Soft-Event-Upset and Soft-Event-Transient Tolerant CMOS Circuit Design for Low-Voltage Low-Power Wireless IoT Applications

I-Chyn Wey[1,2], Chun-Han Chen[3], Si-Zhan Fang[3], Heng-Jui Chou[3]

[1]Graduate Institute of Electrical Engineering, Electrical Engineering Department, AI Innovation Research Center, Green Technology Research Center, and Centre for Reliability Sciences and Technologies, School of Electrical and Computer Engineering, College of Engineering, Chang Gung University, Taiwan.

[2]Department of Neurology, Chang Gung Memorial Hospital, Taiwan.

[3]Graduate Institute of Electrical Engineering, Electrical Engineering Department, School of Electrical and Computer Engineering, College of Engineering, Chang Gung University, Taiwan.

***Abstract* – In the wireless IoT applications, low power is a critical criteria, and low-voltage is a direct way to meet such demand. However, low-voltage criteria in advanced CMOS VLSI designs will lead to critical design challenges in dealing with soft-error interference, especial while the cascade transistor number is limited under low-voltage operations. Some possible low-voltage SEU-tolerant and SET-tolerant circuit design methods are discussed in this paper, such as robust C-element, Error-Correction with Duplication, dual interlocked storage cell (DICE) latch, and such as feedback redundant SEU-tolerant (FERST) latch designs.**

I. Introduction

With the progress of semiconductor technology, no matter CMOS circuit designs or sensor designs are improved greatly. With the progress of wireless internet, the applications of internet-of-thing (IoT) are widely developed as well. In the wireless IoT applications, low power is a critical criteria, and low-voltage is a direct way to meet such demand. However, low-voltage criteria in advanced CMOS VLSI designs will lead to critical design challenges in dealing with soft-error interference, especial while the cascade transistor number is limited under low-voltage operations. Therefore, the Soft-Event-Upset (SEU) and Soft-Event-Transient (SET) tolerant design becomes the major challenge in low-voltage, low-power IoT applications of the nano-scale CMOS circuit designs era. However, individual SEU-tolerant sequential circuit designs and SET-tolerant arithmetic circuit designs cannot meet the requirement in a practical system because the soft-error propagation chains are not broken and the overall soft-error tolerance would be greatly lowered [1]. Especially for the operating voltage is lowered and the serial connected transistor is limited, the SET/SEU-tolerant challenges are further raised [1]. In this paper, we will introduce some low voltage SET-tolerant and SEU-tolerant designs to enhance soft-error immunity of the low-voltage low-power CMOS circuit designs in IoT applications.

II. Low-Voltage SEU-Tolerant Latch Circuit Designs

Soft-error usually attacks advanced CMOS VLSI circuits in the situation of lower supply voltage and smaller feature size. Most soft-errors happen in memory circuits, which are soft-error-upset (SEU) and most of soft-error issues in memory elements, such as SRAM, DRAM, register, and latch have been discussed and overcome in recent years [2]-[7]. However, in the low-voltage low-power applications, the serial connected transistor limitation and the protection of C-element itself are new design issues in the low-voltage SEU-tolerant designs [1]. In the low-voltage environment, the voltage difference between VDD and Vth is critical limited. For the C-element used in the SEU-tolerant or SET-tolerant design, itself should also be protected to be soft-error free. As illustrated in Fig.1 (b) [8], with two feedback charge recovery transistor, the weak node in conventional C-element shown in Fig. 1 (a) can be protected, and the design in Fig.1 (b) [8] can be more robust and reliable.

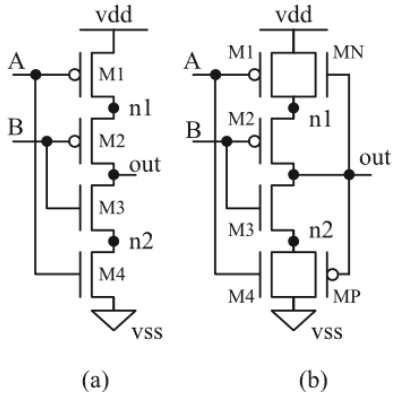
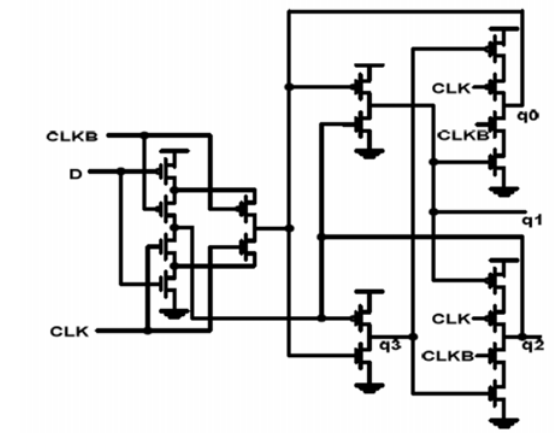
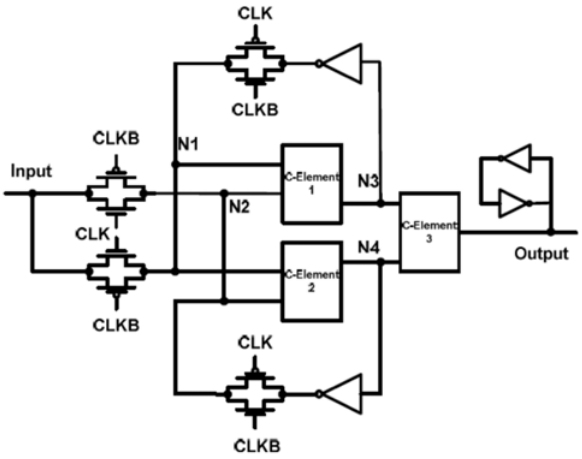


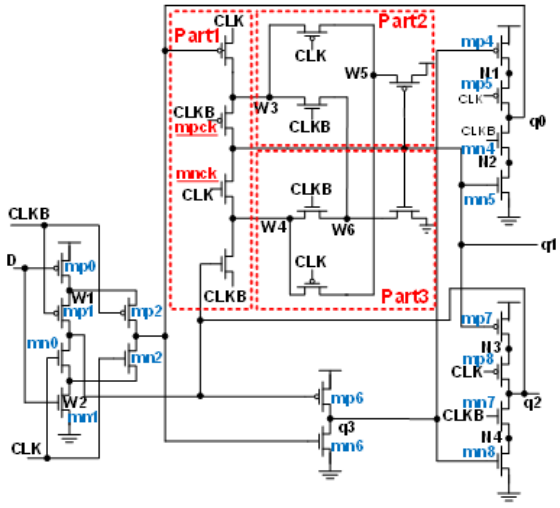
Fig. 1 The C-element cell, (a). Conventional C-element, (b). The robust C-element design presented in [8].



(a)



(b)



(c)

Fig. 2 Various SEU-tolerant latches design. (a) DICE [9], (b) FERST [2], (c) Iso-DICE [10].

In the existing literature designs, there are a variety of methods used to increase the SEU tolerance capability of latch circuits: (1) interlock circuits with a redundant feedback path, such as Dual Interlocked Storage Cell (DICE) [9], Fig. 2(a); (2) latches capable of filtering and masking SEUs, such as feedback redundant SEU-tolerant latch (FERST) [2], Fig. 2(b).; (3) combining the methods of interlock redundancy and SEU masking together, such as Isolated-DICE latch design [10], Fig. 2(c).

Among these design, Isolated-DICE latch design [10] can perform with most superior SEU-tolerance under normal supply voltage operating. However, under lower supply voltage, the floating node issue and serial connection issue will lead it difficult to maintain its internal charges. Therefore, DICE [9] and FERST [2] designs can be more suitable for low-voltage IoT applications instead.

III. Low-Voltage SET-Tolerant Arithmetic Computing Circuit Designs

As compared with the SEU-tolerant latch designs, soft-errors in arithmetic computing circuits or digital signal processing systems are more critical than that in the memory elements because the soft-error in arithmetic circuits will propagation stage by stage to affect all the circuit nodes in its propagation path [1]. Moreover, the circuit architectures in arithmetic computing circuits are irregular, unlike memory cells are usually regular and widely repeated used, which would soft-error issues in arithmetic circuits to be much more difficult encountered [1], [11].

In order to mitigate soft-error interference in CMOS arithmetic circuits, circuit redundancy such as Error Correction with Duplication (ECD), Error-Correction with shift-Timing Output (ECTO) [12], Triple Modular Redundancy (TMR), and Dual Modular Redundancy (DMR) [11], [13] are some common approaches, which is illustrated in Fig. 3. Among these SET-tolerant designs, TMR is the most popular solution because it is simple and can be applied to almost all arithmetic circuits. Is penalty is its area-overhead and waste of power consumption. DMR design is an efficient way to simplify the complex TMR design to need only single duplicated redundancy. However, for the DMR design, the duplicated redundancy circuit is different from its original one in order to generate different fault propagation form [11]. Moreover, for the case of feedback propagation path in arithmetic circuits, the DMR structure in more complex. ECD designs also meet hardware overhead issue and ECTO is more hardware efficient but with speed overhead [11]. Usually, combination with two kinds of SET-tolerant design can break through the limitation of SET-tolerant arithmetic architecture operating in feed-back DSP systems and let the SET-tolerant design can be applied into both feed-forward and feed-back DSP systems [1]. For the low-voltage low-power wireless IoT applications, the SET-tolerant designs usually are realized by architecture redundancy; therefore, they usually will not touch the limitation of transistor serial connection number [1].

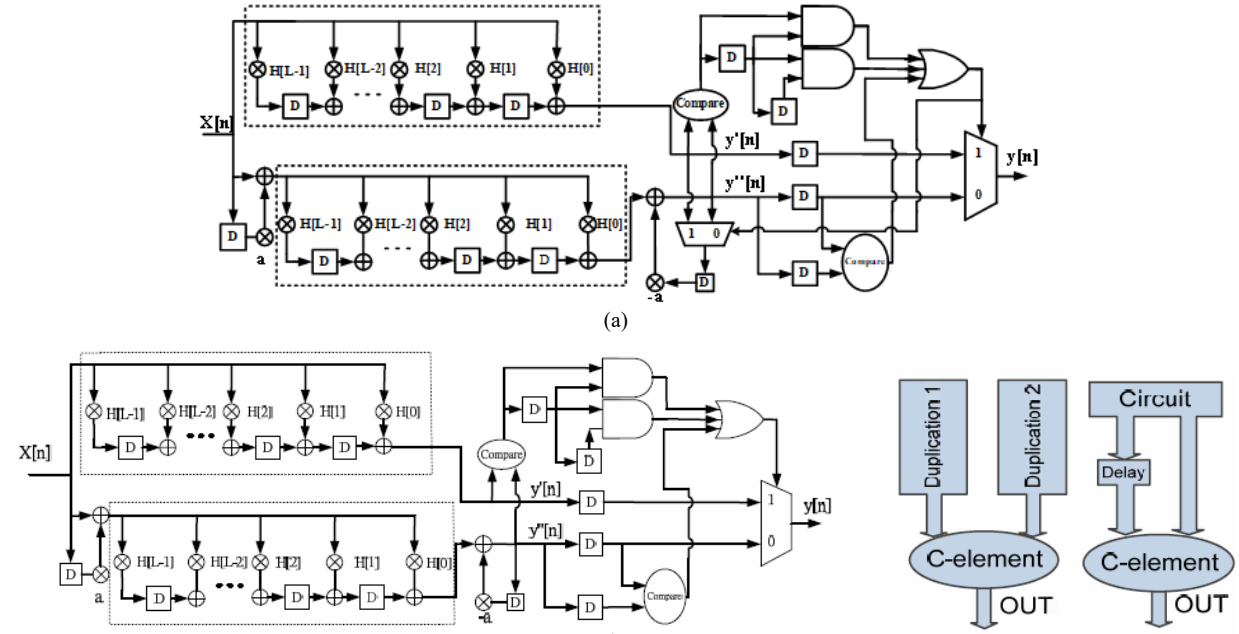


Fig. 3 Some SET-tolerant design approaches. (a). The DMR soft-error tolerant FIR filter presented in [11], (b). The DMR soft-error tolerant FIR filter presented in [10], (c). The ECD and ECTO design [9].

IV. Conclusion

In this paper, we propose a coding-based partial MRF method for multi-logic operations in order to achieve a better trade-off between chip area and noise immunity. First, we put forward an idea of partial clique energy corresponding to the full clique energy used in conventional MRF design [24].

Acknowledgement

This work was supported by the National Science Council, Taiwan, under Grant MOST 107-2221-E-182 -060 and in part by the Chang Gung Medical Research Program under Grant BMRPA77.

References

[1] I. C. Wey, S. Z. Fang, H. J. Chou, Z. Y. Wu, “Soft-Error Tolerant Design in Near-Threshold-Voltage Computing,” IEEE ICASI 2018.

[2] M. Fazeli, S. G. Miremadi, A. Ejlali, and A. Patooghy, “Low energy single event upset/single event transient-tolerant latch for deep submicron technologies,” IET Computers and Digital Techniques, vol. 3, no. 3, pp. 289–303, 2009.

[3] H. Nan, and K. Choi, “Novel soft error hardening design of nanoscale CMOS latch," in Proc. of International SoC Design Conference, pp. 111–114, 2010.

[4] M. Omaña, D. Rossi, and C. Metra, “High-performance robust latches,” IEEE Trans. on Computers, vol. 59, no. 11, pp. 1455–1465, 2010.

[5] H. Nan and K. Choi, “High performance, low cost, and robust soft error tolerant latch designs for nanoscale CMOS technology,” IEEE Trans. on Circuits and Systems-I, Vol. 59, No. 7, pp.1445–1457, 2012.

[6] A. Maru, H. Shindou, T. Ebihara, A. Makihara, T. Hirao, and S. Kuboyama, “DICE-based flip-flop with SET pulse discriminator on a 90 nm bulk CMOS process,” IEEE Trans. on Nuclear Science, Vol. 57, No. 6, pp. 3602–3608, 2010.

[7] S. X. Xuan, N. Li, and J. Tong, “SEU Hardened Flip-Flop Based on Dynamic Logic,” IEEE Trans. on Nuclear Science, Vol. 60, No. 5, pp. 3932–3936, 2013.

[8] I. C. Wey, B. C. Wu, C. C. Peng, C. S. Gong, and C. H. Yu, “Robust C-element Design for Soft-Error Mitigation” IEICE Electronic Express 12(10): 20150268, 2015.

[9] Calinl, M. Nicolaidisl and R. Velazco, “Upset hardened memory design for submicron CMOS technology,” IEEE Trans. Nucl. Sci., Vol 43, pp.2874-2878, Dec. 1996.

[10] I. C. Wey, Y. S. Yang, B. C. Wu, C. C. Peng, “A low power-delay-product and robust Isolated-DICE based SEU-tolerant latch circuit design,” Microelectronics Journal, Vol. 45, Issue 1, PP. 1-13, January, 2014.

[11] I. C. Wey, C. C. Peng, H. J. Chou, P. T. Chen, "Reliable and low error dual modular redundancy FIR filter with wide protection window" IEICE Electronic Express, Vol. 11, No. 9, pp. 20140183, 2014.

[12] S. Mitra, M. Zhang, S. Waqas, N. Seifert, B. Gill, and K. S. Kim, "Combinational Logic Soft Error Correction," IEEE International Test Conference, pp.1-9, 2006.

[13] P. Reviriego, C. J. Bleakley, J. A. Maestro, "Signal shaping dual modular redundancy for soft error tolerant finite impulse response filters," Electronics Letters, vol.47, no.23, pp.1272,1273, 2011.