Radiation Hardened by Design Methodologies for Soft-Error Mitigated Digital Architectures

by

Chandarasekaran Ramamurthy

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved July 2017 by the
Graduate Supervisory Committee:

Lawrence Clark, Chair
David Allee
Bertan Bakkaloglu
Keith Holbert

ARIZONA STATE UNIVERSITY

August 2017

ABSTRACT

Digital architectures for data encryption, processing, clock synthesis, data transfer, etc. are susceptible to radiation induced soft errors due to charge collection in complementary metal oxide semiconductor (CMOS) integrated circuits (ICs). Radiation hardening by design (RHBD) techniques such as double modular redundancy (DMR) and triple modular redundancy (TMR) are used for error detection and correction respectively in such architectures. Multiple node charge collection (MNCC) causes domain crossing errors (DCE) which can render the redundancy ineffectual. This dissertation describes techniques to ensure DCE mitigation with statistical confidence for various designs. Both sequential and combinatorial logic are separated using these custom and computer aided design (CAD) methodologies.

Radiation vulnerability and design overhead are studied on VLSI sub-systems including an advanced encryption standard (AES) which is DCE mitigated using module level coarse separation on a 90-nm process with 99.999% DCE mitigation. A radiation hardened microprocessor (HERMES2) is implemented in both 90-nm and 55-nm technologies with an interleaved separation methodology with 99.99% DCE mitigation while achieving 4.9% increased cell density, 28.5 % reduced routing and 5.6% reduced power dissipation over the module fences implementation. A DMR register-file (RF) is implemented in 55 nm process and used in the HERMES2 microprocessor. The RF array custom design and the decoders APR designed are explored with a focus on design cycle time. Quality of results (QOR) is studied from power, performance, area and reliability (PPAR) perspective to ascertain the improvement over other design techniques.

A radiation hardened all-digital multiplying pulsed digital delay line (DDL) is designed for double data rate (DDR2/3) applications for data eye centering during high

speed off-chip data transfer. The effect of noise, radiation particle strikes and statistical variation on the designed DDL are studied in detail. The design achieves the best in class 22.4 ps peak-to-peak jitter, 100-850 MHz range at 14 pJ/cycle energy consumption. Vulnerability of the non-hardened design is characterized and portions of the redundant DDL are separated in custom and auto-place and route (APR). Thus, a range of designs for mission critical applications are implemented using methodologies proposed in this work and their potential PPAR benefits explored in detail.

DEDICATION

To my parents
Vijayalakshmi and T.R. Ramamurthy

ACKNOWLEDGMENTS

I would like to express my gratitude to the various individuals who helped and supported me throughout the duration of my doctorate.

Firstly, I would like to thank my mother Vijayalakshmi Ramamurthy, for inculcating patience and curiosity, and my father T.R. Ramamurthy for inculcating creativity and steadfastness in me. Their support has been instrumental during the course of my studies as I manoeuvred various challenges.

The Indian tradition of "guru-shishya parampara" or student-teacher lineage states that 'the genuineness of the guru (teacher), and the respect, commitment, devotion and obedience of the shishya (student), is the best way for subtle or advanced knowledge to be conveyed'. In the same vein I would like to thank Professor Lawrence T. Clark for being my mentor during this PhD. I would also like to thank Professors David Allee, Bertan Bakkaloglu and Keith Holbert for being part of my committee and providing valuable feedback.

I want to thank my colleagues Srivatsan Chellappa, Sandeep Shambhulingiah, Vinay Vashishtha, Sushil Kumar, Aditya Gujja, Lovish Masand, Ankita Dosi, Parshant Rana, Chris Lieb, Dan Patterson, Nathan Hindman, Satendra Maurya and Jerin Xavier for the discussions, brainstorming sessions and contributions which helped me achieve my doctoral degree goals. I would like to thank the administrative staff at the electrical engineering department, Toni, Lynn, Jenna, Esther and Donna for their support and help. I would also like to thank Angelica Campos for her emotional support and encouragement.

Finally I would like to thank the 'higher power' that makes our 'pale blue dot' tick because it's the recognition of our insignificance that gives our lives purpose and focus.

TABLE OF CONTENTS

Page

LIST OF TABLES ix

LIST OF FIGURES x

CHAPTER

1. INTRODUCTION 1

1.1. Introduction 1

1.2. Space Weather and Radiation Environment 2

1.3. Radiation Effects on CMOS devices 5

1.4. Single Event Effects 7

1.5. Scaling and SER 14

1.6. Radiation Hardening 21

1.7. Multiple Node Charge Collection (MNCC) and Domain Crossing Errors (DCE) 25

1.8. MNCC Separation in CAD Flows 27

1.9. Summary 31

2. MODULE LEVEL SEPARATION: AES 33

2.1. Introduction 33

2.2. AES Encryption Background 33

2.3. TMR Pulse-clocked Latch for RHBD 40

CHAPTER Page

2.4. Pulsed Latch Operation 45

2.5. Module Level Separation CAD Flow 47

2.6. Spatial Separation Analysis 55

2.7. Test Chip Implementation 57

2.8. Error Injection Simulation Validation 59

2.9. Experimental Setup and Silicon Validation 60

2.10. Design Comparison 63

2.11. Summary 64

3. INTERLEAVED SEPARATION: HERMES 66

3.1. Introduction 66

3.2. HERMES Background 67

3.3. Improved Interleaved Separation 70

3.4. ReAPR Co-design methodology 76

3.5. Implementation 86

3.6. Reliability Analysis and Radiation Testing 88

3.7. Summary 93

4. RADIATION HARDENED PULSED MULTIPLYING DLL 95

4.1. Introduction 95

4.2. Delay Locked Loop Background 95

4.3. Radiation Hardened Pulsed Multiplying DLL 99

4.4. Decoding Logic 111

CHAPTER Page

4.5. Control (Acquisition and Tracking) Logic Design 117

4.6. Functional Logic Simulations 131

4.7. Process Variability 134

4.8. Circuit Simulations and Critical Timing 139

4.9. Performance Overview 144

4.10. Soft-Error vulnerability 148

4.11. TC 25 55-nm Test-chip Structures and Results 151

4.12. TC23 90 nm Test Results 154

4.13. Performance summary and comparison. 159

4.14. Summary 160

5. DMR SEMI-CUSTOM DESIGN FLOW: REGISTER-FILE 161

5.1. Introduction 161

5.2. DMR Registerfile Background 161

5.3. DMR RF Circuit Design 164

5.4. Well-bias for Body Control 169

5.5. RF Column Design 170

5.6. Decoder Synthesis APR design 172

5.7. Checker Circuits 177

5.8. Performance Overview 179

5.9. Implementation Summary 182

5.10. Summary 183

CHAPTER Page

6. CONCLUSION 184

REFERENCES 187

LIST OF TABLES

Table Page

2.i Design Metric Comparison of the Proposed Implementation to Standard Flip-Flop And Temporal 4CE FF Based Designs. 63

3.i: Dumbell (Large Fences), Interleaved Fences and Unhardened AES Design Metric Summary 72

3.ii. Radiation Testing Results and Nodal Separation Summary 91

3.iii HERMES2 (90 nm) [Farn16] Proton Beam Testing Results with the Errors Summarized by Unit/Operation, Error Cross-Section with Statistical Bounds are 93

4.i. Specification Comparison of DDR, DDR2 and DDR3 Memories 96

4.ii (a) DDR Clock Specifications and the Length of the Delay Line Required (B) Number Of Delay Lines and the Distance Between Individual Pulses Based on DDR2 And DDR3 Mode across Corners. 105

4.iii Fine Delay Unit Delay Statistics for an Interpolate By 8. Mean and Standard Deviation are Shown Extracted from Monte Carlo Simulations. 109

4.iv. ADPMDLL Performance Summary and Comparison with Previous Radiation Hardened DLLs. 159

5.i Comparison of Characterized and Simulated Delays for the Register File 180

LIST OF FIGURES

Figure Page

1.1. Cartoon Showing the Space Radiation Environment (Courtesy of NASA, www.meted.Ucar.Edu)... 2

1.2 Galactic Cosmic Radiation Dose Rate Variance with Latitude and Solar Cycle (Courtesy of NASA, www.meted.Ucar.Edu).. 4

1.3. (a) Ion Strike at the Output of a CMOS (Metal and Gate Connectivity not Shown). (b) Funnel Formation and Charge Collections Mechanisms in the Semiconductor Following an Ion Strike. 8

1.4. A Single Event Transient Manifesting on a Combinational Portion of a CMOS Circuit. Collection of Charge and the Change in the State of the Node Capacitance Cl and the Current Steering Mechanism as a Function of the Restoring PMOS after [Koba09]....... 10

1.5. A Single Event Upset Due to Radiation Strike on the Storage Node in a Latch, the Storage Feedback is Upset as the Two Node Reach the Stable Erroneous (10) State from the (01) State. 11

1.6. SET Cross Section with Scaling on Planar Technologies [Bene06], SET Pulse Width Increases as We Scale Due to the Reduction in the Nodal Capacitance and Operating Voltages.

1.7. Critical Charge Reduction Trend with Different Technology Nodes for the Intel Foundry Technology, after [Seif15]. 15

1.8. (a)[Seif15], (b)[Fang16], (c)[Oldi15] and (d)[Lee15] Planar and Finfet SER/SEUCross Section/Failure in Time Measurement from Different Technology Foundries with Enhanced SER Reduction over Planar Technologies. 16

Figure Page

1.9. Drain Depletion in a Finfet Technology Which is at a Distance of the Height of Subfin away from the Substrate, Reducing Charge Collection Efficiency. 17

1.10. SER Increase with Number of Fins, 0-1, 1-0 Transition with Low and High Parasitic Bipolar Transistor Gain (B) are Shown, after [Seif15]... 18

1.11. Onset of Charge Collection Amplification under Laser Irradiation with Increased Bipolar Gain Thereby Increase in SER at Lower Laser Energies is Shown, after [Seif15]. 19

1.12. (a) Cross Section and (b) Soft Error Rate as a Function of Clock Frequencies Measured in [Reed96] and [Seif12] Respectively. Increased Vulnerability with Increased Clock Frequency is Consistently Observed over Multiple Generations. 20

1.13. Triple Modular Redundancy (TMR) with Complete Triplication of Combinationa and Sequential Elements Ensuring Complete Mitigation with Minimal Timing Penalty, (b) Dual Modular Redundancy (DMR) Which Detects a Mismatch in the Copies to Set an Error Flag to Be Used by the Error Handler Ensuring Inhibition of Erroneous Signals and (c) Temporal Hardening Delaying Signals in Time to Ensure That the Set Gets Masked by Majority Voting. 22

1.14. (a) Multi-node Charge Collection Mitigation Cross Section Due to Nodal Separation by N-well, (b) MBU in FPGAS as Demonstrated in [Quin07] Leading to Dces and (c) CAD Methodology Based Separation of Multi-bit TMR Cells with Spacer Between Each Groups to Ensure That Even Non-equivalent Flops in Multiple Domains Cannot Be Upset with a Single Strike.. 24

Figure Page

1.15. Effective Cross Section Seen by an Ionizing Particle That Simultaneously Strikes Two Nodes a and B Causing Upset. Only a Limited Solid Angle Can Pass Through the Collection Region of Both Nodes, Providing a Straightforward Estimate of the Upset Probability, after [Sham14]. 26

1.16. A Method of CAD Based Critical Component Separation of CMOS Gates by Using Critical Spacing Rules (E.G. 5 Mm) Recursively, after [Klei10]. 28

1.17. Verification Based SEUEstimation and Selective Hardening in Synthesis Step, after [Sesh06]. 29

2.1. AES Engine Algorithm Showing 14 Rounds for a 256 Bit Key Design, Expand Key Stage Which Creates the Key for Each round to Be Added in Add round Key Step is Shown in the Dotted Circle. 34

2.2. AES Transformations, Substitute Bytes, Shift Rows and Mix Column Stages are Done on the Input Stage Matrix. Sbox is Shown in the Substitute Bytes Transformation. 37

2.3. Advanced Encryption Standard Architecture as Implemented. It is Pipelined over 15 Stages for High-speed Operation. Transformations by the Combinational Logic (Cl) are Shown in Boxes. 39

2.4 Schematic of Self-correcting Pulse-clocked Latches and Pulse Generators. Multiplexers Select Between Data and Test Mode Input, Majority Voting Internal Nodes (Maj_a, Maj_b and Maj_c) are Also Marked. 41

2.5 Statistical Analysis of the Pulse Latch and Pulse Generator Showing Worst-case Pulse Width for Proper Data Capture Mean and Sigma as Well as Pulse Generator Variation as Determined by Mc Simulation. 42

Figure Page

2.6 Color Coded Schematic (a) and Layout (b) of the 16-bit, TMR Pulse Latch Design with 3 Domains (A-blue, B-green and C-red) Highlighted. Latches and the Shared Pulse Generator are Shown. The Spatial Separation Incorporated Which Makes the Layout Dce Immune. 43

2.7 (a) Pulse-latch Operation with Nominal Pulse Width and Decision Window Timings (Tc2q and Td2q). Nominal Time Borrowing of 88 Ps is Afforded by the Design. (b) Self-correction in the TMR Latch is Shown with an Error in the C Copy, the Onset of the Negative Edge of the Clock Pulse Initiates Correction. Correction Window is a Function of the Slack Afforded in Path is Question and Varies Accordingly. 45

2.8 Non-redundant Mode Operation with Data Db and Dc Held at 1 and 0 Respectively with Open-control Set to Transparent. 46

2.9 RHBD CAD Module Level Separation Using Large Fences, Complete Separation of Custom, APR (Combinational and Clock) Portions is Achieved to Create a Dce Immune Design. 48

2.10 RHBD CAD Module Level Separation Using Large Fences, Complete Separation of Custom, APR (Combinational and Clock) Portions is Achieved to Create a Dce Immune Design. 49

2.11 Timing Waveforms of Self-correction in the Pulse-latch. C Copy is Corrected to 0 after 340.1 Ps. B Copy is Corrected to 1 after 202.8 Ps. 51

2.12 Timing Waveforms of Self-correction in the Pulse-latch. C Copy is Corrected to 0 after 340.1 Ps. B Copy is Corrected to 1 after 202.8 Ps. 52

Figure Page

2.13 (a) Schematic Representation of Separation Analysis, Analysis Histograms in (b) Ab, (c) Bc and (d) Ac of Cell Separation Comparison for the Design Pipeline Shows Very Few Pairs Placed Without Adequate Separation. 54

2.14 AES Implementation on a 4 by 4 Mm Die on a 90 Nm Process, the AES Design is Marked along with Other Structures in the Test Chip. Wire Bond I/O Pad Ring Consists of 211 I/O's 56

2.15 Error Injection Simulation Test Setup. Model and Device under Test are Shown. Error is Injected at the 8th Stage and Subsequent Stages are Observed for Error Propagation. Lfsr Generates the Inputs Data Bits and the Key is Constant. 57

2.16 (a) Non-redundant AES Error Injection Graphical Representation Using Perl. Reds are Incorrect 1's and Green are Incorrect 0's, Correct 1's are in Black and 0's in White. (b) Error Count per Pipeline Stage Plot Showing Correction Capability of TMR (Light Blue) Version and the Error Diffusion in Non-redundant Version (Black). 58

2.17 (a) Measured Test Chip Fmax Vs. Vdd at High Operating Voltages. The Upper Values are Measured Using the Psu Mode, (b) Measured Test Chip Fmax Vs. Vdd at Low Operating Voltages. 60

2.18. Broad Beam Testing Setup at Uc Davis. The Cob Dut is Shown at the Top. The Controlling Fpga is at the Bottom, away from the Beam Track. 61

3.1. Hermes2 Architecture Block Diagram of a 6-stage with the Speculative DMR Pipeline and the Architectural TMR Architectural States. DMR to TMR Crossovers Logic is Also Shown (Also Implemented in TMR) 67

Figure Page

3.2. (a) Large Fence Module Separation Diagram Representation (b) Interleaved Fence Diagram Representation with a, B and C Fences (c) Sequential and Combinational Domain Mismatch If the Fence and the TMR Site Definitions are not Aligned in the Interleaved Fences Creating Potential SE Vulnerabilities. 69

3.3. AES Implemented at 250 Mhz Speed in (a) Large Fence Module Separation with Key and Data Fence (b) Interleaved Fence Encounter Representation with Key and Data Mixed in the a, B and C TMR Domain Fences. Color Coding Pertaining to Key and Data a, B and C Domains is Shown. Both Designs are Implemented in the Same Area with the Same Flip-flops to Ensure Proper Apples to Apples Comparison 71

3.4. (a) ReAPR Flowchart with Steps to Create Domain Separated MNCC Mitigated Logic, Required Inputs and APR Steps (1-7) are Elucidated. Domain Separated RTL is Created by the Triplication Wrapper and Synthesized Verilog is the Output from Synthesis (b) Domains Provide MNCC Induced SE Mitigation. The Multi-bit FFs Straddle Domains so the Associated Storage is in the Same Domain as Combinational Logic. 75

3.5. ReAPR Flow Place and Route Steps Described in a Pseudo Code, with the Specific Domain Separation Related Steps and Subroutines Post RTL Integration and Synthesis.77

3.6. (a) Diagrammatic Representation of the TMR Verilog Creation with Physical Domain Matched to Logical Hierarchies (b) Pseudo Code for Creation of TMR Verilog by Triplication of Non-redundant Verilog. Output Verilog is Instantiated to Create Integrated RTL/Verilog Design. 78

Figure Page

3.7. (a) 4 (a) Site Definitions for Multi-height TMR Cells and Default Cells. (b).Guide Generation in the APR Environment, TMR and DMR Guides Can Be Seen Colored in Red (a), Blue (b) and Green (c). 80

3.8. (a) Guided Initial Placement, TMR Flip-flops are Placed in the Correct TMR Sites. TMR and DMR Combinational Logic is Placed Based on Data Flow and Timing, but Not Domain Separated, (b) TMR Flip-flops are Fixed and the Guides are Converted to Fences Before the Fenced Placement Run Step (6). 82

3.9. Complete Domain Separated Physical Placement Snapshot. The Zoomed Image Has the Color Coded a B and C Domains Placed Within 4 Cell Heights Tall Fenced Regions. DMR Placement Surround the TMR Placement in Fences Akin to the Large Fences of Chapter 2. Integrated Fences Thus Allows Placement of Redundant Logic with the Best Possible Ppa. 83

3.10. Tc25 Top Level Floorplan Diagram with Different Power Domains That Exist in the Chip. The Design Constituents with Their Approximate Placement Location with Respect to the Chip Origin is Shown. Other Design Constituents in the Chip are Sram Arrays for Process Variation Study. 85

3.11. (a) Large Fence Module Separation Diagram Representation (b) Interleaved Fence Diagram Representation with a, B and C Fences (c) Sequential and Combinational Domain Mismatch If the Fence and the TMR Site Definitions are not Aligned in the Interleaved Fences Creating Potential SE Vulnerabilities. 86

Figure Page

3.12. Spatial Separation Analysis Schematic View, a, B and C Paths to the Redundant Flip-flops are Queried and Their Separation is Analyzed for Cells Spacing Less than 4 Standard Cell Heights (6.48 Um). This is Repeated for All of the Design Flip-flops. 88

3.13. (a) Cumulative Probability of the Spatial Separation Analysis Showing 99.86 % Cells Protected from MNCC Upsets up to a Span of ~ 3um. (b) Ab, Bc and Ac Comparison Cumulative Probabilities with the Ac and Bc Cell Adjacencies Higher than the Ab Adjacencies Due to the Size and the Form-factors of the Designed Fences. 89

3.14. 90 Nm Implementation of Hermes2 [Farn16], TMR and DMR Regions are Highlighted, the Base Version of the Interleaved Serpentine Flow is Used to Implement the Design. The Design Was Tested Using Proton Radiation at Uc Davis 63 Mev Cyclotron Beam. 92

4.1. Top Level Architecture of the Radiation Hardened All-digital Dll Implementation. Three Clocks are Generated and Voted out to Create the Soft-error Free Clock Which Clocks the Data in the Dram Capture Path (Dq).. 98

4.2. ADPMDLL Architecture Showing the Digital Delay Line Consisting of Coarse and Fine Delay Units (Cdu and Fdu). A Bang-bang Phase Detector and Tdc are Used to Calculate Phase Difference in Locking and Tracking Mode, Respectively. Control Unit Constituents are Also Shown. 101

4.3. ADPMDLL Coarse Delay Unit is Shown, Propagating and Injecting Path are Highlighted in Blue and Green, Respectively. Dummy Loads Ensure Matched Slews Across the Coarse Delay and Fine Delay Chain. 103

Figure Page

4.4. Pulse Width Sizing Requirements and Critical Timing Relationships for Ensuring That Fidelity of the Multiplied Clock is Maintained. Pulse Injection and Amplification are Shown at Different Time Stamps. 104

4.5. Inverter Phase Interpolator by 8 Design. Interpolation of Edges Derived from Coarse Delay Unit. Four Such Units are Stacked to Create a 32 Bit Fine Delay Unit. 107

4.6 Inverter Phase Interpolator by 8 Design. Interpolation of Edges Derived from Coarse Delay Unit. Four Such Units are Stacked to Create a 32 Bit Fine Delay Unit. 108

4.7 Fine Delay Unit Simulation Waveforms, Interpolated Fine Edges are Zoomed and Shown on the Right, the Values are Derived from the Coarse Delay Unit Delay. 111

4.8 ADPMDLL Top Level Decoding Architecture Shows the Minimized Area Footprint Decoders (8 in Number) That are Implemented for Controlling the Delay Line Width. 112

4.9 DDR Modes of Operation and the Decoder Activity, DDR2, DDR3 and Locking Mode Shown, Idle Decoders in Low Power Mode Shown in Grey. 113

4.10 Decoding Logic Schematic Overview, Individual Decoders and the or Logic Which Enables Selection Between Decoders is Shown. 114

4.11 General 0th Order Type 1 Dll Which Only Has Feed-forward Clock Path Z-domain Block Diagram. 115

4.12 Waveform and Definitions of Cycle-to-cycle Jitter (a) and Period Jitter (b) after [Jede03]. 116

4.13 Control Logic Overview, Constituents of the Control Logic are Shown Here, Colored Portions Indicate APRed Logic and White Background Indicates the Custom Logic. 117

Figure Page

4.14 ADPMDLL Acquisition and Tracking Algorithm Flowchart, Algorithm Shows the Binary Search Acquisition and Step Tracking Using Fine Delay and Arithmetic Approximation. 119

4.15 Successive Approximation Algorithm Tracking a Value of 175 with Initial Seed of 128. Binary Values Used in the Control Logic Sar is Shown in the Shaded Regions. Red and Green Coloring Signifies Phase Frequency Detection Output. 120

4.16 Modified Bang-bang Phase Detector Design Schematic, It Measures the Difference Between the Reference Clock and the Pulsed Clock and Creates a 2 Bit {up,Dn} Signal Processed by Sar Unit. An Asynchronous (Active Low) Reset is Used to Ensure Known State Before the Comparison Begins. 122

4.17 Bang-bang Phase Detector Design Schematic, It Measures the Difference Between the Reference Clock and the Pulsed Clock and Creates a 2 Bit {up,Dn} Signal Processed by Sar Unit. An Asynchronous (Active Low) Reset is Used to Ensure Known State Before the Comparison Begins. Table Inset Shows the Minimum Resolvable Phase Difference. 123

4.18 Time to Digital Converter Design Which Processes 32 Bit Edge Data and Produces a 5 Bit Code That Represents the Phase Error with a Granularity of 6ps. Values Representing Lad and Lead are Shown with the Associated Waveforms. The Centering Delay Ensures That Center Value (16) Corresponds to 0 Ps Phase Error. 124

4.19 Differential Non-linearity for the Fdu Across Corners, Even at the Worst Case the Dnl is Less Than .35lsb. 126

Figure Page

4.20 Arithmetic Multiplied Code Creation for High Frequency Clock Injection, 1/8-7/8th of the Locked Values with the 2-1, 2-2 and 2-3bit Position Values Calculated and Maintained with Shift and Add Arithmetic to Allow Locking Resolution of ~6.25 Ps, Can Be Further Improved with Increasing Bit Positions and Accumulating the Values for Increased Power. 127

4.21 Color Coded ADPMDLL Top Level Diagram Which is the Reference for Waveform Definition of Working of the ADPMDLL in Fig. 21 128

4.22 Color Coded ADPMDLL Top Level Functional Waveforms, Color Corresponds to the Unit Which is Causal to the Signal. 130

4.23 100 Mhz Clock Locked with Initial Single Pulses and with 8 Pulses Post Locking. The Locked Code Value (Addr) is 195 and the Divided Values are Shown for Pulse Injection. 131

4.24 133 Mhz Clock with Single Injected Locked Pulse and Post Locking 8 Pulses Locked by Linear Interpolation with the Code Values and Interpolated Values Circled in Red. 8 Pulses Locked per Reference Clock. Locked Value is 147. 132

4.25 266 Mhz Clock Locked with 8 Pulses, Single Pulse Injected and Locked Circled in Red and the 8 Pulses Injected and Locked Circled in Green. The Locked Value is 71, Rest of the Interpolated Values are Circled in Red. 133

4.26 Coarse Delay 1 Sigma Variation Bound for One Coarse Delay Unit. A Maximum Variation of 19.68 Ps Can Be Accumulated Due to Coarse Delay Random Variation. . 135

4.27 Gaussian Noise Mismatch Analysis Summary for the ADPMDLL, Mean and Sigma of the Corresponding Units are Shown, Only Units Which are in Critical Path and Hence

Figure Page

Contributing to Phase Error/Jitter Specifications are Shown. Green and Red Arrows Indicate the Fast and Slow Paths Contributing to the Variation Leading to Phase Error in the High Frequency Clock. 136

4.28 ADPMDLL Critical Path and Critical Path Timing Diagram Highlighted in Red, the Fastest Pulse Injection (or the Smallest Delay) That Can Meet Timing is the Requirement for the Successful Frequency Multiplication or Pulse Injection in the DDR3 Mode. The Equivalent Path in DDR2 Mode is Shown in Orange and is Less Timing Critical than the DDR3 Path as Explained in Previous Sections.. 139

4.29 Spice (Ultrasim) Simulation Timing Waveforms for a 10ns Input Reference Clock Cycle. Locking is Completed in 32 Clock Cycles and the Pulses are Injected into the Loop Subsequently After. Tracking is Observed for 200 Cycles. Tdc Output Tracks the Phase Error and Eliminates Jitter It with Digital Correction as Described in the Earlier Sections. 140

4.30 Eye Diagrams Showing Peak-to-peak Jitter for TT, FF and SS (Clockwise) Corner Simulations. P2p Jitter is below the Required Limit for DDR2 Transfer as per the Jedec Specs. The Black Line Indicates the Ideal Reference Clock Eye Diagram. The Falling Waveforms with Disparate Waveform Indicates the Across Corner Pulse Amplification/Attenuation Behavior Where the Pulse Width Constraint is Still Met.... 142

4.31 Noise PeRFormance of the Apdmdll in Presence of a 500k 100ps P2p Noise Variation of Input Reference Clock. The Pulsed Clock and its Average is Shown in the Yellow and Black Respectively. Binary Search Algorithm for ADPMDLL Locking in Presence of Input Jitter is Also Shown.. 143

Figure Page

4.32 Power Measurement Waveforms of the Apdmdll, Locking/Idle Mode Power and Multiplication Mode are Both Shown, as Expected Much Higher Activity is Observed While Producing DDR3 Standard Multiplied Clock. 145

4.33 Simulation Waveforms of Soft Error Vulnerability in the Proposed ADPMDLL Design. Sar Unit is Upset with a 400 Ps Set Which is Captured by the Sequential Units and Results in Missed Acquisition and Merged Pulses. 147

4.34 Block Level Schematic of the Test Structure Taped-out for the Purpose of Delay Variability and Fine-delay Non-linearity. The Delay Unit is Different from the Unit Described in This Work, the Implemented Design in Test-chip (Tc25) Was not a Pulsed Design, the Components However Were Shared. 149

4.35 Block Level Schematic of the Test Structure Taped-out for the Purpose of Delay Variability and Fine-delay Non-linearity. The Delay Unit is Different from the Unit Described in This Work, the Implemented Design in Test-chip (Tc25) Was not a Pulsed Design, the Fine Delay Unit Components However Were Identical. 150

4.36 Tc25 Test-chip Snapshot Showing the Ddl Test-structure in Red. The Test-structure is Fabricated Inside a 4 by 4 mm Die with Wire-bond Packaging. 151

4.37 Tc 25 Dll Test Structure for Coarse and Fine Delay Unit for Delay and Non-linearity Testing. The Single Slice Which are Triplicated are Shown in the Zoomed Figure. 152

4.38 Tc 25 Test-setup. The Fpga Board and the Custom Test-board are Shown. The Test-chip Tc25 is Plugged in the Socket and the Power Supplies are Connected to the Test-chip as Shown. 153

Figure Page

4.39 Tc 23 Implemented Coarse and Fine Delay Structures, the Fine Delay Was Implemented as by 4 Interpolate Instead of by 8 Interpolation as in This Chapter. 154

4.40 Tc 23 Fpga Testing Verilog Hierarchy Block Diagram to Capture Tdc Data out as a Result of Phase Shifts Applied Through Clock Manager Module Mmcm. 155

4.41 Code Distribution with Phase Shifts of 14.2 Ps Applied Every 140 Cycles........... 156

4.42 Code Distribution with Phase Shifts of 14.2 Ps Applied Every 74 Cycles............ 157

4.43 Measured Vs Simulated Delay of the Total Tdc Delay for the Two Experiments Shown in Fig4.41 and Fig. 4.42. Measured and Simulated Values Agree Closely and Only Vary at Low Voltages. 158

5.1. DMR RF Architectural Diagram with the a and B Copies and the Checking (WWL, Parity and Comparison) Logic to Detect the Erroneous Pipeline Before Commitment to Architectural State, after [Clar11].. 162

5.2. DMR RF Implementation Hierarchy, Wordline Checker is Implemented in the Registerfile Hierarchy Rfregisterfiledd and the Write Checker Circuits are Implemented in the Rferror Hierarchy to Be Implemented in a Separate Physical Block. 164

5.3. (a)Register File Cell Design, Single Copy of the DMR Cell with 2 Redundant Transistors for Dual Word-line Access, Multiple Ports are Shown, (b) Layout of the Cell in a 3,42 by 1.62 Um Area. 165

5.4. (a)Register File Bit-cell Design, Metal and Active Layer Usage and Layout are Shown by Layer in (a) Poly and Diffusion, (b) M1 and M2 (c) M2 and M3. High Density Layout for the Multi-ports Incorporated in the Cell are Shown.. 166

Figure Page

5.5. Register-file Write Stability Analysis, the N-well Voltage is Varied to Make the PMOS Weaker Increasing the Write Margin. The Table Inset Shows the Simulated Values Summary Across Corners. 167

5.6. (a) Standard Cell Rail and Well (P and N) Continuity Shown in the Interface Cell (b) RF Tap Cell Spacing and Special Keep-out to Alleviate High Voltage Spacing Drc to the Secondary Power Rails for P and N Well Biasing.. 168

5.7. RF Columns with the Rw Circuit Size and Physical Arrangement. All Dimensions are Shown in Micrometers.. 169

5.8. Write and Read Circuits for the RF Columns, Rbl0, Rbl1 and Rbl2 are Read out Statically, with CMOS Gates as Shown in the Schematics, with Rbl0 Connected to the Bit Storage Value of the Cell While the Rbl1 and Rbl2 are Connected to Bitn Storage Value, Resulting in Different Readout Value (1 and 0) Respectively. 171

5.9 (a). DMR RF Decoder APR Flow, Pin and Blockage Assignment is Done in the Perl Module Which Inputs the Locations of the Specific Pins for the Decoder That Drives the Specific Port and Creates Blockages for the Rest of the Pass-through (b) RF Decoder Arrangement That is Used to Create the Automatic Pin, Blockage, Power, and Secondary Pg (Well Biases) for the APRed Decoders (Tap and Interface Cells are Shown). 173

5.10 APRed Rwl0, Rwl1, Rwl2, WWLa or WWLb Decoder Automatic Pin, Blockage, Power (M4), and Secondary Pg (Well Biases on M2) Assignment. Pins and Blockages are Both Created on M4 Based on the Inputs Provided to the Perl Module Which Creates a Def File for Use in Defin Flow. 174

Figure Page

5.11 Decoder Arrangement (a) and Metal 4 Continuity (b) for Abutment with Columns, Decoder a Has the WWLa Version of the Write Decoder and Decoder B (Rfb) Has the WWLb Version of the Write Decoder, the Read Decoders are Identical. 175

5.12 Checker Circuit Hierarchy in Schematic for Write and Wl Checkers. Wl and Write Checkers are 32 and 40 Bit Each. 176

5.13 Checker Circuits Physical Layout, Wl Checker (b) is Horizontal and Write Chercker (a) is Vertical with Respect to the Standard Cell Row Placement (Standard Cells Rows are Horizontal). 177

5.14 Checker Circuits Physical Layout, Wl Checker (b) is Horizontal and Write Chercker (a) is Vertical with Respect to the Standard Cell Row Placement (Standard Cells Rows are Horizontal). 179

5.15 RF Critical Path Timing Path, Showing Address in to Data out Timing in Red. ... 180

5.16 RF Critical Path Timing Path, Showing Address in to Data out Timing in Red. ... 181

5.17 Physical Arrangement of the Dual Redundant Arrays and Word Line Checkers in the 55 nm Implemented Test Chip Tc 25. 182

CHAPTER 1. INTRODUCTION

1.1. Introduction

Integrated circuits (ICs) have increased the processing capacity and speed of electronics in the past few decades, based on Moore's law [Moor65]. Application specific ICs (ASIC) on silicon substrates allow millions of logic gates to be integrated for varying applications such as data processing, data encryption, off–chip data transfer, etc. These ICs can be susceptible to radiation particle induced malfunctions or errors. Historically, lead based isotopes in solder bumps of flip-chip packaging, lead frame alloys and interconnect metallization were initial sources of alpha particles which caused memory transient failures in terrestrial environments [May79]. Such errors could be corrected by rebooting the memory element and therefore are characterized as soft-errors, as opposed to hard errors which manifest due to physical irregularities in the circuit fabrication leading to permanent defects.

While packaging induced soft errors have largely been eliminated in modern ICs, electronic systems operating in radiation environments (e.g. space, nuclear reactors, particle accelerators) are exposed to a host of particles such as heavy ions, protons and neutrons. These particles cause electron hole pair generation in sensitive diffusion regions in complementary metal oxide semiconductor (CMOS) ICs resulting in radiation particle strikes, categorized as single event effects (SEE). SEEs have been identified as the primary failure mechanism in spacecraft malfunctions [Koga93, Ecof94, Sore00, Prit02]. The study, analysis and mitigation of these effects is broadly classified as radiation hardening. Even biomedical, automotive and banking applications [Nara06], which require highly

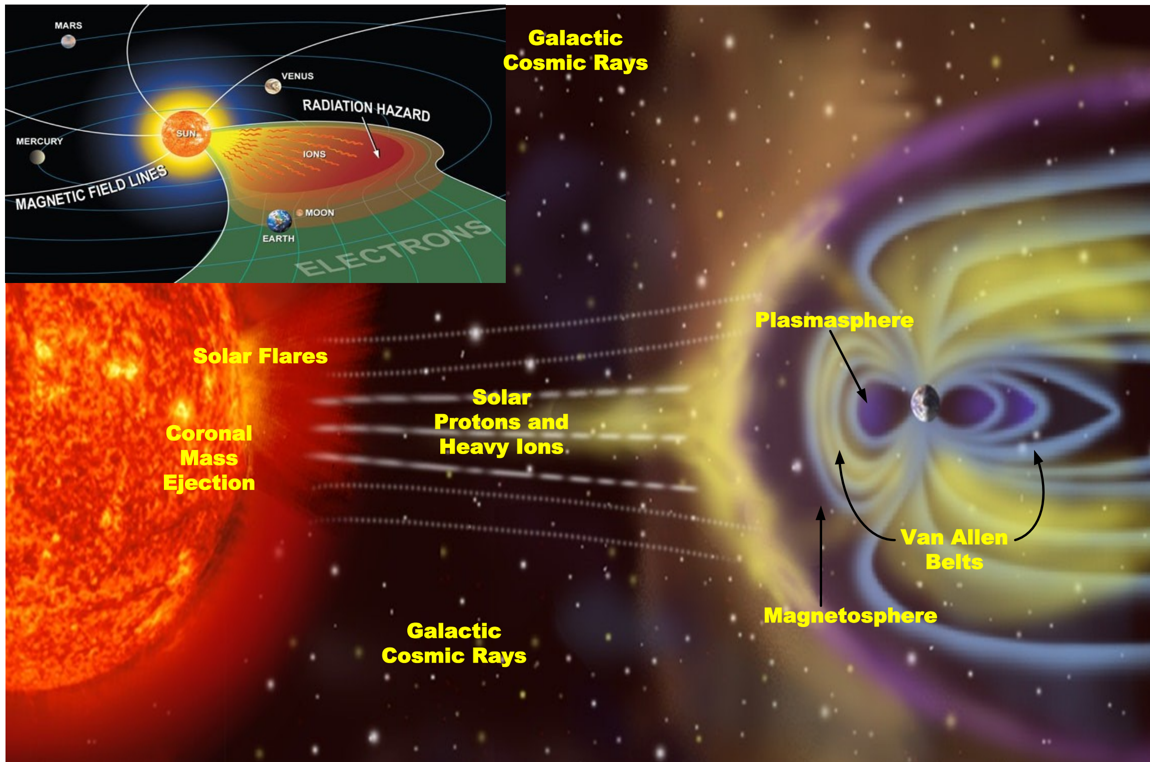


Fig 1.1. Cartoon showing the space radiation environment (courtesy of NASA, www.meted.ucar.edu).

reliable systems also rely on radiation hardening for critical applications. This chapter describes the radiation sources, the resulting effects on CMOS devices and mitigation strategies that are employed to counter radiation induced soft-errors. Following these definitions the motivation for this dissertation is explained.

1.2. Space Weather and Radiation Environment

Space weather, as described by the space weather prediction center, is the "variable condition in the sun and the neighboring space environment". This weather creates the radiation profile that Earth experiences. Figure 1.1 shows the interplanetary space environment with the Van Allen belts and the solar weather that is encountered by the planet Earth.

The typical astrophysical phenomena and resulting radiation particle spectra experienced are:

1. Protons and heavy nuclei ions associated with solar flares and coronal mass ejections (CME)

2. Galactic cosmic rays originating as a result of astrophysical phenomena such as supernova explosions

3. Trapped radiation due to Earth's Val Allen belts

4. Neutrons (Comic-ray albedo neutrons or CRAN particles)

5. Photons (γ-rays, X-rays, ultraviolet, extreme ultraviolet, optical, infra-red and radio waves)

The solar contributions to the space weather consist of solar winds, solar flares and coronal mass ejections. Solar winds are made up of ionized particles and can be visualized as a gas continuously flowing from the sun at 300 to 600 km/s (Fig. 1.1). Generally, solar winds do not cause major impact on Earth, but the particle stream can be enhanced and accelerated when more violent emission events such as flares and CMEs occur. The solar cycle is an approximate 11 year cycle marked by an increase and decrease in the number of sunspots, which are dark, cooler areas where a strong magnetic field consequently inhibits plasma from the sun's interior from interacting with the hotter surface plasma. The activity level of the sun varies from a quiet state with few sunspots, called solar minimum, to a more active state with many sunspots, called solar maximum. The likelihood of violent solar events becomes more significant closer to the solar maximum. Solar flares are the primary cause of sudden variation in brightness across the electromagnetic spectrum. These events accelerate electrons and protons traveling to Earth.

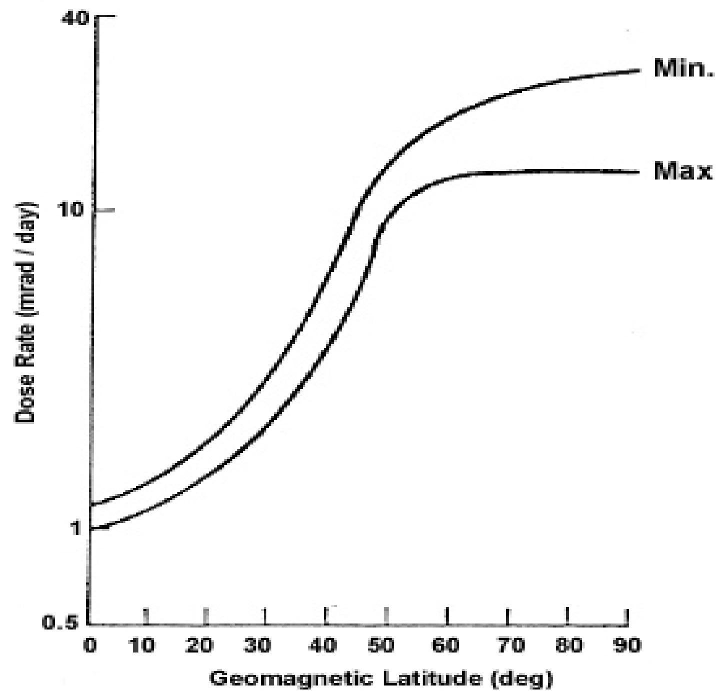


Fig 1.2 Galactic cosmic radiation dose rate variance with latitude and solar cycle (courtesy of NASA, www.meted.ucar.edu).

Radiation effects in low and medium Earth orbits that pass through the Van Allen belts consist of 93% protons, 6% alpha particles, and about 1% heavy nuclei [Stass88]. The Van Allen belts can be described as a toroid of particles trapped by the Earth's magnetic field and consist of a low altitude "inner belt" from 100~6000 km with high energy (tens of MeV/nucleon) protons and electrons; and a high altitude "outer belt" of up to 60,000 km with mostly high energy (1-10MeV/nucleon) electrons [Guss96].

Coronal Mass Ejection is a large burst of coronal material or magnetized plasma ejected away from the sun. The plasma can travel at speeds up to 2000 km/s under extreme circumstances. The material can travel in the direction of Earth where it will interact with Earth's atmosphere and magnetic field.

Earth and its atmosphere are also subjected to galactic cosmic rays (GCRs). This "background" radiation contains mainly protons, electrons, and atomic particles (from all elements of the periodic table) that originate far away in the galaxy. In the absence of significant solar events, cosmic ray intensities increase across the Earth's atmosphere. GCR intensity is modulated by the 11-year solar cycle [Barth03]. GCRs are comprised of 87% protons, 12% helium, with the remainder composed of heavy ions through actinides [Fred96]. Figure 1.2 plots the GCR dosage variation with geometric latitude and solar cycles. Minimum solar activity and greater latitude results in maximum GCR dose.

CRAN particles are secondary cosmic ray neutrons produced by the interaction of GCR with the Earth's atmosphere at about 55km above the planet surface. These particles have a half-life of ~11.7 minutes beyond which they decay into an electron, a proton and an anti-neutrino. Secondary neutrons are the most important contributor to radiation effects on CMOS at altitudes below 60,000 feet [Hazu00].

1.3. Radiation Effects on CMOS devices

Radiation can cause degradation [Denn69], malfunction or damage of CMOS devices and consequently electronic systems [Kern88]. The exact mechanism of such a malfunction is dependent on the type, mass, kinetic energy, charge of the impinging particle, mass, atomic number and density of the target material. When an ion strikes a CMOS device, it loses energy as it passes through the device due to the columbic interaction with the electrons of the silicon lattice, leading to ionization in the particle's track. The particle can also directly strike the nucleus of a silicon atom and lead to direct ionization, however, the probability of such an interaction is very low.

The distance the particle travels inside the silicon lattice is dependent on the "stopping capacity" of the material. This distance is a function of the impinging particle's mass, energy and the density of silicon. Linear energy transfer (LET) refers to the energy loss of the particle per unit length in silicon. LET has units of MeV-cm^2/mg and is given by the equation (1),

$$LET = \frac{1}{\rho}\frac{de}{dx}\ (MeV - {cm^2}/{mg}) \qquad (1)$$

Here $\frac{de}{dx}$ is the energy loss per unit length and ρ is the density of the material in mg/cm^3. The maximum LET value is usually referred to as the Bragg peak and signifies the maximum energy transferred right before the particle comes to rest [Hseih81].

Radiation particle strikes result in two charge deposition mechanisms in materials: direct and indirect ionization. In direct ionization, the electrons of the silicon nucleus are struck by the impinging particle and freed from the silicon bonds, thereby creating a dense track of charge. Indirect ionization results from the impinging particle dislocating the nucleus from its lattice structure. The charged nucleus then creates a track of charge, creating electron-hole pairs along its trajectory.

The two major radiation effects on CMOS devices and systems are single event effects (SEEs) [Mavis02] and total ionizing dose (TID) effects [Barn06]. TID is a non-destructive phenomenon of radiation induced variations in the threshold voltage under sustained ionizing exposure. This variation changes the performance of the CMOS device due to increased leakage and lower noise performance. This work is focused on mitigating errors arising out of single events and hence TID will not be discussed further.

1.4. Single Event Effects

Single event effects as the name suggests is the response of the CMOS circuit to a single radiation particle strike. As a result of charge deposition in the sensitive area of the circuit as shown in Fig. 1.3(a), electron-hole pairs can be collected by the diffusion node to change nodal voltage temporarily (SET) or permanently (an SEU in a memory element). As defined previously, the three main particles that cause single event upsets are heavy ions, protons and neutrons. Heavy ions primarily cause upsets through direct ionization whereas proton based upset mechanism is dominated by indirect ionization through proton-nuclei collision. Upsets due to neutrons are completely as a result of indirect ionization owing to their charge neutrality [Sagg05].

There are three stages of SEE formation: charge generation, charge collection and circuit response. Charge generation is decided by the particle's mass and energy and properties of the material it passes through. Charge is generated due to ionization (direct or indirect) generally within a few microns of the junction. In silicon, one electron-hole pair is produced for every 3.6 eV of energy lost by the incident radiation. Silicon has a density of 2328 mg/cm^3, therefore it is easy to calculate from equation (1) that an LET of 97 MeV-cm^2/mg corresponds to a charge deposition of 1 pC/um. Hence the amount of collected charge in silicon can be given by the formula

$$Q = 0.01036 * LET\ (pC / \mu m) \quad (2)$$

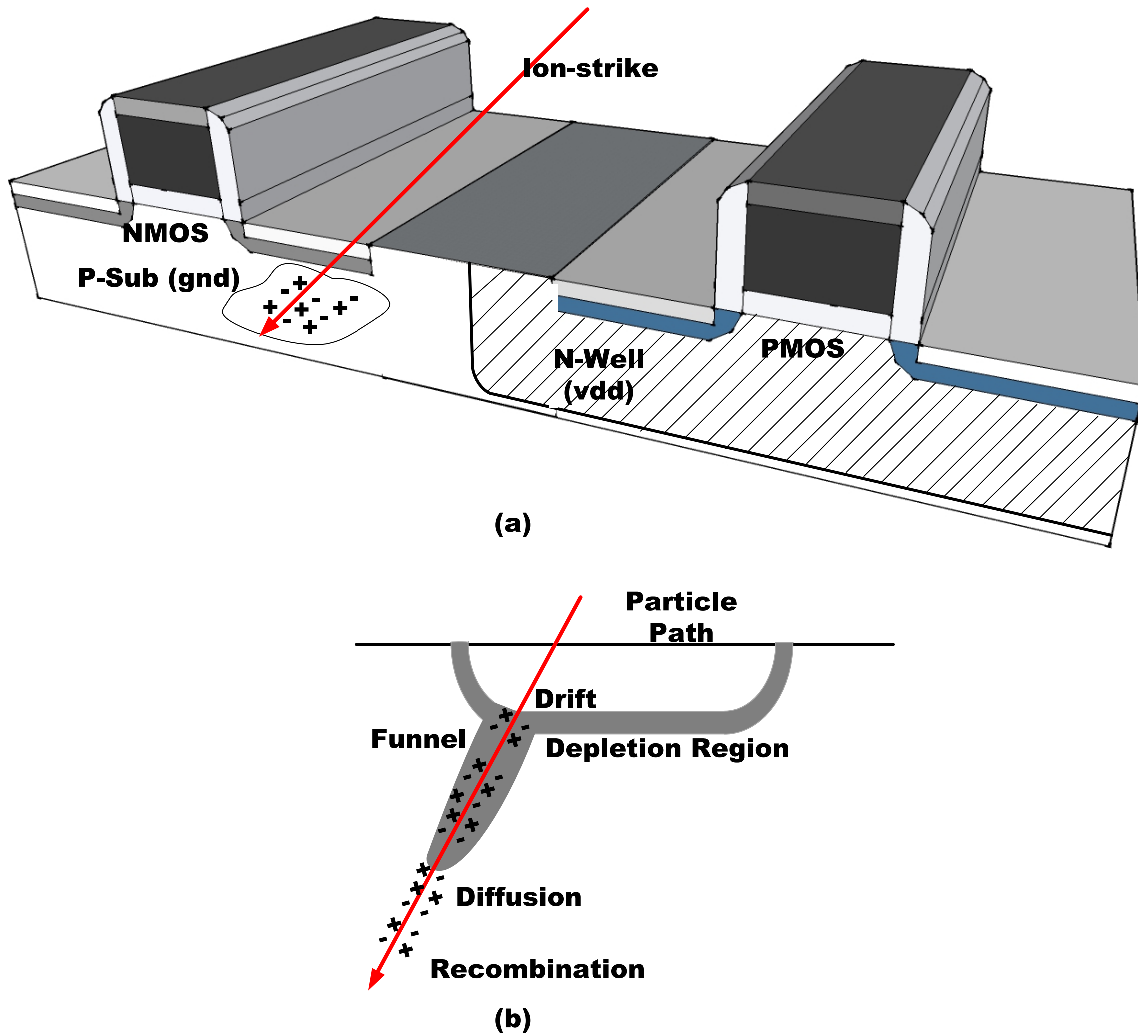


Fig 1.3. (a) Ion strike at the output of a CMOS (metal and gate connectivity not shown). (b) Funnel formation and charge collections mechanisms in the semiconductor following an ion strike.

Thus the collected charge Q for silicon substrate is in the range of 1-100 fC depending on the type of particle, its trajectory, and its energy over the path through or near the p-n junction. The most sensitive semiconductor device structure is the reverse-biased p-n junction. In a worst-case scenario, a p-n junction that is unbiased or floating is extremely sensitive to any charge collected from a radiation event. Circuits likely to have

this scenario include dynamic random access memories (DRAM), dynamic logic circuits, and analog designs like charge pumps. Since gate capacitance in ultra-deep submicron technologies is less than 2 fC/μm, nominally deposited charge can upset technologies with supply voltages less than 1 V. The charge deposited by impinging particles remains constant as gate capacitances are reduced due to scaling in modern technologies.

Three mechanisms that act on the charge created by an energetic particle strike are: 1) carriers can move by drift in response to applied or built-in fields in the device, 2) carriers can move by diffusion due to carrier concentration gradients or 3) carriers can be consumed by recombination through direct or indirect processes. These three mechanisms are not unique to radiation particle strikes and are in fact the governing processes of charge transport in semiconductors under normal operating conditions [Dodd03]. The most sensitive regions in CMOS devices are the reverse biased p-n junctions. A radiation particle strike on the reverse biased junction is illustrated in 1.3(b). Drift, diffusion and recombination processes governing charge collection and propagation are shown. A funneling mechanism results in the ion track distorting electric field lines, allowing collection by drift beyond depletion regions [Hsie81]. Compared to drift, diffusion is a less critical collection process since it is a slower process and spreads charge over multiple collection nodes over time. Nonetheless diffusion does cause upsets in certain scenarios [Sex91].

The characteristic that determines single event upset sensitivity of a device is its critical charge (Q_{crit}). This is the amount of charge that must be collected at the critical nodes of the device to cause the single event upset or soft error [Dod95].

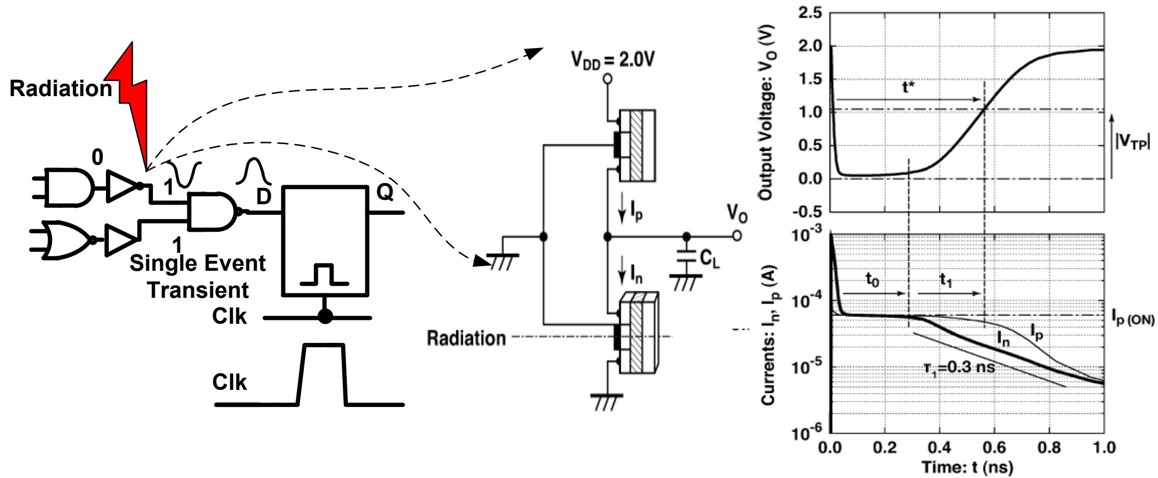


Fig 1.4. A single event transient manifesting on a combinational portion of a CMOS circuit. Collection of charge and the change in the state of the node capacitance CL and the current steering mechanism as a function of the restoring PMOS after [Koba09].

1.4.1. Single Event Transient (SET)

When ionizing radiation particles deposit charge on combinational logic rather than sequential or memory logic, the gate output diffusion node voltage may flip. The collected charge may charge or discharge the output node depending upon the charge polarity and location of the particle strike. Since the charge deposition happens in a period of picoseconds the circuit response takes much longer to remove the charge deposited, a momentary voltage spike is created [Heil89, Bene04, Gadl04].

An SET is a transient disturbance in the voltage and logic value of the node in question. The amplitude and width of such a transient is a function of the driving strength of the transistor which restores the circuit node voltage to the correct state and nodal capacitance of disturbed nodes. The transient may increase the voltage on the node beyond the switching point of a gate (typically VDD/2) thereby switching the gate output in response to erroneous transition as shown in Fig. 1.4. Propagation of the erroneous pulse

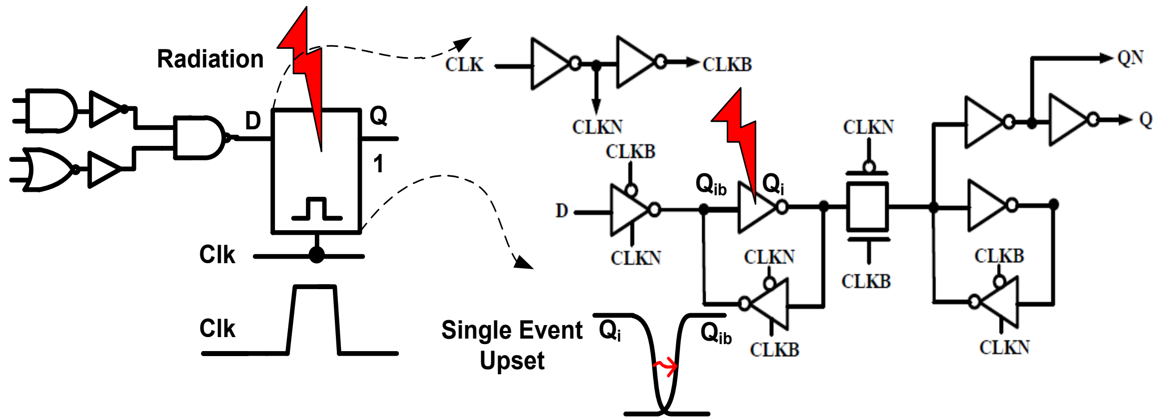


Fig 1.5. A single event upset due to radiation strike on the storage node in a latch, the storage feedback is upset as the two node reach the stable erroneous (10) state from the (01) state.

is based on sizing of gates downstream and in general the low pass nature of CMOS circuits tends to reduce the pulse widths and can in certain cases attenuate the pulse over multiple stages.

1.4.2. Single Event Upsets (SEU) or Soft-Errors

Single event upsets or soft-errors were observed in the late 70's in terrestrial DRAM's [May79] which were caused by alpha particles emitted by the IC packages. Since DRAMs have floating capacitive nodes which are highly susceptible to drift and diffusion mechanisms the charge state and hence node voltage and causes an upset or a soft-error. In static random access memories (SRAM) and other sequential elements (latches and flip-flops) the upset is caused primarily by aforementioned drift mechanisms and diffusion is less critical due to charge restoring paths which can neutralize the diffusion induced charge.

Fig. 1.5 shows a radiation particle strike on a flip-flop internal storage node leading to the flipping of the storage element (a back to back inverter). Voltage of storage nodes Qi and Qib are reversed since the transient on Qi results in a stable Qi=0 and Qib=1 due to

feedback action. This represents the upset due to the radiation event or an SEU [Sagg05]. SEUs can also be caused by travelling SETs that get latched by sequential elements during their sampling window. Once the machine state has been changed, it is impossible to distinguish an SEU from a particle strike on the sequential element and the one from an SET on combinational logic in the fan-in cone of the sequential element.

Single radiation particles can lead to single or multiple bit upsets (MBU) [Muss96] in CMOS circuits. MBU's are studied exhaustively in memory elements due to their highly dense arrayed structure. Multiple bits are placed in close proximity and based on the angle of incidence and the LET imparted by the particle 2, 3 and 4 bit upsets have been observed. MBUs are particularly significant in modern technologies as device dimensions and node capacitances decrease.

1.4.3. Soft-Error Cross Section Measurement

The metric used to calculate the soft-error vulnerability of IC's to proton, neutron and heavy ion radiation particle strikes is called *cross section*. This is the probability of a radiation particle to hit a given target and is given by

$$\sigma = \frac{Errors\ (\#)}{Fluence\ (\frac{particles}{cm^2})}, \tag{3}$$

where cross section is expressed in units of cm^2. This area therefore represents the apparent size of the target. Weibull distribution statistics can be used to analyze cross section data. The Weibull distribution has a threshold LET which signifies the onset of errors with increasing LET. The rate at which soft errors occur is called soft error rate (SER). The unit of measure commonly used with SER and other hard reliability mechanisms is failure in

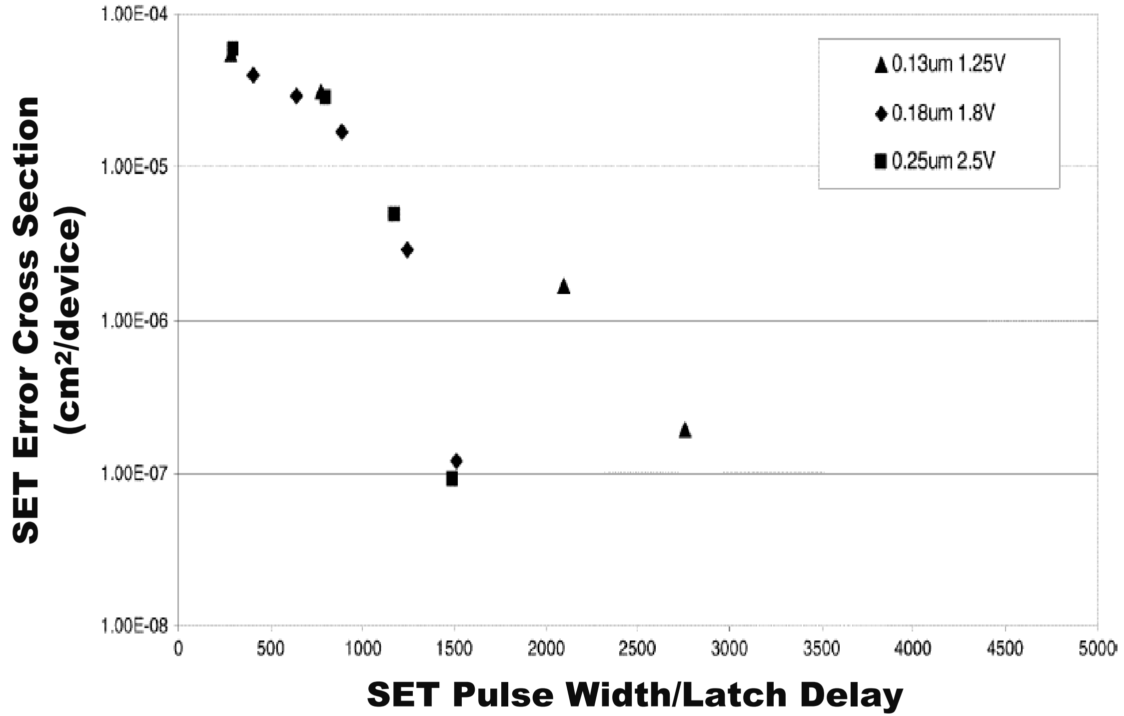


Fig 1.6. SET cross section with scaling on planar technologies [Bene06], SET pulse width increases as we scale due to the reduction in the nodal capacitance and operating voltages.

time (FIT). One FIT is equivalent to one failure in 10^9 device hours. Here, failure rate per hour is defined as the

$$\lambda = \frac{r}{EDH} = \frac{r}{D \times H \times Af}, \quad (4)$$

where EDH is equivalent device hours, D is the number of devices test and Af is the acceleration factor derived from Arrhenius equation [Elle12].

1.4.4. Other Single Event Effects

Another type of soft error occurs when the critical system control register bit is flipped, such as in field programmable gate arrays (FPGAs) or DRAM control circuitry, so that the error causes the product to malfunction. This type of soft error is called a single

event functional interrupt (SEFI) [Koga97]. SEFI leads to a direct product malfunction as opposed to typical memory soft errors that may or may not affect the final product operation depending on the algorithm, data sensitivity, etc.

Single event latch-up (SEL) is a steady high current state that results when a parasitic silicon controlled rectifier (SCR) (p-n-p-n) structure is triggered into a regenerative forward bias [Dodd03]. A circuit in latch-up will continue to malfunction until the IC is reset. If the latch-up current is large enough this can be a destructive in nature.

Other failure modes related to single events are the single event gate rupture (SEGR) and single event breakdown (SEB) [Dodd03]. Both mechanisms are destructive and lead to hard unrecoverable failures. Hard errors (as opposed to soft errors) are beyond the scope of this work and will not be discussed further.

1.5. Scaling and SER

With increase in clock speeds due to scaling, the probability of an SET being sampled to cause an upset in the machine state has also increased. This is due to typical transient pulse widths, which become comparable to clock frequencies. Fig. 1.6 shows experimentally collected SET Pulse width and cross section data on three generations of CMOS technologies. As the planar CMOS technology scaled, the current drive increased steadily and the width of the transistor reduced steadily by a factor of 0.7x. Reduced

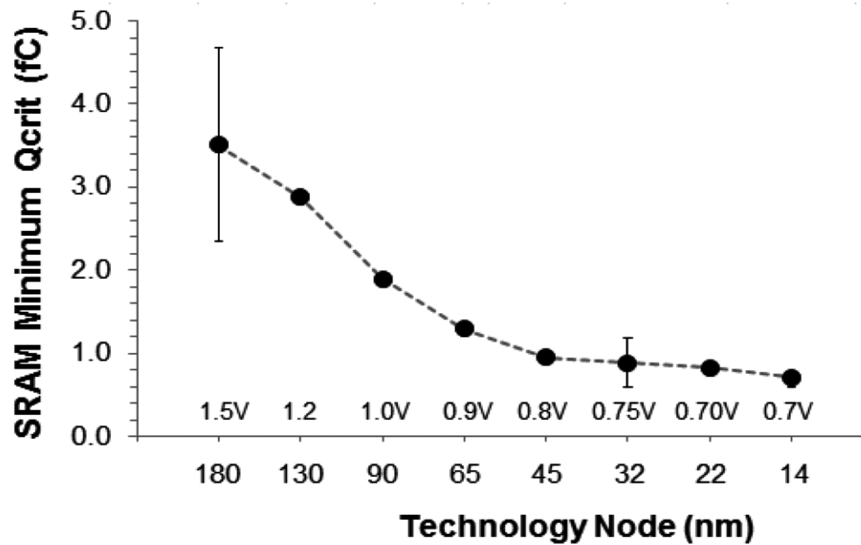


Fig 1.7. Critical charge reduction trend with different technology nodes for the Intel foundry technology, after [Seif15].

physical dimensions have a threefold effect: (1) A reduction in dimension leads to the reduced nodal capacitances, (2) a smaller physical area and (3) lower operating voltage which will reduce amount of circuit nodal charge. Critical charge Q_{crit} is reduced due to these effects and even though the charge injected from radiation on silicon remains invariant, soft errors are steadily declining due to the reduced collection efficiency in scaled planar technologies.

While planar transistors show a steady nominal reduction in the SER rate, finfet or trigate technology has shown a substantial reduction in the soft-error vulnerability trend. Fig. 1.7 shows the crucial SRAM charge Q_{crit} trend for Intel transistors across technology generations [Seif15]. Experimental data published from four major IC foundries (Intel,

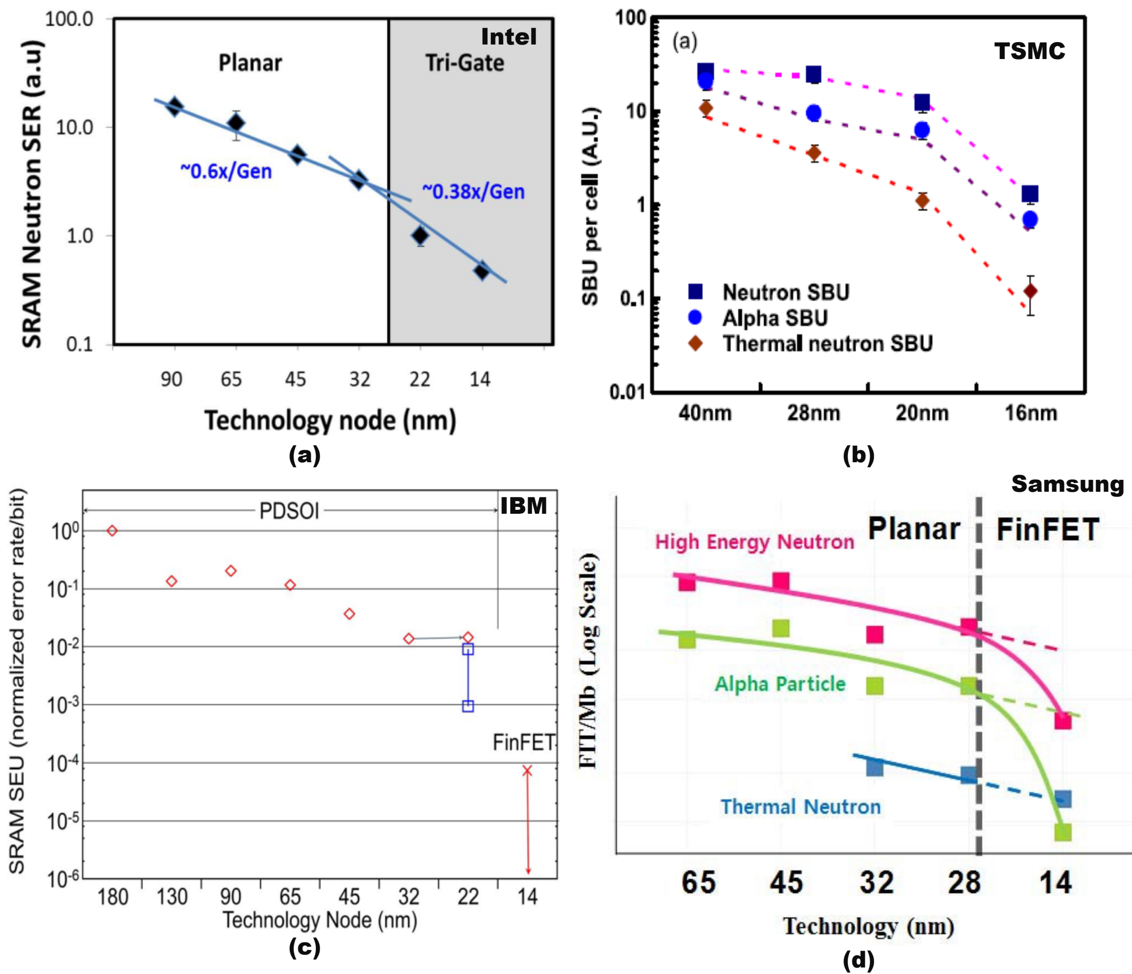


Fig 1.8. (a)[Seif15], (b)[Fang16], (c)[Oldi15] and (d)[Lee15] Planar and finfet SER/SEU cross section/Failure in time measurement from different technology foundries with enhanced SER reduction over planar technologies.

TSMC, Samsung and IBM) validate that the finfet as a structure is generally more robust for SER than the planar technologies.

The soft error rates are also improved in case of IBM's fully and partially depleted silicon on insulator (SOI) transistors. This is due to the increase threshold LET and reduced

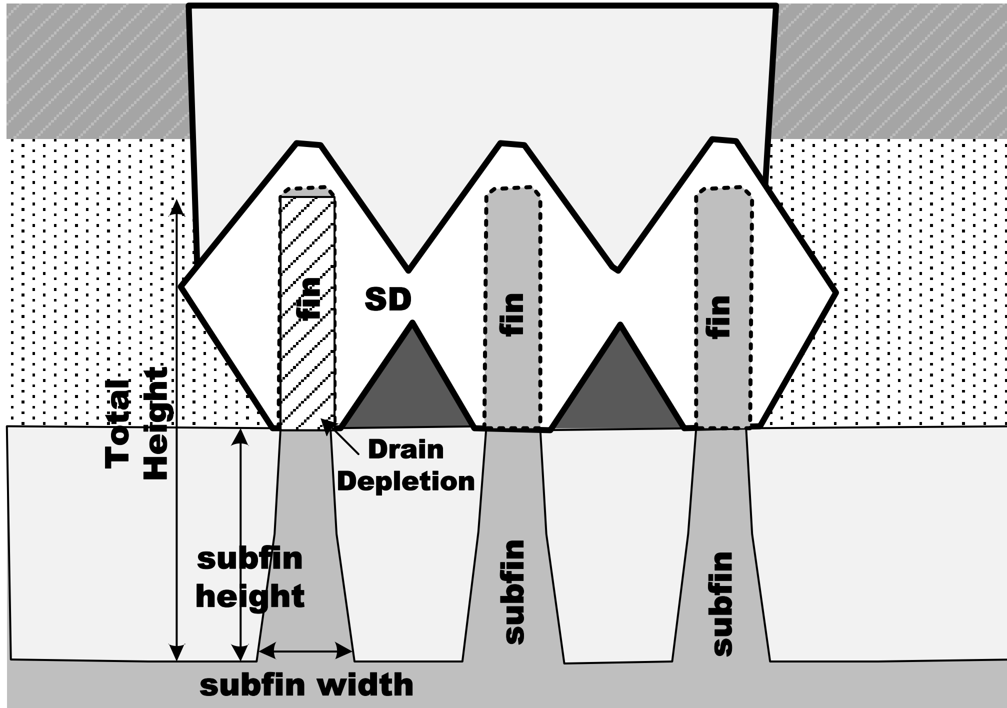


Fig 1.9. Drain depletion in a finfet technology which is at a distance of the height of subfin away from the substrate, reducing charge collection efficiency.

collection efficiency in finfet structures [Mamo11, Fang11, Noh15]. Figure 1.8 shows finfet soft-error vulnerabilities of the four major foundries mentioned above based on respective research publications which proves the reduction of SER beyond the range predicted by scalar bulk transistors. A simplified insight into the factors effecting soft-error rates is given by equation 4:

$$SER \sim A_{diff} \times exp\left(-\frac{Q_{crit}}{Q_{coll}}\right) \quad (4)$$

The critical charge (Q_{crit}) trend for Intel technology over the past few generations is shown in Fig. 1.7. Older technologies had a 30 % reduction over prior generations in the critical charge, while the newer finfet technologies have a 15 % reduction. Q_{coll} is the charge collection due to the radiation event and can only be estimated using TCAD

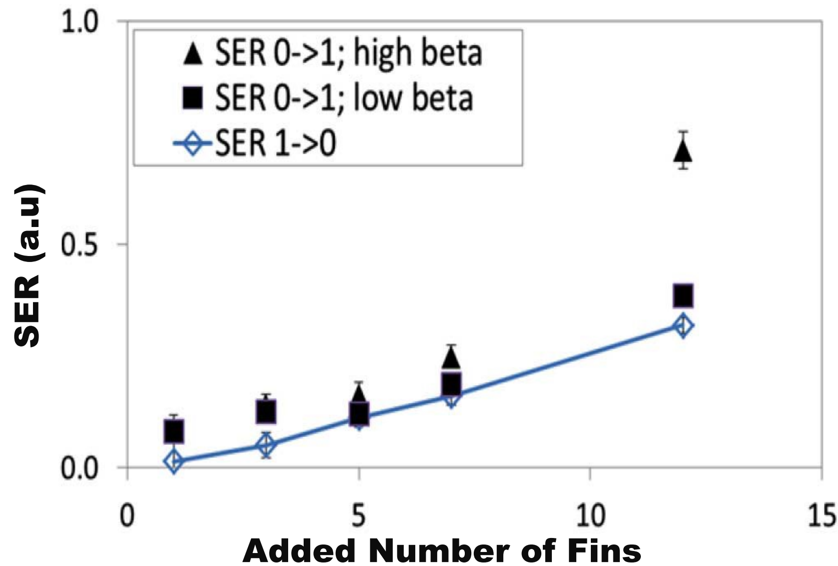


Fig 1.10. SER increase with number of fins, 0-1, 1-0 transition with low and high parasitic bipolar transistor gain (β) are shown, after [Seif15].

simulations and by analyzing measured data. Q_{coll} is a strong function of the doping profiles and the architecture of the MOSFET (planar, SOI, or finfet).

Based on results published by major foundries, the collection efficiency is reduced in finfet devices since it is a function of a) fin footprint, which equals the product of subfin width and the fin length, b) subfin height and c) subfin doping. The dependency of efficiency on fin footprint is almost linear and exponential to the distance of the drain depletion edge to the substrate (Fig. 1.9).

It is important to remember that the scaling beyond 90 nm was not based on classical dimensional scaling (Dennard scaling) but rather due to technology improvements like high-k gates, strained silicon, metal gate and finfet architectures. These improvements

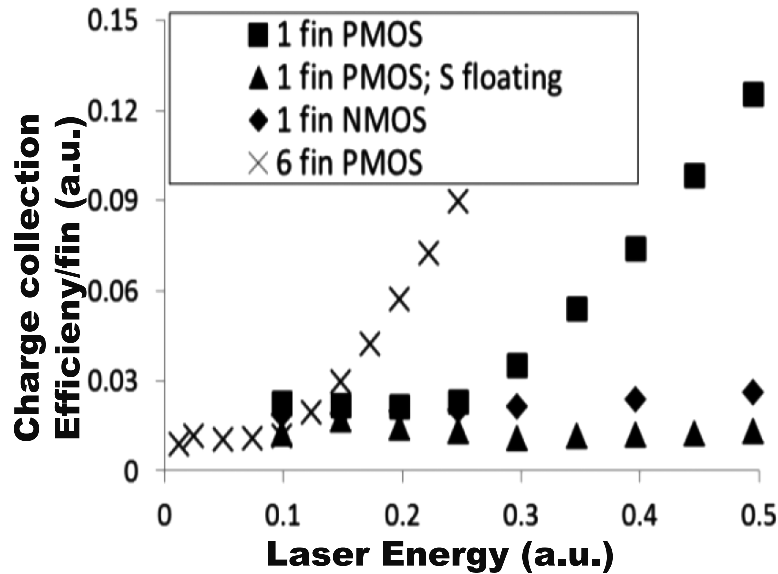


Fig 1.11. Onset of charge collection amplification under laser irradiation with increased bipolar gain thereby increase in SER at lower laser energies is shown, after [Seif15].

have increased the current drive while arresting the reduction of Q_{crit}, hence reducing the SER.

Another effect that has appeared in scaled finfet technologies is the charge amplification due to parasitic bipolar P-N-P device formation in off-state PMOS connected to storage nodes as demonstrated in [Seif15]. This effect is a dependent on the β of the said parasitic device and increases linearly with the number of fins that form the storage nodes. This increase is shown in Fig. 1.10, where the increase in the SER in different latches with storage nodes made up of increasing number of fins is plotted. At higher β values and higher LETs, the charge collection efficiency also increases non-linearly for devices with high number of fins as illustrated in Fig. 1.11.

With increased scaling, clock frequencies continue to scale and hence the probability of capture and sample of single event effects also increases irrespective of the

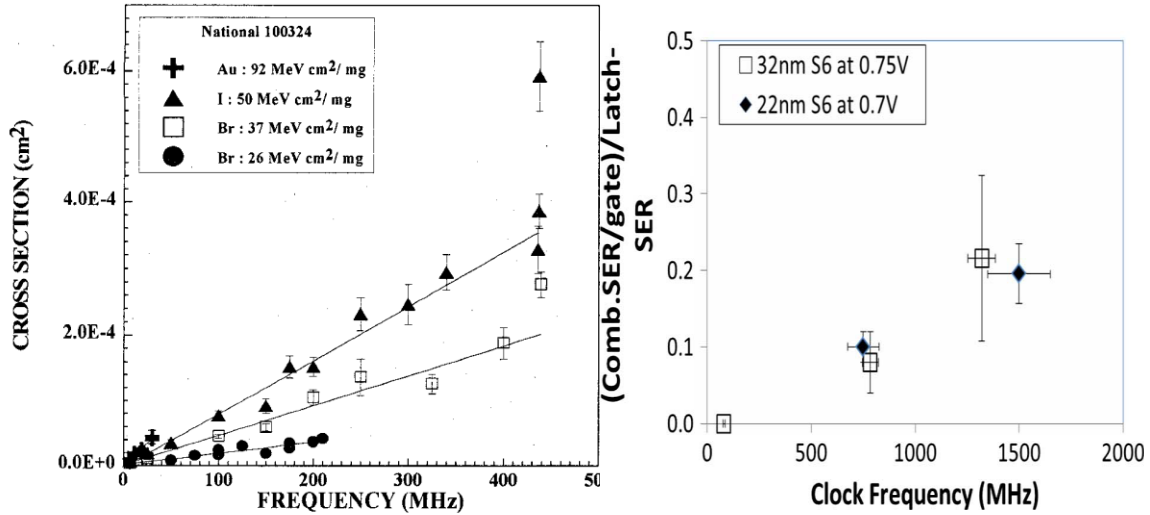


Fig 1.12. (a) Cross section and (b) soft error rate as a function of clock frequencies measured in [Reed96] and [Seif12] respectively. Increased vulnerability with increased clock frequency is consistently observed over multiple generations.

type of technology. Fig. 1.12(a) and (b) show the effect of clock frequencies on the cross section and soft error rates for irradiated test structures across generations and technologies. While finfets are generally less susceptible compared to their planar counterparts of similar dimensions, the increased clock frequency has a similar impact on SER as on the planar transistors. Fig. 1.12(b) specifically shows 22 nm finfet data for increased clock rates and it follows the same trend as a 32 nm planar bulk transistor.

In conclusion, scaled technologies are still susceptible to soft-errors and upsets in the presence of radiation events, though the SER trends are somewhat encouraging due to reduced collection efficiency and newer fin dependent effects. Trends have also shown a negative impact on the SER rates in scaled technologies. Ever increasing clock frequencies further compound these problems. Depending upon the intensity and type of radiation

exposure, this susceptibility of the CMOS devices calls for specific mitigation strategies, which are described in the subsequent sections.

1.6. Radiation Hardening

Having discussed in detail the radiation sources and effects on CMOS devices, methods for mitigating soft errors or single events is studied in this section. Techniques for creating radiation tolerant and radiation immune circuits is referred to as "radiation hardening". Radiation hardening could involve either circuit and system level design techniques, fabrication process techniques or a combination of both.

When integrated circuit fabrication processing is used to harden circuits by increasing the critical charge on sensitive nodes, the hardening is called radiation hardening by process (RHBP) [Lacoe00]. RHBP is cost intensive as a separate fabrication process, needs to be maintained and also limits the maximum speed of the design since intentional RC is introduced on design nodes.

1.6.1. Radiation Hardening by Design

Since IC technology is mature and ubiquitous, a general hardening technique irrespective of the process is more practical since the same circuit or system level design techniques can be applied across a range of commercial processes.

This radiation hardening methodology is referred to as radiation hardening by design (RHBD). The focus of this work is on RHBD. Common RHBD techniques involve adding redundancy to the design either in the spatial domain or temporal domain to mitigate or mask radiation induced soft-errors.

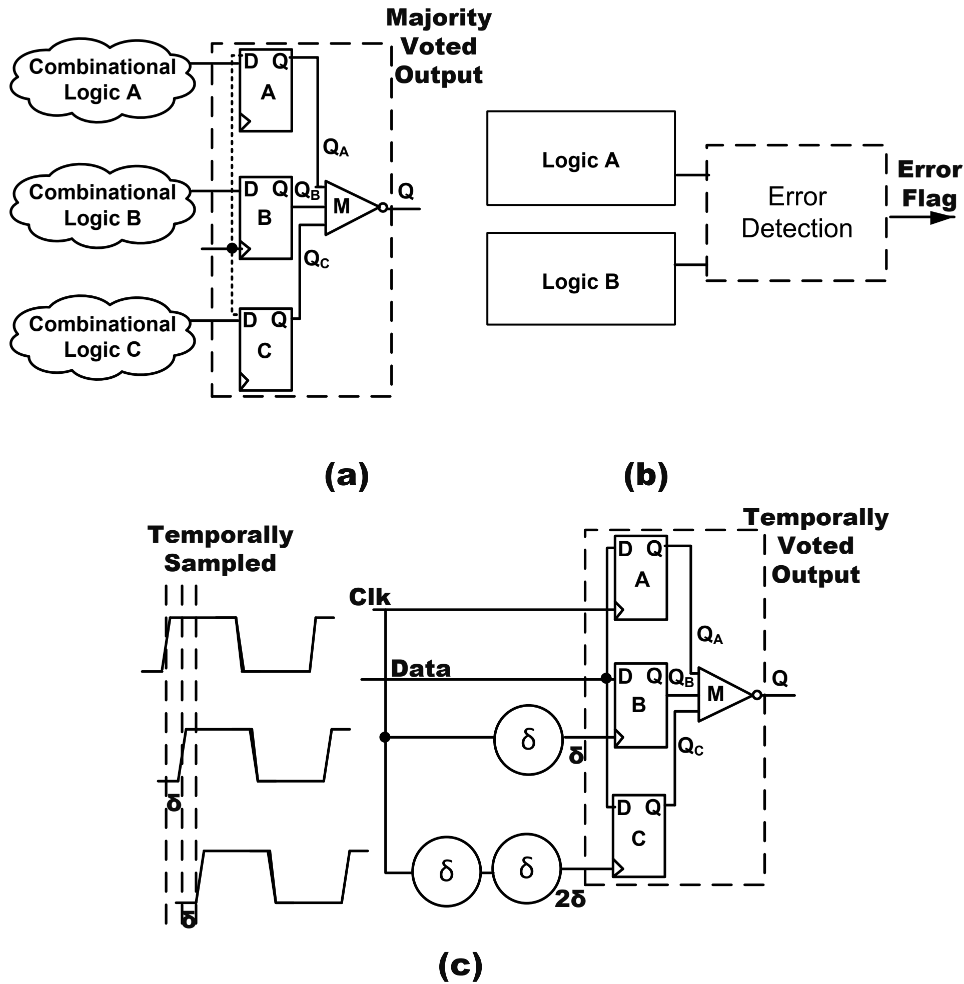


Fig 1.13. Triple modular redundancy (TMR) with complete triplication of combinationa and sequential elements ensuring complete mitigation with minimal timing penalty, (b) Dual Modular Redundancy (DMR) which detects a mismatch in the copies to set an error flag to be used by the error handler ensuring inhibition of erroneous signals and (c) Temporal hardening delaying signals in time to ensure that the SET gets masked by majority voting.

1.6.1.1. Hardening by Spatial Hardware Redundancy

Hardening by design can be accomplished by spatial hardware redundancy techniques such as triple modular redundancy (TMR) [Lyon62] [Hind09] [Hind11] and/or double modular redundancy (DMR) [Clar11] [Teif08] [Furu10]. Triple and double modular redundancy can correct and detect soft errors respectively, as shown in Fig.

1.13(a) and 1.13(b). Fig. 1.13(a) shows the triple mode redundancy with voting circuits that correct a single bit error on one of the copies of the circuitry.

Variants with either the sequential and/or combinational logic triplicated are designed for varying requirements of hardening and area overhead. Fig. 1.13(b) shows dual mode redundancy where the checker logic can detect the onset of errors because of mismatch. Based on the type of auxiliary schemes such as, parity bit and error correcting codes (ECC), the right values can be recovered in DMR hardening. The probability of upsetting two bits of the TMR or DMR logic could be significant if not designed carefully. Mitigating multi-node upsets will be studied in detail in subsequent sections and other chapters in this report.

Error correcting codes (ECC) for detection and correction of bit upsets are used as in [Fuji90]. In error detection and correction (EDAC) schemes, redundant bits are added to a data word to enable the system to detect and correct errors in the data (caused by SEU or SEFI) using enhanced ECC schemes such as Hamming codes [Chen84]. There is generally a trade-off associated with the area overhead (number of ECC bits) and the number of bit upsets that can be corrected.

1.6.1.2. Hardening by Temporal Redundancy

Single event upsets can also be mitigated by sampling data at different time stamps to ensure that any upsets can be filtered and recovered in the time allowed between sampling. Fig. 1.13(c) shows such a sampling system with a δ delay between each sample points. Three copies of sequential elements are created and they are sampled by clocks with

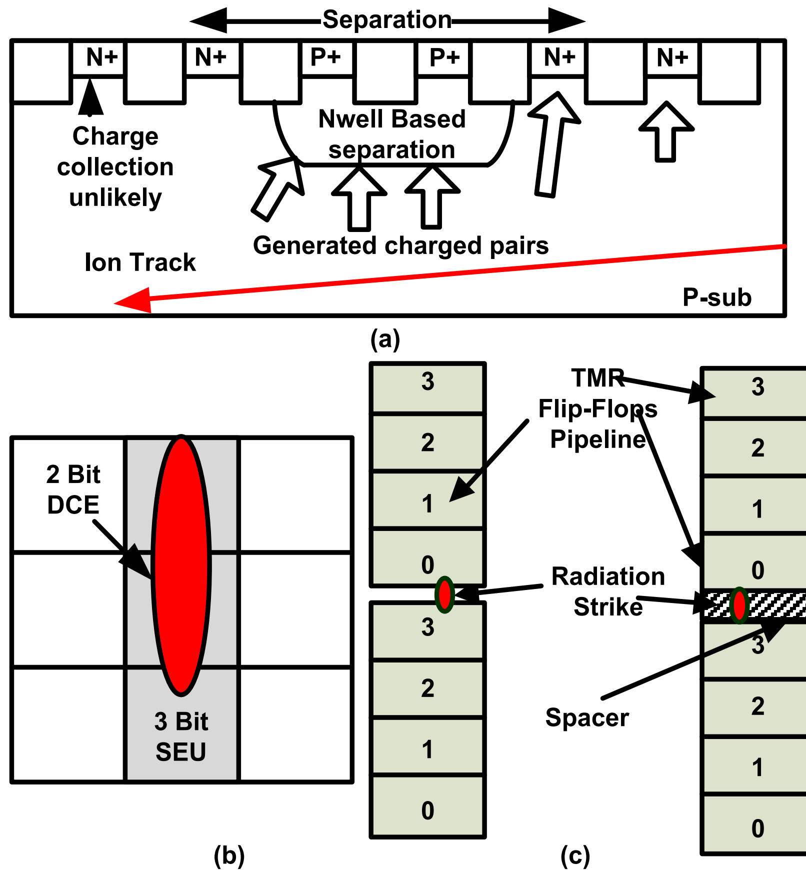


Fig 1.14. (a) Multi-node charge collection mitigation cross section due to nodal separation by n-well, (b) MBU in FPGAs as demonstrated in [Quin07] leading to DCEs and (c) CAD methodology based separation of multi-bit TMR cells with spacer between each groups to ensure that even non-equivalent flops in multiple domains cannot be upset with a single strike.

δ delay between them. In case of an SET the incorrect value will only be sampled by one of the copies, as long as δ>TSET (SET width). This method of hardening is called temporal hardening [Mavi02] [Matu10] [Clar14] [Nase06] .

A dual interlocked cell (DICE) latch [Cali96] is the most common redundant structure, doubling the storage nodes in a configuration that requires two (critical) nodes to be upset to change the state. DICE latch based flip-flops have been shown to be

susceptible to SET induced upsets arising from particle strikes spanning multiple nodes [Black08, Warren09].

1.7. Multiple Node Charge Collection (MNCC) and Domain Crossing Errors (DCE)

Multiple node charge collection (MNCC) occurs when multiple nodes collect charge deposited by the same ionizing radiation particle track. MNCC can span several microns, greatly complicating the design and layout of hardened architectures. Particle strikes that span multiple nodes may affect multiple redundant copies of bits that can thwart such schemes [Koga93] [Black08]. Redundant latches have long been known to be sensitive to such upsets [Hazu04].

In rad-hard FPGAs, these multiple node upsets cause non-recoverable errors [Quin07]. Quinn, et al., termed multiple node charge collection that resulted in upsets despite TMR due to upset of multiple hardened domains as domain crossing errors (DCEs). They quantified the SEU span to be directly proportional to the number of DCEs in FPGAs. Consequently, as the relative physical size of the charge collection area increases, the DCE probability increases. Fig. 1.14(b) shows the representation of a 3 bit upset on a FPGA which can lead to a 2 bit DCE [Quin07].

Previous works provide separation of multiple cell heights, in turn providing intervening N wells that act as efficient bulk charge collectors [Hind11] [Uemu10]. For such designs to fully mitigate DCEs, the combinational logic must also be separated to avoid coincident SET induced upset. Fig. 1.14(a) shows the CMOS cross section explaining charge collection in n-well separated diffusions. Charge collection probability is reduced due to absorption of charge by wells which act as charge collectors. The exact

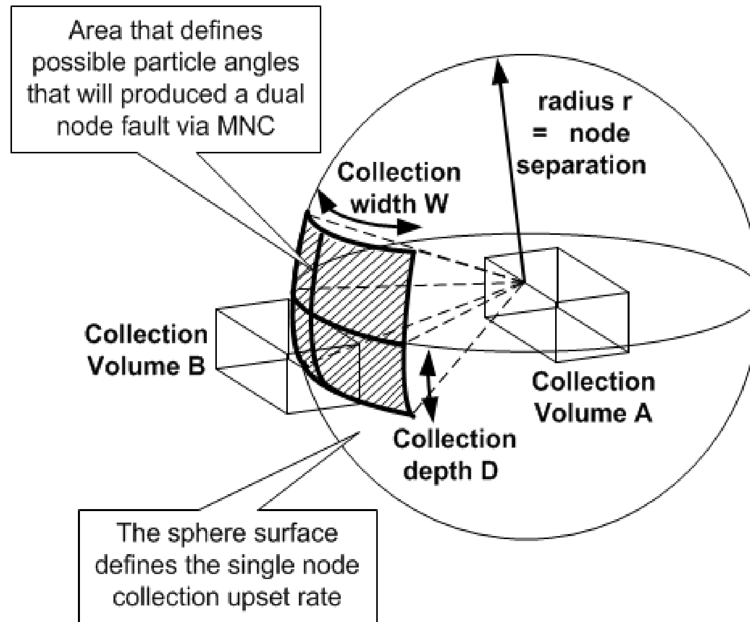


Fig 1.15. Effective cross section seen by an ionizing particle that simultaneously strikes two nodes A and B causing upset. Only a limited solid angle can pass through the collection region of both nodes, providing a straightforward estimate of the upset probability, after [Sham14].

value of spacing is a matter of mathematical and experimental validation and is dependent on doping profiles, the LET of the ionizing particles, as well as, the structure of the MOSFET. The MNCC problem is also exacerbated due to highly scaled technologies which will be used in reliability critical application such as aerospace, automotive and high energy particle physics experiments.

1.7.1. Mathematical Formulation of Nodal Separation

The probability of such MNCC induced upsets can be significantly reduced by providing adequate spatial separation between redundant nodes [Clar14] and is the key to ensuring the success of redundancy based RHBD techniques. Fig. 1.15 shows the illustration used to formulate the mathematical upset probability from a MNCC where A

and B are the two sensitive nodes. By centering a sphere at node A with a radius r defined by the distance to the collection volume of node B, the relative reduction in circuit cross-section afforded by the node separation is calculated. A solitary node susceptible to upset (i.e., a single node upset) can upset from any angle. This shaded area defines the area on the sphere's surface that a particle must pass through to cause MNCC upset on nodes A and B. Therefore, the formulation of cross section reduction due to nodal separation as illustrated is given by equation 5:

$$\sigma_{NODE_{MNCC}} = (\sigma_{base}\, W\, D)/(2\pi r^2) \qquad (5)$$

Where the σ_{base} is the base cross section for an unseparated design. W and D are collection width and depth respectively of rectangular area subtended on the sphere. Therefore, increasing the separation by r reduces the cross-section due to multiple node collection by approximately ($1/(2\pi r^2)$). A spatial separation of 2 µm is estimated to reduce the vulnerability to MNCC by 96% over adjacent nodes on a 90 nm commercial bulk CMOS process.

1.8. MNCC Separation in CAD Flows

With the device physics, circuit response and mitigation strategies in relation to soft-error upsets explained in the previous sections, the question is how to apply these constraints in large scale practical systems? Large designs need to incorporate soft error

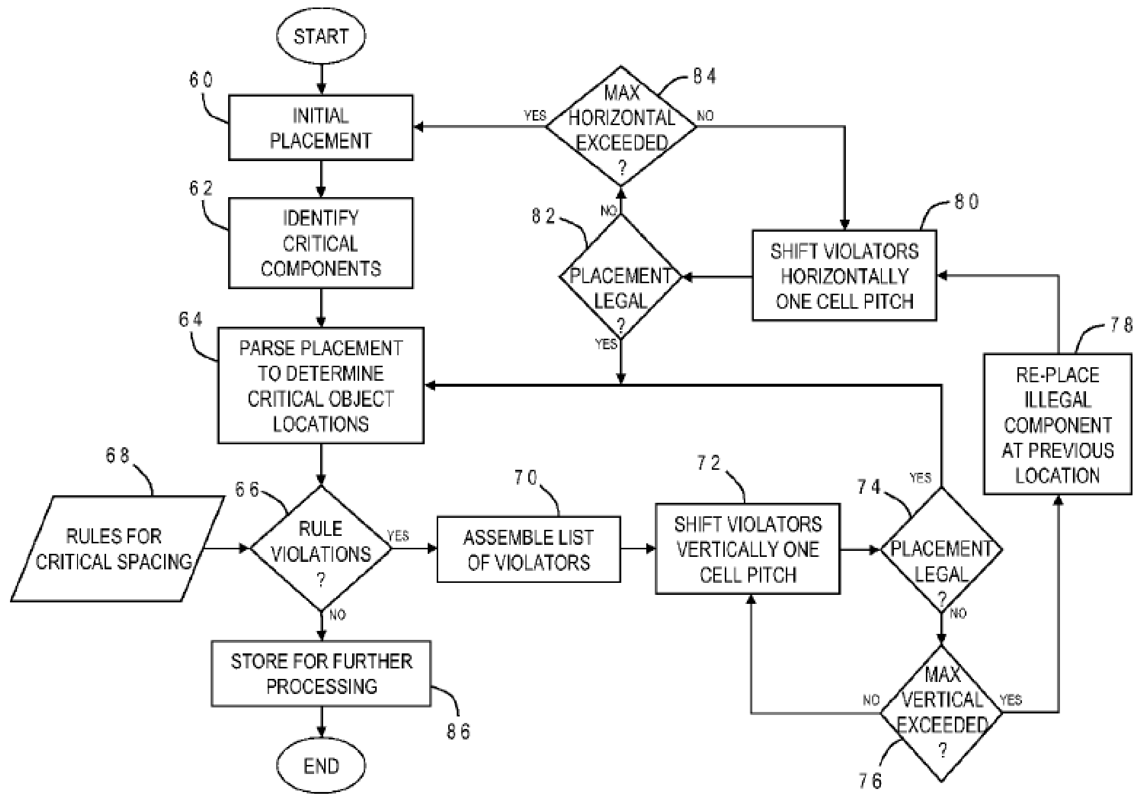


Fig 1.16. A method of CAD based critical component separation of CMOS gates by using critical spacing rules (e.g. 5 µm) recursively, after [Klei10].

resilience techniques into standard design methodologies for practical applications. Standard CAD methodologies have evolved over the past few decades and are capable of handling immense design complexities (>1 Billion transistors) while addressing the standard constraints of power, performance and area (PPA). However, little consideration has been given to addressing soft error concerns in standard CAD design flows.

Long design cycles and illumination of failure modes by broad beam testing [Mitr05] is partly due to the lack of sophisticated RHBD computer aided design methodologies on par with those used for commercial designs [Hind11]. Radiation-effects

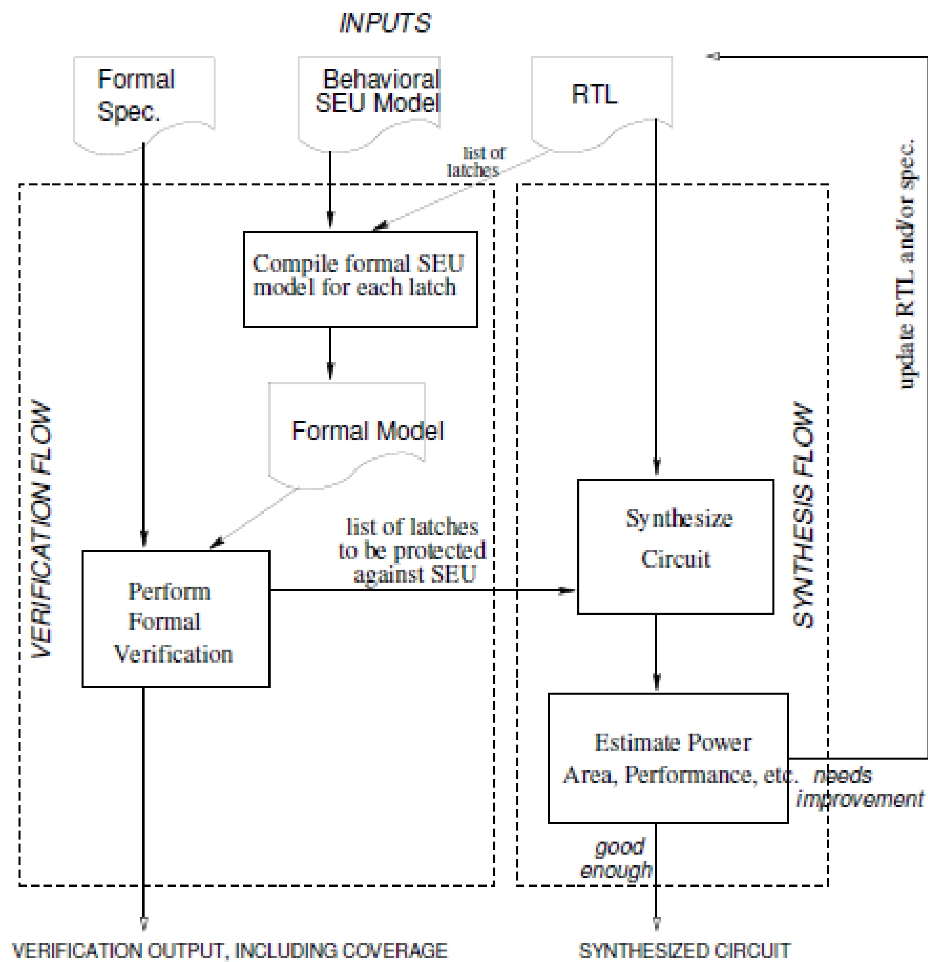


Fig 1.17. Verification based SEU estimation and selective hardening in synthesis step, after [Sesh06].

oriented CAD flows for RHBD designs often involve creating complex frameworks over the standard top-down or bottom-up methodologies [Nick05]. Moreover, there are very few examples of optimized, automated RHBD flows. Kleinosowski et al. patented a placement methodology for CAD based separation to ensure recursive spacing of critical components based on spacing rules. The methodology aims at reducing sensitivity to radiation induced soft-errors by the flowchart shown in Fig. 1.15.

A gate resizing methodology for reduction of SER in flip-flops by utilizing temporal masking produces a 90% SER reduction at a 5% power overhead [Josh06]. A similar gate sizing methodology for the sensitive nodes in a design to reduce the SER is explored in [Zhou06]. The basic idea is to exploit the asymmetric logical masking probabilities of gates and hardening gates that have the lowest logical masking probability. The said methodology incurs an overhead of 38.3%, 27.1%, and 3.8% in area, power, and delay for worst case SEUs tested across the four process technologies. A multi-objective genetic algorithm (MOGA) is implemented in [Shen09] to optimize the soft error tolerance of standard cell circuits with soft-error rate, chip area and critical path delay as the optimization goals for the algorithm. An SER reduction of up to 74.25% is claimed for 5.23% area overhead.

Selective hardware redundancy insertion has also been explored in several works. A selective TMR insertion methodology is explored in [Ruan11]. A feed forward equalizer is implemented with the said methodology and selective portions are TMRed to achieve 50% area reduction over full TMR to achieve 80% SER reduction. Redundancy addition and removal (RAR), aimed at eliminating those gates with large contribution to the overall SER is proposed in [Wu13]. An average 23% SER reduction for 4% area overhead was recorded in this work. RTL level early hardening is explored in [Zoel08]. Here the computational model considers the gate susceptibility, logical masking, electrical masking and latch window masking to ascertain gate susceptibility at pre-syn stage. DMR is used to reduce SER post evaluation. A verification guided SEU protection methodology which assists synthesis flow step to harden targeted logic is shown in [Sesh06]. The flowchart for verification and synthesis strategy is shown in Fig. 1.16.

While there are multiple mitigation strategies proposed, these methods however have neither been proven on silicon nor are applicable to high-speed designs of realistic complexity designs where individual gate sizing is impractical and the resulting SER reductions accrued nominal.

This work introduces custom design techniques and automated place and route CAD flows for designing complex redundant designs with varying degrees of hardware redundancy. The trade-offs that ensue while implementing various designs with radiation mitigation incorporated at circuit and system level are studied. The flows are designed to be independent of the type of IC technology, transistor architecture and design functionality. The separation required to mitigate SEEs and MNCC is a constraint in the proposed methodologies and can be applied to any design architecture and fabrication technology. Additionally, the separation required can be seamlessly modified as a part of the flow and the resulting PPA changes can be studied. The focus of this work is to minimize overhead (PPA) while incorporating quality RHBD design with highly evolved CAD techniques. Silicon test results of designs implemented with the proposed methodologies validate their efficacy.

1.9. Summary

Chapter 1 explained the radiation environment that surrounds the Earth, the kind of radiation sources and the resulting particles that MOS devices are subjected to. The response of CMOS devices to these particles and the mechanisms of upset or soft-errors are established. The historical perspective on soft error rates and the variation in the soft-error rates due to clock frequencies and device architectures is also elucidated. The types of mitigation strategies and the mechanisms of correction and/or detection have been

defined. The need for separation of the design critical nodes and their impact on SER is established. Finally, the need for computer aided design flows which can incorporate nodal separation while optimizing the standard PPA metric is also presented. The next chapter presents the module level separation methodology with a radiation hardened advanced encryption (AES) standard as an example architecture. Chapter 3 describes the improved serpentine fine grained separation methodology with a processor as an example to showcase a redundant and non-redundant co-design methodology. Chapter 4 showcases the circuit and CAD design of a novel radiation hardened TMR pulsed multiplying delay locked loop for DDR2/3 applications. Chapter 6 concludes the thesis while laying the foundations for future work.

CHAPTER 2. MODULE LEVEL SEPARATION: AES

2.1. Introduction

The first chapter explained the effects of radiation particles on CMOS designs and hardening by design techniques to mitigate soft-errors and multi-node charge collection. This chapter describes a module level separation methodology for pipelined designs with an advanced encryption standard design as a case study. A 128 bit data, 256 bit key AES engine is implemented in hardware on a 90 nm low standby process (LSP). Pulse latches are chosen as the sequential element in the AES pipeline for low-power and high-speed implementation. AES design is full TMR in RTL (data and key) and constitutes a 15 stage pipeline. Sequential elements are also implemented as TMR and domain separated in custom design. Spatial separation is incorporated using the large fences CAD methodology for pipelined combinational and sequential logic to mitigate DCEs. Silicon testing shows chip A test chip TC23 is implemented with the AES design prototype and tested for functionality (VDD_{min} of 570 mV and VDD_{max} of 1.5) in a radioactive environment with proton radiation exposure (upset free to 63 MeV broad beam). Verilog simulations at the top level and spice simulations of constituents are performed to prove pre-silicon functionality, reliability and design performance.

2.2. AES Encryption Background

The advanced encryption standard (AES) is a cryptographic standard that is an upgrade on the data encryption standard (DES). AES is based on the Rijndael algorithm proposed by two Belgian cryptographers, Dr. Joan Daemen and Dr. Vincent Rijmen [Rijm01], as a submission to the design contest by the national institute of standards and

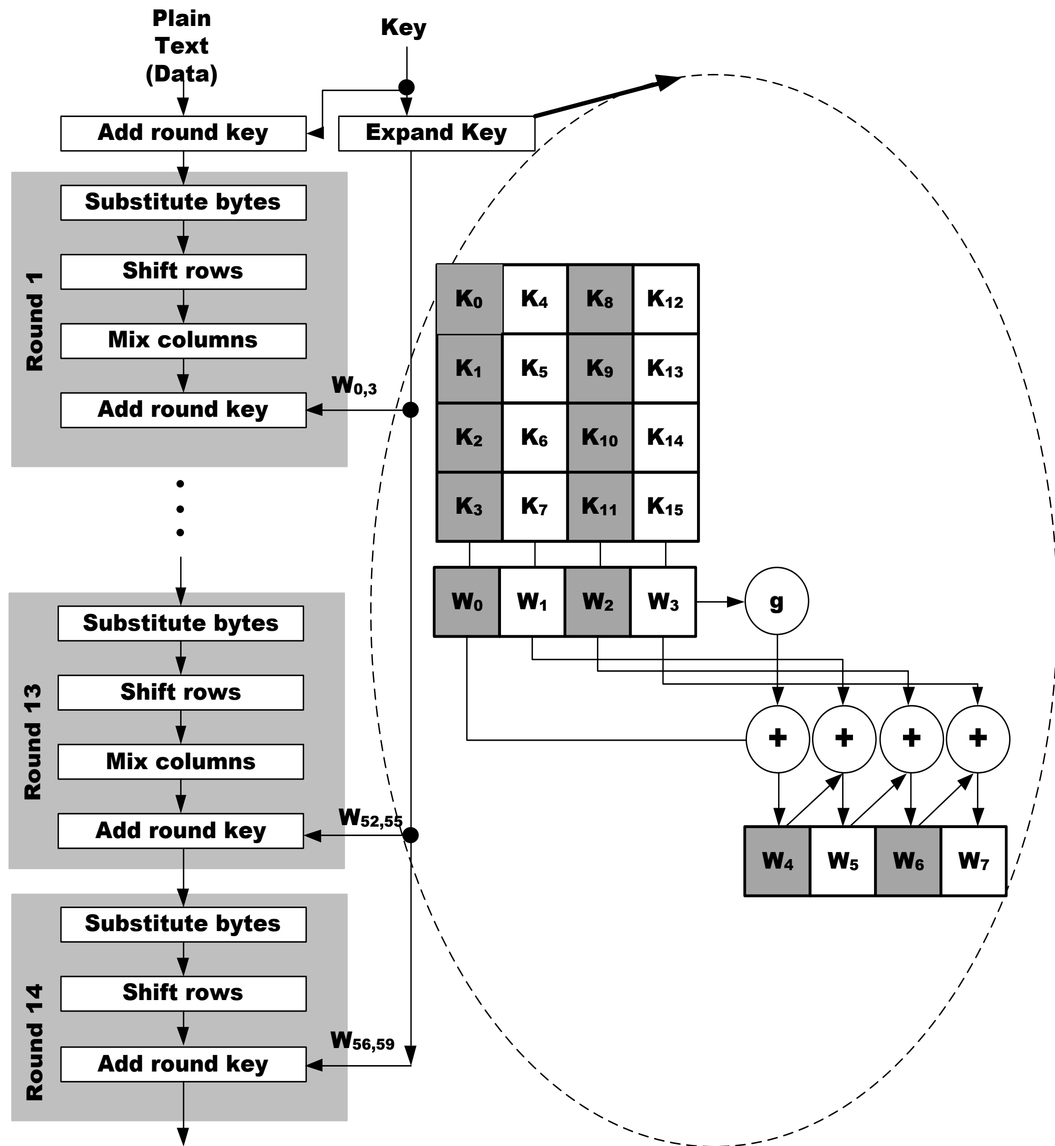


Fig 2.1. AES engine algorithm showing 14 rounds for a 256 bit key design, Expand key stage which creates the key for each round to be added in add round key step is shown in the dotted circle.

technology (NIST) in January 1997. The algorithm Rijndael allows for a variety of block and key sizes unlike the 64 bit block and 56 bit key sizes of DES. The block and key can be chosen independently to be 128, 160, 192, 224, 256 bits and allow design flexibility. However, the AES standard algorithm can only accept a block size of 128 bits and a choice of three key sizes - 128, 192, 256 bits. These three sizes are in turn named AES-128, AES-

192 or AES-256, respectively. AES parameters depend on the key length. For example, if the key size is 128, then it would need 10 rounds to process the key, whereas it takes 12 and 14 rounds for 192 and 256 bit keys, respectively. AES forms the basic cryptographic primitive in a number of standards including Internet Request for Comments (RFCs), Internet Protocol Security (IPsec), high-definition television (HDTV) encryption and Wi-Fi Protected Access 2 (WPA2).

2.2.1. AES Encryption Algorithm

The AES algorithm overall structure is shown in Fig. 2.1. Plain text data and key are arranged as a 128 and 256 bit square matrix of bytes in order to perform encryption. The key schedule array words are then calculated using the key (the W matrix). The AES algorithm consists of a basic stage with four transformations (rounds):

(i) Substitute bytes

(ii) Shift rows

(iii) Mix columns

(iv) Add round keys

For the 256 bit key size a preliminary round of add key, 13 rounds of basic round stage and 14th round of the basic stage (sans the mix column transformation) are undertaken for one complete encryption cycle. The decryption follows a similar inverse transformation.

2.2.1.2. Substitute Byte Transformation

The substitution bytes stage (SubBytes) is simply a transformation based on table lookup using a 16×16 matrix of byte values called an s-box. The said matrix consists of all the possible combinations of an 8 bit sequence ($2^8 = 16 \times 16 = 256$) (Fig. 2.2). However,

the s-box is not a random permutation of these values and there is a well-defined method for creating the s-box tables. The Rijndael algorithm shows how s-boxes are designed, unlike the DES for which no rationale was given. S-boxes designs are not explored here and are simply considered as table lookups. The basic matrix that gets operated on in the AES is called a state. Each byte in the state is mapped into a new byte in the following way: the leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column (Fig. 2.2).

2.2.1.3. Shift Row Transformation

Shift row is a simple transformation with 4 steps (2.2):

(i) The first row of state is not altered.

(ii) The second row is shifted 1 byte to the left in a circular manner.

(iii) The third row is shifted 2 bytes to the left in a circular manner.

(iv) The fourth row is shifted 3 bytes to the left in a circular manner.

2.2.1.4. Mix Column Transformation

This stage is basically a substitution which makes use of the arithmetic of GF (2^8). Each column is operated on sequentially. Every byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the matrix multiplication as shown in Fig. 2.2.

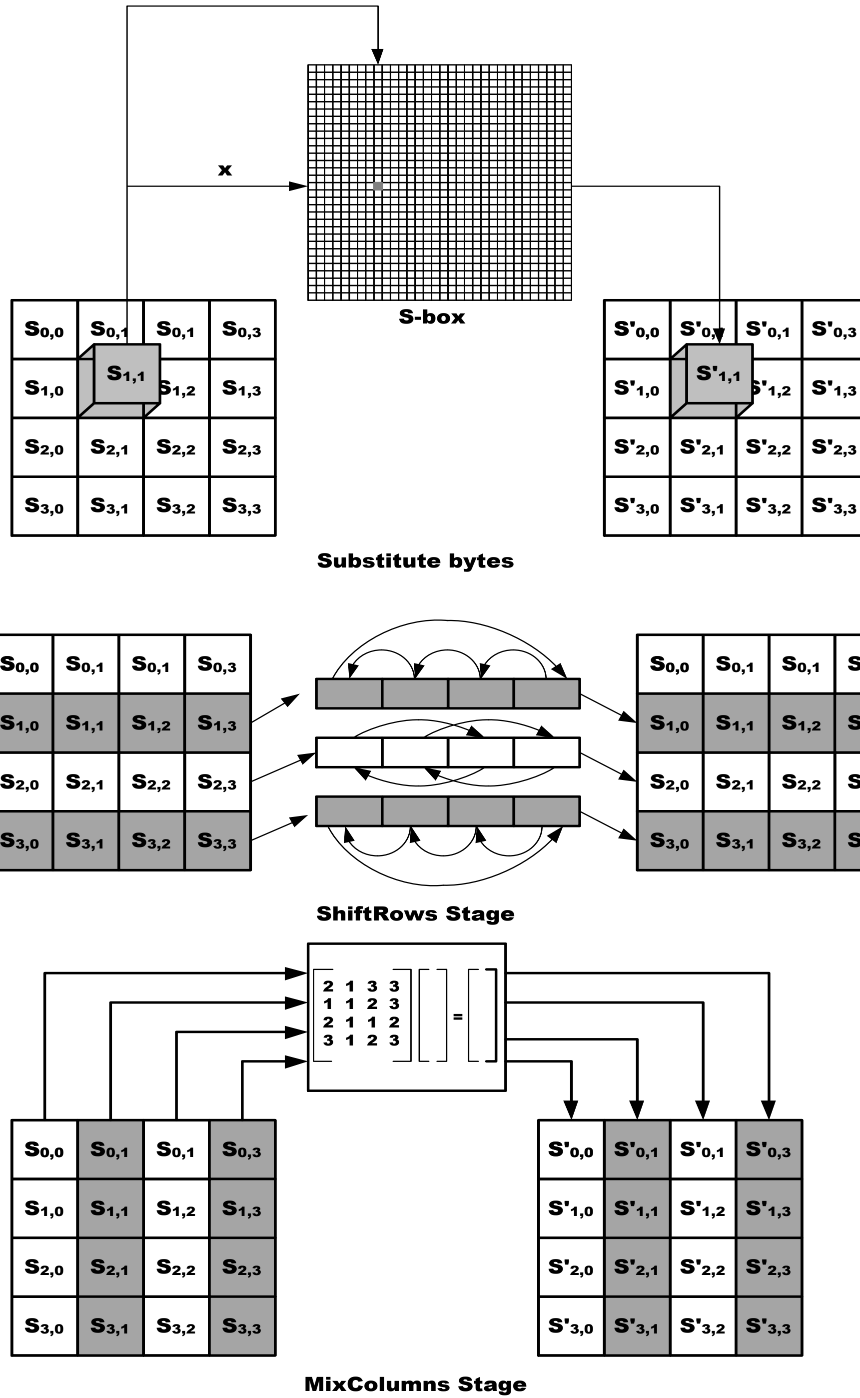


Fig 2.2. AES transformations, Substitute bytes, shift rows and mix column stages are done on the input stage matrix. Sbox is shown in the substitute bytes transformation.

2.2.1.5. Add Round Key Transformation

In this stage the 128 bits of state are bitwise XORed with the 128 (or 256) bits of the round key produced by the key expansion. The operation is a column wise operation between the 4 bytes of a state column and one word of the round key. This transformation is very simple and efficient, but it also transforms every bit of state (2.2).

2.2.1.6. AES Key Expansion

The AES key expansion algorithm takes as an input a 4-word key and produces a linear array of 44 words and 60 words for a 128 bit key and a 256 bit key, respectively.. Each round uses 4 of these words as shown in Fig. 2.1. 128 bit input block is arranged in the form of a state array, arranging 16 bytes of the encryption key in the form of a 4×4 array of bytes. Four of these bytes constitute a word of the expanded key {W_0, W_1, W_2, W_3}. The words {W_0, W_1, W_2, W_3} are bitwise XORed with the input block before the round-based processing, four at a time. The key expansion as explained in Fig. 2.1 is a four-word to four-word operation, such that each current grouping of four words decides what the next grouping of four words will be.

2.2.2. AES Implementation

The demand for AES hardware implementations has grown due to its ubiquitous presence in popular standards and protocols. In resource critical environments, a low power and area implementation is preferred due to power constraints. The architecture and design of AES in hardware is usually driven by the power, latency and area requirements. Combining low area with low power and a relatively low number of cycles makes it harder to design AES for number of emerging resource-critical applications such as RF

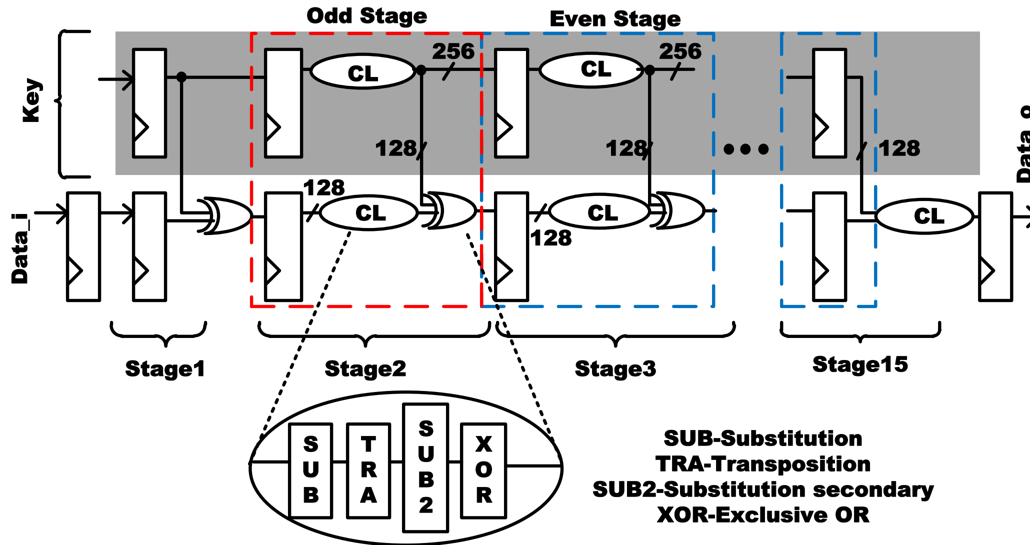


Fig 2.3. Advanced Encryption Standard architecture as implemented. It is pipelined over 15 stages for high-speed operation. Transformations by the combinational logic (CL) are shown in boxes.

identification (RFID), wireless sensor networks (WSNs) and smart cards (operating at 100 kHz with power in microwatts and millisecond latencies) [Good10, Zhao15]. 32 and 128 bit AES architectures are therefore unsuitable for the aforementioned applications. High throughput Gbps designs in 128 bit architectures are usually explored to provide an efficient (P.A.T) solutions in ASICs. The AES design provided for this work is a black-box and the architecture was frozen. Best possible PPA was targeted with a TMR implementation while maintaining soft-error reliability specifications for space applications.

The basic high level block diagram of a fully pipelined AES is shown in Fig. 2.3, where the pipeline operations are also shown. The data is XOR'ed with the output of the sub-key unit. The AES implementation in this work uses a 15-stage pipeline with a 128 bit initialization vector and 256 bit encryption key. Data and cipher texts are 64 bits, streamed continuously, using counter mode, where 64 bit data is XOR'ed with the key pipeline MSB

or LSB. Studies on the effect of pipeline depth on AES power and performance show that full pipelining provided the highest performance [Chitu05]. The number of such stages "N" is 11, 13 or 15 depending on the key width.

Keys and initialization vectors are loaded separately. In the design here, the key is also pipelined, and is clocked parallel with the data pipeline. This is very suboptimal from an energy perspective—the key, since it updates rarely, is typically generated by software. However, it provides excellent visibility into the hardening capabilities of the proposed approach. The pipelined hardware key implementation triples the soft-error cross-section of the design and thus affords demonstration of the correction capabilities of the proposed TMR pulse-clocked latches and the APR CAD methodology. Furthermore, AES as a hardening test vehicle is excellent since the algorithm's diffusion property forces a high fan-out from any SET or SEU, as is shown subsequently with Verilog simulations [Mathu06].

2.3. TMR Pulse-clocked Latch for RHBD

The use of pulse-clocked latches (that are basically just the slave) instead of flip-flops have provided clock and sequential circuit power reductions of over 40% due to the lowering in both the number of sequential elements and clock power [Warn10, Tsch01, Clar01]. In performance limited designs, the soft capture edge provided by the pulse clocking allows higher speed via time-borrowing to the latch closing edge. Delay improves

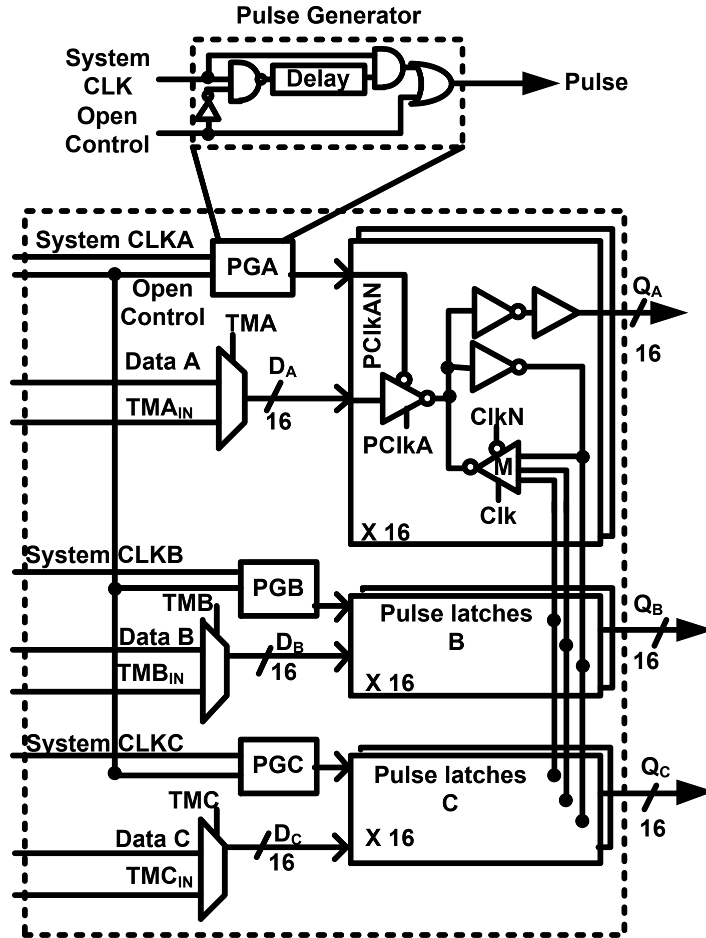


Fig 2.4 Schematic of self-correcting pulse-clocked latches and pulse generators. Multiplexers select between data and test mode input, majority voting internal nodes (maj_a, maj_b and maj_c) are also marked.

by the lower overall dead-time due to a shorter timing critical path through a single latch. This design is first use of TMR pulse-clocked latches in soft-error TMR hardened applications.

Seifert, et al., found that in unhardened designs using pulse latches, 50% of the chip-level soft-error rate (SER) was from radiation induced clock failure [Seif05]. They stated that chip level SER from clock failures for flip-flop based designs is 10%. In particular, clock transients produced in the pulse-generators accounted for up to 90% of

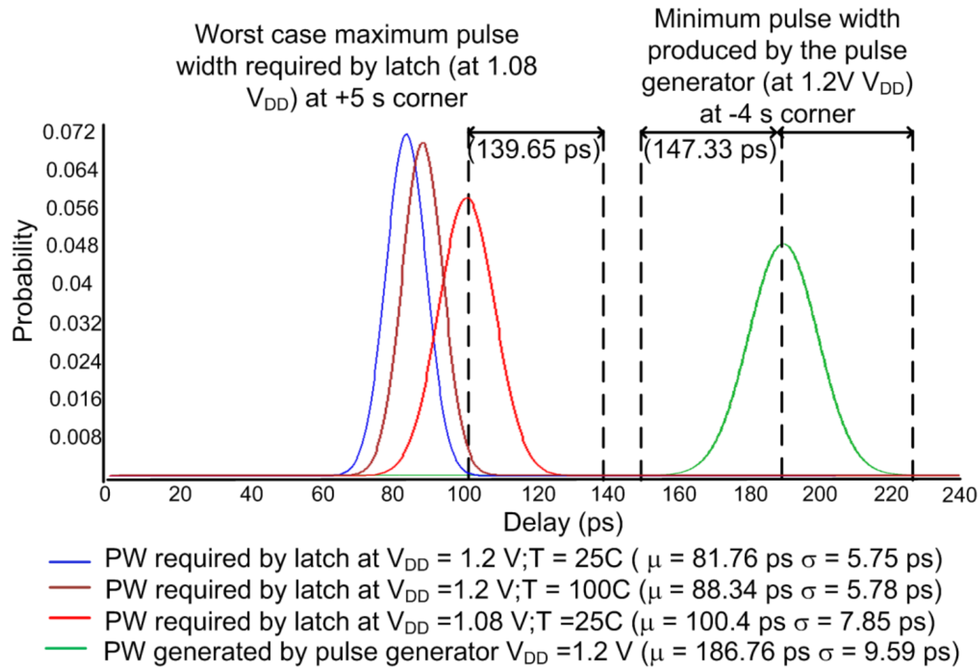


Fig 2.5 Statistical analysis of the pulse latch and pulse generator showing worst-case pulse width for proper data capture mean and sigma as well as pulse generator variation as determined by MC simulation.

unhardened pulse-clocked latch's clock-induced SER. Hansen, et al., in [Hans09] shows that in the case of a TMR flip-flop based design, the cross-section of the clock is greater than the TMR flip-flop cross-section across all linear energy transfer (LETs). Therefore, clock trees are also hardened in this work by providing complete spatial separation for clock domains.

2.3.1. Variation Tolerant Pulse-Latch Circuit Design

The TMR pulse-clocked latch employs three redundant latches with majority-voted latch feedback, providing automatic self-correction (Fig. 2.4). TMR clock trees driving pulse clock generators (PGA, PGB, and PGC) provide independent clocks to each latch domain. The A copy majority voter receives the B and C copy feedback. Voted correction

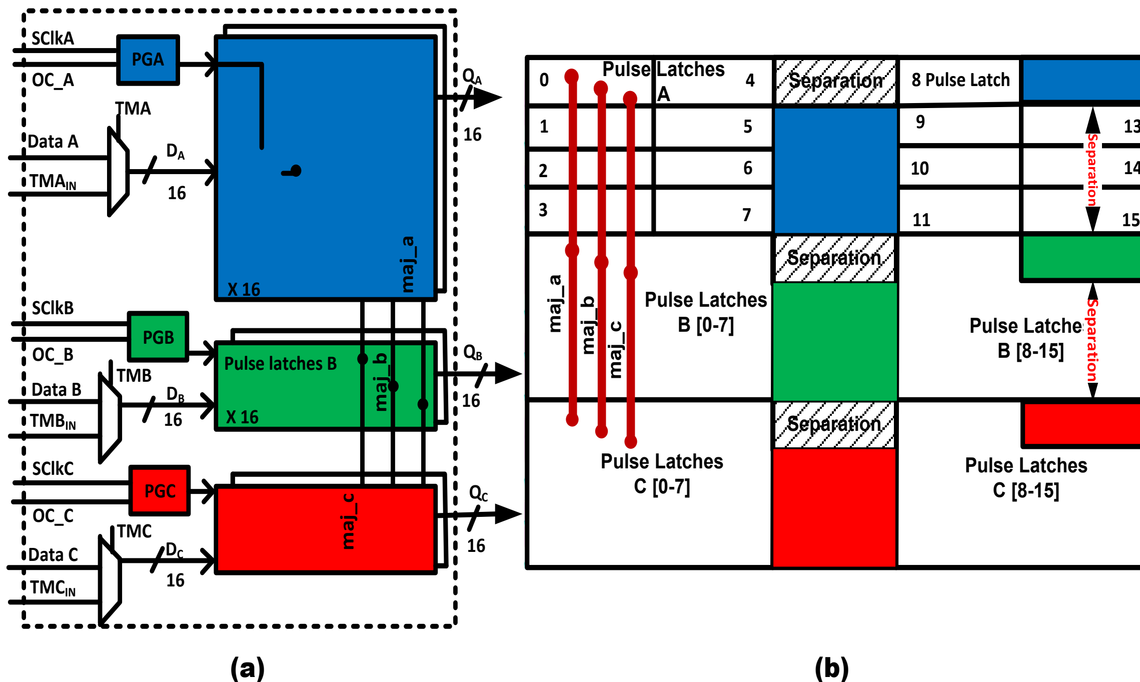


Fig 2.6 Color coded schematic (a) and layout (b) of the 16-bit, TMR pulse latch design with 3 domains (A-blue, B-green and C-red) highlighted. Latches and the shared pulse generator are shown. The spatial separation incorporated which makes the layout DCE immune.

occurs in the clock low phase. This majority-voted feedback is identical in the B and C domain latch copies. Multi-bit latch blocks share pulse generators, reducing the overall clock distribution loading and ensure good pulse fidelity. The number of bits (16) was chosen to optimize the pulse fidelity and minimize the pulse generator overhead. The 16 bit TMR pulse-clocked scheme affords a 42% reduction in sequential circuit and clock energy compared to a flip-flop implementation and reduces the overall circuit area [Chel15]. The size is reduced by 35% over a master-slave flip-flop based design—about 40% due to the removal of the slave masters, but the shared pulse-clock generators add area overhead.

Pulse latch design requires the width of the pulse generated from the pulse generator to be wide enough where the data is always captured reliably. Secondly, the width of the pulse also needs to be minimized for minimum delay (hold) paths such that the hold violations can be mitigated with minimal insertion of hold buffers. These opposing pulse width constraints are achieved by guard-banding statistical simulations. The narrowest pulse width required to prevent a latch failure was determined from the mean required write pulse width $\mu_{MIN\text{-}WRITE}$ of 100.4 ps plus a $5\sigma_{MIN\text{-}WRITE}$ ($\sigma_{MIN\text{-}WRITE}$ = 7.9 ps) of 139.7 ps (Fig. 2.5). The pulse generator was designed to have a worst-case pulse width greater than this at its -4σ tail, ensuring that the worst case pulse generator (producing the shortest pulse) could still sufficiently clock the worst case latch (slowest latch). The pulse generator was designed to generate pulse widths based on $\mu_{PG\text{-}WIDTH}$ = 186.8 ps minus $4\sigma_{PG\text{-}WIDTH}$ ($\sigma_{PG\text{-}WIDTH}$ = 9.6 ps) = 147.3 ps. The minimum hold margin required for the chip was then determined as the largest pulse produced by the pulse generator, i.e., $\mu_{PG} + 4\sigma_{PG}$ = 225 ps.

2.3.2. Custom Design for DCE suppression

The 16 bit macro layout is shown with domain segments and 16 separated latches per domain in Fig. 2.6(b). The equivalent schematic portions of the circuits are shown in Fig. 2.6(a). Majority voting feedback routing, labeled maj_a, maj_b, and maj_c, is shown only for the first four latches. Each line represents four wires (48 total in the macro). The pulse generators are separated by one standard cell row (decoupling capacitor) to reduce the probability of a domain crossing particle affecting two pulse-clocks. The latch copies are separated by three standard cell rows (7.84 μm). The 16 bit macro is 23.52 μm × 29.4

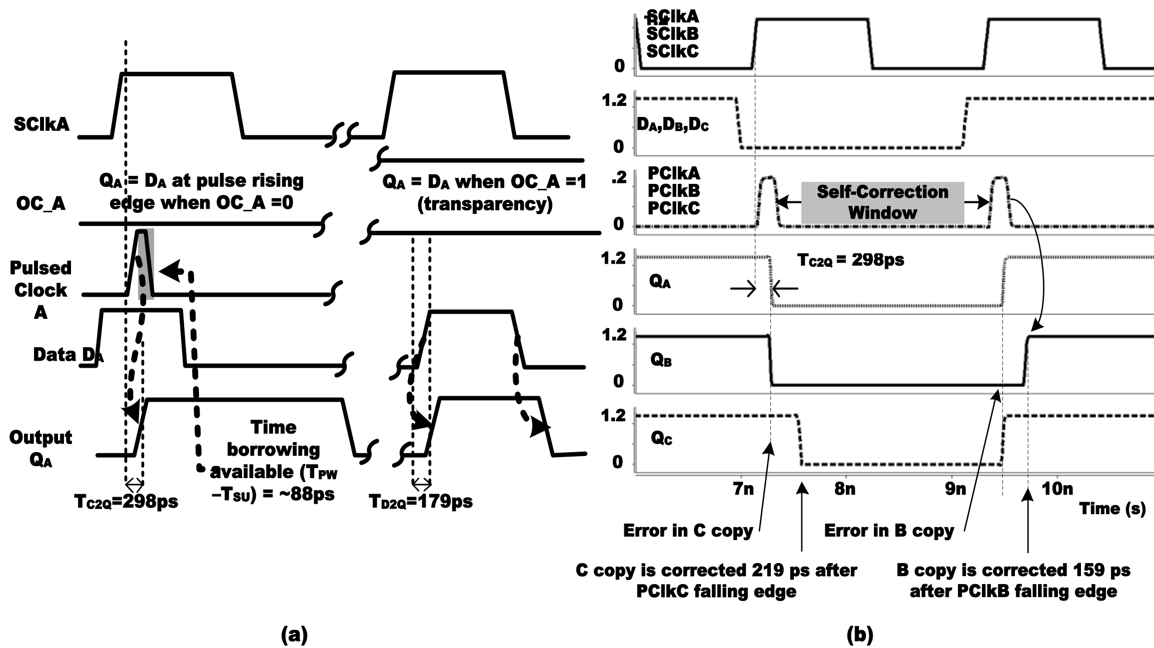


Fig 2.7 (a) Pulse-latch operation with nominal pulse width and decision window timings (T_{C2Q} and T_{D2Q}). Nominal time borrowing of 88 ps is afforded by the design. (b) Self-correction in the TMR latch is shown with an error in the C copy, the onset of the negative edge of the clock pulse initiates correction. Correction window is a function of the slack afforded in path is question and varies accordingly.

μm. The 16 bit macro is then placed in APR driven by pipelined connectivity as will be demonstrated in the CAD sections. As stated in the previous chapter, the spatial separation proven to be DCE immune for a majority of particle strikes (~5um) is less than the custom separation incorporated in this work, ensuring high statistical confidence.

2.4. Pulsed Latch Operation

2.4.1. Timing Diagrams

The basic timing metrics of the designed pulse latch at the typical corner is shown in Fig. 2.7(a). Data to output (T_{D2Q}) delay of 179 ps and a clock to output delay (T_{C2Q}) of 179 ps is observed. The nominal value of time borrowing observed is 88 ps. Importantly,

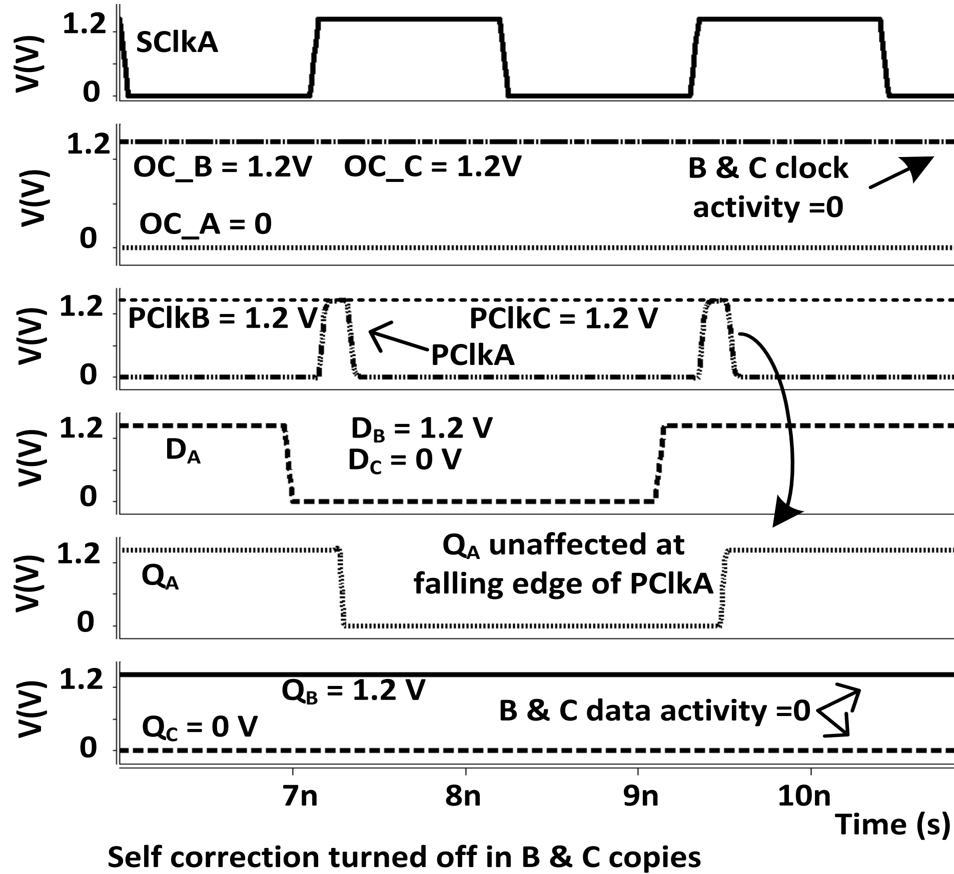


Fig 2.8 Non-redundant mode operation with data D_B and D_C held at 1 and 0 respectively with open-control set to transparent.

since correction occurs in the feedback mode during the negative phase of the pulse (Fig. 2.7(b)), the pulse-clock affords a larger correction window (i.e., greater than half the clock cycle) compared to previous master-slave implementations [Hind11]. The B and the C copies correct at the end of the pulse, after a delay of 219 ps and 159 ps, respectively. The difference in correction delays is due to the different pull-up and pull-down transistor ratios. The pulse-clocked latch macro timing characterization used Synopsys Nanotime and incorporated time-borrowing for synthesis and automated placement and routing (APR) to ease timing closure.

2.4.2. Test Modes

The test mode is controlled by the multiplexer select TMA/B/C and allows for the testing of each pipeline copy by forcing the inputs of the other two copies to logic 1 and 0 individually by controlling TMA/B/CIN inputs, thereby negating the majority voting impact on the third (tested) copy. Fig. 2.8 shows the A pipeline being tested by forcing logic 0 at the B pipeline input and logic 1 at the C pipeline input. B and C clocks are held high to ensure constant propagation of 1 and 0 for B and C copies, reducing dynamic power dissipation. Test mode also allows radiation testing with and without correction thereby enabling a realistic cross-section improvement measurement on silicon.

2.5. Module Level Separation CAD Flow

Fig. 2.9 is a flowchart of the RHBD CAD steps. Highlighted in red are steps which take spatial separation constraints to mitigate domain crossing errors. The pipelined AES design's mixed Verilog and VHDL behavioral descriptions were synthesized using Cadence RTL compiler with the foundry provided standard cells and our TMR self-correcting pulse-clocked latch macros. Normal synthesis options are disabled that would otherwise recognize and remove redundant circuits. Encounter APR tool is used for the AES physical design and spatial separation.

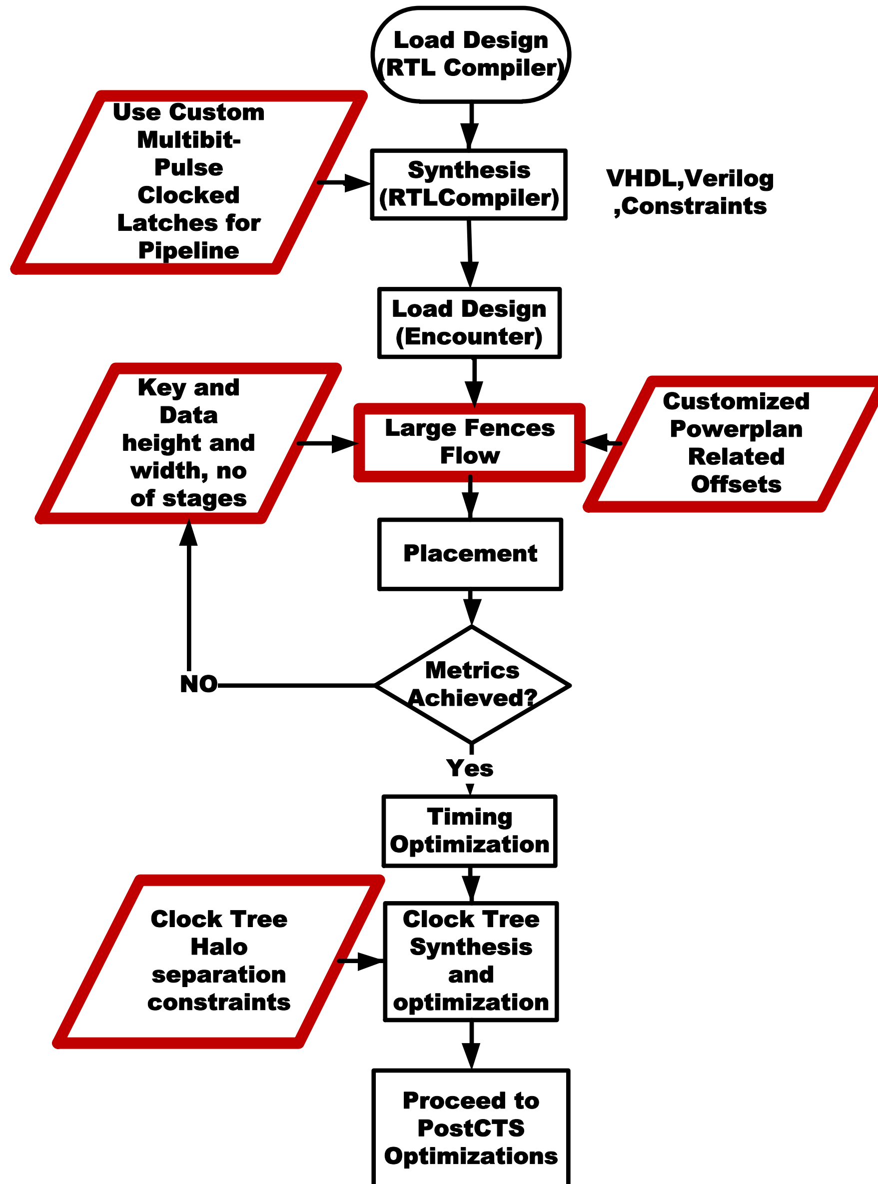
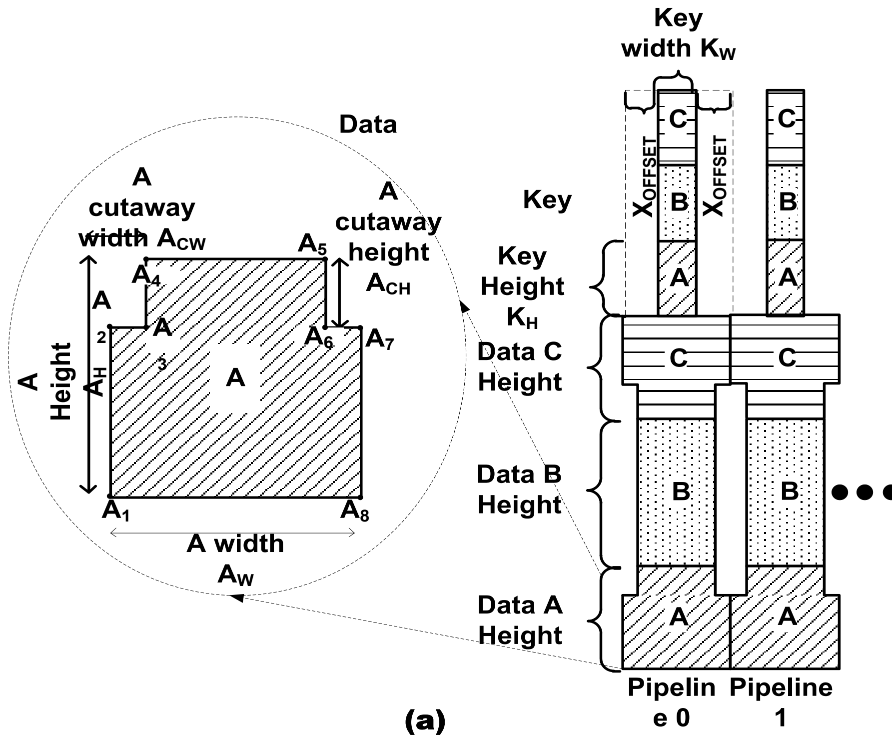


Fig 2.9 RHBD CAD module level separation using large fences, complete separation of custom, APR (combinational and clock) portions is achieved to create a DCE immune design.

The sequential circuit critical node separation was described in the Section 2.3.2. Unlike the previous approaches, this work uses large domain regions (fences), to provide



Step 1: Parse User Inputs (Dimensions of Fences, Offsets and number of stages)
Step 2: Start at X_1,Y_1
Step 3: $X_i = X_1 + X_{OFFSET}$
Step 4: Run steps 5, 6, 7 for all pipelines 0-14

Step 5: Create the Key section

i) Create A key rectangle as contiguous shape using 4 points in clock wise sequence

(X_i,Y_1) (X_i,Y_1+K_H) $(Xi+K_W, Y_1+K_H)$ (X_i+K_W, Y_1)

i) Similarly create B key rectangle starting at (X_i, Y_1+K_H) and height Y_1+2K_H

i) Similarly create C key rectangle starting at (X_i, Y_1+2K_H) and height Y_1+3K_H

Step 6: Create the Data section

i) Create A Data dumbbell as a contiguous shape using the 8 points A1 – A8

(X_{A1},Y_{A1}) (X_{A2},Y_{A2}) (X_{A3},Y_{A3}) (X_{A4},Y_{A4})
(X_{A5},Y_{A5}) (X_{A6},Y_{A6}) (X_{A7},Y_{A7}) (X_{A8},Y_{A8})

The points A1 – A8 are geometrically calculated using A_W, A_H, A_{CW}, A_{CH}

ii) B region is a rectangle defined by 4 points

ii) C region is a polygon similar to A defined by 8 points

Step 7: Reset the starting point X_1,Y_1 to $(X_1+2X_{OFFSET}+K_W, Y_1)$

Step 8: Print A, B, C polygons for fences and cells associated with each fence
Step 9: Print Powerplan definition in tcl format for Encounter

(b)

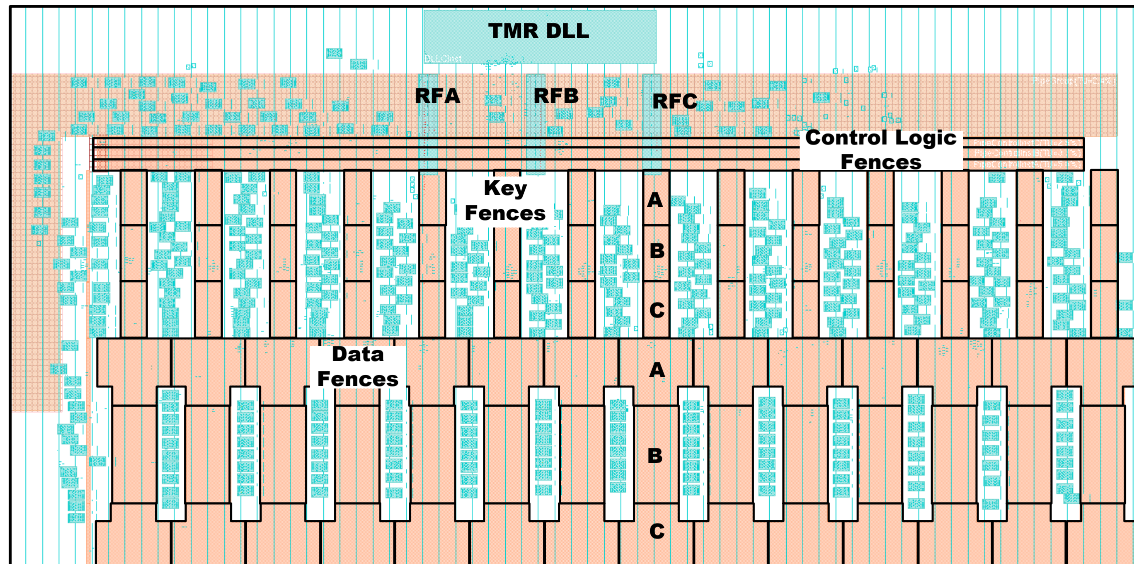
Fig 2.10 RHBD CAD module level separation using large fences, complete separation of custom, APR (combinational and clock) portions is achieved to create a DCE immune design.

the best routing and placement density within a given domain. The spatial separation flow

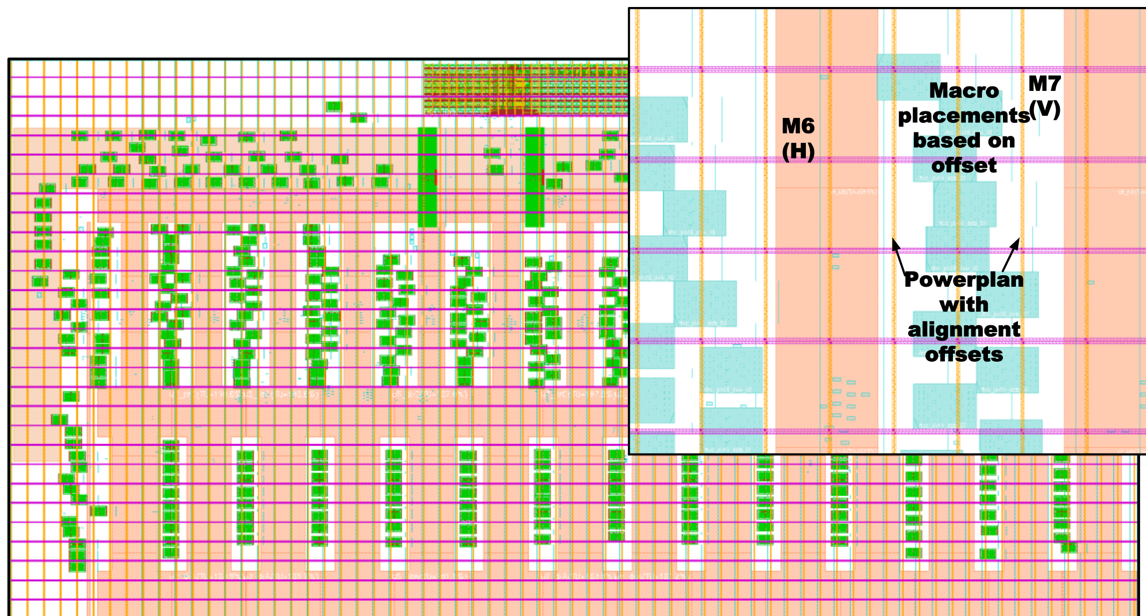
for domain separation begins after loading the synthesized design (Fig. 2.9). In the approach proposed in this work, the combinational logic domains are also separated using hard placement constraints, e.g., fences [Inno14]. Fences are contiguous regions that have a placement group, as assigned by the designer, associated with them. Only cells belonging to a particular group may be placed inside a given fence.

2.5.1. Fence Creation Flow

A Perl program provides arbitrary fence creation based on required region heights, widths and the number of stages in the pipeline. The fences obey power routing offsets for appropriate alignment to upper metal power gridding. The fence creation flow is visualized with the help of a concept diagram (Fig. 2.10(a)) and pseudo code (Fig. 2.10(b)). Each of the separate fences (one key and one data fence for a solitary pipeline stage) created can be visualized in Fig. 2.10(a). The steps numbered 1 to 9 in pseudo-code describes the high-level algorithm for large fences creation. Form factors for the fence were chosen based on signal dataflow and timing. The fences were iteratively sized based on APR experiments, comprehending placement, routing and pin congestion and timing results. The data fences are designed in the form of a dumbbell since the area between the subsequent stages can be used to place sequential pulse-latch macros. Key has twice the number of pulse-latches but smaller combinational logic hence the fences are designed with rectangular shapes so as to accommodate this fundamental change. Dataflow is from pipeline stage (U_0) to (U_{14}) and hence the fences are designed taking into account this basic flow of data and related input and output pin positioning (Fig. 2.11(a).



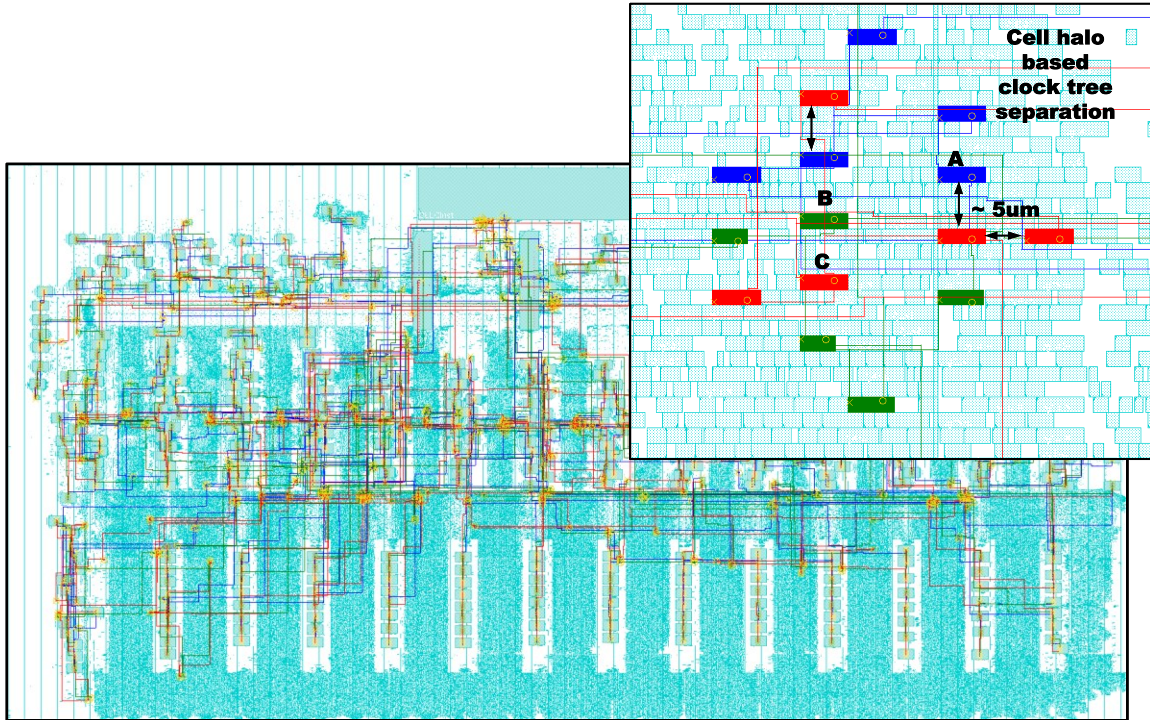
(a)



(b)

Fig 2.11 Timing waveforms of self-correction in the pulse-latch. C copy is corrected to 0 after 340.1 ps. B copy is corrected to 1 after 202.8 ps.

Placement and timing optimization are run on the large fences based floorplan and they are iterated to ensure that timing and placement constraints are met. Fig. 2.11(a) and



(a)

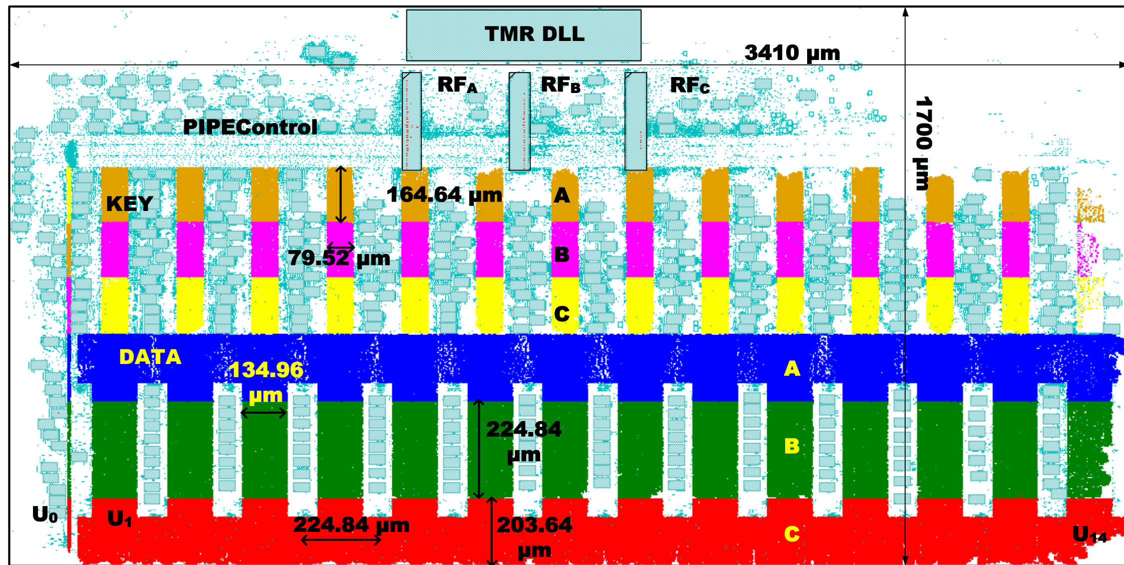


Fig 2.12 Timing waveforms of self-correction in the pulse-latch. C copy is corrected to 0 after 340.1 ps. B copy is corrected to 1 after 202.8 ps.

(b) show the creation of the large key and data fences and the custom power plan in the Encounter APR tool. Inset in Fig. 2.11(b) shows the offset and the metal usage for the

creation of the custom powerplan. As shown in the Fig. 2.11(b), the custom power plan allows the multi-bit latch macro to be placed between the stage fences without conflict between latch power stripes and power plan mesh on metal 6 and metal 7.

Placement of the pulse-latch macro is shown in relation to the fences and the powerplan. The first stages (u0_dr, u0_kr) of data and key have fewer cells associated with them. Stages 1-14 are about the same size due to the uniformity in the number of cells associated with each group. Control logic which is also TMR'ed is also separated in their respective rectangular fences along the encryption pipe (data and key) hierarchy between the register file macros and the encryption pipe fences.

2.5.2. Clock Separation Using Clock Cell halos

The clock tree synthesis connects the innumerable sequential elements in the design and has to do so optimizing the latency and minimizing the skew between interacting clocks. The clock tree synthesis algorithm does not honor the fences and hence tends to introduce a substantial soft-error vulnerability to DCEs. To separate the clocks' cells, halo options of the CTS engine were used to separate the clock tree cells by at least 5 um in the design. Fig. 2.12(a) shows the design with the three clock trees A, B and C highlighted with the blue, green and red colors, respectively. Inset shows the clock tree cells of the same color coding separated from each other by the said spacing. Cell halos ensure complete domain separation in combinational and clock tree cells, the sequential custom cells already having been separated.

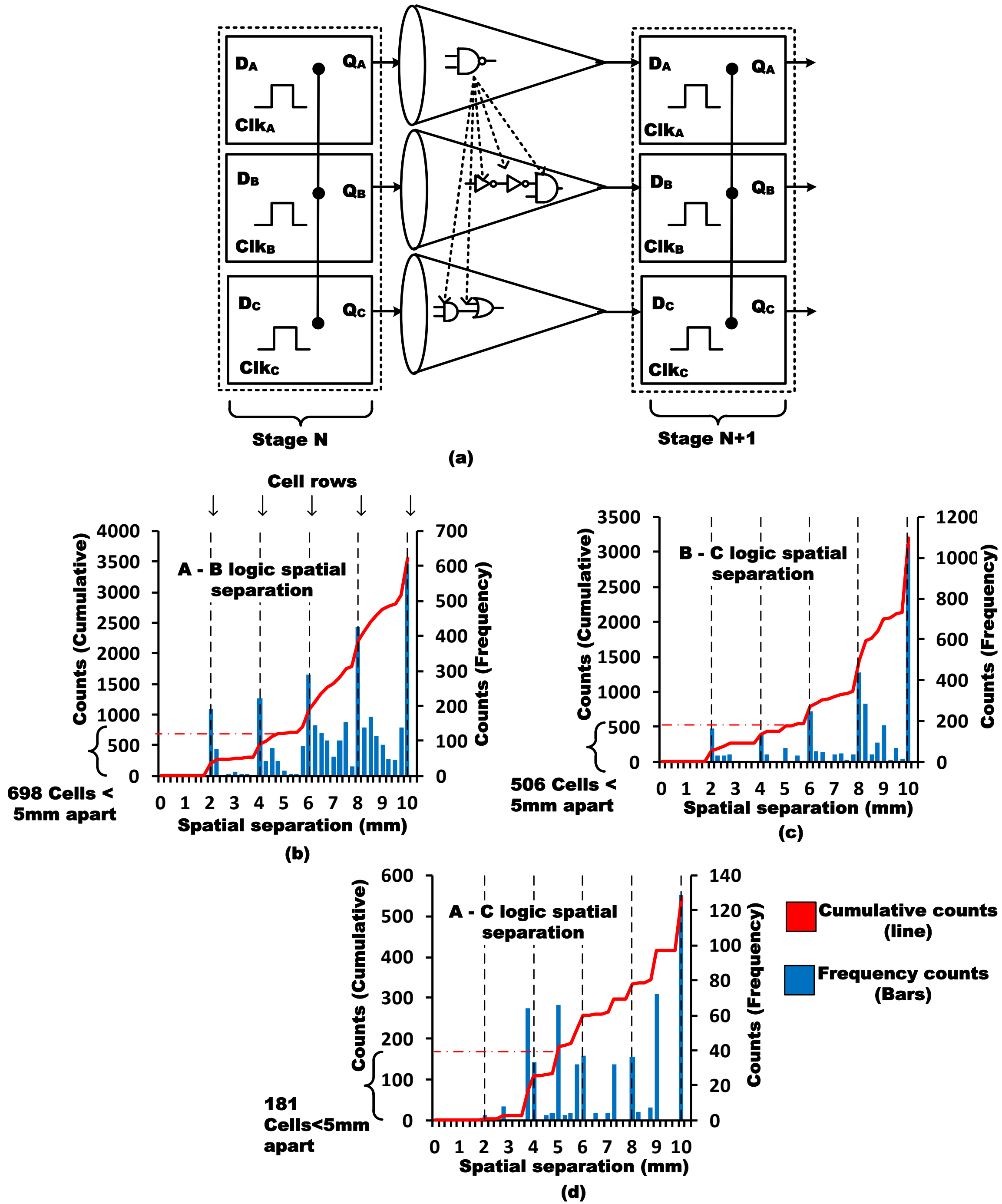


Fig 2.13 (a) Schematic representation of separation analysis, Analysis histograms in (b) AB, (c) BC and (d) AC of cell separation comparison for the design pipeline shows very few pairs placed without adequate separation.

Fig. 2.12 (b) shows the domain separated key and data encryption pipe hierarchy highlighted. Other macros used by the AES engine such as register files (RFA, RFB and

RFC) and a DLL macro are used for providing internal clocking (if necessary). A, B and C domains of the data and key logic are completely separated. The efficacy of the separation will be studied in the analysis sections.

2.6. Spatial Separation Analysis

Spatial node separation in redundant copies provides the mitigation of DCEs. To determine the spatial separation between domains that was actually achieved, the distance between every cell in each logic cone driving one TMR pulse latch copy (e.g., domain A) and all cells in the corresponding logic cones of the redundant copies (e.g., domains B and C) were determined from the layout database (Fig. 2.13(a)). Any two cells with a physical distance of less than 10 μm from redundant copies that fan-in to the same TMR pulse-clocked latch were recorded.

Fig. 2.13(b-d) shows the results from one typical (7th) pipeline stage. In the A-B logic group pairs with more than 278 M cell pairs, only 698 or 0.00025% of the total possibilities, are within 5 μm. The B-C logic cones had 506 (0.00018%) and A-C cones had 181 vulnerable cell pairs of 278 M and 284 M total pairs, respectively. The vast majority of these vulnerable cells were signal buffers placed outside their respective fences during optimization, a consequence of the centralized TMR latch placements. The A copies and C copies have more buffers, which were placed near B buffers in some cases. Many such cells were found clustered at even spacing of standard cell rows as evident in the figure.

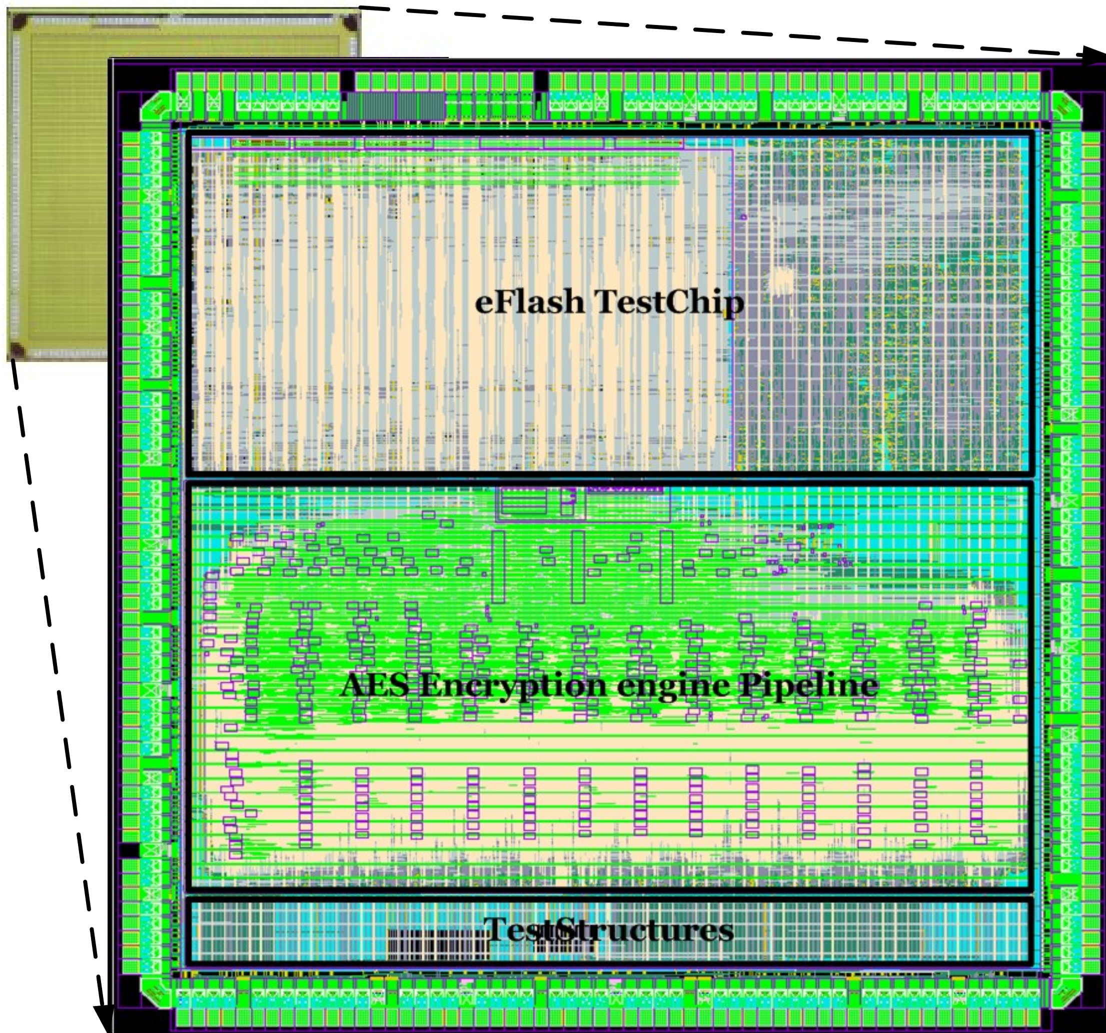


Fig 2.14 AES implementation on a 4 by 4 mm die on a 90 nm process, The AES design is marked along with other structures in the test chip. Wire bond I/O pad ring consists of 211 I/O's

It can be inferred that the overall cross-section due to these placement oversights is small, as the impinging radiation track must have the correct angle and depth to affect both. Nonetheless, the flows have since been modified to place signal and clock buffers inside respective fences, thereby eliminating this issue.

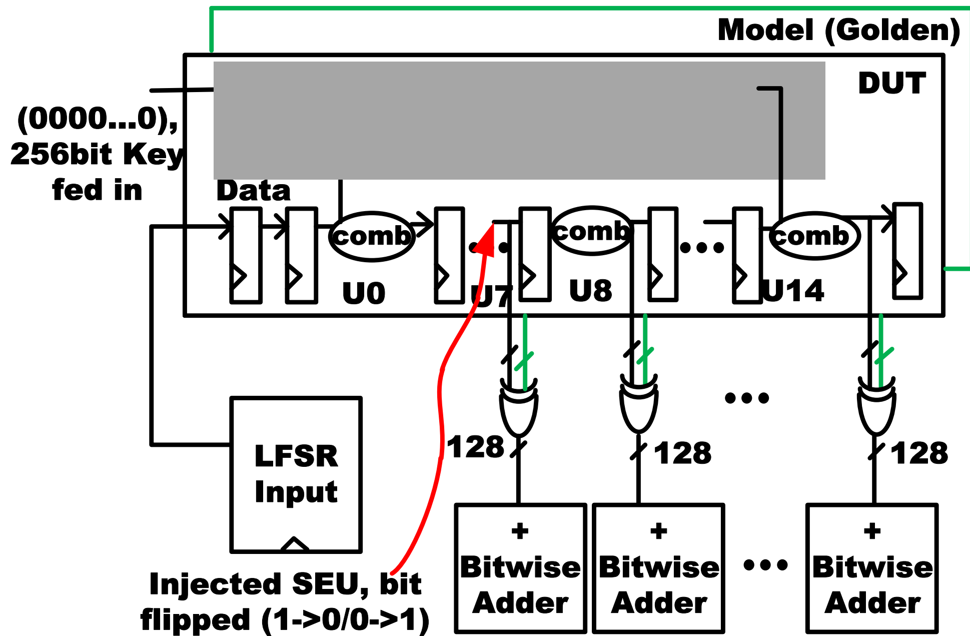
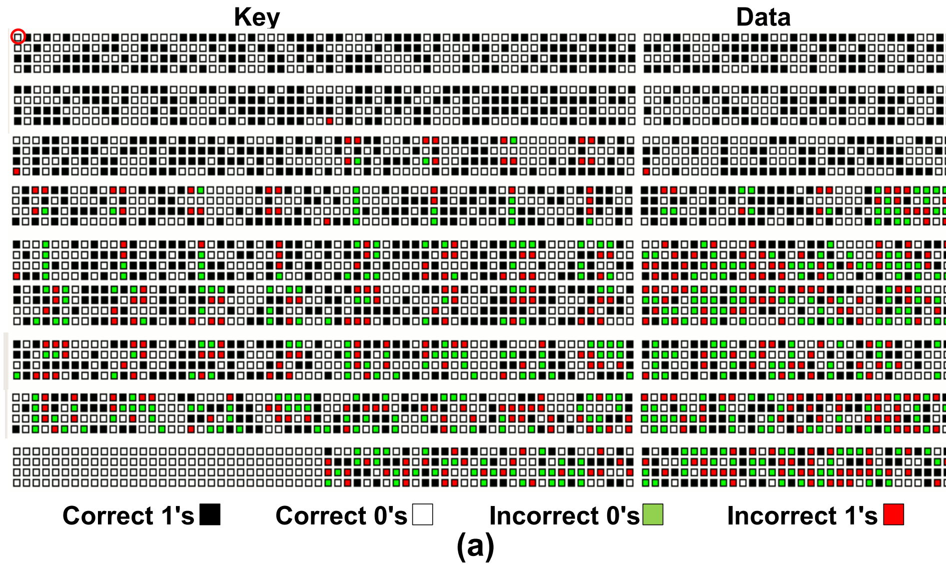


Fig 2.15 Error injection simulation test setup. Model and device under test are shown. Error is injected at the 8th stage and subsequent stages are observed for error propagation. LFSR generates the inputs data bits and the key is constant.

2.7. Test Chip Implementation

The AES block is implemented in a 90 nm LSP process on a 4×4 mm die (2.14). The total area of the AES block is 5.71 mm^2. No effort was made to provide high density outside the primary AES pipeline regions. The other circuits are top-level control and testability features. Overall placement densities of the pipeline fenced A, B and C domains are 64%, 64% and 65%, respectively. TMR register files (labeled RF_A, RF_B and RF_C in the Fig. 2.12(b)) provide control, data, and configuration information, including driving the test mode signals. I/O pad ring consisted of 211 pads which communicate with the 3 separate blocks. AES design has 111 I/O signals which are connected to the FPGA through a chip on board setup. Sufficient power and ground pads were added to ensure minimization of



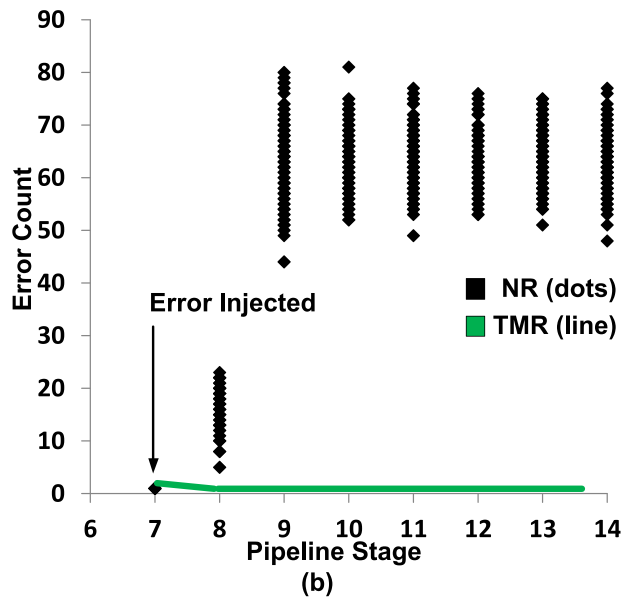


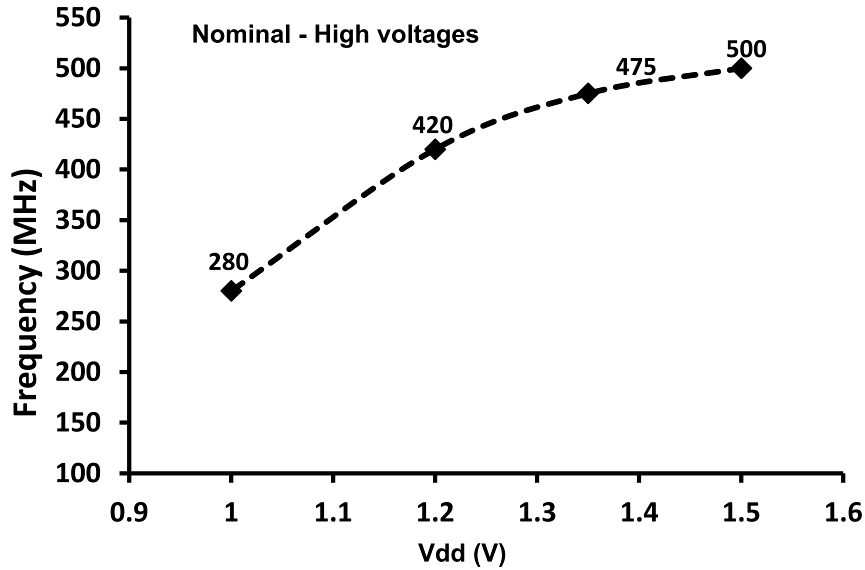
Fig 2.16 (a) Non-redundant AES error injection graphical representation using Perl. Reds are incorrect 1's and green are incorrect 0's, correct 1's are in black and 0's in white. (b) Error count per pipeline stage plot showing correction capability of TMR (light blue) version and the error diffusion in non-redundant version (black).

ground bounce and supply voltage sag based on maximum instantaneous current requirements of the design.

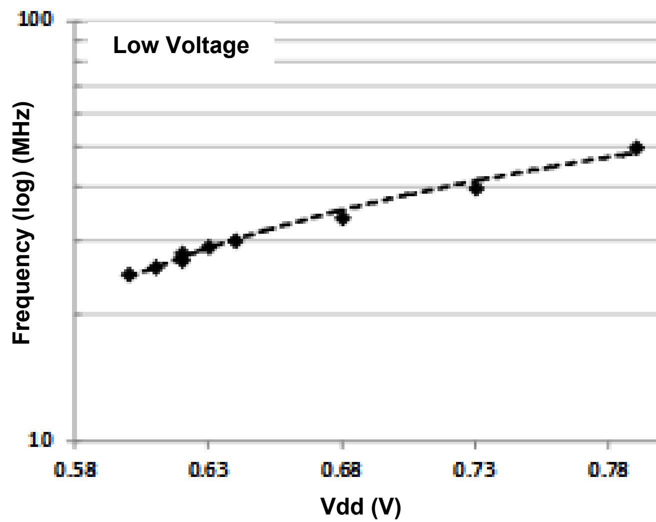
2.8. Error Injection Simulation Validation

The Verilog gate level implementation was simulated in the non-redundant and TMR modes to determine the TMR scheme efficacy in mitigating soft-errors. The test bench instantiates both the device under test (DUT) and the model (golden reference). The test bench checks the output of each pipeline stage against the golden reference, while upsets are systematically injected into the DUT. Bitwise adders that register the fail count at each stage determine the total propagating error count for each injected error (Fig. 2.15). For example, an error is injected at one of the 7th stage pipeline latch outputs and observed in subsequent pipeline stages. Comparing the TMR hardened or unhardened DUT allows comparison of the responses.

No errors propagated in the TMR mode, proving the efficacy of the self-correcting TMR pulse-clocked latches. The resulting error diffusion in the unhardened mode comprises Fig. 2.16 (a) for one example upset. A single bit error is injected into the key pipeline, and the data and the key pipelines are observed. Color coding of the correct and incorrect bits show the resulting error propagation, burgeoning due to the diffusion properties of the AES algorithm to affect about half of the bits. Fig. 2.16(b) shows the statistics of the error diffusion and propagation in both the hardened TMR and unhardened non-redundant mode. No errors propagated in the TMR mode proving the efficacy of the proposed scheme and design flow.



(a)



(b)

Fig 2.17 (a) Measured test chip FMAX vs. VDD at high operating voltages. The upper values are measured using the PSU mode, (b) Measured test chip FMAX vs. VDD at low operating voltages.

2.9. Experimental Setup and Silicon Validation

The design is fabricated on foundry 90 nm LSP process and packaged as a chip-on-board (COB) with the device under test (DUT) board soldered to the main board to achieve

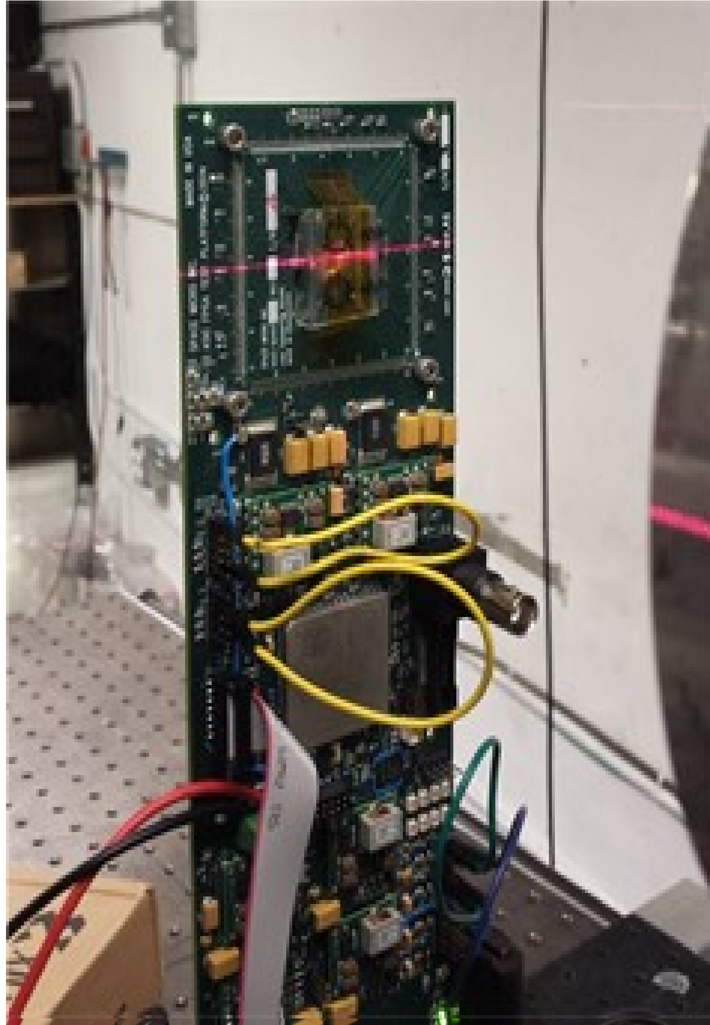


Fig 2.18. Broad beam testing setup at UC Davis. The COB DUT is shown at the top. The controlling FPGA is at the bottom, away from the beam track.

small bond-wire inductance. This allows the foundry supplied standard CMOS I/Os to operate at a maximum frequency of 167 MHz with a 2.5 V I/O voltage. The DUT is coupled to a Xilinx Kintex 7 FPGA for testing. Running the design in AES counter mode meets 10 Gbps throughput through the 64 bit input and output buses at this speed. Internal throughput is much higher and is indicative of the performance in an embedded application where off-chip bandwidth is not limiting.

The pipeline stage unification (PSU) mode allows testing the circuits at faster speeds despite the I/O limitation. It is used to determine the non-PSU effective maximum frequency of the design. Collapsing two stages doubles the stage delay, equivalent to testing the design at twice the frequency. Since the pipeline stage delays are nearly identical, the as-fabricated delays can be accurately determined without higher speed clocks and I/O. Collapsing to groups of four pipeline stages shows a fully pipelined effective maximum frequency of 500 MHz with core VDD = 1.5 V (Fig. 2.17(a)), providing an equivalent throughput of 64 Gbps. The foundry supplied I/O drivers (presumably the level shifters) limit the core VDDMIN to 570 mV (Fig. 2.17(b) even at a reduced I/O voltage of 1.8 V.

2.9.1. Proton Broad Beam Testing

The AES prototype was soft-error tested using 63 MeV broad beam protons at the cyclotron at UC Davis (Fig. 2.18). A proton flux of up to 8.92×107 particles/cm^2-s was used with a total fluence of 3.11×1011 protons/cm^2. A total of 32 errors were observed for the non-redundant mode with the design running at 120 MHz. No errors were observed in the TMR mode at any speed or voltage.

Small error counts here result from limited test time. However, Ladbury shows that for a 95% confidence limit, the error bound decreases rapidly as the event count 'N' for each cross-section point increases [Ladb07]. Above 16 events this decrease is minimal. The bound decreases roughly as the inverse of the number of events on which the cross-sections are based. For the 32 errors we see in the unhardened mode, the possible error is √N (~6), i.e., 17.6%. Using an error bounded (worst-case), we would see 26 errors and

Table 2.i Design Metric Comparison of the Proposed Implementation to Standard Flip-flop and Temporal 4CE FF based Designs.

	Proposed Design (TMR Pulse-Latch)	Standard Flip-flop	Temporal FF 4CE [Sham15]
Area (um2)	2028897	2880865	1035287
Timing (MHz)	408	420	317
Power (mW)	314	453	213

assuming one error was seen in the TMR testing mode (since no statistics can be inferred from 0), we estimate a cross-section improvement of

$$\sigma_{reduction} = \left(1 - \left(\frac{1}{N - \sqrt{\mathrm{N}}}\right)\right) * 100 \tag{2.1}$$

Using this approach, we calculate that our design cross-section is reduced by at least 96%.

2.10. Design Comparison

We compare the proposed design with standard flip-flops and a temporally hardened (4CE) flip-flop [Sham15] in Table 2.I. Power, speed and area metrics are compared. 4CE is a temporally hardened flip-flop using delay filters. It has an area overhead of 2 delay elements per flip-flop, which is equivalent to that of the DF-DICE design. This delay overhead increases the setup time of the flip-flop, thereby limiting the maximum frequency achievable in the design. Also compared is an AES design with standard foundry flip-flops in TMR arrangement with a majority gate and triplicated combinational logic.

The area of the standard flip-flop based implementation is 1.41 times that of the proposed implementation. The speed of the flip-flop based design is essentially the

same at 420 MHz. This design is not self-correcting, as the flip-flop feedback is not interconnected. The slight speedup using conventional flip-flops is attributable to their more flexible placement. However, the area penalty is substantial for a less hard design.

The non-redundant temporally protected 4CE flip-flop based design is 0.51 times the size of our TMR pulse-clocked design but has a maximum clock frequency of 317 MHz due to the increased temporal flip-flop setup time. Power dissipation for the proposed design is 314 mW. The flip-flop based design and the 4CE temporal design are 1.44 times and 0.67 times the power of our proposed implementation, respectively. Accounting for the difference in frequency, the energy per operation saved by the 4CE design is only 13%. This is due to the high power cost of the delay circuits and 100% activity factor operation. Moreover, the TMR design is hard to any SET duration, while the temporal flip-flops are not.

Thus the pulse-clocked latch affords a saving of ~30% power and ~31% area overall compared to flip-flop based implementation at almost the same speed. The comparison of the same metrics with 4CE shows that the proposed design is faster than the temporally hardened flip-flop with increased power. The temporally hardened design cannot correct the errors during operation and only filter the SET's mitigating SEU.

2.11. Summary

This chapter described the module level separation methodology for TMR pipelined designs. A pipelined AES was chosen to implement the domain separation circuit techniques and CAD methodology. Pulse-latches were chosen as the sequential element of choice allowing high-speed operation and test-modes for single pipeline testability. CAD methodology separation efficacy for both combinational and clock tree logic is proven with

nodal-spacing summary which showed minimal critical pairs of adjacent cells belonging to different domains. Logic simulations prove the functionality of the AES in both redundant and non-redundant modes while demonstrating the error diffusion in the AES pipeline. The proposed CAD methodology is used to implement the AES pipeline in 90 nm LSP process and silicon results prove functionality and speed of the implemented design. Beam testing results show 0 errors observed in the TMR mode and 32 errors in the non-redundant mode of operations. A silicon proven design with complete separation of sequential and combinational logic domains through custom design for the pulse-latches and APR based domain separation for the combinational portions demonstrates the validity of the proposed methodology. The next chapter will showcase the improved redundant and non-redundant co-design methodology for complex architectures such as the radiation hardened processor (HERMES2).

CHAPTER 3. INTERLEAVED SEPARATION: HERMES

3.1. Introduction

Chapter 2 explained the module level separation methodology for pipelined designs with an advanced encryption standard design as a case study. Chapter 3 explores improved high density placement and routing interleaved fences for placement of TMR logic and the ReAPR co-design methodology. HERMES2 radiation hardened microprocessor is implemented using the proposed APR methodology on a 55 nm process. The processor is hardened by micro-architectural techniques and software based error-recovery. DMR speculative pipeline and TMR architectural states ensure soft-error mitigation. The ReAPR CAD approach provides critical node separation at the domain and/or module level. The separation provided by the methodology has been proven on silicon using broad beam testing with heavy ions, protons and neutrons. The methodology cleanly supports block by block hardening, where a given RTL IP block can be hardened with n-module redundancy (where n = 1, 2, or 3). The flow leverages commercially available CAD tools, resulting in high quality implementations and allows mixing hardened and unhardened portions having different redundancy schemes, e.g., none, TMR, or DMR. The results have minimal circuit timing and design cycle time impact, while providing the best possible SE immunity. Error injection simulations and beam testing of test chips fabricated using the automated flows provides SE mitigation validation of the proposed APR methodology.

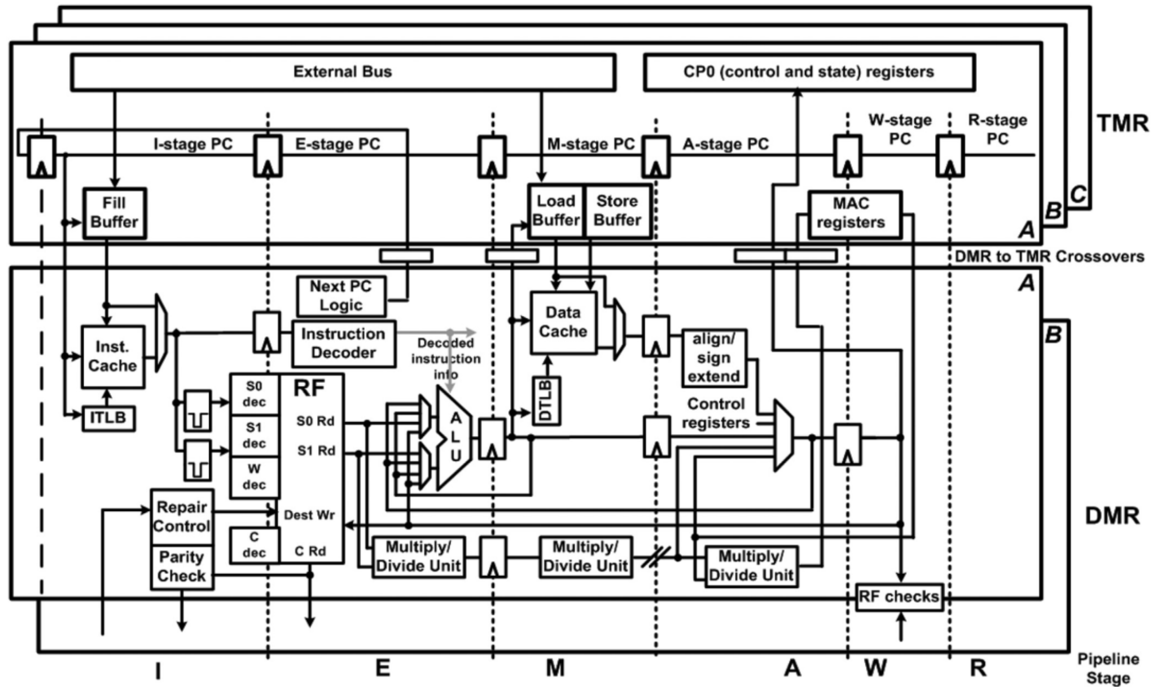


Fig 3.1. HERMES2 architecture block diagram of a 6-stage with the speculative DMR pipeline and the architectural TMR architectural states. DMR to TMR crossovers logic is also shown (also implemented in TMR)

3.2. HERMES Background

The High Performance Embedded Radiation Hardened Microprocessor Enabling Spacecraft (HERMES2) processor core is the test vehicle for the proposed ReAPR methodology [Farn15]. It is a clone of the MIPS 4Kc core with a modified micro-architecture that supports DMR speculative pipeline and TMR architectural state. The speculative DMR copies are compared for agreement before commission to architectural state. Cache, Register-file (RF) and memory-management unit (MMU) are also protected by DMR. A write through policy invalidates the cache when errors are detected. The DMR RF is repaired using parity via software controlled instruction restart. Architectural state, e.g., program counter (PC), write buffers, configuration registers and the bus interface are

protected by self-correcting TMR combinational and sequential circuits. Clock tress are also TMR providing complete domain separation, although the DMR portions dominate in the overall design cell area. TMR clocks allow extensive clock gating and the use of standard APR clock synthesis for minimal clock-skew and low power.

The HERMES2 processor core therefore proves to be a complex test vehicle for the proposed ReAPR methodology, with both TMR and DMR portions with hard macros and standard cell (sea of gates) logic.

3.2.1. Error Detection and Recovery

Soft-error recovery is software based and allows the programmer complete control over the recovery process and error reporting. Error reporting can be simple to complete machine state dumps for error debug and root cause diagnosis. At commission to architectural state, the DMR data from A and B pipelines are compared and an exception is triggered based on the mismatch of the copies. Instructions added to the MIPS instruction set i.e. invalidation and repair instructions are then used to repair the processor state guided by the SE exception handler. Both RF data and addresses are checked before a load operations and any mismatches resulting from cache errors are caught during writes to RF. Address and decode errors that are uncorrectable by EDAC in standard caches, are also protected by the DMR scheme. With full DMR caches, cache specific SE checkers are not required. This change greatly improves portability. Since the data cache is write-through there is always a correct copy in the main system memory. The RF compares DMR data before write operations. DMR to TMR crossover data is also checked before commission to the architectural state.

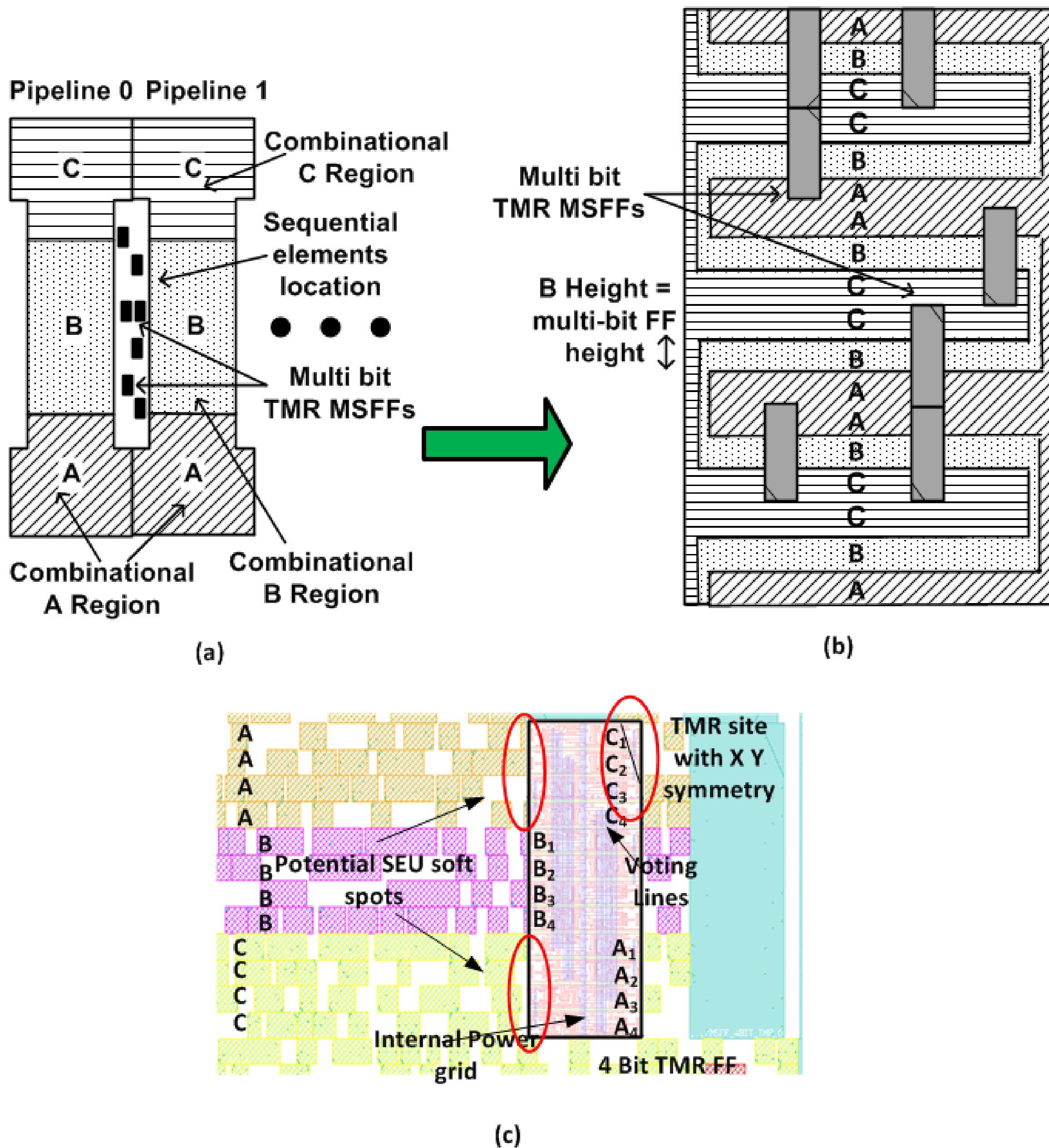


Fig 3.2. (a) Large fence module separation diagram representation (b) Interleaved fence diagram representation with A, B and C fences (c) Sequential and combinational domain mismatch if the fence and the TMR site definitions are not aligned in the interleaved fences creating potential SE vulnerabilities.

The HERMES2 microarchitecture has added co-processor (CP0) registers and instructions for additional soft-error related architecture extensions. Error log and Error mask registers are added for error logging or discrimination and error masking,

respectively. Errors at DMR to TMR crossovers for instruction fetch, load/store, multiply-divide, and instruction execution can be discerned in the RF DMR WWL. Writeback data mismatches, and scrub/repair port data read parity errors are registered based on the error log registers (1 & 2). The SE EPC CP0 register stores the program counter (PC) to return to after a soft-error exception. RF data and address backup registers store the RF entry and value that was over-written by the instruction that triggered the DMR mismatch.

Special instructions are added for rapid error handling and architectural state repair. The back up register file (BURF) instruction restores the RF state to that before the erroneous instruction. Subsequently, the repair general purpose register (RGPR) instructions can be used to repair any SEUs in the DMR register file. DMR copies of a given RF location are compared and 5 bit groups with parity errors are overwritten by the redundant group with correct parity. Single cycle JTLB and cache invalidation instructions have been added as TLBINV. Other added instructions allow non-redundant register files and cache reads and writes with and without parity for data examination and error validation, as well as, testing of the SEE detection logic. Other instructions specifically test data (read or write) or parity state independent of the repair mechanism.

3.3. Improved Interleaved Separation

3.3.1. Need for Fine Grained Separation

The large fences flow described in chapter 2 showed excellent domain separation, but at the cost of lowered cell and increased routing utilization. To address the need for domain separation with increased cell and routing density, the interleaved fences flow was devised. This flow becomes the basis for the ReAPR co-design CAD methodology as we

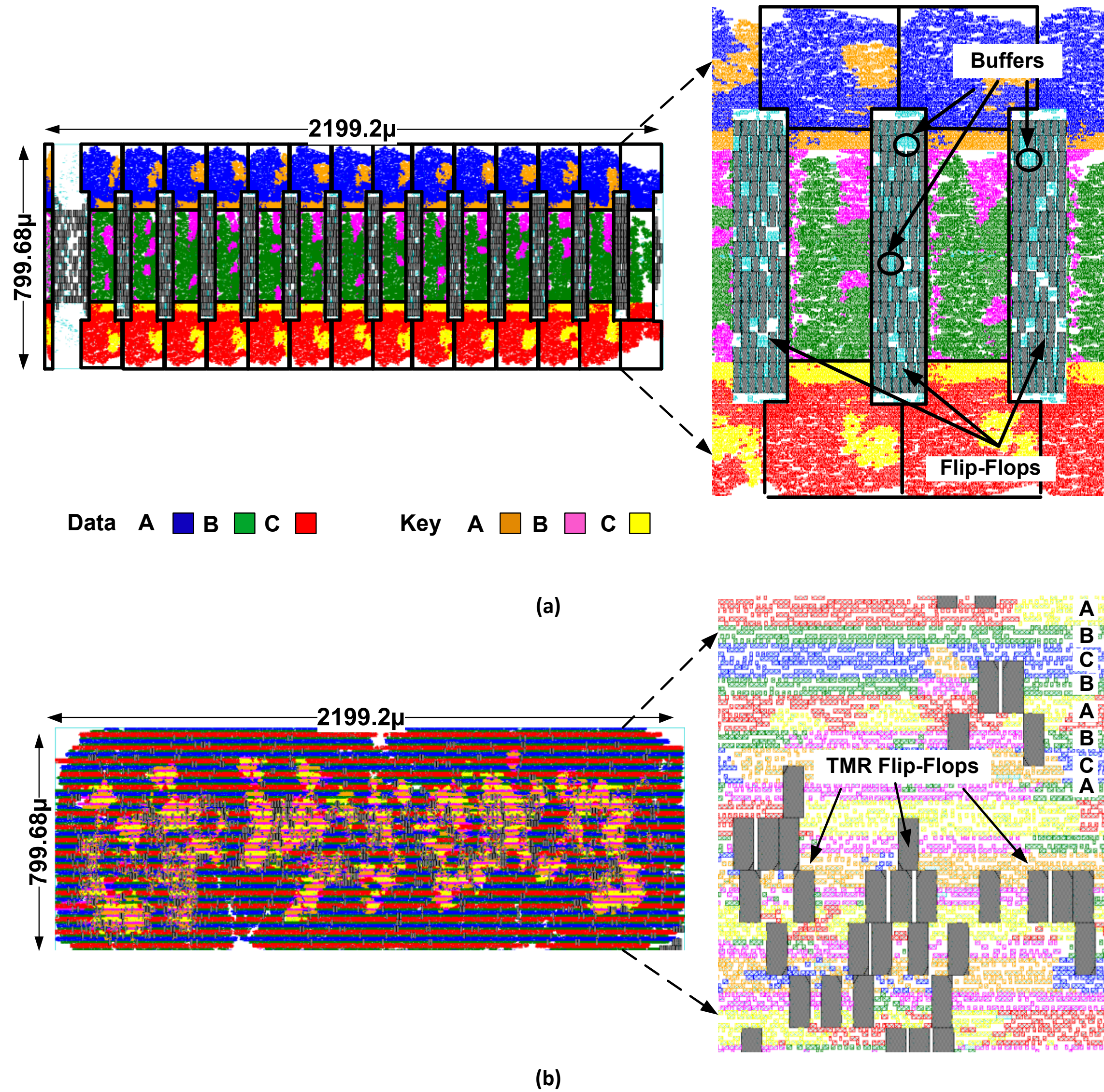


Fig 3.3. AES implemented at 250 MHz speed in (a) Large fence module separation with key and data fence (b) Interleaved fence encounter representation with key and data mixed in the A, B and C TMR domain fences. Color coding pertaining to key and data A, B and C domains is shown. Both designs are implemented in the same area with the same flip-flops to ensure proper apples to apples comparison

will see later in this chapter. Fig. 3.2 showcases the evolution of interleaved serpentine fences. The large fenced methodology which consists of large rectilinear shapes for module level placement of redundant logic are showcased in chapter 2. We devised interleaved A, B and C fences in a repeatable ABCCBA pattern to ensure placement of domain separated

Table 3.i: Dumbell (large fences), Interleaved Fences and Unhardened AES Design Metric Summary

Design Metric	Dumbbell	Serpentine	Unhardened
Cell Area (μm^2)	1065290	1117818	304897
Area (μm^2)	1758592	1758592	431043
Width (µm)	2199.12	2199.12	2199.2
Height (µm)	799.68	799.68	196
Timing slack (ps)	2	21	569
Clock skew (ps)	40.4	52.4	12.6
Clock buffers	729	879	199
Wire Len. (µm)	1097577	7840707	1413268
M2(v) (µm)	1926199	1638507	382702
M3(h) (µm)	2120882	2356154	575893
M4(v) (µm)	2779500	1541242	100192
M5(h) (µm)	1352172	1236133	288740
M6(v) (µm)	2371088	693780	12008
M7(h) (µm)	415445	369555	53732

logic at much higher densities than the base large fences flow. A single multi-bit flip-flop spans 3 fences and the height of the fence and the flip-flop match, ensuring the consistent domain adjacency of the flow. This ensures that unmatched combinational and sequential domains are not placed adjacent to each other, thereby introducing a placement MNCC vulnerability (Fig. 3.2 (c)). The domain relationship is maintained by ensuring the placement site orientation and the fences created span the same domain A, B and C.

3.3.2. Implementation Results

The AES design shown in chapter 2 was implemented at the same clock frequency of 250 MHz on a 90 nm bulk CMOS process for this experiment and comparison. The floorplans were modified to provide approximately the same overall cell area utilizations of 65%. The two full TMR designs were implemented in the same area. The fully TMR designs used 4 bit TMR self-correcting master slave flip-flops. This forces the B regions to be four standard cell rows tall. The regions are unconstrained, but to maintain equal areas, they are 8 cell rows tall. We have developed Perl programs to generate the fence geometries based on high level design parameters, e.g., overall area. Though cells must reside within their respective domains, the APR tool allows free movement, resizing and the addition of buffer during timing and routing optimization. This flexibility allows full performance, while reducing design effort. The resulting design implementations of the large and interleaved fences are shown in the Fig. 3.3(a) and (b), respectively. The implementation results are summarized in the successive sub sections.

3.3.2.1. Placement

The large fence design is 3.49 times larger than the unhardened version, of which 12% is due to buffering added by APR for timing optimization. The B domain contains 16% fewer cells due to its closer proximity to the flip-flops. The serpentine design is 3.67 times larger than the baseline, with 16% due to buffering.

While the total number of cells in both full TMR implementations are nearly equal, the large fence design has a much larger number of buffers (approximately 7,000) inserted

for the A and C domains. The flip-flop macro placements, as well as, color coded combinational logic placement comprises Fig. 3(a) and 3(b).

3.3.2.2. Routing Resources

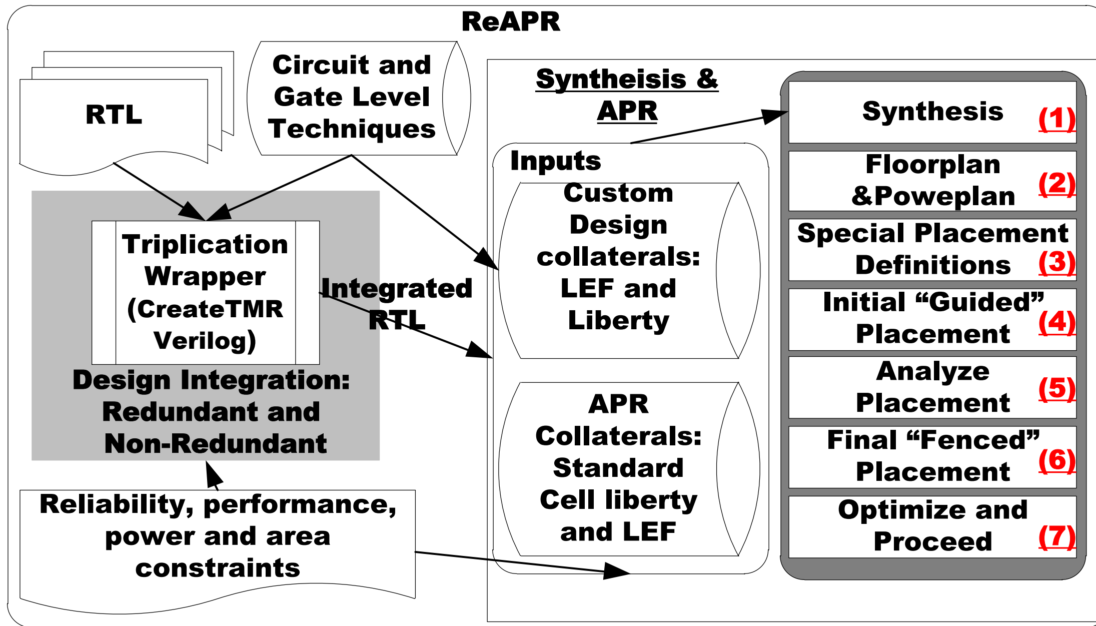
Referring to Table 3.I, the full TMR implementations increase total wire length 7.77 and 5.55 times the base unhardened design, respectively. Much of this is due to the larger area required. In [Matu10], it was pointed out that larger hardened flip-flops actually reduced routing density. The serpentine full TMR implementations has a routing density of 1.36 times over the baseline. Large fence design increases routing density almost 1.9 times. Thus, the serpentine fences while requiring, for instance, A domain logic to route over B and C domains more often, it still requires substantially less routing resources. Vertically oriented metals (M4 and M6) comprise most of the difference, due to the need for long routes from the A and C domains to reach the sequential cells placed in the center.

3.3.2.3. Clock Trees

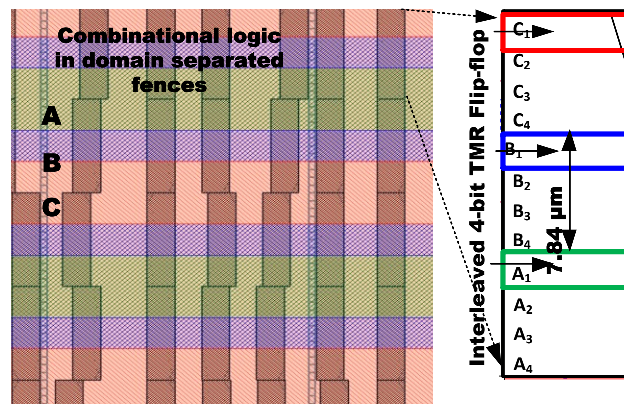
The unhardened implementation achieves 13 ps skew with 199 clock tree cells, driving 67% fewer cells. The large fence design has less skew and requires fewer clock cells. The serpentine geometry has 4.1 times the baseline clock skew and requires the most clock tree cells. This indicates that the sequential circuit grouping allows fewer local clock buffers and routing, as compared to the more dispersed flip-flops in the serpentine approach.

3.3.2.4. Power Dissipation

Active power dissipation measured with extracted parasitics for the unhardened design at 250 MHz is 58 mW. The combinational logic and clock tree power increases



(a)



(b)

Fig 3.4. (a) ReAPR flowchart with steps to create domain separated MNCC mitigated logic, required inputs and APR steps (1-7) are elucidated. Domain separated RTL is created by the triplication wrapper and synthesized Verilog is the output from synthesis (b) Domains provide MNCC induced SE mitigation. The multi-bit FFs straddle domains so the associated storage is in the same domain as combinational logic.

43%, owing to the larger area and tripling of the clock tree size. Sequential circuit (FF) power dissipation exactly triples, with the number of FFs, and all are minimum sized for this operating frequency. The large fence and serpentine methodologies increase the power

considerably, since they triplicate combinational logic and are thus, much larger. These designs dissipate 4.82 and 4.55 times the power of the unhardened baseline, respectively, approximately doubling the non-SET hardened designs' power. These results are in line with the routing and cell areas that contribute linearly to power dissipation.

The improvements in routing, cell density and reduction in power consumption as a result, proves the interleaved fences methodology is a substantial upgrade over the large fences methodology and become the integral part of the ReAPR co-design methodology.

3.4. ReAPR Co-design methodology

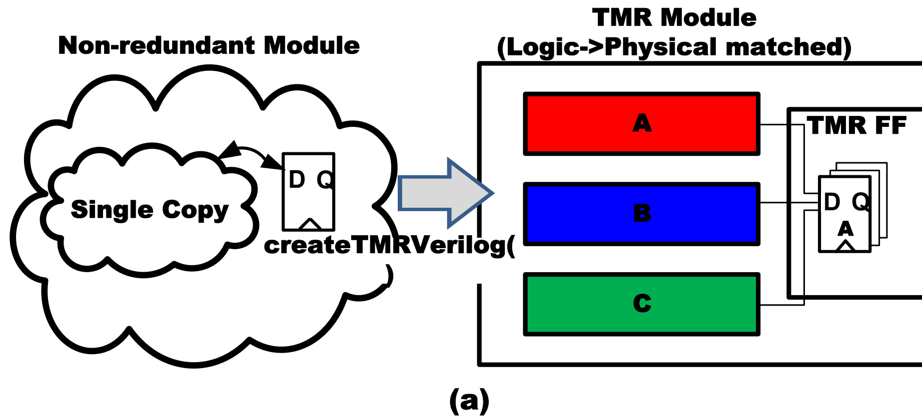
The methodology described in this chapter is correct by construction. Each standard cell is placed in its corresponding domain (A ,B or C) as will be described and proved in the later sections. This methodology ensures that redundant nodes belonging to the same logic cone, but situated in different physical and logical domains, cannot be upset by a single particle strike leading to a DCE. Figure 3.4 shows synthesis and APR flow steps, which constitutes the ReAPR flow for domain separated redundant design. There is some possibility of two gates being placed adjacent, but the cross-section presented is greatly reduced. Each domain is separated by using fences. The flow steps of the ReAPR methodology are listed in the pseudo code in Fig. 3.5.

All circuits are MNCC mitigated using spatial separation. As evident, in this example the three domains (A, B and C) are spatially separated and have a separation of three standard cell rows (6.48 µm separation in an LSP 65 nm design) (3.4 (b)). This spacing can be increased if a higher hardness metric is to be satisfied. This variable separation height constitutes the hardness metric addition to the standard PPA metric in the ReAPR flow. The flow assumes RTL containing redundant and non-redundant blocks

```
Re-APR Flow Steps
1: Procedure Floorplan and Powerplan;
a:   Define FP size, Power Mesh size and pitch;
b:   Place Hard Macros (RF and Caches) and well tap;
c:   Place block level IO pins;
2: Procedure Create Sites;
a:   Create default SITE with required orientation;
b:   Create TMR SITE with required orientation;
3: Procedure Create Fences;
a:   Define DMR fence size and location;
b:   Define TMR fence size and location;
c:   Create and load Integrated fence tcl file;
4: Procedure Create Groups and Assign Modules;
a:   Define groups A, B and C;
b:   Define keyword_A = {IEArchInterfaceC/cla, IFFillBufCInst/
cla, IEPCPipeCInst/cla, BICtlAdrDatCInst/cla  etc. }
c:   Define keyword_B = { IEArchInterfaceC/clb, IFFillBufCInst/
clb, IEPCPipeCInst/clb, BICtlAdrDatCInst/clb etc. }
d:   Define keyword_C = {IEArchInterfaceC/clc, IFFillBufCInst/
clC, IEPCPipeCInst/clc, BICtlAdrDatCInst/clc  etc. }
e;   foreach $Module {
f:     if $modulename contains keyword_A
g:       Assign $module to GroupA
i:     if $modulename contains keyword_B
j:       Assign $module to GroupB
k:     if $modulename contains keyword_B
l:       Assign $module to GroupB }
5: Procedure Initial Placement;
a:   Place design with soft "Guides";
b:   Unplace combinatorial cells;
c:   Fix sequential TMR cell placement;
6: Procedure  Fenced Placement;
a:   Convert soft "Guides" to hard "Fence";
b:   Place standard cells in TMR Fences;
c:   Analyze placement and get unassigned cells;
7: Procedure  Optimize;
a:    Optimize preCTS max_tran, max_cap, setup.
8: Procedure  Clock Tree Synthesis;
a:    Synthesize clock Tree and optimize postCTS.
9: Procedure  Route Design;
a:    Route Design and Optimize PostRoute.
End
```

Fig 3.5. ReAPR flow place and route steps described in a pseudo code, with the specific domain separation related steps and subroutines post RTL integration and synthesis.

defined at the module level. This is essential, because the flows integrate logic redundant blocks at synthesis. To integrate the self-correcting multi-bit TMR FFs, the TMR module interfaces are triplicated. Multi-bit FFs straddle domains, so each portion of the FF has the storage domain consistent with the surrounding logic.



(a)

Algorithm: CreateTMRVerilog

1: Input: Verilog ($Modulename);
2: Create TMR_CL(A,B & C) and Top_$Module verilog files;
2: Query $instance and $portnames **; //** Create lists of instance and port names
3: If (cellname($instance)==*MSFF*) // Sequential cell found
4: Foreach $instance {
a: **convert** $instance to TMR_MSFF* cell // SR to TMR cell
b: **create** (A,B & C) $instance pinnames and (A,B & C) portnames for Top_$Module ;
c: **create** (A,B & C) wirenames for Module Top_$Module;
d: **create** Interface connections of $instance to ports and wires;}
5: **If (cellname(**$instance)==!*MSFF*) // Combinational cell found
6: **Foreach** $instance {
a: **Foreach X** (A B C) {
a: **create** $instance_X in TMR_clX; //A, B & C Instance
b: **create** $instance_X pinnames and Module TMR_clX portnames; // Pin and Portnames creation
c: **create** wirenames_X for Module TMR_clX ;
d: **create** Interface connections of $instance to ports and wires in Module TMR_clX ;}
7: **Create** instances of TMR_clA, TMR_clB, TMR_clC in Top_$Module ; // Instances of TMR modules in Top Module
8: **Create** Interface connections of TMR_clA/B/C in Top_$Module;
h: **END**

(b)

Fig 3.6. (a) Diagrammatic representation of the TMR Verilog creation with physical domain matched to logical hierarchies (b) Pseudo Code for Creation of TMR Verilog by triplication of non-redundant Verilog. Output Verilog is instantiated to create integrated RTL/Verilog design.

A key limitation of commercial APR tools is the requirement that domains be contiguous. To ensure this, we interleave the domains. Thus, in the case of a mixed design such as HERMES, the TMR logic portion is included in the A, B, and C domains, DMR

the A and C domains, and single-redundant only the B domain. This domain re-use allows the APR tools full freedom in placement except for the domain, allowing timing improvement at the interfaces between redundant and non-redundant logic. The choices are made to balance the clock trees as much as possible. Therefore the flow incorporates the added design metric of soft-error reliability into the traditional EDA flow power and PPA metrics. The critical node separation and actual domain shapes and sizes are up to the designer as determined by the data flow and chip floorplan.

3.4.1. Logical Mmodule to Physical Domain Assignment Algorithm

To create domain separated logic as described in the previous sections, the design RTL/Verilog has to be converted to a redundant Verilog. The ReAPR flow triplicates logic using the CreateTMRVerilog wrapper. While running various experiments with APR on redundant logic and fenced domains, we realized that the APR tool adds logic or resizes the existing logic for the optimization of speed, power and area. This logic addition can be in logical hierarchies or modules outside of the redundant domains being implemented and hence, creates potential placement MNCC vulnerabilities by having cells in the design not honoring fenced placement. To fix this limitation of the APR flow, we incorporated complete logical separation of the design at Verilog level using the createTMRVerilog wrapper where the logical modules are perfectly matched to their physical counterparts (fenced domains). Thus, each triplicated module consists of A, B and C logical hierarchies that cannot be modified throughout the design process, ensuring completely domain separated placement.

The pseudo code for the createTMRVerilog wrapper is described in figure 3.6 (b). The non-redundant Verilog in question is parsed and the sequential and combinational cells

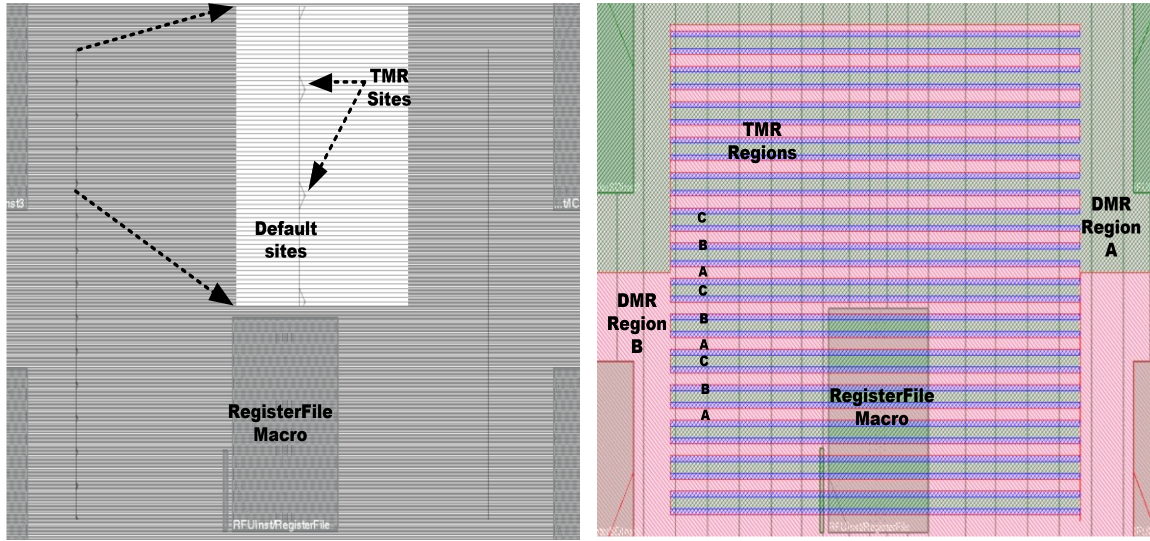


Fig 3.7. (a) 4 (a) Site definitions for multi-height TMR cells and default cells. (b).Guide generation in the APR environment, TMR and DMR guides can be seen colored in red (A), blue (B) and green (C).

in the input Verilog are triplicated by converting the interface wires, I/O ports and cell pin names to their A, B and C versions, respectively. Three unique module definitions are created and the combinational cells belonging to each domain (A, B and C) are assigned to the respective modules (*cla,*clb and *clc). The TMR sequential cell is mapped to the single/multi-bit version of the TMR cells and the interfaces are created to map the sequential cells to each redundant domain (A, B and C). This assignment allows the APR tool to assign individual modules rather than cells. This assignment mitigates any module level vulnerabilities due to tool optimization.

The TMR design can be integrated with other DMR and non-redundant RTL/Verilog to create the design RTL. The design RTL is then synthesized on a target technology with standard cell and custom (Cache and Register-File) liberty (timing abstraction) files. Thus, the ReAPR flow allows the use of bottom up or top down methodologies such that hard macros (lib, lef based) or hierarchical partitions can both be

defined using the same. This design is a bottom up example with custom caches and register files.

3.4.2. Site Creation

Post synthesis, an appropriate floorplan is determined based on chip area, routing track utilization and power budget. Well tap cells for n and p-well-bias voltage connections. Step 2 creates separate sites for standard cells and the multi-bit flip-flops. The former must coincide with the fence placements, as the domains must align. These placements are automatically generated together. Figure 3.7 (a) shows the sites created for the purposes of redundant-domain separated placement. Default placement sites and the TMR sites are shown. Specific arrangement of the sites and their orientations ensure that no domains are placed erroneously juxtaposed to a misaligned domain of the TMR sequential element. TMR sites are only defined in the center, since the TMR flip-flop cells are clustered in the center of the floorplan, thereby minimizing area. This improves TMR domain utilization, critical timing and minimizes routing congestion.

3.4.3. Domain Placement Guide Creation

Once the sites have been created with the proper orientations, regions are created to place combinational domains A, B and C, separated by 4 standard cell heights. A Perl wrapper creates the guide/fence definitions based on the size and location of the TMR and DMR regions in the floorplan. Guides are soft placement constraints and can be violated. This run provides a seed for the TMR flip-flop placement based on data flow and timing slack. This corresponds to step 3 in the flow (3.7(b)).

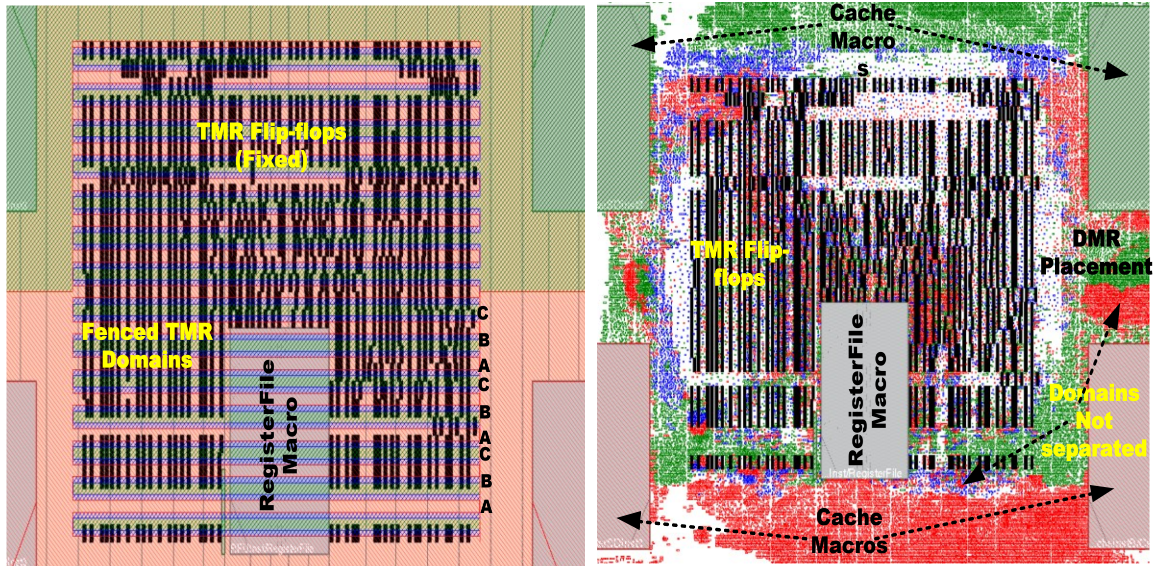


Fig 3.8. (a) Guided initial placement, TMR flip-flops are placed in the correct TMR sites. TMR and DMR combinational logic is placed based on data flow and timing, but not domain separated, (b) TMR flip-flops are fixed and the guides are converted to fences before the fenced placement run step (6).

The Perl wrapper creates an output tcl file to be loaded on the APR tool to create the contiguous domains. The TMR domains are arranged in ABCBABC format and so on, as shown in figure 3.7 (b). The domains are at least 4 standard cells tall (6.48 µm) as in the case of the B domain and 8 standard cells tall in case of the A and C domains (12.96 µm).The TMR region merges with the DMR A and C guides. Size and form-factor of the guides are determined after multiple iterations, studying placement and routing congestion.

After creation of three contiguous combinational placement domains as in Fig. 3.7 (b), cells associated with each domain have to be assigned to their respective placement groups. These placement groups are attached to the domains and become the constraint for initial placement. Step 4 corresponds to this step and the modules (*cla, *clb and *clc

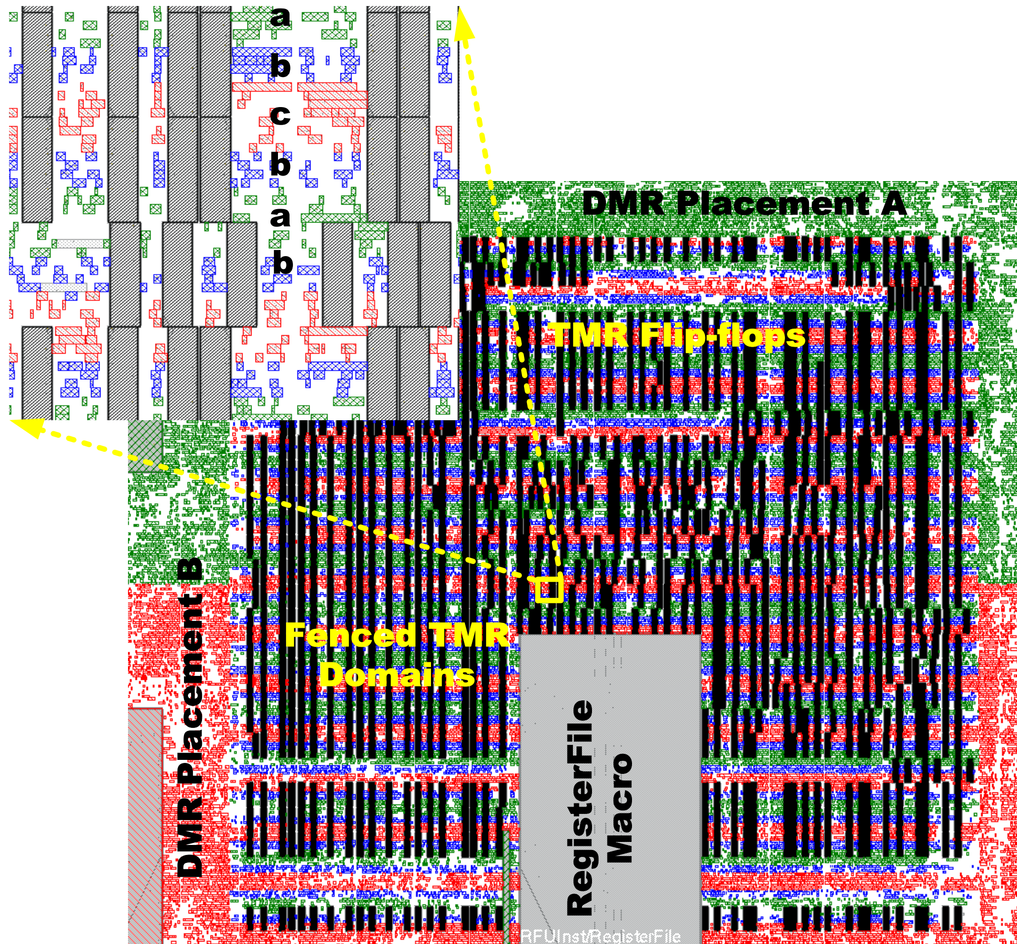


Fig 3.9. Complete domain separated physical placement snapshot. The zoomed image has the color coded A B and C domains placed within 4 cell heights tall fenced regions. DMR placement surround the TMR placement in fences akin to the large fences of chapter 2. Integrated fences thus allows placement of redundant logic with the best possible PPA.

created using the CreateTMRVerilog algorithm) are queried throughout the design and assigned to the placement domains. DMR domains A and B are assigned to the A and C domains of the TMR domain, hence the area of the A and C domains are larger by design. DMR logic can get placed in the TMR regions if the data flow so demands.

Step 5 is the initial placement of the design with guides. Fig. 3.8 corresponds to the placement of TMR flip-flops in the TMR sites described in step 2. Combinational logic is seen scattered and hence not completely domain separated (Fig. 3.8(b)). The TMR flip-

flops are fixed in place and the combinational logic is unplaced so that it can be replaced with fences to create domain-separated placement.

3.4.4. Fenced Placement

After an initial placement is achieved, the guides are converted into placement "fences" that enforce complete domain separation. Fences are a sub-type of a region where placement in the region is a hard constraint and only cells associated with the fences are placed and other cells are strictly kept out. TMR sequential multi-bit cells fixed in place become seeds for hard-fence based placement run. Standard cell logic is unplaced after the initial placement (Fig. 3.9). The magnified inset on the top left corner indicates the correct by construction TMR placement in the design. ABCCBA pattern placement of the cells can be observed in the zoomed image. Color coding indicates the respective domains. There are no MNCC vulnerabilities in this implemented design.

Carefully designed and constrained fences with proper module based assignment allow all the cells belonging to the TMR and DMR logic (green and red regions outside of TMR) to be placed with the required domain separation. The usage of fences with properly constrained module hierarchies to be assigned to those fences result in a correct by construction design with no MNCC placement vulnerabilities.

3.4.5. Optimize and Iterate

After the fenced placement, the flow runs standard timing optimization steps for PPA metric optimization. After pre-CTS optimization, the flow runs clock-tree synthesis (CTS) where the clock-trees in the design are synthesized and optimized for skew and latency. Clock trees are also triplicated which renders them DCE immune and their

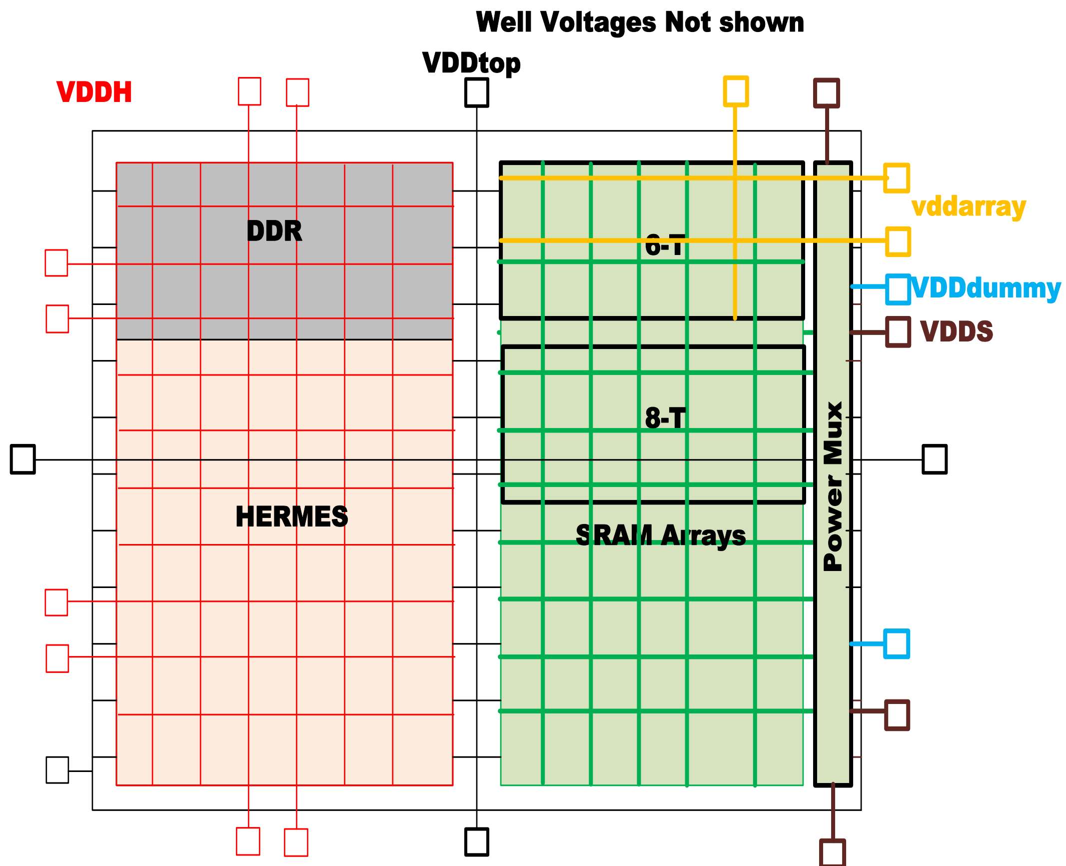


Fig 3.10. TC25 top level floorplan diagram with different power domains that exist in the chip. The design constituents with their approximate placement location with respect to the chip origin is shown. Other design constituents in the chip are SRAM arrays for process variation study.

placements are analyzed for potential placement vulnerabilities. Clock tree cells are also assigned to their respective fences as clocks are extremely vulnerable to upsets due to their high activity and spatial spread. Post-CTS the flow optimizes the design subsequently for setup and hold timing constraints, which introduce hold buffer cells as required. These are properly assigned to their respective domains due to hierarchy demarcation. The flow then proceeds to route and optimize the design while ensuring domain separation constraints are

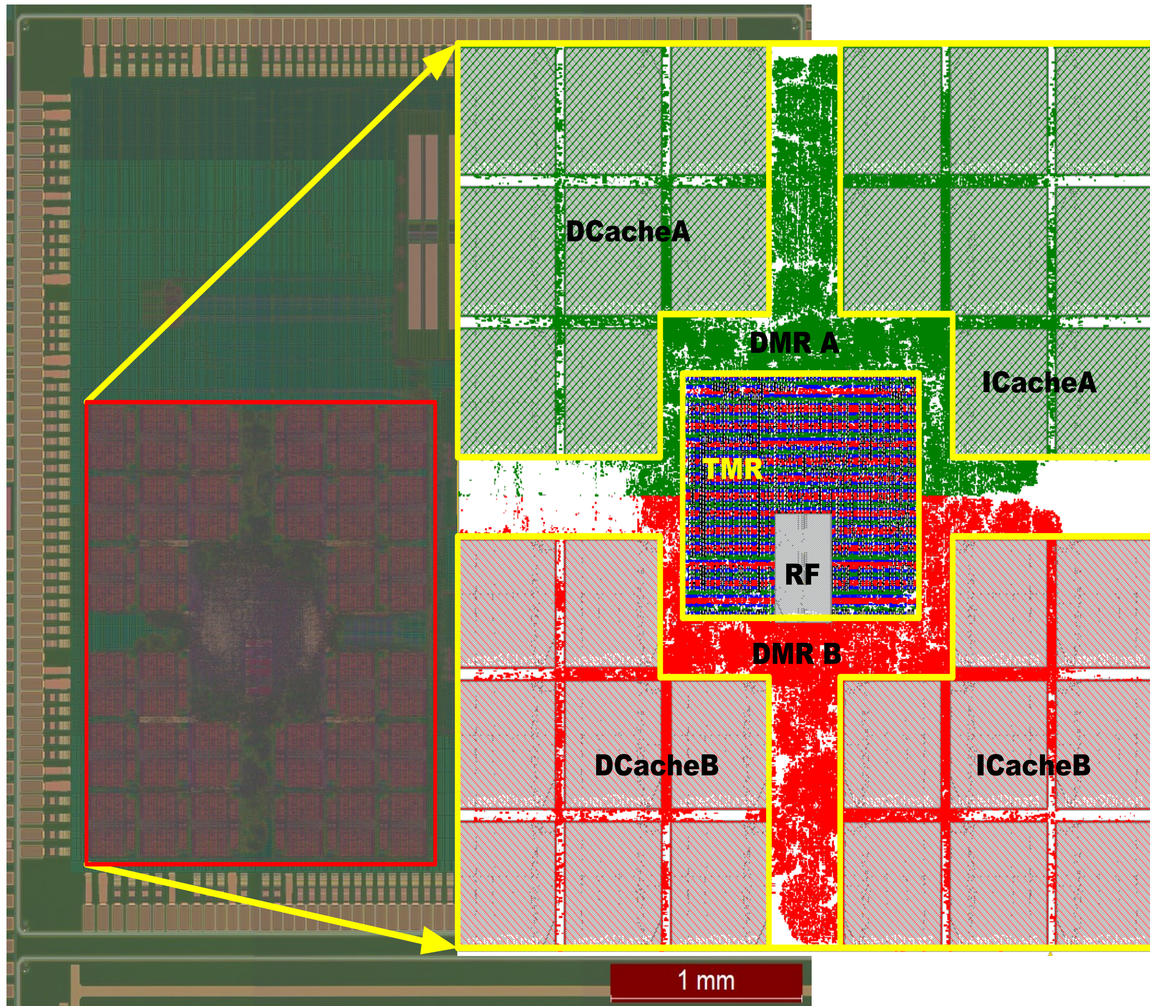


Fig 3.11. (a) Large fence module separation diagram representation (b) Interleaved fence diagram representation with A, B and C fences (c) Sequential and combinational domain mismatch if the fence and the TMR site definitions are not aligned in the interleaved fences creating potential SE vulnerabilities.

not violated at every step. These correspond to steps 7-9 in the flow and ensure that the design is ready for sign-off physical verification subsequently.

3.5. Implementation

The proposed methodology is used in implementing and fabricating HERMES2 processor design on a 55 nm low standby process (LSP). The top level snapshot of the design shows the 32 macros of cache clusters which constitute two DMR data and

instruction caches (Fig. 3.11). Register file is placed in the TMR region and has ubiquitous connectivity and critical timing to the TMR modules.

3.5.1. TC25 Level Floorplan

The HERMES2 design is implemented on test chip TC25, which also contains other test structures such as SRAMs (6-T and 8-T) and delay line for DDR DLL. The top level chip-plan with the various supplies to be used for testing of the processor and SRAM array components are shown in Fig. 3.10. The process allows well-bias controls (P and N wells) and hence the ability to enhance transistor performance and leakage. The design of a chip with well biases involves greater circuit and CAD design effort since well-taps with well-bias control routing becomes an added constraint, which has to be planned early in design.

3.5.2. Performance, Power and Area

The HERMES2 design speed is measured with extracted parasitics and the prototype core achieves speed of 2.4 ns or over 400 MHz at 1.2 V operation measured pre-silicon in Primetime. The area of the HERMES2 implementation is 3.57 mm^2 (1769 × 2020 μm). DMR Cache cluster blocks containing the SRAM arrays are pitch matched to standard cell allowing easy APR based cluster level implementation to be undertaken.

The same processor implemented on a 90 nm LSP process achieved a max speed of 314 MHz at 1.2 V operation [Farn16]. Power measured at the given frequency and voltage are 143 mW at full cache and multiply accumulator activity. The size of the design was 5.7 mm^2. This is, to our knowledge, the best performance vs. power radiation hardened core published.

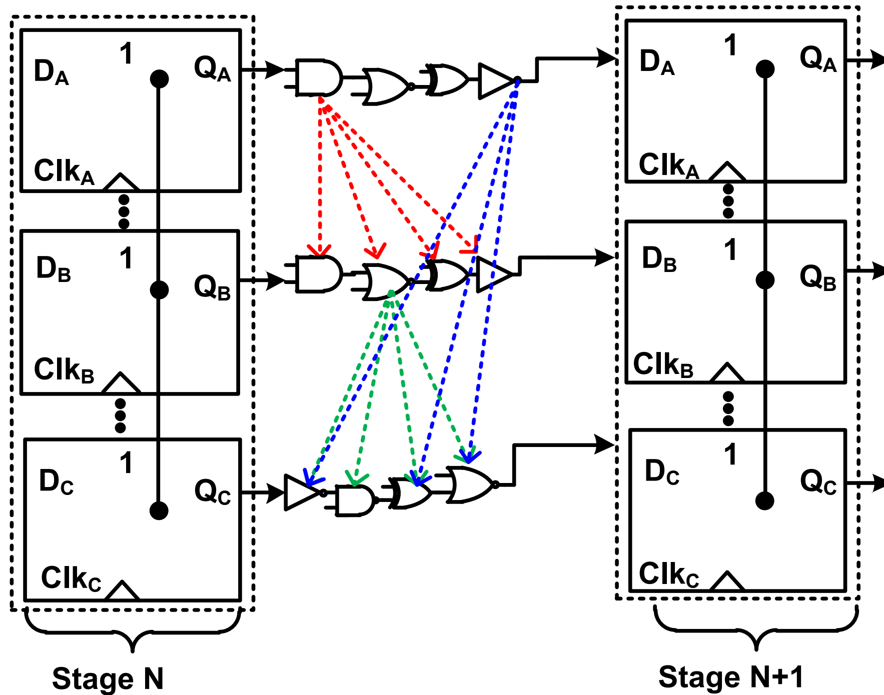
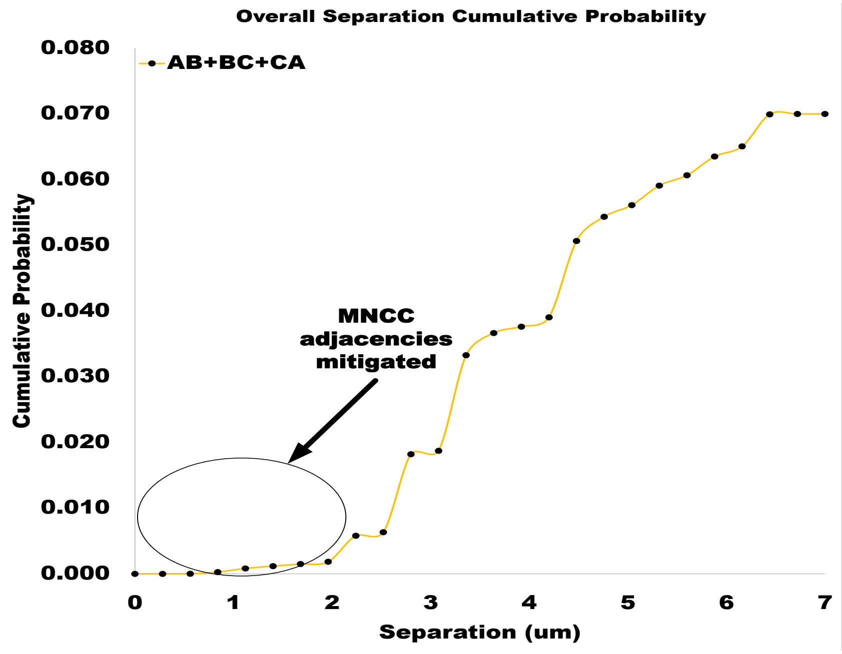


Fig 3.12. Spatial separation analysis schematic view, A, B and C paths to the redundant flip-flops are queried and their separation is analyzed for cells spacing less than 4 standard cell heights (6.48 um). This is repeated for all of the design flip-flops.

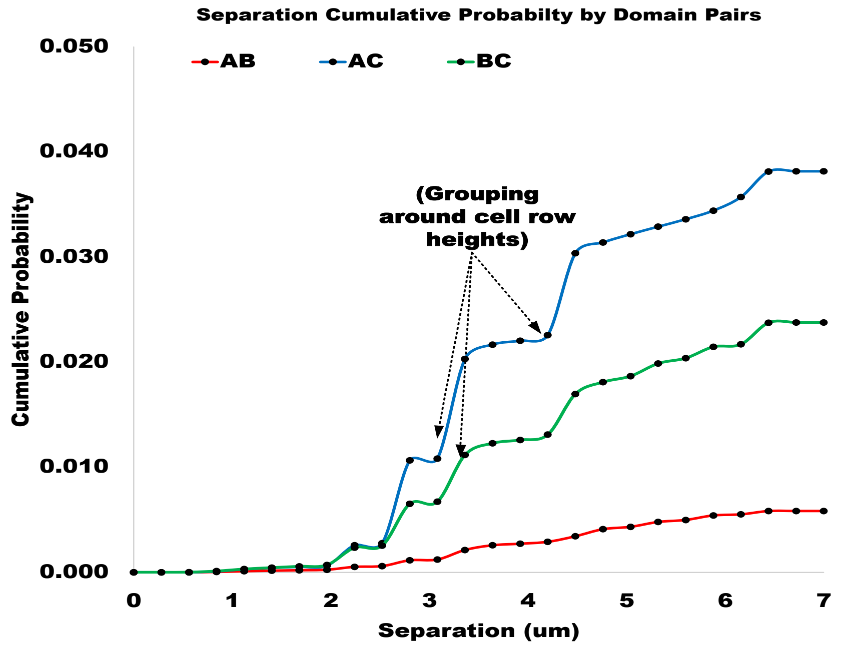
3.6. Reliability Analysis and Radiation Testing

3.6.1. Spatial separation analysis

To study the distribution of the cell separation and the efficacy of out CAD flow, an exhaustive spatial separation analysis is undertaken. 3.13 shows the schematic diagram illustrating how the spatial separation is ascertained. Unique redundant timing paths from register (TMR flip-flop) to register (reg2reg paths) are queried in the design and the cells in the paths are registered into 3 cell lists for AB, BC and AC separation, respectively. It is important to note that while the paths are redundant and the logic cone performs the same



(a)



(b)

Fig 3.13. (a) Cumulative probability of the spatial separation analysis showing 99.86 % cells protected from MNCC upsets up to a span of ~ 3um. (b) AB, BC and AC comparison cumulative probabilities with the AC and BC cell adjacencies higher than the AB adjacencies due to the size and the form-factors of the designed fences.

Boolean operation, the cells specific to each of the domains A, B and C might have different

gates, sizing and inputs. Thus, we comprehensively measure the distance between each gate to the other cells in the redundant domains.

AB, BC and CA separation is measured and stored in their respective lists. 3.14 (a) and (b) plot the cumulative distribution function of all the cell separations (AB+BC+CA) and the individual domains separations (AB, BC and CA), respectively. It can be seen that the absolute adjacencies <2 um have been practically mitigated. We see that there are abrupt jumps in the probability around the standard cell heights due to the cell separations being grouped in the vertical direction. AB, BC and AC cell separation CDF shows that AC and AB cell pairs are more likely due to the shape of the designed fence (ABCCBA and so on). This separation analysis proves that 99.3 % of the cell pairs analyzed were successfully domain separated, thereby making them completely multi-node charge collection immune. Out of the 0.7 % cells that are below 4 standard cells height, realistically only 0.14 % of the cells are potentially vulnerable. Multiplying the above probability with the probability of an actual SEE event causing a multi-node upset, the resulting probability corresponds to an infinitesimally low effective soft-error cross section.

3.6.2. Spatial Separation Previously Implemented

Table 3.II shows the radiation testing results summary of previous and current works on silicon with the spatial separation implemented and the functions of the designs implemented. Multiple publications proving the hardness of the constituent circuit techniques have been published [Clar11][Rama15][Yao10][Hind11]. A programmable built-in test engine implemented entirely using the self-correcting TMR logic as in this

Table 3.ii. Radiation Testing Results and Nodal Separation Summary

Technique	Radiation	Spatial separation (µm)	Function	Errors
DMR [Clar11]	Proton, Neutron, Heavy Ions	67.2, 49.7 µm	Register File, ALU	0 undetected errors
TMR [Hind11, Rama15]	Neutron, Proton, Heavy Ions	29.4, 7.84 µm	BIST Scan Chains, AES	1, Unrecoverable (manufacturing)
DMR+TMR [This work, Farn16]	Neutron	7.84 (90 nm), 6.48 µm (55 nm)	HERMES2 Processor	>500, Recovered

work was tested in [Hind10]. A single error was detected in the TMR self-correcting logic in multiple days of testing. It was concluded that a manufacturing defect nullified the majority voting correction in those sequential elements, since it occurred even at very low effective linear energy transfer (LET).

A RF and DMR ALU combination were tested with heavy ions and protons and published in [Clar11]. The DMR RF was successfully repaired after each error detection. The nodal separation incorporated in this work was 67.2 µm in 90 nm high-performance technology. SEU multi-cell upset extent was found to be well below critical node spacing. In heavy ion broad beam testing with LET_{EFF} from 1.4 to 219.8 MeV-cm^2/mg at fluences from 5×10^5 to 2×10^7 particles/cm^2, all RF and cache upsets were corrected or invalidated, respectively. A hardware AES encryption engine TMR hardened and tested under proton radiation in [Rama15] resulted in no soft-errors in the TMR mode.

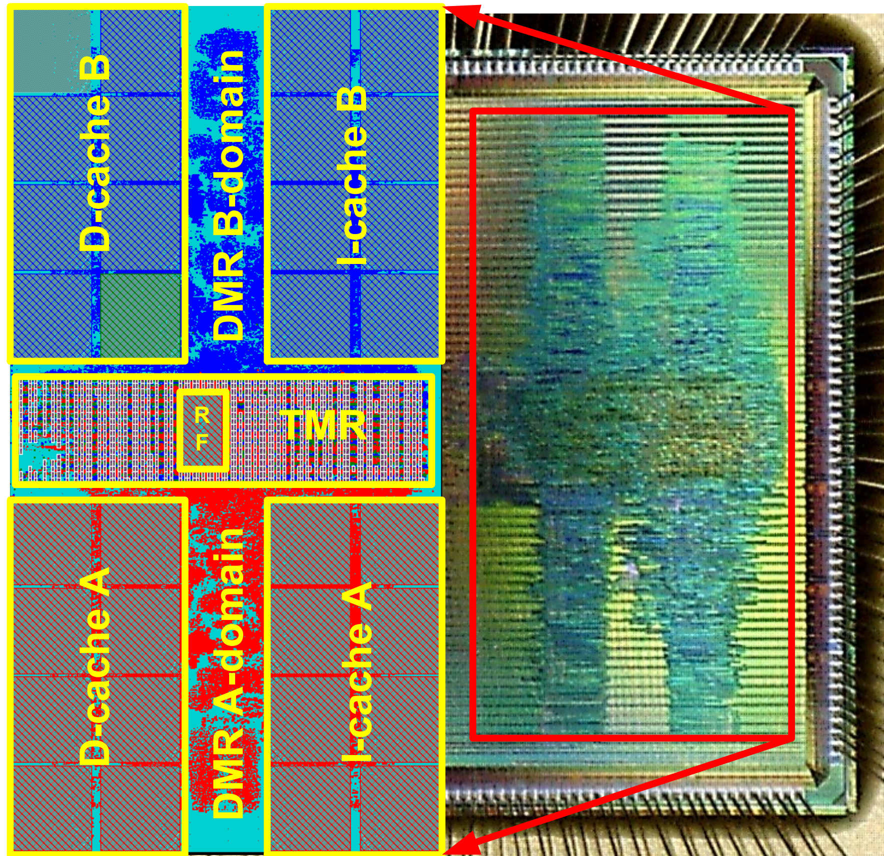


Fig 3.14. 90 nm implementation of HERMES2 [Farn16], TMR and DMR regions are highlighted, the base version of the interleaved serpentine flow is used to implement the design. The design was tested using proton radiation at UC Davis 63 MeV cyclotron beam.

3.6.3. Silicon Testing

The design in this work implemented on 55 nm TC25 is currently under functional testing and has been proven to be working successfully running the basic "Hello World" test program. Radiation testing of this design is to be performed in the future. A previous implementation of the same HERMES2 processor on 90 nm low standby power process has been tested in 63 MeV proton beam at UC Davis Crocker Laboratory [Farn16] (Fig. 3.14). Total fluence of the beam is 1×10^{11} particles/cm^2. The processor demonstrated correct recovery and program resumption from 551 errors as shown in Table 3.III, no

Table 3.iii HERMES2 (90 nm) [Farn16] Proton Beam Testing Results with the Errors Summarized by Unit/operation, Error Cross-section with Statistical Bounds are Shown.

Type of error	Number of errors	Cross section lower bound (cm^2)	Cross section (cm^2)	Cross section upper bound (cm^2)
MDU	5	2.75×10^{-11}	4.98×10^{-11}	7.20×10^{-11}
RF Write Back	104	9.34×10^{-10}	1.03×10^{-9}	1.13×10^{-9}
RF Word Line	0	0	0	0
IFU	25	1.99×10^{-10}	2.49×10^{-10}	2.98×10^{-10}
IEU	180	1.65×10^{-9}	1.79×10^{-9}	1.92×10^{-9}
RF Parity	8	5.15×10^{-11}	7.96×10^{-11}	1.07×10^{-10}
DCU	229	2.13×10^{-9}	2.28×10^{-9}	2.43×10^{-9}
Total	551	5.25×10^{-9}	5.48×10^{-9}	5.72×10^{-9}

unrecoverable errors were encountered. Excellent co-relation between the spacing implemented in the redundant critical domains and the SER of the design has been consistently observed. Based on the mathematical model in [Sham15], spatial separation analysis and silicon results, it can be concluded that the spacing incorporated in this flow is sufficient to mitigate MNCC and improve the overall SE vulnerability.

3.7. Summary

This chapter described the improved domain separation physical methodology of interleaved fences for TMR logic. A co-design methodology for physical design of domain separated complex design is also described. A complex radiation hardened by microarchitecture processor HERMES2 is implemented with the proposed methodology. The design is implemented in 55 nm low standby process with well-bias control for body controls. The domain separated logic is analyzed for cell pairs which are not separated far enough to avoid MNCC. Flip-flop to flip-flop paths are analyzed in the A, B and C domains and 99.86% of redundant pair (AB, BC and CA) cell distances are above 3 um, thereby

proving the effectiveness of the domain separation methodology. The HERMES2 design is proven to be soft-error tolerant, recovering from over 550 errors in the 90 nm version of the implemented design. The current version designed with the improved version of the APR methodology in this chapter shows improved PPA results and MNCC nodal separation statistics. This design therefore establishes state-of-the-art implementation in radiation hardened redundant designs.

CHAPTER 4. RADIATION HARDENED PULSED MULTIPLYING DLL

4.1. Introduction

In this chapter, we discuss the design of a novel RHBD all-digital pulsed multiplying delay locked loop (ADPMDLL) for DDR2-3 applications. An overview of all-digital DLLs (AD-DLL), a need for an all-digital implementation and the design trade-offs involved are discussed. Architecture, modes of operation, design of custom and APR macros such as coarse delay line, fine delay line, control and tracking logic are presented. Design validation is done at a logic level, circuit level and their simulation results are presented. Radiation hardening strategies such as TMR, used in the current ADPMDLL design, are also discussed. Monte Carlo analysis of the design constituents proves variation tolerance of the proposed design. An optimal PPA footprint was chosen as the design goal. Reliability and performance is analyzed across corners with spice circuit simulations on the implemented design showing both hardness and performance. Test chips in 55 nm and 90 nm with test structures implemented are described.

4.2. Delay Locked Loop Background

With CMOS scaling and increased operating frequencies timing margins reduce in critical interfaces such as double data rate (DDR) memories. A DDR memory transfers multiple (2,4 or 8) bits of data per wire during one DRAM clock period. Thus, its timing margin is considerably reduced than that of a single data rate (SDR) memory. Table 4.I shows multiple DDR standard specifications with the jitter specs, memory and bus speeds. The design presented in this work targets DDR2 and DDR3 specifications highlighted in

Table 4.i. Specification Comparison of DDR, DDR2 and DDR3 Memories [www.jedec.org].

	DDR2			DDR3			DDR4
JEDEC Standard name	DDR2-400	DDR2-533	DDR2	DDR3-800	DDR3-1066	DDR3-1333	DDR4-1600
Memory Clock (MHz)	100	133.33	166.66	100	133.33	166.66	200
Cycle Time (ns)	10	7.5	6	10	7.5	6	5
I/O Bus Clock (MHz)	200	266.66	333.33	400	533.32	666.66	800
Data Rate (MT/s)	400	533.32	666.66	800	1066.64	1333.32	1600
Peak Transfer Rate (MB/s)	3200	4266.56	5333.28	6400	8533.12	10666.56	12800
Clock Period Jitter (+/-) (ps)		125	100	90			60

red. Higher speeds can be achieved with faster technology processes or well biasing conditions.

Delay locked loops form a core component of DDR DRAM interfaces. The main purpose of a DRAM DLL is to compensate skew introduced by the clock distribution network such that strobe (DQS) and data (DQ) are aligned to global clock (CK) at the output pin. On the controller side, strobe is then shifted by 90 degrees to sample the received data signal and is then synchronously propagated to the internal clock domain. This conditional timing relationship has to be satisfied over a range of process, supply voltage and temperature variations. A DLL therefore ensures that the interface would meet critical I/O timing under all circumstances. In the DDR interface, input and output circuit paths are controlled by synchronous clocks and a DLL is essential in achieving system performance of the high speed DDR interface. Timing margins have shrunk considerably as we move from SDRAM to DDR4 standard DRAM. With reducing clock periods, timing

margin windows are shrinking, forcing jitter to be even more tightly controlled to meet these shrinking timing margins (<250 ps).

Therefore, the critical challenges for all high-speed I/O related clock recovery are clock skew and jitter. Clock skew is the difference in clock arrival time delays to the different portions of the chip due to mismatch in clock routing and repeater buffers in the clock distribution network. Clock jitter can be static or dynamic. Static jitter refers to the inherent non-idealities in circuit implementations resulting in non-linearity such as duty-cycle distortion. Dynamic jitter is the response of the circuit to supply noise, crosstalk or inter-symbol interference (ISI), voltage, temperature and process (PVT) related variations. Since margins are sensitive to the falling and rising edge of the clocks, DCD further aggravates and the timing margin shrinks. Supply noise, ISI and increased costs of packaging also adds further design constraints.

DLL designers need to control variability of lock-time, tuning-range, resolution, jitter, power and layout, because these constraints affect the overall system performance. Analog DLLs have been designed historically to meet DRAM clock des-skewing requirements. Analog DLLs require matched circuity to alleviate delay mismatches. Consequently, the design constituents need to be adequately sized to ensure that any device mismatch is kept to a minimum leading to increased implementation area. Resistors and capacitors used in charge pumps and other circuits may reduce mismatch through statistical methods at the cost of increased area and power consumption [Chou06].

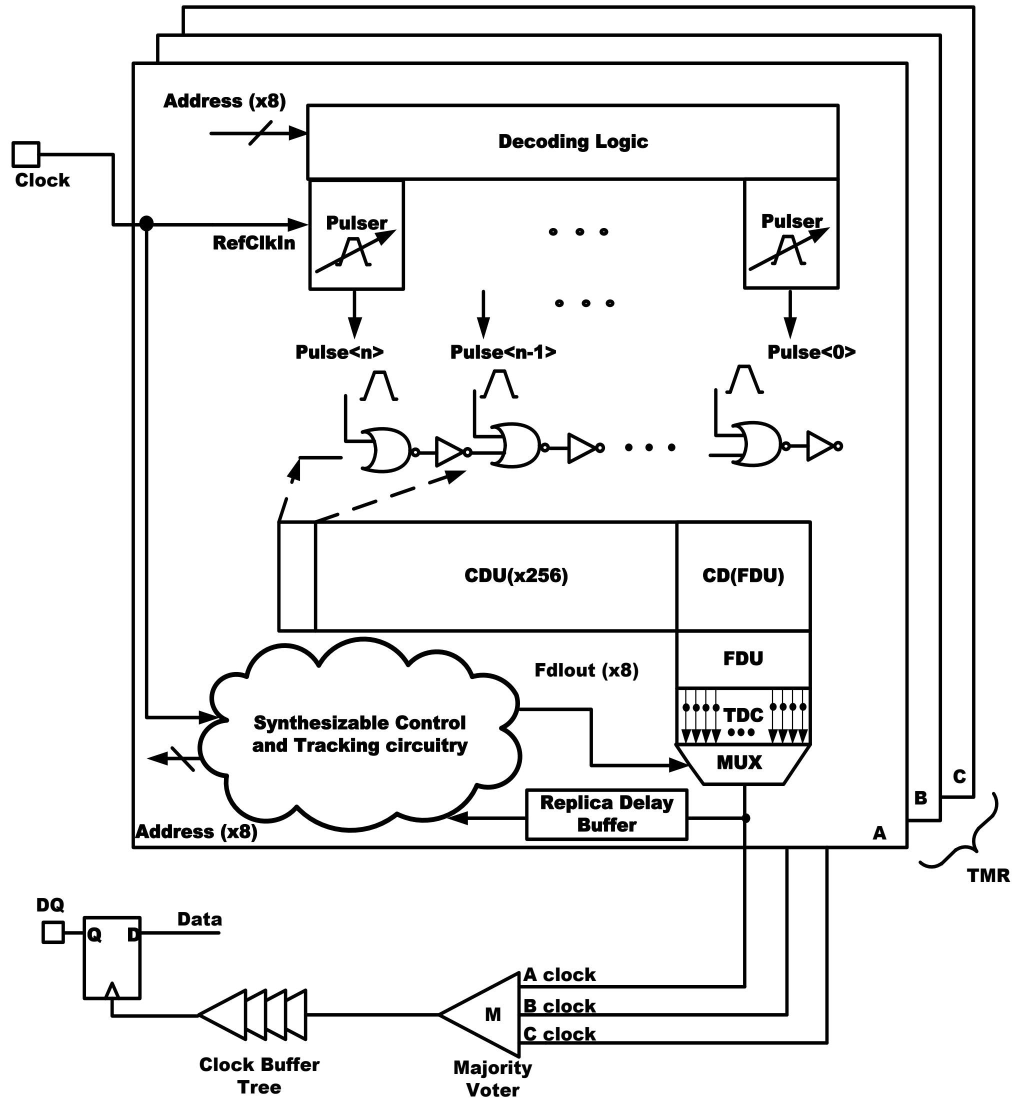


Fig 4.1. Top level architecture of the radiation hardened all-digital DLL implementation. Three clocks are generated and voted out to create the soft-error free clock which clocks the data in the DRAM capture path (DQ).

Analog DLLs are not operable under low-voltage conditions since biasing across varying voltage ranges poses a considerable design challenge.

An all-digital approach on the other hand, allows for greater scalability and portability [Garl99]. The all-digital delay locked loop (AD-DLL) is also inherently more stable being a 0th order system. Hence it is almost always preferred to a PLL for DRAM clock de-skewing. AD-DLLs are also more robust to PVT variations. Lock time of digital

sync circuitry can also be made faster for an all-digital DLL compared to its analog implementation [Hoss14] [Shen10] [Hung15].

The AD-DLLs however have considerably worse jitter and static phase error than analog implementations. Additionally, filter and tracking circuits have digital quantization error, which gets added to ADDLL phase error since delay variations are discrete. ADDLLs, however, do have an advantage over PLLs, as that they do not accumulate jitter as the locked clocks are not fed back to the DLL delay line.

4.3. Radiation Hardened Pulsed Multiplying DLL

4.3.1. Soft-Error Induced Failures

The effect of radiation strikes on digital clock synthesis circuits has been studied in detail in [Chen2014] and shows the digital filter and other control circuitry to be susceptible to upsets leading to loss of lock and/or degradation of performance. DLLs have proven to be susceptible to soft-errors or single event effects [Love06, Boul06, and Mail14]. For instance, an SET can cause the DLL to lose lock or fail to acquire it in the specified interval. SETs can also cause "missing pulses" where the clock signal is completely consumed. Secondly, a false lock to the inverted clock or a lock to π radians as opposed to 2π has been shown. Thirdly, the output duty cycle of the clock can be altered as a result of an SET propagating to the output. Similarly, the phase error (jitter) performance of the DLL can be degraded due to a radiation event. The voltage controlled delay line has been suggested to be the most single-event susceptible block as in DLLs [Mail14] but edges can be directly injected by an SET. The charge pump is also highly susceptible to radiation events and can cause incorrect operation. The phase detector has been observed to be less critical, since a

single incorrect decision can be eliminated due to the low-pass filtering of the phase detector depending on the design bandwidth.

4.3.2. TMR ADPMDLL Architecture

Fig. 4.1 shows top level architecture of the radiation hardened ADPMDLL. Three multiplied phase locked versions of the reference input clock are produced which are voted out to create data capture clock. The data captured is synchronized to the internal clock domains so that it can be processed at a manageable clock rate. Since the clocks produced are fed-forward and not fed-back into the DLL jitter due to a single event, upsets are not accumulated. The DLL presented in this chapter provides jitter performance that conforms to specifications shown in Table I (+/- 90 ps). The DLL presented in this work produces high frequency pulsed clock, as opposed to classical DLLs which produce a 50% duty cycle clock. Replica buffer delay is shown in relation to the external clock tree delay. Replica buffer tree has not been designed into the base version as the actual clock tree delay and structure are a function of the DDR physical layer (PHY) design and layout. Variable clock replica buffer delay can be easily added in the implemented ADPMDLL based on clock distribution network.

Three clocks produced by the TMR ADPMDLL are voted out to produce an error-free clock for the DDR interface or physical layer (PHY). The flip-flop represents the capture flip-flop of the DDR PHY and has to be synchronized to the clock pin on the interface. Voting can be simple or self-correcting in nature depending upon the circuit

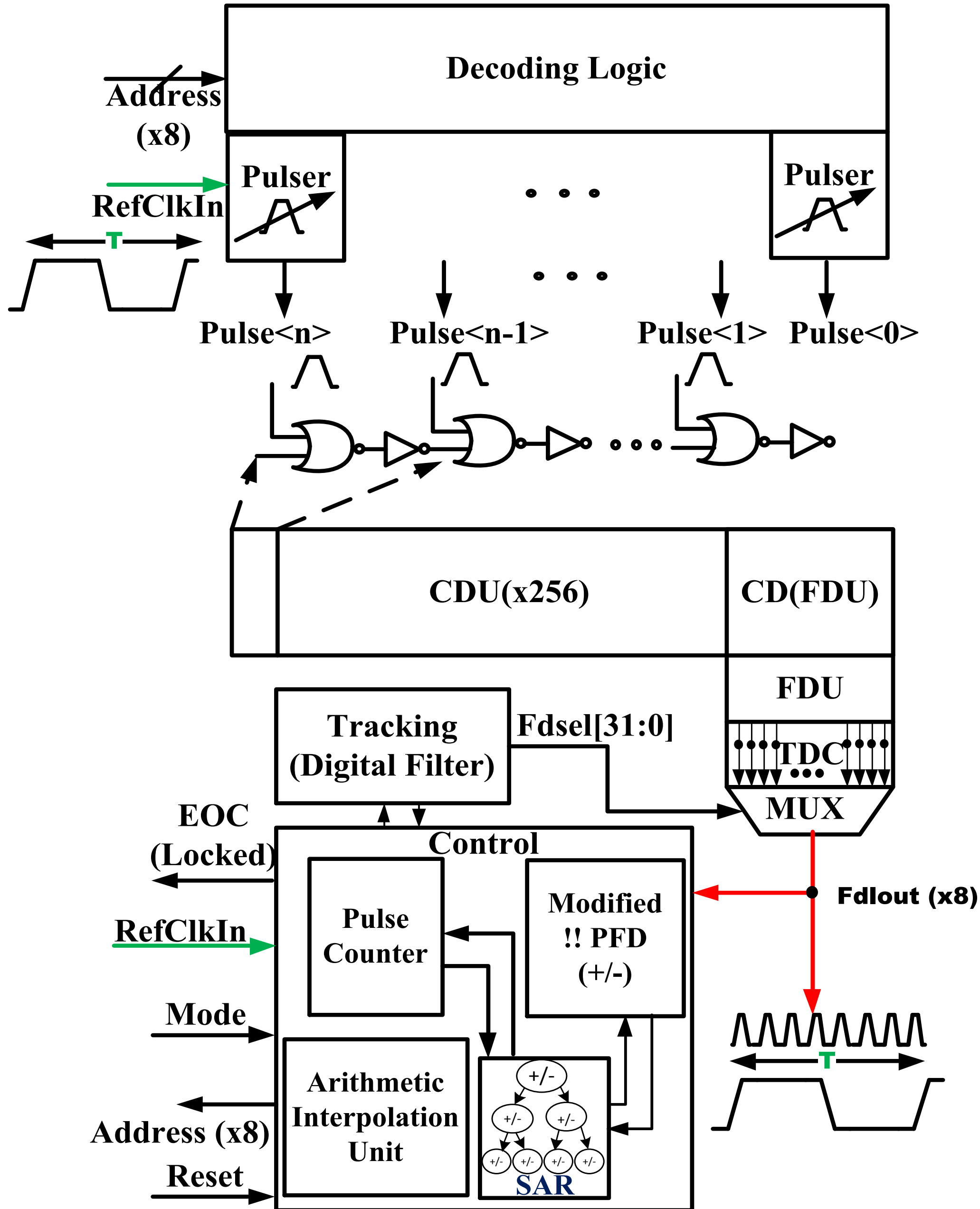


Fig 4.2. ADPMDLL architecture showing the digital delay line consisting of coarse and fine delay units (CDU and FDU). A bang-bang phase detector and TDC are used to calculate phase difference in locking and tracking mode, respectively. Control unit constituents are also shown.

functionality and cross section of the constituents. The APR logic is implemented with self-correcting flip-flops, therefore an error originating from an MNCC has a very low

probability of propagating forward and affecting all three copies.

4.3.3. ADPMDLL Architecture

Fig. 4.2 shows a top level block diagram of the single copy of all-digital pulsed multiplying delay locked loop (ADPMDLL). The proposed ADPMDLL consists of a digitally controlled delay line consisting of coarse (CD) and fine delay (FD) units. The coarse delay unit is a non-inverting OR gate which either injects a pulse into the stage in question or propagates a pulse injected from a previous stage. No dynamic power is dissipated in stages that are not selected as they do not switch. The FD unit is an inverter based phase interpolator, which is derived from the coarse delay unit and hence tracks the coarse delay unit across PVT variations. One coarse delay unit is equal to 8 fine delay units (or a by-8 interpolation of the CD). This is different from other designs where the coarse and fine delay units have different variations across PVT due to differing design elements. The 32 bit FD produces the edges which are processed by a time to digital converter (TDC) to produce a 5 bit binary code by using a thermometer encoder.

The 5 bit (0-31) output from TDC denotes the phase difference between the reference and pulsed clock. Four CD-FDU units together make the fine delay and interpolator combination capable of tracking minute variations in phase difference. The code is centered on a binary value 01111 (or decimal value 15). This indicates 0 ps phase difference. Binary values less than 15 indicate multiplied pulse clock to be lagging and values greater than 15 denote multiplied clock to be leading the reference clock. TDC output provides tracking and control to make decisions during tracking mode of the DLL

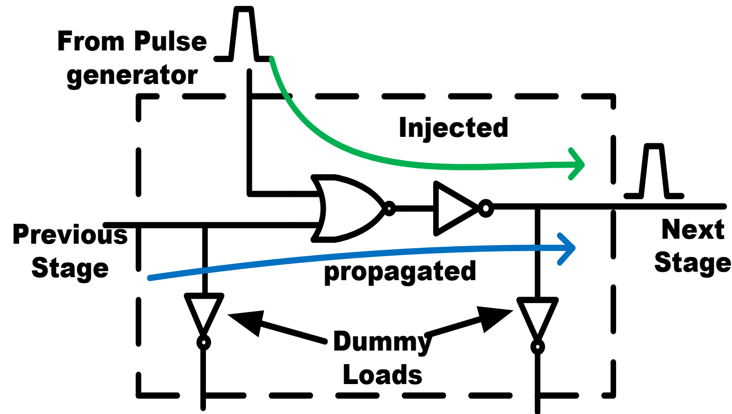


Fig 4.3. ADPMDLL coarse delay unit is shown, propagating and injecting path are highlighted in blue and green, respectively. Dummy loads ensure matched slews across the coarse delay and fine delay chain.

and ensures that fine corrections to multiplied clock phases can be adjusted using a pulse-selection multiplexer as shown in Fig. 4.2.

Tracking and control circuitry is synthesized to implement a successive approximation register for locking of the pulse clock to reference clock based on bang-bang phase detector output. SAR output code is the address for decoders to inject pulses into the delay line (1, 4 or 8 based on the mode signal). A successful lock results in EOC being asserted which also signifies the reference and multiplied pulsed clock are within +/- 2 CD value. This also indicates that before fine adjustment begins in the TDC-MUX logic, the locked clock is within limit of the jitter specs (+/- 90 ps). After locking phase, the multiplied interpolated clocks are injected into the delay line based on binary add and shift arithmetic. Depending on the mode, an additional 3 or 7 pulses are injected to create an x4 or x8 clock for DDR2/DDR3 operation. The tracking circuit adjusts fine and/or coarse

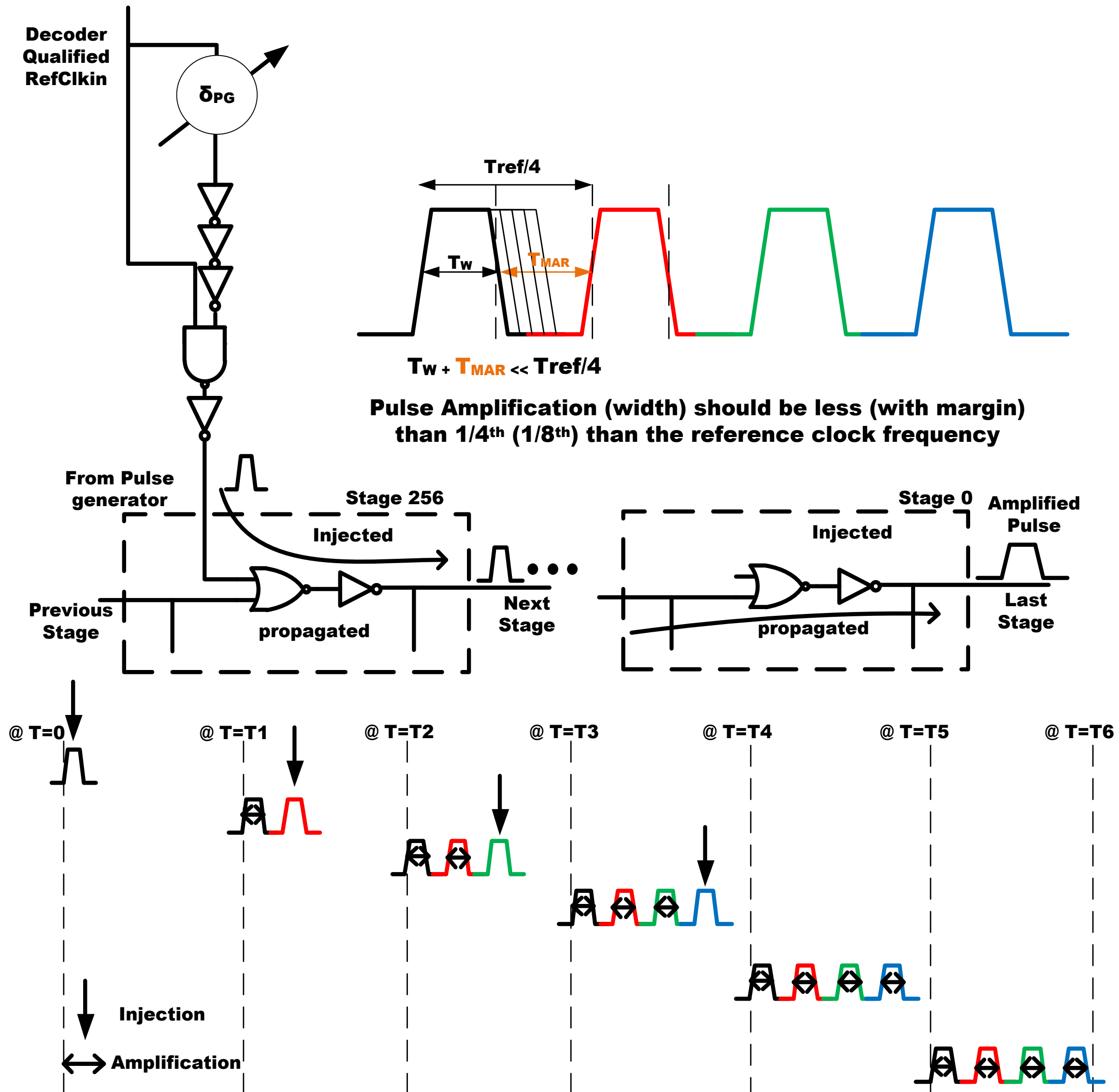


Fig 4.4. Pulse width sizing requirements and critical timing relationships for ensuring that fidelity of the multiplied clock is maintained. Pulse injection and amplification are shown at different time stamps.

delay depending upon variation in reference and pulse clocks. Subsequent sections explain the design and functioning of these blocks in detail. The DLL elements described in this chapter are implemented on a low power 55 nm CMOS process.

Table 4.ii (a) DDR Clock Specifications and the Length of the Delay Line Required (b) Number of Delay Lines and the Distance between Individual Pulses based on DDR2 and DDR3 Mode Across Corners.

(a)

Mode	Memclk (MHz)	Period (ns)	I/O clock	MT/s	DDL period (s)	period (ps)	Length required (ps)
DDR2	100.00	10.00	200.00	400.00	2.50E-09	2500.00	10000.00
	133.33	7.50	266.66	533.32	1.88E-09	1875.05	7500.19
	166.67	6.00	333.34	666.68	1.50E-09	1499.97	5999.88
	200.00	5.00	400.00	800.00	1.25E-09	1250.00	5000.00
	233.33	4.29	466.66	933.32	1.07E-09	1071.44	4285.78
	266.67	3.75	533.34	1066.68	9.37E-10	937.49	3749.95
DDR3	100.00	10.00	400.00	800.00	1.25E-09	1250.00	10000.00
	133.33	7.50	533.32	1066.64	9.38E-10	937.52	7500.19
	166.67	6.00	666.68	1333.36	7.50E-10	749.99	5999.88
	200.00	5.00	800.00	1600.00	6.25E-10	625.00	5000.00
	233.33	4.29	933.32	1866.64	5.36E-10	535.72	4285.78
	266.67	3.75	1066.68	2133.36	4.69E-10	468.74	3749.95

(b)

	FF (ps)		TT (ps)		SS (ps)	
	38.175		50.9		67.697	
	length (gates)	CD apart	length (gates)	CD apart	length (gates)	CD apart
DDR2	262	65	197	49	148	37
	197	49	148	37	111	27
	158	39	118	29	89	22
	131	32	99	24	74	18
	113	28	85	21	64	16
	99	24	74	18	56	14
DDR3	262	32	197	24	148	18
	197	24	148	18	111	13
	158	19	118	14	89	11
	131	16	99	12	74	9
	113	14	85	10	64	8
	99	12	74	9	56	7

4.3.4. Digital Delay Line

4.3.4.1. Coarse Delay Unit (CDU)

The coarse delay length is based on minimum frequency (i.e. maximum delay) needed to lock the DLL to reference clock period. Input frequency is 10 nanoseconds and hence at the fast (FF) corner, the delay line and clock to output path should be able to produce a delay of 10 nanoseconds. Fig. 4.3 shows the CD unit made up of a NOR gate and an inverter (logical OR). Two paths are shown; green indicates the path which is exercised when a pulse is injected into the loop from the pulse generator of the stage in question (n). The blue path shows the forward propagation where the pulse is injected by an earlier stage (n-1th) and the currently (nth) stage merely propagates it.

4.3.4.2. Coarse Unit Design and Pulse width Constraints

The ADPMDLL functionality assumes that pulses injected into the loop will not be consumed or attenuated by the loop. Additionally, pulse width should not be amplified to a point where the pulses injected start to merge or interfere with next stage pulse. This design requirement has to be ensured and hence the sizing of the CD chain and the width of pulse injected are to be tightly controlled.

HSPICE corner simulations are used to determine the minimum pulse width required to ensure pulse fidelity and successful flip-flop operation. Using statistical simulations, optimal pulse width was determined to be ~100 ps for a standard flip-flop to ensure reliable data capture (0 and 1). The pulse width (PW) has to be greater than the minimum PW required at all times. The pulse width is based on sizing the pulse generator delay δ_{PG} (nominally 150ps). This value of the minimum pulse width required is ascertained

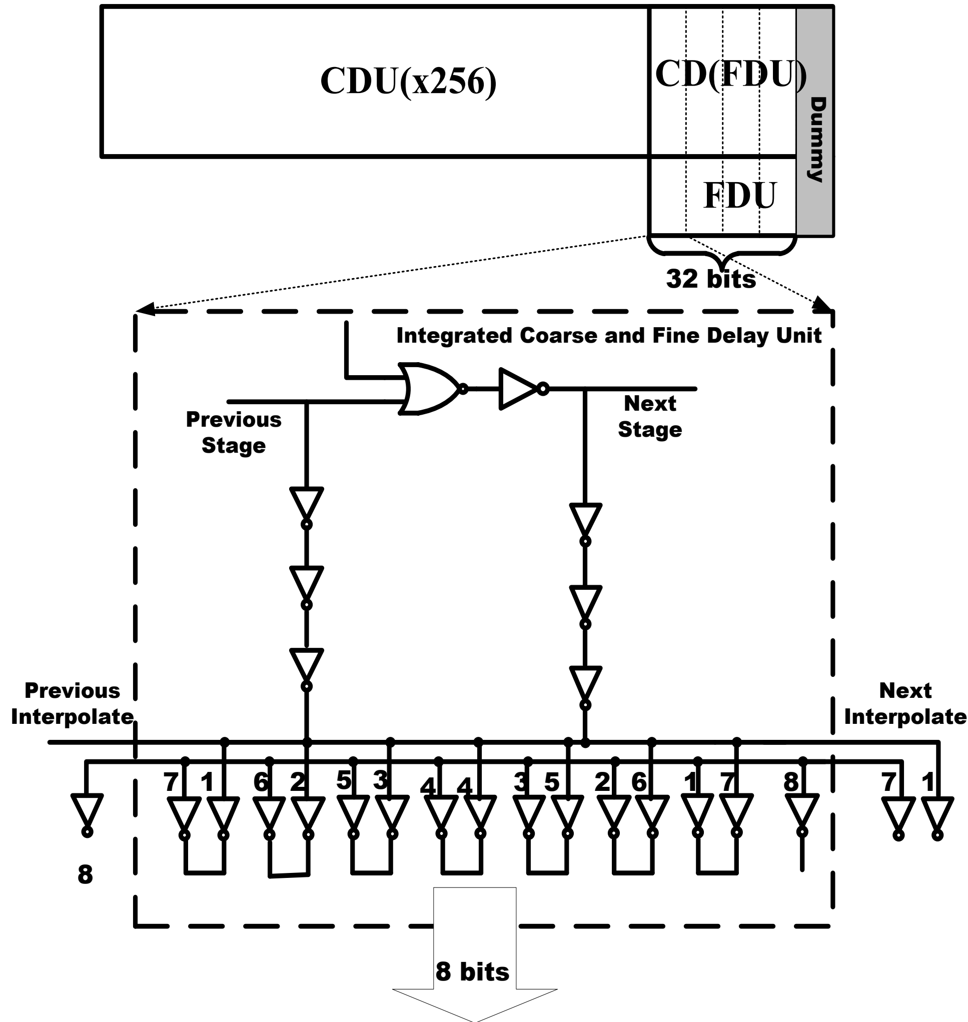


Fig 4.5. Inverter phase interpolator by 8 design. Interpolation of edges derived from coarse delay unit. Four such units are stacked to create a 32 bit fine delay unit.

based on corner (fast, typical and slow) simulations of pulse propagation through a 256 CD long delay line. A pulse of width 150 ps injected into the chain does not get attenuated across corners, ensuring the 1st constraint is met. The second constraint is also met such that no pulse injected duty-cycle distorts to increase to beyond 1/8th of the reference clock period. The pulse width should be well under this upper limit, because the next pulse begins at time T+1/8Tref, T+2/8Tref, T+3/8Tref and so on for the DDR3 mode and T+1/4Tref, T+2/4Tref and so on for the DDR2 mode.

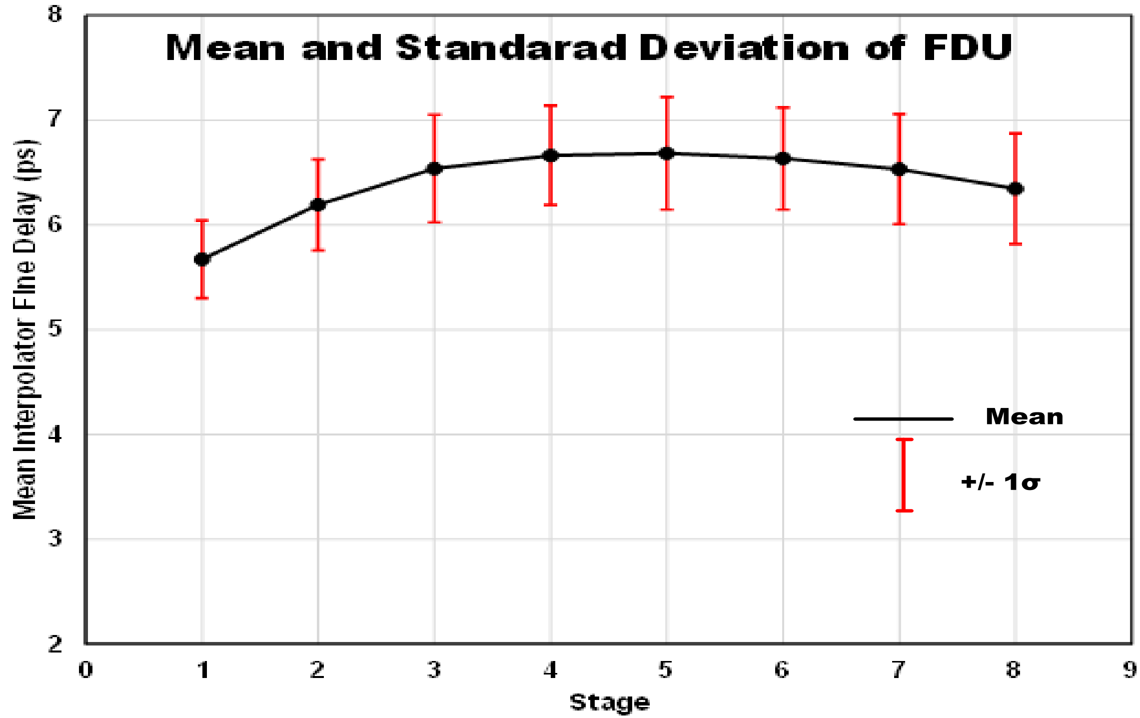


Fig 4.6 Inverter phase interpolator by 8 design. Interpolation of edges derived from coarse delay unit. Four such units are stacked to create a 32 bit fine delay unit.

All the timing relationships are critical in DDR3 mode and hence most of the critical timings addressed will be in relation to DDR3 with 8 total pulses injected to create a high frequency clock. Fig. 4.4 shows the counteracting pulse-widths required for DDR2 (the same extends to DDR3 with 8 pulses; DDR2 mode shown for readability).

Pulse width must be less than 1/4th the reference clock period to ensure all pulses that create the high frequency clock do not interact with each other i.e. fall edge of the injected nth pulse is temporally far away from rise edge of the n+1th pulse. Different colored clocks indicate clocks injected at different points in the delay chain. Injected pulses get amplified over multiple stages. This timing relationship is given by,

$$TPW + TMAR \ll Tref/4, \tag{1}$$

Table 4.iii Fine Delay Unit Delay Statistics for an Interpolate by 8. Mean and Standard Deviation are Shown Extracted from Monte Carlo Simulations.

Stage	Mean (ps)	Standard Deviation (ps)
1	5.67	0.37
2	6.19	0.44
3	6.54	0.51
4	6.66	0.48
5	6.69	0.54
6	6.64	0.49
7	6.53	0.52
8	6.35	0.53

The black pulse (injected first in Fig. 4.4) traverses maximum CDs since it is injected farthest from clock out multiplexer. Therefore, as long as the black pulse is not duty-cycle distorted to a point that it violates equation 1, the rest of the pulses will not violate critical timing at the system level. Transistor sizing is calculated by corner simulations (fast, typical and slow) to ensure that even at the slow corner maximum, pulse amplification does not violate (1).

Delay line delay and chain length are ascertained by across corner simulations. The coarse delay unit OR gate stage delay is 50.9 ps at the typical corner. The summary in Table I shows the size of the chain required to create the delay in order to lock to the reference clock. The basic requirement is the ability to delay and hence, lock to the maximum reference clock of 10 ns at all corners. This is reflected by the number of CD units required in the table across corners. Additionally, there are some constant delays outside of the coarse delay because of the fine delay, multiplexer in the clock out path and the replica buffer delay.

4.3.4.3. Fine Delay Unit (FDU)

The fine delay unit is designed as an integrated coarse and fine delay unit (CD-FDU). Fig. 4.5 shows the fine delay interpolation unit with the coarse and fine delay interpolation inverters (64 inverters). Five such units are stacked to create 40 bit FDU, where the first 32 bits are usable and with the last 8 bits being a dummy to ensure consistent loading across CD and FD stages.

The interpolator is designed to ensure that it is robust across corners to the variations in the coarse delay and the linearity degradation in the fine delay is minimal. Monte Carlo simulations of the designed interpolator unit shows fine delay for 8 steps with mean and sigma to study the potential variation that could be induced (Fig. 4.6). Table II shows the values of stage delay from 1-8. The values show that even in presence of 3σ variation, the codes cannot be erroneously interpreted (<< 6.25 ps).

Simulation waveforms of the fine delay interpolation from the coarse delay is shown in Fig. 4.7. The intermediate input stage to the interpolator is shown, too, since the slew-rate on this node has to be limited to ensure proper phase interpolation as shown. 50.9 ps of coarse delay is interpolated to 51.02 ps worth of total fine delay, which shows a very small variation on the total FD stage delay.

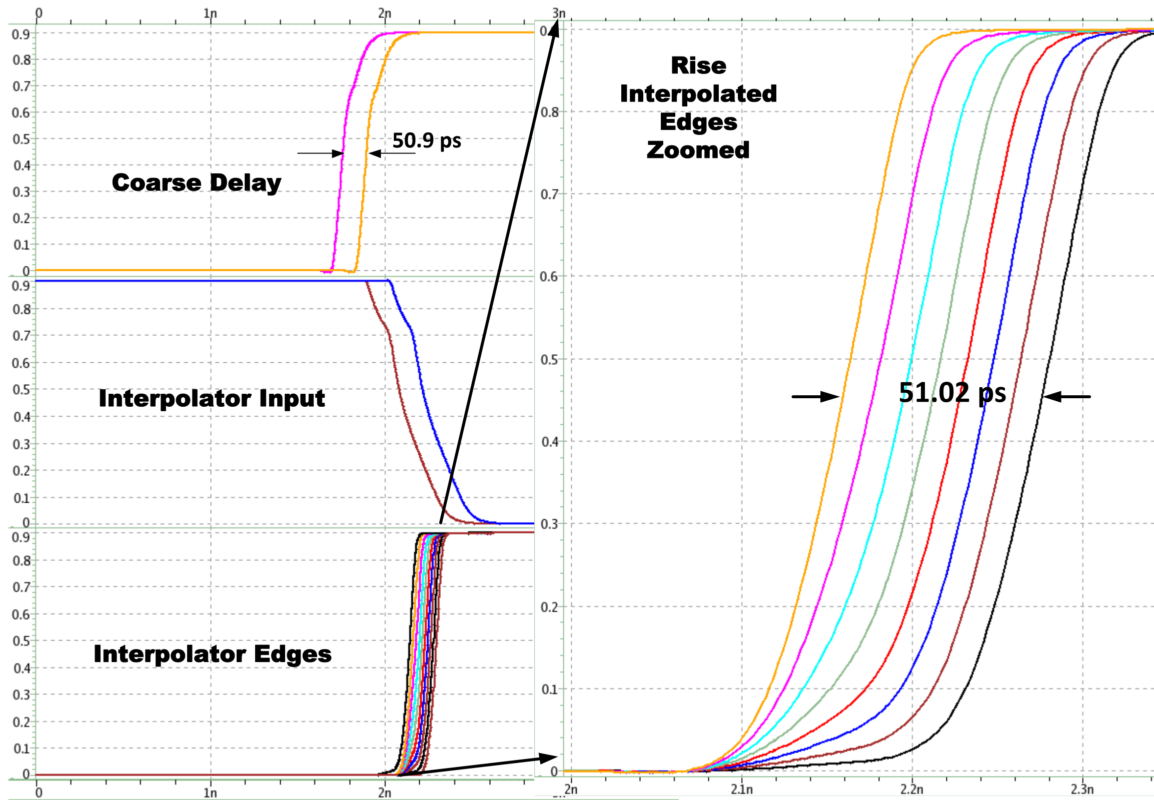


Fig 4.7 Fine delay unit simulation waveforms, interpolated fine edges are zoomed and shown on the right, the values are derived from the coarse delay unit delay.

4.4. Decoding Logic

Pulse injection is central to the ADPMDLL functioning. Decoders select pulse-generators which inject pulses to create a controlled, high frequency multiplied clock. The algorithm of the decoding process will be explained in the control and tracking logic section. The design of the low area footprint decoders is explained in this section. Fig. 4.8 shows the top level decoder arrangement in the ADPMDLL. The number of decoders in this design is based on the maximum number of simultaneous pulses that need to be

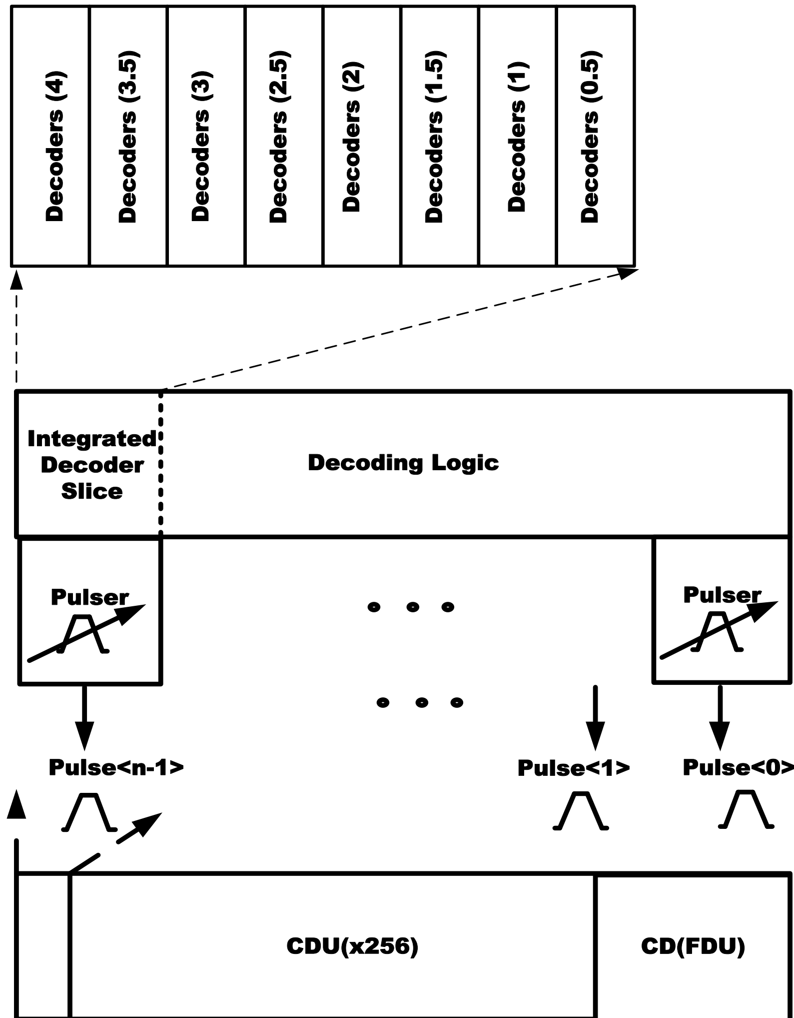


Fig 4.8 ADPMDLL top level decoding architecture shows the minimized area footprint decoders (8 in number) that are implemented for controlling the delay line width.

injected into the delay line. DDR2 mode will inject 4 pulses in the delay line and the DDR3 mode will inject 8 pulses in the delay line. Decoders 4, 3.5, 3, 2.5, 2, 1.5, 1 and 0.5 correspond to the high frequency 360, 315, 270, 225, 180 135, 90 and 45 degree clocks with respect to the reference clock. Thus 8 integrated, pitch matched decoders are designed for the ADPMDLL and arranged with the coarse delay and pulse-generator modules. Additionally, the decoders should not dissipate power during the locking mode, since only

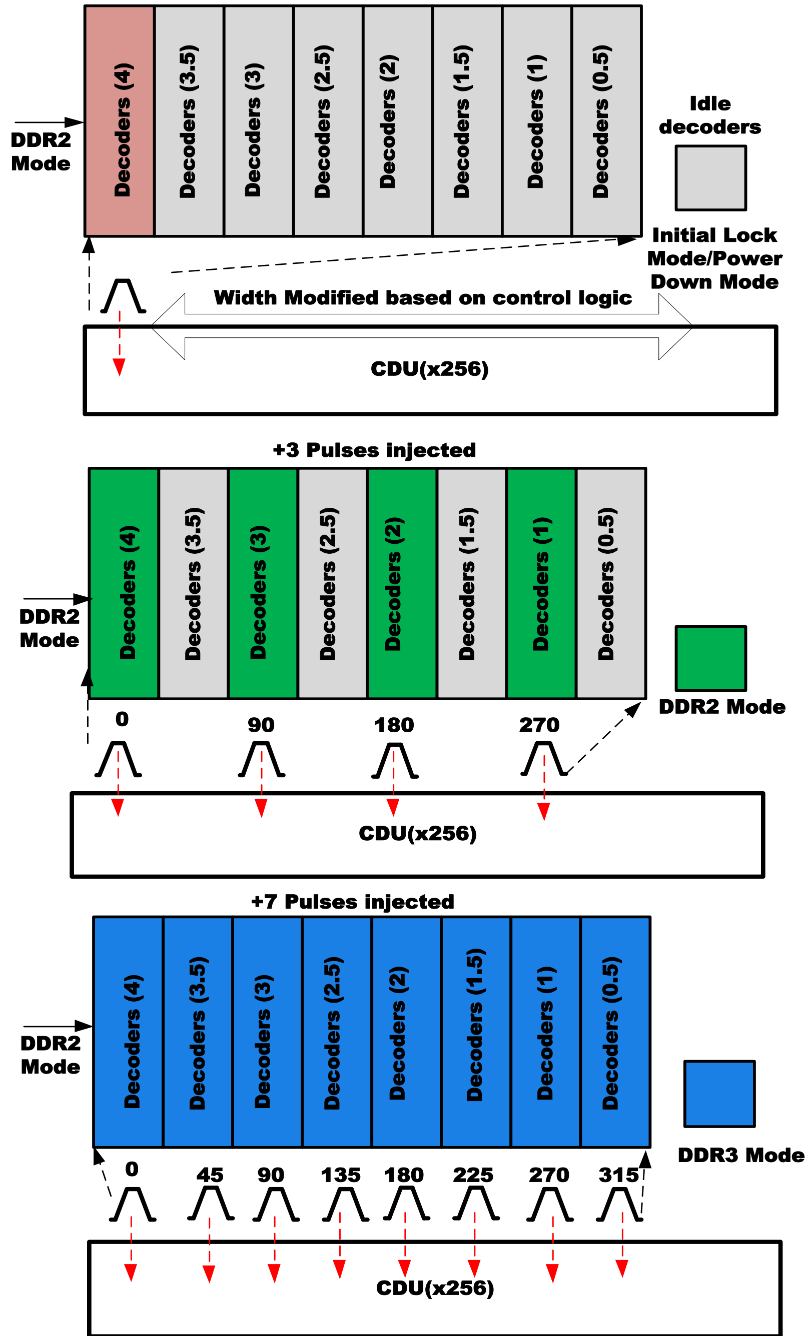


Fig 4.9 DDR Modes of operation and the decoder activity, DDR2, DDR3 and locking mode shown, idle decoders in low power mode shown in grey.

one pulse is circulated in the system and the low power idle mode (where the DLL does

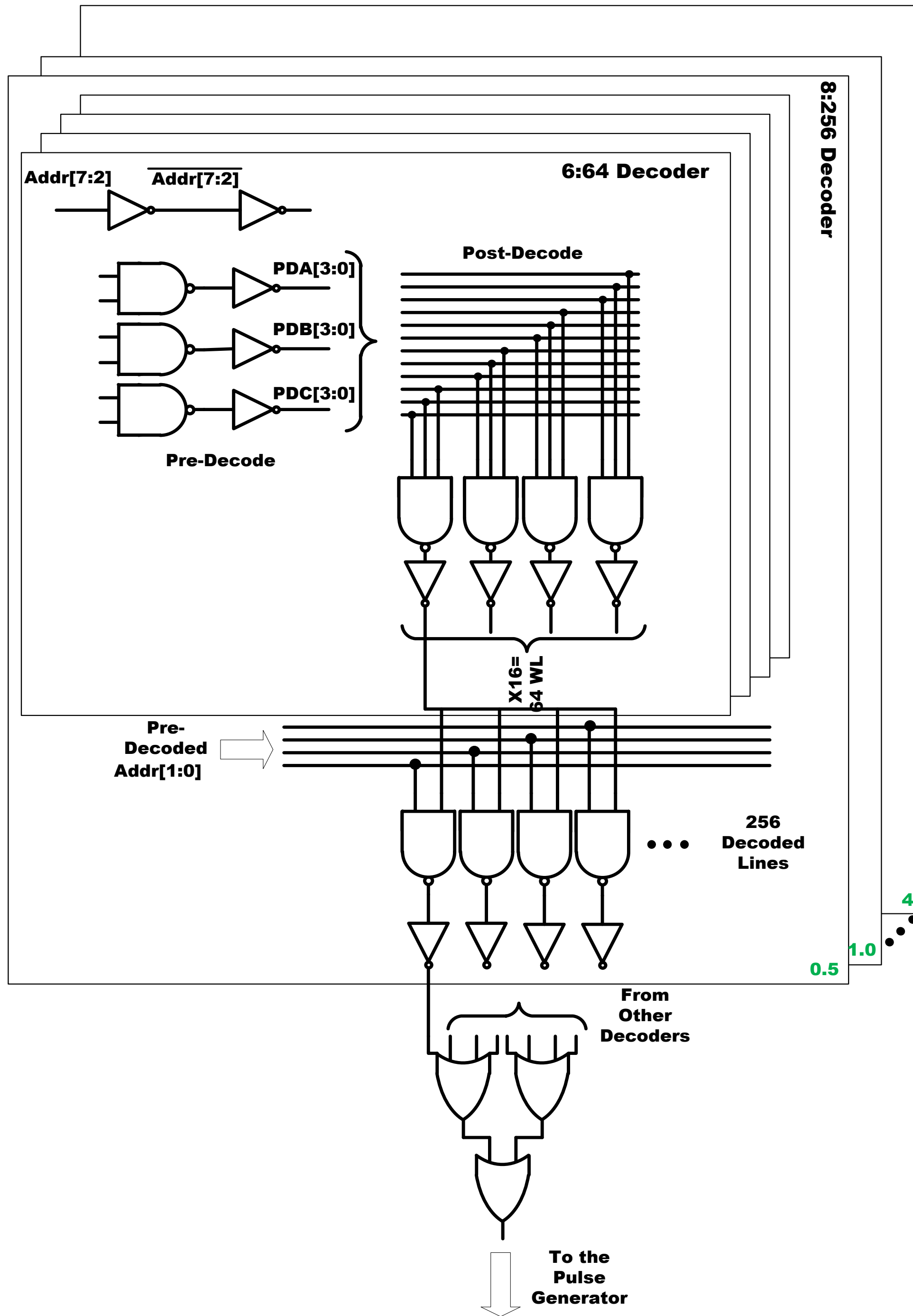


Fig 4.10 Decoding logic schematic overview, individual decoders and the OR logic which enables selection between decoders is shown.

not lose lock but the high frequency clocks are gated).

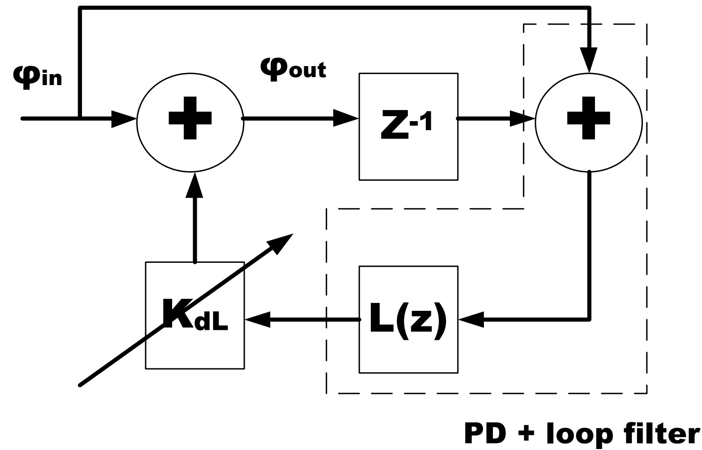
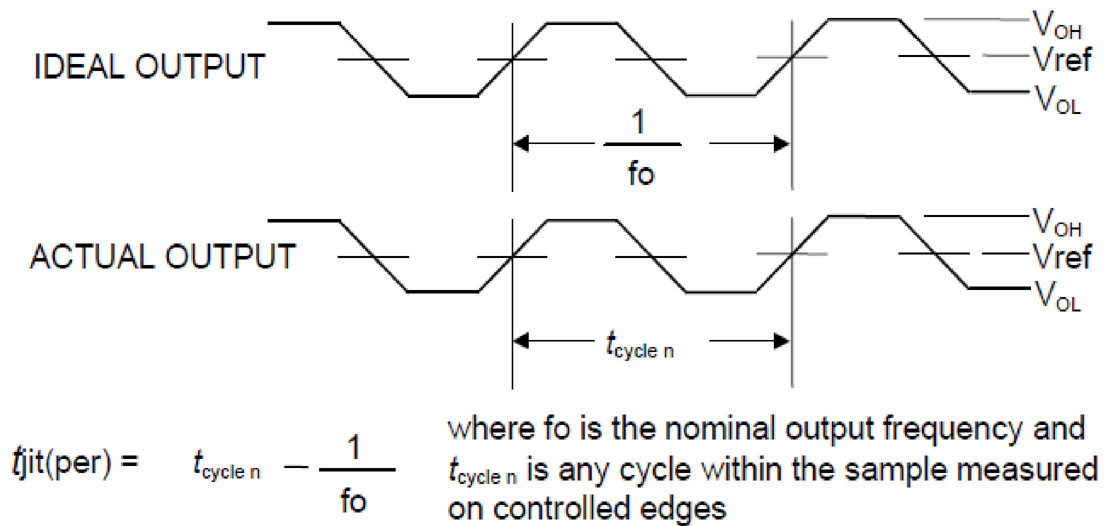


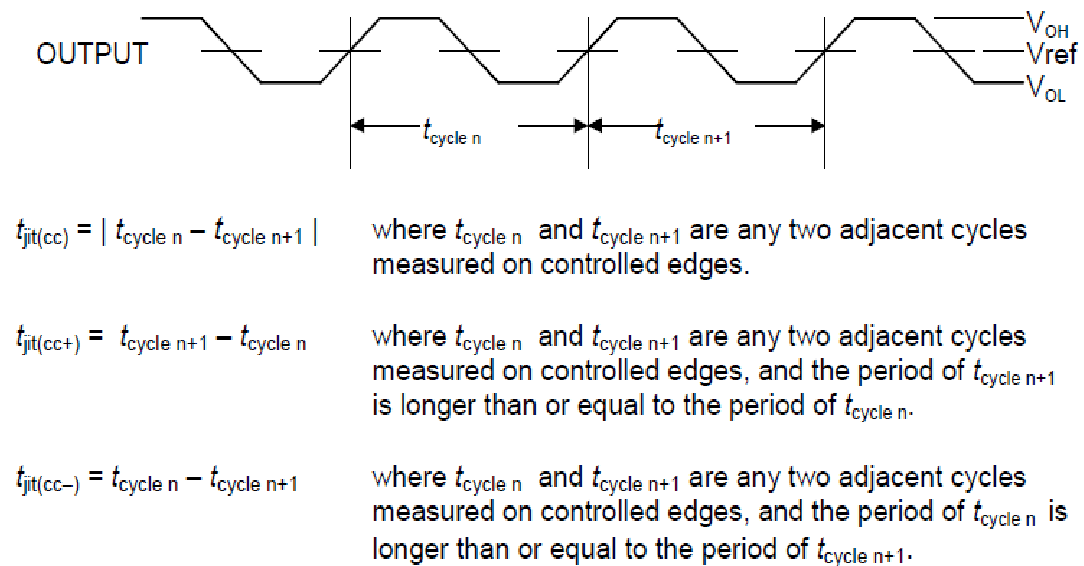
Fig 4.11 General 0th order type 1 DLL which only has feed-forward clock path Z-domain block diagram.

Decoder functioning and the modes of the DLL design is shown in Fig. 4.9. The top level decoder design for the ADPMDLL is shown in Fig. 4.10. The decoder design is not in the timing critical path and hence the design is optimized for minimal area. Decoders are controlled by the DDR mode bits that control whether the DDR operates in locking mode, DDR2 mode, DDR3 mode or low-power lock mode. The decoder (8:256) is divided into the 6:64 and a 2:4 decoding line, which selects one out of every 4 lines for the 256 bit delay line. The loading on the decoded lines is reduced to ensure lower power operation and low area footprint.

The said decoder can also be auto-placed and routed to ensure minimal design effort. At the floorplan level, the pin locations of the decoded output need to be optimized to ensure connection by abutment with the delay line.



(a)



(b)

Fig 4.12 Waveform and definitions of cycle-to-cycle jitter (a) and period jitter (b) after [JEDE03].

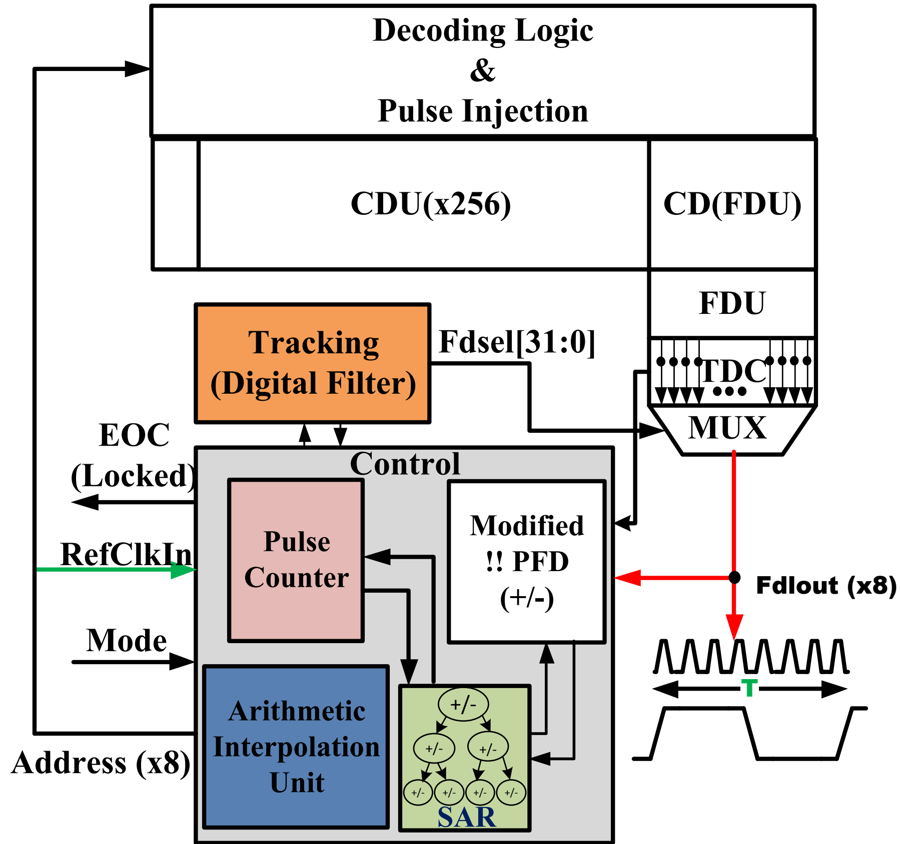


Fig 4.13 Control logic overview, constituents of the control logic are shown here, colored portions indicate APRed logic and white background indicates the custom logic.

4.5. Control (Acquisition and Tracking) Logic Design

4.5.1. Background

An all-digital DLL in this design is a Type I, 0th-order system, so there is no clock feedback involved in this implementation (4.11) [Lee03]. This means that the input jitter can be passed through to the output if the jitter is not filtered. With a low jitter input signal (controlled jitter), a DLL can achieve a quality jitter performance like the analog counterparts. Additionally, the ADDLLs in general can be implemented across various generations of technologies and DRAMs due to easy portability. This portability is

especially useful in radiation-hardened applications due to the extra hardening design effort involved. ADDLLs are also easier to test and debug, which is especially important for high speed DRAM interfaces.

A 0th order ADDLL system provides stability across PVT variations. The operating frequency range is not only determined by the tuning range delay line, but also determined by the input buffer and propagation delay in the clock path. To understand the need for control and tracking, we need to understand the variation in the clock signal. The time variation in clock period is called jitter. When a clock or data signal travels through a non-ideal channel which is affected by noise, there are variations introduced in the clock data edges and slews. The edges can then vary in time and this variation manifests as clock jitter. There are multiple representations of jitter based on how it is calculated. When the variation is calculated in the cycle time of the signal between adjacent cycles over a random number of adjacent cycle pairs, it is referred to as cycle-to-cycle jitter (Tc2cjit), 4.12(a) [JEDE03]. When the variation measured is in the difference of the period time to the ideal period time over a random number of cycles, it is referred to as period jitter (Tperjit) (Fig. 4.12(b)). These definitions are important while categorizing the jitter response of the designed ADPMDLL. The jitter values are further categorized into their root mean square (RMS) or peak-to-peak (P2P) values to further study the effects depending upon the kind of processes that are causal to jitter, i.e. random or deterministic.

The design of the power delivery and clock networks also play an important role in the quality of the jitter response since the circuit responds to external supply noise by introducing timing variations or frequency variations (phase noise, which is the frequency domain manifestation of jitter). Moreover, in radiation hardened DLLs, the radiation can

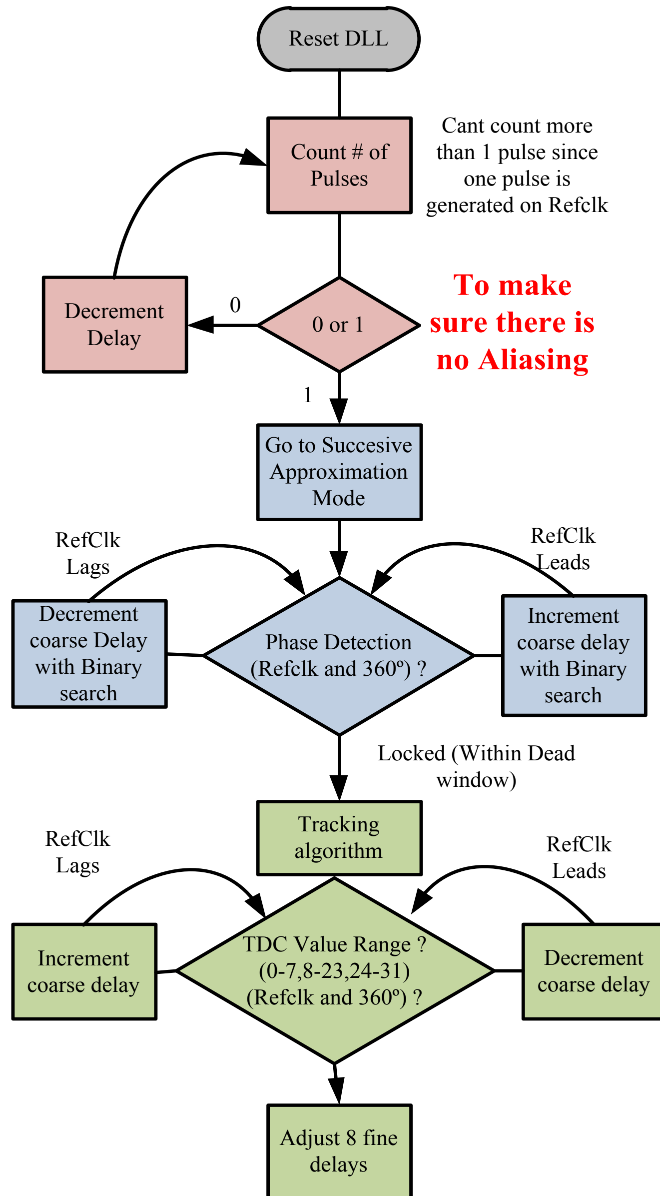


Fig 4.14 ADPMDLL acquisition and tracking algorithm flowchart, algorithm shows the binary search acquisition and step tracking using fine delay and arithmetic approximation.

also result in the change of long term CMOS threshold voltages due to ionizing doses or instantaneous changes in delay which can result in variations in jitter performances.

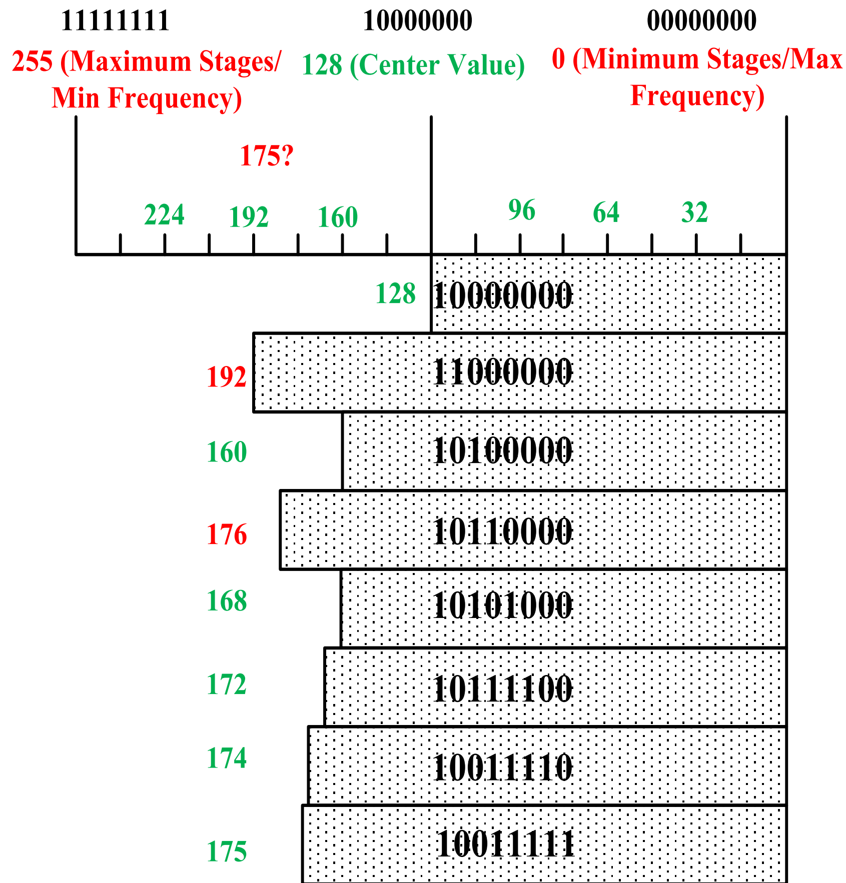


Fig 4.15 Successive approximation algorithm tracking a value of 175 with initial seed of 128. Binary values used in the control logic SAR is shown in the shaded regions. Red and green coloring signifies phase frequency detection output.

4.5.2. Control Logic Overview

The acquisition and tracking logic has been integrated together in the ADPMDLL as control logic i.e. the logic that acquires the DLL lock and multiplies the locked clock through equally spaced pulse-injection. Fig. 4.13 shows the top level overview of the control logic. The basic delay line which consists of the coarse and fine delay elements are controlled through the control logic during acquisition and tracking modes. The lock acquisition uses successive approximation or binary search to hunt and lock for the clock. The binary search process is a fast lock method since it reliably requires 8 phase error

comparisons to acquire a lock. Binary search ensures that a non-aliased delayed pulse clock is locked in 8 cycles of the successive approximation [Dehng00]. Once locked, the tracking process begins which uses fine delay interpolation and time-to digital conversion and thermometer coding to produce a 5 bit signature, which encodes the phase error of the reference and delayed clock. This value is used to track the multiplied clock in response to the reference clock.

4.5.2.1. Acquisition Logic Design

The algorithm for lock acquisition and tracking is shown in Fig. 4.14. The binary search algorithm is simple for the purposes of lock acquisition, but control of the initial conditions is essential. Fig. 4.15 illustrates the acquisition for a code value of 175. Since aliasing is to be mitigated in the ADPMDLL, the delayed pulsed clock needs to lock to the reference clock in one period equivalent delay of the delay line. The initial conditions are monitored by setting the lock acquisition logic code value to 128, which is the mid value in the delay chain of 256 delay elements. The pulse injection of delay corresponding to 128 setting is monitored and the number of reference clocks passed is counted. Beyond 2 reference clock counts, the initial seed value is invalidated and a new seed value of 64, 32 and so on is fed into the SAR unit. This is done using pulse counter logic block, which continuously counts the number of pulsed and reference clock edges that are seen by the control logic. A constant relationship between the two count values is maintained to ensure that the clocks are in synchronization and no aliasing occurs.

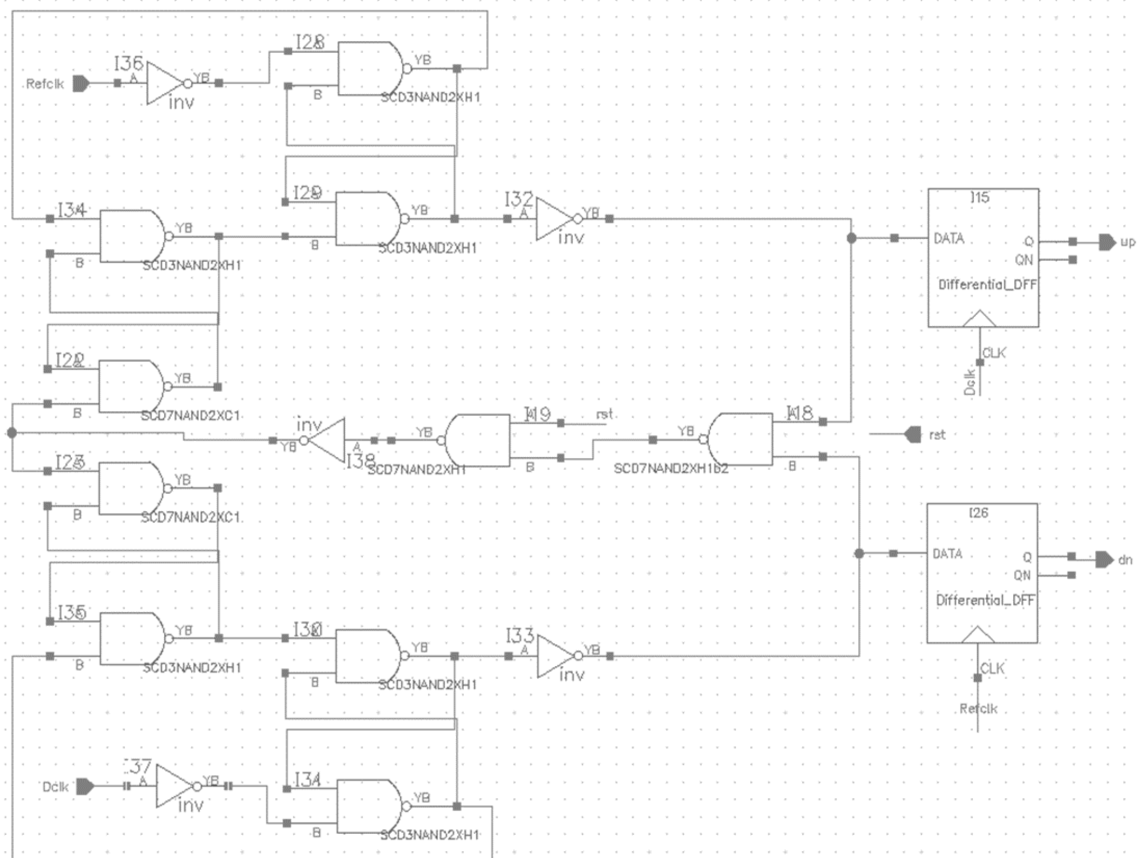
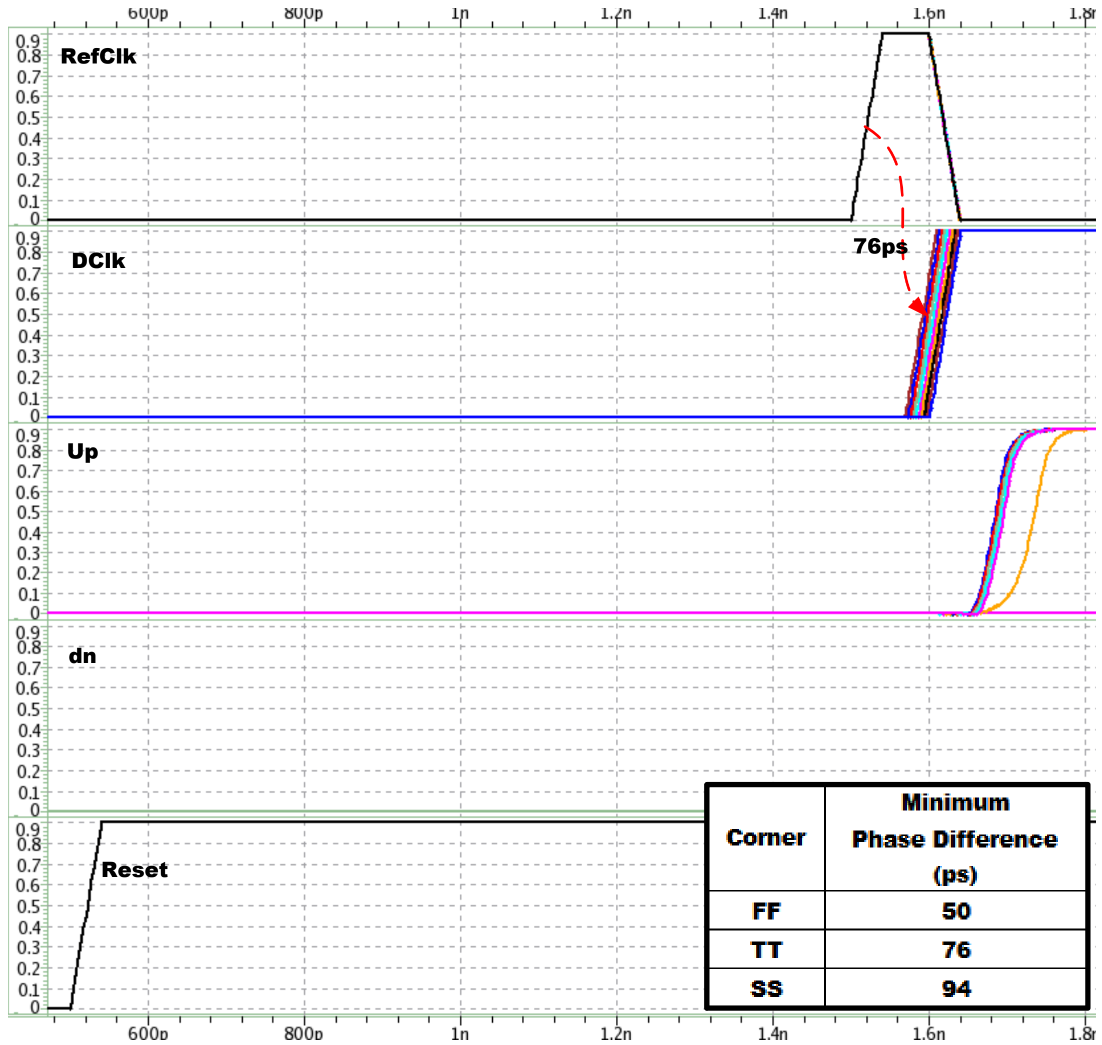


Fig 4.16 Modified bang-bang phase detector design schematic, it measures the difference between the reference clock and the pulsed clock and creates a 2 bit {up,dn} signal processed by SAR unit. An asynchronous (active low) reset is used to ensure known state before the comparison begins.

Once the initial seed is found to be not locked to an aliased value, the successive approximation ensues. The bar chart shows the starting value and the value being searched for i.e. 175. The successive approximation is operated on a divided clock to ensure that timing relationships between phase detection to address decoding can be reliably met; divide by 2 cycle did not meet timing for successive approximation and divide by four clock met this timing across corners. Thus, the total number of reference clock cycles to acquire lock is 32 cycles.



Corner	Minimum Phase Difference (ps)
FF	50
TT	76
SS	94

Fig 4.17 Bang-bang phase detector design schematic, it measures the difference between the reference clock and the pulsed clock and creates a 2 bit {up,dn} signal processed by SAR unit. An asynchronous (active low) reset is used to ensure known state before the comparison begins. Table inset shows the minimum resolvable phase difference.

The tracking algorithm is a constant monitoring of the time-to-digital converter (TDC) values and update of the fine delay values of the individual 8 clock pulses injected. Based on the phase error, the coarse delay can be incremented or decremented when phase error observed is greater than +/- 8 FD or 1 CD. The tracking process outputs are used by

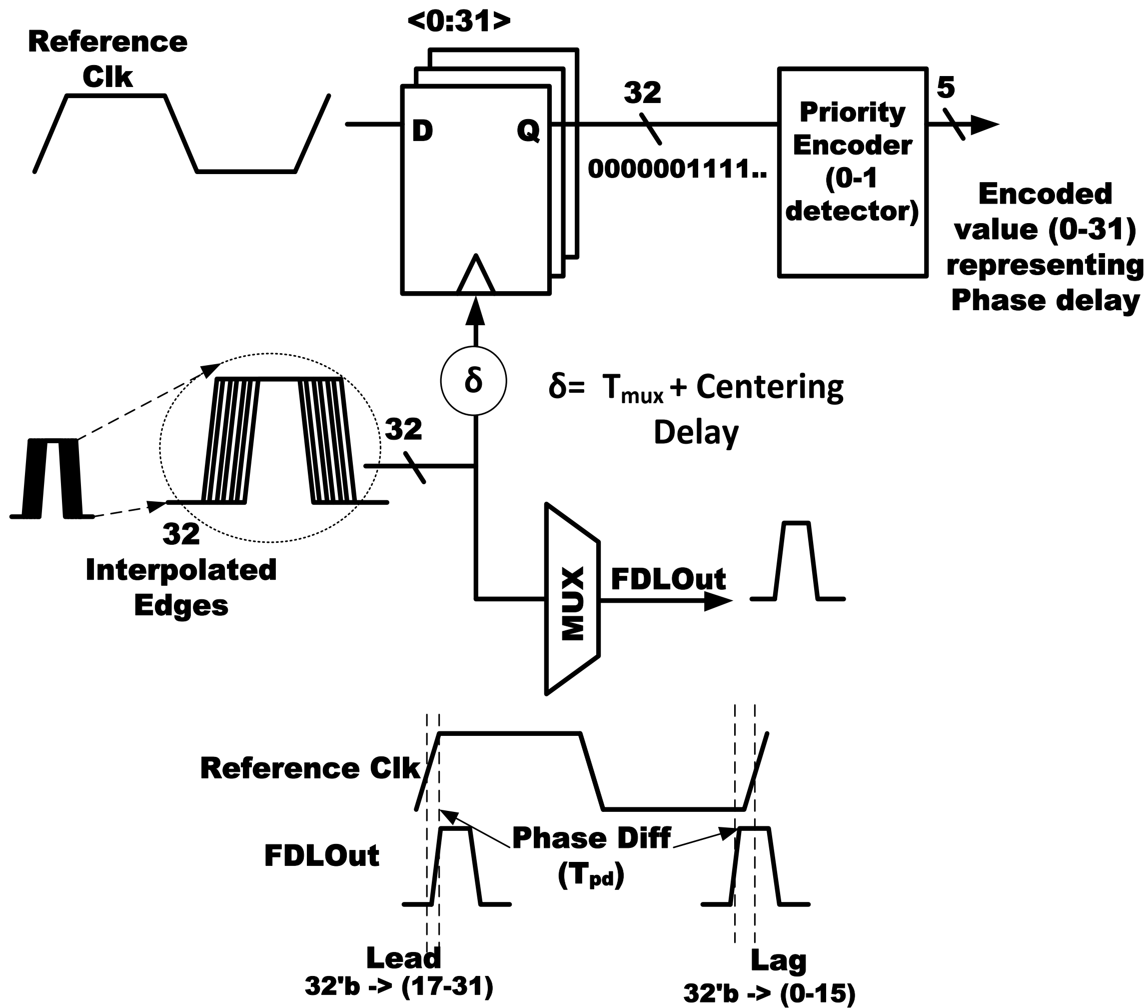


Fig 4.18 Time to digital converter design which processes 32 bit edge data and produces a 5 bit code that represents the phase error with a granularity of 6ps. Values representing lad and lead are shown with the associated waveforms. The centering delay ensures that center value (16) corresponds to 0 ps phase error.

low overhead arithmetic units to individually adjust the pulses with respect to reference clock.

4.5.2.2. Phase Error Measurement

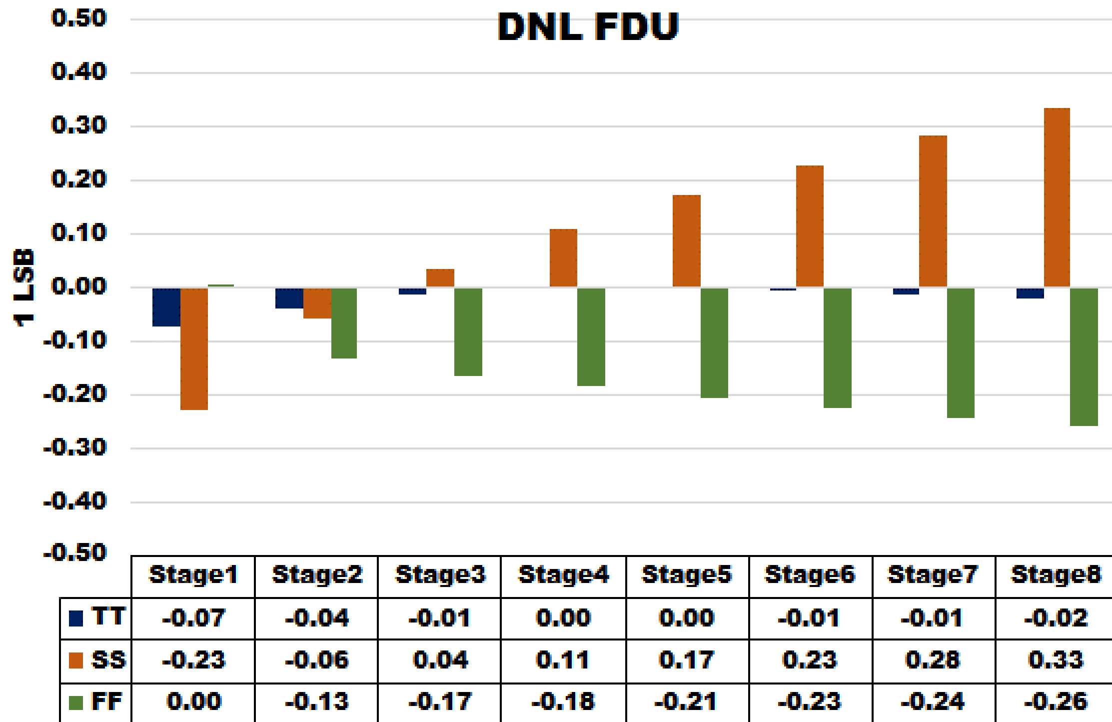
Phase error is measured using bang-bang phase detector and /or TDC depending upon the mode of operation. TDC is a power consuming unit and gating it reduces power dissipation. The design and constraints are explained subsequently.

4.5.2.2.1 Phase Detector

A phase detector is the timing comparator for reference clock and delayed pulsed clock. A 2 bit {up,dn} signal determines phase relationship of the given clocks. The SAR algorithm expects an {up,dn} signal to make decisions during the binary search. This circuit does not only compare the input clocks, but also provides a stable signal to the SAR register. The design of a PFD with a digitization circuit is shown in Fig. 4.16. The PFD has to not only resolve the time difference between the two clocks, but also has to do so processing a pulse for one of the clocks, which complicates the design of the PFD. Fig. 4.17 shows the waveform of the operation of the phase detector. The minimum phase difference that can be reliably resolved is shown in the table inset. Since the TDC is used to discern phase differences lower than one CD, a worst case difference of 76 ps is sufficient in reaching TDC measurement range. The PFD ensures lower power dissipation locking and the TDC is required during tracking but it dissipates more than 10 times the PFD power.

4.5.2.2.2 Time to Digital converter

The TDC along with a thermometer code is used to measure phase error in the order of 6 ps, since the phase interpolation divides the CD by 8. The fine delay design and variability was shown in the previous sections and the variability (σ) was seen to be less



	Stage1	Stage2	Stage3	Stage4	Stage5	Stage6	Stage7	Stage8
TT	-0.07	-0.04	-0.01	0.00	0.00	-0.01	-0.01	-0.02
SS	-0.23	-0.06	0.04	0.11	0.17	0.23	0.28	0.33
FF	0.00	-0.13	-0.17	-0.18	-0.21	-0.23	-0.24	-0.26

Fig 4.19 Differential non-linearity for the FDU across corners, even at the worst case the DNL is less than 0.35LSB.

than one ps. The TDC design is shown in Fig. 4.18. Four CD stages produce 32 bit fine interpolated edges, which are used to clock the reference clock edge and create a thermometer code where the transition from 0-1 determines the useful data of phase difference. The 32 bit code is fed to a thermometer encoder to create a 5 bit signal representing a value from 0-31. Value of 16 denote perfect locking, values less than 16 ensure pulsed clock to be leading and values less than 16 denote pulsed clock to be lagging. TDC is centered to a value of 16 with the use of the δ delay, which ensures that the pulsed clock is delayed by mux and 16 stages of fine delays.

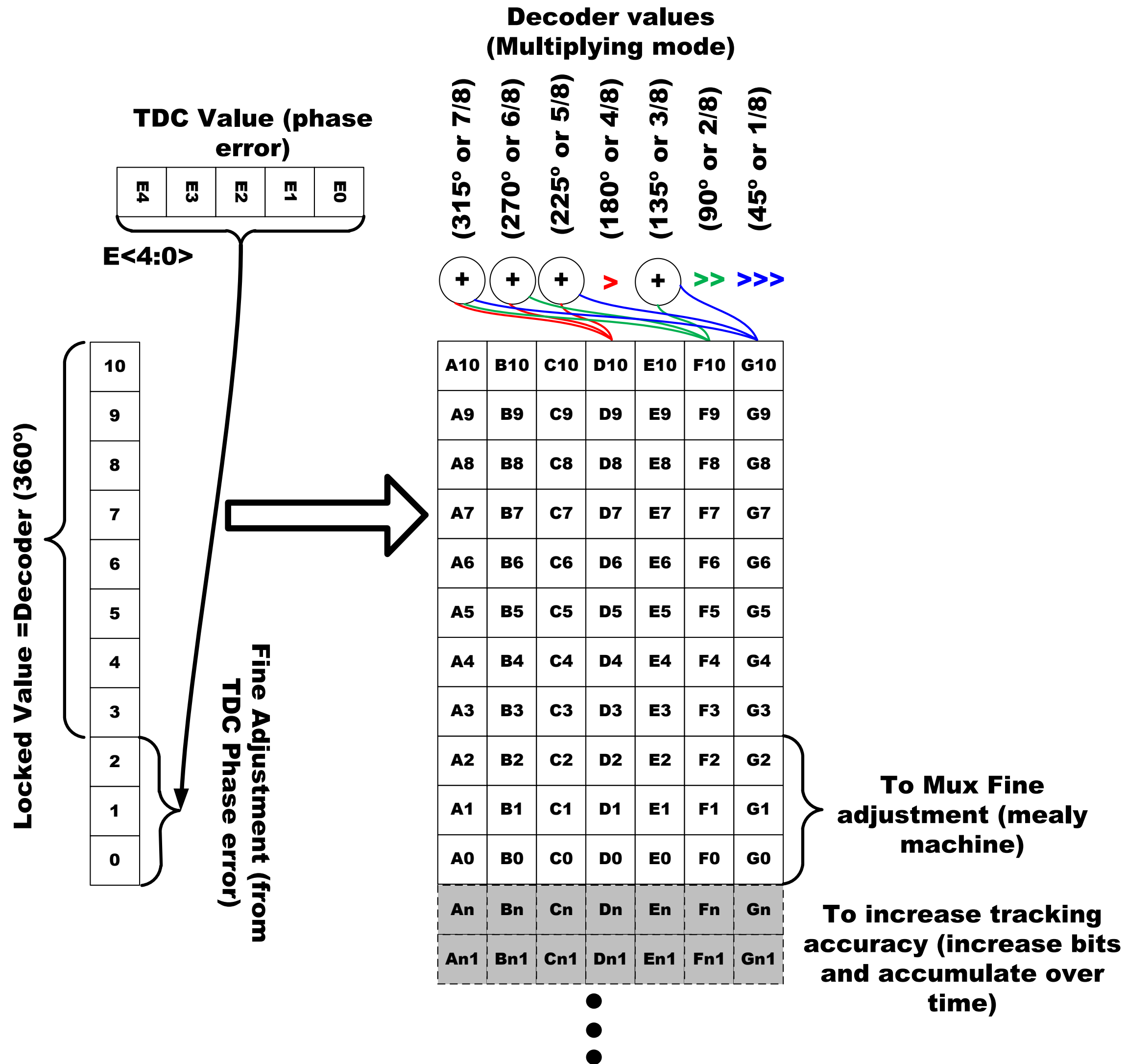


Fig 4.20 Arithmetic multiplied code creation for high frequency clock injection, 1/8-7/8th of the locked values with the 2^{-1}, 2^{-2} and 2^{-3}bit position values calculated and maintained with shift and add arithmetic to allow locking resolution of ~6.25 ps, can be further improved with increasing bit positions and accumulating the values for increased power.

The simulated differential non linearity (DNL) across different corners is shown for the interpolator unit delay (4.19). The worst case DNL is at SS corner (0.33), which means a worst case non linearity of 33% of one fine delay (~ 2 ps).

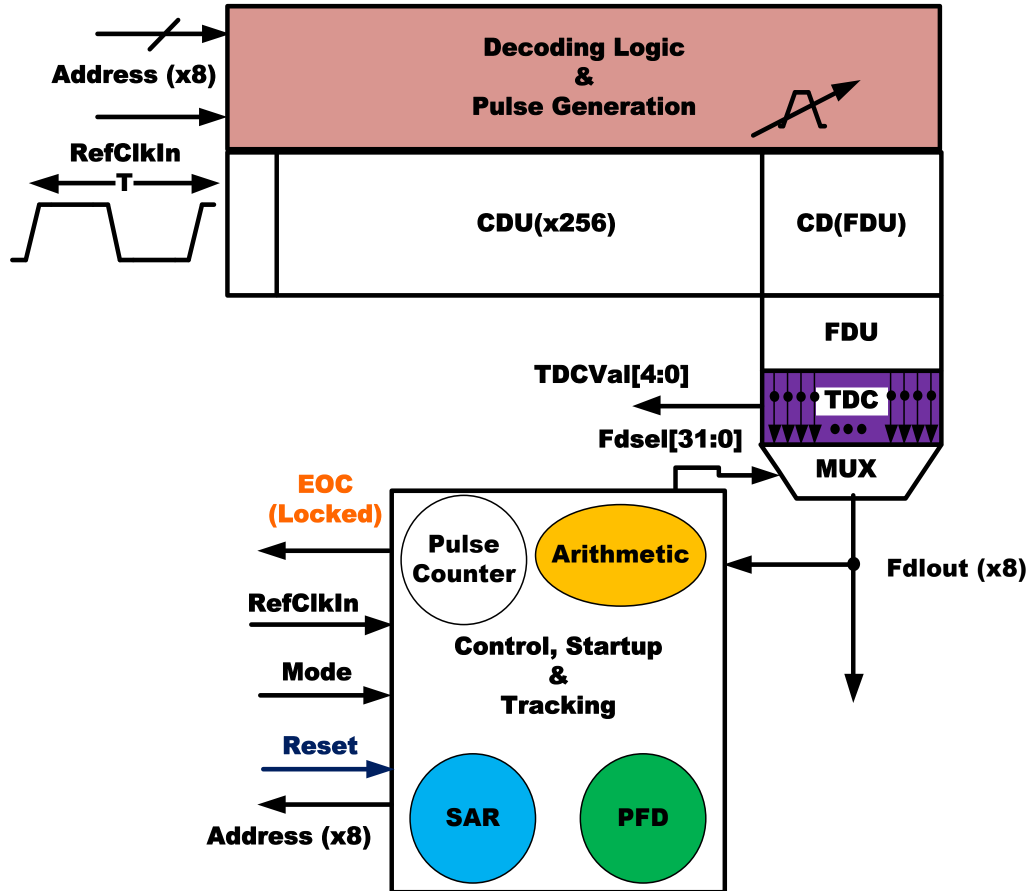


Fig 4.21 Color coded ADPMDLL top level diagram which is the reference for waveform definition of working of the ADPMDLL in Fig. 21.

4.5.2.3. Frequency multiplication through arithmetic pulse injection

The multiplication of reference clock in this ADPMDLL is done using simple binary arithmetic. Arithmetic unit injects 3 or 7 more pulses in the delay line based on the mode of operation (DDR2 or DDR3). The arithmetic unit processes the SAR output locked code value and then injects seven more pulses (related to 1/8, 2/8, 3/8, 4/8, 5/8, 6/8, 7/8 times the SAR lock value T_{ref}). Three out of the seven pulses are generated by right shifting the code SAR value to create 1/8, 2/8 and 4/8 values, then the rest are produced by the addition of these three values. No dividers are used in the synthesis of this arithmetic unit

since the FDU can produce the (1/8th) values of the CDU. Therefore, the overall code can be described with an 11 bit value where the MSB 8 bits defines the decoder values and the LSB 3 bit defines the decimal values from 1/8 or 0.125 to 7/8 or 0.875)\. No values smaller than 1/8 can be tracked in this design. Increasing LSBs and accumulating the bits will allow further accuracy. No values smaller than 1/8 are ever encountered while the divisor is 8 and the SAR lock value is always between 0 and255. Fig. 4.20 represents the diagrammatic representation of the shift and add low overhead arithmetic.

Architecture with the arithmetic unit is shown in Fig. 4.21. SAR code [7:0] shows the code values (MSB) generated to inject 7 extra pulses into the locked design. The top level diagram has a color coding scheme for the different blocks in the ADPMDLL. With color coding, the functional waveforms are explained in the Fig. 4.22.

At time T1, after the reset is de-asserted, the first pulse is injected based on the start-up condition. The control logic makes a decision based on the bang-bang phase detector value. Successive approximation uses the {up, dn} bit to ascertain the new value of the SAR code. At time T2, the new value of the SAR code injects an updated pulse and a new value of PD and hence, a newer SAR code is generated. Pulse clock is brought closer to the reference clock in time (after successive cycles) and thus, the phase error is reduced successively. After 8 clock cycles at time T8 as shown, phase error is brought to less than 2 CD and thus, TDC outputs a value which represents a phase error of the order of fine delay unit (6 ps). The value of LSB for the code which are saved post right shift are used to correct for delay corrections less than 1 CD i.e. 1 FD (1/8CD) to 7 FD (7/8 CD). This

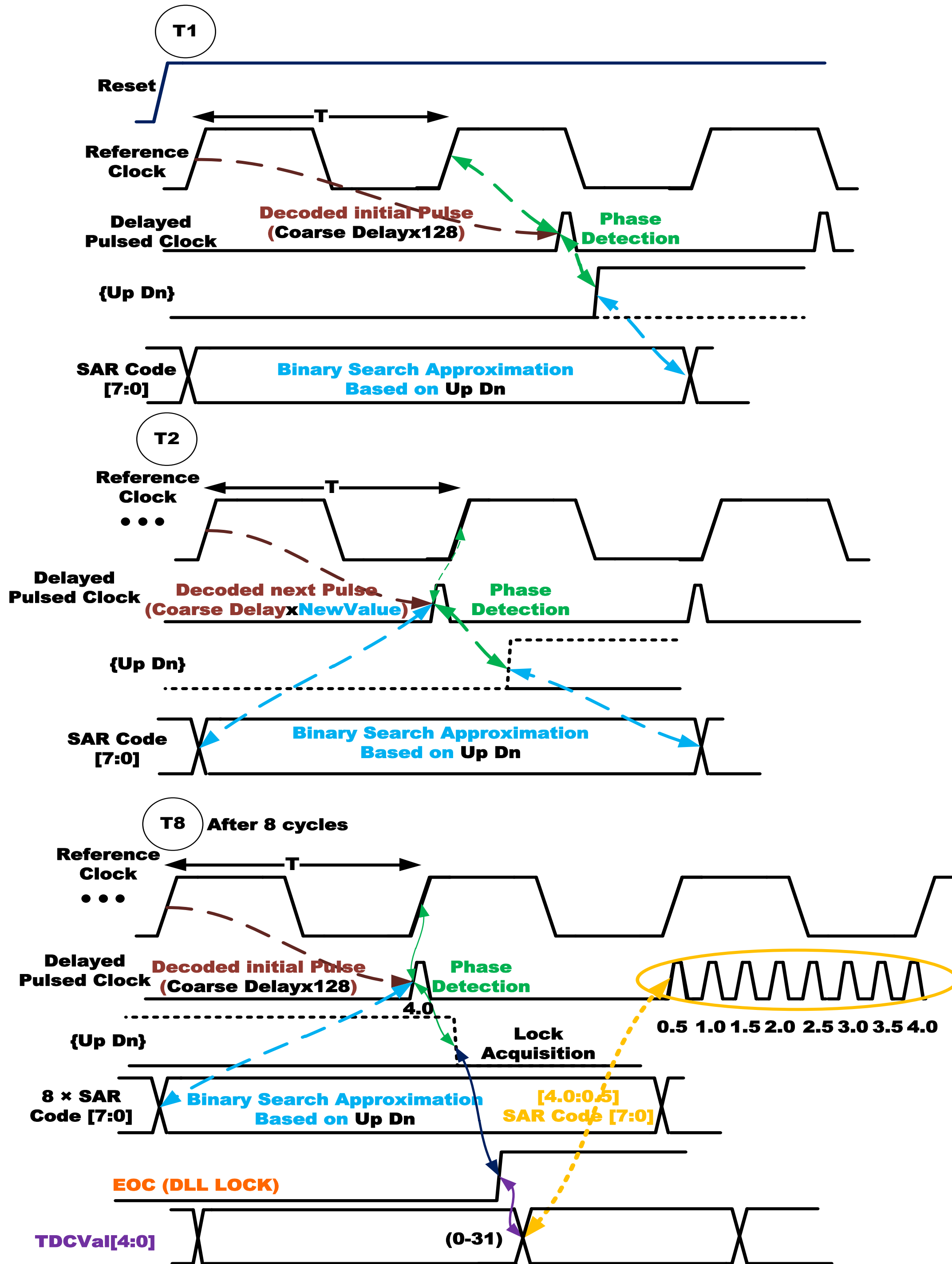


Fig 4.22 Color coded ADPMDLL top level functional waveforms, color corresponds to the unit which is causal to the signal.

correction is applied as a selection to the multiplexer such that each of the pulses can be corrected individually, time withstanding. This mux selection is a simple mealy machine

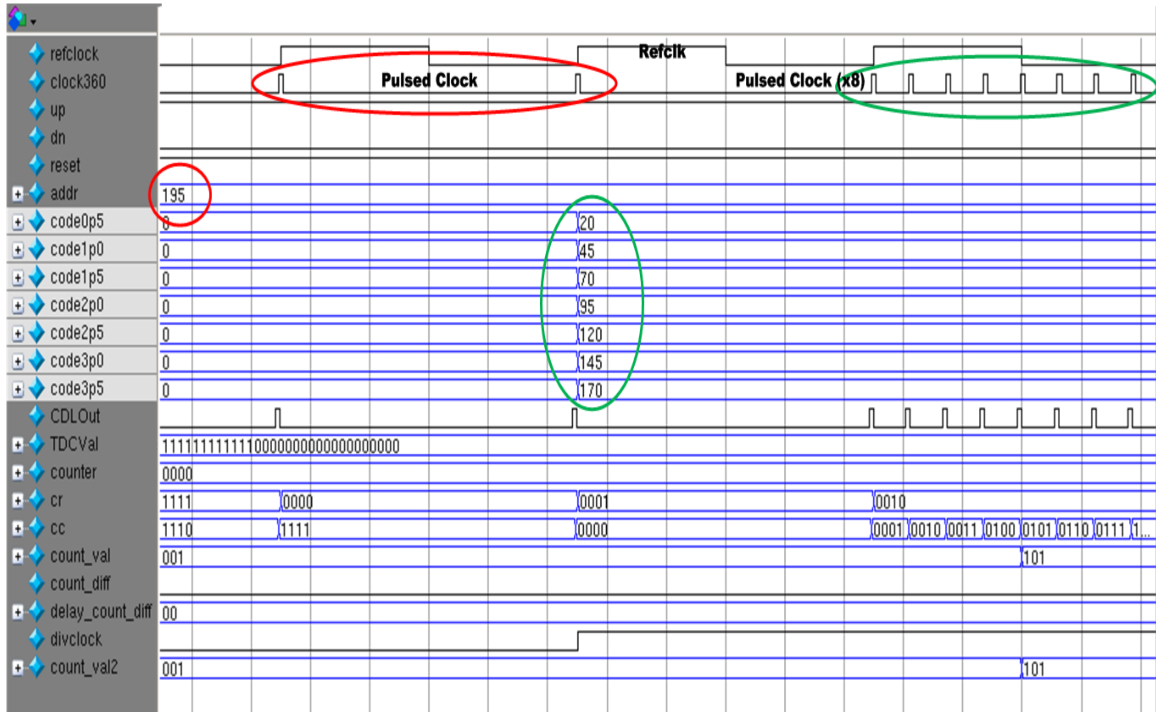


Fig 4.23 100 MHz clock locked with initial single pulses and with 8 pulses post locking. The locked code value (addr) is 195 and the divided values are shown for pulse injection.

such that the output and the state are the selection values to the multiplexer.

The total reference clock time period (TREF) is described in terms of the coarse (TCd) and constant delay (TConst) as per equation (2) where the constant n determines the coarse delay multiplier for locking. Using the value of n, the rest of the pulses are calculated by multiplying n by 1/8, 2/8, 3/8, 4/8, 5/8, 6/8, 7/8 and so on, respectively.

$$TREF = (n \times TCd) + (TConst) \qquad (2)$$

4.6. Functional Logic Simulations

With the circuit blocks and architecture of the ADPMDLL explained in earlier sections, the behavioral Verilog model is used to emulate the ADPMDLL operation.

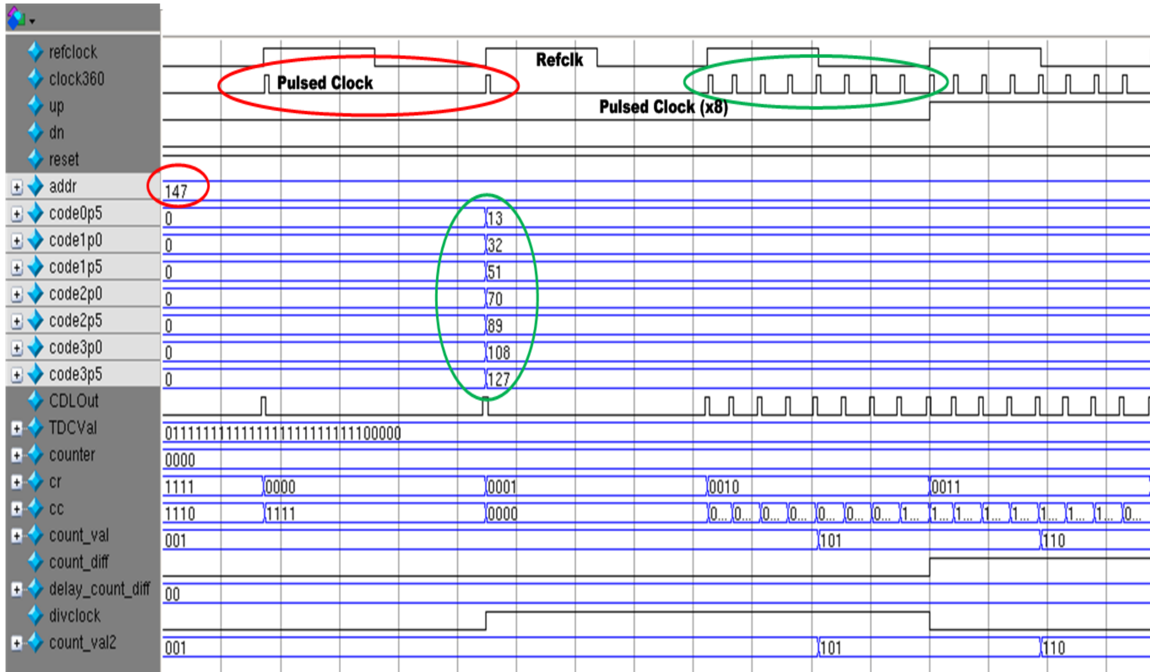


Fig 4.24 133 MHz clock with single injected locked pulse and post locking 8 pulses locked by linear interpolation with the code values and interpolated values circled in red. 8 pulses locked per reference clock. Locked value is 147.

Control blocks are synthesized and their behavioral and gate level models are both used to run and verify the simulations. The behavioral model contains 7 basic logic modules:

1. Digital Delay Line (Coarse Delay Line (CDL) Fine Delay Line (FDL))
2. Arithmetic control unit (ACU)
3. Time-to-digital converter (TDC)
4. Successive Approximation Unit (SAR)
5. Pulse Counter unit
6. Behavioral Decoder unit
7. Phase Frequency Detection unit

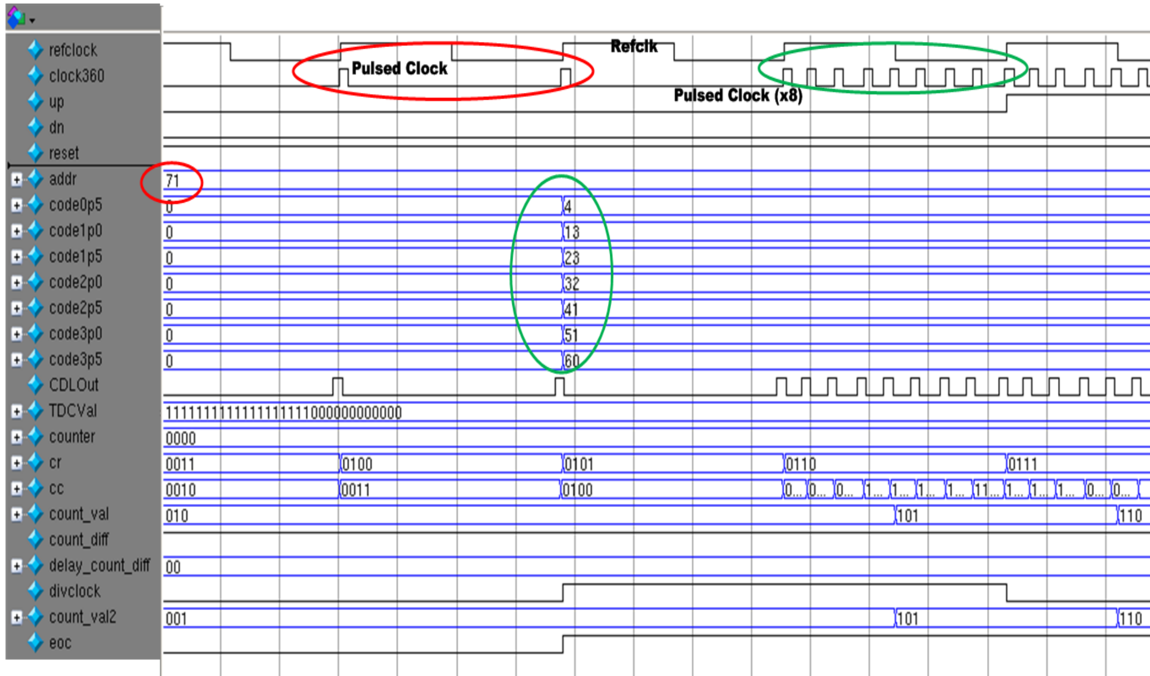


Fig 4.25 266 MHz clock locked with 8 pulses, single pulse injected and locked circled in red and the 8 pulses injected and locked circled in green. The locked value is 71, rest of the interpolated values are circled in red.

The simulations of the behavioral model are conducted with Modelsim simulator, where input reference clock is fed into the test-bench and locking of the delayed pulsed clocks is observed. The control logic uses the locked value to ascertain the locations to inject 7 extra pulses to create 8x clocking that constitutes the multiplied pulse clock. Since all signals cannot be monitored, the waveforms show the locking of three different input frequencies ranging from 100-266 MHz, with the only important signals for readability. Since these are 0 delay simulations, the critical paths will not manifest here. The efficacy of the Verilog modelling is shown through these simulations. The model can be used to improve functionality of the control section and allows for fast verification of newly added modes and modules (independent of timing). Fig. (4.22-4.25) show three different

frequency clocks producing a locked pulsed clock and a multiplied 8x clock (circled in green). The values of the SAR code, which the ADPMDLL is locked to, are circled in red and progressively decrease for increased frequency, signifying smaller number of delay elements in the path. The interpolated values are also circled in code and are named code0p5-code3p5. The naming corresponds to the 45 degree to the 315 degree clocks respectively produced by arithmetic interpolation. Individual control logic blocks and functionalities are verified and debugged using these simulations.

4.7. Process Variability

Process, voltage and temperature (PVT) variations in the ADPMDLL cause the delay of the ADPMDLL elements (coarse and fine delay units) to vary. Variation of voltage and temperature affects the stages in an analogous manner throughout, unless the temperature and potential drop values are localized in nature. A DLL corrects for the PVT variations by counting number of delay elements that make up reference clock time period. When the delay of the coarse and fine delay varies, the count value n for the standard reference clock period varies, too. The variation of the coarse and fine delay determines the quality of jitter performance, since random variation cannot be normally corrected for by design techniques, unless the design is calibrated post-fabrication. Variations can be reduced by increasing gate area, but this increases total area of the design. These can, however, be calibrated out post silicon in this work with a calibration mode that measures the variation of each of the high frequency pulsed clock paths.

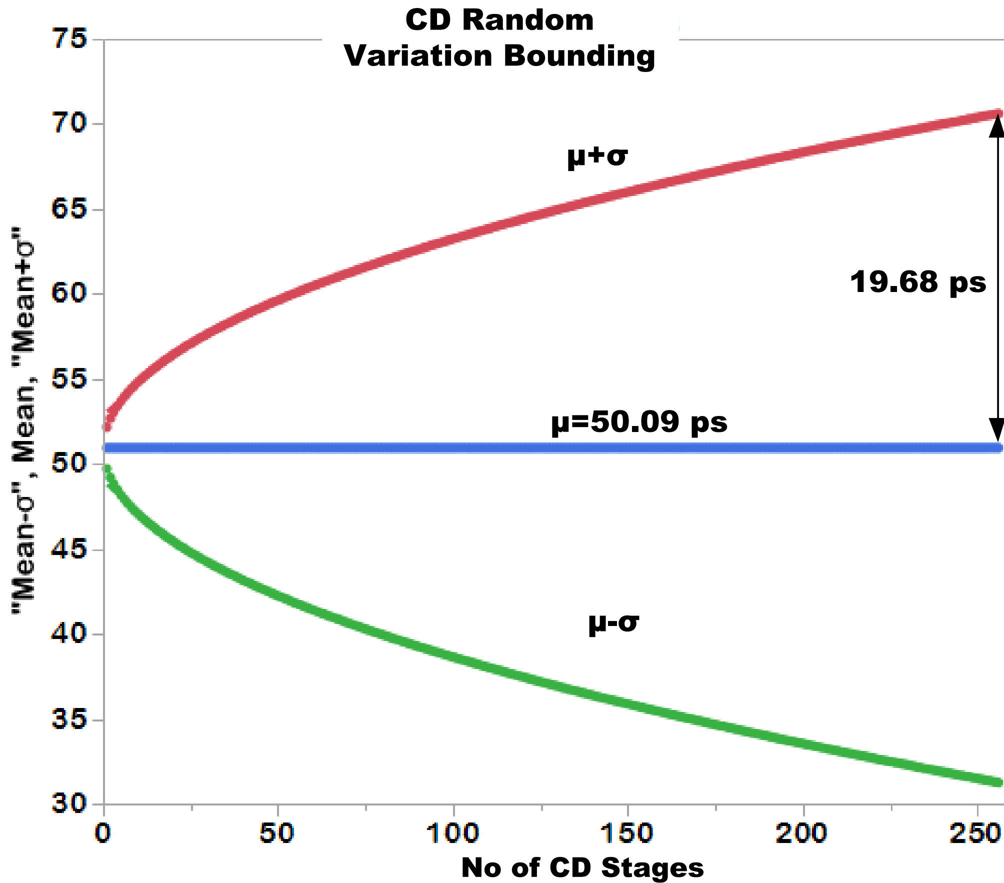


Fig 4.26 Coarse delay 1 sigma variation bound for one coarse delay unit. A maximum variation of 19.68 ps can be accumulated due to coarse delay random variation.

Random Gaussian effects on the other hand affecting the delay variation can be estimated based on the number of samples, measured mean (μ) and standard deviation (σ) for design constituents as calculated using Monte-Carlo simulations. Coarse and fine delay systematic variations in this work are correlated, as opposed to, other implementations where the coarse and fine delays have uncorrelated Gaussian variation i.e. μCD, σCD and μFD, σFD. For example, in a 90 degree phase shift delay locked loop [Kang12], there are

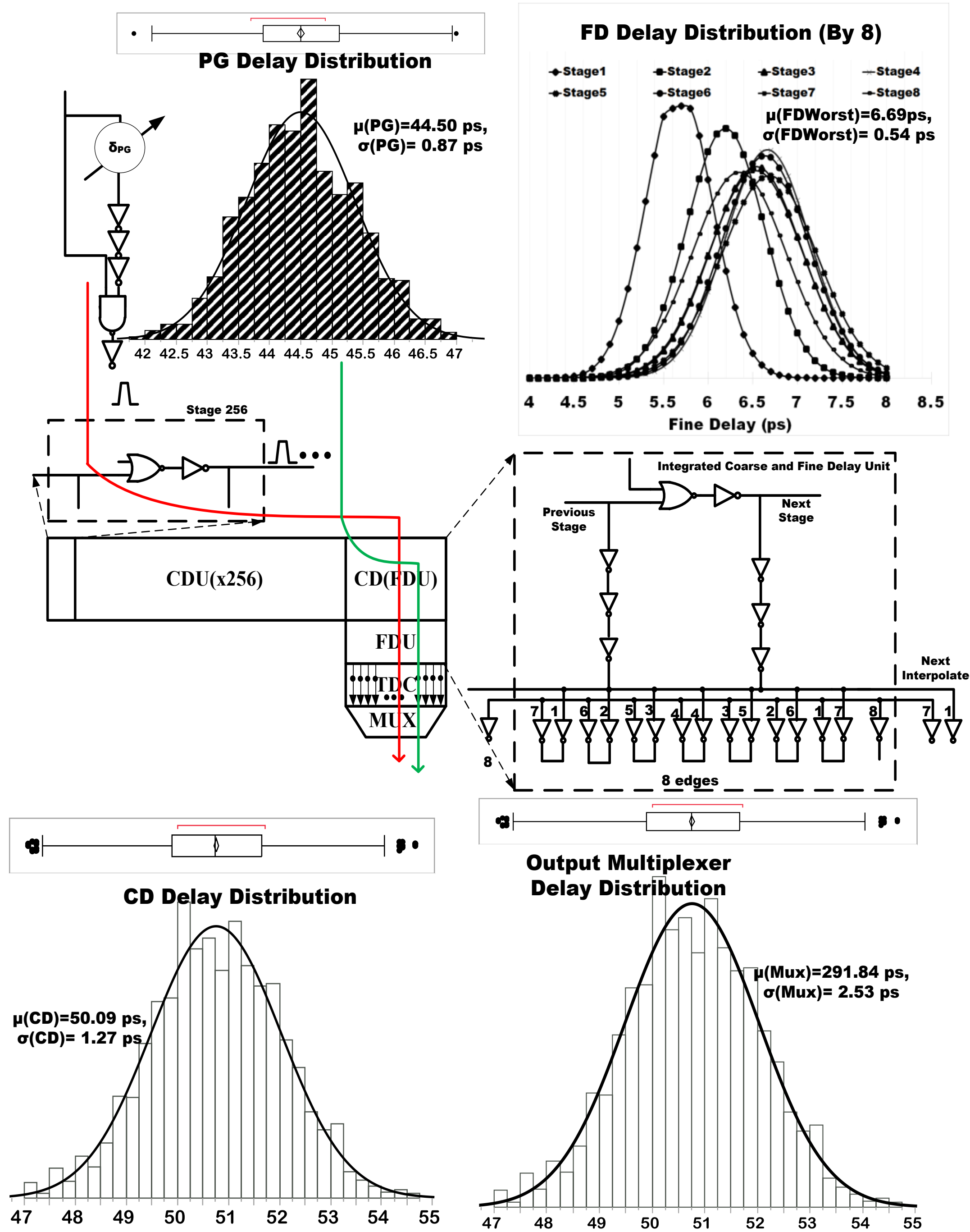


Fig 4.27 Gaussian noise mismatch analysis summary for the ADPMDLL, mean and sigma of the corresponding units are shown, only units which are in critical path and hence contributing to phase error/jitter specifications are shown. Green and red arrows indicate the fast and slow paths contributing to the variation leading to phase error in the high frequency clock.

4 independent delay lines where the CD and FD are controlled through the control logic

and the clocks are XORed to create the high frequency clock. Gaussian mismatch exists within the CD of a single delay line and between the 4 delay lines. Therefore, the mean and sigma increases based on CDU mismatch between either the same delay line or between multiple delay lines. Having a single delay line therefore reduces matching requirements, as opposed to four delay lines. Additionally, since the fine delay is derived from the coarse delay, the systematic effects should completely track, since the loading and input transitions are identical.

The mismatch is not only a function of the PVT variations, but is also a function of the frequency, since at higher frequencies a lower number of CDs are selected in the chain. The coarse delay min. and max. stage delay under presence of variation as calculated by the Monte-Carlo variation is shown in 4.26. Fine delay line is also common to all the pulses and hence, there is no mismatch introduced due to matching between separate elements. The only mismatch is introduced between the 32 unique multiplexer and interpolator paths which are characterized in Fig. 4.27. The mean and sigma of the mismatch that would be introduced between each element is shown. The critical path is only taken into consideration, since the elements outside of the critical path will not play a part in the variability contributing to degradation of the ADPMDLL performance. We know that delay distribution in a delay unit due to process variation can be modelled by a Gaussian distribution with a mean μ and a standard deviation σ and is given by equation (3) [Datt06].

$$Delay\ Mismatch(Random) \sim N(\mu, \sigma^2) \qquad (3)$$

The bounding mismatch in the ADPMDLL can be categorized by studying the longest coarse delay chain length and the shortest delay chain length. The advantage in this

work is that the short path is already common to the long path and the extra added coarse delay stage is the only added variability, simplifying the analysis. Theoretical limits for CD variation are calculated below as follows.

$$Delay\ Mismatch(Max) = \sqrt{256} * \sigma(CDU)$$

$$Delay\ Mismatch(Min) = \sqrt{4} * \sigma(CDU)$$

Assuming uncorrelated delay elements through the critical paths (PG, CD, FD and Mux), the maximum possible variation that can exist in the delay chain for the given design is given by

$$\text{Total Delay Mismatch(Max)} = \sqrt{\left(\left(\sqrt{256}-\sqrt{4}\right)*\sigma(\text{CD})\right)^2 + \sigma(\text{FD})^2 + \sigma(\text{PG})^2 + \sigma(\text{Mux})^2}$$

$$= \sqrt{\left(\left(\sqrt{256}-\sqrt{4}\right)*1.27\right)^2 + 0.54^2 + .87^2 + 2.53^2} = 17.98\text{ps.}$$

At the typical corner, the delay mismatch calculated corresponds to approximately 3 FD taps. This mismatch value can be adjusted in the fine delay in a calibration phase such that at a specific operating frequency and condition, the mismatches can be calibrated out by setting fine delay taps in the output multiplexer that selects between the fine edges for each pulse. All these delay values are maintained in a small programmable memory in the control logic such that these correction values are added in the SAR code post locking. The tracked clock is also compensated for process variations in a completely programmable manner.

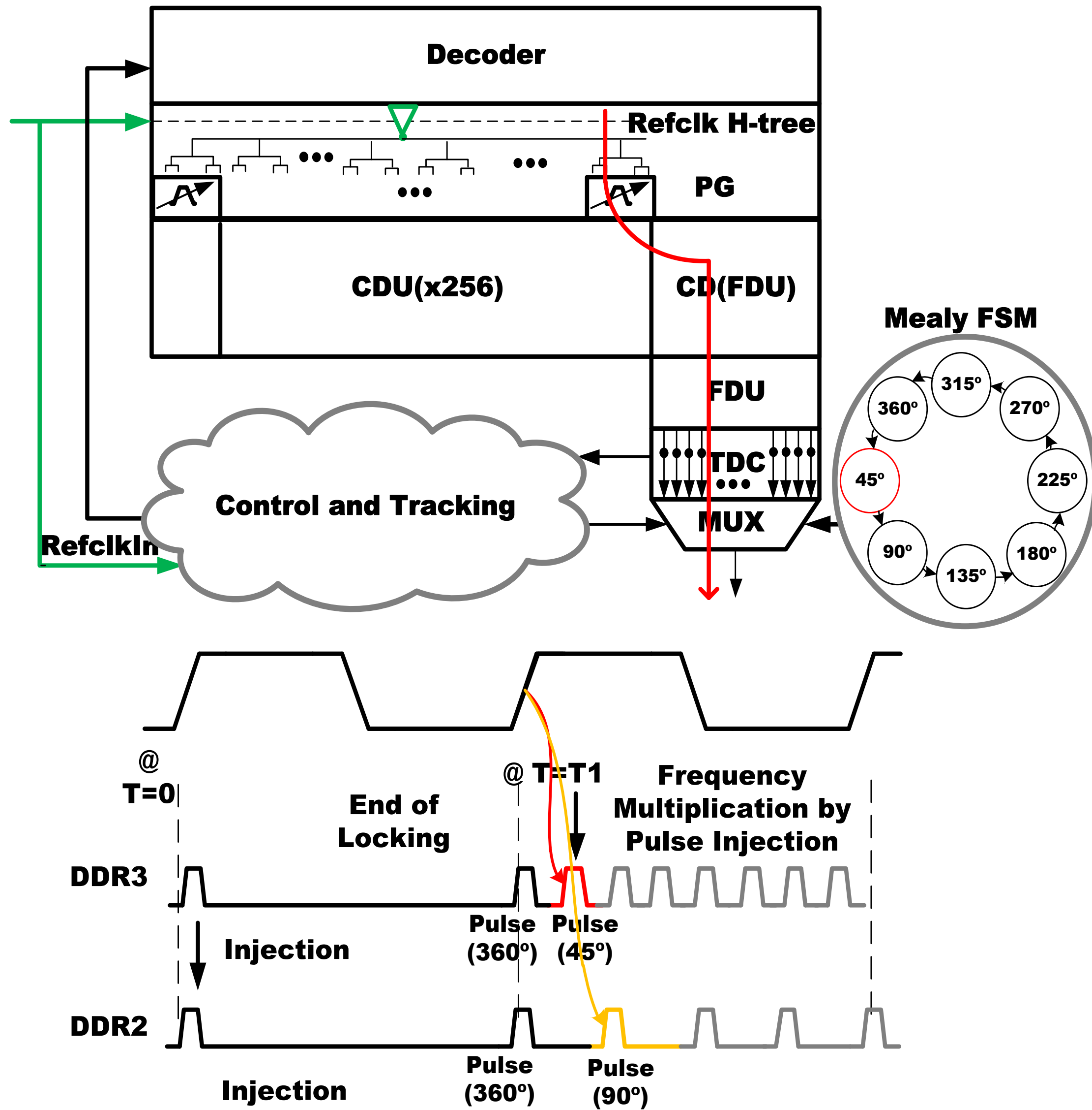


Fig 4.28 ADPMDLL critical path and critical path timing diagram highlighted in red, the fastest pulse injection (or the smallest delay) that can meet timing is the requirement for the successful frequency multiplication or pulse injection in the DDR3 mode. The equivalent path in DDR2 mode is shown in orange and is less timing critical than the DDR3 path as explained in previous sections.

4.8. Circuit Simulations and Critical Timing

With the design proven to be functional in Verilog and the custom design elements designed in custom design environment, the design is integrated on the transistor level with

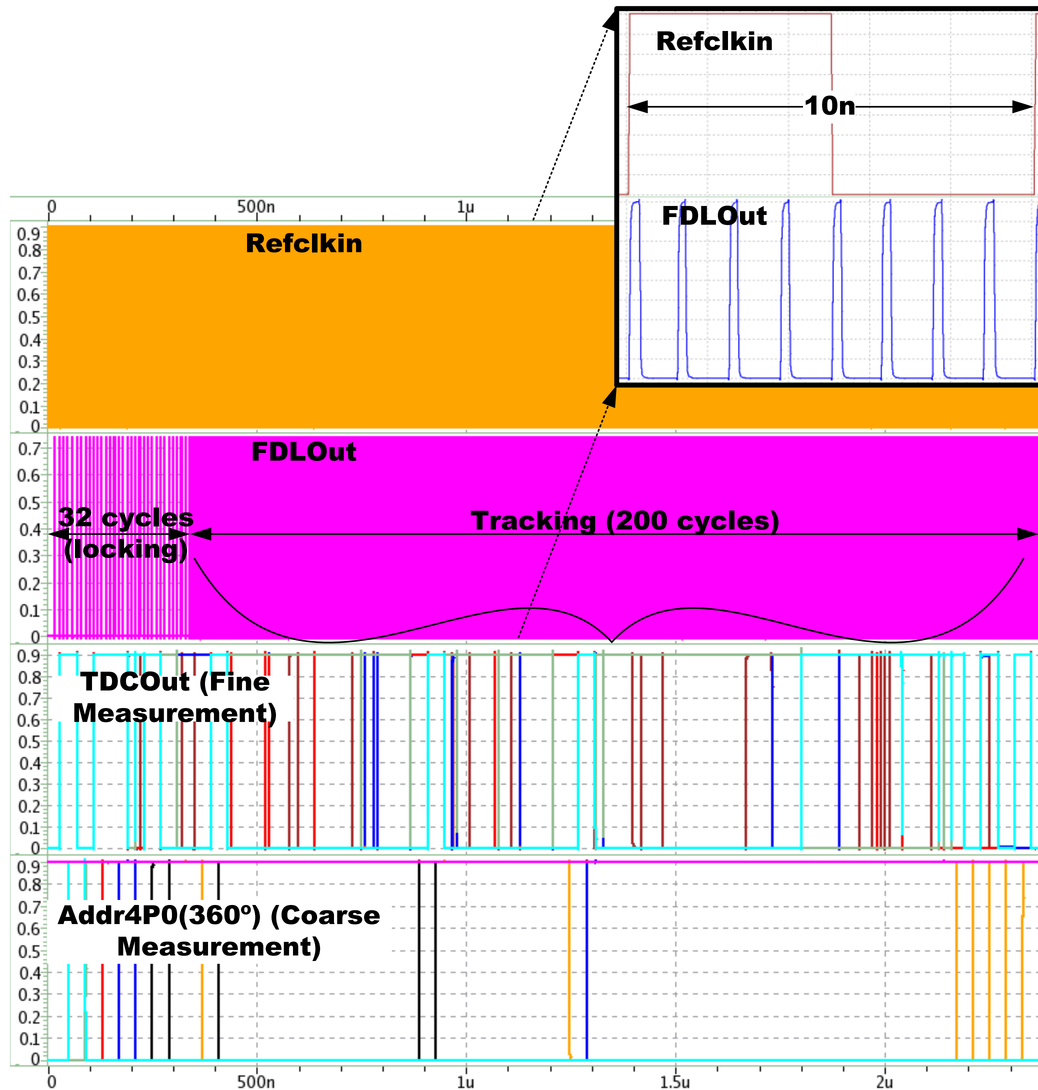


Fig 4.29 Spice (Ultrasim) simulation timing waveforms for a 10ns input reference clock cycle. Locking is completed in 32 clock cycles and the pulses are injected into the loop subsequently after. Tracking is observed for 200 cycles. TDC output tracks the phase error and eliminates jitter it with digital correction as described in the earlier sections.

spice (cdl schematics) to simulate the functioning of ADPMDLL. Across corners, simulations are undertaken to prove the quality of the design and the efficacy of the locking and tracking control logic. Critical timing requirements are also explored in this section, since the critical paths place the basic limit on the functioning of the ADPMDLL. Simulations in noisy environments and jittery input clocks are built on top of these

simulations to calculate performance metrics. The non-idealities that are not reflected in the Verilog simulations are encountered in the spice simulations and facilitates debugging critical timing issues in the design.

4.8.1. Critical Timing Paths

Since the ADPMDLL is based on pulse injection in the delay loop and arithmetic interpolation for frequency multiplication, the critical timing requirement of the ADPMDLL flows from the fastest pulse that can be reliably injected into the loop. To understand this limitation, refer to Fig. 4.28. Based on the value of the SAR code that is generated with binary search, the fastest pulse in the DDR3 mode corresponds to 1/8th the SAR value and this pulse propagates through the matched H-tree, the least number of CD units and then through the FDU and MUX. As the input frequency increases, the delay corresponding to the SAR code decreases and hence, the timing margin for the fastest pulse injection reduces, too. The 1/8th pulse corresponds to the 45 degree clock with respect to the reference clock. As shown in Fig. 4.28, the pulse highlighted in red is injected closest to the fine delay unit or the clock out path. The same path in the DDR2 mode is shown to have more timing margin since the clock is the 90 degree phase clock, which for the same delay, corresponds to higher DDR2 clock frequency.

Simulations are run in the 55 nm process at SS corner and with high body-bias (high-Vt state) show the critical path delays can be easily reduced by 30-50% in the multiplexer and the fine delay line (constant delay). The slow corner value required for

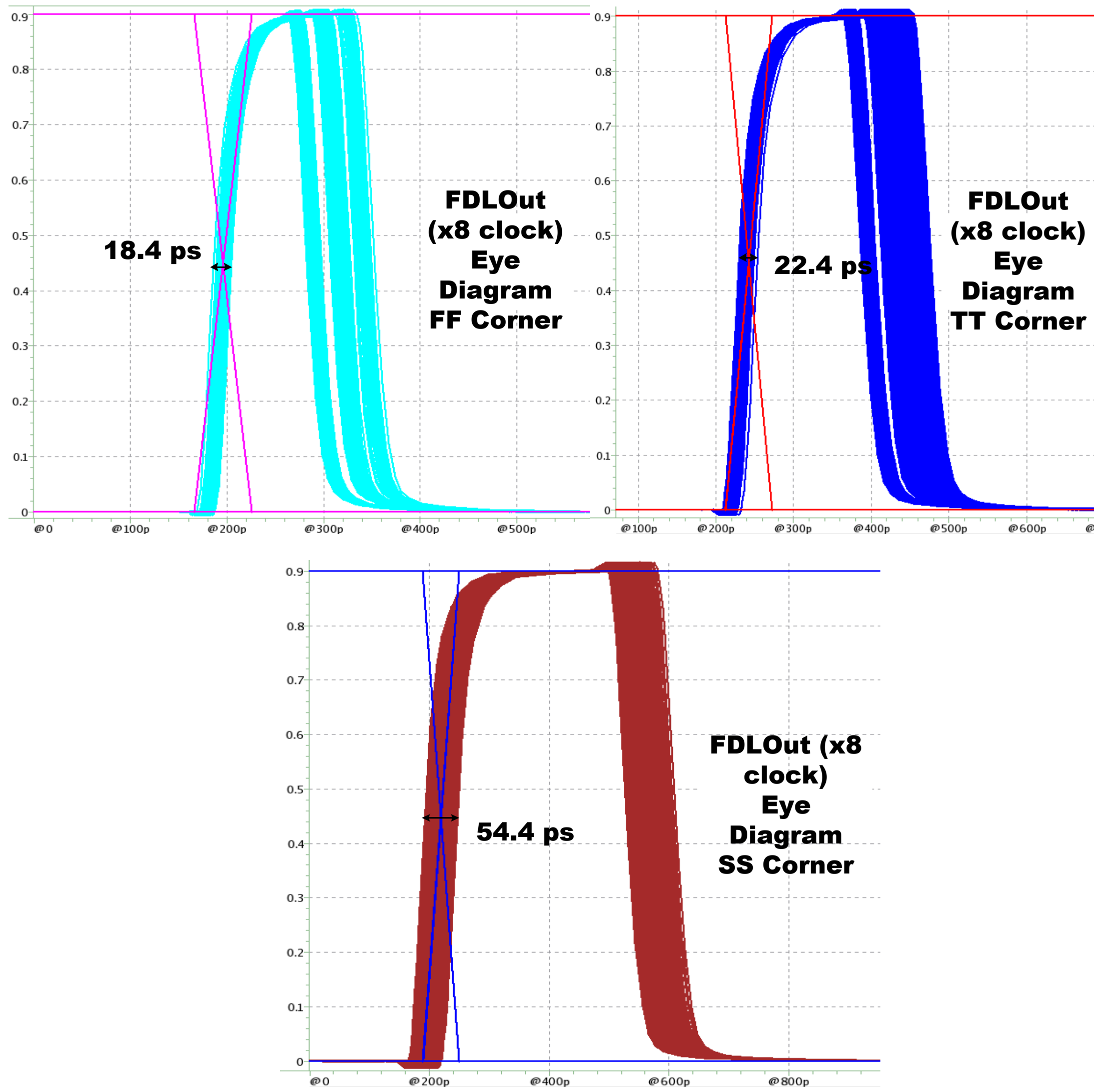


Fig 4.30 Eye diagrams showing peak-to-peak jitter for TT, FF and SS (clockwise) corner simulations. P2P jitter is below the required limit for DDR2 transfer as per the JEDEC specs. The black line indicates the ideal reference clock eye diagram. The falling waveforms with disparate waveform indicates the across corner pulse amplification/attenuation behavior where the pulse width constraint is still met.

successful pulse injection is observed to be ~900 ps. This value reduces with the increase in the clock frequency and at the highest DDR3 standard, the requirement is less than 500 ps. The highest speeds therefore need faster clock out path or an additional clock latency in the clock path. Thus, the scenarios described in this work are with the latency of 1 clock cycle or the best case in terms of total clock latency (non-aliased clock).

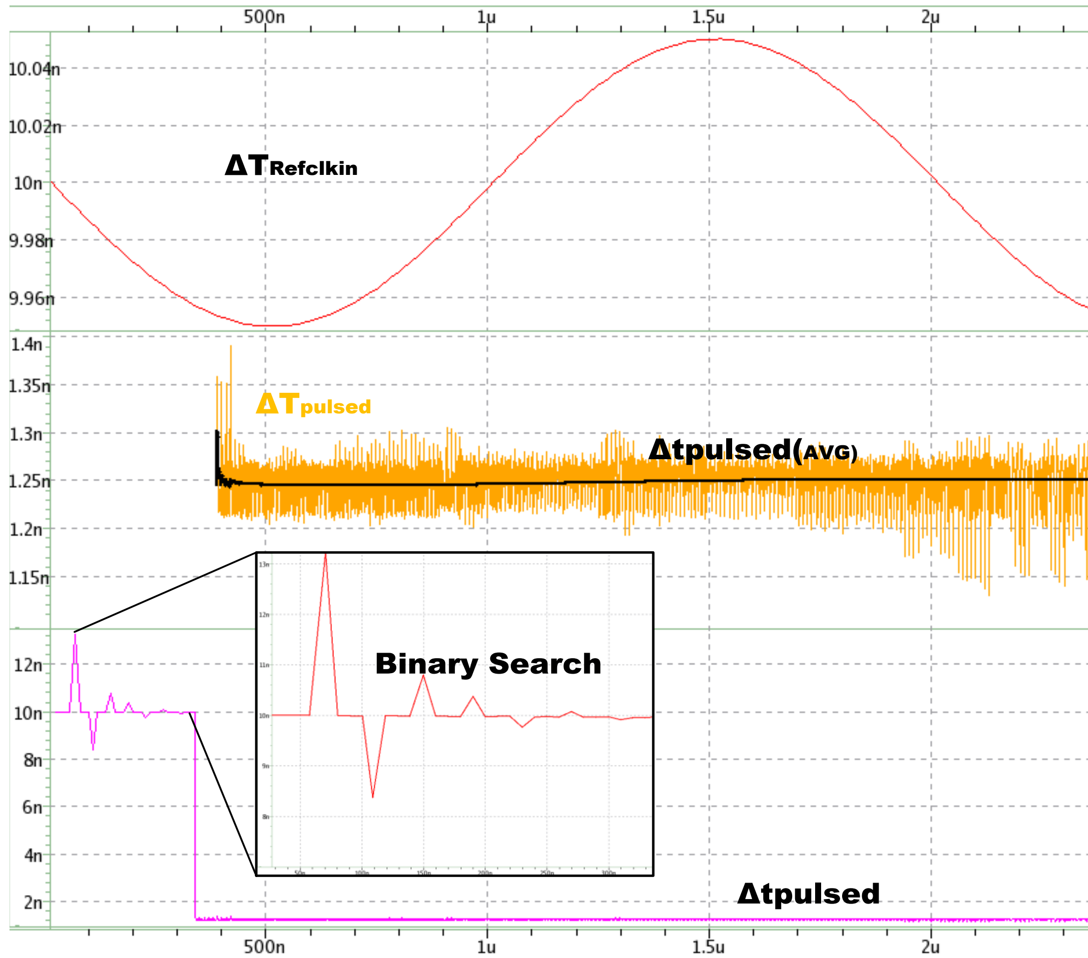


Fig 4.31 Noise performance of the APDMDLL in presence of a 500K 100ps P2P noise variation of input reference clock. The pulsed clock and its average is shown in the yellow and black respectively. Binary search algorithm for ADPMDLL locking in presence of input jitter is also shown.

Fig. 4.29 shows the output multiplied pulsed clock generated from the input reference clock of a 10 ns period. The 32 cycle locking period is shown and the coarse address measurement and the fine measurement of the phase error is also monitored. Other signals corresponding to Addr0p5-Addr3p5, end of conversion (EOC), etc. are not shown due to limitations of page length. The simulation waveforms correspond to run in the SS corner, but the TT and FF corner functionalities are also verified. The tracking algorithm

calculates the CD with variation across FF, TT and SS corners as the code value (code4p0) is decreased from FF to SS corner, since the value calculated depends on the division of reference clock by the variable across corner coarse delay values.

4.9. Performance Overview

The performance metrics of the ADPMDLL are presented in this section. A DLL performance is measured primarily in terms of the range of operation, the jitter performance and the power dissipation of the system. The proposed work can be operated in two operational modes (DDR2 and DDR3) and a low power mode, where the lock is not lost and the interface link can be maintained at minimum power operation between the interfaces. Duty cycle is very important in classical DLLs, but in the pulsed DLL presented here, the individual pulses are easily controlled to an LSB precision of the FDU. Hence, the quality of the high frequency clock is very well maintained and duty cycle correction is not required.

4.9.1. Jitter Performance

We start with measuring the jitter of the ADPMDLL in terms of the P2P jitter observed in the DDR3 mode operation across the 3 corners as simulated. The digital control and tracking circuitry controls the instantaneous jitter value by digital integration and correction. The quality of the control is a function of the non-linearity observed in the FDU and TDC and the tracking of the centering delays across corners. Fig. 4.30 shows the eye diagram for the high frequency pulse clock in the DDR3 mode. The ideal reference clock

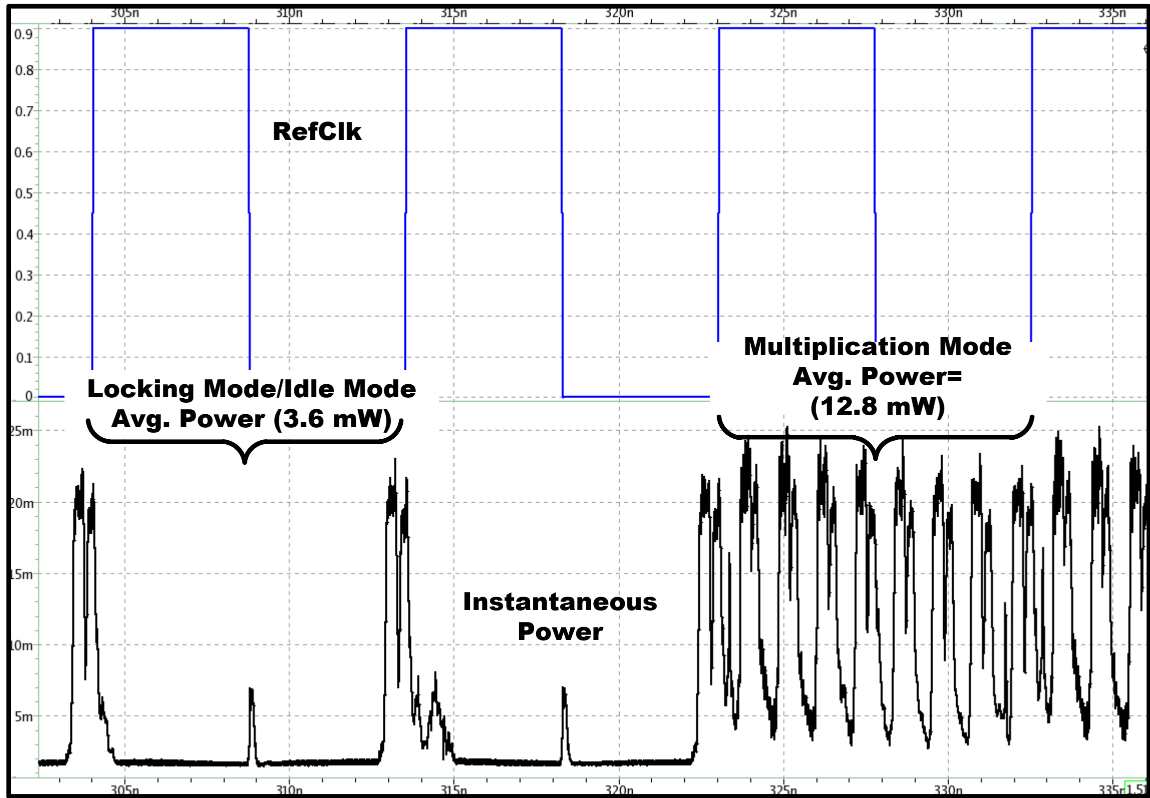


Fig 4.32 Power measurement waveforms of the APDMDLL, locking/idle mode power and multiplication mode are both shown, as expected much higher activity is observed while producing DDR3 standard multiplied clock.

is shown and the peak to peak value observed over 200 cycles according to the JEDEC standards is recorded. Peak to Peak jitter performance does not improve at the FF corner as compared to the TT corner since non-linearity is more pronounced at FF and SS corners as shown in the previous sections.

4.9.2. Noise (Input Jitter) Performance

To simulate a noisy input source and study the tracking characteristics of the ADPMDLL in the presence of input jitter, a sinusoidal variation of the input reference clock in kilohertz range is fed as an input to ADPMDLL. Fig. 4.31 shows the waveforms for tracking of a noisy input reference clock. Output multiplied clock frequency is observed

and the average output frequency shows excellent jitter filtering characteristics. It can be seen that the binary search locking algorithm is not affected by the 100 mV P2P variation. The digital nature of the tracking algorithm makes the simulation and estimation of the jitter performance in the presence of noise relatively simple.

4.9.3. Power Dissipation

As described previously, the ADPMDLL has 4 major operating modes namely, Locking, DDR2, DDR3 and Idle mode. The first three modes are operational modes, whereas, the idle mode as the name suggests is a lower power mode which can be used in scenarios where the high-speed interface/link is idle. This mode allows the DLL to remain locked in a low power mode, as opposed to normal DLLs which require re-acquisition of lock. ADPMDLL can operate in the reduced power mode while it is still locked. Here the high-frequency pulse-injection is stopped, the SAR values are kept constant and the TDC is switched off, leaving only the bang bang phase detector turned on to track the clock by +/- ~1 CD.

The probability of the clock wandering is low, since the input clocks in DDR interfaces are required to maintain the input jitter specifications. The phase-detector can easily maintain the acquired lock by stepping up or stepping down the CD values. In case the lock is lost, the EOC signal is un-set and the lock process can begin, incurring the 32 cycle lock penalty.

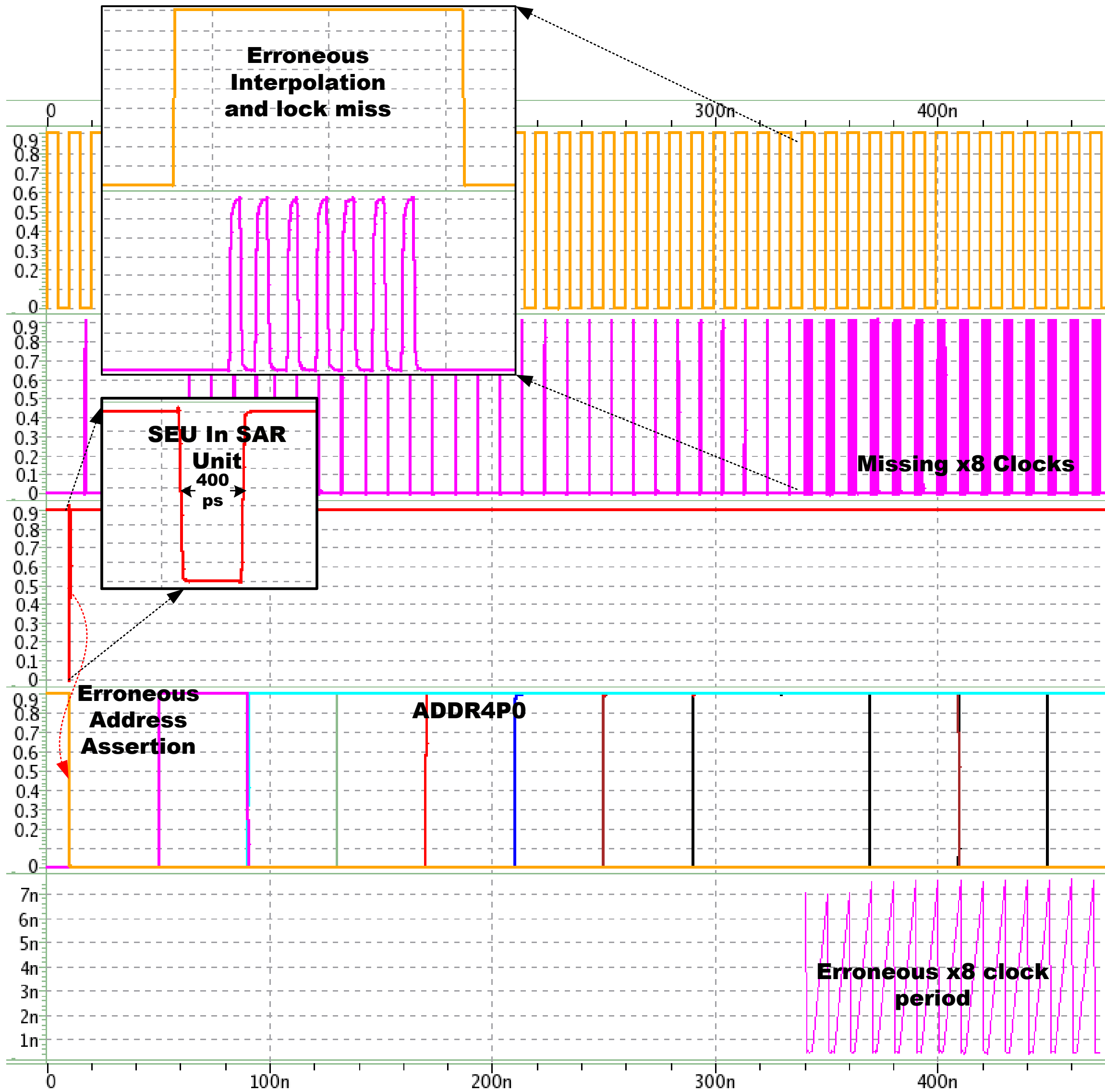


Fig 4.33 Simulation waveforms of soft error vulnerability in the proposed ADPMDLL design. SAR unit is upset with a 400 ps SET which is captured by the sequential units and results in missed acquisition and merged pulses.

Fig. 4.32 shows the simulated power waveforms from Ultraism simulations at the slow corner. All the sources of current (power and well biases), are added up to ensure accurate power calculation. Instantaneous power at the two modes is shown; idle/locking mode and the high frequency DDR3 mode. The power calculated is the integral of the curves over one period (cycle). In lock mode and in high frequency multiplication mode,

the power is 1.6mW and 12.8 mW at 850 MHz (Maximum speed), respectively. Thus, the idle-locked mode allows 88% power savings.

4.10. Soft-Error vulnerability

The vulnerability to digital designs from particle upsets have been discussed in detail in the background sections of this dissertation and the effect of a radiation particle causing charge collection or a soft-error is studied in this section. Since the design is all-digital and based on pulse clocks, it is especially vulnerable to soft-error upsets due to pulse-clock generators and pulsed flip-flops having a much higher soft-error rate compared to standard flip-flops [Seif2005].

The simulation of an SET in the digital control SAR unit is shown in Fig. 4.33. The SET creates an SEU in the SAR unit and the code is erroneously switched as a result. This results in incorrect lock acquisition and clock multiplication. The base SAR address ADDR4p0, which corresponds to the 360 degree clock, is the clock code value that is upset and the pulse clock therefore is neither locked to correct frequency nor produces the correct number of edges for the high frequency clock. This simulation proves the need for radiation hardening by design techniques in our proposed work. The basic technique explored in this work is TMR, where the ADPMDLL is triplicated and voted out prior to capturing the data or sent as 3 clocks to the radiation hardened TMR DDR3 interface physical layer (PHY).

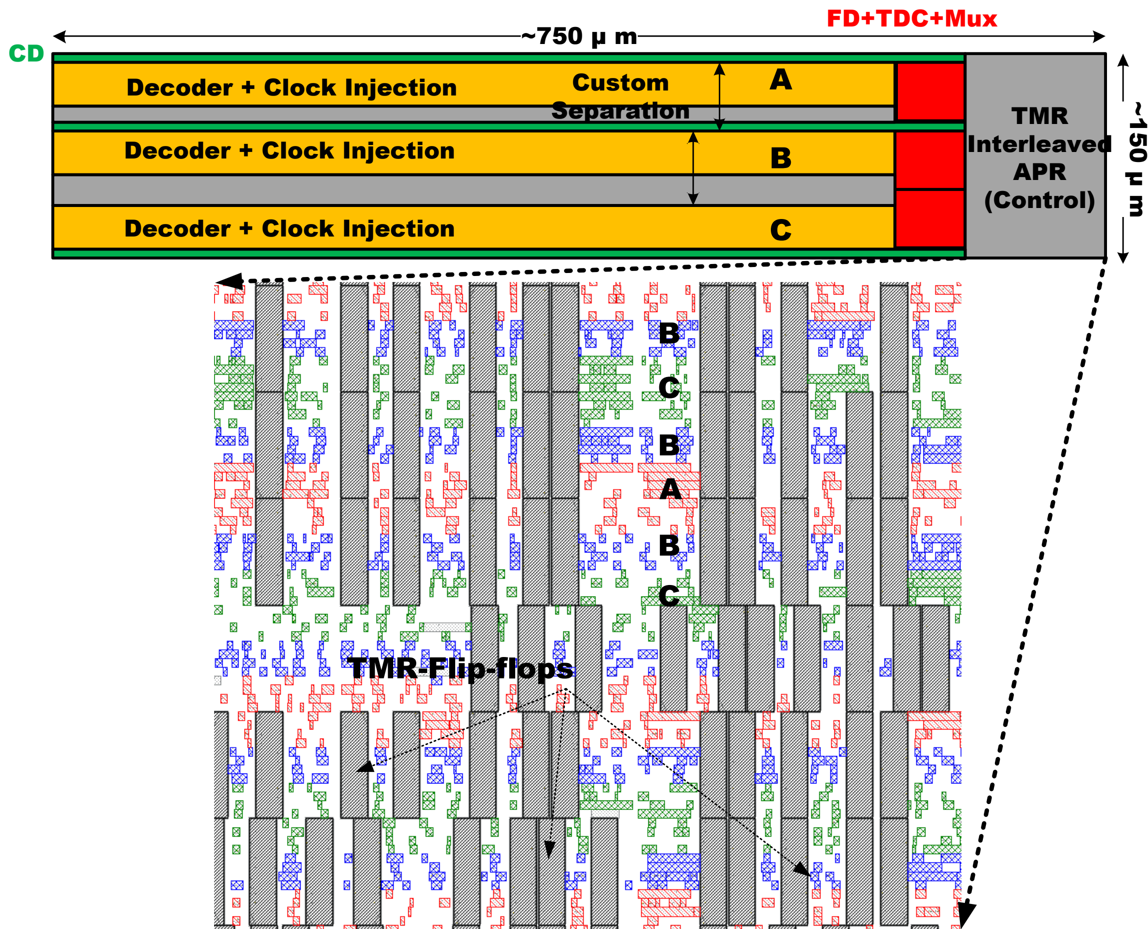


Fig 4.34 Block level schematic of the test structure taped-out for the purpose of delay variability and fine-delay non-linearity. The delay unit is different from the unit described in this work, the implemented design in test-chip (TC25) was not a pulsed design, the components however were shared.

The layout plan of the ADPMDLL is shown in Fig. 4.34. The proposed plan is 0.1125 mm^2 and the non-redundant version is 0.375 mm^2. As explained previously, these majority voted output clocks are matched in routing and buffering in order to produce a matched radiation hardened DDR3 standard clock. The proposed DLL is not only radiation hardened, but also multi-node charge collection immune, since the sensitive nodes are not

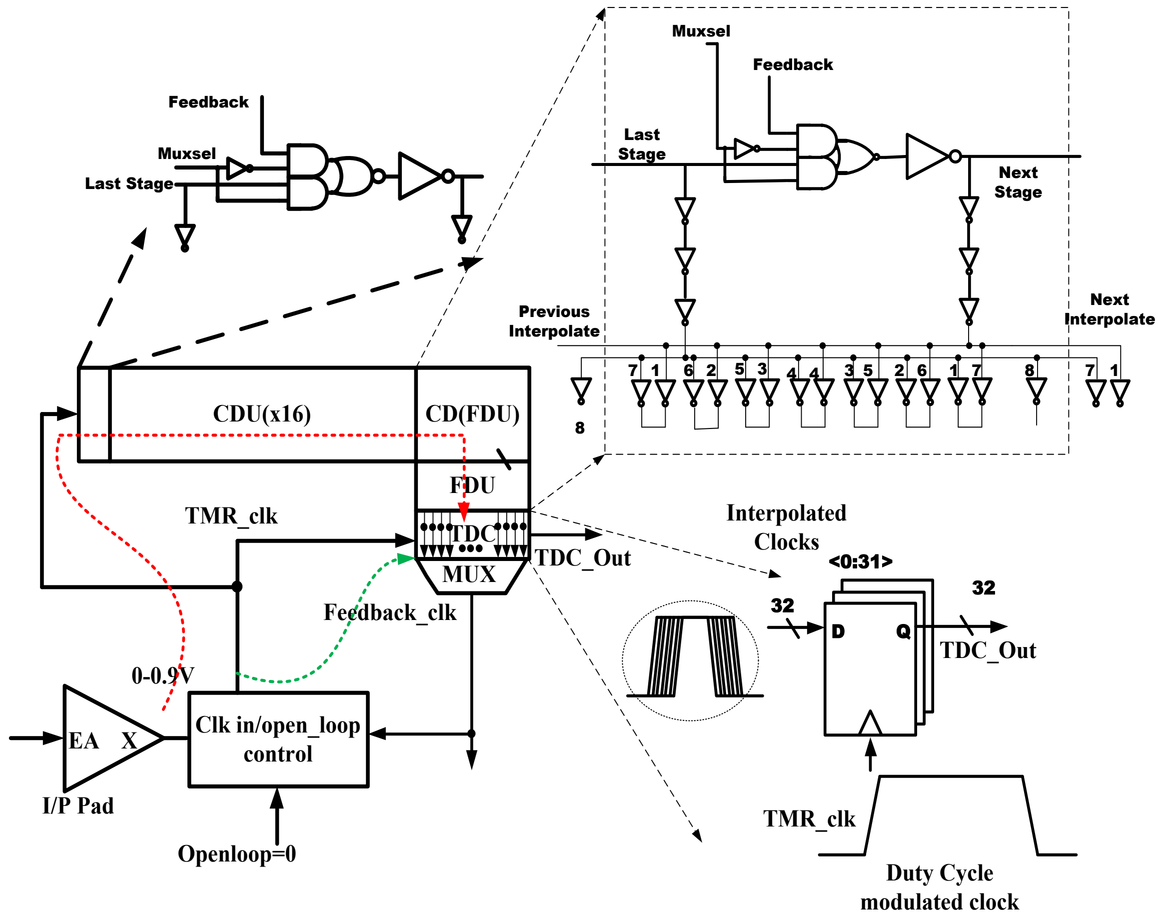


Fig 4.35 Block level schematic of the test structure taped-out for the purpose of delay variability and fine-delay non-linearity. The delay unit is different from the unit described in this work, the implemented design in test-chip (TC25) was not a pulsed design, the fine delay unit components however were identical.

only triplicated, but also separated by sufficient (4 standard cell heights) distances in space, thereby ensuring very insignificant multi node upsets cross section. While previous radiation hardened DLL's use ECC and TMR, both exhibit performance at very low frequencies (DDR-133 MHz/DDR2-267 MHz), with a 90 degree phase shifted clock.

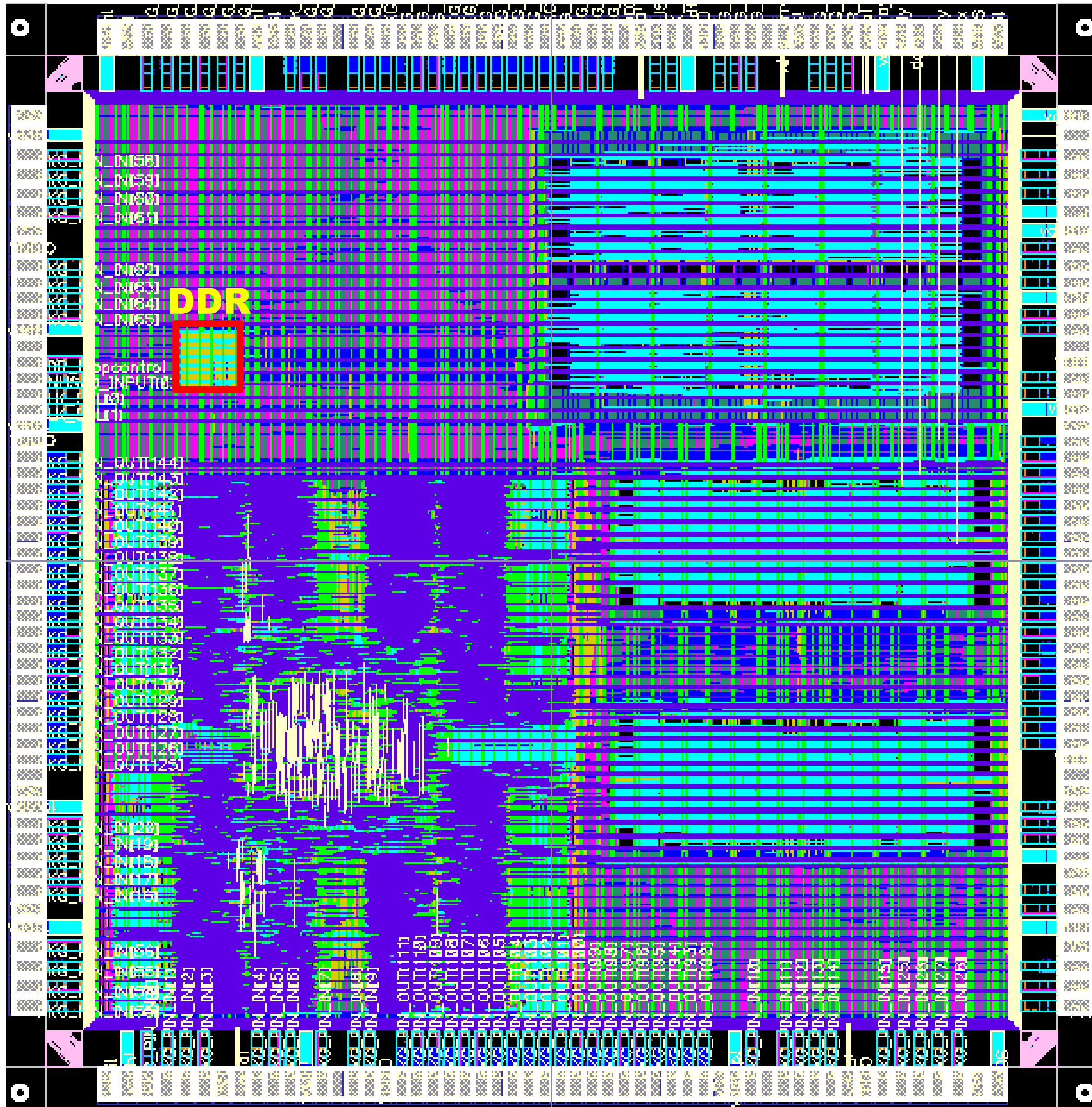


Fig 4.36 TC25 test-chip snapshot showing the DDL test-structure in red. The test-structure is fabricated inside a 4 by 4 mm die with wire-bond packaging.

4.11. TC 25 55-nm Test-chip Structures and Results

To study the quality of delay variation due to random and systematic effects, test-structures were designed and fabricated on a 55 nm low standby power process. A test chip (TC25) contained the test structures shown in Fig. 4.35. A coarse delay element chain and

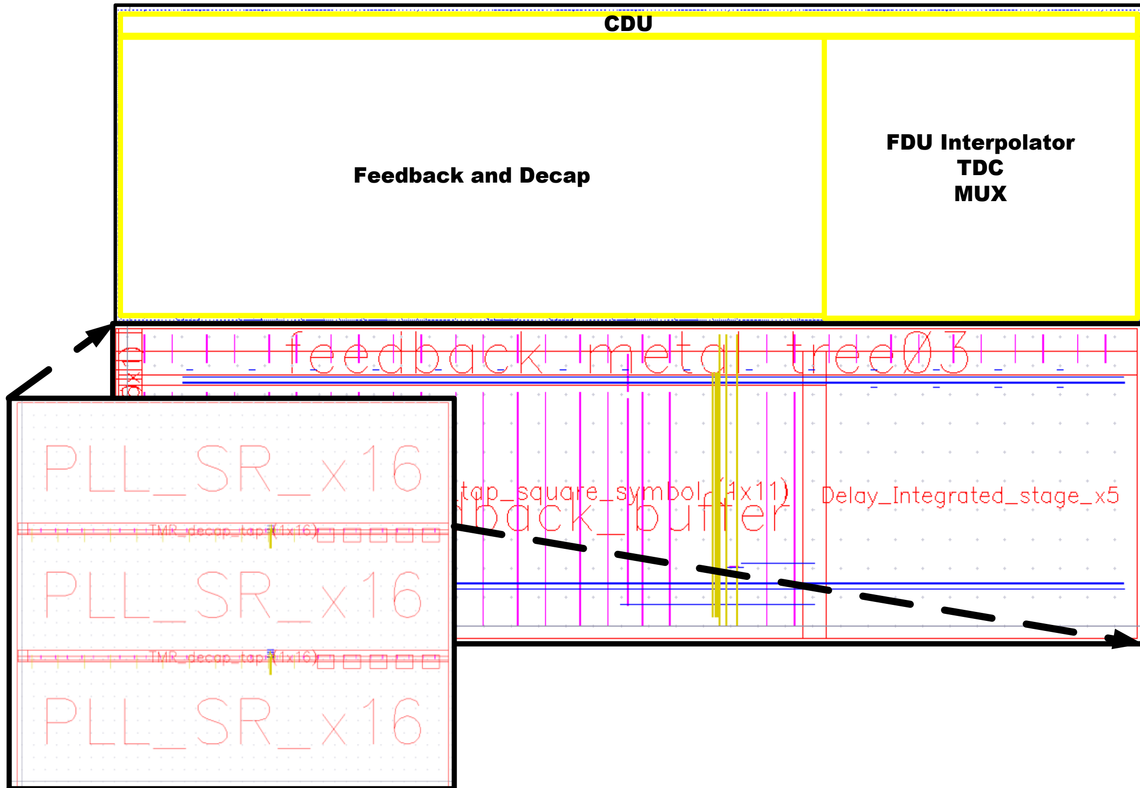


Fig 4.37 TC 25 DLL test structure for coarse and fine delay unit for delay and non-linearity testing. The single slice which are triplicated are shown in the zoomed figure.

a fine-delay interpolation unit with time-to-digital converter unit was designed. The block diagram shows the test-path to clock the TDC in an open-loop mode to ensure fine delay measurement of the phase error. The test-structure can be run in an oscillator mode, as well, where a variable frequency clock can be generated on the chip.

The test chip snapshot and the DDL test structure placement is shown in Fig. 4.36, where the test-structure block "DDR" is highlighted in red. The critical path was optimized by placing I/O pads close to DDR block. The design is implemented in TMR and the clocks are voted out to I/O pads. Voted clocks can also be monitored and the 32 bit TDC output can be monitored independently to measure the DDL delay and variability. The layout snapshot of the TMR test structure implemented on a 55 nm Fujitsu low-leakage process

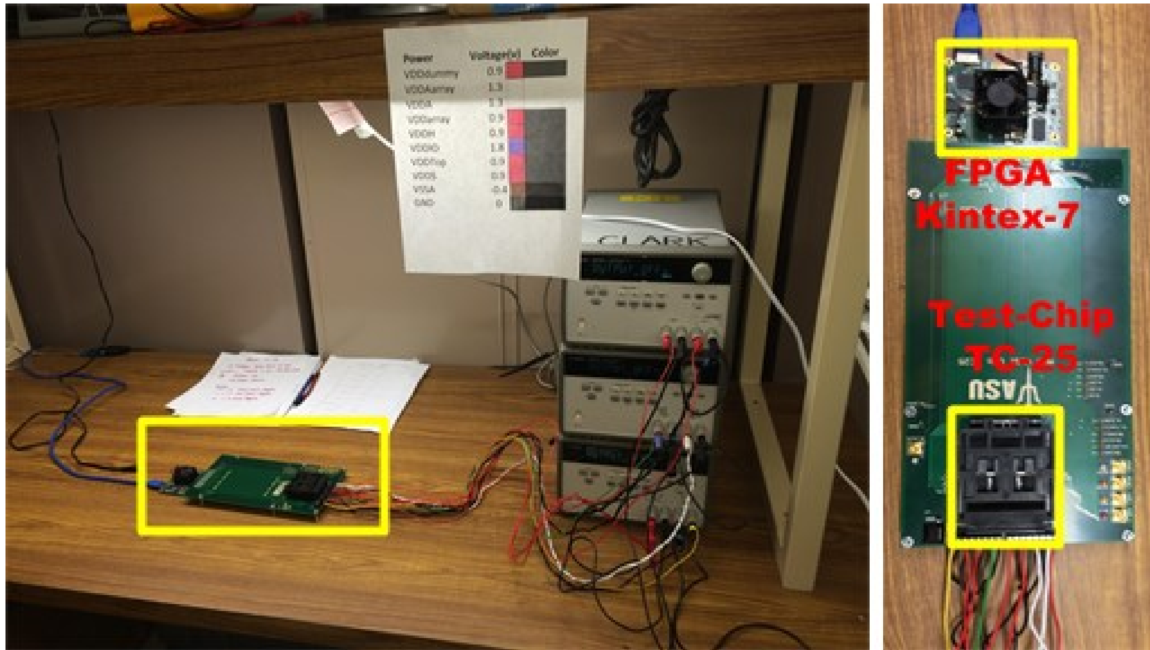


Fig 4.38 TC 25 test-setup. The FPGA board and the custom test-board are shown. The test-chip TC25 is plugged in the socket and the power supplies are connected to the test-chip as shown.

with three redundant stripes placed are shown in Fig. 4.37. The functional units of CDU, FDU, TDC and multiplexer for clock out are shown.

The test setup for the measurement using Xilinx Kintex-7 FPGA and opal-kelly processing interface is shown in Fig. 4.38. Various supplies with body-bias voltages and DLL power and ground bias are shown. Oscillator and open loop mode are implemented in the test-structure and both modes are to be tested to obtain silicon results. Oscillator mode has been verified as functional, but detailed silicon results on oscillator and open-loop modes are still awaited.

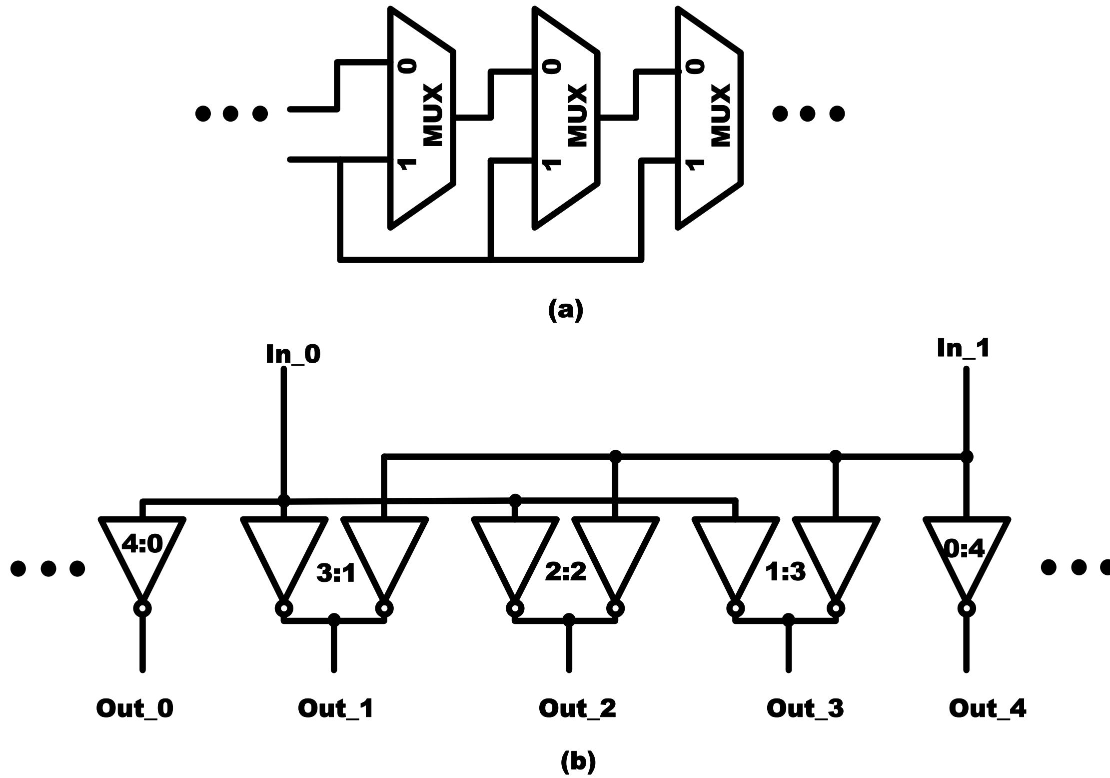


Fig 4.39 TC 23 implemented coarse and fine delay structures, the fine delay was implemented as by 4 interpolate instead of by 8 interpolation as in this chapter.

4.12. TC23 90 nm Test Results

The A 90 nm test chip (TC23) with a similar fine (phase interpolator by 4) and coarse delay (AND-OR multiplexer) units was tested for TDC functioning and fine delay code linearity. A multiplexer based delay element and an inverter interpolator by 4 was used in this design (Fig. 4.39). A Kintex-7 FPGA based chip on board setup was used for testing the device. Block diagram in Fig. 4.40 shows the top level FPGA connectivity and the DUT being driven by the FPGA signals. Top module ASIC_test.v which instantiates the modules required to provide the inputs to the TDC and the connectivity at the board level to ensure the routing of the signals. Under header 'Locals' in the verilog are the

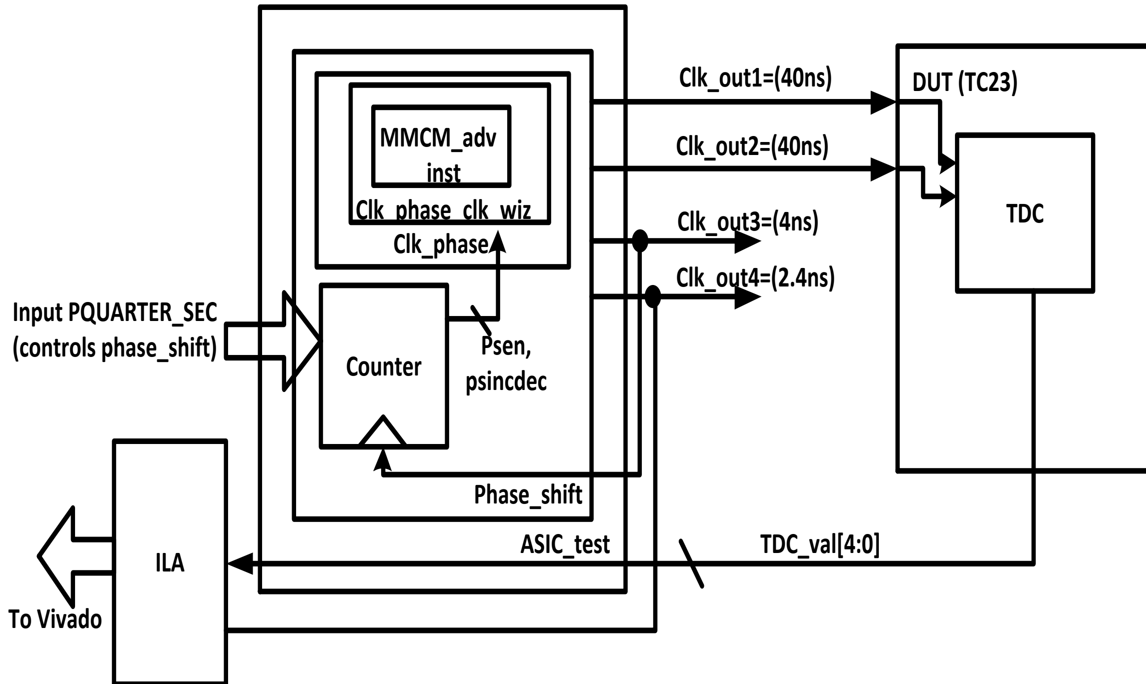


Fig 4.40 TC 23 FPGA testing Verilog hierarchy block diagram to capture TDC data out as a result of phase shifts applied through clock manager module MMCM.

signals which are needed for debugging or observing. MARK_DEBUG=TRUE is the attribute that is used to enable the same in the Verilog. In the base test-case, the signals clk_val_o, tdc_val_o and clk_sample are set for debug. Two clocks are applied to the TDC for the purposes of measuring the TDC code: Clock clk_out1 (phase shifted clock) and clk_out2 (static clock).

4.12.1. TDC Measurement Experiments

TDC measurements are run with different phase shifts and at 4 different voltages that can be controlled through the jumpers. First measured results are at a phase shift

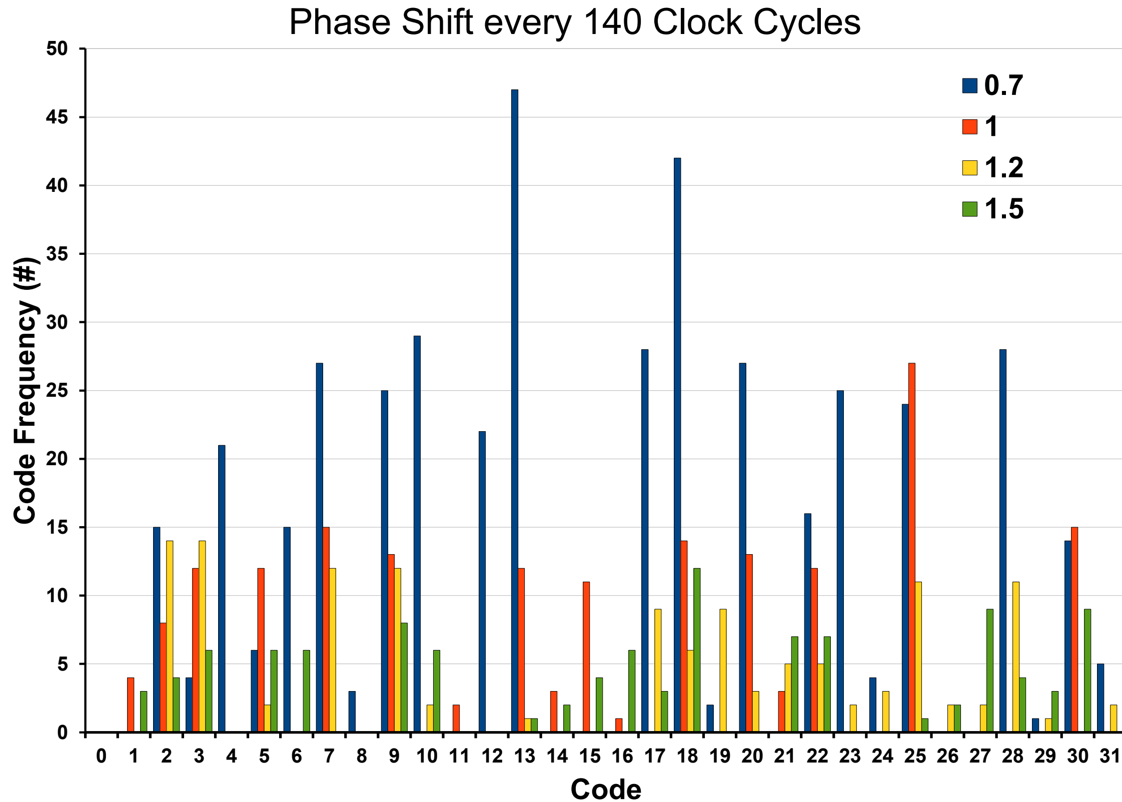


Fig 4.41 Code distribution with phase shifts of 14.2 ps applied every 140 cycles.

applied every 140 cycles of the phase shift clock (4 ns). Fig. 4.41 shows the accumulated code results with delay (14.2 ps) applied every 140 clock cycles. . When nothing is observed, the default value of 0 is assigned.

The second experiment is with a delay applied every 74 cycles (Fig. 4.42). The frequency of the samples seen is reduced due to the increased phase shift rate (approximately 2X). The confidence of the code is higher at lower voltages (higher delays) since the phase shift value has a higher probability to step through each code. Jitter on the measured signals also has an impact on the measured code. High frequency or low delay measurements are challenging and push the ability of the FPGA to produce controllable,

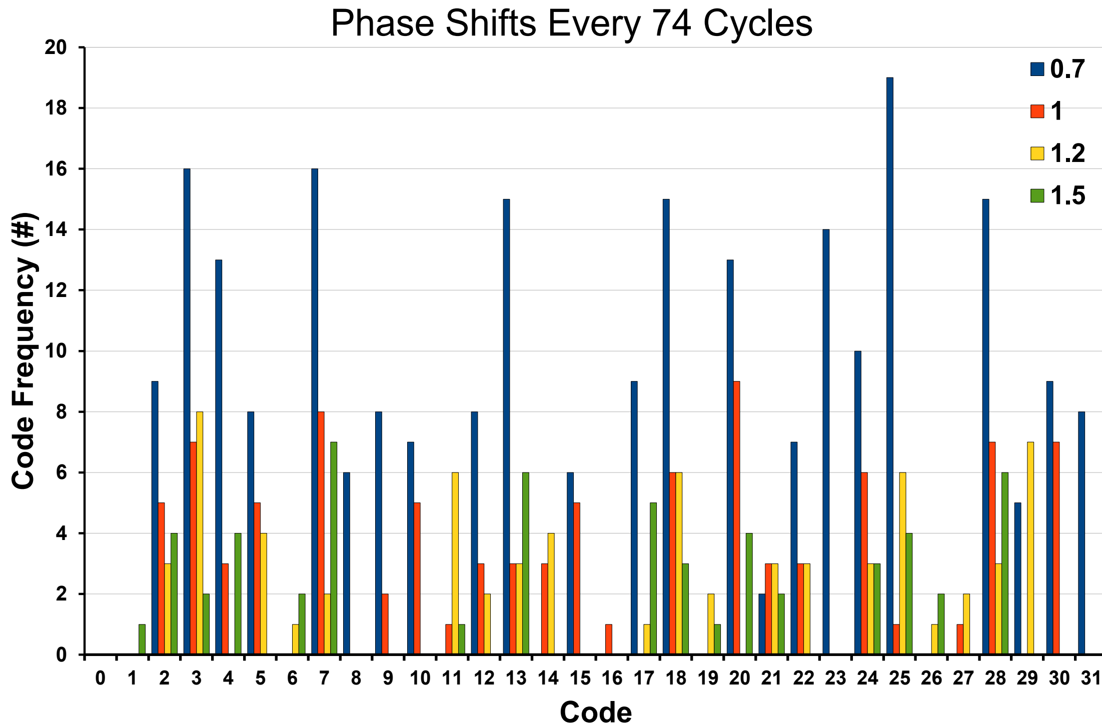


Fig 4.42 Code distribution with phase shifts of 14.2 ps applied every 74 cycles.

low skew and jitter clocks with controllable phase shifts. Better test equipment and setups are required to achieve 1 ps level accuracy in measurement.

4.12.2. Measured vs Simulated Data

The measured data as plotted in the previous section is compared to the simulated data from the simulation results section. We compare the total delay that is seen in terms of the phase shifts applied, for the code to completely traverse on silicon with the simulated delay values. It also allows us to determine if the delay trend shown by simulated data is followed by the measured data. The measured data delay is calculated by the span of the TDC code in terms of the sample ILA clock. The ILA clock time is then converted into the number of phase shifts applied in the same time duration using the formula in equation 4:

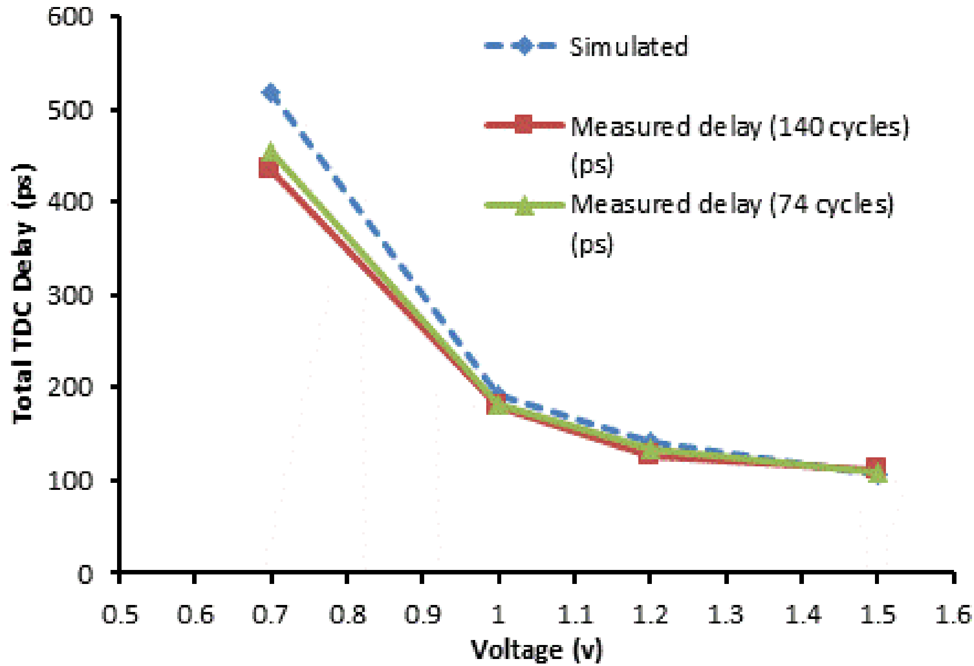


Fig 4.43 Measured vs simulated delay of the total TDC delay for the two experiments shown in Fig4.41 and Fig. 4.42. Measured and simulated values agree closely and only vary at low voltages.

$$TDC\ delay = \frac{(ILA\ clocks)\times 2.4ns}{4ns\times Phase_shifts} \times 14.2ps \qquad (4)$$

Fig. 4.43 shows the comparison of the measured and the simulated data at the two phase shift conditions described above (140 and 74 cycles). The delays of the TDC that are being measured are on the order of (100-550 ps) based on the simulated data from 0.7 to 1.5 V. The phase shift provided using the clock manager is 14.2 ps. The peak to peak jitter on the clocks provided, based on the FPGA clock manager datasheets, are on the order of 180 ps. This high resolution requirement of the measurement setup results in the FPGA implementation and the trigger depth dependence on the code output value or the lack thereof, seen on the ILA output window. The same tests run twice misses the TDC completely when the ILA trigger depth is low (8K samples). This is because the FPGA delay mismatch (as implemented) between the clocks can be large enough where the phase

Table 4.iv. ADPMDLL Performance Summary and Comparison with Previous Radiation Hardened DLLs.

	RHBD DLL Comparison Summary		
	Sengupta10	**Yang13**	**This Work**
Architecture	**digital (TMR + ECC)**	**digital (TMR + ECC)**	**digital (TMR)**
Clock Rate (MHz)	**133**	**267**	**100 - 850**
Lock Time (# cycles)	**X**	**X**	**32**
Idle Power (pJ/cycle)	**X**	**X**	**1.6**
Active Power (pJ/cycle)	**12.48**	**23.68**	**14**
Area (um2)	**0.096**	**X**	**0.1125**
Jitter P2P (ps)	**X**	**X**	**22.4**
Technology (nm)	**130**	**130**	**55nm LL**

shifts applied never hit the TDC code window in the width of the ILA trigger (when it is low). With the trigger depth is set to 32K, the TDC is always hit and a consistent code is seen across different runs.

4.13. Performance summary and comparison.

The proposed DLL is compared with other standard hardened DLLs in this section. The non-redundant version of the ADPMDLL comparison is shown in Table IV. The ADPMDLL exhibits comparable performances to other published non-hardened works, even ones at advanced technology nodes [Hoss14]. The comparison of the proposed design with hardened designs is shown in table IV. There is dearth of radiation hardened DLL designs and hence, 2 other designs were used for comparison. Other designs/design

techniques published in [Mail13] [Mail10] have not shown standard metrics such as jitter, power and area and only provide circuit level hardening techniques to mitigate missing pulses or SET's on a portion of the DLL constituents. In the absence standard metrics, it is difficult to have a normalized comparison of the overhead incurred and the efficacy of the design and architectural techniques implemented. It can be seen clearly that the proposed design has a high quality clock generation and synchronization suitable for DDR3 standard at a comparable or low power.

4.14. Summary

This chapter described the design of a radiation hardened DLL, which is also immune to multi-node charge collection. The architecture and the circuit constituents are described in detail. The DLL produces multiplied pulsed clock using arithmetic and successive approximation control logic. The wide-range ADPMDLL can operate in low-power modes and in high-frequency DDR2 and DDR3 modes. Effects of soft-errors on the base non-redundant design is studied and loss of lock and erroneous frequency multiplication is shown. The effect of random variations is also studied and the performance of the elements in the presence of variations are calculated. Test structures are implemented on 55 nm low-leakage to measure the variability and performance on silicon. Previous test results of test structures in 90 nm are presented to show the difficulty in testing high speed clock synchronization circuitry. Using CAD methodologies proposed in the previous chapters and design techniques explored in this chapter, a low area footprint, low-power design is realized.

CHAPTER 5. DMR SEMI-CUSTOM DESIGN FLOW: REGISTER-FILE

5.1. Introduction

Chapter 4 described the all-digital radiation hardened delay locked loop for DDR2/3 interface. Chapter 5 presents the design methodology for implementation of semi-custom DMR register-file (RF) used for the radiation hardened HERMES2 microprocessor described in chapter 3. The DMR RF forms an important part of the speculative pipeline to ensure soft-error mitigation. Dual redundant copies of the RF are designed and arranged for minimal PPA and fast turn-around time. The proposed RF design is an integral part of the error detection and restart instruction set in the HERMES2 processor. Multi-port RF custom designed column and 4 APR designed decoders are arranged to form a single copy of the RF. Decoders are implemented with custom spaced decoding lines arranged as metals and blockages during floor planning for each of the 4 decoders forming the multi-port RF. The design implemented in 55 nm LSP process uses well-biasing for the control of the P and N- wells which are incorporated in the custom and APR design flow.

5.2. DMR Registerfile Background

Register files are key building blocks in high performance circuits, like microprocessors. RFs are different from standard SRAMs in that they have a single ended readout and can have as few as two, to as many as, dozens of read ports. Their size is much smaller compared to an SRAM, commonly ranging from 32 to 256 entries. In microprocessors, the RF resides in the critical timing paths of the ALU/bypass loop where operands must be read from the RF, operated on by the ALU and used in the subsequent clock cycle.

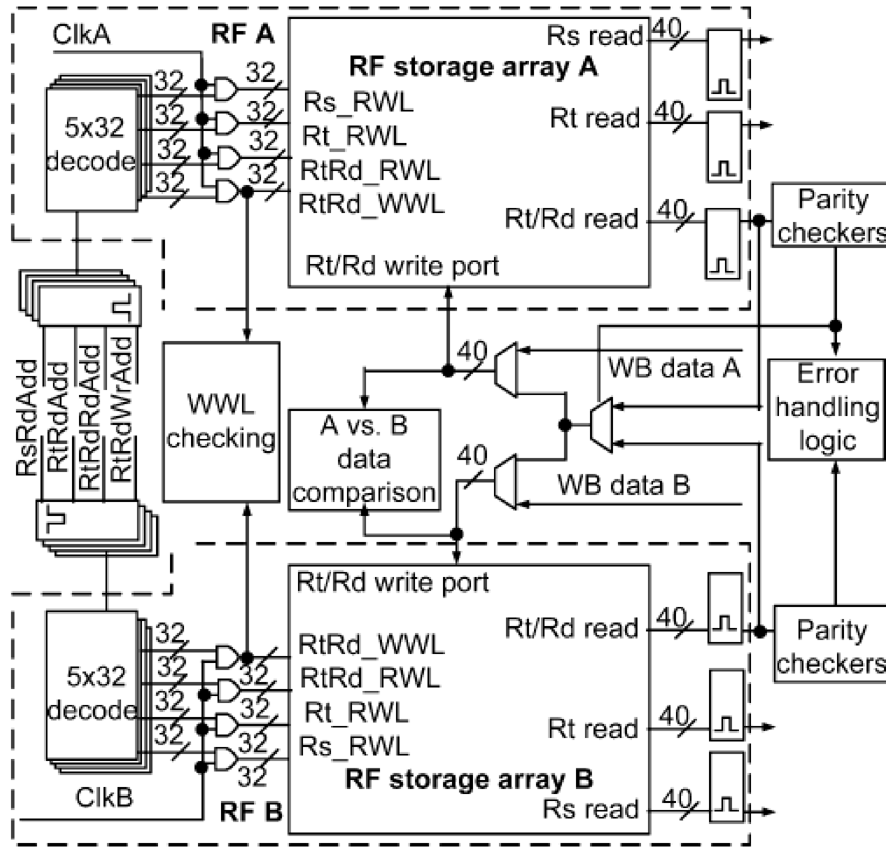


Fig 5.1. DMR RF architectural diagram with the A and B copies and the checking (WWL, parity and comparison) logic to detect the erroneous pipeline before commitment to architectural state, after [Clar11].

The Alpha 21264 microprocessor used two RFs, each supporting decoupled superscalar data paths [Gies97]. Segmenting the RF into two units allowed four read ports for each read data path. The addition of parity to the 90 nm Itanium RF reinforces the increasing importance of mitigating soft errors in terrestrial ICs, particularly in server applications [Fetz06]. A dual mode redundant (DMR) logic data path with instruction restart that detects errors at register file (RF) write-back implemented in a 90 nm process is presented in [Clar11]. The design presented in this chapter is an updated version with minor modifications to the circuit design.

5.2.1. Soft-Error Recovery

Soft-error recovery in RFs is challenging because RF is in the timing critical path of the microprocessor pipeline. Hence, adding extra circuitry, like EDAC, for byte level correction in the path reduces maximum operating frequency, while incurring a considerable area penalty (62.5 %) [Hsia70]. Owing to this overhead, RFs only use error detection parity schemes, which are also comparatively faster to generate due to shallower depth logic trees. Additionally, EDAC does not protect against erroneous data or operations caused by SETs and SEUs, either in the RF or in the ALU/bypass circuitry that produces and consumes data originating in the RF.

The RF design here combines multiple micro-architectural and circuit level techniques (5.1), starting with DMR for compatibility with the data pipeline. DMR decoders generate redundant read and write word line signals. Full SEE protection is provided by DMR combined with large critical node separation through bit interleaving and parity. Parity provides error detection, while DMR allows one copy to provide clean data for SEU corrections. The third Rt/Rd read port can restore the RF destination register contents if the overwriting RF store is cancelled due to a detected data path error (SEU or SET). This restoration happens during the write-back process.

A back up register file (BURF) instruction is added to replace the corrupted values, when executed within the exception handler. The DMR mismatch detection circuit is shown in Fig. 5.1 as the 'A vs B data comparison' block. This block also monitors the WWL mismatch when a single copy of WL is asserted, but another is not leading to a mismatch. Key recovery states are stored in self-correcting TMR circuits which form the architectural states of the pipeline.

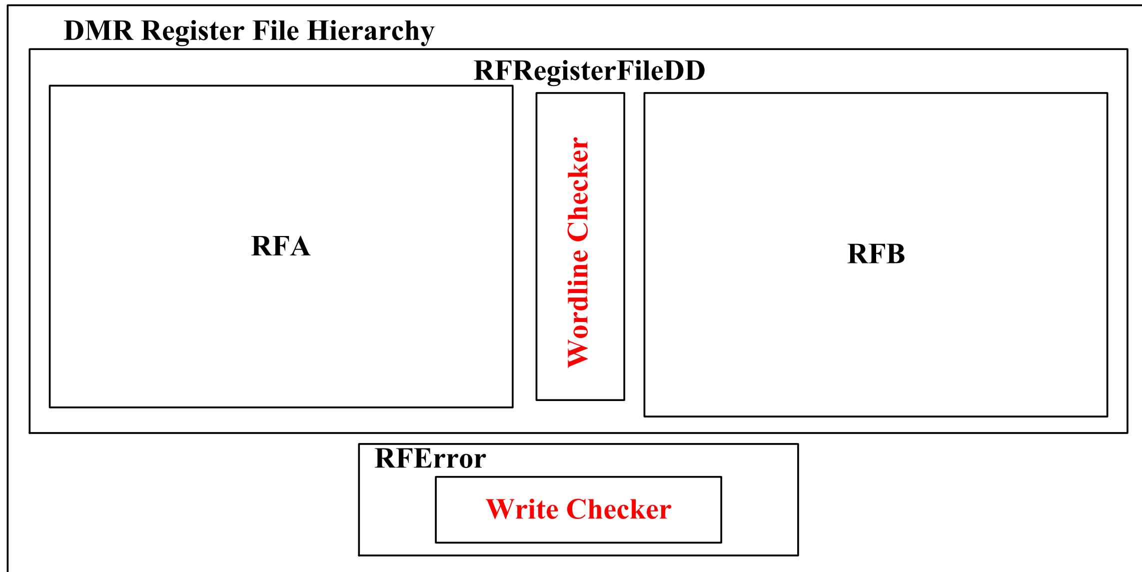


Fig 5.2. DMR RF implementation hierarchy, Wordline checker is implemented in the registerfile hierarchy RFRegisterFileDD and the write checker circuits are implemented in the RFerror hierarchy to be implemented in a separate physical block.

The register file SEU error recovery is attained by a second added instruction i.e., repair general purpose register (RGPR). This instruction writes the parity groups in RF copy A with correct parity, overwrite the version in copy B, and vice versa, in two clock cycles. Thus, an SEU corrupted RF state can be repaired in 64 clock cycles (the time to read each register and then write it back) when an error is detected. The DMR RTL design hierarchy is illustrated in Fig. 5.2 to understand the major design block logical interaction.

5.3. DMR RF Circuit Design

5.3.1. Bitcell Design

The RF bitcell design in this work is different from a conventional RF cell, such that it is controlled by 4 access transistors rather than 2. Two qualifying signals, WWLA and WWLB, respectively, control the bit-cell to ensure that an erroneous WL assertion

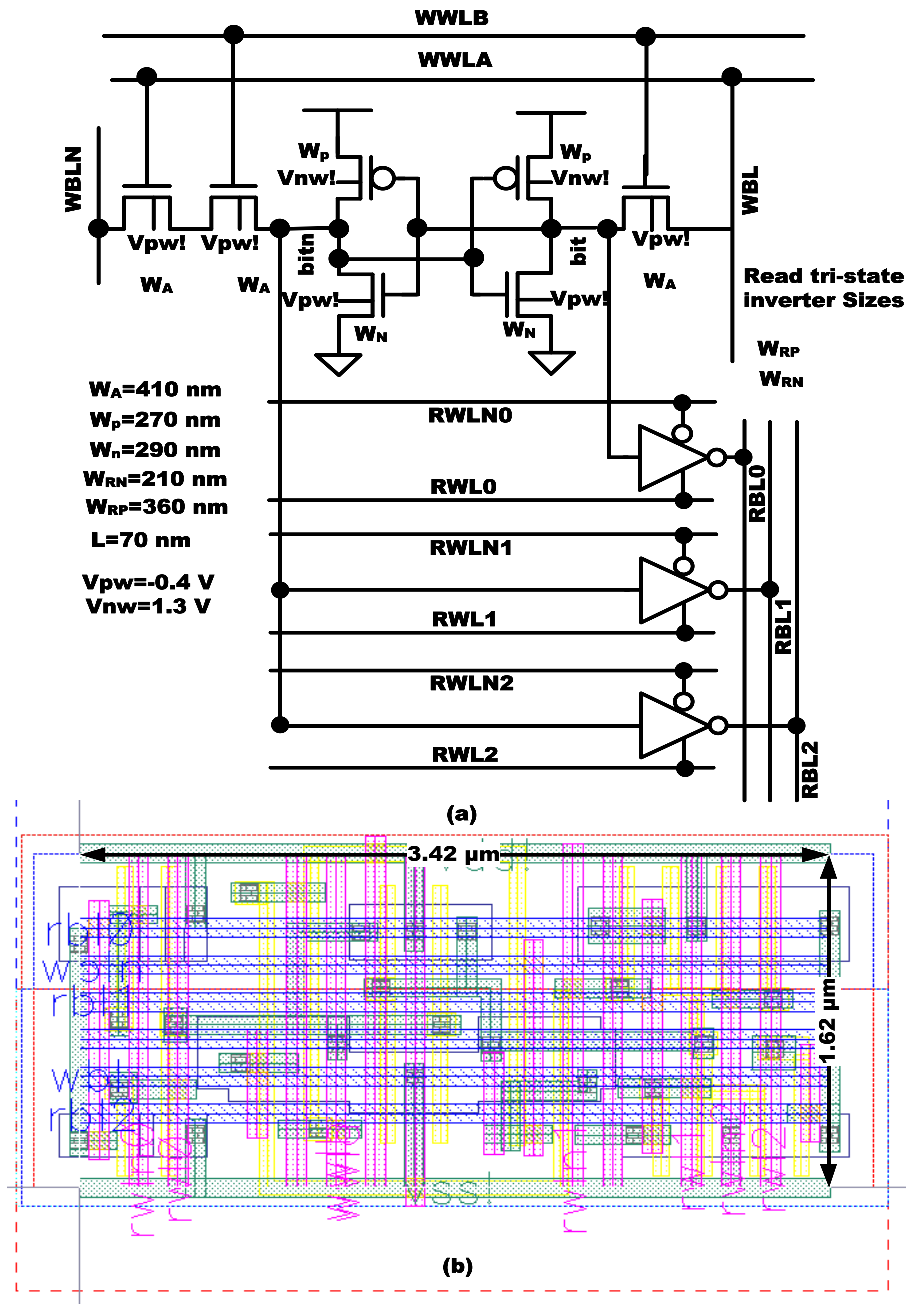


Fig 5.3. (a)Register file cell design, single copy of the DMR cell with 2 redundant transistors for dual word-line access, multiple ports are shown, (b) Layout of the cell in a 3,42 by 1.62 um area.

origination in the control logic cannot assert the RF cell. This ensures erroneous writes in the RF are completely mitigated. Therefore, as explained previously, any SEUs on a single

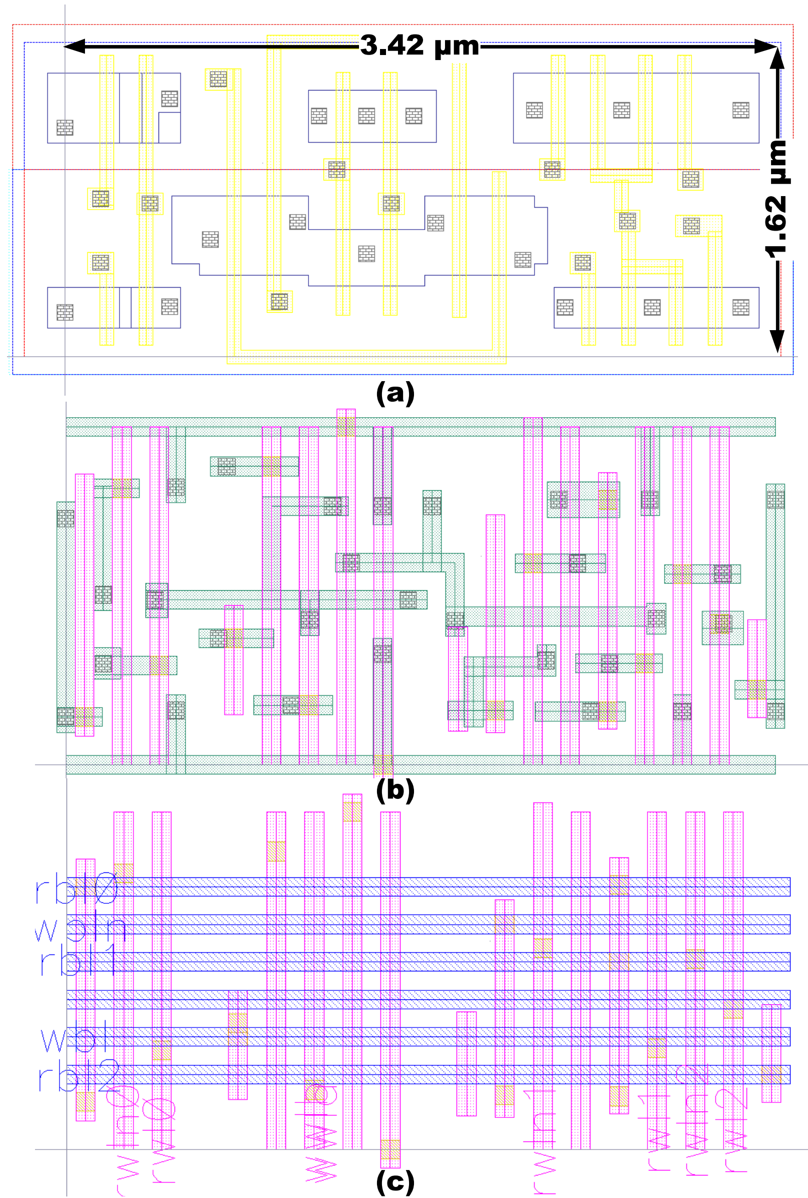
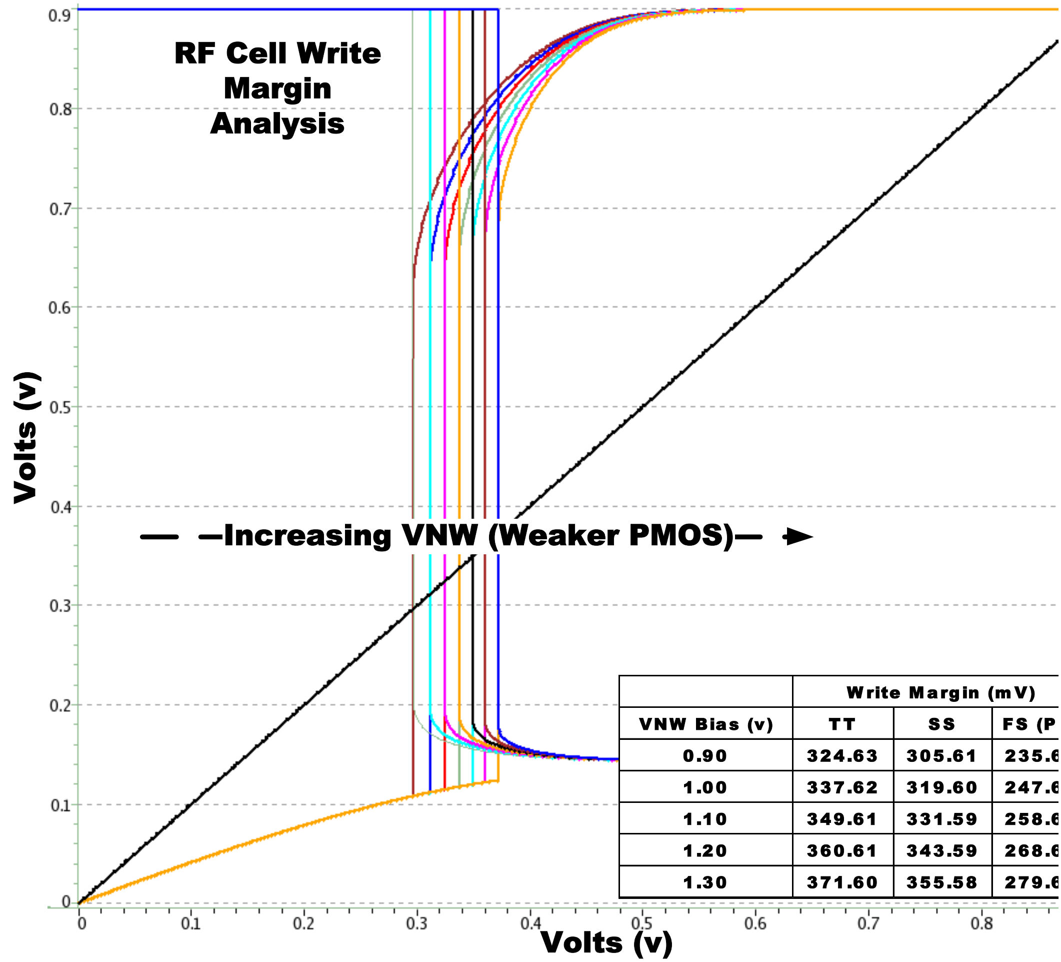


Fig 5.4. (a)Register file bit-cell design, metal and active layer usage and layout are shown by layer in (a) poly and diffusion, (b) M1 and M2 (c) M2 and M3. High density layout for the multi-ports incorporated in the cell are shown.

copy cannot manifest into an architectural state error. DMR RF cell P and N well-bias can be controlled through vpw! and vnw! connections, respectively.

The RF cell is shown in Fig. 5.3(a). The sizing of the transistor for minimal area and sufficient write stability is shown. As can be seen, 3 separate read ports exist for the



	Write Margin (mV)		
VNW Bias (v)	TT	SS	FS (P
0.90	324.63	305.61	235.6
1.00	337.62	319.60	247.6
1.10	349.61	331.59	258.6
1.20	360.61	343.59	268.6
1.30	371.60	355.58	279.6

Fig 5.5. Register-file write stability analysis, the n-well voltage is varied to make the PMOS weaker increasing the write margin. The table inset shows the simulated values summary across corners.

readout of the RF value. Consequently, 2 of the read values are BL (connected to node 'bitn') and 1 of the read values is BLn (connected to node 'bit'). The cell height is matched to the standard cell height. This ensures easy design integration with standard cells, thereby saving design time (Fig. 5.3 (b)). While the standard cell heights are matched, the requirement of larger NMOS for maximum write stability of the cell necessitates larger NMOS transistor sizes and hence different well and diffusion dimensions to the standard cells. Therefore, special interface and tap cells are needed. Their design will be explained

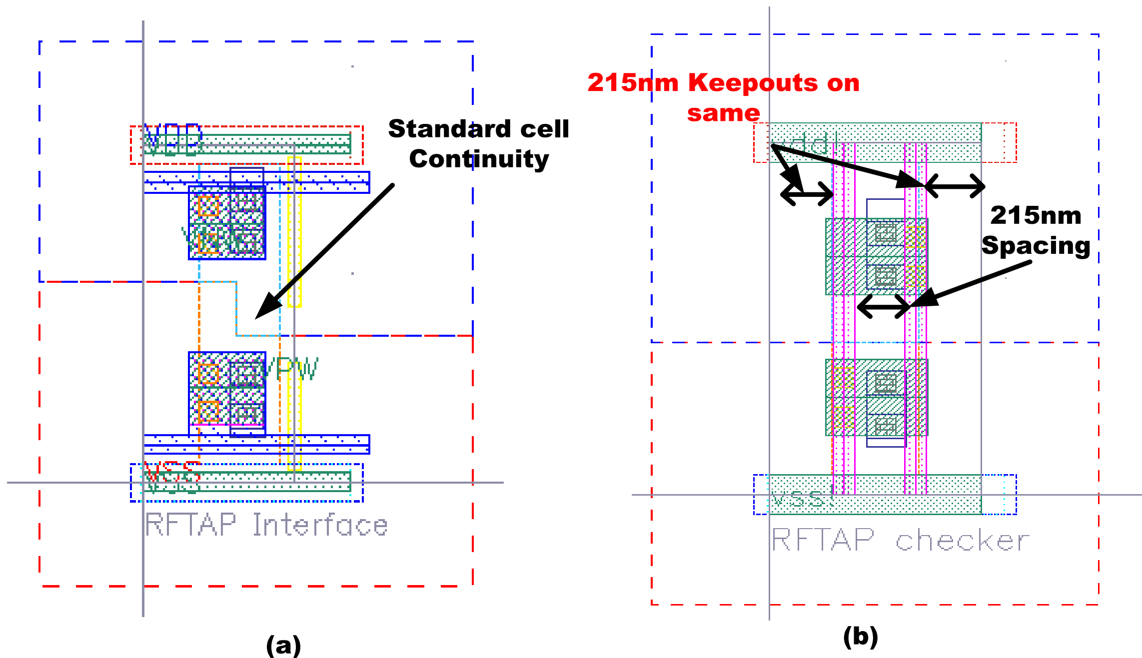


Fig 5.6. (a) Standard cell rail and well (P and N) continuity shown in the interface cell (b) RF tap cell spacing and special keep-out to alleviate high voltage spacing DRC to the secondary power rails for P and N well biasing.

in the next section. Poly, diffusion, metal1, metal2 and metal3 are shown in Fig. 5.4(a), (b) and (c). The design areas are completely optimized for metal 2 and metal3 usage, since the metal2 and metal3 track usage determines the column and array level density of the design.

5.3.2. Write Stability Analysis

Write margin for the RF cell described is run with Hspice and the plots corresponding to the dynamic write margin analysis is shown below in figure 5.5. This analysis is run for TT, SS and SF (NMOS/PMOS) corners and the corresponding write margin in millivolts is shown in the table inset in 5.5. Increasing n-well voltage makes the PMOS weaker, thereby increasing the write margin. The cell is therefore ascertained to be write stable, with unconditional read stability being an inherent property of an RF cell.

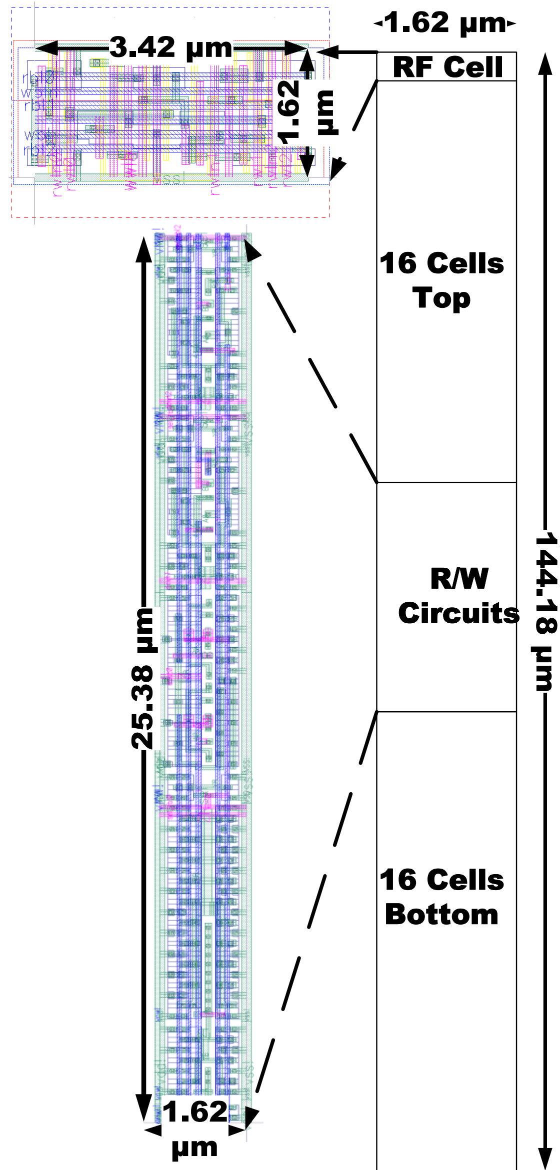


Fig 5.7. RF columns with the RW circuit size and physical arrangement. All dimensions are shown in micrometers.

5.4. Well-bias for Body Control

Isolated well connections need to be made since the well tap connections vnw! and vpw! have to be spaced 215 nm away from every other metal on the same layer (Fig. 5.6(b)). This rule is required to ensure that the high voltage lines are sufficiently spaced

out in order to mitigate dielectric breakdown on the insulator between metals. Layout considerations were made to this end ensuring adequate spacing on the well rails. This spacing had to be followed and matched across the two (A and B) arrays, decoder and the error correction blocks. The spacing is also incorporated into the decoder CAD flow for abutted layout arrangement of the decoders and the RF arrays.

Additionally, a cell with a stepped well and active layers for continuity is made, which is shown in Fig. 5.6 (a). This ensures that the standard cells can be abutted with the custom register file cells ensuring seamless integration into the APR flow and the usage of standard cells for peripheral logic like the read/write circuits. This requirement ensues from the different sizing requirement of standard cell CMOS circuits and write stable RF cell. By using the interface as a tap cell, we save the area that might be potentially wasted making such a well

5.5. RF Column Design

RF cell column consists of 32 RF cells and read/write circuit blocks. Figure 5.7 shows the arrangement of the blocks. The array is therefore made up of 40 columns arranged to ensure 40 bit read out, with a parity bit for every nibble (i.e. 4 + 1 bits, 5*8 =40 bits) [Clar11].

5.5.1.1. R/W Circuitry

RF read and write circuit schematics are shown in Fig. 5.8. An extra inversion is required in two of the ports (connected to RBL1 and RBL2) since they are connected to read bit line complement. The select for each of the multiplexers is a buffered version of the read address MSB corresponding to a unique read port. The multiplexers are

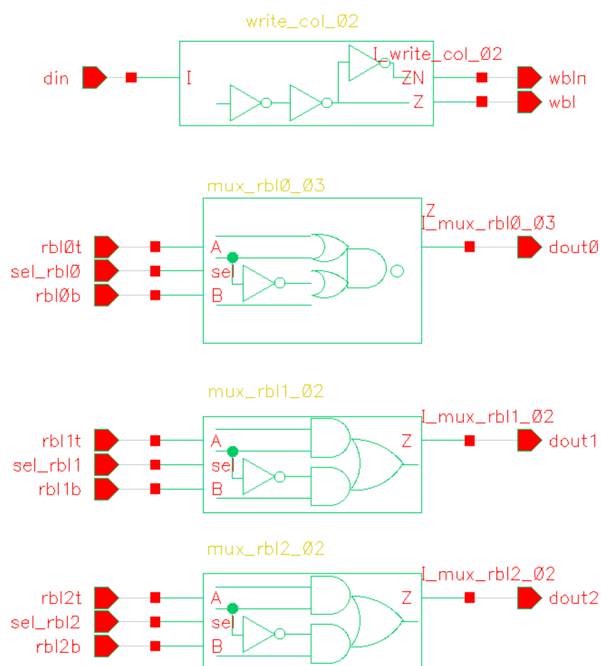


Fig 5.8. Write and read circuits for the RF columns, rbl0, rbl1 and rbl2 are read out statically, with CMOS gates as shown in the schematics, with rbl0 connected to the bit storage value of the cell while the rbl1 and rbl2 are connected to bitn storage value, resulting in different readout value (1 and 0) respectively.

implemented using static AO22 and OAI22 logic gates. The multiplexer for the port connected to the 'bit' node OAI22 gate and those connected to node 'bitn' employ AO22 gates. The read out ports are connected to 'bit' and 'bitn' nodes of the RF cell. Two ports are connected to the bitn nodes, therefore RBL1 and RBL2 read outs are slightly slower than the RBL0 read out due to capacitive loading.

The read speed is a critical factor in the RF design and thus the read bit lines are divided for capacitive decoupling between top and bottom arrays. The same is not undertaken in the write bit lines, since their timing is not critical and the write addresses are gated outside of the arrays for low-power operation. The write circuit is simple

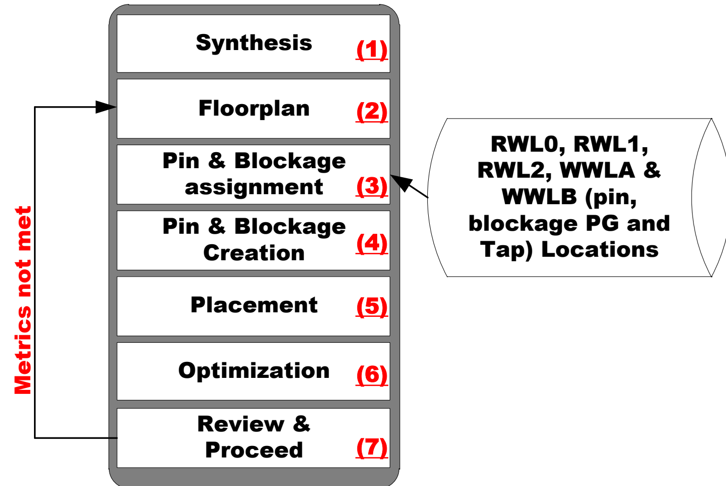
inverting and non-inverting pair driving the RF cell as shown in Fig. 5.8, much like a standard commercial RF cell.

5.6. Decoder Synthesis APR design

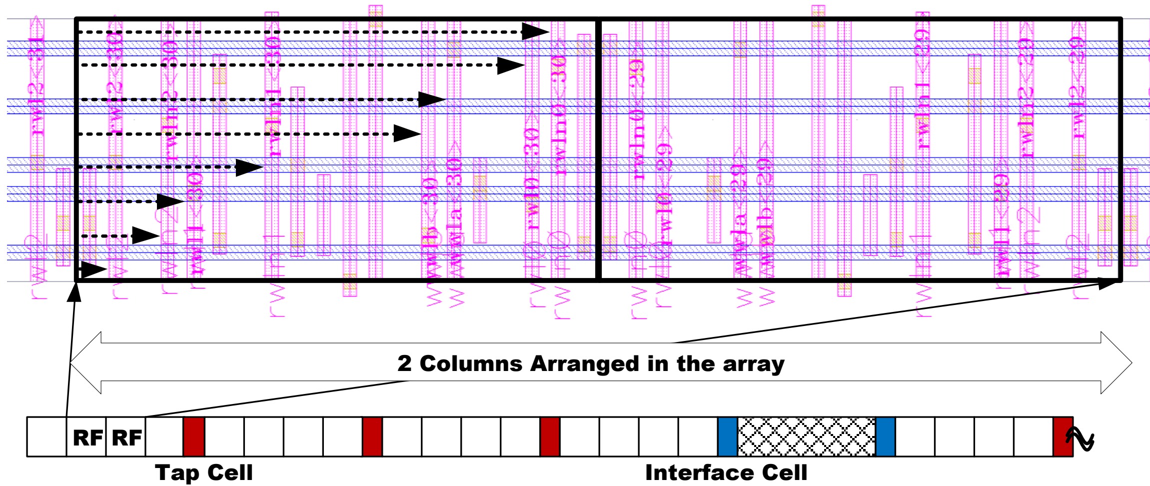
The design of the 3-port DMR RF array requires 8 decoders (2 * [3 read decoder + 1 write decoder]). Decoder design involves considerable time and effort, if designed in a custom fashion. Thus, the decoders were designed using synthesis and APR in this work for minimal design turn-around time and a flow was created to do the same for future designs with varying spacing and speed requirements, albeit with an area penalty.

Based on the parasitic extracted values of word lines from the column, decoders are designed to provide sufficient current drive, while driving the word line loads. Synthesis constraints on read and write word line values are thus provided based on parasitic extracted values. Five unique decoders with different read and write lines are designed; Three Read decoders (RtReaddata, RsReaddata and RtRdReaddata) for the separate read ports and 2 write decoders RtRdWrWLA and RtRdWrWLB for the dual redundant A and B copies of the RF arrays.

Read decoders can be used identically across the two arrays, because the identical metal tracks are available on both A and B decoders. write decoders, on the other hand, need unique tracks across the whole array, since the writes are not bifurcated between top and bottom. The WWL are also checked in the write checker and hence are designed to ensure unique A and B copy implementations. The floorplan layout considerations of the RF in question are discussed in detail in [Vash14].



(a)



(b)

Fig 5.9 (a). DMR RF decoder APR flow, pin and blockage assignment is done in the perl module which inputs the locations of the specific pins for the decoder that drives the specific port and creates blockages for the rest of the pass-through (b) RF decoder arrangement that is used to create the automatic pin, blockage, power, and secondary PG (well biases) for the APRed decoders (Tap and interface cells are shown).

5.6.1. CAD Flow for Multi-decoder APR Implementation

CAD flow for multi-port RF decoder synthesis is shown in Fig. 5.9 (a). The constraints for decoder APR synthesis are derived from the PEX extracted simulations in form of capacitive loading on the wordlines. Once the design is synthesized, the floorplan

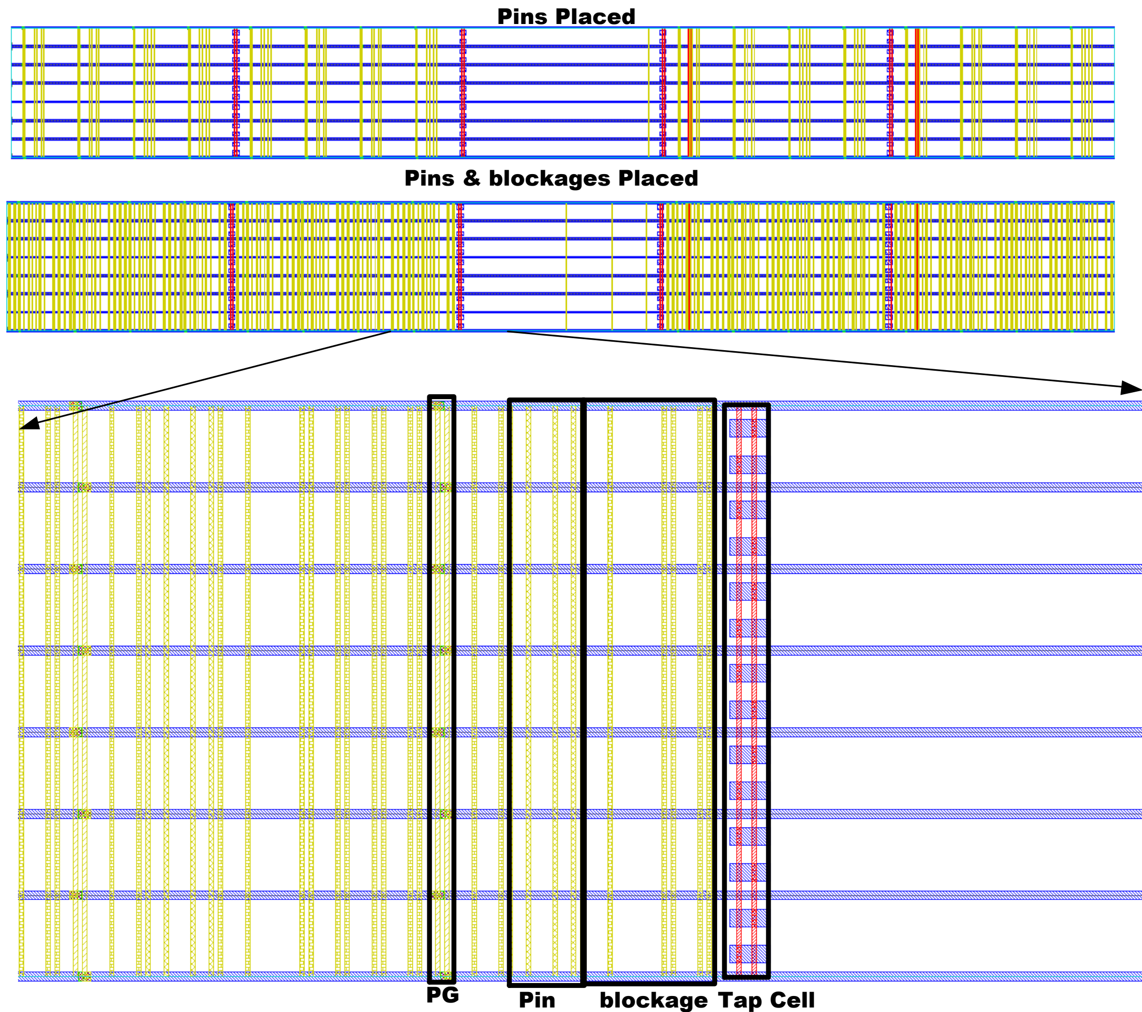


Fig 5.10 APRed RWL0, RWL1, RWL2, WWLA or WWLB decoder automatic pin, blockage, power (M4), and secondary PG (well biases on M2) assignment. Pins and blockages are both created on M4 based on the inputs provided to the perl module which creates a DEF file for use in defIn flow.

is created based on the minimal area, such the decoding logic can be placed and routed with the WL locations and metal tracks being defined in the floorplan.

Based on the design of the RF cell, the locations (Fig. 5.9(b)) of the metal 4 tracks which form the WL for various decoders, are input into a PERL script which creates a DEF file with locations of the pins for each of the unique 3 read and 2 write decoders. Each decoder has an output DEF file corresponding to locations of the pins and blockages. The

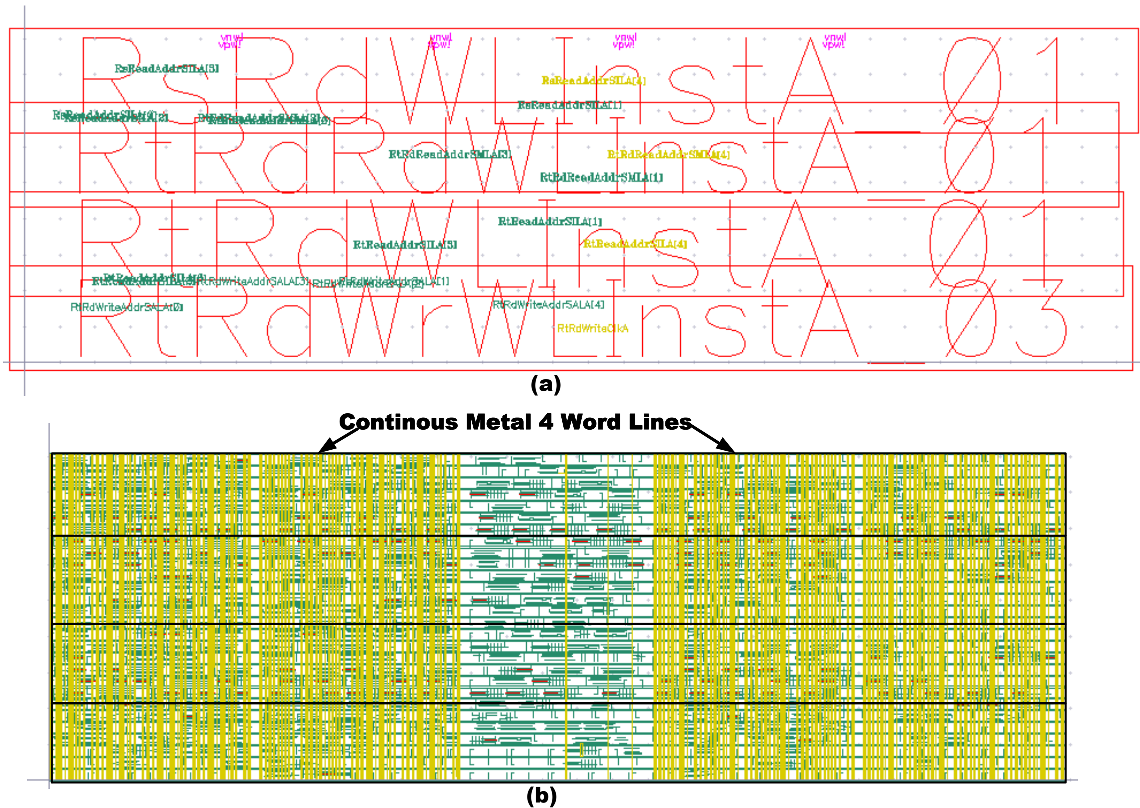


Fig 5.11 Decoder Arrangement (a) and metal 4 continuity (b) for abutment with columns, Decoder A has the WWLA version of the write decoder and Decoder B (RFB) has the WWLB version of the write decoder, the read decoders are identical.

pins for one decoder become blockages for the next as the constant M4 tracks are tapped to in each unique decoder implementation, saving design cycle time.

The output DEF also has the locations of the power, ground, n-wellbias and p-well-bias locations of metals M2 and M4. Fig. 5.10 shows the floorplan view of a decoder implementation with pins and blockages on M4. The locations of pins, blockages, PG and tap cells are shown. These pins become the seed for placement and optimization of the individual decoders. Post pin and blockage creation using the DEF file, placement and optimization steps are run to ascertain the suitability of the APRed design. If the design metrics in terms of placement density, routing density, timing and physical design rule violations are ascertained to the satisfactory, the flow proceeds to physical verification and

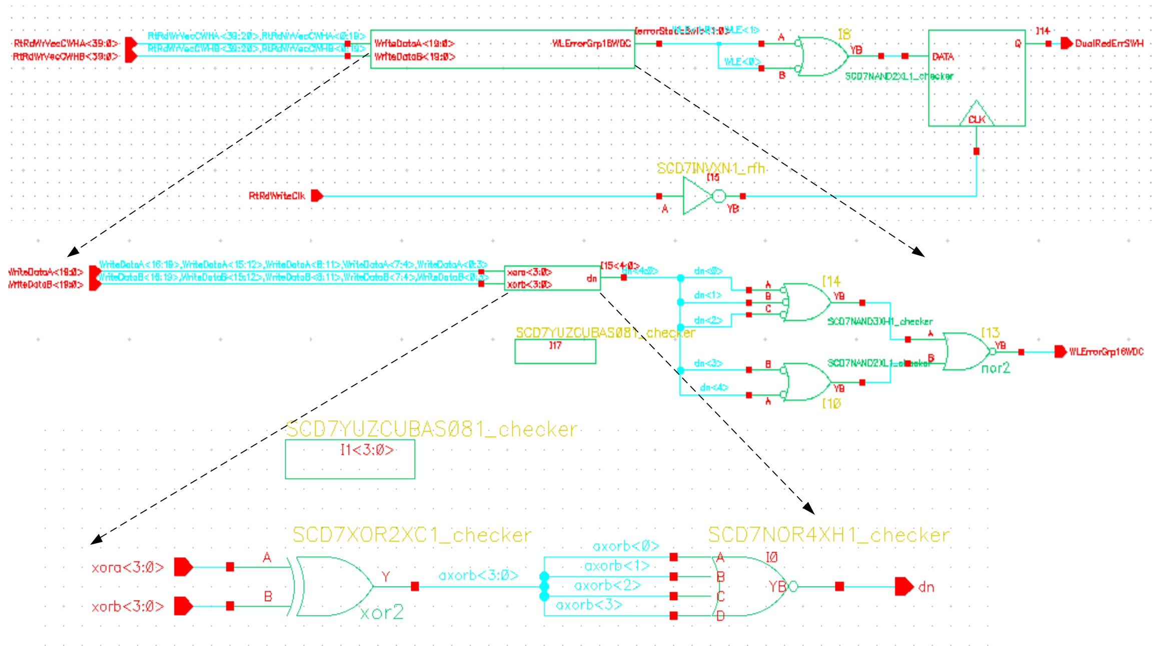


Fig 5.12 Checker circuit hierarchy in schematic for Write and WL checkers. WL and write checkers are 32 and 40 bit each.

signoff. The design output GDS can be integrated seamlessly into the custom designed RF array, since the abutment constraints are handled in APR.

5.6.1.1. Decoder Floorplan

Four decoders are arranged as shown in Fig. 5.11 for abutment in the RF array. Three read decoders (RtReaddata, RsReaddata and RtRdReaddata) and a write decoder (RtRdWrWLA) are shown arranged to form the decoding block for the A copy of the RF array. Another set of four decoders exist for RF array copy B. The simple abutment of the decoders is facilitated by the APR flow described above. Continuous metal 4 lines in yellow are shown, which are created after GDS export of the implemented design after the blockages are converted to metals.

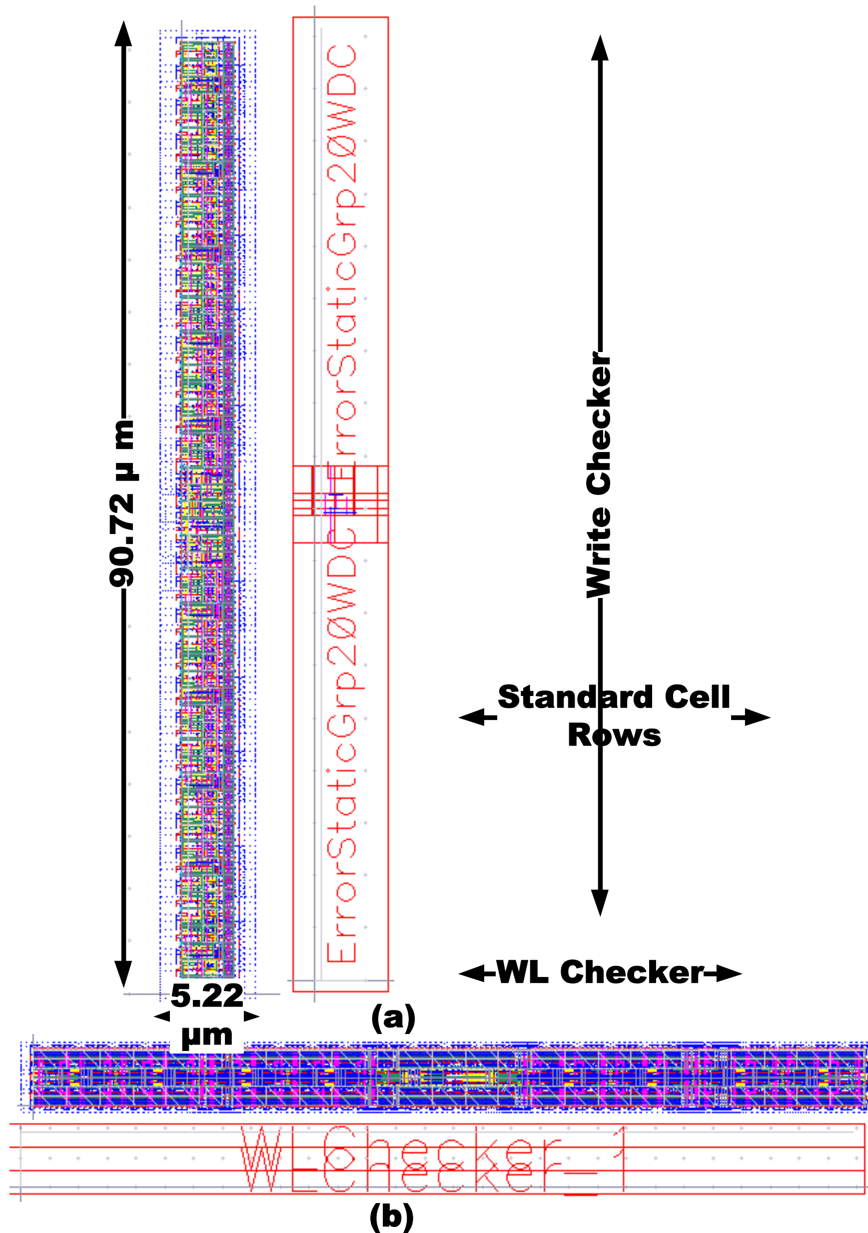


Fig 5.13 Checker circuits physical layout, WL checker (b) is horizontal and write chercker (a) is vertical with respect to the standard cell row placement (standard cells rows are horizontal).

5.7. Checker Circuits

The checker circuits for the DMR RF described in this work are designed using static circuits as opposed to the dynamic implementations described in [Clar11]. The prior

version with ones catching domino logic is used to ascertain mismatched between the A and B WWLs. Similar domino error correction circuits have been implemented in [Yao10a]. Static versions of the ones catching domino circuits have been used in this work for write and WL checking circuits. The implementation of the write checker is undertaken with deep XOR and NOR based trees. The write checker is 40 bit, since there are 40 bit writes (32+8) of the RF data. Word-line checker is 32 bit in order to catch mismatched between the A and B WLs, as explained previously, to be used by the error handler for BURF instruction execution. Fig. 5.12 shows the hierarchical schematics of the error checker circuits. Write checker schematics are shown with the WL checker being identical but for the width of the bus.

5.7.1.1. Physical Implementation

The write and WL checker physical implementation is shown in Fig. 5. 13. The write checker is implemented as a separate macro outside of the RF macro and wired to the RF using APR at the top level implementation of the processor HERMES2. The orientation of the standard cells and the floorplan of the checker with respect to the said orientation is shown. Since all the components of the design are to be integrated in the top level with the standard cell (well orientation), the WL and write checker orientations are to be maintained for well and M1 powerplan continuity. The WL checker is abutted with the decoders and the RF array since the WL checker connect to the dual redundant WLs as the A and B WLs are checked for radiation induced errors or mismatches.

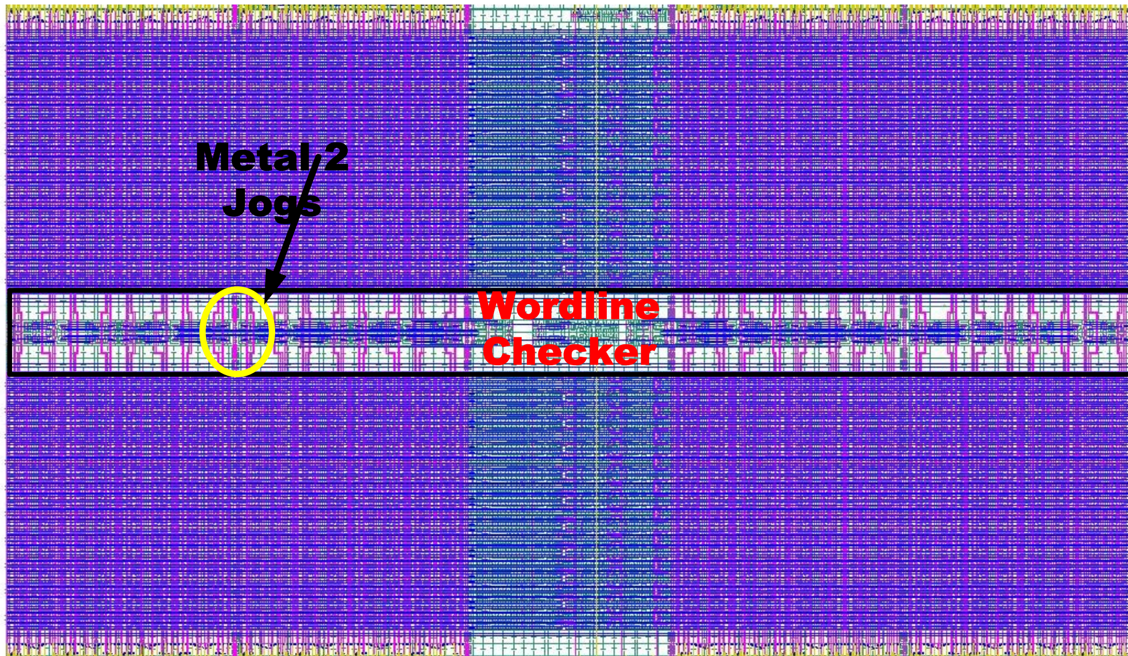


Fig 5.14 Checker circuits physical layout, WL checker (b) is horizontal and write chercker (a) is vertical with respect to the standard cell row placement (standard cells rows are horizontal).

The wordline checkers are implemented using standard cell gates and metal 2 lines need to be jogged on wordline checker for drc spacing alleviation in this implementation. Fig. 5.14 shows the WL checker placement in the array (with the A array on the top and B array on the bottom) and the metal jogs.

5.8. Performance Overview

5.8.1.1. Speed

Register File read port timing is the critical timing in the RF design. The critical timing path is shown in figure 5.15. The corresponding timing was calculated in Ultrasim and Nanotime, respectively. Nanotime runs static timing analysis and Ultrasim runs dynamic simulation using RTL generated simulation vectors. Table 5.I has the timing comparison of Ultrasim and Nanotime read delay numbers. The read delay for 3 read ports

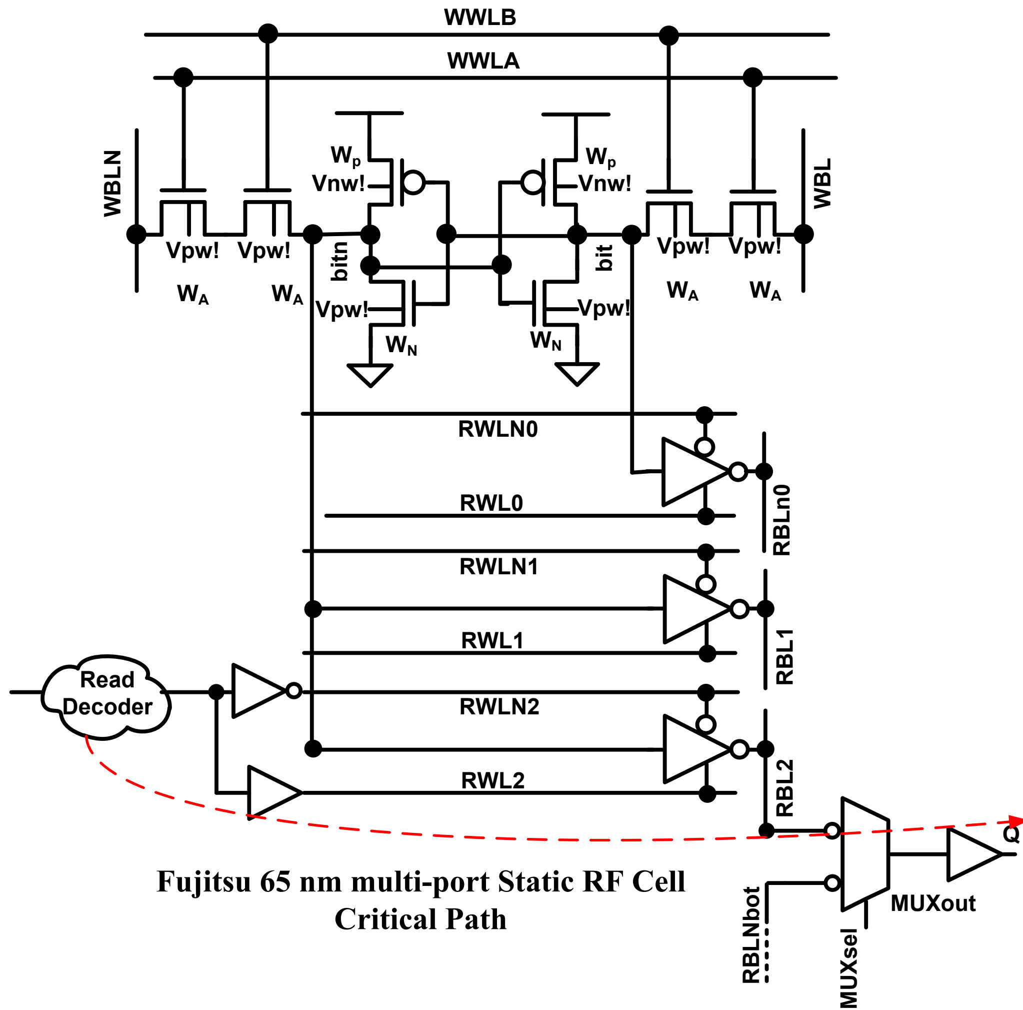


Fig 5.15 RF critical path timing path, showing address in to data out timing in red.

post extracted results are shown. Nanotime numbers are more pessimistic and hence the liberty models extracted can be used with higher confidence due to the pessimism involved.

Table 5.i Comparison of characterized and simulated delays for the register file read ports.

	Nanotime Delays		Ultrasim Delays		Variation Ultrasim vs Nanotime	
Ports	Rise (ps)	Fall (ps)	Rise (ps)	Fall (ps)	Rise (%)	Fall (%)
rtreaddata	789	585	690	490	12.55	16.24
rsreaddata	527	694	480	690	8.92	0.58
rtrdreaddata	755	561	690	480	8.61	14.44

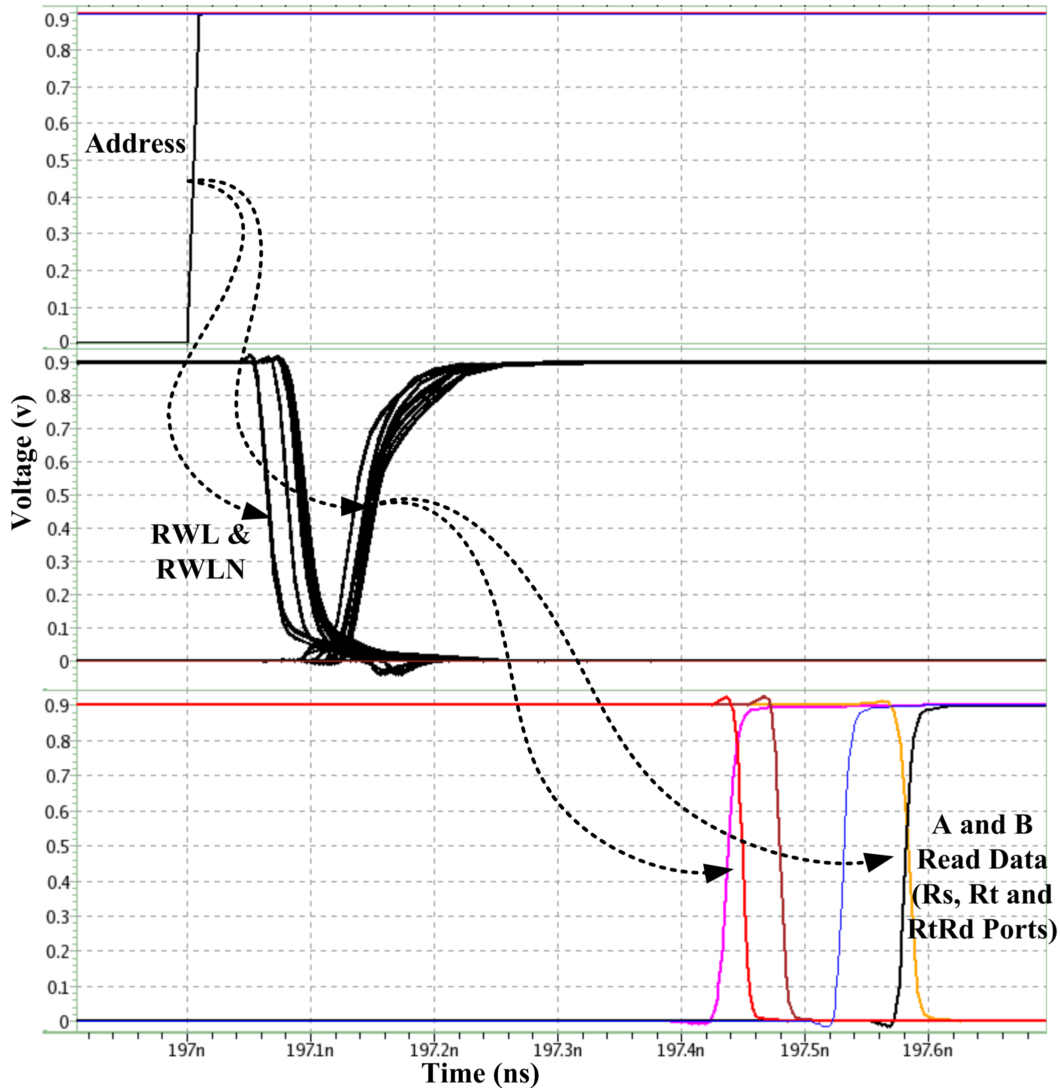


Fig 5.16 RF critical path timing path, showing address in to data out timing in red.

Bias voltages are nominal (VPW=-0.4 and VNW=1.3 v), respectively.

Timing diagrams for the read critical timing is shown in Fig. 5.16. Read address gets decoded by the read decoders and the read word lines access the cell value (on the read bit lines) through the read muxes for 1 of the 3 read ports. The values written into the cells in the ultraism simulations testbench are different, hence we see different assertions on the A and B data. Timing abstract (.lib) is extracted with high effort SI integrity settings to

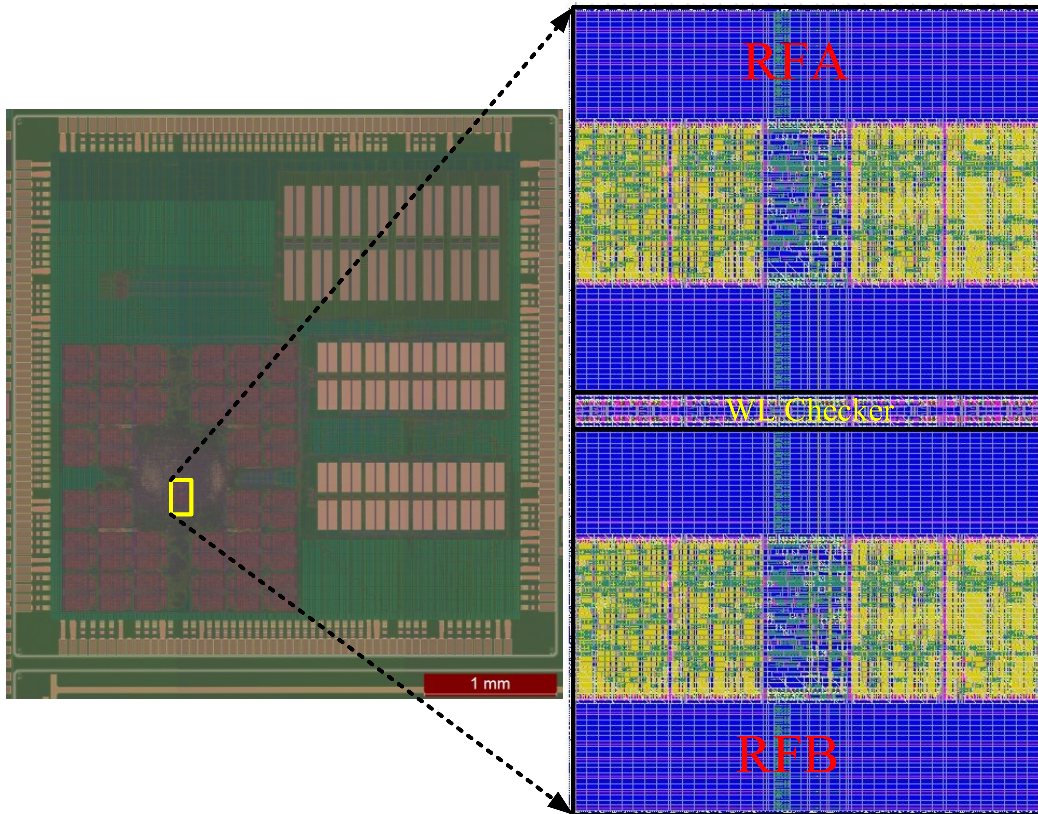


Fig 5.17 Physical arrangement of the dual redundant arrays and word line checkers in the 55 nm implemented test chip TC 25.

ensure maximum accuracy while modelling the RF delays during APR. Ultrasim vectors passed with 100% test coverage (0 errors on the tests run). All the read and error signals were matched on the schematic and extracted parasitic netlist simulations.

5.9. Implementation Summary

The RF design on 55 nm low standby power process is shown in Fig. 5.17. The outline of the RF on the HERMES2 design block of test chip TC25 is shown, the 2 RF copies A and B are highlighted in the zoomed image and the word line checker is placed in the middle for optimal timing and placement area. The HERMES2 design is proved functional in silicon validation as the instructions and data are loaded from/to the RF block.

A test program of print "Hello World" is executed on the processor, which uses the RF to execute the same.

5.10. Summary

This chapter described the semi-custom design flow for the design of a DMR multi-port register file. The basic architecture and error recovery mechanisms of the DMR RF are explained. Custom design of the RF array with bit-cell design optimized for area and routing utilization is demonstrated. The APR decoder synthesis and design methodology is presented to ensure design of decoding logic for the multi-port RF cell. The decoder APR allows fast turn-around design of five unique decoder implementations that are arranged in two redundant DMR decoders. The design is implemented on a 55 nm LSP process as a part of a radiation hardened microprocessor explained in chapter 3. The decoder is proven functional in simulations with operation speeds above a GHz. Silicon validation of the HERMES2 processor has proven functionality of the RF design on the implemented design.

CHAPTER 6. CONCLUSION

This dissertation described in detail, design and CAD techniques to implement radiation hardened digital architectures. Radiation hardened by design techniques like double and triple mode redundancy used in digital architecture such as an AES, HERMES2 microprocessor and pulsed delay locked loops are implemented in this work. The problem of domain crossing errors in redundant logic is addressed in the design and CAD techniques presented. Novel contributions of this dissertation are: Module level separation for a TMR AES design, interleaved high density separation and ReAPR CAD flow used in implementing HERMES2 microprocessor and a radiation hardened, pulsed DLL for DDR2/3 standard clocking. A brief summary of the dissertation chapter is provided in the following paragraphs.

Chapter 1 described the overview of the radiation environment that electronics are subject to, their effect on planar and finfet CMOS devices and the errors that manifest as a result of this interaction. Domain crossing errors that thwart redundancy schemes are discussed and their relation to spatial separation established. Prior works in the field of soft-error mitigation are also discussed to lay the groundwork for this dissertation.

Chapter 2 discusses the large fences domain separation methodology used in implementing an AES engine on a 90 nm process. The design flow used pulse-clocked latches as the sequential elements which are domain separated and designed to withstand statistical and systematic variations. Combinational logic is also domain separated using key and data specific fences derived based on the data flow. Clock cells are domain separated using halos. The design is shown to be DCE immune to high statistical confidence (99.999%) using spatial separation analysis, logic simulations and silicon

validation. Beam testing is conducted with 63 MeV proton beam and recovers successfully from 32 errors.

Chapter 3 introduces the improved interleaved fences and describes the ReAPR methodology for complex redundant architectures. Interleaved fences achieves increased cell density (4.9 %), reduced power (5.6%) and reduced wire length (28.5 %) over the module level separation. HERMES2 processor is used as a test vehicle to demonstrate the domain separated placement of double and triple mode redundant portions of the design. The design is implemented in a 55 nm process and proved to be domain separated (99.99% cell comparisons) using spatial separation analysis. The interleaved fences are also shown to improve routing, placement densities and power consumption in comparison to the large fences. The physical implementation is also proven to be soft-error hard with silicon validation on a 90 nm recovering from errors in different logic units of the processor, validating the CAD and circuit design methodology efficacy.

Chapter 4 introduces a novel, pulsed multiplying DLL for radiation hardened DDR3 interfaces. The architecture of the digital delay locked loop is explained with circuit design of the design constituents for required performance. Statistical and corner simulations prove the efficacy of the design in presence of random and systematic IC corner variations. Control and tracking algorithms are described, which allow DDR3 standard jitter performance across corners. The design achieves an operating range of 100-850 MHz, energy consumption of 14 pJ/cycle and a peak-to peak jitter of 22.4 ps. Physical implementation with separation for DCE suppression using previously described methodologies is also elucidated. The design is compared to other radiation hardened designs and demonstrates improved PPA. The implementation of the top level architecture

on silicon needs further exploration, while portions of the design have been fabricated on 90 and 55 nm.

Chapter 5 showcases the design of a DMR register file in 55 nm technology used in HERMES2 processor speculative pipeline. APR for the decoder design and circuit design for RF array with well-bias are demonstrated. The dual redundant design is proven functional in top level HERMES2 silicon validation.

Thus, a range of designs with varying complexities and redundancy schemes are implemented in this work. These designs are optimized for power, performance area and reliability, thereby advancing state-of-the-art radiation hardened design implementation.

REFERENCES

[Barn06] Barnaby, H. J.; , "Total-Ionizing-Dose Effects in Modern CMOS Technologies," Nuclear Science, IEEE Transactions on , vol.53, no.6, pp.3103-3121, Dec. 2006.

[Barn09] H. J. Barnaby, M. L. McLain, I. S. Esqueda, and X. J. Chen, “Modeling ionizing radiation effects in solid state materials and CMOS devices,” IEEE Trans. Circuits Syst. I, vol. 56, pp. 1870–1883, Aug. 2009.

[Barth03] Barth, J.L.; Dyer, C.S.; Stassinopoulos, E.G.; , "Space, atmospheric, and terrestrial radiation environments," Nuclear Science, IEEE Transactions on , vol.50, no.3, pp. 466- 482, June 2003.

[Baze00] Baze, Mark P., Steven P. Buchner, and Dale McMorrow. "A digital CMOS design technique for SEU hardening." Nuclear Science, IEEE Transactions on47.6 (2000): 2603-2608.

[Baze02] Baze, M. P., et al. "SEU hardening techniques for retargetable, scalable, sub-micron digital circuits and libraries." Single Event Effects Symp., Manhattan Beach, CA, April, klabs. org. Vol. 5. 2002.

[Baze06] M. P. Baze, J. Wert, J. W. Clement, M. G. Hubert, A. Witulski, O. A. Amusan, L. Massengill, D. McMorrow, “Propagating SET Characterization Technique for Digital CMOS Libraries,” IEEE Trans. Nucl. Sci, vol. 53, no. 6, pp. 3472-3478, Dec 2006.

[Beau93] W. Beauvais, P. McNulty, W. A. Kader, and R. Reed, “SEU parameters and proton-induced upsets,” in Proc. Sec. European Conf. on Radiation and its Effects on Components and Systems, pp. 540-545, Sept. 1993.

[Bene04] Benedetto, J.; Eaton, P.; Avery, K.; Mavis, D.; Gadlage, M.; Turflinger, T.; Dodd, P.E.; Vizkelethyd, G.; , "Heavy ion-induced digital single-event transients in deep submicron Processes," Nuclear Science, IEEE Transactions on , vol.51, no.6, pp. 3480-3485, Dec. 2004

[Bene06] J. M. Benedetto, P. H. Eaton, D. G. Mavis, M. Gadlage, T. Turflinger, “Digital Single Event Transient Trends With Technology Node Scaling,” IEEE Trans. Nucl. Sci, vol. 53, no. 6, pp. 3462-3465, Dec 2006.

[Black08] J. Black, et al., “Characterizing SRAM Single Event Upset in Terms of Single and Multiple Node Charge Collection,” IEEE Trans. Nuc. Sci., 55, 6, pp. 2943 – 2947, Dec. 2008.

[Calin96] T. Calin, M. Nicolaidis and R.Velazco, “Upset hardened memory design for submicron CMOS technology,” IEEE Trans. Nucl. Sci., vol. 43, no. 6, pp. 2874-2878, Dec. 1996.

[Carm01] Carmichael, Carl. "Triple module redundancy design techniques for Virtex FPGAs." Xilinx Application Note XAPP197 1 (2001).

[Chandra01] A. Chandrakasan, W. J. Bowhill, and F. Fox, Design of High-Performance Microprocessor Circuits, 2001 :IEEE Press.

[Chel15] S. Chellappa, C. Ramamurthy, V. Vashishtha and L. T. Clark, “Advanced encryption system with dynamic pipeline reconfiguration for minimum energy operation,” Proc. ISQED, pp. 201-206, Mar. 2015.

[Chen84] Chen, C. L.; Hsiao, M. Y.; , "Error-Correcting Codes for Semiconductor Memory Applications: A State-of-the-Art Review," IBM Journal of Research and Development , vol.28, no.2, pp.124-134, March 1984

[Chip12] Chipana, Raul; Kastensmidt, F.L.; Tonfat, Jorge; Reis, R., "SET susceptibility estimation of clock tree networks from layout extraction," Test Workshop (LATW), 2012 13th Latin American , vol., no., pp.1,6, 10-13 April 2012

[Chitu05] C. Chitua, and M. Glesner, “An FPGA implementation of the AES-Rijndael in OCB/ECB modes of operation” Microelectronics Journal, 2005, pp. 139–146.

[Clar01] L. T. Clark, E. J. Hoffman, J. Miller, M. Biyani, Y. Liao, S. Strazdus, M. Morrow, K. E. Velarde and M. Yarch, “An embedded 32-b microprocessor core for low-power and high-performance applications,” IEEE J. Solid-State Circuits, vol. 36, pp. 1599-1608, Nov. 2001.

[Clar11] Clark, L.T., et al. “A dual mode redundant approach for microprocessor soft error hardness,” IEEE Trans. Nucl. Sci., Vol. 58, no. 6, pp.3018-3025, Dec., 2011.

[Clark01] L. Clark, et al., “An embedded microprocessor core for high performance and low power applications,” IEEE JSSC, 36, 11, pp. 498-506, Nov. 2001.

[Clark11] L. Clark, D. Patterson, N. Hindman, K. Holbert, and S. Guertin, “A dual mode redundant approach for microprocessor soft error hardness,” IEEE Trans. Nucl. Sci., vol. 58, no. 6, Dec. 2011, pp. 3018-3025.

[Dehng00] G.K. Dehng, et al. "Clock-deskew buffer using a SAR-controlled delay-locked loop.", IEEE Journal of Solid-State Circuits, 2000, pp 1128-1136.

[Dodd03] Dodd, P.E.; Massengill, L.W.; , "Basic mechanisms and modeling of single-event upset in digital microelectronics," Nuclear Science, IEEE Transactions on , vol.50, no.3, pp. 583- 602, June 2003.

[Dodd95] P. Dodd and F. Sexton, “Critical charge concepts for CMOS SRAMs,” IEEE Trans. Nucl. Sci., vol. 42, no. 6, pp. 1764–1771, Dec. 1995.

[Eaton04] Eaton, P., et al. "Single event transient pulsewidth measurements using a variable temporal latch technique." IEEE transactions on nuclear science 51.6 (2004): 3365-3368.

[Ecof94] R. Ecoffet, S. Duzellier, P. Tastet, C. Aicardi, and M. Labrunee, “Observation of heavy ion induced transients in linear circuits,” Proc. IEEE NSREC Radiation Effects Data Workshop Record, pp. 72–77, 1994.

[Elle12] Ellerman, Paul. "Calculating Reliability using FIT & MTTF: Arrhenius HTOL Model." microsemi, Tech. Rep. (2012).

[El-Mamo11] El-Mamouni, F., E. X. Zhang, N. D. Pate, N. Hooten, R. D. Schrimpf, R. A. Reed, K. F. Galloway et al. "Laser-and heavy ion-induced charge collection in bulk FinFETs." IEEE Transactions on Nuclear Science 58, no. 6 (2011): 2563-2569.

[Fang11] Fang, Yi-Pin, and Anthony S. Oates. "Neutron-induced charge collection simulation of bulk FinFET SRAMs compared with conventional planar SRAMs." IEEE Transactions on Device and Materials Reliability 11, no. 4 (2011): 551-554.

[Fang16] Fang, Yi-Pin, and Anthony S. Oates. "Characterization of Single Bit and Multiple Cell Soft Error Events in Planar and FinFET SRAMs." IEEE Transactions on Device and Materials Reliability 16, no. 2 (2016): 132-137.

[Fetz06] E. Fetzer, D. Dahle, C. Little, and K. Safford, “The parity protected, multithreaded register files on the 90-nm itanium microprocessor,” IEEE J. Solid-State Circuits, vol. 41, no. 1, pp. 246–255, Jan. 2006.

[Fred96] A. R. Frederickson, “Upsets related to spacecraft charging,” IEEE Trans. Nucl. Sci., vol. 43, no. 2, pp. 426-441, 1996.

[Fuji90] Fujiwara, E.; Pradhan, D.K.; , "Error-control coding in computers," Computer , vol.23, no.7, pp.63-72, July 1990.

[Furu10] Furuta, J.; Hamanaka, C.; Kobayashi, K.; Onodera, Hidetoshi, "A 65nm Bistable Cross-coupled Dual Modular Redundancy Flip-Flop capable of protecting soft errors on the C-element," VLSI Circuits (VLSIC), 2010 IEEE Symposium on , vol., no., pp.123,124, 16-18 June 2010.

[Gadl04] Gadlage, M.J.; Schrimpf, R.D.; Benedetto, J.M.; Eaton, P.H.; Mavis, D.G.; Sibley, M.; Avery, K.; Turflinger, T.L.; , "Single event transient pulse widths in digital microcircuits," Nuclear Science, IEEE Transactions on , vol.51, no.6, pp. 3285- 3290, Dec. 2004

[Gasp13] N. Gaspard, et al., "Technology Scaling Comparison of Flip-Flop Heavy-Ion Single-Event Upset Cross Sections," IEEE Trans. Nuc. Sci., 60, 6, pp. 4368-4373, Dec. 2013.

[Gies97] Gieseke, Bruce A., et al. "A 600 MHz superscalar RISC microprocessor with out-of-order execution." Solid-State Circuits Conference, 1997. Digest of Technical Papers. 43rd ISSCC., 1997 IEEE International. IEEE, 1997.

[Gils08] Wirth, Gilson, Fernanda L. Kastensmidt, and Ivandro Ribeiro. "Single event transients in logic circuits—load and propagation induced pulse broadening." Nuclear Science, IEEE Transactions on 55.6 (2008): 2928-2935.

[Good10] Good, Tim, and Mohammed Benaissa. "692-nW Advanced Encryption Standard (AES) on a 0.13-$\ mu $ m CMOS." IEEE Transactions on very large scale integration (VLSI) systems 18, no. 12 (2010): 1753-1757.

[Guss96] Gussenhoven, M.S.; Mullen, E.G.; Brautigam, D.H.; , "Improved understanding of the Earth's radiation belts from the CRRES satellite," Nuclear Science, IEEE Transactions on , vol.43, no.2, pp.353-368, Apr 1996.

[Hans09] Hansen, D.L.; et.al. , "Clock, Flip-Flop, and Combinatorial Logic Contributions to the SEU Cross Section in 90 nm ASIC Technology," Nuclear Science, IEEE Transactions on , vol.56, no.6, pp.3542,3550, Dec. 2009.

[Hazu00] Hazucha, Peter, Christer Svensson, and Stephen A. Wender. "Cosmic-ray soft error rate characterization of a standard 0.6-/spl mu/m cmos process." Solid-State Circuits, IEEE Journal of 35.10 (2000): 1422-1429.

[Heil89] S. J. Heileman, W. R. Eisenstadt, R. M. Fox, R. S. Wagner, N. Bordes, and J. M. Bradley, "CMOS VLSI single event transient characterization," IEEE Trans. Nucl. Sci., vol. 36, no. 6, pp. 2287-2291, 1989.

[Hind09] Hindman, N.D.; Pettit, D.E.; Patterson, D.W.; Nielsen, K.E.; Xiaoyin Yao; Holbert, K.E.; Clark, L.T.; , "High speed redundant self-correcting circuits for radiation hardened by design logic," Radiation and Its Effects on Components and Systems (RADECS), 2009 European Conference on , vol., no., pp.465-472, 14-18 Sept. 2009.

[Hind11] Hindman, N.D.; Clark, L.T.; Patterson, D.W.; Holbert, K.E., "Fully Automated, Testable Design of Fine-Grained Triple Mode Redundant Logic," Nuclear Science, IEEE Transactions on , vol.58, no.6, pp.3046,3052, Dec. 2011.

[Hsia70] M. Hsiao, “A class of optimal minimum odd-weight-column SEC-DEC codes,” IBM J. Res. Develop., vol. 14, no. 4, pp. 395–401, Jul. 1970.

[Hsieh81] Hsieh, C. M.; Murley, P. C.; O'Brien, R. R.; , "Dynamics of Charge Collection from Alpha-Particle Tracks in Integrated Circuits," Reliability Physics Symposium, 1981. 19th Annual , vol., no., pp.38-42, April 1981.

[Hsieh81a] Hsieh, C.M.; Murley, P.C.; O'Brien, R.R.; , "A field-funneling effect on the collection of alpha-particle-generated carriers in silicon devices," Electron Device Letters, IEEE , vol.2, no.4, pp.103-105, April 1981.

[Hugh03] Hughes, H.L, Benedetto, J.M, "Radiation effects and hardening of MOS technology: devices and circuits," Nuclear Science, IEEE Transactions on , vol.50, no.3, pp. 500- 521, June 2003.

[Kehl11] Kehl, N.; Rosenstiel, W., "An Efficient SER Estimation Method for Combinational Circuits," Reliability, IEEE Transactions on , vol.60, no.4, pp.742,747, Dec. 2011.

[Klei10] Kleinosowski, A. J., Scott M. Willenborg, and Bruce B. Winter. "Method for radiation tolerance by automated placement." U.S. Patent 7,774,732, issued August 10, 2010.

[Knud06] J. Knudsen and L. Clark, “An area and power efficient radiation hardened by design flip-flop,” IEEE Trans. Nucl. Sci., vol. 53, no. 6, pp. 3392-3399, Dec. 2006.

[Knud06] Knudsen, J. E.; Clark, L. T.; , "An Area and Power Efficient Radiation Hardened by Design Flip-Flop," Nuclear Science, IEEE Transactions on , vol.53, no.6, pp.3392-3399, Dec. 2006.

[Koba09] D. Kobayashi, T. Makino, and K. Hirose, “Analytical expression for temporal width characterization of radiation-induced pulse noises in SOI CMOS logic gates,” Proc. IRPS, pp. 165-169, 2009.

[Koga93] R. Koga, S. D. Pinkerton, S. C. Moss, D. C. Mayer, S. Lalumondiere, S. J. Hansel, K. B. Crawford, and W. R. Crain, “Observation of single event upsets in analog microcircuits,” IEEE Trans. Nucl. Sci., vol. 40, no. 6, pp. 1838–1844, Dec. 1993.

[Koga97] Koga, R.; Penzin, S.H.; Crawford, K.B.; Crain, W.R.; , "Single event functional interrupt (SEFI) sensitivity in microcircuits,", RADECS 97. Fourth European Conference on , vol., no., pp.311-318, 15-19 Sep 1997.

[Koppa02] J. Koppanalil, et al. "A case for dynamic pipeline scaling," Proc. Intl. Conf. on Compilers, Architecture, Synthesis for Embedded Systems, ACM, 2002, pp. 1-8.

[LaBel96] LaBel, K.A.; Gates, M.M.; , "Single-event-effect mitigation from a system perspective," Nuclear Science, IEEE Transactions on , vol.43, no.2, pp.654-660, Apr 1996.

[Lacoe00] Lacoe, R.C.; Osborn, J.V.; Koga, R.; Brown, S.; Mayer, D.C.; , "Application of hardness-by-design methodology to radiation-tolerant ASIC technologies," Nuclear Science, IEEE Transactions on , vol.47, no.6, pp.2334-2341, Dec 2000.

[Ladb07] R. Ladbury, "Statistical properties of SEE rate calculation in the limits of large and small event counts," IEEE Trans. Nucl. Sci., vol. 54, pp. 2113-2119, Dec. 2007.

[Lee15] Lee, Soonyoung, Ilgon Kim, Sungmock Ha, Cheong-sik Yu, Jinhyun Noh, Sangwoo Pae, and Jongwoo Park. "Radiation-induced soft error rate analyses for 14 nm FinFET SRAM devices." In Reliability Physics Symposium (IRPS), 2015 IEEE International, pp. 4B-1. IEEE, 2015.

[Mathu06] C. N. Mathur, K. Narayan and K. Subbalakshmi, "High diffusion cipher: Encryption and error correction in a single cryptographic primitive," in Applied Cryptography and Network Security, Berlin, Germany: Springer, Jun. 2006, pp. 309-324.

[Matu10] B. Matush, T. Mozdzen, L. Clark and J. Knudsen, "Area efficient temporally hardened by design flip flop circuits," IEEE Trans. Nucl. Sci., vol. 57, no. 6, pp. 3588-3595, Dec. 2010.

[Mavi02] D. Mavis and P. Eaton, "Soft error mitigation techniques for modern microcircuits," Proc. IEEE IRPS, Aug. 2002 pp. 216-225, 2002.

[Mavi02] Mavis, D.G.; Eaton, P.H.; , "Soft error rate mitigation techniques for modern microcircuits," Reliability Physics Symposium Proceedings, 2002. 40th Annual , vol., no., pp. 216- 225, 2002.

[Ming04] Ming Zhang; Shanbhag, N.R., "A soft error rate analysis (SERA) methodology," Computer Aided Design, 2004. ICCAD-2004. IEEE/ACM International Conference on , vol., no., pp.111,118, 7-11 Nov. 2004.

[Ming06] Zhang, Ming, and Naresh R. Shanbhag. "Soft-error-rate-analysis (SERA) methodology." Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 25.10 (2006): 2140-2155.

[Mohr07] K. Mohr and L. Clark, "Experimental characterization and application of circuit architecture level single event transient mitigation," Proc. IRPS, pp. 312-317, 2007.

[Muss96] Musseau, O.; Gardic, F.; Roche, P.; Corbiere, T.; Reed, R.A.; Buchner, S.; McDonald, P.; Melinger, J.; Tran, L.; Campbell, A.B.; , "Analysis of multiple bit upsets (MBU) in CMOS SRAM," Nuclear Science, IEEE Transactions on , vol.43, no.6, pp.2879-2888, Dec 1996.

[Naff02] S. Naffziger et al., "The implementation of the Itanium 2 microprocessor," IEEE Journal of Solid-State Circuits, vol. 37, no. 11, pp. 1448–1460, Nov. 2002.

[Nara06] Narasimham, B.; Ramachandran, V.; Bhuva, B.L.; Schrimpf, R.D.; Witulski, A.F.; Holman, W.T.; Massengill, L.W.; Black, J.D.; Robinson, W.H.; McMorrow, D., "On-Chip Characterization of Single-Event Transient Pulsewidths," Device and Materials Reliability, IEEE Transactions on , vol.6, no.4, pp.542,549, Dec. 2006.

[Nara06b] Narayanan. V, Xie. Y, "Reliability concerns in embedded system designs," Computer , vol.39, no.1, pp. 118- 120, Jan. 2006.

[Nase06] Naseer, Riaz, and Jeff Draper. "DF-DICE: a scalable solution for soft error tolerant circuit design." Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on. IEEE, 2006.

[NIST01] National Institute of Standards and Technology, Advanced Encryption Standard AES, Federal Information Processing Standards Publication FIPS 197, 2001, http://csrc.nist.gov/publications/fips.

[Noh15] Noh, Jinhyun, Vincent Correas, Soonyoung Lee, Jongsung Jeon, Issam Nofal, Jacques Cerba, Hafnaoui Belhaddad, Dan Alexandrescu, YoungKeun Lee, and Steve Kwon. "Study of neutron soft error rate (SER) sensitivity: investigation of upset mechanisms by comparative simulation of FinFET and planar MOSFET SRAMs." IEEE Transactions on Nuclear Science 62, no. 4 (2015): 1642-1649.

[Oldi15] Oldiges, Phil, Kenneth P. Rodbell, M. Gordon, John G. Massey, Kevin Stawiasz, C. Murray, H. Tang, K. Kim, and K. Paul Muller. "SOI FinFET soft error upset susceptibility and analysis." In Reliability Physics Symposium (IRPS), 2015 IEEE International, pp. 4B-2. IEEE, 2015.

[Prit02] Pritchard .B .E, G. M. Swift, and A. H. Johnston, “Radiation effects predicted, observed, and compared for spacecraft systems,” Proc. IEEE NSREC Radiation Effects Data Workshop Record, pp. 7–17, 2002.

[Quin07] Quinn H., et al. "A review of Xilinx FPGA architectural reliability concerns from Virtex to Virtex-5," Proc. RADECS, pp. 1-8, Sep. 2007.

[Rama15] Ramamurthy C., et al. “A High Performance Low Power Pulse-Clocked TMR Circuits for Soft-Error Hardness,” IEEE Trans. Nucl. Sci., Vol. 62, no. 6, pp.3040-8, Dec., 2015.

[Rijm01] Rijmen, Vincent, and Joan Daemen. "Advanced encryption standard." Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology (2001): 19-22.

[Rodb13] K. Rodbell, “Where Radiation Effects in Emerging Technologies Really Matter,” NSREC Short Course, 2013.

[Ruan11] Ruano, Oscar, Juan Antonio Maestro, and Pedro Reviriego. "A fast and efficient technique to apply Selective TMR through optimization." Microelectronics Reliability 51, no. 12 (2011): 2388-2401.

[Sagg05] Saggese, G.P.; Wang, N.J.; Kalbarczyk, Z.T.; Patel, S.J.; Iyer, R.K.; , "An experimental study of soft errors in microprocessors," Micro, IEEE , vol.25, no.6, pp. 30-39, Nov.-Dec. 2005.

[Seif05] N. Seifert, et al., "Radiation induced clock jitter and race," Proc. Int. Phys. Rel. Symp., April 2005, pp. 215-222.

[Seif06] N. Seifert, et al., "Radiation-induced soft error rates of advanced CMOS bulk devices," Proc. Int. Phys. Reliab. Symp, March 2006, pp. 217-225.

[Seif12] Seifert, Norbert, Balkaran Gill, Shah Jahinuzzaman, Joseph Basile, Vinod Ambrose, Quan Shi, Randy Allmon, and Arkady Bramnik. "Soft error susceptibilities of 22 nm tri-gate devices." IEEE Transactions on Nuclear Science 59, no. 6 (2012): 2666-2673.

[Seif15] Seifert, Norbert, Shah Jahinuzzaman, Jyothi Velamala, Ricardo Ascazubi, Nikunj Patel, Balkaran Gill, Joseph Basile, and Jeffrey Hicks. "Soft error rate improvements in 14-nm technology featuring second-generation 3d tri-gate transistors." IEEE Transactions on Nuclear Science 62, no. 6 (2015): 2570-2577.

[Sham15] Shambhulingaiah, Sandeep, Christopher Lieb, and Lawrence T. Clark. "Circuit simulation based validation of flip-flop robustness to multiple node charge collection." IEEE Transactions on Nuclear Science 62.4 (2015): 1577-1588.

[Shen09] Sheng, Weiguang, Liyi Xiao, and Zhigang Mao. "Soft error optimization of standard cell circuits based on gate sizing and multi-objective genetic algorithm." In Design Automation Conference, 2009. DAC'09. 46th ACM/IEEE, pp. 502-507. IEEE, 2009.

[Shiba 06] S. Shibatani and A. Li, "Pulse-latch approach reduces dynamic power,"July 2006, EE Times.

[Shim06] H. Shimada, H. Ando, and T. Shimada, "A hybrid power reduction scheme using pipeline stage unification and dynamic voltage scaling." Proc. IEEE COOL Chips, 2006, pp. 201-214.

[Song10] H. J. Song, "VLSI High-Speed I/O Circuits," Xlibris, ISBN#978-1-4415-5987-6, 2010.

[Sore00] R. Harboe-Sorensen, F. X. Guerre, H. Constans, J. Van Dooren, G. Berger, and W. Hajdas, "Single event transient characterization of analog ICs for ESA's satellites,"

in Proc. IEEE 5th Eur. Conf. Radiation and Its Effects on Components and Systems, 2000, pp. 573–581.

[Sushil15] S. Kumar, S.Chellappa and L.T. Clark, “Temporal Pulse-clocked Multi-bit Flip-flop Mitigating SET and SEU” (Accepted ISCAS 2015).

[Teif08] Teifel, J., "Self-Voting Dual-Modular-Redundancy Circuits for Single-Event-Transient Mitigation," Nuclear Science, IEEE Transactions on , vol.55, no.6, pp.3435,3439, Dec. 2008.

[Tsch01] J. Tschanz, S. Narendra, Z. Chen, S. Borkar, M. Sachdev and V. De, “Comparative delay and energy of single edge-triggered & dual edge-triggered pulsed flip-flops for high-performance microprocessors,” Proc. ISLPED, pp. 147-152, Aug. 2001.

[Uemu10] [1] T. Uemura, Y. Tosaka, H. Matsuyama, K. Shono, C. J. Uchibori, K. Takahisa, M. Fukuda and K. Hatanaka, “SEILA: Soft error immune latch for mitigating multi-node-SEU and local-clock-SET,” Proc. IRPS, pp. 218-223, May 2010.

[Vash14] Vashishtha, Vinay. "Register Files for Embedded Low-Power Applications Including Microprocessors." PhD diss., ARIZONA STATE UNIVERSITY, 2014.

[Wang08] Fan Wang; Agrawal, V.D., "Soft Error Rate Determination for Nanometer CMOS VLSI Logic," System Theory, 2008. SSST 2008. 40th Southeastern Symposium on , vol., no., pp.324,328, 16-18 March 2008.

[Wang10] Wang, Fan, and Vishwani D. Agrawal. "Soft error rate determination for nanoscale sequential logic." Quality Electronic Design (ISQED), 2010 11th International Symposium on. IEEE, 2010.

[Warn10] J. Warnock, L. Sigal, D. Wendel, K. P. Muller, J. Friedrich, V. Zyuban, E. Cannon and A. J. Kleinosowski, “POWER7TM local clocking and clocked storage elements,” IEEE ISSCC Dig. Tech. Papers, pp. 178-179, Feb. 2010.

[Warren09] K. Warren, et al., “Heavy Ion Testing and Single Event Upset Rate Prediction Considerations for a DICE Flip-Flop,” IEEE Trans. Nuc. Sci., 56, 6, pp. 3130-3137, Dec. 2009.

[Warren09] K. Warren, et al., “Heavy ion testing and single event upset rate prediction considerations for a DICE flip-flop,” IEEE Trans. Nucl. Sci., vol. 56, no. 6, pp. 3130-3137, Dec. 2009.

[Weav04] C. Weaver, J. Emer, S. Mukherjee, and S. Reinhardt, “Techniques to reduce the soft error rate of a high-performance microprocessor,” Proc. ISCA, 2004, pp. 264-27.
[Webb97] Webb, Charles F., et al. "A 400-MHz s/390 microprocessor." Solid-State Circuits, IEEE Journal of 32.11 (1997): 1665-1675.

[Wu13] Wu, Kai-Chiang, and Diana Marculescu. "A low-cost, systematic methodology for soft error robustness of logic circuits." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 21, no. 2 (2013): 367-379.

[Yao10] Yao X., et al. "A 90 nm bulk CMOS radiation hardened by design cache memory," IEEE Trans. Nucl. Sci., Vol. 57, no. 4, 2089-97, Aug., 2010.

[Yao10a] X. Yao, L. Clark, D. Patterson, K. Holbert, "A 90 nm bulk CMOS radiation hardened by design cache memory," IEEE Trans. Nucl. Sci, vol. 57, no. 4, pp. 2089-2097, Aug. 2010.

[Yao10b] Yao. X; Clark, L.T.; Chellappa, S.; Holbert, K.E.; Hindman, N.D., "Design and Experimental Validation of Radiation Hardened by Design SRAM Cells," Nuclear Science, IEEE Transactions on , vol.57, no.1, pp.258-265, Feb. 2010.

[Zhang06] M. Zhang et al, "Sequential Element Design with Built-In Soft Error Resilience," IEEE Trans. VLSI Sys., 14, 12, pp. 1368-1378, Dec. 2006.

[Zhang06] Ming Zhang; Mitra, S.; Mak, T.M.; Seifert, N.; Wang, N.J.; Quan Shi; Kee Sup Kim; Shanbhag, N.R.; Patel, S.J., "Sequential Element Design With Built-In Soft Error Resilience," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.14, no.12, pp.1368,1378, Dec. 2006.

[Zhao15] Zhao, Wenfeng, Yajun Ha, and Massimo Alioto. "AES architectures for minimum-energy operation and silicon demonstration in 65nm with lowest energy per encryption." In Circuits and Systems (ISCAS), 2015 IEEE International Symposium on, pp. 2349-2352. IEEE, 2015.

[Zhou06] Zhou, Quming, and Kartik Mohanram. "Gate sizing to radiation harden combinational logic." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 25, no. 1 (2006): 155-166.