A novel radiation hardened by design latch*

Huang Zhengfeng(黄正峰)† and Liang Huaguo(梁华国)

(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: Due to aggressive technology scaling, radiation-induced soft errors have become a serious reliability concern in VLSI chip design. This paper presents a novel radiation hardened by design latch with high single-event-upset (SEU) immunity. The proposed latch can effectively mitigate SEU by internal dual interlocked scheme. The propagation delay, power dissipation and power delay product of the presented latch are evaluated by detailed SPICE simulations. Compared with previous SEU-hardening solutions such as TMR-Latch, the presented latch is more area efficient, delay and power efficient. Fault injection simulations also demonstrate the robustness of the presented latch even under high energy particle strikes.

Key words: soft error; single event upset; radiation hardened by design latch
DOI: 10.1088/1674-4926/30/3/035007 **EEACC:** 2550; 2570D; 7910

1. Introduction

Continuously decreasing CMOS technology feature sizes and supply voltages reduce capacitive node charge and noise margin, increasing sensitivity to radiation-induced soft errors. A single radiation event may cause bit flips in the sequential elements which can last several cycles[1]. This leads to increased susceptibility of SRAM, latches and flip-flops to single event upset (SEU)[2]. Shivakumar predicted that soft error rate (SER) of logic circuits per chip will increase nine orders of magnitude from 1992 to 2011[3]. Soft errors used to be a concern only for space and aero applications. In the era of nanoscale CMOS, radiation-induced soft errors have become a serious issue at ground level as well. As we know, there are several radiation mechanisms that induce the soft errors at ground level: alpha particles from IC packaging and cosmic rays.

With the increasing integration of devices on a chip, the chip-level SER contribution from SEU is continuously rising. According to estimated SER contributions in typical designs such as microprocessors, network processors and network storage controllers by Intel Corporation, SEU occupies 89% of the overall SER[4]. Fault injections in the DLX processor and the Alpha processor also demonstrate that SEU is the predominant issue, such that protecting only 30% of processor states can cover nearly 80% of the failures[5]. In a word, most of the soft error mitigation schemes put emphasis on SEU-tolerance.

In this paper, a new radiation hardened by design (RHBD) latch with internal dual interlock is proposed to be immune to SEU. The proposed latch utilizes space redundancy inside the latch to mitigate SEU induced soft errors with the following merits. First, the RHBD methodology allows hardened circuits to be fabricated in commercially available state-of-the-art CMOS manufacturing processes[6]. The RHBD methodology is also compatible with current design flow and EDA tools. The proposed RHBD latch can be implemented as a standard cell for nanometer CMOS technologies. The engineers just need to replace the original latch with the proposed RHBD latch. Second, the proposed latch has no vulnerable internal nodes for its internal dual interlocked scheme. As is widely known, the Achilles' heel of previous RHBD latch/flip-flop is vulnerable internal nodes[7].

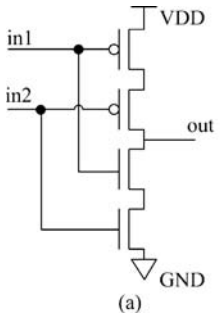
2. Previous work

There are several potential solutions to design SEU-hardened latch such as space redundancy and/or time redundancy.

Space redundancy mainly includes dual modular redundancy (DMR) and triple modular redundancy (TMR). TMR is the most commonly used scheme to perform SEU-hardening. The European Space Agency implemented the 32-bit LEON-FT processor based on the SPARC V8 instruction set[8]. LEON-FT processor tolerates SEU using TMR registers. Each of the three lanes of the TMR registers can have separate clock-trees. Other TMR scheme integrates triple homogenous latch and a voter into a standard cell[9−11], in order to avoid the influence induced by unpredicted interconnect delay after place and route. However, TMR always incurs great area overhead and power dissipation penalty. Traditional DMR compares dual identical sequential elements to check error, without ability to mitigate soft errors. Novel DMR such as Razor compares dual different sequential elements. Razor compares the main flip-flop and shadow latch to find error, and the error will trigger rollback-recovery at pipeline level[12]. To combat high energy particle strike, latest DMR schemes utilize interlock scheme inside the latch which can improve the robustness effectively[7, 13]. Nevertheless, TMR or DMR both incur non-trivial impact on hardware overhead and power dissipation.

Time redundancy such as rollback-recovery is popular

* Project supported by the National Natural Science Foundation of China (Nos. 60633060, 60876028).
† Corresponding author. Email: hanson_hfut@sina.com
Received 30 July 2008



in1	in2	out
0	0	1
1	1	0
0	1	Hold
1	0	Hold

(b)

Fig. 1. (a) C-element; (b) C-element truth table.

because it is cost-effective, low overhead as compared to space redundancy. Time redundancy uses slack time to insert SEU-hardening latches on the path. Novel time redundancy techniques are always applied together with TMR or DMR through temporal sampling[9, 10]. However, temporal sampling has the following disadvantages: (1) It suffers from very large hardware overhead to generate time-shifted clock or data signal. (2) Process and environmental parameter variations will introduce non-trivial delay uncertainty which can be as large as 20% in the worst case[14]. (3) It may incur impact on performances when used on critical paths[15]. In the worst case, it may impact slack on critical paths by 3τ (τ is the time-shifted value which is decided by the maximum pulse width).

3. Internal dual interlocked latch

In this section we will detail the principles and implementation of the presented RHBD latch. To eliminate vulnerable internal nodes, the proposed latch utilizes dual interlocked use of internal feedback lines. The Muller C-element is inserted to block the soft errors induced by SEU. Figure 1 shows the structure and truth table of C-element. The C-element propagates the inverse value of input to output if two inputs are of identical logic value. C-element holds the current state if two inputs are different. State holding characteristics of C-element can block SEU from occurring at the internal nodes with minimal hardware overhead. C-element used to be clocked CMOS (C^2MOS) or synchronizer to synchronize handshake signals. Latest SEU-tolerant latches use C-element to mitigate the SEU[15], which also face the problem of large hardware overheadf and sensitivity to high energy particle strike. The proposed RHBD latch uses C-element in an internal dual interlocked scheme with feedback from outputs to inputs, which can effectively tolerate high-energy particle strike.

Figure 2 shows the structure of the proposed SEU-tolerant latch. The whole structure is symmetric and dual interlocked. There are three identical C-elements in the proposed latch: CE1, CE2, and CE3. CE2 and CE3 are used as C^2MOS to construct keeper when the latch is not transparent. CE1 is used to block the radiation-induced SEU in the internal nodes, whether the latch is transparent or not. The whole structure is elaborate for its symmetry and dual interlock. Although there are several different internal nodes inside the proposed latch, we can partition equivalent node pairs for

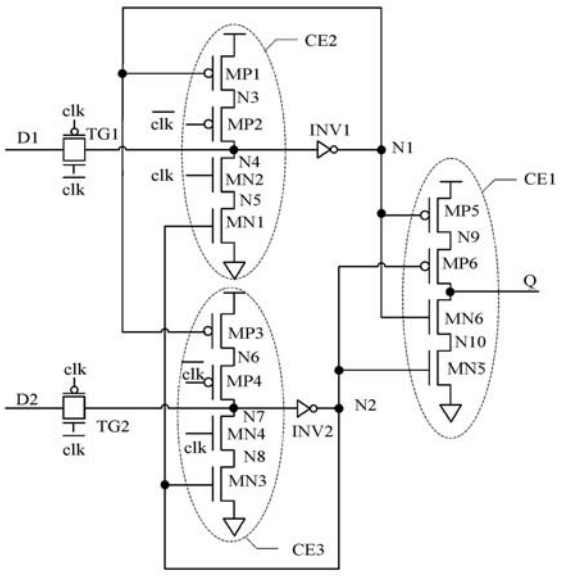


Fig. 2. Electrical structure of the proposed RHBD latch.

its symmetric structure. Also radiation-induced SEU can be classified into several cases: {N1, N2}, {N4, N7}, {N3, N5, N6, N8, N9, N10}. SEU injection can only need to be done at internal nodes such as N1, N4, N9.

Two inputs D1 and D2 are identical. If D1 is delayed by τ time units to obtain D2, the proposed RHBD latch can effectively mitigate SET with pulse width less than τ. The time-shifted SET-tolerant solution always suffers great area overhead and performance penalty[16].

As mentioned in section 1, the Achilles' heel of previous SEU-hardening latch scheme is particular vulnerable internal nodes. The proposed RHBD latch has no such limitations because of its symmetric and dual interlocked structure which is validated by detailed SPICE simulations.

4. Simulations

Detailed SPICE simulations were carried out on the proposed RHBD latch using advanced Predictive Technology Model (PTM) invented by the nano-scale Integration and Modeling (NIMO) Group of Arizona State University. As an evolution of traditional Berkeley Predictive Technology Model (BPTM), PTM of bulk CMOS is successfully generated for 130 to 32 nm technology nodes. The PTM can be easily customized to cover a wide range of process uncertainties. PTM is more physical, scalable, and continuous over technology generations and suitable for emerging variability and reliability issues[17]. The 45 nm technology model card was chosen to perform the simulations.

4.1. SEU injection simulation

As mentioned in section 3, all the internal nodes were partitioned into different equivalent class of nodes so that SEU injection was only performed on three internal nodes from each equivalent class of nodes: {N1, N2}, {N4, N7}, {N3, N5, N6, N8, N9, N10}. SEU injection methodology is to simulate the high-energy particle striking. The current induced by SEU

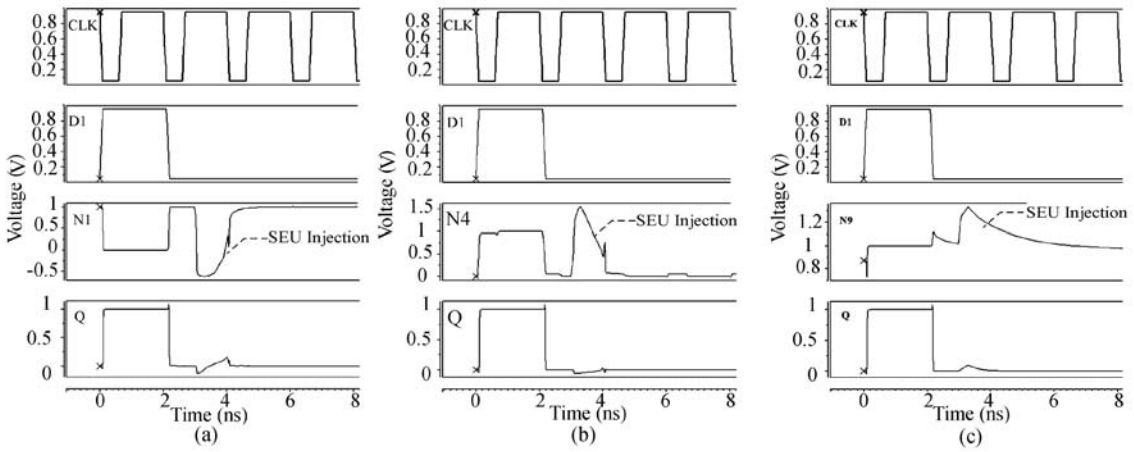


Fig. 3. Behavior of the proposed RHBD latch with injection at (a) node N1, (b) node N4, and (c) node N9.

can be modeled as traditional double-exponential function current source, which can accurately represent the electrical impact of particle striking[18]. The pulse can be expressed as

$$I(t) = \frac{Q}{\tau_\alpha - \tau_\beta}(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta}). \quad (1)$$

The parameter Q represents the total amount of charge colleted at the affected node, τ_α accounts for the collection time-constant of the junction, and τ_β accounts for the ion-track time-constant. Time constants are process-dependent. For simulation purposes, we consider the values given in Ref. [19]: $\tau_\alpha = 200$ ps and $\tau_\beta = 50$ ps.

SEU injection at internal nodes N1, N4 and N9 is shown in Figs. 3(a) to 3(c). As can be seen clearly from Fig. 3, the proposed latch can mitigate all the SEU occurring inside the latch. As is well known, the area cost is mainly decided by the amount of transistors. The proposed latch occupies 20 transistors. The proposed latch makes improvement in immunity to radiation-induced SEU. As reported in the latest papers[7], most previous SEU-hardening latches have internal vulnerable nodes that impact the whole robustness, while the proposed latch can solve the problem because of its dual interlocked structure.

4.2. SER comparison

To compare the robustness of internal nodes of the proposed latch, we calculate the SER using the following equation[20]:

$$\mathrm{SER} = \sum_{i=1}^{n} \frac{\mathrm{WOV}_i}{T_{\mathrm{CK}}} \kappa_i \frac{\alpha}{\beta} e^{-\beta Q_{\mathrm{crit}(i)}}. \quad (2)$$

WOV_i is the Window of Vulnerability of internal node i[21], T_{CK} is a clock period, and the coefficient k_i and the fitting parameters α and β are process-dependent. For the technology considered, the value of the fitting parameter β is $\beta = 62.5 \times 10^{12}$ C^{-1}[22]. We perform SPICE simulations of the proposed RHBD latch to evaluate the critical charge $Q_{\mathrm{crit}}(i)$ of all nodes using 45 nm technology model.

We consider a CK frequency of 500 MHz. We have obtained the following relationship between the WOV_i and

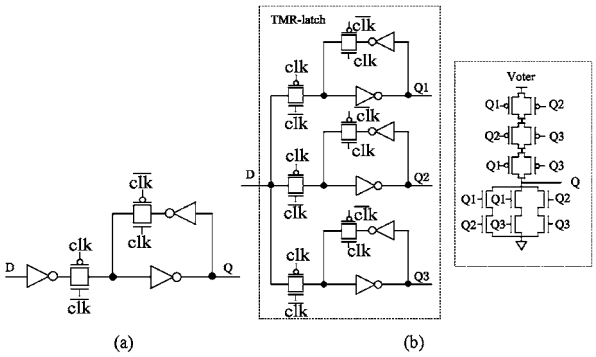


Fig. 4. (a) Static reference latch; (b) TMR-latch.

$Q_{\mathrm{crit}}(i)$ of different internal nodes:

$\mathrm{WOV_{N1}} = \mathrm{WOV_{N4}} = \mathrm{WOV_{N9}} = 489.337$ ps.
$Q_{\mathrm{crit(N1)}} = 61.27$ fC, $Q_{\mathrm{crit(N4)}} = 23.43$ fC,
$Q_{\mathrm{crit(N9)}} = 5.80$ fC.

Thus, we can calculate the SER of different nodes.

$\mathrm{SER_{N4}/SER_{N1}} = 10.64$, $\mathrm{SER_{N9}/SER_{N1}} = 32.04$.

From the above relations, we can find out the susceptibilities of internal nodes N9 and N4 are comparable and they are about 10 times greater than the susceptibility of N1.

4.3. Delay and power comparison

Figure 4 gives the structure of the reference latch and TMR-latch. Figure 5 gives a performance comparison between the proposed latch, the reference latch and TMR-latch (note that the result is normalized by the reference latch). As shown in Fig. 5, the propagation delay of the proposed latch is 83% of the TMR-latch, and the power dissipation of the proposed latch is 68% of the TMR-latch. In short, the simulation results reveal that the proposed latch is delay and power efficient in comparison with TMR-latch.

5. Conclusion

In this paper, a novel RHBD latch that can effectively mitigate SEU induced soft errors was proposed and evaluated.

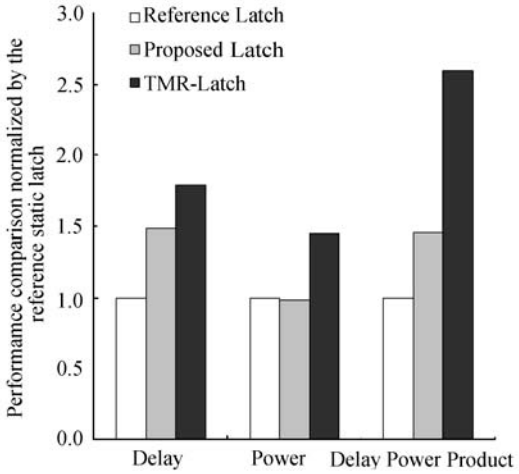


Fig. 5. Performance comparison.

It is confirmed that the dual interlocked and symmetric structure of the proposed latch accounts for its robustness. SPICE simulations were employed to validate the robustness of the proposed latch without internal nodes vulnerable to SEU induced soft errors. The propagation delay, power dissipation and power delay production of the proposed latch were also compared with the reference latch and TMR-latch.

References

[1] Baumann R. Soft errors in advanced computer systems. IEEE Trans Desing & Test of Computers, 2005, 22(3): 258

[2] Karnik T, Hazucha P. Characterization of soft errors caused by single event upsets in CMOS processes. IEEE Trans Dependable and Secure Computing, 2004, 1(2): 128

[3] Shivakumar P, Kistler M, Keckler S W, et al. Modeling the effect of technology trends on the soft error rate of combinational logic. Proc Int Conf Dependable Systems and Networks, Washington DC, USA, 2002: 389

[4] Mitra S, Seifert N, Zhang M, et al. Robust system design with built-in soft-error resilience. IEEE Trans Comput, 2005, 38(2): 43

[5] Saggese G P, Wang N J, Zbigniew T, et al. An experimental study of soft errors in microprocessors. IEEE Trans Micro, 2005, 25(6): 30

[6] Lacoe R. CMOS scaling, design principles and hardening-by-design methodologies. Proc IEEE NSREC Short Course, 2003

[7] Fazeli M, Patooghy A, Miremadi S G, et al. Feedback redundancy: a power efficient SEU-tolerant latch design for deep sub-micron technologies. Proc Int Conf Dependable Systems and Networks, Edinburgh, UK, 2007: 276

[8] Gaisler J. A portable and fault-tolerant microprocessor based on the SPARC V8 architecture. Proc Int Conf Dependable Systems and Networks, Washington, DC, USA, 2002: 409

[9] Mavis D G, Eaton P H. SEU and SET modeling and mitigation in deep submicron technologies. Proc Int Conf Reliability Physics Symp, Phoenix, Arizona, USA, 2007: 293

[10] Chen M, Orailoglu A. Improving circuit robustness with cost-effective soft-error-tolerant sequential elements. Proc 16th IEEE Asian Test Symp, Beijing, China, 2007: 307

[11] Krishnamohan S, Mahapatra N R. Combining error masking and error detection plus recovery to combat soft errors in static CMOS circuits. Proc Int Conf Dependable Systems and Networks, Yokohama, Japan, 2005: 40

[12] Ernst D, Das S, Lee S, et al. Razor: circuit-level correction of timing errors for low-power operation. IEEE Trans Micro, 2004, 24(6): 10

[13] Calin T, Nicolaidis N, Velazo R. Upset hardened memory design for submicron CMOS technology. IEEE Trans Nucl Sci, 1996, 43(6): 2874

[14] Velenis D, Sundaresha R, Friedman E G. Buffer sizing for delay uncertainty induced by process variations. Proc Int Conf Electronics, Circuits and Systems, Tel-Aviv, Israel, 2004: 415

[15] Mitra S, Zhang M, Waqas S. Combinational logic soft error correction. Proc Int Test Conf, Santa Clara, California, USA, 2006: 1

[16] Naseer R, Draper J. DF-DICE: a scalable solution for soft error tolerant circuit design. Proc Int Symp Circuits and Systems, Island of Kos, Greece, 2006: 3890

[17] Zhao W, Cao Y. New generation of predictive technology model for sub-45nm early design exploration. IEEE Trans Electron Devices, 2006, 53(1): 2816

[18] Messenger G C. Collection of charge on junction nodes from ion tracks. IEEE Trans Nucl Sci, 1982, 29(6): 2024

[19] Nagpal C, Garg R, Khatri S P. A delay-efficient radiation-hard digital design approach using CWSP elements. Proc Design, Automation and Test in Europe Conference and Exhibition, Munich, Germany, 2008: 354

[20] Omana M, Rossi D, Metra C. Latch susceptibility to transient faults and new hardening approach. IEEE Trans Comput, 2007, 56(9): 1255

[21] Seifert N, Zhu X, Moyer D, et al. Frequency dependence of soft error rates for sub-micron CMOS technologies. Technical Digest Int Electron Devices Meeting, 2001: 14.4.1

[22] Hazucha P, Svensson C. Impact of CMOS technology scaling on the atmospheric neutron soft error rate. IEEE Trans Nucl Sci, 2000, 47(6): 2586