

Soft Error Modeling and Protection for Sequential Elements

Hossein Asadi and Mehdi B. Tahoori
Northeastern University
Boston, MA 02115
{gasadi,mtahoori}@ece.neu.edu

Abstract

Sequential elements, flip-flops, latches, and memory cells, are the most vulnerable components to soft errors. Since state-of-the-art designs contain millions of bistables, it is not feasible to protect all system bistables using hardening techniques that impose area, performance, and power overhead. A practical approach is to rank system bistables based on their contribution to the overall system vulnerability and protect the most problematic bistables. This analysis is traditionally performed by fault injection and simulation methods which are intractable for large designs and multi-cycle analysis. In this paper, we present an analytical framework to analyze multi-cycle error propagation behavior and then rank system bistables based on their effects on system-level soft error rate. The number of clock cycles required for an error in a bistable to be propagated to system outputs is used to measure the vulnerability of bistables to soft errors.

1 Introduction

As the aggressive technology scaling continues and exponentially more devices are integrated in the same chip, soft errors become the main reliability concern during lifetime operation of digital systems. Soft errors, also called *Single Event Upsets* (SEU), are intermittent malfunctions of the hardware that are not reproducible [11]. These errors, which can occur more often than hard (permanent) errors [4], are caused from energetic particles, namely neutrons from cosmic rays and alpha particles from packaging material. *Soft Error Rate* (SER) for a device is defined as the error rate due to SEUs. SER depends on both the particle flux and circuit characteristics. Device parameters that influence the error rate include the amount of stored charge, the vulnerable cross-sectional area, and the charge collection efficiency [14].

Soft error susceptibility per transistor remains roughly unchanged with technology scaling [14]: reduction in the amount of the required charge to change the state of a transistor is canceled by its reduced active area susceptible to particle strike. However, in the absence of effective error correction schemes, the error rate will grow in direct proportion to the number of devices on the chip. Thus, while Moore's Law gives an exponential increase in the transistor count, this growth comes at the cost of exponential increases in error rates for unprotected chips [10].

Sequential components, namely flip-flops, latches, register files, and memory cells, are the most vulnerable components to soft errors. Estimated soft error rate of typical designs such as microprocessors, network processors, and network storage controllers shows that sequential elements and unprotected SRAMs contribute to 49% and 40% of the overall soft

error rate, respectively [6]. Moreover, it is observed that the nominal soft error rate of sequential elements increases with technology scaling [3].

Since memory arrays and register files have regular structures, they can be easily protected by popular redundancy techniques such as parity and error correcting codes (ECC). The area and power overhead of these redundancy techniques is about 10-20% [15]. However, protection of system bistables (flip-flops and latches) is a major challenge. Since these elements are scattered all over the physical layout, they cannot be protected by array-based protection methods, such as parity or ECC. Soft error protection techniques for system bistables come with extra area, performance, and power overhead [9, 17, 6]. As state-of-the-art designs contain millions of bistables, it is not feasible to protect all bistables using hardening techniques due to unacceptable overhead for the entire design.

While particle flux uniformly encounters the entire circuit, the probability that an SEU event in a system bistable causes a system failure (i.e. the error appears at system outputs) changes for each bistable drastically. Due to this fact, soft error hardening and protection across the chip should not be uniform. Therefore, a practical approach for soft error protection of sequential elements is to rank system bistables based on their contributions to the overall system vulnerability and only protect the most vulnerable bistables. This bistable ranking is traditionally performed by fault injection and simulation methods. However, since this analysis required multi-cycle simulations, the complexity of simulation-based fault injection methods increases exponentially with the number of clock cycles to be simulated. This makes simulation-based approaches impractical for industrial designs.

In this paper, we present an analytical framework to analyze multi-cycle error propagation behavior in sequential circuits to be used for ranking bistables based on their soft error vulnerability. We exploit our previous work on *combinational error propagation probability* (C-EPP) estimation to analyze bistable-to-bistable¹ error propagation behavior. Using C-EPP values, we develop a mathematical formulation for *sequential error propagation probability* (S-EPP) analysis. For each bistable, we compute the number of clock cycles between an SEU event in that bistable and a system failure. This information is used as the figure of merit for soft error vulnerability and bistable ranking.

The rest of this paper is organized as follows. In Sec. 2, the related work on soft error estimation and protection is presented. In Sec. 3, the analytical SER estimation in sequential circuits is described. In Sec. 4, the experimental results are presented. Finally, Sec. 5 concludes the paper.

2 Related Work

Previous work on SER estimation can be classified into three categories, namely *circuit level* [5, 12], *gate level* [7, 8, 11, 13], and *architectural level* [10, 16]. Circuit level SER estimation methods compute the probability of an SEU producing an error (glitch) on the output of the gate hit by a particle. These techniques use SPICE simulations to obtain these probabilities.

Gate-level SER estimation techniques try to compute the SER rate of a circuit node by computing the SEU occurrence rate, the *error propagation probability* (EPP), and the error latching probability. The work presented in [11] introduces logic and timing derating factors and describes how these factors reduce the susceptibility of combinational logic to soft errors. To compute the error susceptibility of a node to SEUs, it is required to compute

¹In this paper, the terms “latch”, “flip-flop”, and “bistable” are used interchangeably.

the probability that the node is functionally sensitized by the input vectors to propagate the erroneous value from the error site to system outputs [8]. Traditionally, several random vectors are applied to the circuit inputs to determine the propagation probability of an erroneous value from the struck node to the outputs [5, 7, 11, 12, 13, 14]. It is shown in [5] that the size of simulated vectors should be around 1% of all possible input combinations to achieve an acceptable (95%) accuracy. Therefore, simulation time increases exponentially with the size of the circuit.

Shivakumar et. al. explored the effect of micro-architectural trends on the rate of soft errors in CMOS memory and logic circuits [14]. Their analysis illustrates the effect of technology trends on electrical and latching-window masking, which provides combinational logic with a form of natural protection against soft errors. Finally, in [10, 16], a modern-processor's error rate is computed at the architectural level. The notion of a structure's *Architectural Vulnerability Factor* (AVF) was introduced in [10], which expresses the probability that a fault in that particular structure will result in an error.

A flip-flop hardening technique against both dynamic and static SEUs has been presented in [9] at the expense of 30% area, power, and delay overhead. Recently, a built-in soft error resilience technique for protecting system bistables has been presented in [6]. In this technique, scan cells with an additional level of latches which are originally used for debug purposes, are reused for error checking.

In our prior work, we have presented an analytical *combinational error propagation probability* (C-EPP) computation approach to estimate SER in combinational circuits [1, 2]. This approach uses the *signal probabilities* (SP) of all nodes and computes EPPs based on the topological structure of the circuit by traversing the paths from struck node to reachable outputs. The time complexity of this approach is linear to the size of the circuit, since each gate along the path is examined only once in the topological order. Since SP is widely used for power consumption analysis, by reusing calculated SP values from previous design steps, the complexity of SER estimation approach will not increase. Experiments show that the analytical C-EPP estimation technique is 4-5 order of magnitude faster than simulation-based methods while more than 94% accurate.

3 SER Estimation in Sequential Circuits

3.1 Sequential Error Propagation

A typical synchronous circuit consists of combinational logic and flip-flops. Fig. 1 shows the conventional representation of a sequential circuit. Primary Inputs (PIs) and the outputs of flip-flops (FFs) are inputs of combinational logic. Also, Primary Outputs (POs) and the inputs of the flip-flops are outputs of the combinational logic.

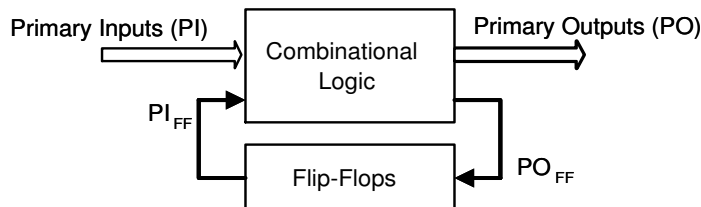


Figure 1. A typical block diagram of a synchronous sequential circuit

In a sequential circuit, error propagation from an error site (for example, a bit-flip in a flip-flop) to primary outputs can happen several clock cycles after the SEU event. The error can be first propagated to other flip-flops in some clock cycles and finally appears at the primary outputs. The average number of clock cycles it takes before the error appears at the primary outputs depends on the particular flip-flop the error originated from. A flip-flop i is considered more vulnerable to soft errors than flip-flop j if an error originated in i takes less time, in average, to appear at the outputs than an error originated in j . The sequential error propagation probability (S-EPP) depends on combinational error propagation probabilities of reachable flip-flops and primary outputs from an erroneous flip-flop, as well as the sequential structure of the design.

In this section, we analyze how an erroneous value in a flip-flop can cause a system failure in several clock cycles after the particle strike. We exploit our C-EPP estimation method as a basis for sequential EPP analysis [1, 2]. Given a particular error site (such as primary input, flip-flop output, or any internal node) and an observation point (such as primary output or flip-flop input), we are able to accurately estimate the combinational error propagation probability from the error site to the observation point.

For S-EPP analysis, we need to capture the sequential error propagation behavior of the circuit. We define an $n \times n$ *S-EPP matrix* \mathbf{M} where M_{ij} is the probability of an error in flip-flop FF_j given flip-flop FF_i is erroneous. The elements (m_{ij}) of this matrix are obtained using combinational-EPP estimation approach presented in [2] by setting flip-flop FF_i as the error site and flip-flop FF_j as the observation point.

Sequential error propagation probability (S-EPP) matrix \mathbf{M} :

$$M_{ij} = P(\text{error appear in } FF_j | FF_i \text{ is erroneous})$$

$$\mathbf{M} = \begin{pmatrix} P(FF_1|FF_1) & P(FF_2|FF_1) & \dots & P(FF_n|FF_1) \\ P(FF_1|FF_2) & P(FF_2|FF_2) & \dots & P(FF_n|FF_2) \\ \vdots & \vdots & \ddots & \vdots \\ P(FF_1|FF_n) & P(FF_2|FF_n) & \dots & P(FF_n|FF_n) \end{pmatrix}$$

Also, a *system failure vector* \mathbf{S} is defined, where S_i is the probability of system failure (SF) given the content of FF_i is erroneous (i.e., $S_i = P(SF|FF_i)$). In other words, it gives the probability of a system failure in the same clock cycle that an SEU event occurs. This vector is obtained by computing C-EPPs between each pair of system bistable and primary output.

System failure probability vector \mathbf{S} : $S_i = P(\text{system failure} | FF_i \text{ is erroneous})$

$$\mathbf{S} = \begin{pmatrix} P(SF|FF_1) \\ P(SF|FF_2) \\ \vdots \\ P(SF|FF_n) \end{pmatrix}$$

We use S-EPP matrix and system failure probability vector for our multi-cycle sequential error propagation analysis. The following theorem is used as the basis of this analysis.

Theorem 1. The probability of a system failure at c clock cycles after the SEU event in FF_i (i.e. given FF_i is erroneous), $P^c(SF|FF_i)$, is calculated as follows:

$$P(SF \text{ at cycle } c | FF_i \text{ erroneous}) = P^c(SF|FF_i) = i^{th} \text{ element of } M^{c-1}S \quad (1)$$

Proof. Assume that the content of FF_i is erroneous. The probability of a system failure at the first clock equals to the i^{th} row of S , i.e. $S_i = P(SF|FF_i)$, based on the definition of S (the basis of induction). Error can be propagated to the output two clock cycles after the SEU event if the error is propagated from FF_i to another flip-flop FF_j in the first clock cycle, and then propagated from FF_j to the output in the second clock cycle. Since FF_j can be any flip-flop in the circuit and given the independent error propagation probabilities to each flip-flop FF_j , we have to sum the probabilities for all FF_j . The following expressions show the probability of a system failure at the second clock ($c = 2$) after the SEU event:

$$\begin{aligned} P^2(SF|FF_i) &= P(FF_1|FF_i)P(SF|FF_1) + \dots + P(FF_n|FF_i)P(SF|FF_n) \\ &= M_{i1}S_1 + M_{i2}S_2 + \dots + M_{in}S_n = \sum_{j=1}^n M_{ij}S_j \\ &= [M_{i1} \ M_{i2} \ \dots \ M_{in}] \cdot S = \text{Row}_i(M \cdot S) \end{aligned} \quad (2)$$

Similarly, the probability of system failure at the third clock ($c = 3$) after bit-flip is calculated as follows:

$$\begin{aligned} P^3(SF|FF_i) &= S(1) \sum_{j=1}^n P(FF_1|FF_j)P(FF_j|FF_i) \\ &\quad + S(2) \sum_{j=1}^n P(FF_2|FF_j)P(FF_j|FF_i) \\ &\quad + \dots + S(n) \sum_{j=1}^n P(FF_n|FF_j)P(FF_j|FF_i) \\ &= \sum_{k=1}^n S(k) \sum_{j=1}^n P(FF_k|FF_j)P(FF_j|FF_i) \\ P^3(SF|FF_i) &= \text{Row}_i(M \cdot M \cdot S) = \text{Row}_i(M^2S) \end{aligned} \quad (3)$$

Based on the induction, it can be shown that the probability of system failure at c clock cycles after a bit-flip event in FF_i is computed as $P^c(SF|FF_i) = \text{Row}_i(M^{c-1}S)$. Therefore, the proof is complete Q.E.D.

After computation of system failure probabilities for any particular clock cycle c after the SEU event, the system failure probability for this period, i.e. from the clock cycle at which the bit-flip occurs to c clock cycles after that, is computed as follows:

$$\begin{aligned} P_1^c(SF|FF_i) &= P^1(SF|FF_i) + (1 - P^1(SF|FF_i)) \times P^2(SF|FF_i) \\ &\quad + (1 - P^1(SF|FF_i)) \times (1 - P^2(SF|FF_i)) \times P^3(SF|FF_i) + \dots \\ P_1^c(SF|FF_i) &= \sum_{n=1}^c \left(P^n(SF|FF_i) \prod_{m=1}^{n-1} (1 - P^m(SF|FF_i)) \right) \end{aligned} \quad (4)$$

Note that the complexity of the simulation-based method increases exponentially with c , making simulation-based analysis intractable for large sequential circuits. However, the presented approach requires only a matrix multiplication to compute the system failure rate in next clock cycles, and hence, its time complexity is linear to c .

It has to be mentioned that in the above theorem, independent probabilities of error propagations between each pair of flip-flops have been considered. This results in over-estimation of S-EPPs calculated based on this approach if C-EPPs are not independently computed. However, the experiments presented in the next section show that this approach is sufficiently accurate. Moreover, this accuracy of this method is adequate to rank system bistables based on their soft error vulnerability.

3.2 Mean Time To Manifest Error

As a metric to compute the vulnerability of individual flip-flops to soft errors, we use the concept of *mean time to manifest* error (MTTM). MTTM for a flip-flop is defined as the average time (the number of clock cycles) from an SEU event in that flip-flop to a system failure (error appearing at primary outputs) due to that bit-flip. Flip-flops with smaller MTTM are more vulnerable to soft errors. Therefore, we use MTTM as a metric to rank system bistables.

MTTM for each flip-flop can be computed based on Equation 4. MTTM for each flip-flop FF_i is computed as the smallest number of clock cycles c such that $P_1^c(SF|FF_i) = 1$ but $P_1^{c-1}(SF|FF_i) < 1$. In other words, MTTM is equal to the minimum number of clock cycles that is required for a system failure with probability of one.

4 Experimental Results

We have used the approach presented in [1, 2] to compute C-EPPs for ISCAS'89 sequential circuits. Each row of S-EPP matrix can be computed in just one traversal of the combinational part of the circuit starting from the corresponding flip-flop. Therefore in n passes, where n equals to the number of system bistables, the entire matrix can be computed. Table 1 shows S-EPPs for five representative flip-flops of some ISCAS'89 circuits in twenty clock cycles after the SEU event. As can be seen in this table, the probability of system failure increases in the subsequent clock cycles after the SEU event.

Figure 2 shows the MTTM distribution for some ISCAS'89 benchmark circuits. These results are separated for small and large circuits. In smaller circuits, which have at most 21 flip-flops, majority of flip-flops have very low MTTM due to small depth of the combinational logic. However in larger circuits, which have up to 211 flip-flops, a small subset of flip-flops have very low MTTM and hence, very vulnerable to SEUs. This figure shows that MTTM is an effective metric to distinguish flip-flops based on their soft error vulnerability. In other words, the range and distribution of MTTM values for different flip-flops in a circuit is quite wide.

Figure 3 shows the average MTTM values (the average over all flip-flops in a circuit) for these circuits. As can be seen in this figure, the average MTTM is very application-specific and does not necessarily scale with the size of the circuit.

The accuracy of the analytical C-EPP estimation method presented in [2], which is the basis of the flip-flop ranking technique presented in this paper, is more than 94% compared to simulation-based method while 4-5 orders of magnitude faster. For smaller circuits in which simulation-based multi-cycle analysis is feasible, we have computed simulation-based MTTM values and compared them with the values obtained from our analytical method.

circuit/ number of FFs	1st clock cycle	2nd clock cycle	3rd clock cycle	4th clock cycle	10th clock cycle	20th clock cycle
s1423 /74 FFs	0	0	0	0.0001	0.0039	0.0466
	0	0	0	0.0001		0.0032
	0	0	0.0010	0.0042	0.1428	0.8673
	0	0	0.0019	0.0079	0.2205	0.9400
	0	0.0467	0.1428	0.2827	0.9933	1
s5378 /179 FFs	0.1731	0.3163	0.4599	0.6138	1	1
	0.2953	0.5035	0.6503	0.7538	0.9709	1
	0.2953	0.5035	0.6502	0.7537	0.9708	1
	0.5774	0.8572	0.969249	0.998926	1	1
	0	0	0	0.0004	0.0163	0.2800
s9234 /211 FFs	0	0.02722	0.0861	0.1780	0.9284	1
	0	0.0135	0.0683	0.1903	0.9901	1
	0	0	0	0	0	0.0011
	0.0542	0.1415	0.2609	0.4169	1	1
	0	0.0014	0.0048	0.0196	0.9072	1

Table 1. System failure probability vectors for five representative flip-flops of some ISCAS'89 benchmark circuits

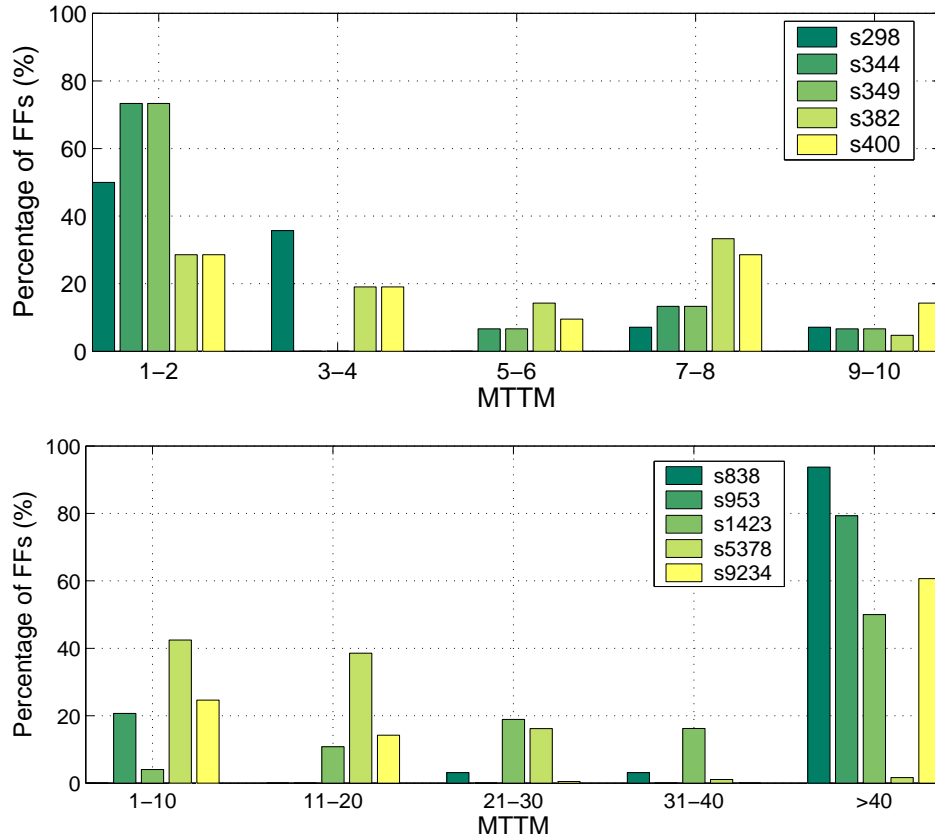


Figure 2. Percentage of flip-flops vs. MTTM for ISCAS'89 circuits

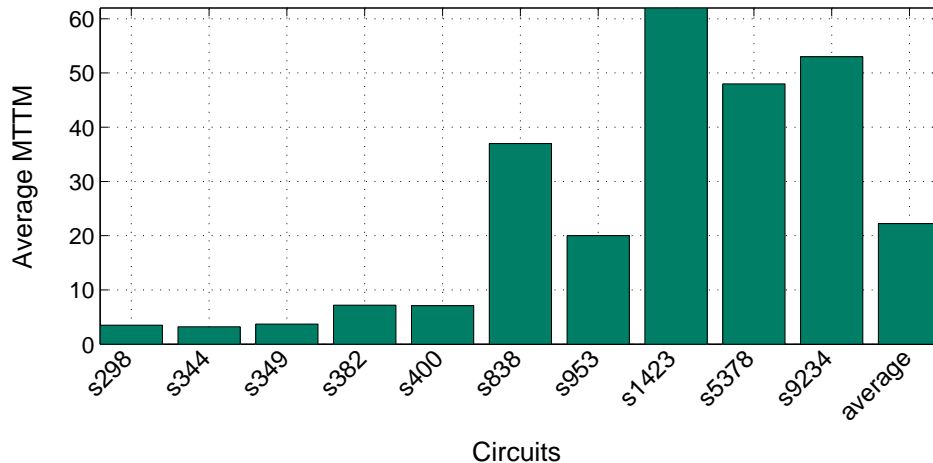


Figure 3. Average mean time to manifest error (MTTM) for ISCAS'89 circuits

This experiment shows that the difference between these two methods is around 12%. However, the flip-flop ranking obtained from both methods are exactly the same. In other words, while the accuracy of the MTTM values achieved by our analytical method is within 12% of the simulation-based method, the flip-flop ranking is 100% accurate. Note that the analytical method is 5-6 orders of magnitude faster than multi-cycle simulation methods.

5 Conclusions

Soft errors due to single event upsets are the main reliability threat for digital systems. In particular, vulnerability of digital systems grows in direct proportion to the Moore's law. In this paper, we have presented an analytical approach for soft error rate estimation of sequential elements, latch and flip-flops, in digital designs.

We have developed a mathematical framework for the estimation of system failure probability in multiple cycles after the SEU event. By computing combinational error propagation probabilities between bistables we have devised a matrix formulation to represent the probability of error in each bistable or primary output at any given clock cycle. Based on this formulation, we have computed mean time to manifest an error (MTTM) for each flip-flop. Unlike simulation-based methods which have exponential time complexity, the complexity of the presented approach is linear to the size of the circuit.

Using this analysis, we have been able to rank system bistables based on their soft error vulnerabilities. This ranking can be used for selective protection of system bistables against soft errors in order to maximize soft error suppression with bounded overhead.

References

- [1] G. Asadi, M. B. Tahoori, "An Accurate SER Estimation Method Based on Propagation Probability", Proc. Design and Test Conf. in Europe (DATE), 2005.
- [2] G. Asadi, M. B. Tahoori, "An Analytical Approach for Soft Error Rate Estimation In Digital Circuits", Proc. IEEE Int'l Symposium on Circuits and Systems (ISCAS), 2005.

- [3] R. Baumann, "Soft Errors in Commercial Semiconductor Technology: overview and scaling trends", IEEE 2002 Reliability Physics Tutorial Notes, Reliability Fundamentals, pp. 121.01.1-121.01.14, April 2002.
- [4] J. Karlsson, P. Ledan, P. Dahlgren, and R. Johansson, "Using Heavy- Ion Radiation to Validate Fault Handling Mechanisms", IEEE Micro, 14(1), pp. 8-23, February 1994.
- [5] A. Maheshwari, I. Koren, and W. Burleson, "Techniques for Transient Fault Sensitivity Analysis and Reduction in VLSI Circuits," Proc. IEEE Int'l Symp. on Defect and Fault-tolerance, pp. 597-604, 2003.
- [6] S. Mitra, N. Seifert, M. Zhang, Q. Shi and K. Kim, "Robust System Design with Built-In Soft-Error Resilience", IEEE Computer, vol. 38, pp. 43-52, Feb. 2005.
- [7] K. Mohanram and N. A. Touba, "Cost-Effective Approach for Reducing Soft Error Failure Rate in Logic Circuits", Proc. Int'l Test Conf. (ITC), pp. 893-901, 2003.
- [8] K. Mohanram and N. A. Touba, "Partial Error Masking to Reduce Soft Error Rate in Logic Circuits", Proc. IEEE Int'l Symp. on Defect and Fault Tolerance in VLSI Systems, pp. 433-440, 2003.
- [9] T. Monnier, F. M. Roche, G. Cathebras, "Flip-flop Hardening for Space Applications", Proc. IEEE Int'l Workshop on Memory Technology, Design and Testing, pp. 104-107, 1998.
- [10] S. S. Mukherjee, C. Weaver, J. Emer, S. K. Reinhardt, and T. Austin, "A Systematic Methodology to Compute the Architectural Vulnerability Factors for a High-Performance Microprocessor", Proc. IEEE/ACM Int'l Symp. on Micro-architecture (MICRO-36), pp. 29-40, 2003.
- [11] H. T. Nguyen and Y. Yagil, "A Systematic Approach to SER Estimation and Solutions", Proc. Int'l. Reliability Physical Symp., pp. 60-70, 2003.
- [12] M. Omana, G. Papasso, D. Rossi, and C. Metra, "A Model for Transient Fault Propagation in Combinatorial Logic", Proc. IEEE Int'l On-Line Testing Symp., 2003.
- [13] M. Sonza Reorda and M. Violante, "Accurate and Efficient Analysis of Single Event Transients in VLSI Circuits", Proc. IEEE Int'l On-Line Testing Symp., 2003.
- [14] P. Shivakumar, M. Kistler, S.W. Keckler, D. Burger, and L. Alvisi, "Modeling the Effect of Technology Trends on the Soft Error Rate of Combinatorial Logic", Proc. Int'l Conf. on Dependable Systems and Networks (DSN), pp. 389-398, 2002.
- [15] K. Thaller and A. Steininger, "A Transparent Online Memory Test for Simultaneous Detection of Functional Faults and Soft Errors in Memories", IEEE Trans. on Reliability, Vol. 52 , Issue 4, pp. 413-422 , Dec. 2003.
- [16] N. J. Wang, J. Quek, T. M. Rafacz, and S. J. patel, "Characterizing the Effects of Transient Faults on a High-Performance Processor Pipeline", Proc. Int'l Conf. on Dependable Systems and Networks (DSN'04), pp. 61-70, 2004.
- [17] W. Wang, H. Gong, "Edge Triggered Pulse Latch Design With Delayed Latching Edge for Radiation Hardened Application", IEEE Trans. On Nuclear Science, Vol. 51, No. 6, pp. 3626-3630, 2004.