Efficient Flip-Flop Designs for SET/SEU Mitigation with Tolerance to Crosstalk Induced Signal Delays

Aditya Jagirdar
Department of Electrical and Computer Engineering
Rutgers University
Piscataway, New Jersey - 08904
Email: jagirdar@eden.rutgers.edu

Roystein Oliveira
Department of Electrical and Computer Engineering
Rutgers University
Piscataway, New Jersey - 08904
Email: roystein@eden.rutgers.edu

Tapan J.Chakraborty
Lucent Technologies
Whippany, New Jersey - 07981
Email: tchakraborty@alcatel-lucent.com

***Abstract*— Radiation from outer space comprising of charged particles can affect transistors in an integrated circuit, resulting in unexpected switching of transistors. This temporary disturbance is called *Soft-Error*. With decreasing feature sizes and noise margins, circuits become more prone to such effects. A soft-error could manifest itself in a system as a *Single Event Upset* (SEU) or a *Single Event Transient* (SET), depending on whether a storage element or a combinational circuit was affected. In this paper, we propose two unique register designs that provide tolerance to SEU and SET effects, by making efficient use of space and time redundancy techniques. Our results on ISCAS'89 benchmark circuits indicate an average transistor overhead of 28% and 20% for design 1 and 2 respectively. The designs provide concurrent error correction with minimal degradation of system performance.**

I. Introduction

SEU or soft error may occur in a chip when exposed to radiation (Cosmic rays, α-particle, Neutrons etc.). This may cause an erroneous change in state of a system, thus affecting its operation. The effect of the error is temporary and if detected, the system can be restored to its normal operation by resetting the system or by re-execution, if possible. These errors are of concern in mission critical operations (space, medical) where a downtime or delay for system recovery is not affordable.

Exposure to radiations brings the devices on the chip under constant strike by charged particles. A high energy particle striking a node in these devices generates electron hole pairs. In the presence of strong electric field, these charged carriers move toward their respective device contacts. If the collected charge is greater than the threshold value required for determining a logic level for a transistor, an erroneous value is registered [1]. This minimum threshold value is also known as critical charge.

Earlier, soft error was a concern only in space applications. The altitude at which these systems operate exposes them to strong cosmic rays [2] which corrupts logic, thus affecting systems. The cosmic ray flux incident at sea level (terrestrial cosmic rays), consisting mainly of neutron particles loses most of its energy as it passes through the atmosphere [2] and would cause a negligible change in the threshold charge value to result in a SEU. The problem of SEU arising due to α-particle radiation from minute traces of radioactive elements in packaging material is also significant and can be addressed by ensuring a higher degree of purity of packaging materials [3]. Recently, the problem of SEU has become severe and recurrent with shrinking device geometry. Shorter channel lengths means lesser number of charge carriers and a smaller value of threshold charge [4]. The problem of SEU which was initially associated with small and densely packed memories is now commonly observed in combinational circuits and latches [5][6]. SEU's in memories has been addressed by *Error Detecting and Correcting codes* (EDC). In sequential circuits, a flip-flop (FF) input may observe transients caused by SEU's at the FF input node or due to SEU's in the *Combinational Logic Blocks* (CLB) being propagated to the FF input. A FF is also vulnerable to SEU's that cause bit flips during the opaque cycle. Figure 1 shows the *Window of Vulnerability* (WOV) [7] for a FF. The latches in a FF are vulnerable to SEU's during the latch setup time (T_{setup}) and a period T_{tf}. T_{tf} is the time interval during which a transient fault can occur. T_{nvd} is the period when the latch is transparent; T_{prop} is the time required for resulting fault to propagate to the output. In this paper we present two schemes for a FF, both of which provide SEU and SET tolerance over the WOV. Both schemes have minimal transistor and clock to Q delay overhead.

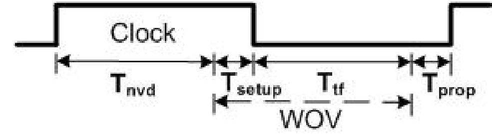

Fig. 1. Window Of Vulnerability (WOV) [7]

II. Prior Work and Motivation

Traditional techniques to provide soft-error tolerance rely on *Triple Modular Redundancy* (TMR)[8], in which the original circuit is triplicated and a majority voter used to determine the final output. However, this technique involves high overhead in terms of area and cost, which limits its usage. A low overhead TMR scheme is shown in [9]. Redundancy and/or sampling at delayed intervals provide limited cost effective

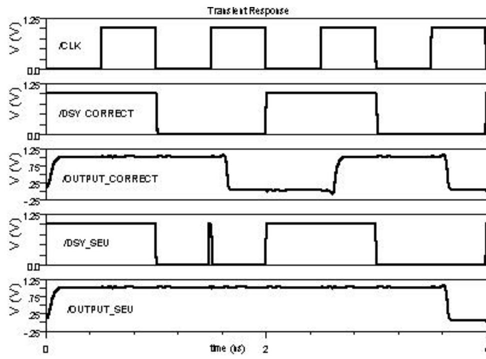

Fig. 2. Error condition in Error Blocking Scan flip flop

solutions in latches [10][11]. Designs have been suggested in [4][7] for improved latch immunity to soft errors during the storage cycle. Designs in [12][13] provide schemes for mitigating combinational transients . The *Error Blocking Scan FF* (EBSFF) [14] and *Error Trapping Scan FF* (ETSFF) [14] makes use of redundant scan hardware, to block and identify the occurrence of an SEU in a FF respectively. The *Error Blocking Scan Hold FF* (EBSHFF) [15] provides a low transistor overhead scheme for soft error detection and blocking, by making use of output buffers. The error correcting LSSD FF [16] is a modified *Level Sensitive Scan Design* (LSSD) [17] FF that provides tolerance to SEU's during the opaque period by detecting, voting and refreshing the contents of the latches in case of an error.

However, the designs in [14],[15],[16] are vulnerable to SEUs during T_{setup} of the master latch. The error condition is illustrated in Figure 2. The simulations in this paper were carried out using *Spectre* tool with the 70nm BPTM at 1GHz clock frequency and 1 V supply. Simulations (*Data-SYstem_condition, OUTPUT_condition*) are shown for correct operation (*DSY_CORRECT, OUTPUT_CORRECT*) and faulty operation (*DSY_SEU, OUTPUT_SEU*) resulting from SEU in master latch.

The time domain majority voter presented in [10] has a performance overhead since the sampling is started after the longest path in the circuit settles. Hence, an online error detection and retry procedure was considered better [18]. *Concurrent error detection* (CED) schemes use an output characteristic predictor which is then compared (using a checker) with actual circuit output to detect an error [19]. The output characteristic predictor can be implemented using hardware or time redundancy. Some of the schemes used for CED are parity prediction, self-checking circuits constructed using error detection codes, transition count and residue checking [20]. Self checking circuits may require high hardware cost for arbitrary logic functions. The work presented in [18] suggests re-doing the computation to get the correct value which requires many clock cycles, very high area and energy overhead, and is difficult to implement. Error masking, which refers to error correction on-line, has also been used to tackle soft errors. Error masking techniques are presented in [21][22]. These designs are vulnerable to SEU's on their output node as charge is stored dynamically or by means of a keeper. Prior efforts have also focused on combinational logic design for preventing pulse spreading [23], latch hardening [24], gate sizing to prevent SEU generation (which requires area and performance overhead) [25]. Time redundancy based architectural approaches also have significant performance and power overheads and design time cost [26]. A time redundancy based flip flop is proposed in [27]. It incorporates a decision circuit that helps select the output through a multiplexer. It has a performance overhead and is suitable only for the condition when an error is latched in the master system latch. In this paper we propose two designs for soft error tolerance with an aim to provide design flexibility. The designs make use of the concept of time redundancy to achieve error masking. The first design provides a simplified clocking scheme with almost no performance degradation. The second design has a low transistor overhead and has a tolerable performance degradation. Our designs make use of the scan hardware in the functional mode to store samples. The decision circuitry is a majority voter that avoids soft errors over the entire WOV. Both designs are also tolerant to transients from the CLB's.

III. Our Proposed Designs

Our designs make use of the basic scan FF (BSFF) as described in [14]. It facilitates scan based structural testing using automated test pattern generation tools, for functional testing using signature analysis, and for efficient post silicon debug [14]. It has two modes of operation, the Functional mode and the Test mode.

A. XSEUFF 1

The block diagram for the XSEUFF 1 is shown in Figure 3. This design can provide tolerance over the WOV from

- SEU in FFs.
- SET due to SEU in combinational blocks and due to crosstalk.

Latches PH2 and PH1 are the master and slave system latches. LA and LB are the master and slave scan latches. The FF captures the data on the input D by loading latches PH2, LA and LB. Latches LA and LB are clocked using $\overline{CLK}$ and *CLK*. *CLK* is delayed by Δ_1 to obtain *SYS_CLK*. Latches PH2 and PH1 are clocked using $\overline{SYS_CLK}$ and *SYS_CLK*. The clocking scheme is shown in Figure 4. The delay Δ_1 is given by the equation.

$$\Delta_1 = t_{Hold_LA} + W_{MTT} + t_{Setup_PH2} \quad (1)$$

Where W_{MTT} is the *Width of Maximum Tolerable Transient*. It is the design variable that gives the tolerance of the designed circuit to an SEU pulse. The *CLK* can be distributed using the existing scan clock routing structure in a circuit, thus simplifying the task of the designer. A keeper is used at the output node of the FF. The output of the keeper is multiplexed with the output of LA with the *CLK* signal as the select to the multiplexer. The output of the multiplexer, LB and PH1 are inputs to the majority voter. The FF is tolerant to errors over the entire window of vulnerability.

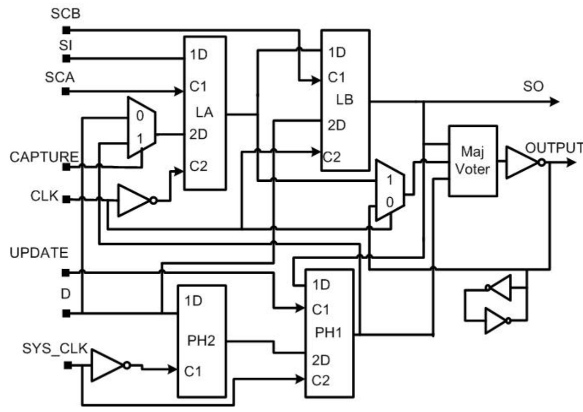

Fig. 3. The XSEUFF 1

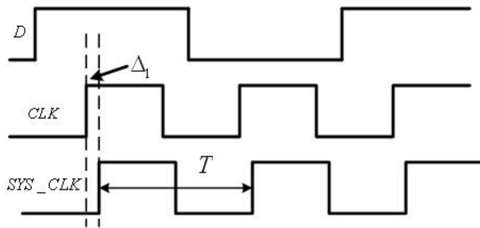

Fig. 4. Clocking scheme for the proposed design

1) Functional mode operation with tolerance to SEU: When *TESTBAR* is high, the system is in functional mode. Latch LA loads the data from D when *CLK* is low and latch LB loads the data from D when *CLK* is high. Latch PH2 loads the data from D when *SYS_CLK* is low and latch PH1 loads from PH2 when *SYS_CLK* is high. LA and LB act as the shadow of the system latches, capturing data at different time intervals for comparison. Δ_1 is selected as in Equation (1), to ensure that a SEU is never captured by LA and PH2 at the same time. The voter votes on LA, LB and PH1 when *SYS_CLK* goes high. This value is captured by the keeper at the output node. When *CLK* goes low, the voter votes on keeper, LB and PH1. This arrangement prevents data corruption at the output due to a SEU in LA or PH1, during latching or during their opaque cycle. As shown in Figure 5, LA latches the value from D. LB goes transparent before PH2 latches in the input data. PH2 latches in an incorrect data due to a SEU from the CLB and is propagated to PH1. The majority voter computes the correct output on the rising edge of *SYS_CLK*. When *CLK* goes low, the voter computes the output based on the value stored on the keeper instead of LA. The design is tolerant to only one latch being corrupted by an SEU over the WOV.

2) Test mode operation: When *TESTBAR* signal is low, the system is in test mode. The scan latches LA and LB are clocked using the scan clocks *SCA* and *SCB* respectively. LA receives the scan data input *SI*. Alternate pulsing of *SCA* and *SCB* loads LA and LB with the test vector and this enables scanning through the scan chain. The vector is then loaded into PH1 by the pulsing of the *UPDATE* signal. The system is switched from test mode to functional mode by asserting

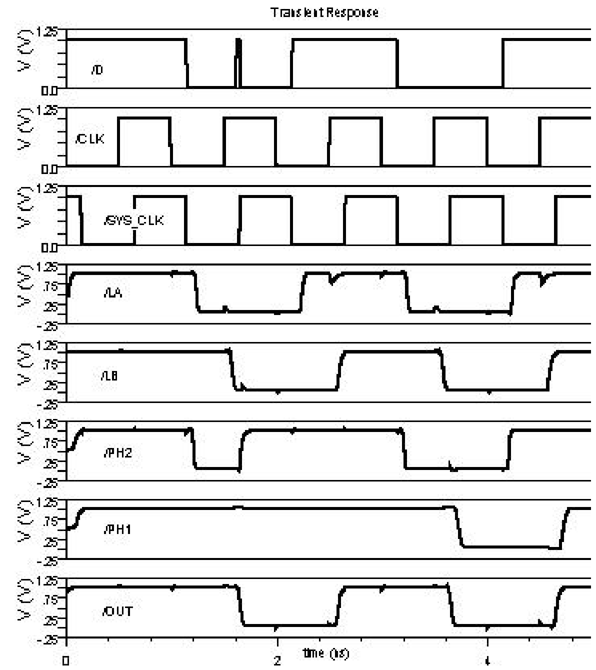

Fig. 5. Functional mode simulation

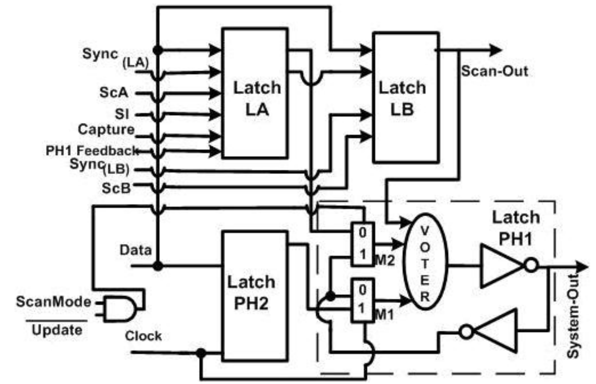

Fig. 6. The XSEUFF 2

TESTBAR. The response of the *Circuit Under Test* (CUT) to the applied vector is captured after one functional clock cycle. PH2 is loaded with the response of the previous CUT and is propagated to PH1 at the end of the cycle. *CAPTURE* is then asserted and the final output of the applied vector is captured in LA. The system is then switched to test mode and the captured response is scanned out by alternate assertion of *SCB* and *SCA* for fault analysis.

B. XSEUFF 2

The XSEUFF 2 shown in Figure 6. This design provides tolerance over the WOV from

- SEU in FFs.
- SET due to SEU in combinational blocks and due to crosstalk.
- Signal delays arising due to crosstalk.

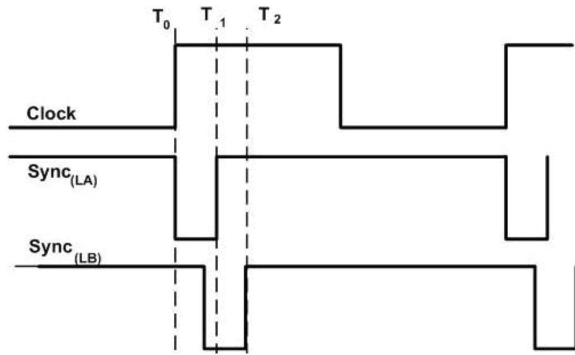

Fig. 7. Waveforms for $Sync_{LA}$ and $Sync_{LB}$

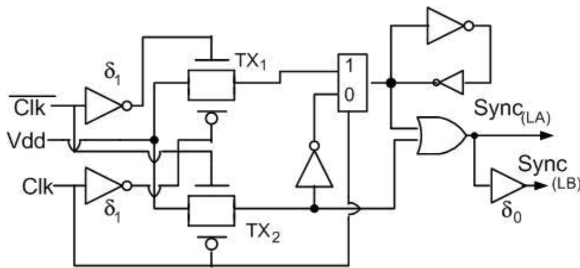

Fig. 8. Synchronous Signal Generator for the XSEUFF 2

Temporal sampling of the data line is carried out at the active clock edge, using clocks $Sync_{LA}$ and $Sync_{LB}$ as shown in Figure 7. This filters out any incoming noise that may cause a setup and/or hold time failure. Latches PH2, LA and LB are transparent when their gating signals are low and opaque when they are high. Latch PH1 has been modified to contain the majority voter circuit. In functional mode, PH2, LA and LB get data from the combinational circuit. The pulses $Sync_{LA}$ and $Sync_{LB}$ can be generated by using the circuit shown in Figure 8. The signal controlling the transmission gate TX1 is delayed through inverters (with respect to TX2) that have equal delays. By controlling this delay (δ_1), the designer can set the width of the pulse $Sync_{LA}$ and $Sync_{LB}$. The keeper at the output of the multiplexer is used to hold a zero for a brief interval of time when LA and LB turn transparent. After a delay (δ_1), TX1 gate turns on, and the output of this circuit becomes one, thus allowing LA and LB to latch in redundant values of data stored in PH2. $Sync_{LB}$ can be derived by delaying $Sync_{LA}$ through a static buffer. The delay (δ_0) of the output buffer determines the skew between $Sync_{LA}$ and $Sync_{LB}$. The buffer at the output controls the skew between the two synchronous signals while the ones at the input of Figure 8, control their widths. Any variations in the fabrication process may shift the edges of these signals relative to the active clock edge, in either direction. The XSEUFF 2 can tolerate such variations to an extent, thus avoiding any stringent constraints on the response of the signal generator. Besides, a single signal generator can be shared by multiple instances of the XSEUFF 2 cell and hence its contribution to the transistor overhead reduces significantly.

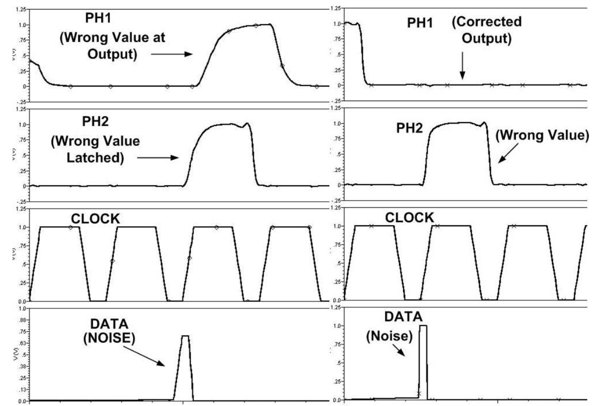

Fig. 9. Response of a BSFF Vs. XSEUFF 2 to noise pulses

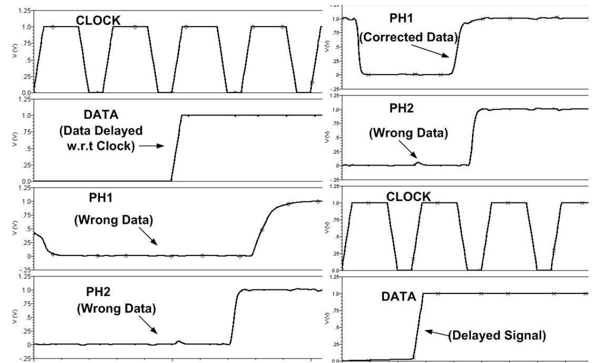

Fig. 10. Response of a BSFF Vs. XSEUFF 2 to signal delays

1) Functional mode operation with tolerance to SEU: The temporal sampling is carried out by reuse of the scan latches LA and LB. $Sync_{LA}$ and $Sync_{LB}$ are used as gating signals for LA and LB respectively. Pulses $Sync_{LA}$ and $Sync_{LB}$ are driven low after the active clock. This allows LA and LB to sample copies of the expected data in PH2. When Clock goes high, the majority voter gets data from PH2, LA and LB thus ensuring that the corrected data is always latched into it. When PH1 goes opaque (Clock = 0), the redundant values stored in LA and LB ensure that an SEU hit on any of them does not affect the value at the FF output. The FF output changes only after the arrival of the next active clock edge. Temporal sampling at the active clock edge combined with the unique design of PH1 ensures complete immunity of the XSEUFF 2 over the WOV.

During simulations, the XSEUFF 2 was subjected to noise pulses and signal delays of varying magnitudes. Its response to a worst case transient pulse is shown in Figure 9. In Figure 9, we compare the behavior of the BSFF [14] and the XSEUFF 2. Latch PH1, in the BSFF receives wrong data from PH2 after the arrival of active clock edge. In the case of XSEUFF 2, time-redundant samples are evaluated by the majority voter and PH1 receives corrected data at the end of the clock cycle. Figure 10 shows the response of the BSFF and the XSEUFF 2 to signal delays. In Figure 10, although PH2 latched in a wrong value, PH1 received the corrected

value from the majority voter circuit. Although the XSEUFF is able to transmit corrected data to PH1 in both cases, its tolerance is limited and depends on several circuit parameters. We define the limits for the width of a noise pulse and magnitude of signal delay that this FF can tolerate. If T_{XPulse} is the maximum tolerable width of a single event transient, then Equation (2) gives the relationship between the various sampling instants, the setup time of the FF t_{setup}, the hold-time t_{hold} and the delays of the multiplexers at the input of latches LB and PH1. For instance $t_{cd(LB),r}$ represents the combinational delay of a rising transition at the input of LB. Similarly $t_{cd(LB),f}$ represents the combinational delay of a falling transition at the input of LB. Equation (3) gives the maximum tolerable delay (Δ_{max}) of the XSEUFF 2.

$$T_{XPulse} = \{T_2 - t_{setup} + max(t_{cd(LB),r}, t_{cd(LB),f})\} - \{T_0 + t_{hold} - min(t_{cd(PH2),r}, t_{cd(PH2),f})\} \quad (2)$$

$$\Delta_{max} = \{T_1 - t_{setup} + max(t_{cd(LA),r}, t_{cd(LA),f})\} - \{T_0 - t_{setup}\} \quad (3)$$

2) Test mode operation: The *ScanMode* signal is analogous to the inverted *TESTBAR* in XSEUFF 1. During Scan operation, LA and LB become part of a large scan-chain. LA gets data from *SI*, which is connected to the output of a previous FF or the tester pin. *SCA* and *SCB* control data transfer between LA and LB during the test mode. *UPDATE* and *CAPTURE* are used to apply the test vector and capture the circuit response respectively. The XSEUFF 2 can be tested for stuck-at-0 and stuck-at-1 faults on all its internal nodes by enabling the scan mode of operation and applying the appropriate vector. A stuck-at fault present on any of the input nodes of the majority voter can be tested by scanning in opposite values in latches LA and LB and disabling the signal generator, so that value latched in PH2 can be used to sensitize this fault.

IV. Limitations

XSEUFF 1 and XSEUFF 2 are proposed with the assumption that there can be only one SEU affecting the FF system in a clock cycle. The schemes of XSEUFF 1 and 2 would fail if the width of the maximum tolerable transient exceeds the designed value which causes incorrect values to be latched in more than one FF in a given cycle. XSEUFF 1 increases the setup time of the FF due to the presampling by *CLK* and requires the data to be steady for at least half a clock period.

V. Results

A. Percentage overhead comparison

Table I gives the transistor counts of different standard cell FF designs, normalized to the transistor count of the BSFF. For each design in this comparison we have only considered transistors local to a cell. All globally routed signals are considered to be inverted at the cell level. The EBSFF [14] and ETSFF [14] designs have 13% and 15% overhead respectively. The EBSHFF [15] has a lower transistor count as compared to the BSFF. The transistor overhead for XSEUFF 1 is 54%. The transistor overhead for the XSEUFF 2 is 37%.

TABLE I
NORMALIZED TRANSISTOR COUNT, CLOCK TO Q AND POWER CONSUMPTION RATIOS

Circuit type	Normalized transistor count	Normalized Clock to Q delay	Normalized power consumption
BSFF [14]	1.00	1.00	1.00
EBSFF [14]	1.13	1.23	2.77
ETSFF [14]	1.15	1.01	2.13
EBSHFF [15]	0.91	1.25	1.72
XSEUFF 1	1.54	1.00	2.70
XSEUFF 2	1.37	1.25	1.95

TABLE II
ISCAS '89 BENCHMARK OVERHEADS

Circuit	XSEUFF 1 Transistor Overhead (%)	XSEUFF 2 Transistor Overhead (%)
s5378	29.3	20.2
s9234	21.8	15.0
s13207	32.1	22.1
s15850	27.3	18.9
s35932	31.3	21.6
s38417	29.9	20.6
s38584	27.0	18.6
Average	28.4	19.6

B. Relative cell level timing

The normalized values of Clock to Q delay for different designs are shown in Table I. For each design, the transistor sizes were maintained for equal rise and fall times. The ETSFF [14] and the XSEUFF 1 have clock to Q delay overhead comparable to the BSFF. The EBSFF [14] and the EBSHFF [15] have a clock to Q delay overhead of about 25%. The XSEUFF 2 has a clock to Q delay overhead of 25 %.

C. Relative cell power consumption

The simulations for power were carried out on *Nanosim* tool using the 70 nm BPTM with supply of 1 V at 1 GHZ clock frequency for five clock cycles. The average power consumption values are compared for the functional mode of operation. The normalized values of power consumption for different designs are shown in Table I.

D. ISCAS '89 benchmark overheads

The transistor overhead for the seven largest ISCAS '89 benchmark circuits is shown in Table II. The comparison is with reference to the BSFF. All FFs were replaced with the XSEUFF 1 and XSEUFF 2 designs for each benchmark circuit comparison. The average transistor overhead is approximately 28% for XSEUFF 1. The XSEUFF 2 has a overhead of approximately 20%

VI. Conclusion

Two designs that provide tolerance to SEUs and transients from the combinational circuit have been proposed in this paper. Transistor, power and timing overheads for the same have been analyzed. With decreasing feature sizes, transistor designs have become more susceptible to soft errors. This increase mandates use of designs that are not just immune to them but also capable of correcting data at run-time, thus ensuring fault-free operation of the entire system. The XSEUFF 1 and 2 offer a convenient trade off between reliability and various overheads.

References

[1] H. H. K. Tang, *'Nuclear physics of cosmic ray interaction with semiconductor materials: Particle-induced soft errors from a physicist's perspective'*,IBM J. Res. Develop., vol 40, no. 1, Jan. 1996, p. 91-108.

[2] J. F. Ziegler, *'Terrestrial Cosmic Rays'*, IBM J. Res. Develop., vol. 40, no. 1, Jan. 1996, p.19-39.

[3] J. F. Ziegler et al., *'IBM experiments in soft fails in computer electronics'*,IBM J. Res.Develop., vol. 40, no. 1, Jan. 1996, p. 3-18.

[4] Arima Y.; Yamashita T.; Komatsu Y.; Fujimoto T.; Ishibashi K.,*'Cosmic-ray immune latch circuit for 90nm technology and beyond'*,.; Solid-State Circuits Conference, 2004. Digest of Technical Papers. ISSCC. 2004 IEEE International 15-19 Feb. 2004 Page(s):492 - 493 Vol.1

[5] R. Wilson, D. Lammers. *'Soft Errors Become Hard Truth for Logic.'*, EE Times, 3 May 2004; `www.eetimes.com/semi/news/showArticle.jhtml?articleID=19400052`.

[6] Robert Baumann. *'The impact of technology scaling on soft error rate performance and limits to the efficacy of error correction.'* In International Electron Devices Meeting (IEDM), pages 329–332, 2002.

[7] Omana, M.; Rossi, D.; Metra, C., *'Novel transient fault hardened static latch'*, in Proc. of the International Test Conference, 2003. ITC 2003., Volume 1, Sept. 30-Oct. 2, 2003 Page(s):886 - 892.

[8] J. V. Neumann. *'Probabilistic logics and the synthesis of reliable organisms from unreliable components'*, In Automata Studies, Ann. of Math. Studies, No. 34, pages 43 98, 1956.

[9] Oliveira R., Jagirdar A., Chakraborty T.J., *'A Soft Error Tolerant, Low Overhead TMR Design for Flip-Flops'*,15th IEEE North Atlantic Test Workshop (NATW), May 2006, Page(s):97-104.

[10] Nicolaidis, M.*'Time redundancy based soft-error tolerance to rescue nanometer technologies'*; VLSI Test Symposium, 1999. Proceedings.

[11] D. Mavis and P. Eaton. *'Soft Error Rate Mitigation Techniques for Modern Microcircuits'*, International Reliability Physics Symposium, 2002.

[12] Cha H. and Patel J.H., *'Latch design for transient pulse tolerance'*, in Proc. ACM International Conf. Computer Design, Oct. 1994, Page(s). 385388.

[13] Hass K.J., Gambles J.W., Walker B. and Zampaglione M., *'Mitigating single event upsets from combinational logic'*, in Proc. 7th NASA Symposium on VLSI Design. 1998, NASA.

[14] S. Mitra, N. Seifert, M. Zhang, Q. Shi and K.S. Kim, *'Robust System Design with Built-In Soft Error Resilience'*, IEEE Computer, Vol. 38, Number 2, pp. 43-52, Feb. 2005.

[15] Goel, A.; Bhunia, S.; Mahmoodi, H.; Roy, K., *'Low-overhead design of soft-error-tolerant scan flip-flops with enhanced-scan capability'*, Proc. of Asia and South Pacific Conference on Design Automation 2006, 24-27 Jan. 2006 Page(s):6 pp.

[16] Alan J. Drake, AJ KleinOsowski, Andrew K. Martin, *'A Self-Correcting Soft Error Tolerant Flop-Flop'*, 12th NASA Symposium on VLSI Design, Coeur d'Alene, Idaho, USA, Oct. 4-5, 2005.

[17] DasGupta S., Walther R. G., Williams T. W., and Eichelberger, E. B., *'An Enhancement to LSSD and some Applications of LSSD in Reliability, Availability and Serviceability'*, Proc. of International Symposium on Fault Tolerant Computing, June 1981, Maine, U.S.A.

[18] Anghel L.and Nicolaidis M., *'Cost reduction and evaluation of a temporary faults detecting technique'*, in Proc. Design Automation and Test Europe, March 2000, Page(s):591-598.

[19] Pradhan D.K.,*'Fault-tolerant computer system design'*, Prentice Hall, first edition, 1996.

[20] Mitra S. and McCluskey E.J., *'Which concurrent error detection scheme to choose?'*, in Proc. International Test Conference, Oct. 2000. Page(s):985 - 994

[21] Krishnamohan S. and Mahapatra N.R., *'A highly-efficient technique for reducing soft errors in static CMOS circuits'*, in Proc. ACM International Conf. Computer Design (ICCD), Oct. 2004. Page(s):126 - 131.

[22] Krishnamohan S. and Mahapatra N.R.,*'Combining error masking and error detection plus recovery to combat soft errors in static CMOS circuits'*,in Proc. International Conference on Dependable Systems and Networks, 2005, July 2005. Page(s):40 - 49.

[23] Baze M.P. and Buchner S.P., *'Attenuation of single event induced pulses in CMOS combinational logic'*, IEEE Transactions on Nuclear Science, vol. 44, Dec 1997 page(s):22172223.

[24] Krishnamohan S. and Mahapatra N.R., *'Analysis and Design of Soft-Error Hardened Latches'*,in Proc. 15th ACM Great Lakes symposium on VLSI, April 2005, Page(s)328-331.

[25] Zhou Q. and Mohanram K., *'Cost-Effective Radiation Hardening Technique for Combinational Logic'*, in Proc. ACM/IEEE International Conf. Computer-Aided Design, Nov. 2004.Page(s):100 - 106.

[26] Mukherjee S., Weaver C., Emer J., Reinhardt S.K., and Austin T., *'A systematic methodology to compute the architectural vulnerability factors for a high-performance microprocessor'*, in International Symposium on Microarchitecture, Dec. 2003.Page(s):29 - 40.

[27] Elakkumanan, P., Prasad, K., Sridhar, R., *'Time redundancy based scan flip-flop reuse to reduce SER of combinational logic'*, International Symposium on Quality Electronic Design, 2006.