Low-Power Soft Error Hardened Latch

Hossein Karimiyan Alidash[1] and Vojin G. Oklobdzija[2]

[1] ECE Department, Isfahan University of Technology, Isfahan 74155, Iran
[2] University of Texas at Dallas, Richardson, TX 75080, USA
Hkarimiyan@ec.iut.ac.ir, Vojin@utdallas.edu

Abstract. This paper presents a low-power soft error-hardened latch suitable for reliable circuit operation. The proposed circuit uses redundant feedback loop to protect latch against soft error on the internal nodes, and transmission gate and Schmitt-trigger circuit to filter out transient resulting from particle hit on combinational logic. The proposed circuit has low power consumption with negative setup time and low timing overhead. The HSPICE post-layout simulation in 90nm CMOS technology reveals that circuit is able to recover from almost any single particle strike on internal nodes and tolerates input SETs up to 130ps of duration.

Keywords: soft-error, static latch, hardened latch, reliability.

1 Introduction

Continuous advances of microelectronic technology are leading to an aggressive shrinkage of device dimensions. The consequent node capacitance reduction along with the power supply voltage reduction [20], the amount of stored charge on each circuit node is becoming smaller. That smaller stored charge and higher operating frequency now make circuits more vulnerable to soft errors caused by charge deposited directly by alpha particle or indirectly by cosmic ray neutrons [1]. As a result soft errors which were traditionally regarded as reliability issue for space applications are going to be a terrestrial issue.

A study on radiation flux noted that particles with lower energy occur far more frequently than particles with higher energy [1]. So as CMOS device sizes decrease, it becomes more possible to be affected by lower energy particles, potentially leading to higher soft error rate.

Although package and process engineering may reduce alpha particle problem, there is no physical obstacle to cosmic neutrons. Thus improved circuit designs to reduce soft error vulnerability are becoming mainstream approach for high reliability systems.

Latches and flip-flops are also becoming more susceptible to particle strike on external logic and their own internal nodes, hence more hardening and soft error protection is required. Most common protective methods at circuit level are based on redundancy, namely temporal and spatial redundancy. Those methods, as well as scan based soft error resilient latch [16] and even transient detection of RAZOR I & II

J. Monteiro and R. van Leuken (Eds.): PATMOS 2009, LNCS 5953, pp. 256–265, 2010.

flip-flop [14] cannot tolerate soft error due to particle hit in combinational logic. The temporal redundancy based latches as well as those based on Schmitt-trigger [11] and transmission gate [13] filtering effects has extended setup time problem. The idea in this work is to reduce single event upset (SEU) and single event transient (SET) susceptibility with less timing overhead.

The rest of this paper is organized as follows. In section 2, the previous works will be reviewed quickly. Section 3 proposes the SER-tolerant latch. Section 4 gives simulation results and section 5 concludes the paper.

2 Latch-Hardening Methods

In this section, starting with some basic definitions recent publication and latch hardening methods will be reviewed. An energetic particle may hit logic gates, storage elements, or clock network of a digital circuit. When it hits the logic gates, it causes a glitch in the output voltage of the gate which is called single event transient (SET) [1][2]. When a particle directly hits an internal node of a latch or flip-flop, it may change stored data and cause single event upset (SEU). Also SET may generate and propagate through the combinational part and captured by storage element which turns into an SEU [3]. If a particle hits a control signal, such as the clock signal, it generates a false control signal which can results in an unwanted data latch or timing violation [4]. The rate at which soft errors occur is referred to as soft error rate (SER).

Traditionally memories are protected by Error Correction Codes (ECC). Storage elements, i.e. latches and flip-flops, have also received more attention to make them more robust to soft errors [11]. However, recent studies indicate that logic also will be more vulnerable to soft error [2][5]. Gate sizing to mitigate SET effect at logic level [15] as well as guard ring effect [18], and negative feedback effect are studied extensively [17]. The objectives of those studies are to design and size gates in a way that they attenuate transient voltages caused by particle strike.

During the process of transient voltage propagation in logic circuits, a SET could be masked by logical, electrical, or latching-window masking [5][20]. These three mechanisms prevent some SETs from being latched and alleviate the soft error rate in digital systems. However, due to continuous scaling trends, increased frequency and wide spectrum of particle energy, the probability that transient voltage reaches storage elements in capturing window and getting latched is increasing, and so does the soft error rate. Thus circuit level hardening techniques are required.

The simplest form of hardening technique for latches and flip-flops is to increase stored node charge by adding resistance or capacitance [8] which degrade circuit speed and increase power consumption.

While error-correcting codes and latch-hardening designs can be used to reduce the effect of SEUs, complete protection against SETs is much more difficult and involves either spatial or temporal redundancy. The spatial redundancy uses multiple copies of a given circuit with majority voting to determine correct outputs. One effective way to overcome SEU effects is to triplicate each latch of the system and use Triple Module Redundancy (TMR-latch). Although TMR-latches are highly reliable and widely used [6], this technique suffers from high area and energy consumption overhead.

The temporal redundancy technique uses delayed sample of data, and is more acceptable for conventional designs due to its lower power consumption. This technique can eliminate all SET pulses which are smaller than a certain threshold value. The major drawback of this method is its delay penalty. Moreover it cannot guarantee fault-free operation.

The dual interlock storage element (DICE) is another SER-hardened topology based on spatial redundancy. It has been introduced [9] and applied to a standard 6T memory cell [10] and used in pulsed latch [10][19]. The hardened feedback of DICE circuit has the potential to improve SEU robustness of latch circuits without degrading its speed too much; however it comes with area and power penalty [19].

Redundant feedback loop is another soft error hardening method used in basic latch. According to analyses in [3], soft error of the internal nodes in feedback loop, i.e. node B and C in Fig. 1, has the major contribution to the total SER. If a particle strike causes an unexpected voltage drop or rise inside the loop during the holding mode, the stored value in the latch may change depending on the amount of deposited charge. Our study also shows that node B is much more sensitive than node C.

The SIN-LC latch [3] is proposed to solve the SER issue of basic latch; Fig. 2(a) shows the detailed schematic of this latch. It consists of duplicating feedback loop and C-element making the latch output change only when both duplicated nodes have the same logic value. Besides to sizing issue, the SIN-LC suffers from contention

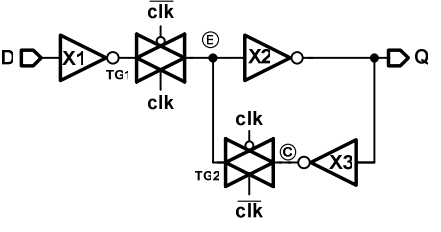

Fig. 1. Positive Level Sensitive Latch

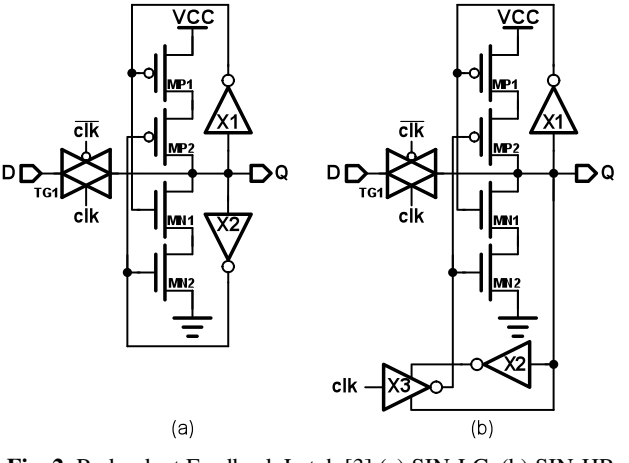

Fig. 2. Redundant Feedback Latch [3] (a) SIN-LC, (b) SIN-HR

drawback that occurs when the latch is in the transparent mode. The SIN-HR [3] of Fig. 2(b) is proposed to solve those problems, but the main problem still exists. The FERST [7] is another latch which is also based on duplicated feedback loop idea and tries to solve contention problem, but it comes up with large area, timing and power overhead.

Those methods, as well as scan based SER resilient latch [16] and even transient detection of RAZOR II flip-flop [14] cannot tolerate soft error due to capturing SET which resulted from particle hit in combinational logic. The transient filtering effect of Schmitt-trigger is studied and a latch based on its property is proposed [11]. The transmission gate [13], negative feedback [17], and circuit layout effect [18] on soft error are also reported separately.

3 Proposed Soft Error Hardened Latch

This section proposes a new soft error hardened latch which is based on temporal redundancy, dual feedback loop and incorporates extra glitch filtering. The detailed schematic of proposed latch is shown in Fig. 3. It employs C-element and controlled feedback loops to achieve low-power and filter out particle strike effect. Data redundancy and glitch filtering is used to reduce SET coming from combinational logic. Filtering is done in two steps. First the transmission gate based filter with hysteresis effect attenuates SETs and also adds delay to create temporal redundancy. At the second step, a C-element is used to filter out more SETs and reduce SEUs.

The proposed circuit is a pulsed latch and operates as follows in transparent and hold modes. A general purpose pulse generator circuit is used to generate tiny pulses on each clock edges. During the small period of tiny pulses the latch is transparent and feedback loops composed by X3-TG3 and X4-TG4 pairs are open. The data path is divided into two paths, normal and filtered. The pass transistors in the data paths, i.e. TG1 and TG2, are conducting and works as a low-pass filter [13]. The hysteresis

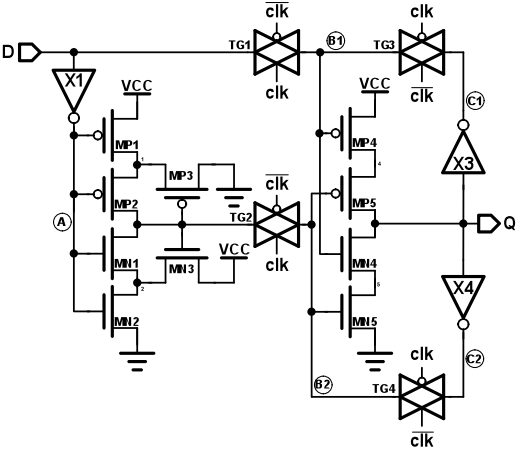

Fig. 3. The Soft Error Hardened Latch

effect is achieved using MP3 and MN3. During transparent time input data and its delayed/filtered version are applied to the C-element composed by MP4, MP5, MN4, and MN5. If both versions are the same and it is not a glitch, the output will change accordingly, unless the previous value is preserved. In other words, the data will be latched on the condition that it is not a single transient.

After tiny transparent pulse, the latch switches to hold state. In this period data paths are blocked and feedback loops are closed. The sensitive nodes in the proposed circuit are B1, C1, B2, and C2. If particle hit one of those nodes, it generates voltage spikes but dual feedback connection and C-element will remove its effect.

The temporal redundancy is implemented by adding a delay to the data path. The required delay value in the data path should be longer than the duration of the possible longest SET in order to effectively filter it out. The timing diagram in Fig. 4(a) shows the positive setup time of an ordinary clocked storage element. Applying temporal redundancy increases setup time (Fig. 4(b)) resulting in performance penalty. As a result, window of vulnerability (WOV) [3] to particle hit is also increases. The proposed topology uses the resulted negative setup time [21] of pulsed latches to mitigate setup time penalty. Applying the temporal redundancy to the pulsed latch (Fig. 4(c)) adds the positive delay value to the negative setup time, thus the setup time of hardened pulsed latch in Fig. 4(d) is still smaller than ordinary latch.

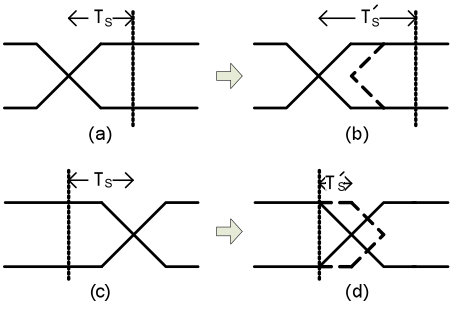

Fig. 4. Setup time (a) and (b) ordinary clocking, (c) and (d) pulsed clocking, (b) and (d) after applying hardening methods

5 Simulation Result

The proposed latch has been implemented using 90nm CMOS technology with 1.2V power supply voltage. In order to have realistic waveforms and rise/fall times the simulation setup, shown in Fig. 5**,** is used for all cases [21]. Due to inverted output of proposed circuit, inverter is added to the inputs whenever that it was needed.

Regardless of the type of particle (alpha particle or neutron), when it hits the drain of the MOSFET and loses energy, electron-hole pairs with a very high carrier concentration are generated. The resulting charges can be rapidly collected by the electric field to create a large transient current at that node [1]. The whole process of charge deposit and distribution is complicated, but for sake of simplicity, it is modeled by exponential current source with varying current levels and time constants to emulate particles with different energy level [3][7].

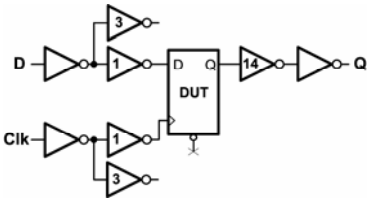

Fig. 5. Simulation Setup

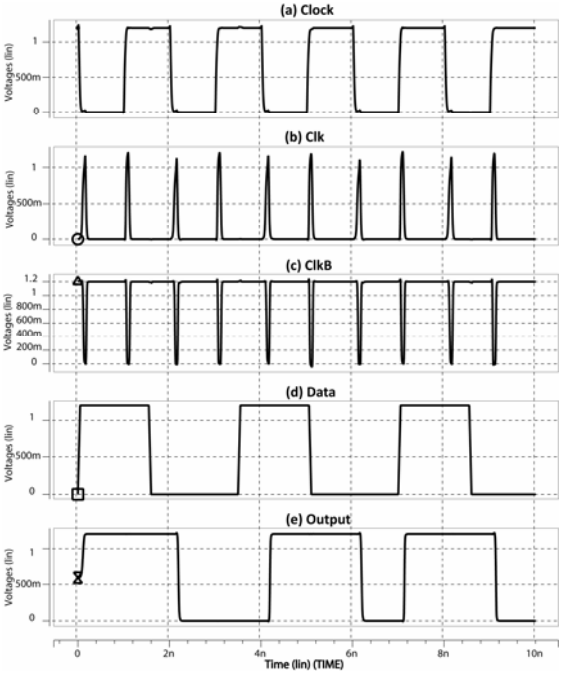

Fig. 6. Latch normal operation (a) System Clock, tiny pulses (b) "CLK" and (c) "CLKB", (d) Data Input "D", and (d) Output "Q"

The performance of the proposed latch has been verified in the normal and particle affected mode. The particle affected mode is also divided in two modes. The first is SEU verification on internal nodes, which verifies robustness of the circuit against particles which hit on internal sensitive nodes. The second verifies filtering effect and circuit robustness against the particle hit on combinational part and the resulted SET, which reaches the latch on the sampling window.

Fig. 6 shows circuit's normal operation and Fig. 7 indicates its basic data to output delay (t_{DQ}) and setup time variation. This figure also gives the setup time and delay for ordinary latch of Fig. 1 in inverted mode, and proposed circuit in level sensitive mode for comparison. The flat region on the data-to-output delay and negative setup time of proposed latch reveals that if data arrive close to clock edge or even 40ps after clock edge, the latch is still able to capture it correctly [12]. While same circuit in

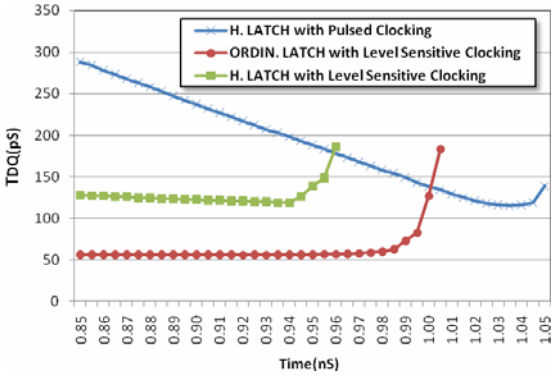

Fig. 7. Data to output delay variation and setup time of hardened latch with pulsed clocking, ordinary latch and hardened latch with level sensitive clocking

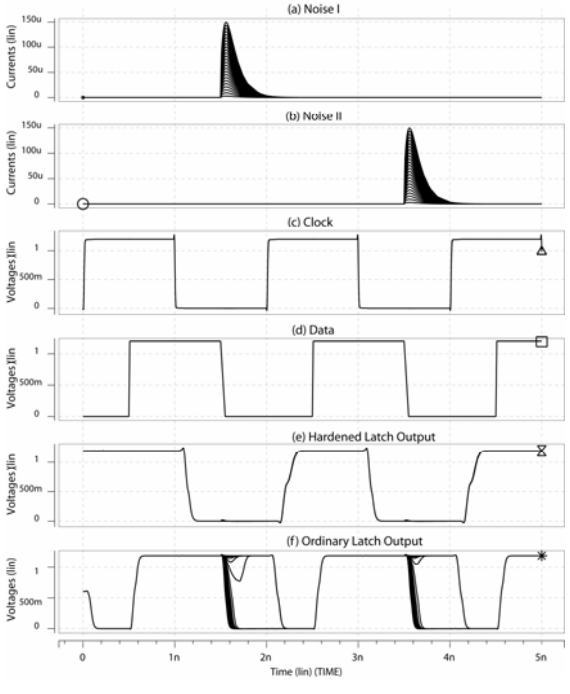

Fig. 8. Latch operation under particle affected mode, (a) Injected charge at 1.5ns, (b) Injected charge at 3.5ns, (c) Clock, (d) Data, and (e) Hardened latch output is still stable after particle hit on node B1 and C1 in Fig. 3, and (f) Ordinary latch output of Fig. 1 is unstable after 12.6fC and 19.8fC charge injection to nodes B and C, respectively.

level sensitive mode and with almost same output delay comes with large positive setup time. The extra negative setup time could be invested in input path by adding extra delay, to filter out more SETs.

The single particle hit on sensitive nodes is modeled by current injection to those nodes. Different current level is used to model particles with different energy levels. Charges are injected at 1.5ns and 2.5ns, to the nodes B1 and C1 in Fig. 3, and nodes B and C in Fig. 1. Fig. 8 shows the results and indicates that the ordinary latch output is unstable after 12.6fC and 19.8fC charge injection to nodes B and C, respectively. While the dual feedback structure of proposed circuit is able to recover from almost any single particle hit and resulting charge deposit.

The particle hit on combinational logic deposits charge which causes voltage glitch at gate's output. After passing levels of logics, those glitches convert to voltage pulses which may reaches to the latch "on-time" and gets captured. This phenomenon is modeled by voltage pulses with different width on the data line to represent various

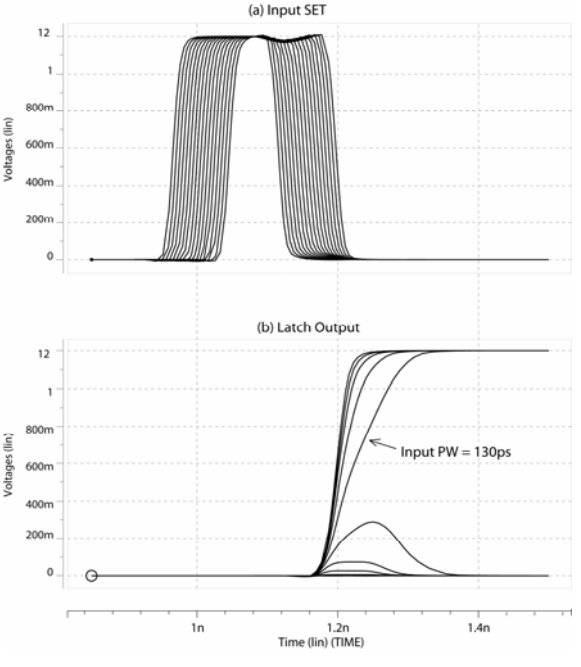

Fig. 9. SET filtering, (a) input, (b) latch output

Table 1. Different latches' setup time, delay, power consumption and power-delay-product comparison (* - TMR Specification is estimated)

Latch Type	*Setup Time*	*Delay*	*Power*	*PDP*
Basic latch (Fig. 1)	20ps	55ps	8.0µW	0.44fJ
Fig. 3 in level sensitive	60ps	120ps	23.3µW	2.8fJ
Fig. 3 in pulsed mode	-35ps	120ps	21.2µW	2.5fJ
TMR Latch*	60ps	120ps	24 µW	2.88fJ

particle energy levels. Fig. 9 shows the results and indicates that the proposed latch is able to filter out SETs with up to 130ps pulse width. Table 1 compare the specifications of basic latch and proposed circuit with TMR latch as a representative of hardened latches.

5 Conclusion

In this work, an SER-Hardened pulsed latch is proposed. The latch is able to tolerate particle strike on internal nodes as well as SET occurring in combinational logic. The HSPICE simulation on 90nm CMOS technology is conducted to precisely evaluate the proposed circuit in normal and under particle strike mode. The circuit operates as edge triggered flip-flop which is resilient to SET from combinational logic as well as SEU resulting from internal nodes. Extra reliability enhancement is achievable by careful layout design. In comparison with the TMR-Latch as a representative for SER-hardened designs, proposed circuit has less power consumption and lower timing overhead, which make it suitable for low-power reliable applications.

Acknowledgment

This work was performed at the Univ. of Texas at Dallas and supported in part by the SRC, under Grant No. 2008-HJ-1799. The authors would like to appreciate Dr. Mustafa AKTAN and Dursun BARAN for their review and valuable comments.

References

1. Baumann, R.: Soft Errors in Advanced Computer Systems. IEEE Design and Test of Computers 22(3), 258–266 (2005)
2. Mitra, S., Zhang, M., Mak, T.M., Seifert, N., Zia, V., Kim, K.S.: Logic soft errors: a major barrier to robust platform design. In: Proc. Int. Test Conference, November 2005, pp. 687–696 (2005)
3. Omana, M., Rossi, D., Metra, C.: Latch susceptibility to transient faults and new hardening approach. IEEE Trans. Comput. 56(9), 1255–1268 (2007)
4. Seifert, N., Shipleg, P., Pant, M.D., Ambrose, V., Gil, B.: Radiation induced clock jitter and race. In: Int. Physics Reliability Symposium, April 2005, pp. 215–22 (2005)
5. Shivakumar, P., Kistler, M., Keckler, S.W., Burger, D., Alvisi, L.: Modeling the effect of technology trends on the soft error rate of combinational logic. In: Proc. Int'l Conference on Dependable Systems and Networks (DSN), June 2002, pp. 389–399 (2002)
6. Kastensmidt, F., Sterpone, L., Sonza Reorda, M., Carrro, L.: On the optimal design of triple modular redundancy logic for SRAM-based FPGAs. In: Proc. IEEE Design, Automation and Test in Europe, pp. 1290–1295 (2005)
7. Fazeli, M., Miremadi, S.G., Ejlali, A., Patooghy, A.: Low energy single event upset/single event transient-tolerant latch for deep subMicron technologies. IET Computers & Digital Techniques 3(3), 289–303 (2009)
8. Karnik, T., Vangal, S., Veeramachaneni, V., Hazucha, P., Erraguntla, V., Borkar, S.: Selective node engineering for chip-level soft error rate improvement. In: IEEE Symp. VLSI Circuits, June 2002, pp. 204–205 (2002)

9. Calin, T., Nicolaidis, M., Velazco, R.: Upset hardened memory design for submicron CMOS technology. IEEE Trans. Nucl. Sci. 43, 2874–2878 (1996)
10. Hazucha, P., Karnik, T., Walstra, S., Bloechel, B.A., Tschanz, J.W., Maiz, J., Soumyanath, K., Dermer, G.E., Narendra, S., De, V., Borkar, S.: Measurements and analysis of SER-tolerant latch in a 90-nm dual-VT CMOS process. IEEE Journal of Solid-State Circuits 39(9), 1536–1543 (2004)
11. Sasaki, Y., Namba, K., Ito, H.: Circuit and Latch Capable of Masking Soft Errors with Schmitt Trigger. J. Electron. Test., 11–19 (June 2008)
12. Oklobdzija, V.G.: Clocking and Clocked Storage Elements in a Multi-Gigahertz Environment. IBM J. of Research and Development 47(5/6), 567–584 (2003)
13. Kumar, J., Tahoori, M.B.: Use of pass transistor logic to minimize the impact of soft errors in combinational circuits. In: Workshop on System Effects of Logic Soft Errors (2005)
14. Das, S., Tokunaga, C., Pant, S., Ma, W.-H., Kalaiselvan, S., Lai, K., Bull, D.M., Blaauw, D.T.: RazorII: In Situ Error Detection and Correction for PVT and SER Tolerance. IEEE J. of Solid-State Circuits 44(1), 32–48 (2009)
15. Dabiri, F., Nahapetian, A., Massey, T., Potkonjak, M., Sarrafzadeh, M.: General Methodology for Soft-Error-Aware Power Optimization Using Gate Sizing. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems 27(10), 1788–1797 (2008)
16. Mitra, S., Seifert, N., Zhang, M., Shi, Q., Kim, K.S.: Robust system design with built-in soft-error resilience. Computer 38(2), 43–52 (2005)
17. Narasimham, B., Bhuva, B.L., Holman, W.T., Schrimpf, R.D., Massengill, L.W., Witulski, A.F., Robinson, W.H.: The Effect of Negative Feedback on Single Event Transient Propagation in Digital Circuits. IEEE Trans. on Nuclear Science 53(6), 3285–3290 (2006)
18. Narasimham, B., Shuler, R.L., Black, J.D., Bhuva, B.L., Schrimpf, R.D., Witulski, A.F., Holman, W.T., Massengill, L.W.: Quantifying the Reduction in Collected Charge and Soft Errors in the Presence of Guard Rings. IEEE Trans. on Device and Materials Reliability 8(1), 203–209 (2008)
19. Stackhouse, B., Bhimji, S., Bostak, C., Bradley, D., Cherkauer, B., Desai, J., Francom, E., Gowan, M., Gronowski, P., Krueger, D., Morganti, C., Troyer, S.: A 65 nm 2-Billion Transistor Quad-Core Itanium Processor. IEEE J. of Solid-State Circuits 44(1), 18–31 (2009)
20. Degalahal, V., Ramanarayanan, R., Vijaykrishnan, N., Xie, Y., Irwin, M.J.: Effect of Power Optimizations on Soft Error Rate. In: IFIP Series on VLSI-SoC, pp. 1–20. Springer, Heidelberg (2006)
21. Oklobdzija, V.G., Stojanovic, V.M., Markovic, D.M., Nedovic, N.: Digital System Clocking: High Performance and Low-Power Aspects. Wiley-IEEE (2005)