Novel Transient-Fault Detection Circuit Featuring Enhanced Bulk Built-in Current Sensor with Low-Power Sleep Mode

Rodrigo Possamai Bastos, Frank Sill Torres, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode

R. Possamai Bastos[a,*] , F. Sill Torres[b], G. Di Natale[a], M. Flottes[a], B. Rouzeyre[a]

[a] *LIRMM (Université Montpellier II / CNRS UMR 5506), 161, rue Ada, 34095, Montpellier Cedex 5, France*
[b] *UFMG (Department of Electronic Engineering), 6627, Av. Antônio Carlos, 31270-010, Belo Horizonte, MG, Brazil*

Abstract

This work presents a novel circuit for detecting transient faults in combinational and sequential logic. The detection mechanism features a built-in current sensor connected to the bulks of the monitored logic. The proposed circuit was optimized in terms of power consumption and enhanced with low-power sleep-mode. In addition, a calibration method for bulk built-in current sensors is presented. Overhead results indicate an increase of only 15% in power consumption which represents an improvement of factor 7 compared to similar existing sensors.

1. Introduction

Error resilience is a drastically rising demand on integrated systems while, at the same time, the application of ultra-deep submicron technologies requires higher robustness to natural aging processes or environment sources like radiations from cosmic origin or every day material [1]. In addition to these natural phenomena, malicious fault-based attacks can be used to bypass security mechanisms of secure systems and extracting information on confidential data [2]. Both these natural or malicious phenomena on integrated circuits can induce transient effects that provoke bit-flips of stored results during the system lifetime.

Until the early 2000's, researches on transient faults focused essentially on memory elements, which were considered the system's most vulnerable circuits. Many concurrent error detection and/or correction mechanisms were proposed to mitigate soft errors induced by transient faults in memory cells. In the last decade, however, more sensitive deep-submicron technologies as well as the increasing demand for secure systems have also pushed for the development of countermeasures against transient faults in combinational parts of the circuits. These faults indeed can propagate up to storage elements and thus cause soft errors as well. On the other hand, if the transient fault does not induce any error due to an electrical, logical or latching-window masking effect, its detection is crucial all the same in secure applications since the fault itself reveals an attempt of attack.

The today's trend in efficient protections against transient faults is applying mitigation techniques at different abstraction levels of the design [3][4]. The idea behind is the avoidance of costly fault-tolerance mechanisms like triple modular redundancy, taking advantage of cheaper mitigation techniques that ensure satisfactory soft error coverage for the system's most recurrent operations. This strategy is exemplified through system's recovery schemes fired in function of the indication of concurrent error detection (CED) circuitries.

CED mechanisms implemented at transistor or gate level guarantee an early detection, as soon as the faults happen, preventing more critical failure scenarios such as the induction and propagation of multiple errors to other clock cycles, stages, or parts of the system. In case of a fault, the generated error flag is able to activate, for instance, recovery machines already implemented in modern systems for dealing with branch misprediction

* corresponding author: bastos@lirmm.fr, fax: +33 4 67 41 85 00, phone: +33 4 67 41 86 35

[3][4]. Thereby, faulty operation can be repeated in fault-free conditions, adapting the system to perform again its normal computational sequence.

This paper proposes a new low-cost CED scheme that efficiently identifies transient faults. The proposed circuit monitors transistor bulks of system's blocks such as similar existing Bulk Built-In Current Sensor (BBICS) [5][6], which we further discuss in section 2. Our solution, though, is optimized to satisfy today's need for low-power transient-fault robust systems. More precisely, to the best of our knowledge, the innovative contributions of this paper are:

- An optimization of the original BBICS's circuitry [5][6] to achieve reasonable overheads in power consumption (section 3);
- The introduction of the sleep-mode for BBICS that allows additionally energy savings when the system is on standby (section 3);
- A design method for calibrating BBICS with the capability of detecting a minimum transient-fault profile (section 4);
- An extensive transistor-level simulation-based exploration of the BBICS size limits in function of their response times and power consumptions (section 5).

2. Fundamentals

This section presents preliminary information regarding soft errors, built-In current sensors and leakage currents in nanometer technologies.

2.1. Transient faults in integrated circuits

Transient voltage variations during the lifetime of combinational or sequential circuits are defined as transient faults. The first harmful effects of transient faults are soft errors by inverting stored results of system operations (i.e. bit-flips of storage elements).

Due to the transistor shrinking and the growing communication of confidential data, soft errors can happen today even at ground level by means of perturbation events arisen from environmental or intentional sources. Examples of environment events are alpha particles released by radioactive impurities and more importantly neutrons from cosmic rays [1]. On the other hand, intentional perturbation events are usually produced by optical sources such as flashlights or laser beams [2] that can maliciously induce transient effects on secure circuits like smartcards to retrieve their secret information.

Soft errors and transient faults are also known as single event upsets (SEU) and single event transients (SET) in fault-tolerance-related fields. If provoked by malicious fault-based attacks, such circuit misbehaviors provide fundamental information for cryptanalysis methods that break security applications.

The modeling of transient faults in CMOS circuits is done by injecting a double exponential current pulse I_{fault} at the sensitive node. Thereby, the shape of the pulse can be approximated by following equation [7]:

$$I_{fault} = \frac{Q_f}{t_f - t_r}\left(e^{\frac{-t}{t_f}} - e^{\frac{-t}{t_r}}\right) \quad (1)$$

with Q_f is the charge collected due to the particle strike, t_f means the decay time of the current pulse, and t_r labels the time constant for initially establishing the ion track

2.2. Built-in current sensors detecting transient faults

Built-In Current Sensors (BICS) were initially proposed as a mechanism for detecting large increases in the current I_{DDQ} consumed by a CMOS circuit during its quiescent state, i.e. when the circuit is not switching. The mechanism allows thus testing CMOS circuits against permanent faults [8]. Further, BICS were also adapted for detecting transient faults in memory cells (i.e. bit-flips) [9][10][11][12]. Recently, efforts were made for monitoring transient faults in combinational logic as well [13]. All these techniques connect BICS to the power lines (V_{DD} and GND) of the monitored circuit to distinguish anomalous transient currents from normal currents. The today's problem is that the amplitude of transient currents induced by radiation effects or fault attacks can have the same order of currents normally generated by switching activities in combinational logic circuits. Hence, schemes monitoring power lines are very limited for detecting just small range of transient faults.

On the other hand, BICS connected to the bulks of the monitored circuit's transistors are able to detect a wide range of transient faults [5][6][14]. As Fig. 1 (a) and (b) illustrate, Bulk-BICS (BBICS) identify anomalous transient currents I_{fault} flowing through the junction between a bulk and a reversely-biased drain of a perturbed transistor (MOSFETs "off" in Fig. 1). BBICS indeed take advantage of two facts:

(1) In fault-free scenarios (i.e. $I_{fault} = 0$) the bulk-to-drain (or drain-to-bulk) current I_B is negligible even if the MOSFET is switching in function of new input stimuli;

(2) During transient-fault scenarios, I_{fault} is much higher than the leakage current flowing through the junction.

The range of detectable transient faults is easily adjustable by calibrating the size of the transistors that constitute the BBICS. Hence, schemes based on BBICS can be designed to latch a flag of fault indication for abnormal currents within a defined range that represents a risk of resulting in soft errors.

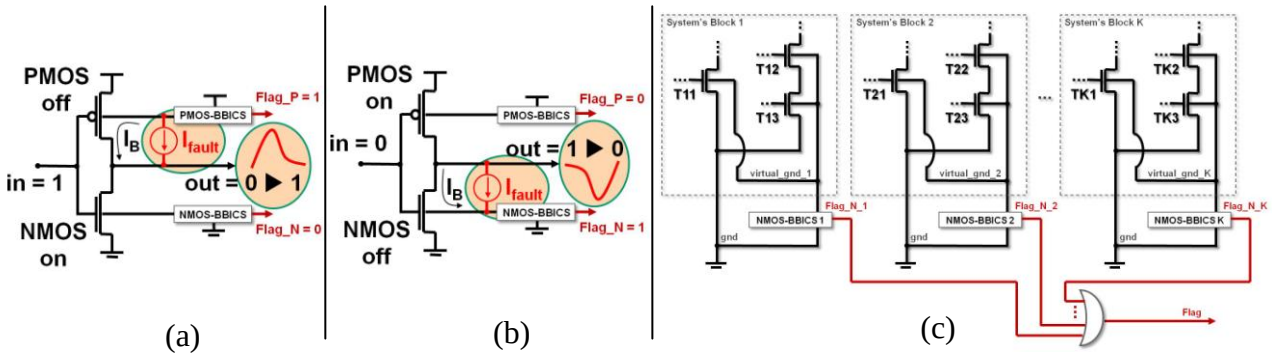

Fig. 1. The two cases of transient faults in a CMOS inverter perturbed by an anomalous current "I_{fault}" in (a) and (b), and "K" blocks of a system protected by "K" BBICS in (c)

Fig. 1 (c) summarizes the strategy for protecting system's blocks against transient faults in pull-down networks by using BBICS. An equivalent strategy must be taken for detecting transient faults in pull-up networks as well. Note that in such a strategy the connection between the monitored circuit (e.g. system's block 1) and the BBICS circuitry (e.g. NMOS-BBICS 1) is done via metal – from the body-ties of each monitored transistor (e.g. T11, T12, and T13) up to the input of the BBICS circuitry. Thereby, the peak of the anomalous transient current (i.e. the transient fault) is almost not attenuated, ensuring thus an efficient detection [14]. In fact, this very small attenuation is a function of the local distance between the struck zone of the monitored transistor and its body-tie.

The work in [3] shows that area overheads imposed by BBICS's mechanisms for protecting adder circuits can be up to 13.4 % without impact on the system's operating frequency. The costs therefore are considerably smaller than the ones due to classic CED schemes [15]. Moreover, BBICS approach is much more efficient for dealing with transient faults of long duration and multiple faults. Nevertheless, the negative issue of existing BBICS is the elevated power consumption to provide high detection sensitivity in ultra-deep submicron technologies [5][6][16].

2.3. Leakage in nanometer technologies

Ideally, CMOS cells draw no current or rather dissipate no power when idle. Unfortunately, this is not true for real cells realized in nanometer technologies. A major impact originates from sub-threshold leakage current I_{sub} which is the current between source and drain of a transistor when the device should in fact be cut off. A commonly used approximation of I_{sub} is [17]:

$$I_{sub} = a_1 \frac{W}{L} e^{\left(\frac{q}{nk_BT}\left[V_{gs} - v_{th}\right]\right)} \qquad (2)$$

with a_1 is a technology factor, W means the gate width, L labels the gate length, q corresponds to the charge of an electron, n means the sub-threshold swing coefficient, k_B is Boltzmann's constant, T labels the operating temperature, V_{gs} is the gate-source voltage, and v_{th} labels the threshold voltage. Further, the threshold voltage can be modeled with [17]:

$$v_{th} = v_{th0} + \gamma a_2 V_{sb} - \eta a_3 V_{ds} \qquad (3)$$

with v_{th0} is the zero-bias threshold voltage, γ is the body-bias coefficient, a_2 and a_3 label technology constants, η corresponds to the Drain Induced Barrier Lowering (DIBL) coefficient, V_{sb} labels the source-bulk voltage, and V_{ds} is the drain-source voltage.

3. Sleep-mode improved bulk built-in current sensor

The circuit of our Sleep-mode Improved Bulk Built-In Current Sensor (SIBBICS) is presented in Fig. 2 (a). If the mode of operation is identical to the original BBICS circuit [6] shown in Fig. 2 (b), our structure is optimized in such a way that the power consumption could be largely reduced. The following subsections detail the basic structure and the low-power features of our proposed scheme.

3.1. Basic structure

BBICS circuits in Fig. 2 are designed for monitoring NMOS bulks in pull-down networks, and thus they represent the blocks NMOS-BBICS in Fig. 1 (c). W_{min} represents the minimum diffusion width of the transistors, L_{min} is the minimum channel length, and design factors X and Y are used for calibrating the sensors (see section 4).

The PMOS-BBICS structures for monitoring pull-up networks are the complement counterparts of the schemes in Fig. 2. For the sake of simplicity, the similar illustrations and behaviors of PMOS-BBICS are omitted in this section, although their results have been also taken into account in analysis of section 4 and 5.

(a) "sibbics_esref2012" (b) "bbics_tns2008"

Fig. 2. The proposed NMOS sleep-mode improved BBICS circuit in (a) and the original NMOS-BBICS version [6] in (b)

The NMOS-BBICS's basic structure in Fig. 2 is composed of a latch (transistors 5, 6, 7, and 8) that is responsible for amplifying the anomalous transient currents coming from the bulk "NMOS_Bulk" of the monitored block (e.g. "virtual_ gnd_1" of system's block 1 in Fig. 1 (c)). Higher gain of amplification is obtained by increasing factors X and Y, hence higher BBICS's sensitivity in detecting transient faults is also determined in terms of these design factors.

BBICS's latch has, moreover, the function of memorizing a flag in case of a transient fault within a defined current range – i.e. "Flag_N" in Fig. 2 keeping V_{DD} level. On the other hand, as soon as the flag of fault is processed by higher instances of the system, BBICS's latch must be reset (through the input "Reset" in Fig. 2) to detect other transient faults.

3.2. Low-power features

Previous subsection highlights that growing factor X of Fig. 2's transistors 6 and 8 allows improving the BBICS sensitivity in detecting transient faults. However, it also contributes considerably to the increase of static power consumption, which is today responsible for up to 50% of the power dissipation of systems based on ultra-deep submicron technologies [19].

In fact, if higher BBICS sensitivity is desired, the sensor amplification has to be increased by higher X, i.e. greater diffusion widths and decreased v_{th} of transistors 6 and 8. As consequence, lower v_{th} makes possible "Flag_N" switches (from GND to V_{DD} level) with lower amplitudes of anomalous transient currents on "NMOS_bulk". The sensor is thus able to detect smaller profiles of transient faults (I_{fault} from section 2) that propagate from the "NMOS_bulk" (through transistor 2) to the node "Flag_N". On the other hand, following from equation (2), lower v_{th} results in considerably higher I_{sub}, and thus greater static power consumption.

One could argue that V_{gs} of transistors 6 and 8 are zero in fault-free condition, and then from equation (2) I_{sub} would be negligible. However, we have to consider that there is a very small voltage drop on nodes "Flag_N" and "node1" (complement) due to transistor 5 and 7, which act as high ohmic transistors (large channel lengths), creating an offset on V_{gs} of transistors 6 and 8. In addition, a small offset is also induced on V_{sb} of monitored transistors (e.g. T11, T12, and T13 in Fig. 1 (c)), and thus, from (3) and (2), their v_{th} are slightly lower, and their I_{sub} are higher.

Our solution for reducing this static power consumption is introducing transistor 9 such as illustrated in Fig. 2 (a). It allows the utilization of a sleep-mode when the system is left on standby. Transistor 9 is, in this case, set "on", making a less resistive path between the node "NMOS_bulk" and GND. Consequently, V_{gs} of transistors 6 and 8 and V_{sb} of monitored transistors approach zero, I_{sub} becomes much lower, and thus the static power consumption is drastically reduced.

Furthermore, based on simulation experiments by using a 32-nm CMOS technology [18], we identified that the costly transistors 9, 10, and 11 from original BBICS in Fig. 2 (b) are not necessary to efficiently and quickly detect short and long duration transient faults.

4. Method for calibrating bulk built-in current sensors

The previous section defines the two factors X and Y in Fig. 2 that allow calibrating the amplification of the anomalous transient current, and thus, adjusting the BBICS sensitivity in detecting transient faults. This section defines a calibration method that searches, at design time and in function of X, for the smallest and the largest Y able to detect a minimum transient-fault profile (I_{fault} in section 2).

In order to find these factors Y_{max} and Y_{min}, several sensor versions are designed in function of different values for Y and X. Transistor-level simulations are performed with the injection of a single transient fault. Firstly, for a determined X, if the simulation result for a chosen value Y shows that a flag is not latched (i.e. the transient fault could not be detected), it can be concluded that the chosen Y is lesser than Y_{min}. Then, greater amplification is required and another higher Y must be tested up to a simulation result illustrating a sensor version that detects

the fault. In contrast, if the simulation result shows that a flag is always latched even before the fault occurrence, the sensor is not capable of identifying a fault, and the chosen value Y is greater than Y_{max}. Then, other lower Y must be tested to search a value that makes a good detection sensor. This calibration method, thus, allows finding, for any technology, the optimal BBICS design factors within a range between Y_{max} and Y_{min}.

The definition of the smallest transient-fault profile I_{fault} that the sensor must be capable of detecting is given in function of a chosen reasonable minimum amplitude and duration. A minimum profile must be able to propagate without masking through a combinational logic and result in soft error (i.e. a bit-flip of a storage element). A larger profile than the smallest chosen one will be then also detectable since BBICS are capable of amplifying and latching its higher and longer induced voltages. Evidently, the largest profile of transient fault is limited by the highest current that does not cross the technology specification for causing permanent effects on the circuit.

The shortest durations of transient faults induced by radiation effects on integrated circuits are of the order of tens of picoseconds [20]. Hence, this paper had defined the minimum profile of transient fault that the sensors must detect as a double-exponential transient current I_{fault} with duration of 50ps (measured at the half amplitude of the current). Moreover, the resultant transient voltage must have minimum detectable amplitude of 50% of V_{DD}.

5. Simulation results

Transistor-level simulations were performed for comparing the proposed "sibbics_esref2012" with the previous BBICS labelled as "bbics_tns2008". The circuit versions were designed with V_{DD} of 0.9V and in nominal conditions of a 32-nm CMOS technology [18]. Table 1 illustrates the resultant values for Y_{max} and Y_{min} of the schemes in Fig. 2 by using the method of section 4.

Fig. 3 shows the normalized power consumption and area of a reference circuit (10 chains of 10 inverters) in which all its transistors are monitored by only one BBICS cell composed of two parts (PMOS and NMOS). The "bbics_tns2008" and "sibbics_esref2012" versions were designed with Y_{max}, Y_{min}, and different X. In addition, Fig. 3 illustrates the results when the sleep mode is active. The 200 transistors of the chains were designed with minimum size to analyze the technology's smallest capacitances, which represent the most sensitive nodes. Thus, this case-study circuit allows inducing the smallest profiles of transient fault as well as evaluating the minimum detection sensitivity of the BBICS.

We can conclude from Fig. 3 that "bbics_tns2008" versions present the largest power consumption and area overheads. On the contrary, "sibbics_esref2012" versions have smaller area and very lower power consumption, which is further reduced during sleep-mode. Note that the results allow defining the minimum and maximum increases since our calibration method searches for the smallest and the largest possible Y. Moreover, the method identifies the optimal trade-off between power and area.

Finally, Fig. 4 illustrates that the response times of "sibbics_esref2012" versions are at least equivalent to "bbics_tns2008" versions, and they can be of the order of hundreds of picoseconds.

6. Conclusions

The paper presents a promising solution for detecting transient faults in integrated circuits. With no performance penalty and much lower overheads in terms of area and power consumption than state-of-the-art's CED techniques, the SIBBICS are perfectly suitable for system design flows based on CMOS standard-cell layout approach. In fact, the standard cells of commercial libraries are never modified but a set of SIBBICS cells is designed in function of them. Ongoing works are the fabrication of a prototype and the validation of the approach by using a laser beam to inject transient faults.

Table 1

Results of the calibration method for a profile of fault: the minimum and maximum factors Y for a range of X. It means, in function of X, the largest and the smallest sensor versions that can detect a transient fault with amplitude of 50% of V_{DD} and 50ps of duration.

		X:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
BBICS TNS 2008	NMOS	Y_{max}:	23.6	17.7	14.7	12.7	11.3	10.2	9.3	8.6	8.0	7.5	7.0	6.6	6.3	6.0	5.7	5.5	5.2	5.0
		Y_{min}:	10.1	8.1	6.3	5.3	4.7	4.3	4.0	3.8	3.6	3.5	3.3	3.3	3.2	3.1	3.0	2.9	2.9	2.8
	PMOS	Y_{max}:	74.2	47.2	34.7	27.2	22.3	19.2	16.4	14.4	12.9	11.7	10.7	9.8	9.1	8.5	7.9	7.4	7.0	6.7
		Y_{min}:	45.9	26.2	18.1	13.7	12.4	11.1	8.1	7.3	6.5	5.9	5.4	5.0	4.7	4.5	4.4	4.4	4.2	4.1
SIBBICS ESREF 2012	NMOS	Y_{max}:	70.6	46.1	34.1	27.0	22.2	18.8	16.3	14.4	12.9	11.7	10.6	9.8	9.1	8.4	7.9	7.4	7.0	6.6
		Y_{min}:	29.7	10.1	7.3	5.8	5.3	4.8	4.4	4.1	3.9	3.8	3.8	3.6	3.5	3.4	3.3	3.2	3.2	3.1
	PMOS	Y_{max}:	74.2	47.2	34.7	27.3	22.4	18.9	16.4	14.5	12.9	11.7	10.7	9.8	9.1	8.5	7.9	7.4	7.0	6.7
		Y_{min}:	44.1	25.1	17.5	13.2	10.7	9.2	7.9	7.1	6.5	5.8	5.4	5.0	4.7	4.4	4.2	4.0	3.8	3.7

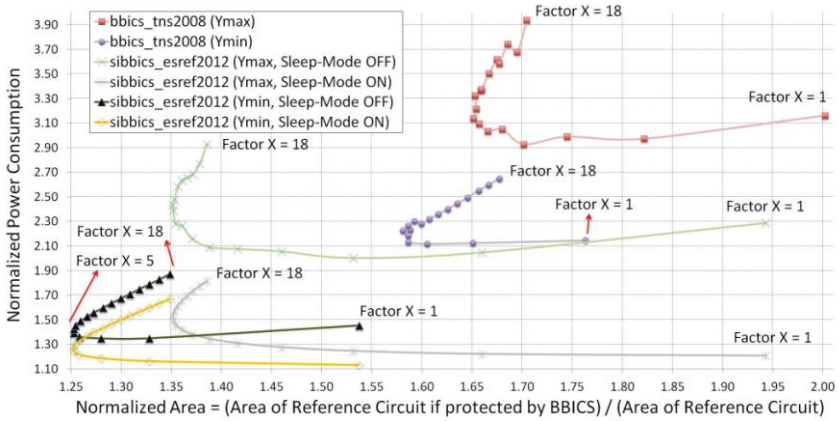

Fig. 3. Normalized power consumption and area of a reference circuit composed of 100 NMOS and 100 PMOS monitored by one NMOS-BBICS and one PMOS-BBICS. The BBICS versions are defined in function of design factors X, Y_{max}, Y_{min}. For instance, "sibbics_esref2012 (Ymin, Sleep-Mode ON)" version with X=5 represents the optimal design. When the sleep mode in active state, this design version imposes around 25% of power consumption and area overhead over the reference circuit due to the SBBICS implementation with a factor X=5 and its corresponding Y_{min}= 5.3 (NMOS) and Y_{min}= 10.7 (PMOS).

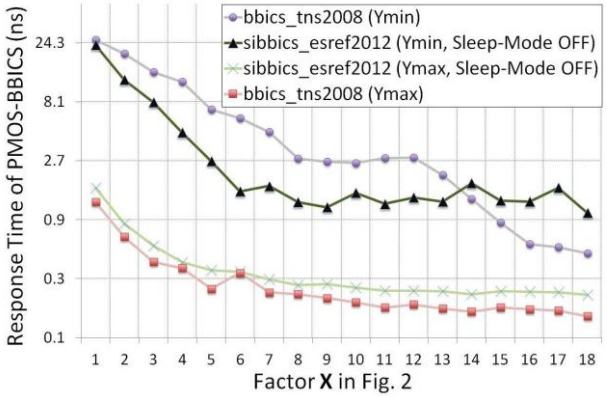

Fig. 4. Response times of PMOS-BICS versions for raising a flag due to a transient fault with amplitude of 50% of V_{DD} and 50ps of duration, the response times for NMOS-BICS versions are omitted here but they are always lower

References

[1] T. Karnik, P. Hazucha, and J. Patel, "Characterization of Soft Errors Caused by Single Event Upsets in CMOS Processes", IEEE Transactions on Dependable and Secure Computing, v.1, n.2, pp. 128-143, 2004.

[2] R. Leveugle, "Early Analysis of Fault-Based Attack Effects in Secure Circuits", IEEE Transactions on Computers, v.56, n.10, pp. 1431-1434, 2007.

[3] C. Lisboa et al., "Using Built-in Sensors to Cope with Long Duration Transient Faults in Future Technologies", in Proc. ITC, IEEE, 2007, pp. 1-10.

[4] S. Z. Shazli, and M. B. Tahoori, "Transient Error Detection and Recovery in Processor Pipelines", in Proc. DFT, IEEE, 2009, pp. 304-312.

[5] E. H. Neto et al., "Using Bulk Built-in Current Sensors to Detect Soft Errors", IEEE Micro, v. 26, n. 5, pp. 10–18, Sep. 2006.

[6] E. H. Neto et al., "Tbulk-BICS: A Built-In Current Sensor Robust to Process and Temperature Variations for Soft Error Detection", IEEE Transactions on Nuclear Science, v. 55, n. 4, pp. 2281-2288, Aug. 2008.

[7] G. R. Srinivasan, P. C. Murley, and H. K. Tang, "Accurate, predictive modeling of soft error rate due to cosmic rays and chip alpha radiation", in Proc. IRPS, IEEE, 1994, pp. 12-16.

[8] S. P. Athan et al., "A Novel Built-in Current Sensor for I_{DDQ} Testing of Deep Submicron CMOS ICs", in Proc. VTS, IEEE, 1996, pp. 118-123.

[9] J. Lo et al., "Design of Static CMOS Self-checking Circuits using Built-In Current Sensing", in Proc. FTCS, IEEE, 1992, pp. 104-111.

[10] F. Vargas, M. Nicolaidis, "SEU-tolerant SRAM design based on current monitoring", in Proc. FTCS, IEEE, 1994, pp.106-115.

[11] B. Gill et al., "An Efficient BICS Design for SEUs Detection and Correction in Semiconductor Memories", in Proc. DATE, IEEE, 2005, pp. 592-597.

[12] P. Ndai et al., "A Soft Error Monitor Using Switching Current Detection", in Proc. ICCD, IEEE, 2005, pp. 185-190.

[13] A. Narsale, M. C. Huang, "Variation-tolerant hierarchical voltage monitoring circuit for soft error detection", in Proc. ISQED, IEEE, 2009, pp. 799-805.

[14] G. Wirth, "Bulk built in current sensors for single event transient detection in deep-submicron technologies", Elsevier Microelectronics Reliability, v. 48, n. 5, pp. 710-715, May 2008.

[15] R. P. Bastos et al., "How to Sample Results of Concurrent Error Detection Schemes in Transient Fault Scenarios?", in Proc. RADECS, IEEE, 2011, pp. 635-642.

[16] Z. Zhang et al., "A new bulk bult-in current sensing circuit for single-event transient detection", in Proc. CCECE, IEEE, 2010, pp. 1-4.

[17] S. Hu, et. al., "Berkeley short channel igfet model", Dpt. Of EECS, University of California, Berkeley, 2005.

[18] Predictive Technology Model (PTM) Web site: http://www.eas.asu.edu, last visited at June, 2011 (link "Nano-CMOS").

[19] Kim, N.S., et. al.: "Leakage Current: Moore's Law Meets Static Power", IEEE Computer, p. 68, no. 12, 2003.

[20] V. Ferlet-Cavrois et al. "Statistical analysis of the charge collected in SOI and bulk devices under heavy ion and proton irradiation—implications for digital SETs", IEEE Transactions On Nuclear Science, IEEE Computer Society, 2006, v. 53, n. 6 (part 1), pp. 3242-3252.