The Impact of Production Defects on the Soft-Error Tolerance of Hardened Latches

Stefan Holst, Ruijun Ma, and Xiaoqing Wen

Kyushu Institute of Technology, Iizuka, 820-8502, Japan

***Abstract*—As modern technology nodes get more and more susceptible to soft-errors, various hardened latch cells have been proposed. The added redundancy used to tolerate transient faults in the field at the same time reduces the test coverage of cell-internal production defects. Moreover, the test escapes reduce the soft-error tolerance of the defective latches. This work introduces a new soft-error vulnerability metric called *Post Test Vulnerability Factor* that correctly measures the added vulnerability to transient faults such as particle strikes caused by undiscovered production defects within hardened latches.**

Keywords*–*soft-error vulnerability, test escapes, latent defects

1. Introduction

Advanced technology nodes have become more and more vulnerable to soft-errors caused by cosmic rays, alpha particles and neutron interactions even at the sea level [1–4]. In a logic circuit, memory elements such as latches are most vulnerable to particle strikes as they may cause single-event upsets at any time while a value is stored. Extensive research has been conducted to develop latches that can tolerate many of these particle impacts without loosing their correct state [5–12].

A common way to harden latches against soft-errors is to add redundant feedback loops that allow the latch to detect and correct state changes caused by a particle strike. Figure 1 shows such a hardened latch [7]. The latch has two independent feedback loops FL1 and FL2. Whenever one of these loops is hit by a particle, the change in state is corrected via the information stored in the other loop. Now suppose a bridge defect is introduced between D and INT1a during production. A SPICE simulation in Figure 2 shows that this defective latch still works as expected and the defect cannot be observed. However, if a particle hits the defective latch on net INT3, it is not able to correct the impact on FL2, because FL1 is compromised by the production defect. Consequently, the defective latch suffers from single-event upsets where a defect-free latch does not.

This simple experiment demonstrates several important points:

- Production defects within hardened latches may be untestable by common logic and delay tests. A lower defect coverage may lead to over-estimation of production quality and reliability, and may compromise yield learning.
- Certain production defects in hardened latches reduce their soft-error tolerance. Hardened latches that contain production defects may not perform as expected in high radiation environments.
- There are production defects that at the same time compromise the soft-error tolerance and are not detectable during production test. The actual soft-error tolerance

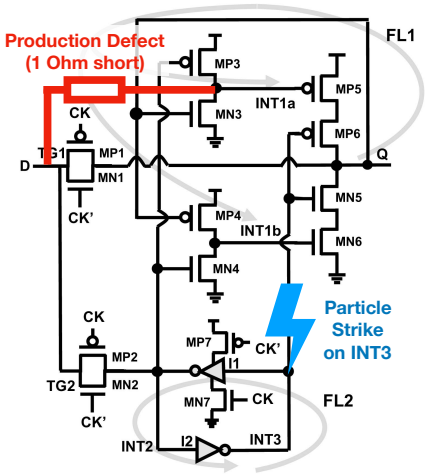

Figure 1. A hardened latch (HiPeR [7]) with D and N2 being shorted during production and INT3 being hit by a particle in the field.

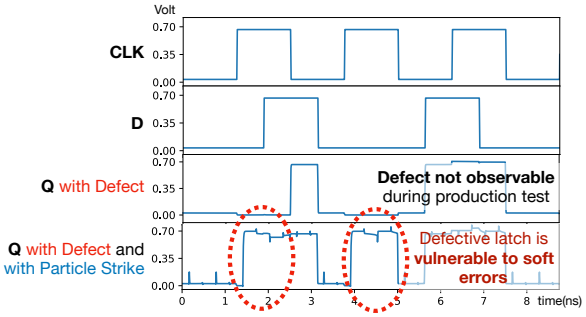

Figure 2. SPICE simulation results show that defect is not observable during production test, but renders the latch vulnerable to soft-errors.

978-1-5386-3728-9/18/$31.00 ©2018 IEEE

of hardened latches after production is therefore unknown.

To the best of our knowledge, this work is the first to analyze in detail the relations between hardened latch designs, production defects, testability, and soft-error tolerance. This paper is organized as follows: Section 2 describes the background and related work in soft-error tolerant design in relation to production defects and testing. In Section 3, we introduce a new metric that quantifies testability and soft-error tolerance of hardened latches affected by production defects. Section 4 introduces a simple procedure to calculate the introduced metric for a given latch design, fault model, and test. Section 5 applies the new metric to common hardened latch designs and demonstrates that the new metric uncovers large differences among the latch implementations. Section 6 concludes the paper.

2. Background

There are two common metrics to characterize standard cells regarding testability and soft-error tolerance, namely defect coverage (DC) and soft-error vulnerability (SEV).

Defect coverage (DC) describes the portion of all potential cell-internal production defects that are testable in a typical production test setting [13–17]. A high defect coverage is desirable as undiscovered (latent) defects often get more and more serious during operation and cause chips to fail eventually in the field. As soon as soft-error tolerance measures are introduced, defect coverage decreases significantly [18]. Typical production tests consist of a series of structural logic, timing, and functional tests. This work is concerned with latch cells that are directly observable via scan chains during structural test. We therefore assume that any erroneous value at the output of a latch cell will eventually fail the production test.

The second common metric to characterize radiation-hardened logic is soft-error vulnerability (SEV) [1, 19]. The soft-error vulnerability describes the probability that a transient fault (e.g. a particle strike) on some cell-internal structure leads to a noticeable effect (a soft-error) in the state or at the outputs of the latch. SEV is similar to the *time vulnerability factor* or *time derating* presented in [19] in that it provides a factor for calculating the soft-error rate of a latch in a given radiation environment. However, in the context of this work, SEV is used to reason about the vulnerability of the internal structures of the latch and not about the vulnerability over time. The vulnerability of a cell-internal structure to particle impacts depends on many factors such as the angle of the impact [20], and threshold voltage variations [21]. Soft-error rates can be measured directly by using radiation sources [3], or it can be estimated by structural analysis and fault simulation [22, 23]. A combination of irradiation experiments and hardware-based fault injection has also been used to characterize the resilience on complex processors [24]. In order for a soft-error to disrupt the operation of a system, the faulty output of the affected latch must propagate to the next state of the circuit or to the outputs. The probability of a system-level error is captured in the *architectural vulnerability factor* or *logic derating* [19] and is beyond the scope of this work. The vulnerability metric presented below is only concerned with the latch cells themselves.

All above methods are used for characterizing the soft-error resilience of the used technology or the designs. They are clearly not practical for characterizing individual chips during volume production. Considering the combination of soft-error tolerance and production test, some works propose to reduce hardware overhead by reusing enhanced scan infrastructure for soft-error hardening [25–27] or integrating scan design with error-correcting codes [28]. So far, no previous work has considered the interplay between production defects, the added redundancy of hardened latches, and the residual soft-error tolerance of latches with untestable defects.

3. Soft-Error Vulnerability Metric

3.1. Cells, Defects and Test

Let c be a standard cell of a latch, and d be a production defect. Let $D(c)$ be a set of production defects the cell c can be affected by. A cell c may be affected by at most one defect d, and we note the defective cell as c_d. Let $P_D : D(c) \rightarrow (0 \ldots 1]$ be a probability density function that gives the relative occurrence probability of the defects given that the cell is defective. By definition, we have $\sum_{d \in D(c)} P_D(d) = 1$. The set $D(c)$ and the probabilities P_D are determined by the used defect model, which can be chosen freely from the literature [13, 14]. This modeling does not assume a single defect or single fault in a latch. It is easy to model defects that affect multiple structures within the cell at once or defects that lead to various cell-internal timing or bridging faults as elements of $D(c)$.

After production of the cell, we assume a simple pass-fail test modeled by a characteristic function $t : C \rightarrow \{1, 0\}$ with C being the set of all instances of a cell. For any production defect $d \in D(c)$, the characteristic function evaluates to $t(c_d) = 1$, if the cell c with defect d passes the production test, and to $t(c_d) = 0$; otherwise. Clearly, the test passes always for the defect-free cell: $t(c) = 1$.

The defect coverage of the test t is:

$$\mathrm{DC}(c, t) = \sum_{d \in D(c)} P_D(d) \cdot (1 - t(c_d))$$

If the test t fails ($t(c_d) = 0$) for all possible defects, then the defect coverage $\mathrm{DC}(t)$ is 1. If the test does not detect all possible defects, $\mathrm{DC}(t)$ will be reduced by the probability that the cell contains an untested defect.

3.2. Soft-Errors and Vulnerability

Let $F(c)$ be a set of transient faults that may hit the cell c during operation. Similar to the definition of $D(c)$, we assume that a cell is hit by a single transient $f \in F(c)$ at a time, but depending on the underlying fault model, particles may hit multiple structures in the cell. Let $P_F : F(c) \rightarrow (0 \ldots 1]$ be the probability density function that gives the relative occurrence probability of particular transient fault given that the cell is hit by a particle. Again, we have $\sum_{f \in F(c)} P_F(f) = 1$. The fault set $F(c)$ and probabilities P_F are determined by the chosen transient fault model, e.g. [7]. This modeling does not put any restrictions on the number of cell-internal structures being hit by a particle. As multiple-node-upsets are getting more and more common in modern technology nodes, they can be easily added as elements to $F(c)$ with their corresponding probabilities in P_F.

The vulnerability of a latch cell for a soft-error can be defined as a characteristic function $v : C \times F \rightarrow [0 \ldots 1]$. This function gives for a cell $c \in C$ and a transient fault $f \in F(c)$ the probability that the output of the cell shows an erroneous value.

The overall vulnerability of a latch cell c is measured by:

$$\mathrm{SEV}(c) = \sum_{f \in F(c)} P_F(f) \cdot v(c, f)$$

The soft-error vulnerability is the probability that a latch cell shows an erroneous output (a soft-error) given that the cell is hit by a particle.

3.3. Post-Test Vulnerability

In previous works, defect coverage $\mathrm{DC}(t)$ and soft-error vulnerability $\mathrm{SEV}(c)$ have only been considered independently. However, whenever the defect coverage is less than 1, some defective cells c_d pass the test ($t(c_d) = 1$). In these cases, the actual particle strikes do not happen to the original defect-free cell c, but to the defective cell c_d that escaped the test t. Clearly, the vulnerability to some transient faults f can change if some defect d is present: $v(c, f) \neq v(c_d, f)$. The new soft-error vulnerability metric is called *post test vulnerability factor* (PTVF) and takes the probabilities of the test-escaping defects into account:

$$\mathrm{PTVF}(c, t) = \frac{\sum_{d \in D(c)} P_D(d) \cdot t(c_d) \cdot \mathrm{SEV}(c_d)}{1 - \mathrm{DC}(c, t)}$$

The PTVF gives the probability of a soft-error of the cell given that the cell has a production defect and is hit by a transient fault. It depends both on the production defect test coverage and the soft-error vulnerability of the test escapes. In case of a complete defect coverage, $\mathrm{DC}(c, t) = 1$, we define $\mathrm{PTVF}(c, t) = 0$. If all defects $d \in D(c)$ that escape the test ($t(c_d) = 1$) do not affect the hardness of the latch cell ($\mathrm{SEV}(c_d) = 0$), then the $\mathrm{PTVF}(c, t)$ is 0 as well. The PTVF is independent from the overall defect rate and the overall soft-error vulnerability. It is therefore useful for characterizing and comparing latch cell designs and their test procedures.

Let $Q(c)$ be the product quality of the cell c, i.e. the probability that a produced cell is free of any defect after production test. The product quality can be estimated based on the yield Y of the cell and the defect coverage $\mathrm{DC}(t)$ by the well-known Williams Brown formula [29]: $Q(c) = Y^{1-\mathrm{DC}(c,t)}$. Note, that the product quality is usually less than 100% and reduces even further with the lower defect coverage observed in hardened latches. Since the yield Y of a single cell is very close to 1, the product quality for a single cell $Q(c)$ will be very close to 100%. Still, the effect on the overall product quality of the chip (Q) is considerable with a large number n of instances of the cell: $Q = Q(c)^n$. With the estimate on product quality, the PTVF can be used to calculate the *effective soft-error vulnerability* ($\mathrm{SEV}_{\mathrm{eff}}$) of a hardened latch after production:

$$\mathrm{SEV}_{\mathrm{eff}}(c, t) = Q(c) \cdot \mathrm{SEV}(c) + (1 - Q(c)) \cdot \mathrm{PTVF}(c, t)$$

The lower the product quality Q, the more the effective soft-error vulnerability of the latch cell is determined by the PTVF instead of the classic soft-error vulnerability $\mathrm{SEV}(c)$ for the defect-free case. The effective soft-error vulnerability for a single cell c is very close to its $\mathrm{SEV}(c)$, because $Q(c)$ is close to 100%. But again, the overall effect on the system cannot be ignored since the chip contains many instances of c.

4. Calculating the PTVF

To calculate the PTVF, a series of SPICE simulations are performed. The necessary inputs to calculate the PTVF are the latch cell design c as SPICE netlist, the set of production defects $D(c)$ and their probabilities P_D, the set of transient faults $F(c)$ and their probabilities P_F, and the test t. Each defect $d \in D(c)$ must be injectable into the SPICE netlist (e.g. by inserting additional components like resistances between nets). Each transient fault $f \in F(c)$ must be injectable during transient analysis e.g. by using additional current sources. The test t is given in form of a set of measurement times, expected values, and tolerances at the output of the latch. The details of these measurements are derived from the test architecture and the design-for-test measures used during production test, which are beyond the scope of this work. Without loss of generality, we assume a latch cell to be exhaustively tested with all possible combinations of inputs and state. A defect in the latch is considered to be detected, if the latch outputs a wrong logic value for longer than a quarter of a clock cycle. Each SPICE simulation is a transient analysis of a few clock cycles and varying inputs similar to the inputs shown in Figure 2. A particle strike is considered to lead to a soft-error, whenever the output of the latch has settled on a wrong logic value after the injected current surge.

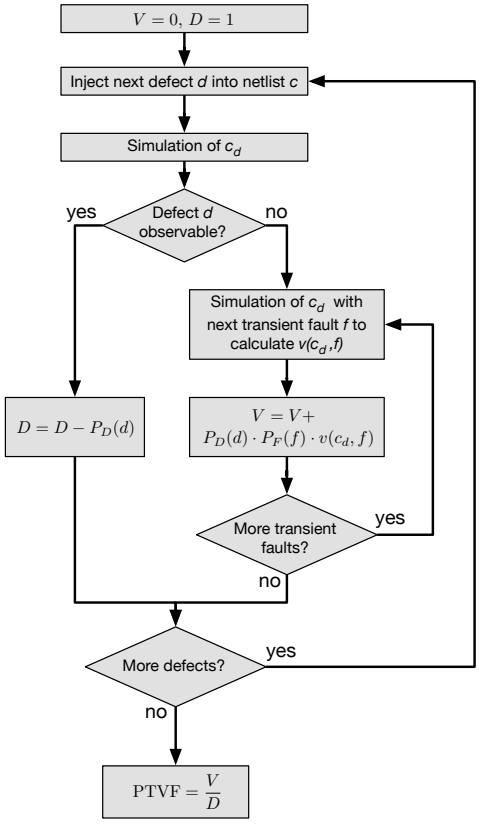

Figure 3. Flow for calculating PTVF.

The overall flow is shown in Figure 3. After initialization of two variables $V = 0$ and $D = 1$ for accumulating the results, a production defect $d \in D(c)$ is injected into the original SPICE netlist to generate a model for c_d. The new netlist is simulated and the output of the defective latch is checked for erroneous values. If the defect d is observable ($t(c_d) = 0$), D is updated to reflect the defect coverage. The PTVF will not be changed, so the loop continues with the next production defect. If the defect d is not observable, all transient faults $f \in F(c)$ are injected into the model c_d and for each fault, $v(c_d, f)$ is calculated. If the model c_d is vulnerable to a transient fault f, $v(c_d, f)$ will be positive. The PTVF is increased by the combined probability of the defect, the transient fault occurring, and the fault leading to a soft-error of the latch cell: $P_D(d) \cdot P_F(f) \cdot v(c_d, f)$.

Calculating the PTVF calls for a large number of SPICE simulations, since each latch is simulated with all possible combinations of production defects and transient faults. However, each of the simulations is rather quick since only a few clock cycles and a single cell. Furthermore, most SPICE simulations are independent and can therefore be executed in parallel.

5. Experimental Results

In this section, we demonstrate how the PTVF can be used for characterizing hardened latch designs.

All latches have been implemented as SPICE netlists. The 16nm predictive technology model [30] is used for the transistors and the supply voltage is 0.7V. Most published hardened latches do not provide actual standard cell layouts. To get consistent results for all latches, we therefore did not consider layout parasitics, layout-based defect models, or parametric variations in these experiments.

The set of production defects $D(c)$ contains transistor open defects and shorts between internal nets of the latch. For the transistor open defects, a 10MΩ resistor is inserted at the source connection of each transistor of the latch cell c. Obviously, the number of different open defects equals the number of transistors in the cell. For the bridge defects, the set of nets are first classified into external and internal nets. External nets are the connections to the outside and typically include GND, VDD, CLK, D, and Q. Internal nets are all the remaining nets without direct outside connections. Since shorts between two external nets (e.g. between VDD and GND) are always detected, the set of shorts included in $D(c)$ are all shorts between either two internal nets or an internal net with an external net. A short is injected into the SPICE netlist using a 1Ω resistor between the two affected nets.

Since the goal of these experiments is to demonstrate the PTVF metric, we chose rather simplistic models for latch implementation, defects, and particle strikes in order to obtain results that are easily verifiable. Clearly, to obtain more realistic absolute PTVF numbers for a latch implementation, one needs to consider layout parasitics, realistic defect models, test architecture as well as parametric variations. Still, we believe that the simple models used here are sufficient to demonstrate the workings and the usefulness of the PTVF metric. Furthermore, the simple models can be easily substituted by more realistic ones and the PTVF is calculated in the same way.

Table 1 shows some basic statistics of the latch cells considered in our experiments. The columns show the latch name, the number of transistors, the number of external nets, the number of internal nets and the number of production defects, respectively. The *Standard*-latch is a simple, non-hardened latch design used for comparison, *TMR* is a standard triple-modular redundancy implementation consisting of three standard latches and a voter. The remaining latches are various published hardened latches and their variants.

The test conditions are as follows. Between the ideal power supply and the cell, a 10Ω resistor is inserted to allow for supply voltage drop in case of excessive power consumption of a defective cell. The slopes of the input signals like CLK and D are 10ps, and soft errors are injected as a short (5ps) pulse of 0.1mA or −0.1mA at an internal net of the latch. For the sake of easy reproducibility of these experiments,

TABLE 1. LATCH CELL STATISTICS.

latch	*FETs*	*extNets*	*intNets*	*defects*
Standard	12	5	5	47
TMR	36	5	15	216
HiPeR [7]	18	5	9	99
ISEHL [8]	24	5	15	204
FERST [6]	28	5	14	189
HLR [12]	24	5	13	167
HLR-CG1 [12]	18	5	7	74
HLR-CG2 [12]	24	5	16	224

we assigned equal probability to all production defects and all transient faults.

Table 2 shows the results for the defect coverage DC and classic soft-error vulnerability SEV. The table is sorted by production defect coverage. As expected, the standard latch has the highest defect coverage among all latches. The hardened latches show lower defect coverage because of the added redundancy with the TMR latch showing the lowest coverage because of its rather large size. This means that hardened latches are much more likely to pass production test despite having cell-internal production defects. All hardened latches are able to tolerate every transient fault (therefore showing a $\mathrm{SEV} = 0$) if they are defect-free. Just the standard latch shows, as expected, a soft-error vulnerability of 80%. With this common metric for measuring soft-error vulnerability, all hardened latches show the same performance.

TABLE 2. LATCH CELL DEFECT COVERAGE AND SOFT-ERROR VULNERABILITY.

latch	DC	SEV
Standard	89.4%	80.0%
FERST [6]	63.5%	0.0%
ISEHL [8]	52.5%	0.0%
HiPeR [7]	50.5%	0.0%
HLR [12]	49.1%	0.0%
HLR-CG1 [12]	43.2%	0.0%
HLR-CG2 [12]	32.1%	0.0%
TMR	21.3%	0.0%

Table 3 shows the post test vulnerability factor (PTVF) for all latches, sorted by increasing value. It can be seen that the standard latch has the highest possible PTVF of 100%, because all test escapes are vulnerable to all injected transient faults. All hardened latches show a PTVF ranging from about 54% to 82%. This means that if a latch is defective from the time of production and the production test does not catch the defect, its soft-error tolerance is indeed greatly reduced.

There are significant differences in the PTVF of different hardened latches. While the classic soft-error vulnerability measure report 0% for all hardened latches, we can see from the PTVF that the HLR-CG1 latch will tolerate more soft-errors than all the other hardened latches when production defects and test escapes are taken into account. The worst performing hardened latch is the TMR. If a production defect escapes the test in this latch, its soft-error vulnerability increases from 0% to more than 80%. This is again expected, because TMR is only effective in masking single errors. Once a defect is present, an additional transient fault is very likely to change the voting result. It is common practice to test the individual modules of a TMR structure separately in order to avoid this problem. This was not done in these demonstration experiments, so the low defect coverage and the high PTVF correctly indicate this shortcoming.

TABLE 3. POST TEST VULNERABILITY FACTOR FOR ALL LATCH CELLS.

latch	PTVF
HLR-CG1 [12]	54.8%
HLR [12]	70.5%
HiPeR [7]	71.5%
HLR-CG2 [12]	71.7%
ISEHL [8]	76.4%
FERST [6]	79.7%
TMR	81.8%
Standard	100.0%

6. Conclusions

We have shown for the first time that the added redundancy used to tolerate transient faults in hardened latches at the same time reduces the test coverage of cell-internal production defects. Moreover, the test escapes reduce the soft-error tolerance of the defective latches. This work introduced a new soft-error vulnerability metric called *Post Test Vulnerability Factor* (PTVF) that correctly measures the added vulnerability to transient faults such as particle strikes caused by undiscovered production defects within hardened latches. The PTVF of hardened latches can be easily calculated with a series of SPICE simulations. A characterization of various common latches showed large differences in their PTVF, which underlines the usefulness of the new metric to compare hardened latch designs.

In the future we plan to investigate new latch designs and design-for-test methods that optimize for low PTVF in order to improve the effective soft-error tolerance of produced chips.

Acknowledgments

This work was supported in part by JSPS Grant-in-Aid for Scientific Research (B) #17H01716 and #25280016 as well as JSPS Grant-in-Aid for Scientific Research on Innovative Areas #15K12003.

References

[1] R. Baumann, "Soft errors in advanced computer systems," *Design & Test of Computers, IEEE*, vol. 22, no. 3, pp. 258–266, May-June 2005.

[2] ——, "Radiation-induced soft errors in advanced semiconductor technologies," *IEEE Transactions on Device and Materials Reliability*, vol. 5, no. 3, pp. 305–316, 2005.

[3] S. Mitra, N. Seifert, M. Zhang, Q. Shi, and K. S. Kim, "Robust system design with built-in soft-error resilience," *Computer*, vol. 38, no. 2, pp. 43–52, Feb 2005.

[4] T. Karnik and P. Hazucha, "Characterization of soft errors caused by single event upsets in cmos processes," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 2, pp. 128–143, April 2004.

[5] M. Omana, D. Rossi, and C. Metra, "Latch susceptibility to transient faults and new hardening approach," *IEEE Transactions on Computers*, vol. 56, no. 9, pp. 1255–1268, Sept 2007.

[6] 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 Digital Techniques*, vol. 3, no. 3, pp. 289–303, May 2009.

[7] M. Omana, D. Rossi, and C. Metra, "High-performance robust latches," *IEEE Transactions on Computers*, vol. 59, no. 11, pp. 1455–1465, Nov 2010.

[8] H. Liang, Z. Wang, Z. Huang, and A. Yan, "Design of a radiation hardened latch for low-power circuits," in *Proc. 23rd IEEE Asian Test Symposium*, Nov 2014, pp. 19–24.

[9] Z. Huang, H. Liang, and S. Hellebrand, "A high performance seu tolerant latch," *Journal of Electronic Testing*, vol. 31, no. 4, pp. 349–359, Aug 2015.

[10] S. Krishnamohan and N. R. Mahapatra, "Analysis and design of soft-error hardened latches," in *Proc. 15th ACM Great Lakes Symposium on VLSI*, ser. GLSVLSI '05. New York, NY, USA: ACM, 2005, pp. 328–331.

[11] Y. Komatsu, Y. Arima, T. Fujimoto, T. Yamashita, and K. Ishibashi, "A soft-error hardened latch scheme for soc in a 90 nm technology and beyond," in *Proceedings of the IEEE 2004 Custom Integrated Circuits Conference (IEEE Cat. No.04CH37571)*, Oct 2004, pp. 329–332.

[12] H. Nan and K. Choi, "High performance, low cost, and robust soft error tolerant latch designs for nanoscale cmos technology," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 7, pp. 1445–1457, July 2012.

[13] A. Jee and F. J. Ferguson, "Carafe: An inductive fault analysis tool for CMOS VLSI circuits," in *Digest of Papers. Eleventh Annual IEEE VLSI Test Symposium, 1993*, 1993, pp. 92–98.

[14] F. Hapke, W. Redemund, J. Schloeffel, R. Krenz-Baath, A. Glowatz, M. Wittke, H. Hashempour, and S. Eichenberger, "Defect-oriented cell-internal testing," in *International Test Conference (ITC)*, Nov. 2010, pp. 1–10.

[15] B. Kruseman, A. Majhi, C. Hora, S. Eichenberger, and J. Meirlevede, "Systematic defects in deep sub-micron technologies," in *2004 International Conferce on Test*, Oct 2004, pp. 290–299.

[16] S. Eichenberger, J. Geuzebroek, C. Hora, B. Kruseman, and A. Majhi, "Towards a world without test escapes: The use of volume diagnosis to improve test quality," in *2008 IEEE International Test Conference*, Oct 2008, pp. 1–10.

[17] A. Bosio, L. Dilillo, P. Girard, A. Todri-Sanial, A. Virazel, S. Bernabovi, and P. Bernardi, "An intra-cell defect grading tool," in *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, April 2014, pp. 298–301.

[18] M. Hunger and S. Hellebrand, "The impact of manufacturing defects on the fault tolerance of tmr-systems," in *2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems*, Oct 2010, pp. 101–108.

[19] H. T. Nguyen and Y. Yagil, "A systematic approach to ser estimation and solutions," in *2003 IEEE International Reliability Physics Symposium Proceedings, 2003. 41st Annual.*, March 2003, pp. 60–70.

[20] H. Zhang, H. Jiang, T. R. Assis, D. R. Ball, B. Narasimham, A. Anvar, L. W. Massengill, and B. L. Bhuva, "Angular effects of heavy-ion strikes on single-event upset response of flip-flop designs in 16-nm bulk finfet technology," *IEEE Transactions on Nuclear Science*, vol. 64, no. 1, pp. 491–496, Jan 2017.

[21] H. Zhang, H. Jiang, T. R. Assis, N. N. Mahatme, B. Narasimham, L. W. Massengill, B. L. Bhuva, S. J. Wen, and R. Wong, "Effects of threshold voltage variations on single-event upset response of sequential circuits at advanced technology nodes," *IEEE Transactions on Nuclear Science*, vol. 64, no. 1, pp. 457–463, Jan 2017.

[22] M. Zhang and N. Shanbhag, "Soft-error-rate-analysis (SERA) methodology," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 10, pp. 2140–2155, Oct. 2006.

[23] Y. S. Dhillon, A. U. Diril, and A. Chatterjee, "Soft-error tolerance analysis and optimization of nanometer circuits," in *Proceedings of the Conference on Design, Automation and Test in Europe (DATE '05)*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 288–293.

[24] P. N. Sanda, J. W. Kellington, P. Kudva, R. Kalla, R. B. McBeth, J. Ackaret, R. Lockwood, J. Schumann, and C. R. Jones, "Soft-error resilience of the IBM POWER6 processor," *IBM Journal of Research and Development*, vol. 52, no. 3, pp. 275–284, May 2008.

[25] A. Goel, S. Bhunia, H. Mahmoodi, and K. Roy, "Low-overhead design of soft-error-tolerant scan flip-flops with enhanced-scan capability," in *Proc. of Des. Automation Asia South Pacific Conf.*, 2006, pp. 665–670.

[26] T. Ikeda, K. Namba, and H. Ito, "Soft error hardened latch scheme for enhanced scan based delay fault testing," in *Proc. 22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems*, Sept 2007, pp. 282–290.

[27] P. Elakkumanan, K. Prasad, and R. Sridhar, "Time redundancy based scan flip-flop reuse to reduce ser of combinational logic," in *7th International Symposium on Quality Electronic Design (ISQED'06)*, March 2006, pp. 6 pp.–624.

[28] M. E. Imhof, H.-J. Wunderlich, and C. G. Zoellin, "Integrating scan design and soft error correction in low-power applications," in *14th IEEE International On-Line Testing Symposium*, Jul. 2008, pp. 59–64.

[29] T. W. Williams and N. C. Brown, "Defect level as a function of fault coverage," *IEEE Trans. on Computers*, vol. C-30, no. 12, pp. 987–988, Dec. 1981.

[30] Predictive technology model for spice. [Online]. Available: http://ptm.asu.edu/