M. Hofbauer, H. Dietrich, H. Zimmermann, K.O. Voss, and B. Merk. Position dependent measurement of single event transient voltage pulse shapes under heavy ion irradiation. *Electronics Letters*, 48(3):171–172, 2012.

[130] N. Seifert, P. Shipley, M.D. Pant, V. Ambrose, and B. GiII. Radiation-induced clock jitter and race. In *Proceedings 43rd Annual IEEE International Reliability Physics Symposium*, pages 215–222, 17-21, 2005.

[131] N. Seifert, P. Slankard, M. Kirsch, B. Narasimham, V. Zia, C. Brookreson, A. Vo, S. Mitra, B. Gill, and J. Maiz. Radiation-induced soft error rates of advanced cmos bulk devices. In *2006 IEEE International Reliability Physics Symposium Proceedings*, pages 217–225, March 2006.

[132] M. Shams, J. Ebergen, and M. Elmasry. A comparison of cmos implementations of an asynchronous circuits primitive: the c-element. In *Proceedings of the 1996 international symposium on Low power electronics and design*, ISLPED '96, pages 93–96, 1996.

[133] P. Shivakumar, M. Kistler, S.W. Keckler, D. Burger, and L. Alvisi. Modeling the effect of technology trends on the soft error rate of combinational logic. *Proceedings International Conference on Dependable Systems and Networks(DSN'02)*, pages 389–398, 2002.

[134] J. Sklansky. Conditional-sum addition logic. *IRE Transactions on Electronic Computers*, EC-9(2):226 –231, june 1960.

[135] J. Sparsø. Asynchronous circuit design - a tutorial. In *Chapters 1-8 in "Principles of asynchronous circuit design - A systems Perspective"*, pages 1–152. Kluwer Academic Publishers, dec 2001.

[136] G.R. Srinivasan, P.C. Murley, and H.K. Tang. Accurate, predictive modeling of soft error rate due to cosmic rays and chip alpha radiation. *Proceedings 32nd Annual IEEE International Reliability Physics Symposium*, pages 12–16, Apr 1994.

[137] Andreas Steininger, Varadan Savulimedu Veeravalli, Dan Alexandrescu, Enrico Costenaro, and Lorena Anghel. Exploring the state dependent SET sensitivity of asynchronous logic - the muller-pipeline example. In *32nd IEEE International Conference on Computer Design, ICCD 2014, Seoul, South Korea, October 19-22, 2014*, pages 61–67, 2014.

[138] I. E. Sutherland. Micropipelines. *Commun. ACM*, 32:720–738, June 1989.

[139] A. Swecker, A. Strojwas, Xiaolei Li, and A. Levy. Simulation of defect detection schemes for wafer inspection in vlsi manufacturing. In *Simulation of Semiconductor Processes and Devices, 1997. SISPAD '97., 1997 International Conference on*, pages 145–148, Sept 1997.

[140] M. Takai, T. Kishimoto, Y. Ohno, H. Sayama, K. Sonoda, S. Satoh, T. Nishimura, H. Miyoshi, A. Kinomura, Y. Horino, and K. Fujii. Soft error susceptibility and immune structures in dynamic random access memories (drams) investigated by nuclear microprobes. *Nuclear Science, IEEE Transactions on*, 43(2):696–704, Apr 1996.

[141] A. Torres, J.E. Sauvestre, B.E. Fischer, and P. Barberet. Charge collection measurements on soi capacitors using heavy ion microprobe at gsi. In *Proceedings 8th European Conference on Radiation and Its Effects on Components and Systems (RADECS'05).*, pages PG1–1 –PG1–5, sept. 2005.

[142] Y. Tosaka, S. Satoh, T. Itakura, H. Ehara, T. Ueda, G.A. Woffinden, and S.A. Wender. Measurement and analysis of neutron-induced soft errors in sub-half-micron CMOS circuits. *IEEE Transactions on Electron Devices*, 45(7):1453–1458, Jul 1998.

[143] M. Trevisan Moreira and N. Laert Vilar Calazans. Voltage scaling on c-elements: A speed, power and energy efficiency analysis. In *Computer Design (ICCD), 2013 IEEE 31st International Conference on*, pages 329–334, Oct 2013.

[144] Balaji Vaidyanathan, Yuan Xie, N Vijaykrishnan, and Hao Zheng. Soft error analysis and optimizations of c-elements in asynchronous circuits. *The Second Workshop on System Effects of Logic Soft Errors*, 2006.

[145] Kees van Berkel. Beware the isochronic fork. *Integr. VLSI J.*, 13:103–128, June 1992.

[146] V. S. Veeravalli and A. Steininger. Performance of radiation hardening techniques under voltage and temperature variations. In *Aerospace Conference, 2013 IEEE*, pages 1–12, March 2013.

[147] V. S. Veeravalli and A. Steininger. Study of a delayed single-event effect in the muller c-element. In *2016 21th IEEE European Test Symposium (ETS)*, pages 1–2, May 2016.

[148] Varadan Savulimedu Veeravalli, Thomas Polzer, Ulrich Schmid, Andreas Steininger, Michael Hofbauer, Kurt Schweiger, Horst Dietrich, Kerstin Schneider-Hornstein, Horst Zimmermann, Kay-Obbe Voss, Bruno Merk, and Michael Hajek. An infrastructure for accurate characterization of single-event transients in digital circuits. *Microprocessors and Microsystems*, 37(8, Part A):772 – 791, 2013. Special Issue {DSD} 2012 on Reliability and Dependability in {MPSoC} Technologies.

[149] V.S. Veeravalli, T. Polzer, A. Steininger, and U. Schmid. Architecture and design analysis of a digital single-event transient/upset measurement chip. In *15th Euromicro Conference on Digital System Design (DSD)*, pages 8–17, 2012.

[150] V.S. Veeravalli and A. Steininger. Long term on-chip monitoring of set pulsewidths in a fully digital asic. In *Microelectronics (Austrochip), 22nd Austrian Workshop on*, pages 1–6, Oct 2014.

[151] V.S. Veeravalli, A. Steininger, and U. Schmid. Measuring set pulsewidths in logic gates using digital infrastructure. In *Quality Electronic Design (ISQED), 2014 15th International Symposium on*, pages 236–242, March 2014.

[152] J. Velamala, R. LiVolsi, M. Torres, and Yu Cao. Design sensitivity of single event transients in scaled logic circuits. In *Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE*, pages 694–699, June 2011.

[153] John von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Automata Studies*, pages 43–98, 1956.

[154] S. Whitaker, J. Canaris, and K. Liu. SEU Hardened Memory Cells for a CCSDS Reed-Solomon Encoder. *IEEE Transactions on Nuclear Science*, 38(6):1471–1477, Dec 1991.

[155] G.I. Wirth, M.G. Vieira, and F.G.L. Kastensmidt. Computer efficient modeling of sram cell sensitivity to seu. In *Proc. IEEE Latin American Test Workshop*, pages 51–56. IEEE CS Press, 2005.

[156] G.I. Wirth, M.G. Vieira, E.H. Neto, and F.G.L. Kastensmidt. Single event transients in combinatorial circuits. In *Integrated Circuits and Systems Design, 18th Symposium on*, pages 121 –126, sept. 2005.

[157] F. Wrobel, L. Dilillo, A.D. Touboul, V. Pouget, and F. Saigne. Determining realistic parameters for the double exponential law that models transient current pulses. *Nuclear Science, IEEE Transactions on*, 61(4):1813–1818, Aug 2014.

[158] F. Wrobel, L. Dilillo, A.D. Touboul, and F. Saigne. Comparison of the transient current shapes obtained with the diffusion model and the double exponential law – impact on the ser. In *Radiation and Its Effects on Components and Systems (RADECS), 2013 14th European Conference on*, pages 1–4, Sept 2013.

[159] Y.Z. Xu, H. Puchner, A. Chatila, O. Pohland, B. Bruggeman, B. Jin, D. Radaelli, and S. Daniel. Process impact on sram alpha-particle seu performance. In *Reliability Physics Symposium Proceedings, 2004. 42nd Annual. 2004 IEEE International*, pages 294 – 299, april 2004.

[160] Y. Yanagawa, K. Hirose, H. Saito, D. Kobayashi, S. Fukuda, S. Ishii, D. Takahashi, K. Yamamoto, and Y. Kuroda. Direct measurement of SET pulse widths in 0.2 - um SOI logic cells irradiated by heavy ions. *IEEE Transactions on Nuclear Science*, 53(6):3575–3578, Dec. 2006.

[161] S. Yancey and S.C. Smith. A differential design for c-elements and ncl gates. In *Circuits and Systems (MWSCAS), 2010 53rd IEEE International Midwest Symposium on*, pages 632–635, Aug 2010.

[162] Bin Zhang, Ari Arapostathis, Sani Nassif, and Michael Orshansky. Analytical modeling of sram dynamic stability. In *Proceedings of the 2006 IEEE/ACM international conference on Computer-aided design*, ICCAD '06, pages 315–322, New York, NY, USA, 2006. ACM.

[163] Quming Zhou and K. Mohanram. Transistor sizing for radiation hardening. In *Reliability Physics Symposium Proceedings, 2004. 42nd Annual. 2004 IEEE International*, pages 310–315, April 2004.

[164] Quming Zhou and K. Mohanram. Gate Sizing to Radiation Harden Combinational Logic. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(1):155–166, Jan. 2006.

[165] James F. Ziegler. SRIM-2003. *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms*, 219-220(0):1027 – 1036, 2004. Proceedings of the Sixteenth International Conference on Ion Beam Analysis.

[166] Reto Zimmermann. Non-heuristic optimization and synthesis of parallel-prefix adders. In *In Proc. Int. Workshop on Logic and Architecture Synthesis*, pages 123–132, Gernoble, France, December 1996.

APPENDIX A

Appendix A

A.1 FRad Chip Pin Description

The pin list are shown in Table. A.1, A.2, A.3 and provides the following information:

- ⋆ Signal Name - Name used inside the ASIC
- ⋆ Pad Number - Refers to the number of the pad
- ⋆ Port Type - Defines which signal standard is used
- ⋆ Output Drive (mA) - Defines the driver strength of the output port. If it is left blank then it means this pin is an input
- ⋆ In/Out - Specifies the interface direction (in, out, bidirectional (in/out))
- ⋆ Load - Defines with which laod the pin was analyzed

A brief description of the cells used in the ASIC are listed below:

→ IVDD is the power pad for 1.2V power in digital section

→ IVDDIO is the power pad for 1.8/2.5/3.3V power in digital section

→ IVSS/IVSSIO is the ground pad in digital section

→ There are two types of IO cells provided by the IO library (refer Sec. 7.2.3): IUMA and IUMB. We chose to use the IUMB cell with 2.5V voltage utilization. There are several pins within the cell that can be used to configure it as both input and outputs

Table A.1: FRad Pin List

Signal Name	Pad Number	Port Type	Output Drive (mA)	In/Out	Load (pF)
PISO RST	1	IUMB	–	In	–
PISO SHIFT	2	IUMB	–	In	–
PISO CLK30	3	IUMB	–	In	–
Core VSS	4	IVSS	–	–	–
Core VDD	5	IVDD	–	–	–
PISO CLK84	6	IUMB	–	In	–
PISO CLK75	7	IUMB	–	In	–
PISO CLK110	8	IUMB	–	In	–
PISO CLK55	9	IUMB	–	In	–
IO VSS	10	IVSSIO	–	–	–
IO VDD	11	IVDDIO	–	–	–
PISO CLK25	12	IUMB	–	In	–
CNT-SET	13	IUMB	–	In	–
TAR-A-D	14	IUMB	–	In	–
RST-TAR-CNT	15	IUMB	–	In	–
Core VSS	16	IVSS	–	–	–
Core VDD	17	IVDD	–	–	–
TAR-CLK	18	IUMB	–	In	–
TAR-SEL0	19	IUMB	–	In	–
TAR-SEL1	20	IUMB	–	In	–
TAR-WRITE	21	IUMB	–	In	–
TAR-READ	22	IUMB	–	In	–
PISO30-1	23	IUMB	12	Out	26.9611
PISO30-2	24	IUMB	12	Out	26.9611
PISO30-3	25	IUMB	12	Out	26.9611
IO VDD	26	IVDDIO	–	–	–
IO VSS	27	IVSSIO	–	–	–
PISO30-4	28	IUMB	12	Out	26.9611

Table A.2: FRad Pin List

Signal Name	Pad Number	Port Type	Output Drive (mA)	In/Out	Load (pF)
PISO84-1	29	IUMB	12	Out	26.9611
PISO30-5	30	IUMB	12	Out	26.9611
PISO75-1	31	IUMB	12	Out	26.9611
Core VDD	32	IVDD	–	–	–
Core VSS	33	IVSS	–	–	–
PISO75-2	34	IUMB	12	Out	26.9611
PISO84-2	35	IUMB	12	Out	26.9611
PISO84-3	36	IUMB	12	Out	26.9611
PISO84-4	37	IUMB	12	Out	26.9611
IO VDD	38	IVDDIO	–	–	–
IO VSS	39	IVSSIO	–	–	–
PISO84-5	40	IUMB	12	Out	26.9611
PISO84-6	41	IUMB	12	Out	26.9611
PISO84-7	42	IUMB	12	Out	26.9611
PISO84-8	43	IUMB	12	Out	26.9611
PISO84-9	44	IUMB	12	Out	26.9611
PISO110-1	45	IUMB	12	Out	26.9611
PISO30-6	46	IUMB	12	Out	26.9611
Core VDD	47	IVDD	–	–	–
Core VSS	48	IVSS	–	–	–
PISO30-7	49	IUMB	12	Out	26.9611
PISO30-8	50	IUMB	12	Out	26.9611
PISO30-9	51	IUMB	12	Out	26.9611
PISO110-2	52	IUMB	12	Out	26.9611
IO VDD	53	IVDDIO	–	–	–
IO VSS	54	IVSSIO	–	–	–
PISO30-10	55	IUMB	12	Out	26.9611
PISO30-11	56	IUMB	12	Out	26.9611

Table A.3: FRad Pin List

Signal Name	Pad Number	Port Type	Output Drive (mA)	In/Out	Load (pF)
PISO30-12	57	IUMB	12	Out	26.9611
PISO30-13	58	IUMB	12	Out	26.9611
Core VDD	59	IVDD	–	–	–
Core VSS	60	IVSS	–	–	–
PISO110-3	61	IUMB	12	Out	26.9611
PISO84-10	62	IUMB	12	Out	26.9611
PISO84-11	63	IUMB	12	Out	26.9611
PISO84-12	64	IUMB	12	Out	26.9611
PISO84-13	65	IUMB	12	Out	26.9611
PISO84-14	66	IUMB	12	Out	26.9611
IO VDD	67	IVDDIO	–	–	–
IO VSS	68	IVSSIO	–	–	–
PISO84-15	69	IUMB	12	Out	26.9611
PISO84-16	70	IUMB	12	Out	26.9611
PISO84-17	71	IUMB	12	Out	26.9611
PISO75-3	72	IUMB	12	Out	26.9611
Core VDD	73	IVDD	–	–	–
Core VSS	74	IVSS	–	–	–
PISO55-1	75	IUMB	12	Out	26.9611
PISO25-1	76	IUMB	12	Out	26.9611
PISO30-14	77	IUMB	12	Out	26.9611
PISO84-18	78	IUMB	12	Out	26.9611
IO VDD	79	IVDDIO	–	–	–
IO VSS	80	IVSSIO	–	–	–
PISO30-15	81	IUMB	12	Out	26.9611
PISO30-16	82	IUMB	12	Out	26.9611
PISO30-17	83	IUMB	12	Out	26.9611
PISO30-18	84	IUMB	12	Out	26.9611

- **Input cell** - To use the IUMB as an input cell we configure the pins in the cell as follows:
  PU, PIN1, PIN2, DO, SR, OE, IDDQ are connected to IVSS.
  SMT, PD are connected to IVDD.
  DI is connected to the core input signal.
- **Output cell** - To use the IUMB as an output cell we configure the pins in the cell as follows:
  PU, PD, PIN2, SMT, SR, IDDQ are connected to IVSS
  PIN1, OE are connected to IVDD.
  DO is connected to the core output signal. Note, that DI is left open.

The above mentioned configuration for the cells are extremely important to have the ASIC function properly. Also note that PIN1 and PIN2 can be configured to increase the drive strength to 16mA.

A.2 ASIC Signal Description

A.2.1 Clock

The FRad ASIC uses seven different clock inputs. Reason behind not using just one clock input with an on-chip clock tree to generate the seven clocks are:

- Faults in the clock tree could create unreliable operations in the ASIC during read out
  - Any fault in the clock tree would propagate to the target circuit and change the counter data; that is being read out. Note that the SET in the clock tree will be recognized as an SET in the sequential target. If it occurs during $T_{radiationtime}$ then the SET will be recorded in the counters. If it occurs during $T_{readout}$ then"
    - After/during first readout - SET data is recorded by the counters
    - After second redout - SET data would be neglected
    - During seconf readout - possibility of all three readouts being different
    - After/during third readout - SET data would be neglected.
- asynchronous and reliable operation of the PISOs
- avoiding SET pulses in the input of the targets; due to a fault in the clock tree

We could use two separate clock inputs for the targets and the PISO. Moreover, instead of using six different clocks inputs for the PISO we could use one clock input with a clock tree that generates six clocks for the PISOs. All the PISOs will be activated at the same time in the ASIC, hence using one clock should be fine.

Furthermore, any SET in the clock tree will be recovered, when we read the data out three times.

Note: In the event we need extra pins for testing purposes, the pins used for the clocks of the PISO can be borrowed.

Hence, for the second fabrication run we will employ a clock tree and reduce the number of pins used by the PISOs to 1 instead of 6.

PISO CLK30 - The FRad ASIC receives a clock signal at the input of PISO CLK30 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to all the 18 30-bit PISOs in the ASIC.

PISO CLK84 - The FRad ASIC receives a clock signal at the input of PISO CLK84 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to all the 18 84-bit PISOs in the ASIC.

PISO CLK75 - The FRad ASIC receives a clock signal at the input of PISO CLK75 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to all the 3 75-bit PISOs in the ASIC.

PISO CLK110 - The FRad ASIC receives a clock signal at the input of PISO CLK110 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to all the 3 110-bit PISOs in the ASIC.

PISO CLK55 - The FRad ASIC receives a clock signal at the input of PISO CLK55 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to the only 55-bit PISO in the ASIC.

PISO CLK25 - The FRad ASIC receives a clock signal at the input of PISO CLK25 with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to the only 25-bit PISO in the ASIC.

TAR-CLK - The FRad ASIC receives a clock signal at the input of TAR-CLK with a frequency of 100MHz$\pm$10%. The duty cycle of the signal needs to be 50%. This clock signal will be fed to the flip-flop chains (radiation target) in the ASIC.

A.2.2 Reset

There are three reset pins in the ASIC.

RST-TAR-CNT - The targets and the measurement counters are reset when RST-TAR-CNT is low (minimum reset pulse width is 40ns) and the whole ASIC is ready for use when RST-TAR-CNT is high. The reset function is not dependant on any clock or other signal. When this signal is active: the target flip-flops are reset to “0”, the LFSRs are reset to “0”, and the Muller C-elements with “rst” signal used

by the up/down counters are set to “1”. Note, that the output signals are not affected by this signal

CNT-SET - The Muller C-elements with “set” signal used by the up/down counters are set to “0” when CNT-SET is high (minimum pulse is 40ns). This signal must be high atleast for 10ns when RST-TAR-CNT is active low.

PISO RST - All the output signals in the ASIC are reset when PISO RST is low (minimum reset pulse width is 40ns). This signal basically resets all the PISO data to “0”, it does not affect the counter data. During multiple read outs we could reset the PISO to avoid having any faults (SEU in the FFs when exposed to radiation) when the first read out is complete and the second read out is on the way.

The functional behavior of the ASIC after it is initialized will be presented in Sec. 7.4

A.2.3 Input Data Signals

There are three input data pins in the ASIC.

TAR-A-D - TAR-A-D is an input data signal to the target circuits in the ASIC. It is normally operated at a frequency of 100MHz$\pm$10$\%$ with a duty cycle of 50$\%$. To analyse the targets in static mode it can also be operated at static low or high.

TAR-WRITE - TAR-WRITE is an input data signal to the target circuit Muller pipeline in the ASIC. It is normally operated at a frequency of 100MHz$\pm$10$\%$ with a duty cycle of 50$\%$. It can also be operated in a static way.

TAR-READ - TAR-READ is an input data signal to the target circuit Muller pipeline in the ASIC. It is normally operated at a frequency of 100MHz$\pm$10$\%$ with a duty cycle of 50$\%$. It can also be operated in a static way.

Note that with the help of both the TAR-READ and TAR-WRITE signals we can operate the pipeline in three different modes:

- **Full**: Stimulating the TAR-WRITE signal and steering the TAR-READ signal either to low or high; we could fill the pipeline with “1”, thereby making it full.

- **Empty**: Having activity in the TAR-READ signal and steering the TAR-WRITE signal either to low or high; we could fill the pipeline with “0”, thereby making it empty.

- **Full/Empty**: Stimulating both the TAR-WRITE and the TAR-READ signal we could have a half-full/half-empty pipeline. By properly steering these two signals we could make sure that the pipeline is neither full nor empty.

A.2.4 Input Control Signals

There are three input control pins in the ASIC.

PISO SHIFT - PISO SHIFT is the key input control signal in the ASIC. This signal remains "high" during and after the initialization of the ASIC. When this signal is steered "low" (minimum 10ns) data is sampled into the PISOs and when it is high data is shifted out. When we want to read the data of the counters out we set this signal to low, and sample the data into the flip-flops of the PISOs. After the data is sampled we set the signal to high and read the data serially out of the ASIC.

TAR-SEL0, TAR-SEL1 - TAR-SEL0 and TAR-SEL1 are input control signals to the MUXes in the ASIC. They are normally set to either low or high.

Using the TAR-SEL0 and TAR-SEL1 we could choose which combinational gate to analyze. The device under test with the different combination of these signals are given in Table. A.4.

Table A.4: MUX and CUT combination

TAR-SEL0	TAR-SEL1	Circuit Under Test
0	0	NOR
0	1	XOR
1	0	NAND
1	1	Inverter

A.2.5 Data Output Signals

There are totally 44 output data pins in the ASIC.
PISO30-i - PISO30-i (where i ranges from 1 to 18) is an output data signal of the FRad ASIC generated by the 30-bit PISOs. The output data is controlled by the signals: PISO RST, PISO SHIFT, and PISO CLK30.

PISO84-i - PISO84-i (where i ranges from 1 to 18) is an output data signal of the FRad ASIC generated by the 84-bit PISOs. The output data is controlled by the signals: PISO RST, PISO SHIFT, and PISO CLK84

PISO110-i - PISO110-i (where i ranges from 1 to 3) is an output data signal of the FRad ASIC generated by the 110-bit PISOs. The output data is controlled by the signals: PISO RST, PISO SHIFT, and PISO CLK110

PISO75-i - PISO75-i (where i ranges from 1 to 3) is an output data signal of the FRad ASIC generated by the 75-bit PISOs. The output data is controlled by the

signals: PISO RST, PISO SHIFT, and PISO CLK75

PISO55 - PISO55 is an output data signal of the FRad ASIC generated by the 55-bit PISO. The output data is controlled by the signals: PISO RST, PISO SHIFT, and PISO CLK55

PISO25 - PISO25 is an output data signal of the FRad ASIC generated by the 25-bit PISO. The output data is controlled by the signals: PISO RST, PISO SHIFT, and PISO CLK25