ISSN (e): 2250 – 3005 || Volume, 07 || Issue, 09|| September – 2017 ||
International Journal of Computational Engineering Research (IJCER)

Fault Tolerance Systems for Combinational Circuits

Jyoti M Gadekar[1], Prof. S.S. Badhe[2]

[1] M.E. Student, E&TC Department, D.Y. Patil College of Engineering, India,
[2] E&TC Department, D.Y. Patil College og Engineering, India.

ABSTRACT

Due to advancement in CMOS technology and shrinking of feature size to nano scale, systems are turning out to be more susceptible to manufacturing defects and soft errors. This paper is focused on designing combinational circuits for soft error tolerance with minimal area overhead, which is necessary to overcome error probability. The idea is based on analysing random pattern testability of faults in a circuit and protecting sensitive transistors, whose soft error detection probability is relatively high, until desired circuit reliability is achieved or a given area overhead constraint is met. Protection to transistors is provided by duplicating and sizing a subset of transistors necessary for providing the protection. The proposed algorithms are used to protect sensitive transistors whose probability of failure is relatively high and to compute the circuit failure rate/reliability at the gate level. Simulation results show that the proposed algorithms achieve better soft error rate reduction than other transistor sizing-based techniques.

***Keywords*:** Fault tolerance, radiation hardening, single event multiple upsets, single event transient(SET), single event upset (SEU), soft error tolerance.

Date of Submission: 10-08-2017 Date of acceptance: 25-09-2017

I. INTRODUCTION

With fabrication technology reaching nanolevels, systems are becoming more prone to manufacturing defects with higher susceptibility to soft errors. This paper is focused on designing combinational circuits for soft error tolerance with minimal area overhead[1]. As the increase in CMOS technology and shrinking of feature size to the nanometer scale, studies have indicated that high-density chips will not only be increasingly accompanied by manufacturing defects but also susceptible to dynamic faults during chip operation [2], [3]. Nanoscale devices are limited by several characteristics; most dominant are the devices higher defect rates and the increased susceptibility to soft errors. Both of these types of errors affect the operations of a circuit if they are not addressed.

Reliability of a circuit can be defined as its ability to function properly despite the existence of such errors. Transient (soft) errors can arise due to multiple sources. These include high-energy particles, coupling, power supply noise, leakage, and temporal circuit variations. A soft error leads to transient error(s), which can last for one or several clock cycles. A single event transient (SET) occurs when a charged particle hits the combinational logic resulting in a transient current pulse. If this transient has enough width and magnitude, it can result in an erroneous value at the gate output. If the erroneous value is latched at a memory element, an SET becomes a single event upset (SEU). A single SET can produce multiple transient current pulses at the output [4]. This is due to the logic fan-out in the circuit.

Ziegler et al. [5] presented intensive experimental study over the period of 15 years to evaluate the radiation-induced soft fails in large scale integrated electronics at different terrestrial altitudes. Baumann [6] highlighted the dominant sources responsible for the creation of soft errors in terrestrial applications. Shivakumar et al. [7] modeled the effects of soft errors in memory devices and logic devices and demonstrated that with each technology generation, soft errors will increase by orders of magnitude in logic devices and projected that soft errors in logic devices will be comparable to that of memory devices. The minimum charge required to create a soft error in a transistor is referred to as Qcrit . It has been shown that Qcrit is going to be reduced with technology improvement and with the advent of low-power devices [7], [8].

This paper focuses on a selective-transistor scaling method that protects individual sensitive transistors of a circuit. A sensitive transistor is a transistor whose soft error detection probability is relatively high. This is in contrast to previous approaches where all transistors, series transistors, or those transistors connected to the

output of a sensitive gate, whose soft error detection probability is relatively high, are protected. Transistor duplication and asymmetric transistor sizing are applied to protect the most sensitive transistors of the circuit. In asymmetric sizing, nMOS and pMOS transistors are sized independently. Reliability is evaluated for different protection thresholds and area overhead constraints.

II. LITERATURE SURVEY

The purpose of this section is: 1) to list representative techniques that could be (or are already) used to address SEU related concerns in mainstream electronics and 2) to point out limitations (overhead and cost) that motivate research in alternate cost-effective strategies for SEU-tolerant design.

In this paper [4], non-destructive SEE are caused by charge deposition by direct ionization from heavy ions and indirect ionization from protons and neutrons. The deposited charge can be collected by drift and diffusion in semiconductor devices, causing current transients that can result in circuit malfunction. Funneling can increase the charge collected due to drift processes and is especially important for DRAMs and devices not fabricated on epitaxial substrates. In SRAMs, voltage transients can cause upsets by mimicking the write process. In complex and high-speed circuits such as microprocessors, even a momentary glitch can propagate through an IC to cause upsets. Multiple-bit upsets occur when more than one bit in a digital circuit is upset by a single particle strike. Mitigation techniques for SEU include system-level methods such as error detection and correction, lockstep execution, and redundant systems using voting. Circuit-level methods are also effective, and several SEU-hardened latch designs have been proposed. These techniques have the advantage of allowing the use of commercial fabrication technologies but usually lead to greatly increased transistor counts and area penalties. Traditional radiation hardened circuits use process techniques such as lightly doped polysilicon feedback resistors to provide SEU immunity. While very effective, passive feedback elements reduce circuit performance and degrade IC manufacturability. Simulations of SEE have been crucial to developing an understanding of the mechanisms behind SEE and for suggesting methods for hardening devices. As devices continue to evolve to smaller dimensions, device-level modeling will encounter new challenges such as the ion strike affecting more than a single transistor at a time.

A greater level of usefulness can be reached when simulation tools prove to be validated and predictive. At this level, simulations become essential during the design process for reducing the number of fab-and-test cycles that must be completed to develop radiation-hardened technologies. Technology trends are unfortunately such that SEE are likely to become even more of a concern for the future. Decreasing feature sizes, lower operating voltage, and higher speeds all conspire to increase susceptibility to SEU. Upset in avionics is an established concern. Upset at the ground level will continue to be an increasing concern for manufacturers of microelectronics for terrestrial applications. The use of ip-chip packaging and multiple levels of metals will further exacerbate the problem. Typical methods of mitigation that either increase the transistor count or reduce IC performance will likely not be acceptable to commercial manufacturers, and new methods will need to be developed. SOI technology may help in this regard, but is not a magic bullet to end all SEE concerns. Hopefully, the fact that commercial manufacturers must deal with SEE concerns will provide a collateral benefit to the radiation effects community as more resources are brought to bear on the problem.

This paper [7] examines the effect of technology scaling and microarchitectural trends on the rate of soft errors in CMOS memory and logic circuits. It describes and validate an end-to-end model that enables us to compute the soft error rates (SER) for existing and future microprocessor style designs. The model captures the effects of two important masking phenomena, electrical masking and latching window masking, which inhibit soft errors in combinational logic. This paper quantify the SER due to high-energy neutrons in SRAM cells, latches, and logic circuits for feature sizes from 600nm to 50nm and clock periods from 16 to 6 fan-out-of-4 inverter delays. Our model predicts that the SER per chip of logic circuits will increase nine orders of magnitude from 1992 to 2011 and at that point will be comparable to the SER per chip of unprotected memory elements. Result emphasizes that computer system designers must address the risks of soft errors in logic circuits for future designs.

In this paper [16], a generalized modular redundancy (GMR) scheme to enhance the reliability of combinational circuits is proposed. Additionally, several aspects regarding the application of this scheme are explored. Also, a methodology for applying GMR scheme is developed. Reliability analysis shows that the proposed methodology can achieve reliability figures higher than that of triple modular redundancy (TMR). In general, significant over-head savings are accomplished in addition to that superior reliability. A gate-level radiation hardening technique for cost effective reduction of the soft error failure rate in combinational logic circuits is described [23]. The key idea is to exploit the asymmetric logical masking probabilities of gates, hardening gates that have the lowest logical masking probability to achieve cost effective tradeoffs between overhead and soft error failure rate reduction. The asymmetry in the logical masking probabilities at a gate is leveraged by decoupling the physical from the logical (Boolean) aspects of soft error susceptibility of the gate. Gates are hardened to single-event upsets (SEUs) with specified worst case characteristics in increasing order of their logical masking probability,

thereby maximizing the reduction in the soft error failure rate for specified overhead costs (area, power, and delay). Gate sizing for radiation hardening uses a novel gate (transistor) sizing technique that is both efficient and accurate. A full set of experimental results for process technologies ranging from 180 to 70 nm demonstrates the cost effective tradeoffs that can be achieved.

Reliability in systems can be achieved by redundancy. Redundancy can be added at the module level, gate level, transistor level [9], or even at the software level [10]. Design of reliable systems by using redundant unreliable components was proposed in [11]. Since then, plethora of research has been done to rectify soft errors in combinational and sequential circuits by applying hardware redundancy [12], [13]. Triple modular redundancy (TMR), a popular and widely used technique, creates three identical copies of the system and combines their outputs using a majority voter [14], [15]. The generalized modular redundancy [16] scheme considers the probability of occurrence of each combination at the output of a circuit. The redundancy is then added to only protect those combinations that have high probability of occurrence, while the remaining combinations are left unprotected to save area. El-Maleh and Al-Qahtani [17] proposed a fault tolerance technique for sequential circuits that enhances the reliability of sequential circuits by introducing redundant equivalent states for states with high probability of occurrence.

Mohanram and Touba [18] proposed a partial error masking scheme based on TMR, which targets the nodes with the highest soft error susceptibility. Two reduction heuristics are used to reduce soft error failure rate, namely, cluster sharing reduction and dominant value reduction. Instead of triplicating the whole logic as in TMR, only those nodes with high soft error susceptibility are triplicated; the rest of the nodes are clustered and shared among the triplicated logic.

In [19] and [20], sensitive gates are duplicated and their outputs are connected together. Physically placing the two gates with a sufficient distance reduces the probability of having the two gates hit by a particle strike simultaneously and, therefore, reduces the soft error rate (SER). Another technique based on TMR maintains a history index of correct computation module to select the correct result [21].

III. EFFECT OF ENERGETIC PARTICLE STRIKE

When an energetic particle strikes a semiconductor, it ionizes the region around it, resulting in the generation of electron hole pairs. The charge due to the particle strike is then transported by drift and diffusion, resulting in the establishment of transient electric field, i.e., SET. The change in voltage observed at the output due to SET depends on the energy and angle of incidence of energetic particle. Source and drain regions are the most sensitive nodes to such events due to the large field around the junction regions, which sweeps in the generated electron holes and result in large currents. If the energy of a striking particle is high enough, it will ip the output of a gate resulting in an SET [4], [6]. To explain the STR principle, we first consider the effect of an energetic particle striking a CMOS inverter. When the inverter input is LOW and the energetic particle strikes the drain of an nMOS transistor, the output voltage is temporarily lowered. Whereas, when the inverter input is HIGH and the energetic particle strikes the drain of a pMOS transistor, the output voltage is temporarily raised. In both the cases, the output logic value of the inverter can be changed to a wrong value if enough charge is collected. This is shown in Fig.1, using 130-nm predictive technology model. Fig.2 shows the fault injection mechanism employed in this paper. The output load is assumed to be equal to an inverter load.

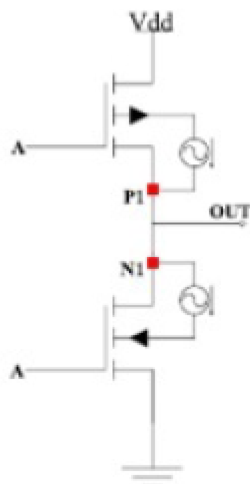

Figure.1 Effect of energetic particle strike on CMOS inverter at t = 5 ns

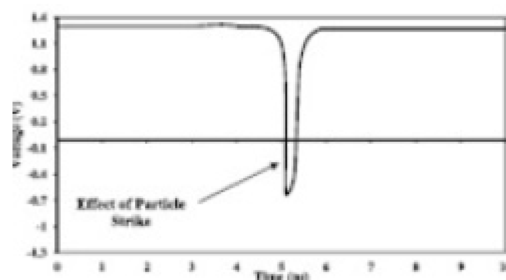

Figure.2 Effect of particle strike at nMOS drain

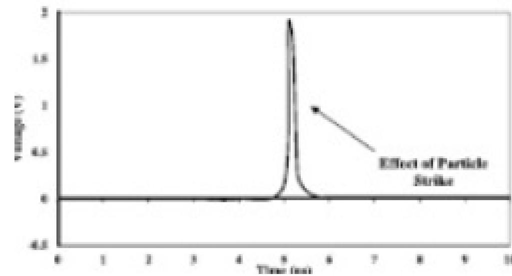

Figure.3 Effect of particle strike at pMOS drain

The soft error is modeled by injecting a current I of charge Q at the drain of a transistor. The direction of injected current is from drain-to-body (bulk) in the nMOS transistor and from body (bulk)-to-drain in the pMOS transistor. The double exponential current pulse I is used to model the charge deposited due to a particle strike at the drain of nMOS or pMOS transistor and is depicted as

$$I(t)=\frac{Q}{(\tau_f-\tau_r)}\left(e^{\frac{t}{\tau_f}}-e^{\frac{t}{\tau_r}}\right) \quad (1)$$

where Q is the charge deposited by a particle strike, f denotes the falling time of the pulse, and r denotes the rising time of injected current pulse andvvaries for each process technology. The value of f is greater than r . The supply rail Vdd is connected to 1.3 V. We will be taking 130-nm technology as our case study in this paper; however, the technique is general and applicable to any process technology. Fig.2 shows the effect of a particle strike on the drain of an nMOS transistor when the true output of an inverter is HIGH. The particle strike at N1 will cause a sudden drop in the output voltage (approximately 0.7 V) of an inverter. This type of soft error will be modeled as a stuck-at-0 (sa0) fault at the output of the gate. To protect from this fault, the pMOS transistors of an inverter must be scaled enough, so that the output voltage becomes greater than Vdd/2. Fig.3 shows the effect of a particle strike on the drain of a pMOS transistor when the true output of an inverter is LOW. The particle strike at P1 will cause a sudden rise in the output voltage (1.9 V) of an inverter. This type of soft error will be modeled as a stuck-at-1 (sa1) fault at the output of the gate. To protect from this fault, the nMOS transistor of an inverter must be scaled enough, so that the output voltage becomes less than Vdd/2.
Now, consider the transistor arrangement shown in Fig.4 where duplicate pMOS transistors are connected in parallel.

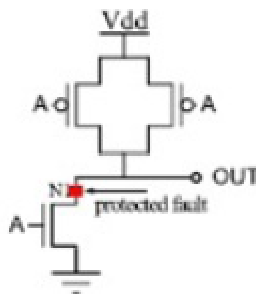

Figure.4 Proposed protection schemes and their effect Particle hit at nMOS drain, OUT = HIGH

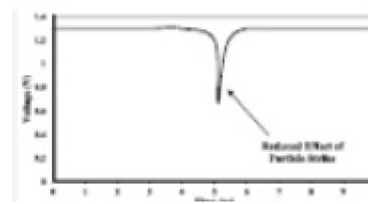

Figure.5 Reduced effect of particle strike at nMOS drain

The width of the redundant transistors must also be increased to allow dissipation (sinking) of the deposited charge as quickly as it is deposited, so that the transient does not achieve sufficient magnitude and duration to propagate to the output. If the output is currently high and an energetic particle hits the drain N1 of the nMOS transistor (with the same current source used in the simulations shown in Fig.1), this should result in a lowered voltage observed at the output. But, due to the employed transistor configuration, the net negative voltage effect will be compensated, as evident from Fig.5, resulting in a spike that has lesser magnitude as compared with the one shown in Fig.2.
The spike magnitude is reduced due to increased output capacitance and reduced resistance between the Vdd and the output. Consider another arrangement of transistors in Fig.6 where redundant nMOS transistors are connected in parallel. If the output is low and the incident energetic particle strikes the drain P1 of pMOS transistor, then the raised voltage effect at the output shown in Fig.3 will be reduced, as shown in Fig.7. This reduction in the spike magnitude is due to the same reasons mentioned for the nMOS transistor. Similarly, to protect from both sa0 and sa1 faults, the transistor structures in Fig.4 and Fig.5 can be combined to fully protect the NOT gate. A fully protected NOT gate offers the best hardening by design, but at the cost of higher area

overhead and power. It must be noted that the optimal size of the transistor for SEU immunity depends on the charge Q of the incident energetic particle.
Due to aggressive nodes and voltage scaling, the effect of transient fault is no more constrained to a node where the incident particle strikes. This could result in the possibility of deposited charge being simultaneously shared by multiple circuit nodes in the circuit, leading to the single event multiple upsets, also referred to as multiple-bit upsets [4]. Considering the inverter example in Fig.1, if two particles strike at the drain of nMOS and pMOS transistors simultaneously, then the charge collection at the nMOS and pMOS transistors will offset each other, resulting in an insignificant change in voltage at the output. Therefore, by the duplication of transistors, it is intended to increase the probability of multiple fault hits at the same gate, so that the victim transistors could cancel the effect of each other. For that matter, LEAP placement technique can be utilized. This scheme places the drain contact nodes of nMOS and pMOS transistors in an interleaved fashion, so that multiple drain contact nodes can act together to fully or partially suppress the SETs. Another advantage of using parallel duplicate transistors is the defect tolerance of transistor stuck-open faults for protected transistors.

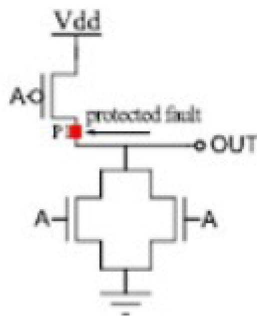

Figure.6 Proposed protection schemes and their effect:Particle hit at pMOS drain

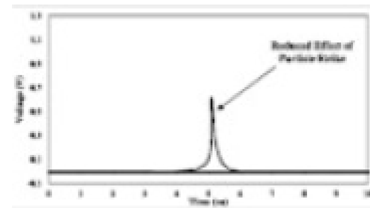

Figure.7 Reduced effect of particle strike at pMOS drain

IV. CIRCUIT PROBABILITY OF FAILURE

Let us first define the POF of a transistor. In all discussions, subscripts i and j refer to gate i and transistor j , respectively. The POF_{ij} of the j th transistor of gate i is defined as the probability of circuit failure due to a fault hitting the transistor. It is computed using the following relation:

$$POF_{ij} = PDET_{ij} \times PHIT_{ij} \quad (2)$$

where $PDET_{ij}$ is the probability of detecting a fault hitting transistor j of gate i at a primary output, and $PHIT_{ij}$ is the probability that transistor j of gate i is hit by a fault. The greater the transistor width/area is, the greater its hit probability is.

$PHIT_{ij}$ is computed separately for nMOS and pMOS transistors as they have different drain widths. Let NW_{ij} and PW_{ij} be the width of nMOS and pMOS transistors, respectively, and Area be the total circuit area; then, the probability of a transistor j of gate i to be hit by a fault, $PHIT_{ij}$, is computed using the following relation:

$$PHIT_{ij} = \frac{W_{ij}}{Area} \; W_{ij} \in \{NW_{ij}, PW_{ij}\} \quad (3)$$

$PDET_{ij}$, as defined before, depends on two factors: 1) probability of input patterns for which a fault that hits the transistor is propagated to the output of a gate, i.e., controllability conditions to excite the fault and 2) stuck-at fault observability probability of the gate at one of the primary outputs of a circuit, i.e., observability probability. $PDET_{ij}$ Is computed using the following relation:

$$PDET_{ij} = P_{Excitationij} \times P_{Prpagationij} \quad (4)$$

where $P_{Excitationij}$ denotes the probability that the fault is excited at gate i output due to a fault hit at transistor j. $P_{Prpagationij}$ denotes the probability that an error that is excited at the gate's output is observable at one of the primary outputs. Let S be a set of patterns for which an error that strikes transistor j is propagated to the output of gate i ; then, $P_{Excitationij}$ is computed as

$$P_{Excitationij} = \sum_{k=1}^{|s|} Prob.S_k \quad (5)$$

where Prob. S_k denotes the probability of occurrence of the kth input pattern. Similarly, $P_{Prpagationij}$ can be computed using the following relation:

$$P_{Prpagationij} = \frac{stuck-at-detection-prob_i}{PC_i} \quad (6)$$

where stuck-at-detection-$prob_i$defines stuck-at fault detection probability of gate i and $PC_i$is the controllability probability to produce logic value opposite to the fault effect at the gate output. Finally, the circuit POF POFc for a single fault is simply the summation of POFs of all transistors n over all gates m of a circuit

$$POF_c = \sum_{i=1}^{m} \sum_{j=1}^{n} POF_{ij} \quad (7)$$

V. PROBABILITY OF FAULT INJECTION

The fault injection probabilities of a gate depend on the conditional fault excitation probability ($CFEP_{ij}$) and probability of hit/selection. A general relation to compute $CFEP_{ij}$ of the jth transistor of a gate i can be derived as follows. Let S be a set of patterns for which an error is excited to the output of a gate and PC_i be the controllability probability to produce a logic value opposite to the fault effect at the gate output. Then, $CFEP_{ij}$can be defined as

$$CFEP_{ij} = \frac{\sum_{k=1}^{|s|} Prob.S_k}{PC_i} \quad (8)$$

$CFEP_{ij}$ of any MOS transistor depends on the process technology and the charge of the incident particle. Therefore, in order to get the exact $CFEP_{ij}$ probability for each MOS transistor, transistor-level simulations are performed using SPICE. Now, the sa0 fault injection probability of gate G_i is computed using the following equation:

$$G_i \text{sa0 inj. Prob} = \sum_{j=1}^{n} CFEP_{N_{ij}} \ x \left(\frac{NW_{ij}}{\sum_{k=1}^{n} NW_{ik}} \right) \quad (9)$$

where n is the total number of nMOS transistors in gate G_i , $NW_{ij}$is the width of the drain of the jth nMOS transistor, and $CFEP_{N_{ij}}$is the CFEP due to a fault hit at the jth nMOS transistor of gate i . Similarly, the sa1 fault injection probability of gate $G_i$is computed as follows:

$$G_i \text{sa1 inj. Prob} = \sum_{j=1}^{p} CFEP_{p_{ij}} \ x \left(\frac{PW_{ij}}{\sum_{k=1}^{p} PW_{ik}} \right) \quad (10)$$

where p is the total number of pMOS transistors in gate G_i , $PW_{ij}$is the width of the drain of the jth pMOS transistor, and $CFEP_{P_{ij}}$is the CFEP due to a fault hit at the jth pMOS transistor of gate i .

VI. FLOWCHARTS OF PROPOSED SYSTEM

In this section, the proposed STR algorithm is presented. The algorithm protects sensitive transistors whose probability of failure (POF) is relatively high. The proposed algorithm can be utilized in two capacities: 1) apply protection until the POF of circuit reaches a certain threshold and 2) apply protection until certain area overhead constraint is met.

Flowchart of Fault Detection Probability

The selective redundancy technique is applied to protect the transistors of a circuit that have relatively high POFij . Sensitive transistors that have relatively high POF are identified based on fault simulation of random input patterns. Different arrangements of nMOS and pMOS transistors are proposed for each gate for various transistor protection scenarios. Flowchart 1 highlights the steps of proposed system. In this, after selecting the transistor, we first marks the faulty bit. Then we compare the correct bits with faulty bits (outputs). If both the outputs are same, then increment the correct counter otherwise increment fault counter.

Flowchart of Hit Probability

Following flowchart 2 shows the flow of calculation of hit probability. First we select the transistor. Then we calculate width and area ratio, according to ratio we update the POF of the circuit.

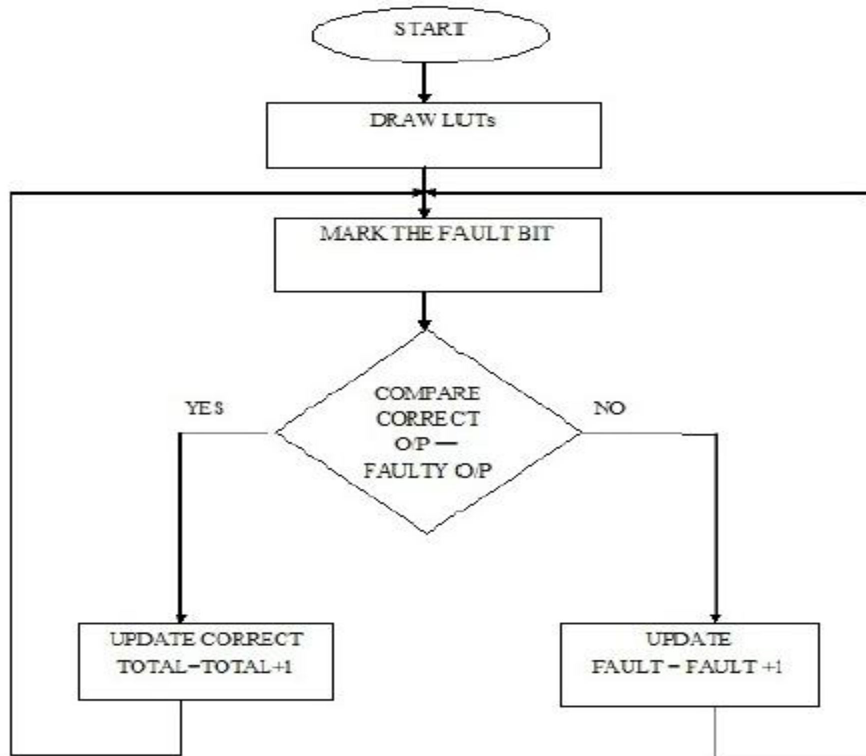

Figure.8 : Flowchart 1:Fault Detection Probability.

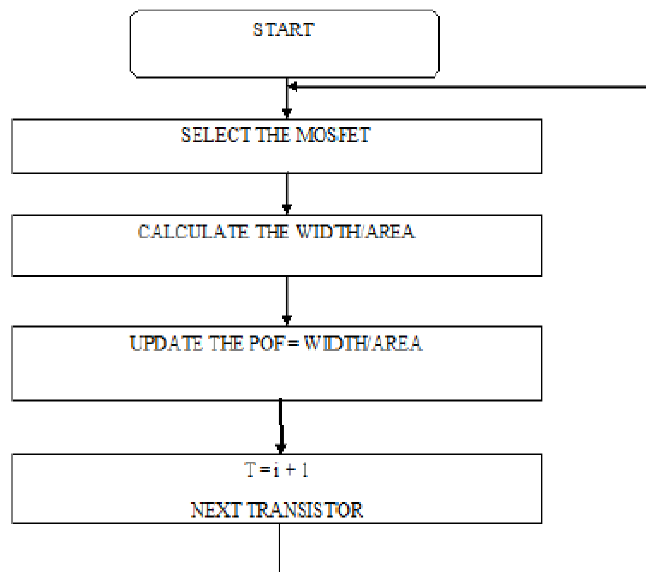

Figure.9: Flowchart 2:Hit Probability.

VII. RESULTS AND DISCUSSION

Xilinx ISE 14.7 has been used for programming. The results obtained after coding are shown below.

Result of Fault Detection Probability

- To detect propagation and excitation error due to faulty transistor, we are creating a fault bit and comparing the output for fault state.
- If the output is not matched then fault is detected and this is contributed to PoF for given bit. Trough bit we can mark the transistoras faulty or correct transistor.

Following Fig.10 shows the result for fault detection probabitily.

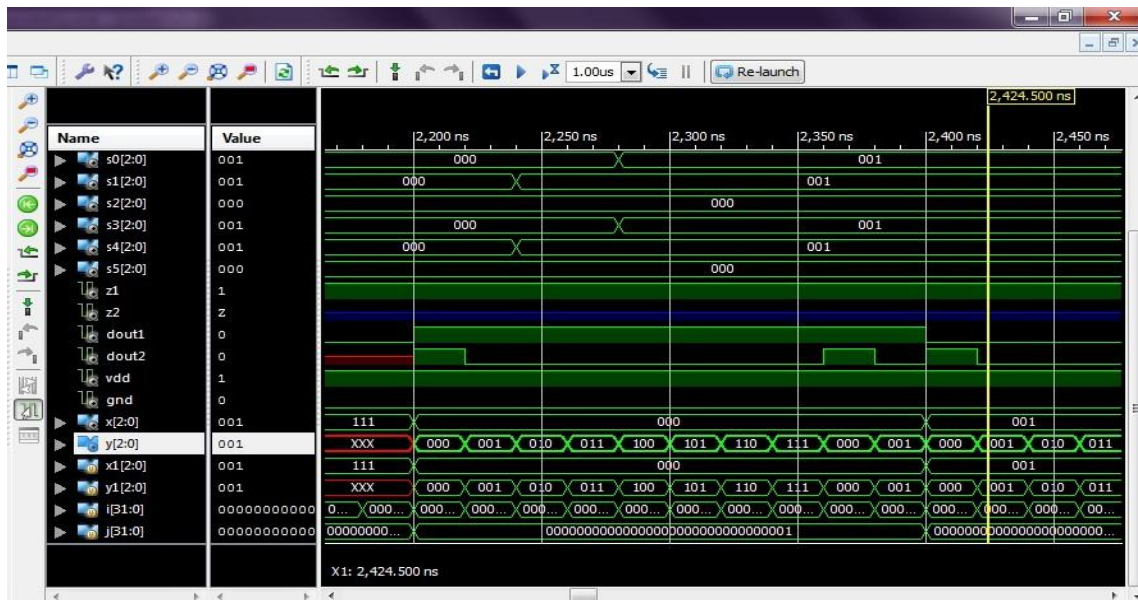

Figure.10: Result of Fault Detection Probability.

Result of Probability that Transistor j of Gate i is Hit by a Fault

The greater the transistor width/area is, the greater its hit probability is. Following Fig.11 shows the result of hit probability.

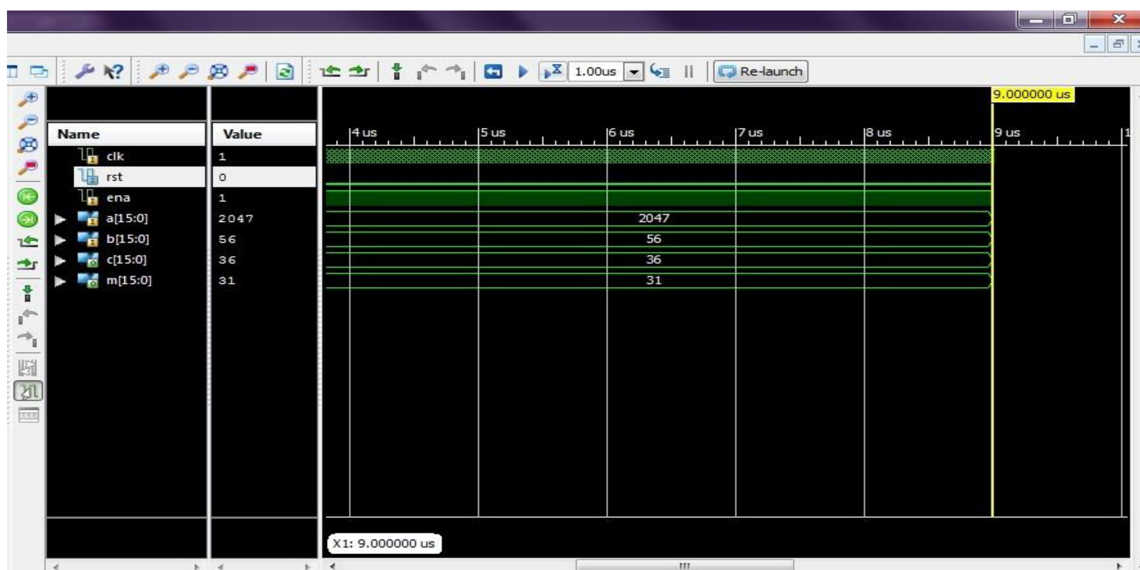

Figure.11: Result of Hit Probability.

VIII. CONCLUSION

In this paper, we have proposed an STR-based fault tolerance technique for combinational circuits. The technique can be applied to achieve a given circuit reliability or enhance the reliability of a circuit under a given area constraint. The technique is based on estimating the POF of each transistor and iteratively protecting transistors with the highest POF until the desired objective is achieved. Transistors are protected based on duplicating and scaling a subset of transistors necessary for providing the protection.

In this paper we had design a NOR and MUX circuit with extra fault transistor. This extra transistor act as a backup which save with reduce the probability of failure which may caused by manufacturing or due to stuck at fault. We had proposed two algorithms for probability detection which compensate the fault in circuit.

These algorithms assign extra transistor depend on the probability depend on the area and propagation fault. This extra transistor reduces the faults in circuit. This makes our system extra sufficient and more durable which automatically reduce the probability of failure due manufacturer error or aging error.

REFERENCES

[1] Ahmad T. Sheikh, Aiman H. El-Maleh, Muhammad E. S. Elrabaa, Sadiq M. Sait,"A Fault Tolerance Technique for Combinatonal Circuits Based on Selective Transistor Redundancy", in IEEE Transactions on Very Large Scale Integration Systems, 2016.

[2] Bolan Su, Shijian Lu, and Chew Lim Tan, Senior Member, "Robust Document Image Binarization Technique for Degraded Document Images",in IEEE Transactions On Image Processing, Vol. 22, No. 4, April 2013

[3] J.R. Heath, P.J. Kuekes, G.S. Snider, and R.S. Williams, "A defect tolerant computer architecture: Opportunities for nanotechnology", Science, vol.280, no. 5370, pp. 1716-1721, 1998.

[4] N. Cohen, T. S. Sriram, N. Leland, D. Moyer, S. Butler, and R. Flat- ley,Soft error considerations for deep-submicron CMOS circuit applications,in Proc. Int. Electron Devices Meeting (IEDM), Dec. 1999, pp. 315318.

[5] P. E. Dodd and L. W. Massengill, Basic mechanisms and modeling of single-event upset in digital microelectronics, IEEE Trans. Nucl. Sci.,vol. 50, no. 3, pp. 583602, Jun. 2003.

[6] J. F. Ziegler et al., IBM experiments in soft fails in computer electronics (19781994), IBM J. Res. Develop., vol. 40, no. 1, pp. 318, Jan. 1996.

[7] R. C. Baumann, Radiation-induced soft errors in advanced semiconductor technologies, IEEE Trans. Device Mater. Rel., vol. 5, no. 3, pp.305316, Sep. 2005.

[8] P. Shivakumar, M. Kistler, S. W. Keckler, D. Burger, and L. Alvisi, Modeling the effect of technology trends on the soft error rate of combinational logic, in Proc. Int. Conf. Dependable Syst. Netw. (DSN), 2002, pp. 389398.

[9] T. Karnik and P. Hazucha, Characterization of soft errors caused by single event upsets in CMOS processes, IEEE Trans. Dependable Secure Comput., vol. 1, no. 2, pp. 128143, Apr./Jun. 2004.

[10] J. Henkel et al., Reliable on-chip systems in the nano-era: Lessons learnt and future trends, in Proc. 50th ACM/EDAC/IEEE Annu. Design Autom. Conf. (DAC), May/Jun. 2013, pp. 110.

[11] S. Rehman, F. Kriebel, M. Sha_que, and J. Henkel, Reliability driven software transformations for unreliable hardware, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 33, no. 11, pp. 15971610, Nov.2014.

[12] J. von Neumann, Probabilistic logics and the synthesis of reliable organisms from unreliable components, Autom. Stud., vol. 34, pp. 4398,1956.

[13] J. Han, Fault-tolerant architectures for nanoelectronic and quantum devices, Ph.D. dissertation, Dept. Appl. Sci., Delft Univ. Technol., Delft, The Netherlands, 2004.

[14] D. P. Siewiorek and R. S. Swarz, Reliable Computer Systems: Design and Evaluation, 3rd ed. Natick, MA, USA: A. K. Peters, Ltd., 1998.

[15] A. Namazi and M. Nourani, Reliability analysis and distributed voting for NMR nanoscale systems, in Proc. 2nd Int. Design Test Workshop (IDT), Dec. 2007, pp. 130135.

[16] M. Hamamatsu, T. Tsuchiya, and T. Kikuno, On the reliability of cascaded TMR systems, in Proc. IEEE 16th Paci_c Rim Int. Symp. Dependable Comput. (PRDC), Dec. 2010, pp. 184190.

[17] A. H. El-Maleh and F. C. Oughali, A generalized modular redundancy scheme for enhancing fault tolerance of combinational circuits, Microelectron. Rel., vol. 54, no. 1, pp. 316326, 2014.

[18] A. H. El-Maleh and A. S. Al-Qahtani, A finite state machine based fault tolerance technique for sequential circuits, Microelectron. Rel., vol. 54, no. 3, pp. 654661, 2014.

[19] K. Mohanram and N. A. Touba, Partial error masking to reduce soft error failure rate in logic circuits, in Proc. 18th IEEE Int. Symp. Defect Fault Tolerance VLSI Syst., Nov. 2003, pp. 433440.

[20] A. K. Nieuwland, S. Jasarevic, and G. Jerin, Combinational logic soft error analysis and protection, in Proc. 12th IEEE Int. On-Line Test. Symp. (IOLTS), Jul. 2006, p. 6.

[21] C. Zoellin, H. Wunderlich, I. Polian, and B. Becker, Selective hardening in early design steps, in Proc. 13th Eur. Test Symp., May 2008, pp. 185190.

[22] Y. Dotan, N. Levison, and D. Lilja, Fault tolerance for nanotechnology devices at the bit and module levels with history index of correct computation, IET Comput. Digit. Techn., vol. 5, no. 4, pp. 221230, Jul. 2011.

[23] Q. Zhou and K. Mohanram, Gate sizing to radiation harden combinational logic, IEEE Trans. Comput.-Aided Design Integr., vol. 25, no. 1, pp. 155166, Jan. 2006.

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.

Jyoti M Gadekar. “Fault Tolerance Systems for Combinational Circuits.” International Journal of Computational Engineering Research (IJCER), vol. 7, no. 9, 2017, pp. 11–19.