Exploiting Body Terminals of Transistors for Performing Post-Fabrication Tests, Run-Time Tests, and Self-Adaptive Bias in Integrated Circuits

Rodrigo Possamai Bastos

Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir l'Habilitation à Diriger des Recherches (HDR) de la

COMMUNAUTÉ UNIVERSITÉ

GRENOBLE ALPES

Spécialité : **Nano Électronique & Nano Technologies**

Présentée par

Rodrigo POSSAMAI BASTOS

Préparée au sein du **Laboratoire TIMA**
dans **l'École Doctorale Electronique, Electrotechnique, Automatique & Traitement du Signal (E.E.A.T.S)**

Exploiting Body Terminals of Transistors for Performing Post-Fabrication Tests, Run-Time Tests, and Self-Adaptive Bias in Integrated Circuits

Thèse soutenue publiquement le **30/01/2018**,
devant le jury composé de :

M. Pascal FOUILLAT
Full Professor, Bordeaux INP, IMS (France), Président
Mme. Edith BEIGNE
Senior Scientist, CEA Leti (France), Rapporteur
M. Bernabé LINARES-BARRANCO
Full Professor, IMSE-CNM (Spain), Rapporteur
M. Matteo SONZA REORDA
Full Professor, Politecnico di Torino (Italy), Rapporteur
M. Patrick GIRARD
CNRS Research Director, LIRMM (France), Examinateur
M. Raoul VELAZCO
CNRS Research Director, TIMA (France), Examinateur
M. Haralampos STRATIGOPOULOS
CNRS Researcher, UPMC, LIP6 (France), Examinateur

Table of contents

Abstract

Ubiquitous integrated circuit applications help the humanity to rapidly evolve by supporting electronics systems that are more and more assuming autonomous functions and decisions of important responsibility for the society. In this context, dealing with security, reliability, and power issues of integrated circuits is fundamental to ensure the operation of systems within reasonable levels of privacy, safety, and energy consumption. Exploiting body terminals of transistors in CMOS technology-based systems, this work contributes with new techniques dedicated to: (a) test circuits – just after fabrication – for detecting possible hardware Trojans inserted to maliciously compromise systems; (b) test circuits on the fly for detecting transient faults provoked by radiation effects or malicious attacks; and (c) perform body bias adaptation in systems aiming to optimize speed and power but also compensate threshold voltage alterations induced by aging, process, voltage, and temperature variations. Moreover, herein, ongoing and near-future related activities and insights are discussed as potential perspectives of this work.

Part I

Research activities

Chapter 1

Introduction

Many types of new-generation electronics systems surround nowadays our lives, providing solutions, utilities, and conveniences we had never experimented before. Biomedical, agricultural, industrial, commercial, service, entertainment, home, automobile, aeronautical, space, and telecommunication appliances help us to solve quotidian problems related, for instance, to the health of living beings, transport over short and long distances, satellite TV broadcast, weather forecast, and communication between computers and people. From a new world of the Internet of things (IoT) in which billions of communicating devices harvest data from tens of billions of sensors, dealing with security, reliability, and power issues becomes more and more important for integrated circuit (IC) applications.

The information technology (IT) sector – as the heart of the IoT with its data centers, communication networks, and end-user devices – was already responsible in 2012 for around 7 % of the world's electricity demand [25], including the energy required to manufacture IT infrastructures and equipments. It is approximately fourfold higher than the total energy consumption of a Brazil-like country in the same year. The need for reducing power is, therefore, immediate, not only to have our mobile telephones and battery-powered portable gadgets working for a longer time without recharging, but also to make our planet greener again by saving natural resources.

Parallelly, in the advent of self-adaptive systems like geolocation satellites, aircraft, drones, autonomous cars, nuclear power plant robots, in-body-implanted medical devices – which are all applications of high risk in case of failure – embedded circuits must be sufficiently reliable, safely operating within a specified range of low-power performance even in harsh environments. Furthermore, circuits embedded in such critical applications must also be conveniently secure, hiding confidential data, restricting access to private information, and defending themselves from intentional attacks that aim to hack into systems for maliciously carrying out illegal actions or inducing catastrophic situations.

This work is specifically interested to deal with three important issues related to the security, reliability, and power of integrated systems in complementary metal–oxide–semiconductor (CMOS) technologies: (a) hardware Trojans (HT), which are malicious slight layout alterations or furtive mechanisms [126] included in outsourced IC design, fabrication, or manufacturing phases by third-party suppliers willing to hack, disturb, or intentionally disable, at run time, the Trojan-infected circuits; (b) transient faults (TF), as voltage glitches induced by radiation [55] or malicious sources [5, 15, 39, 56] of perturbation, can provoke bit flips in memory elements – i.e. soft errors that may lead entire systems to fail, compromising critical applications or even providing relevant information for cryptanalysis methods that exploit results of fault-injection attacks over secure circuits; and (c) transistor threshold voltage (Vth) alterations – induced by

aging, process, voltage, and temperature (PVT) variations as well as by body bias modifications – are able not only to slow down gates of circuits, violating critical timing constraints, but also speed up them at the expense of static power consumption increase [37, 128].

Efficiently making integrated systems low-power, reliable, and secure to HT, TF, and Vth alterations requires the inclusion of dedicated hardware-level techniques, incurring extra costs in terms of area, power, or speed. For detecting HT, post-fabrication testing schemes [1,2,13,16, 52, 86, 92, 97, 134, 144] have to be implemented for seeking malicious hardware modifications in the IC under test. For detecting TF, otherwise, run-time testing mechanisms [3, 12, 29, 82, 91, 93, 94, 100, 113, 121] need to be embedded in the systems for dynamically monitoring illegal voltage glitches. And for compensating Vth alterations, adaptive body bias generators [10, 37, 44, 53, 77, 128] are added to intelligently tune Vth of transistors in function of aging and PVT variations.

Exploiting the body terminals of transistors, this work contributes with new techniques of: (a) post-fabrication test for detecting HT; (b) run-time test for detecting TF; and (c) body bias for systems targeting adaptive compensation of Vth alterations but also optimization of speed and power. Chapter 2 of this work evaluates the effectiveness of state-of-the-art TF-detection techniques, moreover it proposes a new concurrent error detection scheme. Chapter 3 analyzes different architectures of bulk built-in current sensors (BBICS) able to monitor body terminals of transistors for detecting single or multiple TF. A new low-cost and efficient dynamic BBICS architecture is also presented in chapter 3. Chapter 4, on the other hand, presents a novel post-fabrication testing method for the detection of HT by using BBICS, which also operate to detect TF at run time. Chapter 5 studies a mechanism that is fundamental for applying adaptive body bias strategies: the voltage level shifter. In addition, it introduces a new level shifter architecture for dynamically biasing low-voltage subcircuits of fine-grained systems. Finally, chapter 6 analyzes the suitability of asynchronous circuits, which deal with data without using a clock, for receiving adaptive body bias schemes, properly operating with low voltages, and controlling themselves their static power consumption and speed. Chapter 7 concludes this work discussing the most important contributions and results, and ongoing and near-future perspectives.

Chapter 2

Effectiveness of error detection techniques in identifying transient faults

With the downscale of integrated systems, increasing their robustness against environment- or human-induced perturbations motivates considerable design challenges. Aging effects, alpha particles released by radioactive impurities, and more importantly, neutrons from cosmic rays are examples of environmental events [55]. In addition, fault injections to the end of retrieving secret data from security applications or disabling embedded secure protocols are human-produced attacks, which try to obtain fundamental information for cryptanalysis methods [56] or to activate hardware Trojans maliciously inserted in systems [126].

Radiation exposure and environmental variations are able to induce parasitic transient currents that may lead integrated circuits to critical failures. Similar electrical effects are also caused by optical sources like flashlights or laser beams [39], which allow, moreover, finely controlling the injected current thanks to the high spatial and temporal resolutions of laser shots [5]. The induced transient faults (TFs) – i.e. temporarily voltage level modifications – are active only for a short duration of time, their occurrence are not predictable, and they may provoke soft errors (SEs) in stored results of system operations. TFs need thus to be detected at run time.

Error detection during circuit normal operation is typically called concurrent error detection (CED) [81]. Several CED techniques have been proposed [3,12,29,34,91,93,100,113,115,121] with the intent to design more reliable computing systems. These techniques mainly differ in their detection capabilities and in the constraints they impose on the system design. This chapter presents a simulation-based method to evaluate and compare different detection techniques regarding their effectivenesses in detecting TFs arisen in combinational logic blocks and resulting in SEs. The method proposes 32 different scenarios of TF injection. Results of all detection techniques studied here are summarized in a table that provides a direct insight of the effectiveness of each technique. Furthermore, in this chapter, another CED technique is introduced and compared among the other techniques. It uses an effective Transition Detector (TD) and a controllable adaptive detection window (DW). As a result, the introduced technique offers increased SE detection capability but also allows the detection of Delay Errors (DEs). The works of this chapter are the prospects of my postdoctoral activities started at 2010, and within the thesis context of my Ph.D. student Raphael Viera, it was presented in the international conference ESREF 2017 and published in the international journal Microelectronics Reliability 2017.

Section 2.1 of this chapter describes the main CED techniques in the literature and section 2.2 details our improved CED technique. In the following, section 2.3, 2.4, and 2.5 present our method for evaluating the effectiveness of CED techniques, simulation results, and comparative analysis.

2.1 Techniques for Concurrent Error Detection (CED)

State-of-the-art CED techniques are classified in this section into four categories: spatial redundancy, temporal redundancy, Transition Detector (TD)-based schemes, and Built-In Current Sensors (BICSs). We could still mention a fifth category – information redundancy – in which its structure is similar to a spatial redundancy; however, instead of a copy block, a code prediction block and a coder are added [109]. Furthermore, we highlight the well-known acronym CED is indeed a misuse of language as there exist concurrent detection schemes able to detect transient faults (TFs) not necessarily producing errors. The detection of TFs that are masked – not resulting in hard or soft errors (SEs) – is also of importance for secure applications. All these approaches are implementable at different abstraction levels of a design, this work is interested in techniques at hardware level.

2.1.1 Spatial redundancy

- **Duplication With Comparison (DWC)** technique [115] – illustrated in Fig. 2.1a – is conceptually the simplest CED scheme. Based on the principle of spatial redundancy, the outputs $D_{<1>}$ and $D_{<1>}copy$ (duplication of the circuit's logic) are connected to two D-type Flip-Flops (DFFs), which have their outputs compared, generating an error signal in case of difference.

2.1.2 Temporal redundancy

- **Time Redundancy (TR)** technique [93] (Fig. 2.1b) repeats the same computation with the same hardware at different time instants. The output of the two DFFs are compared, and if the outputs are divergent, the error signal is raised.

2.1.3 Transition Detector (TD)-based schemes

- **RAZOR-II** [29] is a TD-based technique dedicated to detect Delay Errors (DEs) but also the advent of SEs. A simplified circuit diagram of this scheme is shown in Fig. 2.1c. The design assumption is that the latch output $Q_{<1>}$ is allowed to shortly switch only after a rising edge of the clock CLK. The latch output $\overline{Q}_{<1>}$ is connected to a TD block that is thus able to detect TFs. To avoid false error signaling, a detection clock generator disables the TD block for at least the duration of the CLK-to$Q_{<1>}$ delay after a rising edge of CLK.

- **Transition Detector With Time Borrowing (TDTB)** technique [12] is similar to Razor-II. It consists in the coupling of a latch and a TD as illustrated in Fig. 2.1d. The transition detector raises the error signal for any input transitions during the low state of the clock ($\overline{CLK}$), thus requiring the signal $D_{<1>}$ to be stable before the low period of the clock.

- **Double Sampling With Time-Borrowing (DSTB)** technique [12] presented in Fig. 2.1e is like TDTB scheme although a shadow flip-flop replaces the TD block. DSTB double samples signal $D_{<1>}$ and compares the latch and shadow flip-flop outputs to generate the error signal. Furthermore, DSTB retains the time-borrowing feature of TDTB to eliminate data-path metastability.

- **Transient Fault Monitoring Scheme (TFMS)** proposed in [113] detects TFs affecting the DFF input such as signal $D_{<1>}$. As shown in Fig. 2.1f, this scheme includes a *Transition Detector*, which generates a high signal when there is a TF inside the *Detection Window* (signal "DW"). The *Sticky Block* is used to validate TFs occurring only inside the DW and to merge the error signal since the TD produces two pulses.

2.1.4 Built-In Current Sensors (BICSs)

- **Single Bulk Built-In Current Sensor (SBBICS)** [108] [34] is an optimized version of the original bulk BBICS [91] designed to monitor radiation- or laser-induced transient currents passing through the bulk of transistors. The SBBICS architecture allows monitoring simultaneously the pull-up and pull-down of CMOS networks [108] [34] as shown in Fig. 2.1g. Chapter 3 further details how BICS architectures detect TFs.

- **Dynamic Bulk Built-In Current Sensor (DBBICS)** [121] operates similarly to SBBICS, although it features a dynamic memory cell. The TF occurrence information is stored in the gate-source capacitance of a storage transistor. Two DBBICS architectures are abstracted in Fig. 2.1h to individually monitor the pull-up and pull-down CMOS networks.

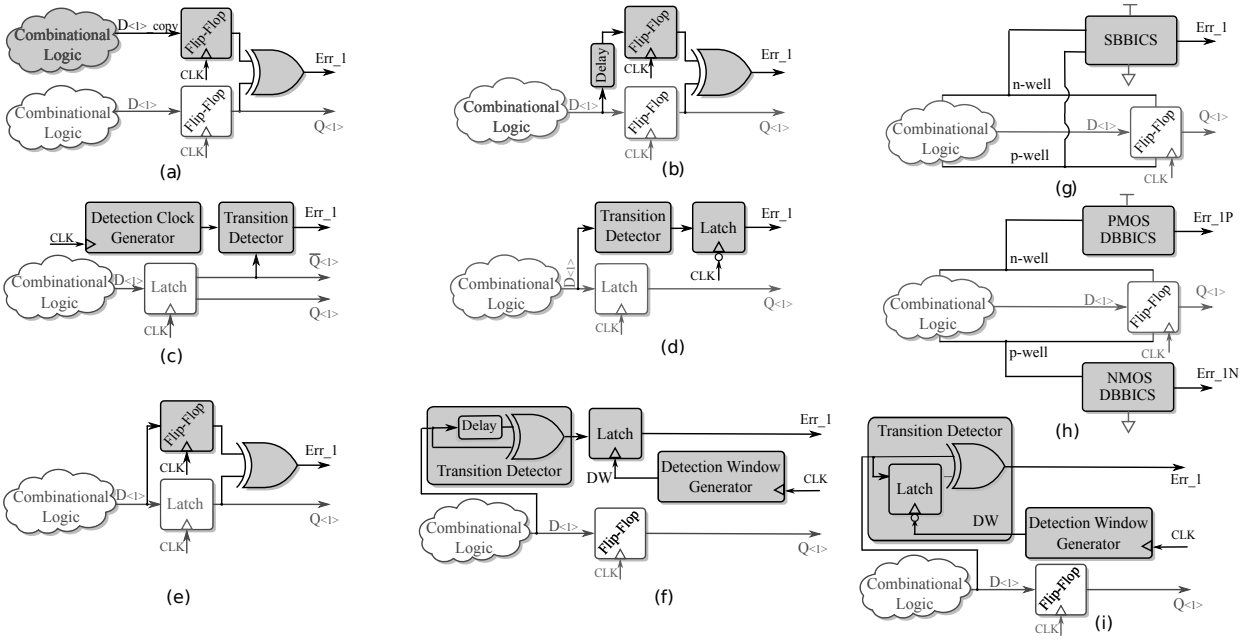


Fig. 2.1: CED techniques: (a) DWC [115]; (b) TR [93]; (c) Razor-II [29]; (d) TDTB [12]; (e) DSTB [12]; (f) TFMS [113]; (g) SBBICS [34]; (h) DBBICS [121]; and (i) the CED technique proposed in section 2.2: Latch Based Transient-Fault Detection (LBTFD).

2.2 Proposed CED technique

The technique presented in this section is proposed to improve the effectiveness of TD-based schemes in detecting transient faults. The operation mode is similar to schemes [113] and [100]. However the devised 1-bit TD circuit is formed by a latch instead of the delay block suggested

in [113] and [100], as shown in Fig. 2.1i. In addition, unlike previous works [113] and [100], our proposition combines the error signals of each 1-bit TD circuit (Err_1 to Err_N) with the help of a single dynamic OR gate (Fig. 2.2), and not using parity trees (i.e. xor trees) that may electrically filters TF and prevent the possibility of detecting them. The proposed TD circuit and dynamic OR gate are particularly activated during a Detection Window (DW) in which the monitored combinational circuit's output $D_{<1>}$ (i.e. D-type Flip-Flop (DFF) input) is prone to present TF-induced illegal transitions. Therefore, any abnormal transition at $D_{<1>}$ within DW would be detected. We denote our technique herein as Latch Based Transient-Fault Detection (LBTFD). The scheme in Fig. 2.3 is used to specify the signal called DW.

One of the advantages in using a latch as a TD is that only one pulse is generated by the error signal output. In the case of a TD, as the one used in [113], the transition detection block produces two pulses, therefore, needing to recur to an additional block to merge the two generated pulses. A second advantage is the ability to detect TFs during the hold time (thus TFs inducing SE). An additional increase in $\delta 2$ will enable the detection to further cover SEs and DEs. Furthermore, the use of a latch in a TD will guarantee the detection of TFs in recent technologies as TDs using inverters connected to a XOR gate [12] need an increased delay in order to be triggered, thus, having more static power consumption and higher area overhead.

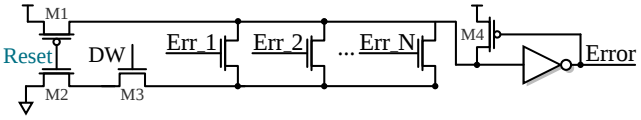


Fig. 2.2: Dynamic OR gate for combining error signals from TD circuits.

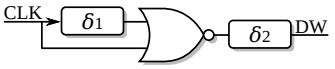


Fig. 2.3: Generator of the Detection Window (DW) signal.

2.2.1 Defining the Detection Window (DW)

In order to choose a proper configuration for DW, Fig. 2.4a refers to a data-path with a clock period denominated clk_per. Labels t_{setup} and t_{hold} define the DFF setup and hold times respectively. The setup time is the minimum amount of time before the clock edge during which the signal $D_{<1>}$ must be valid, whereas the hold time is the minimum amount of time after the clock edge during which the signal $D_{<1>}$ must be valid for a correct operation of the DFF. δ_{DW} is the time overhead due to the DW. According to the width of TFs (TF_W), the width of the DW (DW_{width}) can be designed in a way in which only faults resulting in SEs are detected:

$$DW_{width} = (t_{setup} + t_{hold}) \tag{2.1}$$

or, in which TFs resulting or not resulting in SEs are detected:

$$DW_{width} = (t_{setup} + t_{hold}) + \delta_{DW}. \tag{2.2}$$

Note that, the greater the δ_{DW} (lower $\delta 1$ in Fig. 2.3), the earlier the signal $D_{<1>}$ must be steady. Indeed it must reach its final steady state before $(t_{setup} + \delta_{DW})$. For a DW configuration as the one in Fig. 2.4a the maximum operating clock frequency of the circuit is penalized,

however, $\delta 2$ allows a shift in DW meanwhile maintaining its same width as can be seen in Fig. 2.4b, thus allowing an increased operation frequency of the circuit. In fact there are many ways to design DW to coper with timing specifications. The main advantage in having $\delta_{DW} \neq \emptyset$ is the possibility to assure the detection of transient faults with $TF_W \leq (t_{setup} + t_{hold} + \delta_{DW})$ that will cause a SE.

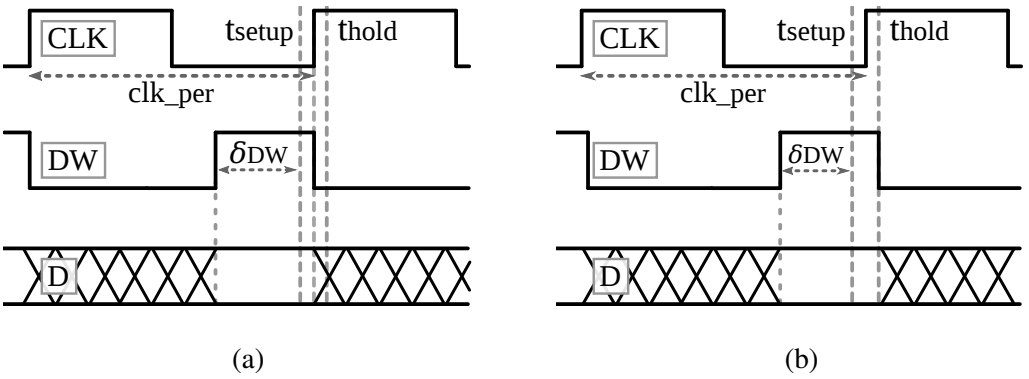


Fig. 2.4: Detection Window (DW) configuration: (a) $\delta 1 \neq 0$ and $\delta 2 = 0$ (b) $\delta 1 \neq 0$ and $\delta 2 \neq 0$.

2.2.2 Verification by electrical simulation

The operation mode of the proposed technique has been verified by electrical simulation to detect the advent of a single induced transient fault arriving at node $D_{<1>}$ as presented in Fig. 2.5. The simulation has been performed in the FD-SOI 28 nm technology with VDD = 1 V. The injected transient current magnitude was a value from which the associated transient voltage amplitude (created at node $D_{<1>}$) is equivalent to 100% of VDD, i.e. 1 V. The transient fault width was set to be around 150 ps, with rise time (tr) shorter than the fall time (tf) to keep the traditional shape of transient faults [137] [80] [17] [32] [36]. The transient current has been injected from a NMOS sensitive drain $D_{<1>}$ to its p-well bulk, i.e. the current has been applied when $D_{<1>}$ was steady at 1 V. It could be clearly noted that any variation inside the DW is sufficient to trigger the error signal independently of its polarity (rising or falling). Therefore, any fault occurring in the NMOS or PMOS sensitive drains within the DW is detectable.

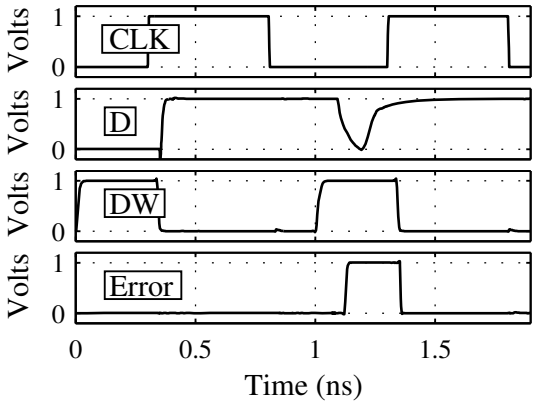


Fig. 2.5: Electrical simulation of the proposed technique detecting a single TF (width of around 150 ps) injected on node $D_{<1>}$.

2.3 Method for evaluation of CED techniques

The method proposed in this section evaluates the effectiveness of CED techniques in detecting single TFs by taking advantage of four facts:

(1) The harmful consequence of TFs induced in a target combinational circuit under protection of a CED circuitry is the generation of a SE in one or several DFFs;

(2) TFs induced inside of a target combinational circuit – at the worst case – propagate up to an input $D_{<1>}$[1] of one or several DFFs flipping their bits (SEs);

(3) TFs partially or fully propagated up to $D_{<1>}$ produce a profile of TF on $D_{<1>}$ that is perfectly representable by profiles of single TFs injected directly on $D_{<1>}$; and

(4) TFs induced inside of a target combinational circuit and fully mitigated by a logical or electrical masking effect [55] make no effect on $D_{<1>}$. These TFs are indeed attenuated by the target combinational circuit, and not by the CED technique protecting it.

With these four TF-related facts in mind, the evaluation of the CED technique effectiveness can be simplified by injecting TFs only on $D_{<1>}$. Furthermore, as the goal is evaluating the degree to which a CED technique is successful in detecting TFs – and not the ability of the target combinational circuit in logically or electrically masking TFs – the logic function of the target combinational circuit is not relevant. Latching-window masking effects, otherwise, have to be considered because the sampling window of DFFs is directly related to the design of most CED techniques included into systems synchronized by a clock.

The proposed simulation-based method applies, therefore, only on $D_{<1>}$ a double exponential current source with parameters configurable according to the classical single TF model for CMOS circuits [137] [80]. Diversified profiles of single TFs are thus injected on $D_{<1>}$ at different instants, and the results of the TF-injection campaigns are synthesized through evaluation metrics.

2.3.1 Profiles of injected TFs

Campaigns of single current injections reproduce 32 scenarios having different profiles of TFs: transient faults with different widths, current amplitudes, and polarities (sensitive drain). The rise times of the injected double exponential current sources have been set on the order of 5 ps to keep the typical shapes of TFs: short rise time and longer fall time [32] [36]. Additionally, the slack time left by the target combinational circuit is changed to verify how a CED technique behaves when data on $D_{<1>}$ stabilizes during high and low levels of the clock. By scenario, a total of one thousand TFs, for instance, are injected across a clock period of 1 ns, resulting in a simulation step of 1 ps.

The 32 scenarios are summarized in Table 2.1. By considering a simulation start time of 0 ns, the TF start column represents the instant at which the first transient fault begins to be injected on node $D_{<1>}$. Note that the combination of each column in the table comprises a different scenario, resulting in a total of 32 scenarios, for instance, the eight scenarios in the first row (1, 2, 9, 10, 17, 18, 25 and 26) have the following possible configurations: TF width of 10 ps, TF start at 0.2 ns or 0.58 ns, sensitive drain of PMOS or NMOS and TF amplitude of 60%VDD or 100%VDD.

[1] $D_{<1>}$ represents 1 bit of N bits, e.g., a system of 32 bits would require the inclusion of 32 CED circuitries.

Table 2.1: Profiles of injected TFs

Scenario	TF width (ps)	TF start (ns)	Sensitive Drain	TF amplitude (% VDD)
1, 9, 17, 25 2, 10, 18, 26	10	0.20	PMOS	60
3, 11, 19, 27 4, 12, 20, 28	50			
5, 13, 21, 29 6, 14, 22, 30	200	0.58	NMOS	100
7, 15, 23, 31 8, 16, 24, 32	450			

2.3.2 Analysis of injected TF effects

The injection of single TFs on $D_{<1>}$ is able to induce four effects :

(1) TFs that completely overlap the sampling window always produce a SE in the DFF [84];

(2) TFs that rise and fall inside the sampling window are either masked or they cause a DE or a SE;

(3) TFs that partially overlap with the sampling window provoke a CLK→Q time variation, i.e. a DE;

(4) TFs that do not overlap with the sampling window are always masked [84].

In order to evaluate the proposed scenarios in function of the time and their consequences, Fig. 2.6 defines three color bars that represent the instants at which a single TF starts to be injected:

(1) Green color bar: Masked Fault (MF): the injected single TF do not perturb the output Q of the monitored DFF, i.e. no SE is induced;

(2) Blue color bar: Delay Error (DE): the injected single TF increases the CLK→Q delay of the DFF more than 10% in relation to the typical CLK→Q delay under no TF effects;

(3) Red color bar: Soft Error (SE): the injected single TF provokes a SE.

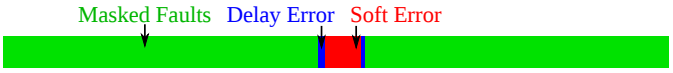


Fig. 2.6: Definition of color bars for MFs (green), DEs (blue) and SEs (red).

Figure 2.7 shows, for each scenario the clock signal CLK, the monitored data signal $D_{<1>}$ and the color bars representing the behavior of eight scenarios regarding the TF profile. Note that, due to the different slack values provided, the TF for each scenario had its beginning at a specific time, e.g., for scenario 1, the TF begins at 0.2 ns, the same instant in which the signal $D_{<1>}$ reaches its high voltage level (1 V), however, for scenario 2, the TF begins at 0.58 ns since, due to the different slack, signal $D_{<1>}$ has its high voltage level at this time. For the others scenarios, the same principle applies, i.e., for each scenario there is a difference in the slack time provided, in the TF polarity, in the width, or in the amplitude of the TF. It can be

noted that the number of SEs caused in each scenario is highly dependent on the width of the injected transient fault.

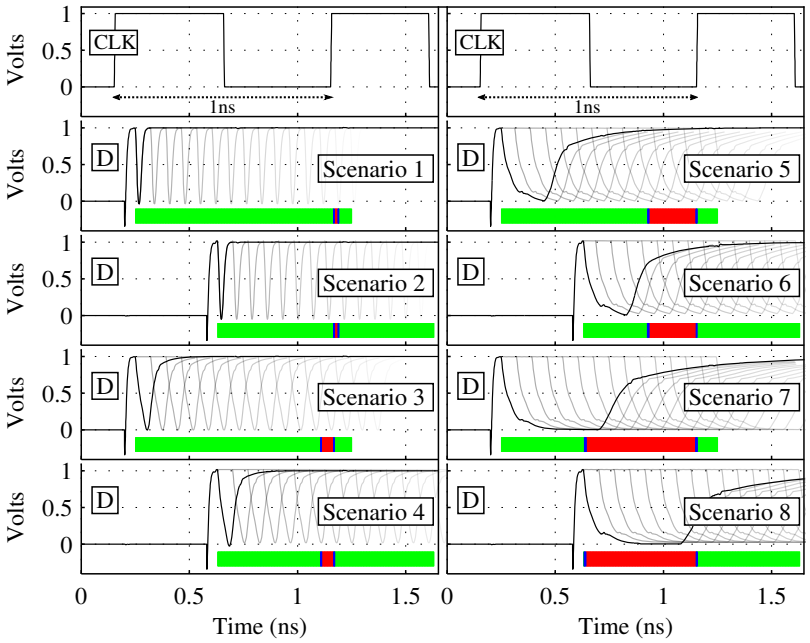


Fig. 2.7: Fault injection scenarios and color bars for MFs, DEs, and SEs.

2.3.3 Evaluation metrics

Figures of merit are defined herein to better compare and to quantify effectiveness of the CED techniques. For a total, for instance, of 1000 single TFs of a scenario, the first metric below measures how many times the CED technique is able to detect the injected single TF:

$$TF_{\ Detection\ Ratio} = \frac{\#TF_{detected}}{\#TF_{injected}}. \tag{2.3}$$

The second and third metrics measure the CED technique effectiveness in detecting injected single TFs that induce, respectively, SEs and DEs:

$$SE_{\ Detection\ Ratio} = \frac{\#SE_{detected}}{\#SE_{induced}}. \tag{2.4}$$

$$DE_{\ Detection\ Ratio} = \frac{\#DE_{detected}}{\#DE_{induced}}. \tag{2.5}$$

The fourth metric measures how many times the CED technique is able to detect a injected single TF that induces a SE or a DE:

$$SE + DE_{\ Detection\ Ratio} = \frac{(\#SE + \#DE)_{detected}}{(\#SE + \#DE)_{induced}}. \tag{2.6}$$

Finally, global metrics are defined by taking into account all the 32 scenarios described in previous subsections, and not only a specific scenario as the evaluation metrics 2.3, 2.4, 2.5, and 2.6 consider. These global metrics are formalized as the arithmetic means of the results over 32

scenarios, or if S is the total number of scenarios and $X_{\,Detection\,Ratio}$ is one of the evaluation metrics 2.3, 2.4, 2.5, and 2.6, we have:

$$X_{\,Detection\,Ratio\,Global} = \frac{\left(\sum_{i=1}^{S} X_{\,Detection\,Ratio[i]}\right)}{S} \tag{2.7}$$

2.4 Simulation results and comparative analysis

Simulation results and comparative analysis of the CED techniques described in previous sections are provided herein by using the proposed evaluation method detailed in section 2.3.

2.4.1 Description of simulation experiments

In order to simulate the effects of single TFs on a complex system, the critical path of an ARM7 processor – designed in a commercial CMOS FD-SOI 28-nm technology – has been extracted as this is potentially the critical part of the system. Fig. 2.8 summarizes the extracted data path represented by the *ARM7 Critical Path* block connected to the input $D_{<1>}$ of a DFF.

Two current sources are shown in Fig. 2.8 because depending on the input $Di_{<1>}$ of the *ARM7 Critical Path* block, the injected transient current will follow a path from the NMOS sensitive drain to its p-well bulk or from the PMOS sensitive drain to its n-well bulk.

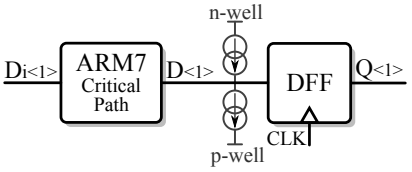


Fig. 2.8: Simulated circuit: a critical path of an ARM7 processor in a commercial CMOS FD-SOI 28-nm technology.

2.4.2 Comparative analysis for scenario 5

Comparative results are analyzed in this subsection for scenario 5 of the method described in section 2.3, i.e. TFs on NMOS with 200 ps of width and amplitude of VDD, cf. Table 2.1. Fig. 2.9 shows the instants at which a TF with such a profile starts to be formed and a CED technique is able to detect it (orange) or not (light gray). The rising edge of the clock happens at 1.2 ns. The orange color means, therefore, the error signal of the CED scheme raised, and the light gray color means the opposite. Each row of Fig. 2.9 is composed of 1000 simulated points, meaning that 1000 simulations were performed for each scenario and for each CED technique. Taking as example the results of the DWC scheme in Fig. 2.9, the DWC's error signal is raised only when a TF reaches the monitored memory element causing a SE. Consequently, the orange part matches with the red one. For the proposed scheme (LBTFD), note in Fig. 2.9 that the error signal is raised when there are transitions within the detection window, which has been calibrated to accommodate TFs with width up to 450 ps. Therefore, the LBTFD's error signal is also raised at instants when there is no occurrence of soft error.

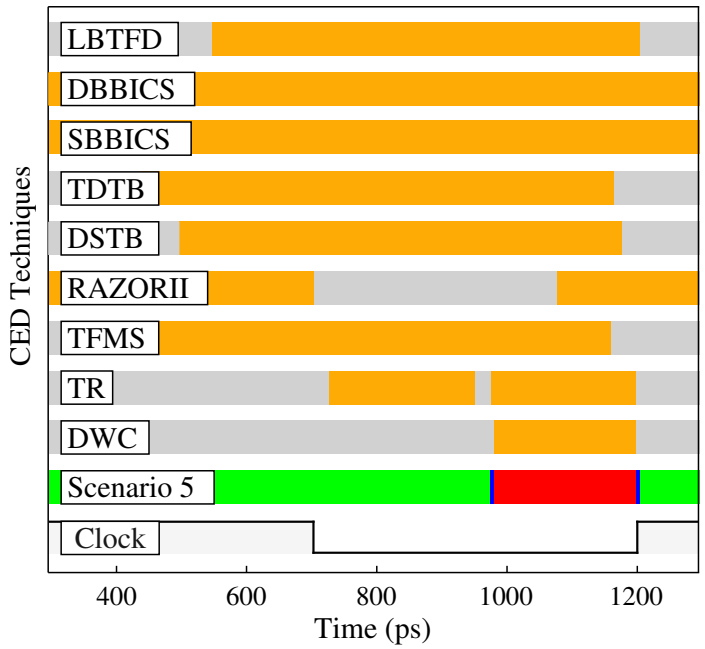


Fig. 2.9: Detection results regarding scenario 5.

2.4.3 Global comparative analysis

Simulation results for each CED technique regarding its effectiveness in detecting single TFs as well as its total power consumption are provided in Table 2.2. For a global comparative analysis, Table 2.2 present results that take into account all the 32 scenarios, i.e. the global metrics detailed in subsection 2.3.3. If a CED technique, for instance, works better in scenario 1 than scenario 3, Table 2.2 is not suitable to analysis it. However, as the aim of this work is also to provide an insight of the global effectiveness of a CED technique in different scenarios of TFs, Table 2.2 is a great asset to it.

Note in Table 2.2 the results of the TFMS technique, it shows that 87.39% of SEs and 44.97% of DEs were detected, meanwhile the proposed technique LBTFD – aiming mainly the

Table 2.2: Total power and effectivenness of the CED techniques under analysis

CED Technique	**Power (μW)**	$\frac{\mathbf{TF_{detected}}}{\mathbf{TF_{injected}}}$	$\frac{\mathbf{SE_{detected}}}{\mathbf{SE_{induced}}}$	$\frac{\mathbf{DE_{detected}}}{\mathbf{DE_{induced}}}$	$\frac{\mathbf{(SE+DE)_{detected}}}{\mathbf{(SE+DE)_{induced}}}$
DWC [115]	$>$ 100 %	16.69 %	100.00 %	0.34 %	28.87 %
TR [93]	3.86 /bit	23.64 %	74.47 %	16.04 %	33.16 %
SBBICS [34]	6.56	100.00 %	100.00 %	100.00 %	100.00 %
DBBICS [121]	5.65	94.23 %	100.00 %	94.75 %	96.38 %
RAZORII [29]	199.21 /bit	43.70 %	72.53 %	37.82 %	47.95 %
TDTB [12]	3.32 /bit	77.98 %	95.54 %	75.32 %	81.49 %
DSTB [12]	3.26 /bit	47.02 %	83.70 %	45.25 %	56.94 %
TFMS [113]	3.02 /bit	50.50 %	87.39 %	44.97 %	57.92 %
LBTFD [this]	2.64 /bit	57.17 %	100.00 %	100.00 %	100.00 %

detection of SEs – was able to detect 100% of the injected TFs that result in SEs. Otherwise, if the TF width is longer than the designed DW, a few SEs will pass undetectable by LBTFD. Results are interesting if compared to the other CED techniques. Moreover, the design of the proposed LBTFD is easier than BBICS-based techniques because only standard cells can be used, implicating directly in less time to conceive the circuit. Although SBBICS was able to detect 100% of the injected TFs, it is not a known standard cell and requires to partition the substrate into islands with separated n-well and p-well regions.

2.5 Conclusions

A technique capable to detect TFs has been presented and analyzed in this chapter. Furthermore, a simulation-based method for classifying and evaluating CED techniques has been defined. For the target scenarios of the method, the proposed CED technique is able to detect all the TFs that result in SEs or DEs in the DFF. The evaluation method takes into account only single TFs that survive the attenuation of logical or electrical masking effects in order to compare exclusively the effectiveness of the different CED techniques – and not the ability of target combinational circuits in masking TFs. This evaluation strategy allows, therefore, to quickly analyze a CED technique independently of the logic complexity of the system. Results in Table 2.2 enable designers to choose the CED technique (or techniques) that suit best for their purposes.

Chapter 3

Architectures of body built-in current sensors for detection of transient faults

Among the many design strategies for detection of transient faults caused by radiation or optical sources, Bulk or herein Body Built-In Current Sensors (BBICS) [89] [91] offer a promising solution that is perfectly suitable for system design flows based on CMOS standard cells of commercial libraries [42]. BBICS combine the high detection efficiency of costly fault-tolerance schemes (e.g. duplication with comparison) with the low area and power overheads of less efficient mitigation techniques such as time redundancy approaches [68]. BBICS approach was experimentally validated in bulk CMOS 28-nm and 90-nm chips under the effects of laser sources [11, 19, 133, 146], and designed, moreover, with transistors of carbon nanotubes [111].

In the last 10 years, several BBICS architectures composed of static memories have been proposed [33,34,90,104,106–108,118,119,138,139,145]. In [104], we have compared them in terms of their sensitivities in detecting transient faults. More recently, with the aim of reducing area and power overheads, Simionovski and Wirth devised a new class of BBICS constituted of dynamic memories [120–122]. Unlike previous works and our comparison study in [104], herein we discuss and compare both, static and dynamic, state-of-the-art BBICS architectures, analyzing their area offsets and detection sensitivities in typical and corner conditions. Furthermore, we introduce a new dynamic BBICS architecture with improved detection sensitivity and lower area penalty than its predecessors. The works of this chapter are the perspectives and the sequence of my postdoctoral research activities started at 2011, and within the thesis context of my Ph.D. student Leonel Guimarães, it was published in the international Microelectronics Journal 2017.

Section 3.1 of this chapter classifies and describes the different state-of-the-art BBICS architectures and their basic principles. Section 3.2 presents our new dynamic BBICS architecture, and section 3.3 defines what we call as the sensitivity of a sensor or a memory element in detecting single transient faults. Finally, section 3.4 provides comparative results and analysis of BBICS architectures, and section 3.5 concludes this work highlighting the main BBICS features and perspectives.

3.1 State-of-the-art architectures of built-in current sensors

Built-in current sensors (BICS) were initially proposed as a mechanism for detecting high increases in the current I_{DDQ} consumed by a CMOS circuit during its quiescent state (i.e. when the circuit is not switching). This type of mechanism enables the testing of CMOS circuits against

permanent faults [4]. Further, BICS were also adapted for detecting transient faults – anomalous transient currents produced on the circuit by external perturbation sources [137] [80] [17] [120] (Fig. 3.1). Firstly, BICS schemes for identifying transient faults in memory cells (bit flips) were devised [38, 69, 88, 130]. More recently, efforts were made for monitoring transient currents in combinational logic too [87]. All these techniques connect BICS circuits between the sources of the monitored transistors and the power rails (V_{DD} or GND), targeting on distinguishing anomalous currents from normal currents. Nevertheless, in today's technologies the amplitude of transient currents induced by radiation effects or fault attacks have the same order of magnitude than currents (source to drain or drain to source) normally generated by switching activities of logic circuits. Hence, schemes monitoring transistor sources are very limited for detecting just a restricted range of transient faults.

For overcoming this BICS problem, Neto et al. proposed in [89] [91] the first architectures of bulk built-in current sensors (BBICS). The major innovation of the BBICS is the connection of sensors between the bulks (i.e., body-ties of the target monitored transistors) and the power rails, rather than applying between the transistor sources and the power rails. Thanks to such a difference, BBICS are able to efficiently detect a wider range of transient faults than the classic BICS.

BBICS-based strategy for the protection of a system is illustrated in Fig. 3.2. A pair of sensors is integrated to monitor pull-up and pull-down CMOS networks of the system blocks, hereinafter respectively PMOS-BBICS and NMOS-BBICS. Melo et al. have analyzed in [79] [78] the robustness of BBICS architectures to substrate noise. Wirth in [139] [138] has studied and verified the device-level operation of a BBICS by using TCAD (technology computer-aided design) simulations. In case of an anomalous current such as I_{FaultN} or I_{FaultP}, for instance, it will flow through the junction between the bulk and a reversely biased drain of the disturbed transistor (MOSFET "off"), and the sensors will be able to detect it by considering two phenomena:

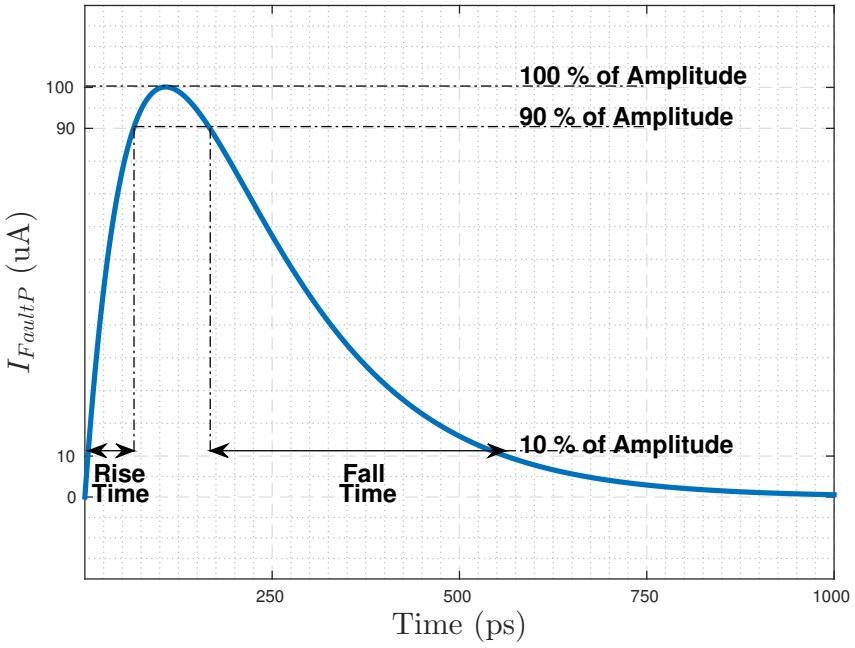


Fig. 3.1: Typical double-exponential profile of a transient fault, which is defined as a transient current generated on the circuit by a external perturbation such as radiation sources or laser beams.

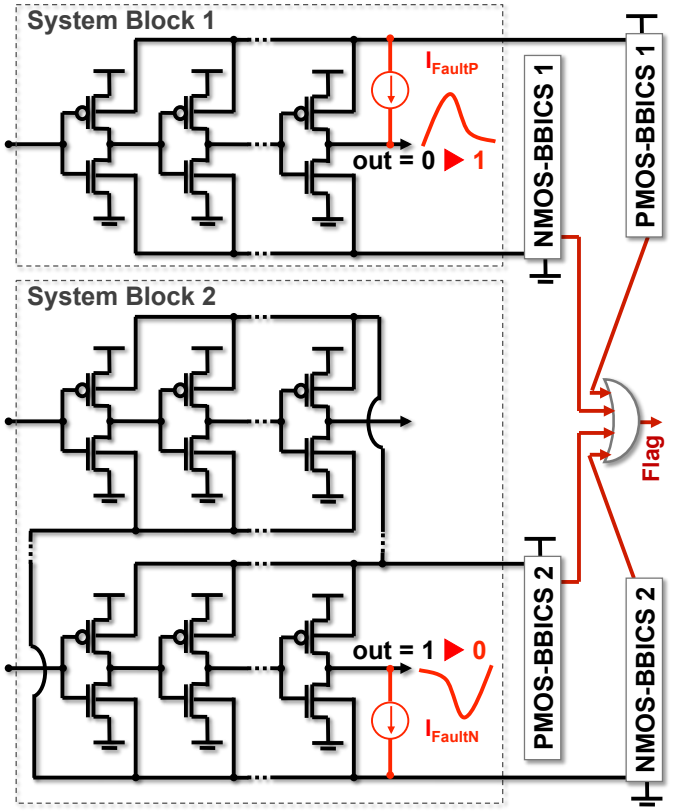


Fig. 3.2: Basic illustrations of BBICS monitoring two system blocks. I_{FaultP} and I_{FaultN} are current sources acting as external perturbations that produce abnormal current effects on the circuit defined as transient faults.

1. In fault-free scenarios (i.e., $I_{FaultP} = 0$ and $I_{FaultN} = 0$), the bulk-to-drain (or drain-to-bulk) current is negligible even if the MOSFET is switching due to a new input stimuli;

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

The sensitivity of a sensor to identify transient faults declines by increasing the number of transistors under monitoring. Hence, target systems have to be split into several blocks that contain a certain number of transistors monitorable by a sensor with sufficient sensitivity in detecting a desired range of transient faults. Fig. 3.2 shows an exemplary system (chains of inverters) divided into two blocks monitored by two pairs of BBICS.

The range of detectable transient faults is adjustable by calibrating the size of some specific transistors of the sensors. Furthermore, BBICS are designed to latch a flag that indicates the detection of the abnormal currents within a defined range representing a risk of consequent soft errors (i.e., bit flips of memory elements).

In according with the latch structure responsible for storing the flag of fault indication, we classify BBICS architectures into static and dynamic. Static BBICS, which contain a static memory cell, are able to monitor transient faults independently of any periodic signal. In contrast, dynamic BBICS feature a dynamic memory, which requires by nature a periodic refresh signal to eliminate harmful leakage effects on its voltage output. In the following subsections, we summarize the state-of-the-art BBICS architectures in four types of static sensors and one type of dynamic sensor.

3.1.1 Single BBICS architectures

The sensor architecture illustrated in Fig. 3.3 is the simplest static BBICS in the literature. It counts only 9 transistors, 4 of which constitute two cross-coupled inverters, i.e., a latch used to register a flag in case of transient faults. This architecture presented in [104] combines concepts proposed in different works [139] [138] [90] [107] [108].

The principle of using a single BBICS circuit to check at the same time both pull-up and pull-down CMOS networks was suggested for the first time in [107] [108] with the aim of saving area. PMOS and NMOS bulk nodes of a single sensor like that in Fig. 3.3 are connected to the monitored body-ties (i.e., bulks of PMOS and NMOS transistors under monitoring) with the help of metal lines. The high ohmic transistors 5 and 7 (with large channel lengths) ensure appropriate voltage bias to the bulks during fault-free scenarios as well as prevent the complete attenuation of the anomalous transient currents in fault contexts. On the contrary, the low-threshold voltage transistors 8 and 6 (with large diffusion widths) are sensing transistors ready to quickly switch in case of transient faults, inverting the latch logic by consequence. This transistor sizing strategy stated in [139] [138] [90] improves the detection sensitivity of the sensor and makes the leakage power overhead negligible.

In order to enhance even more the sensor sensitivity in detecting transient faults, Dutertre et al. [33] [34] propose replacing standard transistors 5 and 7 by high-threshold voltage transistors (HVT), and transistors 6 and 8 by low-threshold voltage transistors (LVT). Dutertre et al. also highlighted in [34] the importance of using triple-well CMOS technology in networks of NMOS transistors monitored by BBICS. This strategy, which embeds NMOS transistors into P-type wells isolated from P-substrate by N-type well implants, increases the robustness of monitored circuits and considerably improves the sensitivity of the sensor in detecting transient faults in pull-down CMOS networks. As the classic N-type wells in PMOS transistors

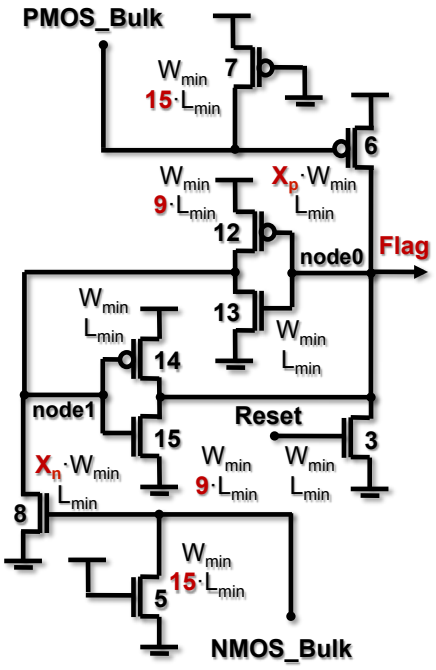


Fig. 3.3: Single BBICS architecture [104]. W_{min} represents the minimum diffusion width of the transistors, L_{min} is the minimum channel length, and X_n and X_p are design factors used for calibrating the sensitivity of the sensor in detecting transient faults.

of pull-up networks, the P-type wells play in monitored NMOS transistors a role of isolation from P-substrate that efficiently helps BBICS in identifying transient faults in pull-down CMOS networks. LVT and HVT transistors as well as the triple-well feature are provided by most of modern commercial technologies.

Champeix et al. [19] and Borrel et al. [11] have tested a single BBICS architecture in a bulk CMOS 90-nm chip. Moreover, they have performed fault injection campaigns with a laser facility for validating the approach.

3.1.2 BBICS architectures of Neto et al.

Authors of the first versions of BBICS [89] [91] present in [90] an enhanced architecture formed by a pair of sensors: PMOS-BBICS and NMOS-BBICS. Fig. 3.4 details only the NMOS-BBICS circuit for the sake of simplicity. The illustration omits the PMOS-BBICS and the trimming transistors, which work to compensate process variability in transistors 5 and 7.

The sensor shown in Fig. 3.4 also consists of two cross-coupled inverters that create a latch for fault register. Furthermore, it has additional transistors 9, 10, and 11 acting to increase the sensitivity of the sensor in detecting transient faults. On the contrary, we evidenced in [106] that the leakage power consumption is considerably grown by including these three transistors and using transistors 2 and 5 between NMOS_Bulk and gnd. As a compensation, a sleep-mode feature dedicated for BBICS is proposed in [106] to reduce the power consumption when the system is left on standby.

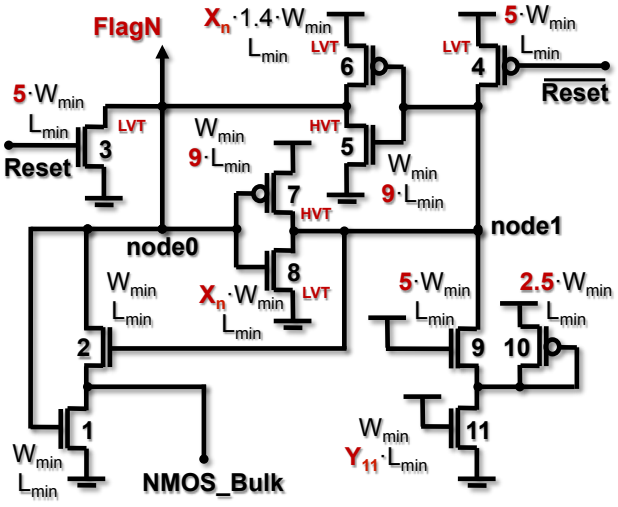


Fig. 3.4: State-of-the-art NMOS-BBICS architecture of Neto et al. [90]. W_{min}, L_{min}, X_n, and X_p are defined in captions of Fig. 3.3.

3.1.3 BBICS architectures of Zhang et al.

Zhang et al. [145] propose architectural improvements to BBICS of Neto et al. [90] with the intention of eliminating the leakage penalty. The architecture is also formed by a pair of PMOS-BBICS and NMOS-BBICS. Fig. 3.5 shows the PMOS-BBICS devised by Zhang et al. It is operationally similar to its predecessors, excepting by the presence of PMOS transistor 8. The sensor transistors 6 and 7, which make the leakage overhead negligible, were preliminarily

studied and suggested by Wirth [139] [138]. The circuit of the NMOS-BBICS of Zhang et al. is complementary to that illustrated in Fig. 3.5 for the PMOS-BBICS.

The architecture of Zhang et al. [145] has been improved in work [22] with the inclusion of CMOS amplifiers. The function of sensing the transient faults on the bulks is attributed to high-gain CMOS amplifiers, such as the previous works [4, 38, 69, 87, 88, 130] have proposed for monitoring and identifying faults on power rails. Even though an amplifier-based solution seems to be promising in terms of sensitivity in detecting transient faults, the sensor [22] built in a bulk 28-nm chip was experimentally reported in [133] as sensitive to voltage and temperature variations.

Zhang et al. [146] also reported practical results of Fig. 3.5 sensor embedded on bulk CMOS 90-nm chip. The sensor was tested under the effects of laser-based injection sources.

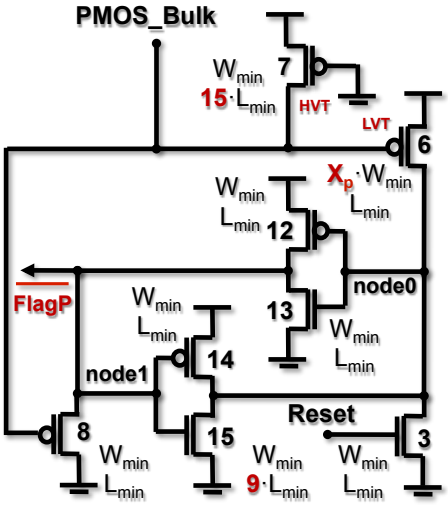
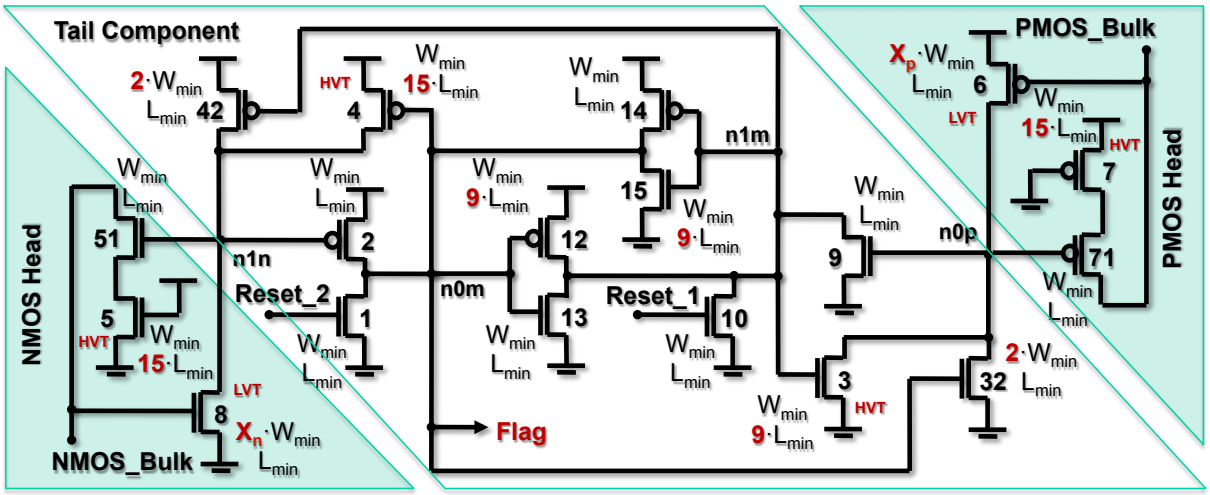


Fig. 3.5: State-of-the-art PMOS-BBICS architecture of Zhang et al. [145]. W_{min}, L_{min}, X_n, and X_p are defined in captions of Fig. 3.3.

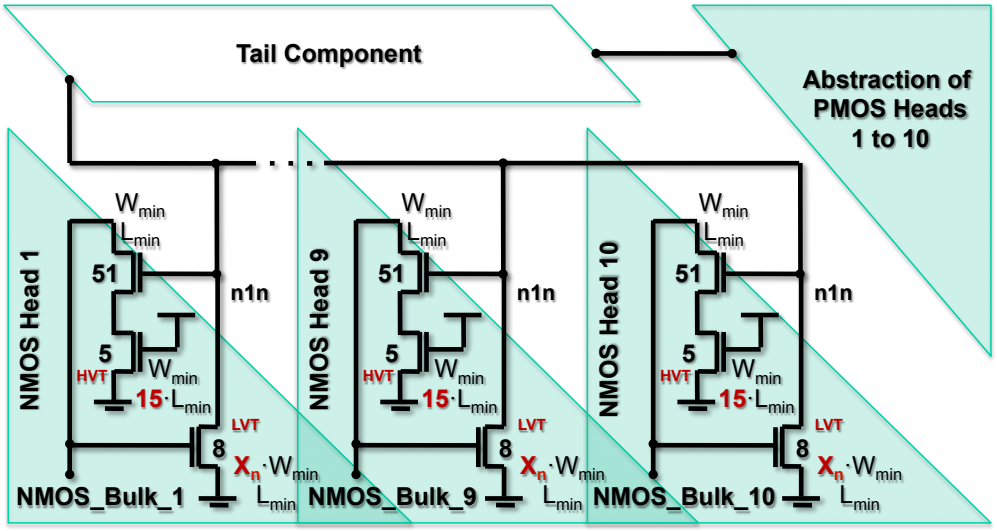
3.1.4 Modular BBICS architectures

We have presented in [118] [119] an efficient modular technique for reducing the area overhead introduced by BBICS architectures. The idea is to split the sensor into modules named as tails and heads. Fig. 3.6a details this technique applied on a BBICS architecture proposed in [104]. The sensor could be otherwise designed for monitoring the occurrence of transient faults in 10 pull-up and 10 pull-down CMOS networks, for instance; then the architecture will have 10 NMOS heads, 10 PMOS heads, and a single tail circuit shared by them, see Fig. 3.6b. This modular feature is also able to provide process and temperature robustness to the sensors thanks to the use of the several modules spread on the circuit under monitoring [118] [119].

In addition to take benefit from the modular technique, the circuits of Fig. 3.6a architecture [104] have been devised with attributes (operated by transistors 4 and 3) that facilitate the logic inversion of the latch (transistors 12, 13, 14, and 15). Consequently, it considerably improves the sensitivity of the sensor in detecting transient faults. Negligible power penalty is also reported due to the configurations of transistors 5 and 51 as well as 7 and 71, which ensure respectively the bias GND to the P-type wells and V_{DD} to the N-type wells.



(a)



(b)

Fig. 3.6: BBICS architecture [104] (a) using modular technique [118] (b). W_{min}, L_{min}, X_n, and X_p are defined in caption of Fig. 3.3.

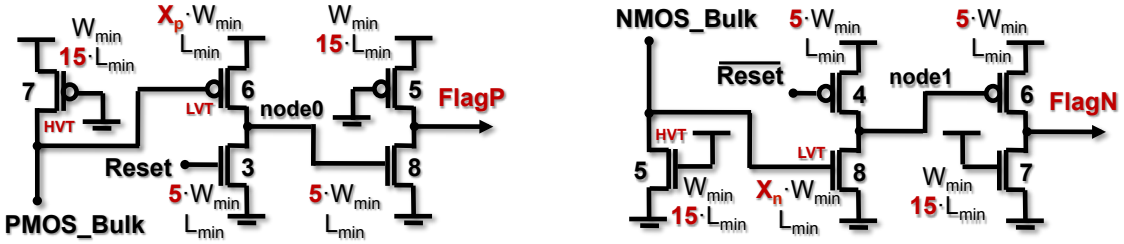
3.1.5 Dynamic BBICS architectures of Simionovski and Wirth

Simionovski and Wirth introduce in [120] the class of the dynamic BBICS architectures. Instead of the conventional latch of the previous static architectures, dynamic memory cells are used for smoothing the switching capacity of the memory node responsible for the fault register. With no feedback circuit wired to the memory node, the sensitivity of the sensor in detecting transient faults is increased and the transistor count of the sensor is reduced. Fig. 3.7 depicts the dynamic circuits featuring the detection of transient faults in pull-up and pull-down CMOS networks.

As any dynamic CMOS circuit, this first version of the dynamic BBICS [120] operates with the help of a reset signal. It periodically refreshes the sensor memory node that is not wired by a feedback circuit. The periodic reset is mandatory to remove accumulative leakage effects on the sensor output, and preventing consequent false indications of fault. Results in [120] show a dynamic BBICS designed on bulk CMOS 130-nm technology is able to properly function by using a short reset pulse with a period of 50 ns. It leaves, therefore, appropriate time for

digital systems deal with the fault indication provided by the sensor in case of transient faults. Simionovski and Wirth [121] have experimentally tested a bulk CMOS 130-nm chip with the sensor presented in Fig. 3.7.

The leakage current effects on the dynamic BBICS have been also studied in [122], and a solution for eliminating the periodic reset signal was presented. The strategy proposes to bias the reset transistors of the sensor for operating in the weak inversion region. Accordingly, a steady very low voltage offset is permanently applied on the place of the periodic reset voltage, ensuring, in fault-free scenarios, a stable operation of the dynamic memory nodes. This important BBICS feature [122] baptized of self reset copes with the former insensitivity of dynamic sensors in detecting transient faults during the short but periodic phases of reset.

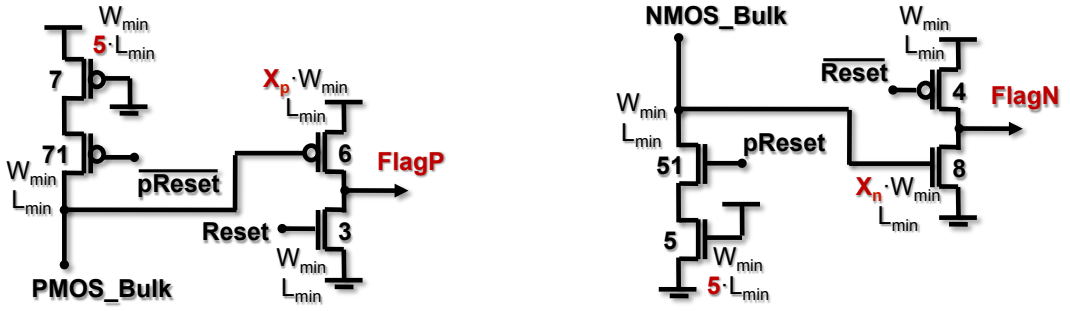


(a) (b)

Fig. 3.7: State-of-the-art dynamic BBICS architectures (a) and (b) of Simionovski and Wirth [120] for monitoring transient faults, respectively, in pull-up and pull-down CMOS networks. W_{min}, L_{min}, X_n, and X_p are defined in captions of Fig. 3.3.

3.2 New dynamic BBICS architecture

A new dynamic BBICS architecture is presented in Fig. 3.8. The innovations of the proposed BBICS considerably increment the sensor sensitivity in detecting transient faults at expense of negligible power overhead and with lower transistor count than previous architectures.



(a) (b)

Fig. 3.8: New dynamic BBICS architectures (a) and (b) proposed in this chapter for detecting transient faults in pull-up and pull-down CMOS networks. The bulks of the PMOS and NMOS transistors under monitoring are biased, respectively, by the voltages on PMOS_Bulk and NMOS_Bulk nodes, rather than the voltages on the power rails V_{DD} and GND. W_{min}, L_{min}, X_n, and X_p are defined in captions of Fig. 3.3.

The new features and differences of the proposed architecture (Fig. 3.8) with regard to the preceding dynamic BBICS [120] illustrated in Fig. 3.7 are:

1. In fault-free scenarios, the high ohmic transistors 7 and 5 detailed in Fig. 3.8 are responsible for biasing the bulks of the monitored PMOS and NMOS transistors, which are made more robust with the use of triple-well CMOS technology. Moreover, unlike other BBICS architectures, transistors 71 and 51 (respectively arranged in series with transistors 7 and 5) have the role of temporally including PMOS and NMOS bulk nodes in a floating state that facilitates the switch of the sensing transistors 6 and 8 during scenarios of transient faults. The detection sensitivity of the sensors are, therefore, improved at the cost of a periodic reset ($pReset$ in Fig. 3.8 and 3.9) on the gates of transistors 71 and 51, which operate to systematically ensure a suitable voltage bias of PMOS and NMOS bulks.

2. The large channel-length transistors 7 and 5 are isolated from the bulks through the minimum-size transistors 71 and 51. The number of parasitic elements connected directly to PMOS and NMOS bulk nodes is thus reduced, and the detection sensitivity of the sensor is enhanced by consequence;

3. With the two features described above, the proposed sensor does not need to use special HVT and LVT transistors for obtaining higher detection sensitivity than all previous BBICS architectures;

4. Thanks to the large channel-width transistors 6 and 8, the dynamic memory nodes $FlagP$ and $FlagN$ provide steady voltage signals during enough time to be dealt by other system's blocks that have the responsibility of applying recovery actions when transient faults occur;

In addition to the periodic reset $pReset$, the same conventional reset applied on any BBICS architecture for initializing their memory nodes ($Reset$ in Fig. 3.8) is employed on the gates of transistors 3 and 4. This reset signal can be either periodic such as in dynamic architecture [120] or can feature the self-reset property [122] mentioned in previous section.

The operation mode of our dynamic BBICS architecture (Fig. 3.8) is illustrated in Fig. 3.9, which details simulation results of a chain of 10 inverters being monitored by a PMOS-BBICS (Fig. 3.8a) and NMOS-BBICS (Fig. 3.8b). The injected single transient fault, represented by the transient voltage glitch on the PMOS bulk node, is successfully detected by the PMOS-BBICS when the sensor's output $FlagP$ goes to V_{DD}. The pulse on the node $Reset$ is generated by other system's block after the end of the procedure that processes the event of fault indication on the node $FlagP$.

The proposed dynamic BBICS (Fig. 3.8) were designed and verified on a commercial bulk CMOS 65-nm technology. Two cells representing the PMOS-BBICS (Fig. 3.8a) and NMOS-BBICS (Fig. 3.8b) were developed in the same way as the technology's standard cells were designed. The BBICS cells are applicable on the circuit under monitoring by replacing the filler cells that are liable for making the body-ties of the standard cells [33]. The layout of the NMOS-BBICS cell is presented in Fig. 3.10, and its design factors X_n and X_p in Table 3.1, which is further explained in section 3.4.

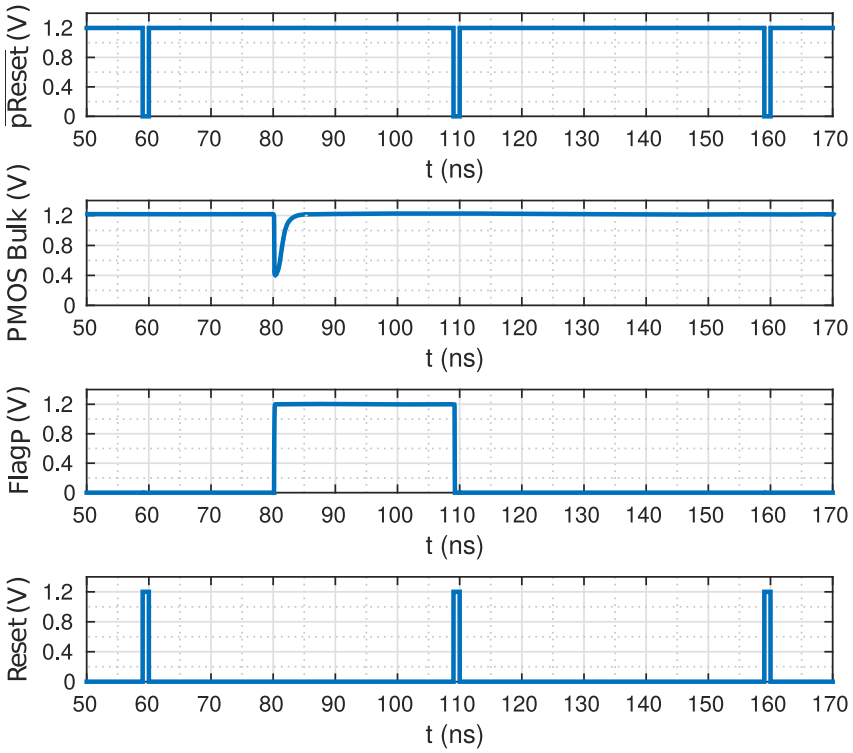


Fig. 3.9: Operation mode of the proposed dynamic PMOS-BBICS detecting the event of a single transient fault on the PMOS bulk node. The fault was injected on a chain of 10 inverters designed on CMOS 65-nm technology.

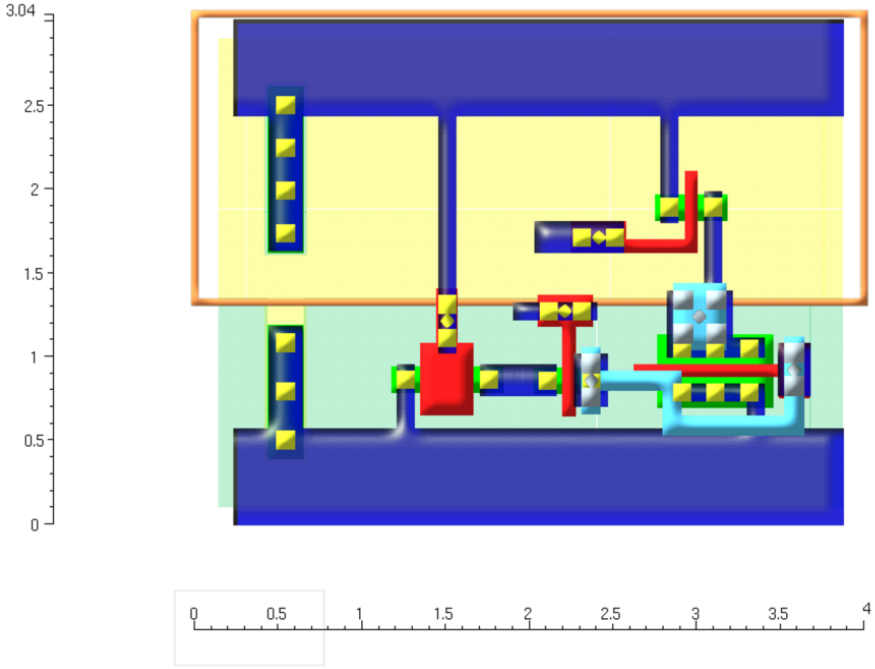


Fig. 3.10: Layout of the new dynamic NMOS-BBICS cell on CMOS 65-nm technology. The divisions of the dimension axis are in μm. The area of the proposed cell is comparable to the sum of three technology's NAND cells with minimum drive capabilities. The layout design of the PMOS-BBICS cell, which is not illustrated here, is complementary to this figure.

3.3 Sensitivity of a flip-flop in detecting transient faults

Memory elements like flip-flops or latches are sensitive to transient faults that have the capability to reach them and provoke primary transient harmful effects known as: (1) soft errors, which are non-permanent logic inversions of memory elements; or (2) delay errors, i.e. remarkable non-permanent variations on the typical delays of memory elements due to setup time violations.

Soft or delay errors will be produced in the circuit depending on the charge of the transient fault – the integral of the current curve in Fig. 3.1. If an anomalous current has a profile (charge) able to overcome electrical, logical, and latching-window masking effects [55] on a circuit; single or multiple soft errors or delay errors will be generated in memory elements. The smallest anomalous current profile that provokes non-permanent errors (soft or delay errors) is defined in this chapter as the sensitivity of a memory element in detecting transient faults. The threshold at which the memory element becomes sensitive to transient faults is, therefore, the lower bound of the range of transient faults able to induce non-permanent errors in the memory element. The upper bound of this range would be the smallest transient fault that makes permanent errors and can definitely damage the circuit.

3.3.1 Experiments for analyzing the sensitivity of a flip-flop in detecting transient faults

The sensitivity in detecting transient faults of the flip-flops, as numerous and fundamental memory elements of integrated systems, is a significant reference to determine the smallest profiles of transient faults that need to be detected by schemes like BBICS. Hence, we have studied in this work the sensitivity of the smallest flip-flop cell of a commercial CMOS 65-nm technology. The goal is to evaluate and compare it with the sensitivities of different BBICS architectures. Fig. 3.11 illustrates the circuit used as reference in this study. Electrical-level simulations were initially performed with typical conditions, nominal Vdd (1.2 V), 25 ^{o}C, and standard threshold voltage (SVT) transistors. The technology's smallest sized standard cells with parasitic elements were applied with the purpose of creating the circuit conditions that produce the smallest profiles of transient faults.

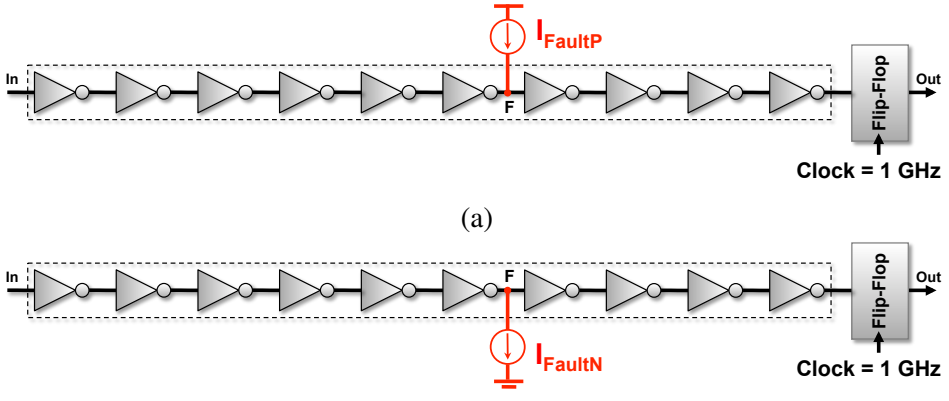


Fig. 3.11: Reference circuits of this study: chains of 10 inverters with a flip-flop. It is designed with the target technology's smallest standard cells with the aim of identifying the smallest profiles of transient faults (I_{FaultP} and I_{FaultN}) detectable by a flip-flop.

The influence of several different profiles of single transient faults was investigated on the reference circuits (Fig. 3.11) by using the classical transient-fault model for CMOS circuits [137] [80] that is detailed in [17] and [120]. The faults were electrically simulated by injecting either a double exponential current source I_{FaultP} or I_{FaultN} (Fig. 3.1) on the technology's most sensitive drain node, which is the drain with the lowest capacitance – i.e. node F (Fig. 3.11) between two inverter cells with the smallest dimensions in the technology's standard cell library.

Different profiles of single transient faults were injected by adjusting different current amplitudes and fall times on the parameters of I_{FaultP} (or I_{FaultN}). The rise times were always set on the order of 5 ps to keep the typical shapes of transient faults: short rise time and longer fall time [32] [36]. Several electrical-level simulations were thus done by sweeping the parameters of I_{FaultP} (or I_{FaultN}) up to find the smallest profiles of single transient faults that propagate through the inverters and provoke a soft error or a delay error in the flip-flop. In this study we consider as a delay error any flip-flop's typical delay variation that is higher than 10 %. In addition, as the shape of a transient fault is technology and event dependent, the sweep of the parameters of I_{FaultP} (or I_{FaultN}) was limited to not create voltage amplitudes higher than 110 % of Vdd. This strategy prevents the injection of voltage peaks that could lead the circuit to permanent errors or out of the technology's specifications.

3.3.2 Results and analysis of the sensitivity of a flip-flop in detecting transient faults

Fig. 3.12 shows the electrical-level simulation results of the circuits in Fig. 3.11. The vertical axis represents the minimum peak-to-peak voltage (on node F and normalized to Vdd) that is detectable by the flip-flop after I_{FaultP} (or I_{FaultN}) is injected with a fall time defined in the horizontal axis. For instance, if I_{FaultN} is applied on node F with a fall time of 200 ps (measured between 90 % and 10 % of the injected current amplitude), the resulting minimum detectable peak-to-peak voltage on node F is around 0.9 V (i.e. 75 % of 1.2 V). The flip-flop will thus suffer a soft or delay error if a single transient fault with 200 ps of fall time produces a peak-to-peak voltage on the node F greater or equal to 0.9 V. Fig. 3.12 allows, therefore, identifying the range of single transient faults that reach and produce non-permanent errors in the flip-flop. Note that single transient faults making peak-to-peak voltages on the order of 57 % of Vdd are still able to provoke soft or delay errors; however they require very long fall times to accomplish it (approximately 2200 ps).

Fig. 3.13 and Fig. 3.14 detail the smallest profiles of transient faults (I_{FaultP} and I_{FaultN}) that produce the peak-to-peak voltages of Fig. 3.12. Thereby, a single transient current injected into node F with a fall time of 200 ps needs at least an amplitude of nearly 120 μA (NMOS case) or 160 μA (PMOS case) to provoke a soft or delay error in the flip-flop. In Fig. 3.14, the respective minimum detectable injected charges (critical charges), which correspond the areas of the injected current curves (Fig. 3.1), are presented on the order of 13 fC (NMOS case) and 17 fC (PMOS case).

3.4 Analysis and comparison of BBICS sensitivities in detecting transient faults

This section analyzes previously discussed state-of-the-art BBICS architectures in terms of their sensitivities in detecting transient faults. In addition, we compare them with the dynamic BBICS proposed in this chapter.

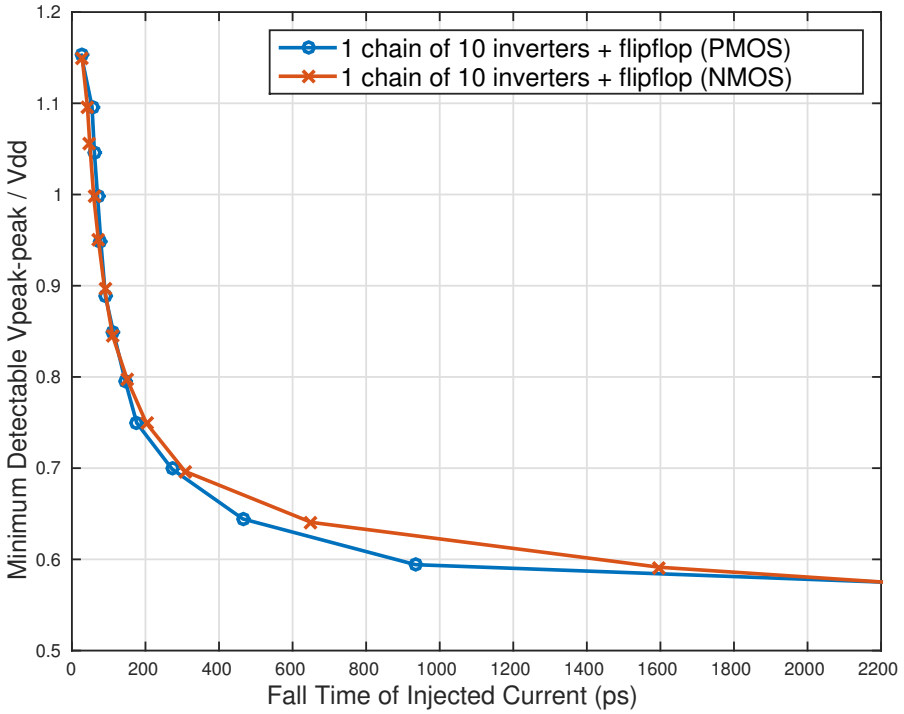


Fig. 3.12: Minimum peak-to-peak voltages (on node F and normalized to Vdd) that are detectable by a flip-flop (Fig. 3.11) after the injection of single transient faults (I_{FaultP} or I_{FaultN}) with fall times between 10 ps and 2200 ps; and a rise time on the order of 5 ps.

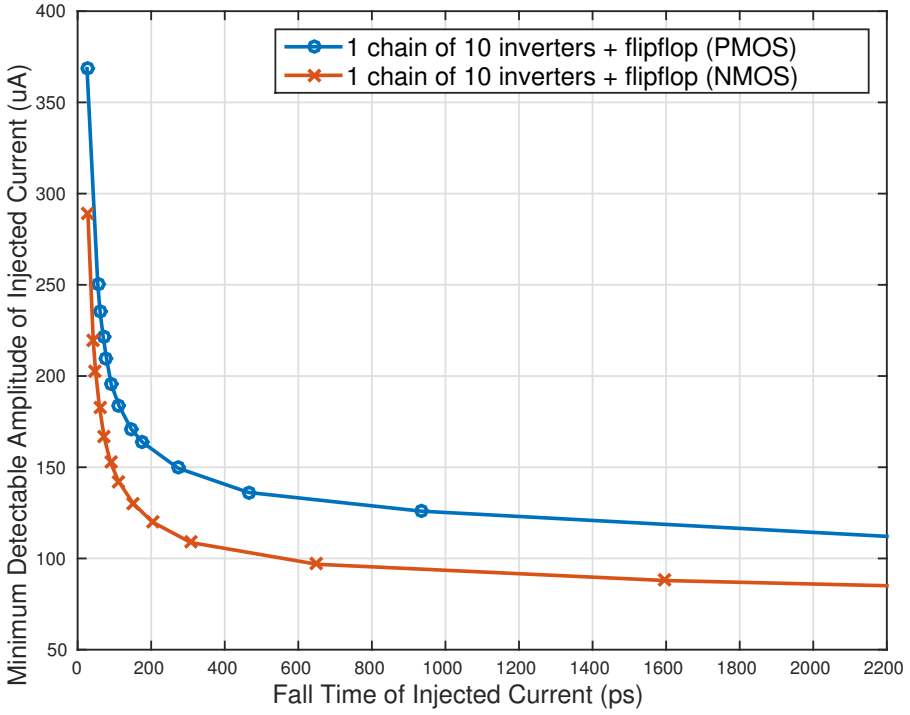


Fig. 3.13: Minimum current amplitudes (injected on node F) that are detectable by a flip-flop (Fig. 3.11). The related injected currents, in function of different fall times (horizontal axis), create the peak-to-peak voltages illustrated in Fig. 3.12.

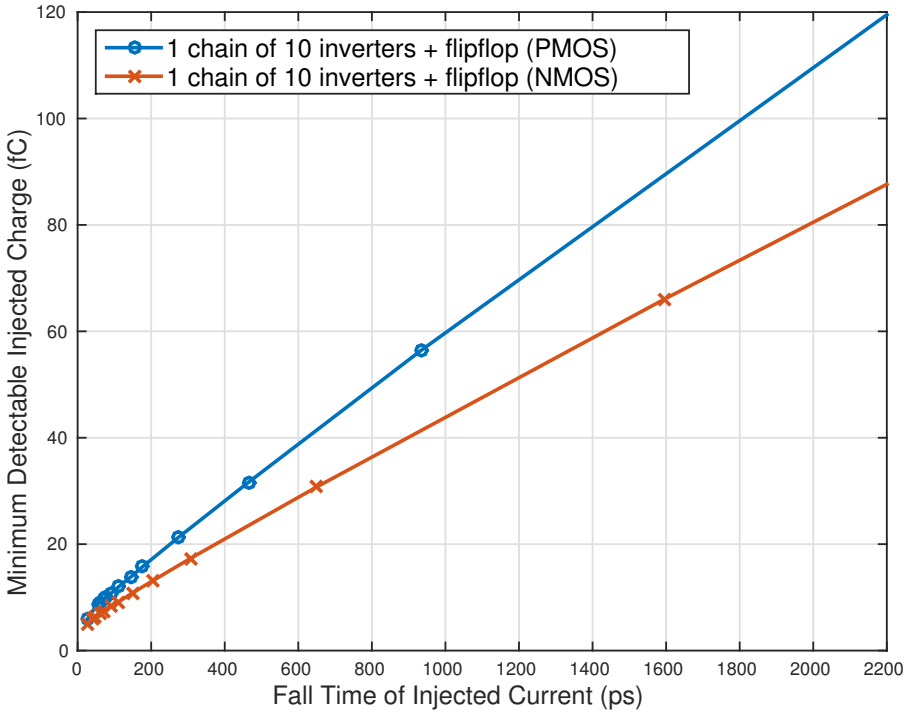


Fig. 3.14: Minimum charges (injected on node F) that are detectable by a flip-flop (Fig. 3.11). The related injected currents, in function of different fall times (horizontal axis), create the peak-to-peak voltages illustrated in Fig. 3.12.

3.4.1 Experiments for sizing BBICS architectures

All BBICS architectures were electrically simulated monitoring chains of 10 minimum-sized inverters under the same conditions of experiments described in section 3.3.

BBICS in Fig. 3.3 is denominated herein as "sbbics", and its improved version (using HVT transistors instead of SVT transistors 5 and 7, and LVT transistors replacing transistors 6 and 8) is defined as "shsbbics". Furthermore, the sensors in Fig. 3.4, 3.5, 3.6a, 3.6b, and 3.7 are named respectively "bbics", "zbbics", "t1hbbics", "t10hbbis", and "dbbics". The dynamic BBICS proposed in this chapter (Fig. 3.8) is labeled with "idbbics". Both NMOS-BBICS and PMOS-BBICS circuits of "bbics", "zbbics", "dbbics", and "idbbics" architectures were taken into account in the analysis of this section.

For the "bbics" architecture, we have set $Y_{11} = 9 \cdot L_{\text{min}}$ in PMOS-BBICS; $Y_{11} = 45 \cdot L_{\text{min}}$ in NMOS-BBICS [90]; and the trimming configuration calibrating the sensors with their best sensitivities in detecting transient faults. The dynamic architectures "dbbics" and "idbbics" were both simulated with a periodic reset pulse of 500 ps repeated each 50 ns (Fig. 3.9). In addition, even though the original circuit propositions of "bbics" [90], "zbbics" [145] [146], and "dbbics" [120] [121] do not mention the use of LVT and HVT transistors for improving the sensor sensitivity [33] [34], we have used them in the simulated designs of this experiment in order to perform the full potential of such BBICS architectures. Original architectures "zbbics", "bbics", and "dbbics" were, therefore, also enhanced with LVT and HVT transistors in the same way of the other state-of-the-art BBICS analyzed in this chapter with the aim of making a fair comparison of their sensitivities in detecting transient faults. In the proposed "idbbics" architecture, nevertheless, LVT and HVT transistors are not required to calibrate competitive sensitivity, then only SVT transistors were used.

For each BBICS architecture under analysis, similar transistor sizing strategy was applied, and the optimal values for the design factors X_n and X_p were obtained from several simulations under the effect of a typical single short transient fault [32] [36]. The single fault was injected into the node F (Fig. 3.11) with a rise time of 5 ps, a fall time of 50 ps, and a current amplitude that create a voltage amplitude below 100 % of Vdd in each simulation scenario. Moreover, the simulations have swept X_n from 1 to 15, and X_p from 1 to 21. The minimum values of X_n and X_p with which the sensors have succeeded in detecting the lowest current amplitude were elected as the optimal. Table 3.1 summarizes the optimal values of the design factors X_n and X_p that were found.

Table 3.1: Taxonomy of BBICS architectures analyzed in this chapter: total number of transistors (NMOS-BBICS + PMOS-BBICS circuits), and optimal values for the design factors X_n and X_p

BBICS Architecture	Reference	Section	Figure	Class	Number of Transistors	X_n	X_p
sbbics	[107] [108] [19]	3.1.1	3.3	Static	9	10	16.8
shsbbics	[107] [108] [33]	3.1.1	3.3 with HVT and SVT transistors	Static	9	11	16.8
bbics	[90]	3.1.2	3.4	Static	$11 + 11 = 22$	12	12
zbbics	[145] [146]	3.1.3	3.5	Static	$8 + 8 = 16$	14	16.8
t1hbbics	[104]	3.1.4	3.6a	Static	$1 \cdot 3 + 1 \cdot 3 + 12 = 18$	10	16.8
t10hbbics	[104] [118] [119]	3.1.4	3.6b	Static	$10 \cdot 3 + 10 \cdot 3 + 12 = 72$	8	12.6
dbbics	[120] [121]	3.1.5	3.7	Dynamic	$5 + 5 = 10$	13	14
idbbics	this work	3.2	3.8	Dynamic	$4 + 4 = 8$	5	5.6

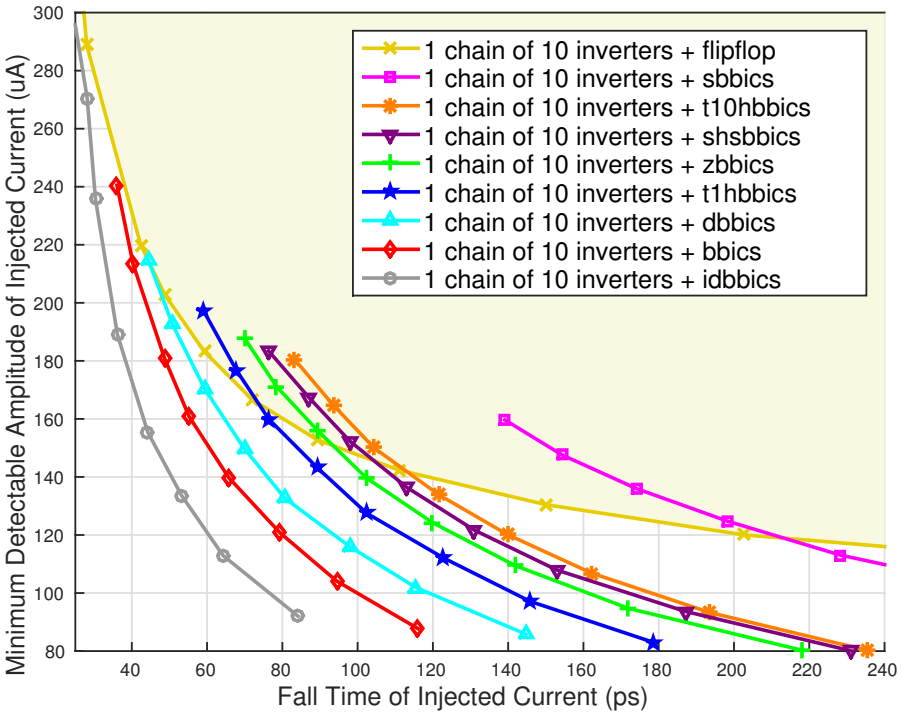
3.4.2 Experiments for analyzing the sensitivities of BBICS architectures in detecting transient faults

Several electrical-level simulations were performed such as the experiments described in section 3.3 for a flip-flop; however the goal here was to identify the minimum injected currents that can be detected by a BBICS architecture monitoring the same chain of 10 inverters (Fig. 3.11).

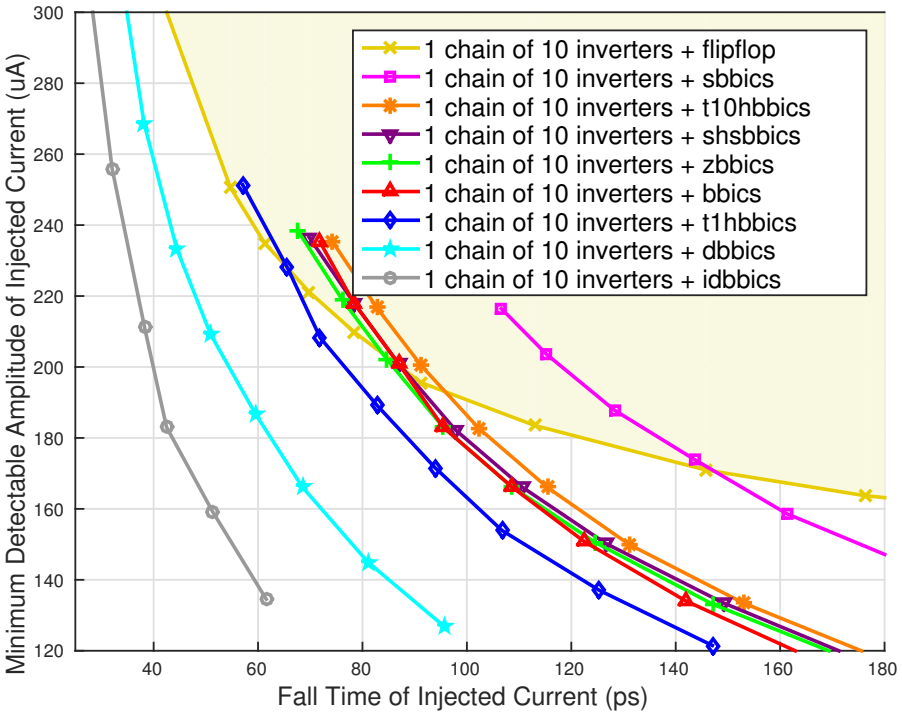
The previously determined curves of minimum injected currents that are detectable by a flip-flop (Fig. 3.13) are also used in this section as references to evaluate the different target BBICS architectures. Theses references allow verifying if a sensor is sufficiently sensitive to detect the smallest profiles of transient faults that cause soft or delay errors in the technology's smallest flip-flop. Moreover, if a sensor is able to detect these reference profiles of injected currents; currents with larger profiles will be also detectable as they have more charge to overcome the thresholds of the sensor.

3.4.3 Comparative analysis of BBICS detection sensitivities

Fig. 3.15a and 3.15b present respectively the curves of minimum injected currents I_{FaultN} and I_{FaultP} that are detectable by the sensors protecting a chain of 10 inverters (Fig. 3.11). The graphics show thus the trends of each sensor in terms of their sensitivities in detecting transient faults. For instance, Fig. 3.15a highlights that a transient fault with 5 ps of rise time, 150 ps of fall time, and 130 μA of amplitude will cause a soft or delay error in the flip-flop; and it will be detected by all BBICS architectures except the "sbbics". Supposing however another scenario in which the fault has also 5 ps of rise time, 150 ps of fall time, and 160 μA of amplitude; even the architecture "sbbics" is able to detect it. Therefore, the lower is the curve of a sensor regarding the reference (flip-flop's curve), the higher is the sensor's sensitivity in detecting transient faults.



(a)



(b)

Fig. 3.15: Minimum injected currents I_{FaultN} (a) and I_{FaultP} (b) that are detectable by a BBICS architecture monitoring a chain of 10 inverters. Flip-flop's curves from Fig. 3.13 were redrawn here to indicate reference thresholds in which a single transient fault provokes a soft or delay error in the flip-flop.

Comparing the curves of the different BBICS architectures in Fig. 3.15, we note the proposed dynamic sensor "idbbics" has the lowest curves regarding the flip-flop's references, thereby the highest sensitivity in detecting transient faults. The key difference of such a proposed architecture is indeed the propriety of periodically biasing bulks of monitored PMOS and NMOS transistors on triple-well CMOS technology. The sensor is even able to cover the detection of short and long transient faults that do not provoke soft and delay errors in the flip-flop ("idbbics" curves below flip-flop's curves). This extra coverage of transient faults is extremely useful for either advancing preventive security alarm actions against fault injection-based attacks or, as discussed in next subsection, reducing the area overhead to the monitored system.

We also observe only dynamic sensors ("dbbics" and "idbbics") are able to detect all short transient faults (with fall time below 70 ps) that produce soft or delay errors in the flip-flop ("dbbics" and "idbbics" curves below flip-flop's curve). Otherwise, all BBICS architectures have the ability of detecting longer transient faults (with fall time above 220 ps).

On the other side, the static architecture "sbbics" reveals having the lowest detection sensitivity, although the application of HVT and LVT transistors [33] (instead of SVT transistors) consistently improves the sensor as Fig. 3.15 notices with the lower curves of the architecture "shsbbics" (legends in figures are on the same order of the curves). This result clearly illustrates the effectiveness of HVT and LVT transistors in enhancing the detection sensitivity of BBICS architectures.

Fig. 3.15a also highlights NMOS-BBICS of the static architecture "bbics" with a high detection sensitivity, confirming the contribution of transistors 9, 10, and 11 that create a voltage offset on node1 for reducing the switching efforts of the sensor's latch. Nevertheless, the consequent power consumption of the monitored system, for example, a chain of 10 inverters, is increased by a factor of 80. It is substantially different from all other BBICS architectures that impose negligible power overhead thanks to the direct connection of the sensor's high-ohmic and low-threshold transistors to the bulks of the monitored circuit.

Note additionally in Fig. 3.15, the application of the modular technique with multiple heads and a single tail slightly attenuates the detection sensitivity of the sensor (compare "t10hbbics" and "t1hbbics" curves). This reduction is related to the higher number of transistors monitored by the architecture "t10hbbics", whose tail circuit is influenced by more parasitic elements. Equivalent reduction would happen on the detection sensitivity of the other state-of-the-art BBICS architectures if they were organized in the same way, i.e. with multiple heads and a single tail. The trick of splitting the sensor into multiples heads and tails is however useful like an additional parameter to make better trade-offs between detection sensitivity of the sensor and its resulting area overhead to the monitored system.

3.4.4 Influence of the monitored area size on the detection sensitivities of BBICS architectures

The sensitivity of a BBICS in detecting transient faults is decreased in function of the number of monitored transistors. As more parasitic elements are included in the network monitored by the sensor, the amount of anomalous current (I_{FaultN} or I_{FaultP}) able to reach the sensor is reduced, lowering the sensor's ability in identifying it. Results in Fig. 3.16 demonstrate this phenomenon in the cases of only one PMOS-BBICS architecture monitors either 1, 4, or 6 chains. The dynamic architectures ("dbbics" and "idbbics") present similar detection sensitivities when 4 chains of 10 inverters are monitored, however they are lower whether compared with the case of 1 chain of 10 inverters. Besides, the curves show that the detection sensitivity of the static

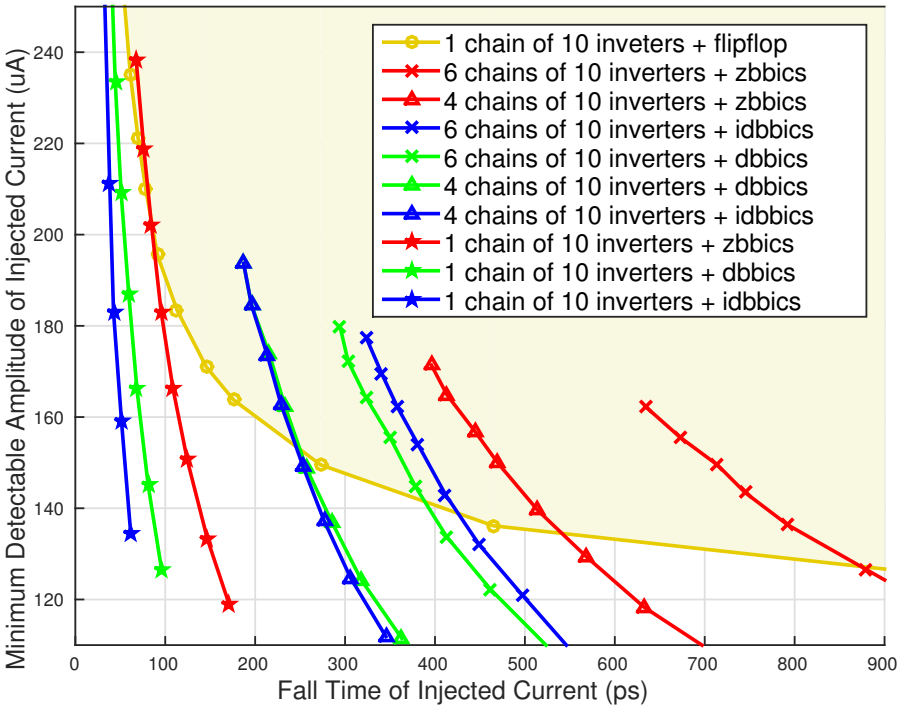


Fig. 3.16: Minimum injected currents I_{FaultP} that are detectable by a PMOS-BBICS architecture monitoring either 1, 4, or 6 chains of 10 inverters.

architecture "zbbics" is much more reduced with the number of monitored transistors than its dynamic counterparts. Finally, note that different from all other BBICS architectures, the sensor "idbbics" proposed in this chapter has still design space to improve the results from Fig. 3.16 by increasing the design factors X_n and X_p as well as by using LVT and HVT transistors.

3.4.5 Estimation of the area overhead imposed by BBICS architectures on the monitored systems

Fig. 3.17 estimates the area overhead imposed by each BBICS architecture based on the diffusion areas of the transistors ($W \cdot L$), which were calculated with help of the design factors discussed in previous subsection 3.4.1. The architecture "idbbics" proposed in this chapter imposes the lowest area overheads on the monitored systems (chains of 10 inverters) thanks to its smaller design factors and the lower number of transistors. For instance, if one PMOS-BBICS and one NMOS-BBICS of the sensor "idbbics" are applied to monitor 6 chains of 10 inverters, the consequent area overhead will be around 12 %, while other BBICS architectures will lead to values higher than 36%.

The area overhead can be further reduced, at expense of lowing the sensor's detection sensitivity, whether more transistors are included in the network monitored by one sensor (see previous subsection). This strategy would be suitable for applications requiring lower detection sensitivity or with a known range of transient faults to be detected. On the other side, if a single sensor (or a pair of NMOS-BBICS and PMOS-BBICS) is protecting a system's block with a size on the order of a chain of 10 inverters, the area overhead might be prohibitive whether all system has to be monitored (see Fig. 3.17); however the detection sensitivity would be much higher. Alternatively, if only the most sensitive parts of the systems are selected to be monitored

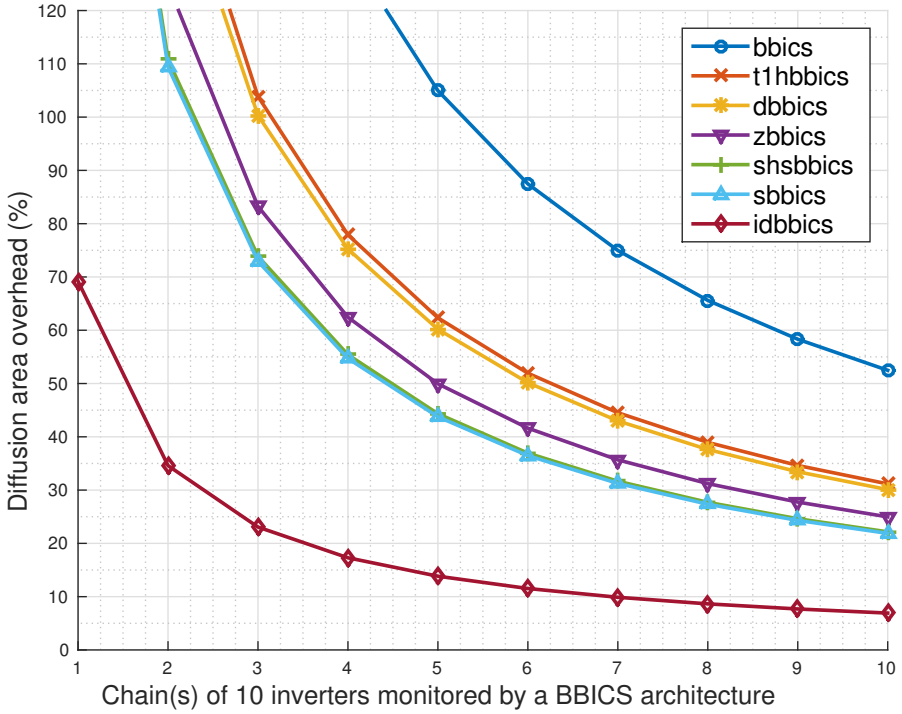


Fig. 3.17: Estimated area overhead included by a BBICS architecture (a single sensor or one PMOS-BBICS and one NMOS-BBICS) that monitors a system with X chain(s) of 10 inverters (X between 1 and 10).

by BBICS circuits, the overall area overhead can still be significantly reduced.

3.4.6 Corner analysis of BBICS architectures

The same electrical-level simulation experiments described in previous section 3.3 were applied for analyzing the BBICS architectures under process and temperature variations.

Normalized results of the minimum injected charges (integral of I_{FaultP} or I_{FaultN}) detectable by the BBICS architectures are presented in Table 3.2 for the following corner conditions: FF 25 ^{o}C; SS 25 ^{o}C; TT 25 ^{o}C; TT 75 ^{o}C; and TT -40 ^{o}C. The charges are normalized to the minimum injected charges able to provoke soft or delay errors in the flip-flop. All normalized charges in the table correspond to the smallest profiles of single transient faults (with 5 ps of rise time) that create a voltage on the order of 80 % of Vdd (0.96 V) on the node F of a chain of 10 inverters (Fig. 3.11) monitored by a BBICS architecture.

From the table, excepting the architecture "bbics", which requires another on-the-fly trimming bit configuration for compensating the variations in FF and SS corners, all other BBICS architecture are able to operate under process and temperature variations. Nevertheless, depending on the corner condition, the detection sensitivities of the sensors are reduced. The proposed architecture "idbbics" are in all corners either much more sensitive to detect transient faults than the flip-flop or very close to it. This result gives an important margin to reduce the area overhead as we discuss in previous subsections 3.4.4 and 3.4.5.

Table 3.2: Normalized corner results: minimum injected charges that are detectable by the BBICS architectures when I_{FaultP} (PMOS case) or I_{FaultN} (NMOS case) induces a voltage on the order of 80 % of Vdd on the node F (Fig. 3.11).

BBICS Architecture	**Normalized Minimum Detectable Injected Charge**									
	PMOS Case					**NMOS Case**				
	FF	**SS**	**TT**	**TT**	**TT**	**FF**	**SS**	**TT**	**TT**	**TT**
	25 ^{o}C	**25 ^{o}C**	**25 ^{o}C**	**75 ^{o}C**	**$-$40 ^{o}C**	**25 ^{o}C**	**25 ^{o}C**	**25 ^{o}C**	**75 ^{o}C**	**$-$40 ^{o}C**
flipflop	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
bbics	NO	NO	1.08	0.81	0.71	NO	1.75	0.82	0.67	0.26
sbbics	1.20	1.62	1.40	1.25	1.68	1.47	2.21	1.84	1.64	2.19
shsbbics	0.85	1.30	1.08	0.99	1.26	0.99	1.53	1.27	1.14	1.45
t1hbbics	0.80	1.14	0.97	0.89	1.09	0.85	1.31	1.08	0.98	1.22
t10hbbics	0.90	1.32	1.12	1.04	1.27	1.07	1.58	1.33	1.24	1.45
zbbics	0.85	1.26	1.06	0.97	1.25	0.93	1.45	1.19	1.08	1.39
dbbics	0.35	0.42	0.70	0.60	0.67	0.60	0.59	0.92	1.23	1.31
idbbics	0.40	0.45	0.54	0.57	0.66	0.26	0.27	0.68	1.13	1.19

3.5 Conclusions

This chapter reviews the different types of static and dynamic BBICS architectures by analyzing their sensitivities in detecting single transient faults. Moreover, a new dynamic BBICS architecture is presented, offering considerable advantages in terms of detection sensitivity and area overhead.

The BBICS application on integrated system designs brings several other complementary benefits. The integration in commercial IC design flows is feasible by simply replacing standard filler cells [42]. The reuse of the filler cell areas, besides making the sensors more sensitive in detecting transient faults, reduces the inherent costs associated with any type of robustness technique. BBICS-based recomputing techniques are applicable for recovering processors from the effects of transient faults [68] [65] [105] [109]. Furthermore, unlike most existing techniques, long-duration and multiple transient faults are also detectable by BBICS [68] [131]. All these features represent important contents for the design of more robust integrated systems in modern technologies.

In the advent of advanced fabrication processes, such as FD-SOI technology with which different body voltages are allowed for managing system performance and power consumption, the design space becomes even wider with the double function of BBICS cells in locally biasing system blocks as well as detecting the occurrence of transient faults.

Chapter 4

Monitoring body terminals of transistors for detection of layout-level Trojans

Over the last years with the fast technology enhancement, IC companies tend to outsource phases of their production chains in order to reduce time-to-market and development costs. Despite the outsourcing benefits, serious security concerns today affect all phases of IC-design flows. Malicious third-party suppliers may, for instance, intentionally cause operational disturbances, disable functions, alter layout masks, and even leak sensitive information from original circuits, all by including mechanisms defined as hardware Trojans (HT) [126]. As a consequence of circuit vulnerabilities to HT insertions, engineers and researchers systematically inspect possible new threats. Prominent taxonomy [114, 136] abstracts HT implementations at different IC-design levels: system, development environment, register transfer, gate, layout, and physical. On the other side, HT issues also motivate the development of counter-measures to protect the trustworthiness of circuit designs. Diverse effective test-time methods based on side-channel analysis have been devised to detect HT without destructing the device under Trojan test (DUTT); they are classified into 7 side-channel categories [83, 85], each one with several interesting works not exhaustively cited in the following: (1) transient current (power consumption) [2, 134]; (2) quiescent current (Iddq) [1]; (3) delay (circuit paths) [16, 52]; (4) thermal [97]; (5) oscillation frequency (embedded ring-oscillators) [144]; (6) radiation (electromagnetic) [2, 92]; and (7) multiple parameters (combination of different side-channel categories) [13, 86, 97].

This chapter proposes a novel HT-detection method that implies the creation of a new category in the previously mentioned taxonomy of side-channel analysis-based techniques. The proposed method indirectly analyzes HT-induced variations on the electrical impedances of DUTT subcircuits by injecting a short train of current pulses into body terminals of their MOSFETs. More precisely, the analyzed side channel is indeed digital signatures related to the impedance of the subcircuit's substrate, and provided by a preexisting built-in current sensor connected to all body terminals of the subcircuit's transistors. This type of sensor [91], which ensures also appropriate bias to the body terminals by replacing certain filler cells of the DUTT [42], was only used until now as online-testing devices for detecting radiation- or laser-induced transient currents that may provoke soft errors in memory elements [19, 68, 121]. Nevertheless, we reuse it here as an offline-testing mechanism, without degrading its run-time feature of detecting transient currents. By applying a short train of current pulses (with different amplitudes) into a DUTT's global body terminal, each sensor will detect or not the pulses in function of their amplitudes and the impedance of the subcircuit's substrate, delivering a train of voltage

pulses that represent a digital signature of the DUTT. In case of a Trojan-infected subcircuit, the impedance of the subcircuit's substrate will modify with the presence of any HT, altering, consequently, the digital signature of the DUTT, and making the HT detection likely by comparing it with a Trojan-free signature. On the contrary, sampling a set of digital signatures by subcircuit is necessary for statistically distinguishing HT-induced variations from process variations. Unlike most existing side-channel analysis-based techniques, the proposed method requires no switching activity in data paths and no analog measurements. Hence, input test-vector generation and measurement noise are not issues, and the detection of stealth and tiny HT that have only turned-off transistors and negligible leakage currents are more likely.

Next sections detail the three main innovative contributions of this work: (1) current pulses are injected into body terminals of DUTT subcircuits; (2) built-in current sensors are connected to body terminals for identifying or not the injected currents, providing digital signatures of the subcircuit's substrates; (3) resulting digital signatures allow indirect analysis of the impedance of subcircuit's substrate, which is modified with the presence of HT, opening a new category of side-channel analysis-based techniques. The works of this chapter are within the thesis context of my Ph.D. student Leonel Guimarães, it was presented in the international conferences DAC 2017 and ISVLSI 2017.

4.1 Background

4.1.1 Testing methods for detection of HT

For ensuring the IC trustworthiness, post-manufacture testing phase must fit for the detection of threats such as HT. If the concern is an untrusted foundry, three main classes of techniques for detecting Trojan are known [85]: (1) physical inspection by scanning optical microscopy or scanning electron microscope (SEM); (2) functional testing; and (3) side-channel analysis.

Physical inspection techniques propose reverse engineering the DUTT by analyzing its physical layout and checking if the fabricated circuit is Trojan-free. For instance, a SEM-based method [27] demonstrates the possibility of detecting Trojans in CMOS 130-nm technology. Despite presenting reliable results, these techniques feature some drawbacks such as being expensive, time-consuming, destructive, and difficult to be integrated into the regular testing phase. Hence, even though a DUTT is stated as Trojan-free, it cannot be reused after the physical inspection. On the other hand, the approach is suitable to certify Trojan-free DUTT samples (i.e. golden IC samples), providing a set of fingerprints that are indeed referential data collected before the physical inspection alters the chips. The data from Trojan-free DUTT samples are afterwards statistically comparable with results from a DUTT sample, allowing to classify it as infected or not.

Functional-testing techniques like in [18, 51] apply data vectors at DUTT primary inputs with the intention of stimulating the HT activation and checking possible modifications at DUTT primary outputs. If the expected outputs are not obtained, DUTT is classified as a potentially Trojan-infected candidate. Nevertheless, activating HT may be a very complicated issue as attackers can design it to be activated only under rare circumstances [126], making the detection by functional testing quite challenging.

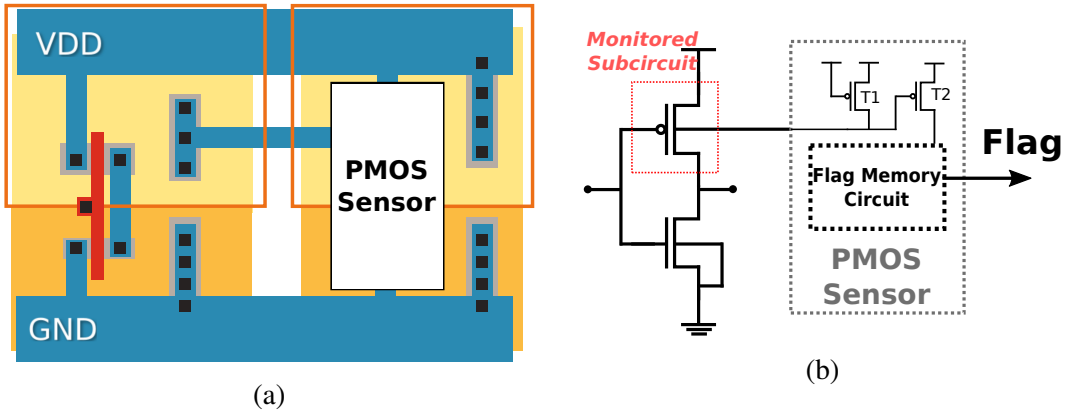
Inactive HT alter, however, DUTT side-channel signals such as quiescent current, delay, power, or electromagnetic activity variations. Hence, side-channel analysis, unlike functional-testing techniques, are able to detect even inactive HT. Many HT detection methods, comparing DUTT side-channel signals with referential data (from Trojan-free DUTT samples), are pro-

posed by measuring, for instance, power [2, 134], quiescent supply current (Iddq) [1, 13], path delay [16, 52], thermal property [48, 97], and electromagnetic radiation [2, 92] signatures. Furthermore, another technique [144] proposes implementing several ring oscillators distributed across the chip in order to evaluate a possible oscillation frequency deviation caused by a HT. Side-channel analysis may fit properly for the detection of HT that have at least one MOSFET in ohmic or active modes (turned-on), since an extra current is thus allowed to flow between transistor's drain and source. If it is the case for gate-level Trojans, the same may not be for layout-level Trojans in which not necessarily there is a turned-on transistor. Consequently, as a HT can be a few MOSFETs in subthreshold mode (turned-off) [6,41,62], HT-induced variations on the subthreshold leakage currents (which are already intrinsically low) would be difficultly detectable in today's complex integrated systems.

4.1.2 Built-in sensors for detecting anomalous transient currents in subcircuit's substrate

Built-in current sensors connected to MOSFET body terminals are originally proposed to detect transient currents [91]. The so-called body or bulk built-in current sensors (BBICS) explore the presence of an abnormal current peak flowing from the bulk (body) to the drain (or vice versa) of the disturbed transistor if a transient current is induced by radiation or laser sources [19,68,121]. Whenever this current is detected, the sensor indicates it by setting its output flag. BBICS are implemented in the DUTT design by replacing the regular filler cells used to bias the body terminals of DUTT transistors [42]. Therefore, the sensor becomes responsible to bias and monitor the body terminals of DUTT transistors. Fig. 4.1 illustrates the sensor's implementation showing the layout (Fig. 4.1a) of a single inverter being monitored by a PMOS sensor. Note that PMOS body terminal of the target subcircuit is attached to the PMOS sensor instead of being connected directly to the Vdd line. Fig. 4.1b presents the basic BBICS architecture composed of a biasing and a sensitive transistor (T1 and T2). The occurrence of a transient current can lead T2 to its active mode, generating the output flag. The flag memory circuit is responsible for holding and resetting the output.

For monitoring both pull-up and pull-down CMOS networks, the sensor architecture must be designed in CMOS triple-well technology [34] with its body terminal attached to the NMOS sensor. As the scope of this chapter is not precisely detecting transient currents, the NMOS sensor is omitted from our study in order to simplify the analysis; however its operation is



(a) (b)

Fig. 4.1: Layout of an inverter monitored by the PMOS sensor (a) and its schematic view (b).

analog to the PMOS. PMOS sensor will be applied in this chapter to detect gate-level Trojans as well as layout-level Trojans modifying PMOS networks. However, if NMOS sensor is also applied, even layout-level Trojans in NMOS transistors are able to be detected.

BBICS operation is presented in Fig. 4.2. The current pulse in the PMOS body terminal causes a disturbance on its voltage, and the sensor is able to detect it depending on its sensitivity in detecting transient currents [79, 104]. Thus, the sensor generates a flag indicating the incoming current if its amplitude and duration (current profile) are sufficient to exceed the detection threshold of the sensor.

The sensor sensitivity in detecting transient currents depends essentially on two conditions: the transient current profile and the monitored circuit. In short, considering the same profile of transient current, the lower the amount of transistors under monitoring by the sensor, better the sensor sensitivity. As a circuit in today's technology has about billions of transistors, as a way to improve the sensor sensitivity, the designer can split the circuit into smaller subcircuits. Each subcircuit must have a sensor monitoring all transistor that compose it. Therefore, the designer can choose conveniently the amount of transistors that the sensor will monitor in each subcircuit depending on the desired sensitivity.

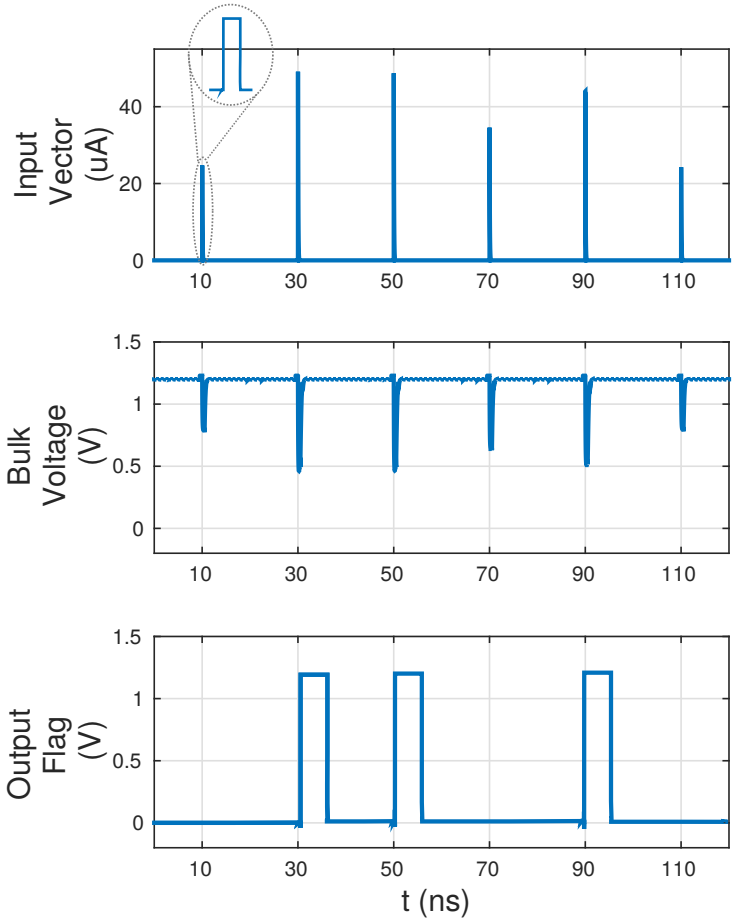


Fig. 4.2: Representation of current injections on the PMOS bulk, the consequent impacts on the PMOS bulk voltage, and the output flags generated or not by the sensor.

4.2 Proposed HT detection method

The proposed method relies on the assumption that the modification or addition of instances to the DUTT leads to physical alterations of the original substrate impedance. Moreover, considering the number of transistors influencing the substrate impedance is lower if the DUTT size is smaller, the HT effects will be more accentuated, facilitating its detection. To this end, the substrate of the DUTT is partitioned into several subcircuits, each one with an independent body bias, i.e. the transistors of a subcircuit share their body terminals independently of the other subcircuits. The proposed method monitors the body terminals of subcircuits by using current sensors built in each one of the subcircuits. Injecting a train of current pulses into the body terminal of the subcircuits, the sensors are able to identify voltage peaks induced on the body terminals. If a HT is inserted in a subcircuit, the substrate impedance of the subcircuit is modified, and the sensor may or not detect on the body terminals the induced voltage peaks that are slightly altered with the HT presence. Thereby, the sensor responses (signatures) to a given train of different current pulses are statistically compared with golden results from Trojan-free DUTT samples in order to classify if a set of DUTT samples is infected or not.

4.2.1 Injection of current pulses into MOSFET body terminals of DUTT subcircuits

In order to inject a current in the body terminal of the circuit, one can promptly highlight three alternatives: internal or external current direct injection and laser attack to induce current. The direct insertion of a current peak in the body terminal by an external source gives total controllability of the current profile and can be simply integrated to the testing phase. Despite featuring such properties, it requires an extra analog pin in the DUTT, which could be an issue depending on the design constraints. On the other hand, an internal source can be implemented to produce current pulses with controllable amplitude set by a digital input vector. Although the addition of a new analog pin is not needed, the range of possible amplitudes is limited by the size of the input vector as well as other waveform parameters. If the DUTT is divided into several subcircuits, such approaches require at least an additional transistor to replicate the incoming current to each subcircuit, resulting in an extra area overhead. To mitigate this area overhead, the subcircuit's substrate could be attacked with a laser beam that would induce a current in the body terminal. Even though this approach does not require extra on-chip circuitry, it presents some inconveniences such as delay, cost, and complex integration with the regular testing phase.

Designers can choose conveniently the current injection strategy that better fits according to their needs. Further, the current amplitude must be set in such a way as to avoid latch-up. Some other waveform parameters such as the pulse width can be also exploited to evaluate the sensor sensitivity. In the following analysis, the method is evaluated with an external current source generating pulses with different amplitudes. Fig. 4.3 shows the current injection set-up used in the subsequent analysis. In this topology, the current generated by the external source is replicated to the body terminal of each subcircuit composing the DUTT. Nevertheless, the same analysis can also be applied for other current injection techniques.

4.2.2 Monitoring of current sensors built in DUTT subcircuits

To track the whole DUTT substrate, each DUTT subcircuit must have its body terminal attached to its own sensor. Initially, the sensor is designed to detect the current pulses generated by the

source presented in Fig. 4.3. Basically, the detection is achieved whether the injected current profile is larger than the detection threshold of the sensor. Therefore, if a set of subsequent current pulses with different amplitudes are injected in the body terminal, only the peaks that exceed sensor threshold are detected. The Fig. 4.2 shows an example of a train of current pulses that can be employed. In this case, the sensor is able to detect only the pulses inserted at 30, 50 and 90 ns, indicating it by pulses in its output flag. Considering a given train of current pulses with different amplitudes, the generated sensor output is assumed as the digital signature of the subcircuit. As the sensor sensitivity also depends on the subcircuit characteristics, the digital signature is unique for each subcircuit.

The area overhead imposed by the sensor results from the ratio between the sensor area and the subcircuit area. The designer is able to set a target area overhead defining the number of sensors to be inserted in the DUTT design, and consequently the number of subcircuits that compose it. For instance, considering a sensor architecture having an area equivalent to 3 minimum-sized standard cell inverters, and the target design constraint is an area overhead of 10%, the designer would place a sensor to monitor subcircuits on the order of 30 inverters. However, as distinct gates have different areas, the sensor can be placed according to the number of transistors that compose a subcircuit. As the sensor sensitivity is improved in smaller subcircuits, the number of transistors monitored by each sensor must be chosen in order to ensure that the effects of process variations are less significant than HT implementation. Therefore, the minimum area overhead is limited by the sensor sensitivity and process variations. In any case, as the method proposition is reusing these built-in sensors to detect Trojans, a DUTT already covered by this on-line testing technique to monitor transient currents would not require such an area overhead.

4.2.3 Compilation of signatures collected from subcircuit's substrate by the sensors

As the sensor provides signatures for each subcircuit of each DUTT sample, the compilation of the obtained signatures is needed to analyze a possible alteration in their original values that would indicate the presence of HTs. For instance, if the sensor of a Trojan-free DUTT sample presents a certain amount of detections (flags), the same sensor must provide similar result – slightly different according to process variations – for another Trojan-free DUTT sample. As

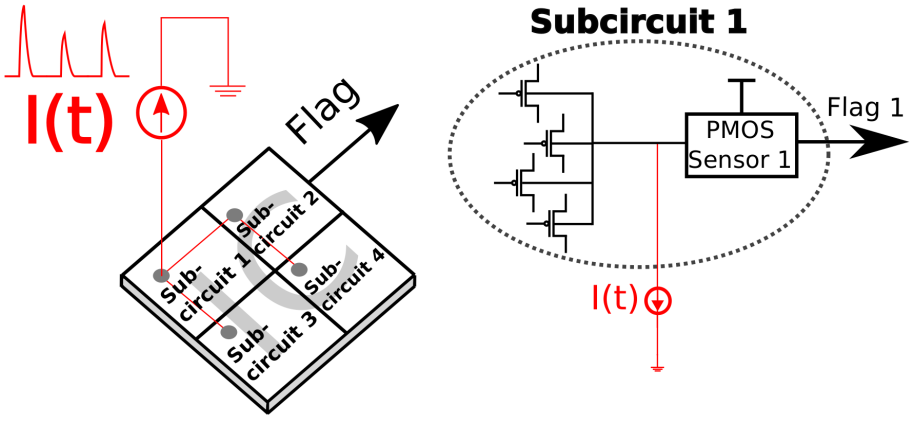


Fig. 4.3: Current insertion topology and its schematic view: an external current source able to insert subsequent peaks in the PMOS body terminal.

a mean to evaluate the generated signature, one can analyze the number of detections for a given train of current pulses. Therefore, the sensor efficiency is defined as the ratio between the number of achieved detections and the total number of pulse injections as show in (4.1). If the obtained signature is altered, the sensor efficiency is also modified and thus, a HT can de detected.

$$Sensor\ Efficiency = \frac{\#of\ Detections}{\#of\ Injections} \times 100\% \tag{4.1}$$

4.2.4 Statistical analysis for identifying DUTT subcircuits infected with HT

The analysis of the sensor efficiency also has to consider the process variations on the DUTT. In fact, for a given train of current pulses, the sensor efficiency of each DUTT sample will be different due to process variations. For example, the graph in Fig. 4.4 depicts the histogram of the sensor efficiency considering a set of Trojan-free DUTT samples subjected to process variations. Moreover, a Trojan-free DUTT profile is represented by a curve surrounding the obtained histogram, it provides a possible parameterization for the obtained results. If a HT is added to the substrate of a DUTT, the sensor efficiency will be altered, leading to a new profile curve (Trojan-infected DUTT profile in Fig. 4.4). A statistical analysis of the obtained DUTT profiles is, therefore, able to indicate whether a DUTT is effectively Trojan-infected.

With the purpose of verifying if a set of DUTT samples belongs to the distribution of the Trojan-free DUTT profile, Kolmogrov-Smirnov (KS) hypothesis test [75] is applied considering two hypotheses for a DUTT: H0: DUTT belongs to the Trojan-free class; and H1: DUTT does not belong to the Trojan-free class. KS test provides the probability value (p-value) of accepting H0, i.e. the closer to zero the p-value is, the stronger the hypothesis that a DUTT is Trojan-infected.

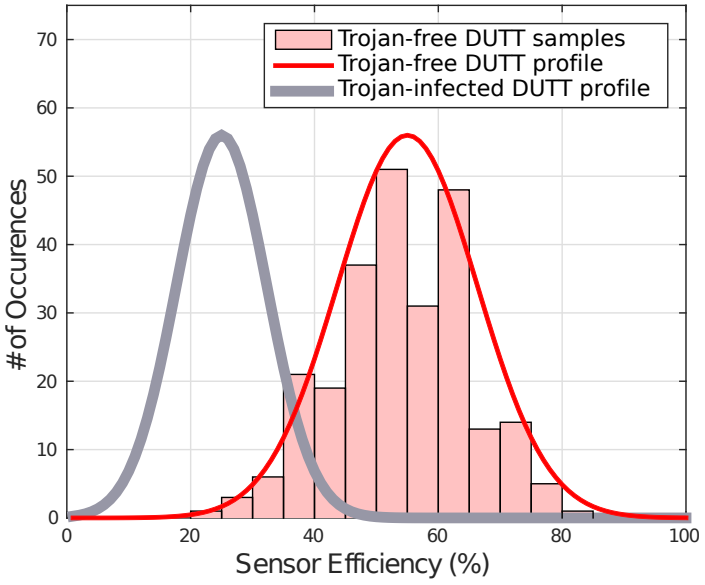


Fig. 4.4: Histogram example of the sensor efficiency based on Trojan-free DUTT samples. The corresponding Trojan-free DUTT profile and a Trojan-infected DUTT profile are also illustrated.

4.3 Simulation results and analysis

4.3.1 Description of simulation experiments

The effectiveness of the proposed method is evaluated by simulating some DUTTs from benchmarks ISCAS'85, ITC'99, and chains of inverters, all monitored by one or more built-in sensors. The DUTTs were designed in a commercial technology CMOS 65 nm by using standard cells and standard threshold voltage (SVT) transistors. Simulations were done in nominal conditions (1.2 V and 27^{o}C) by performing Monte Carlo analysis with technology local and global process distributions using Spectre simulator in the Cadence environment.

A Trojan-free DUTT was simulated by analyzing 250 Monte Carlo runs in order to generate the Trojan-free DUTT samples (golden data). DUTT primary inputs were set to V_{DD}, since our method takes no account of the system's switching activity. A train of 31 current pulses with different amplitudes was injected such as presented in Fig. 4.2 with the aim of evaluating the sensor efficiency. Subsequently, the efficiency was calculated for each run considering different process variations. At the end of this first test, results of the Trojan-free DUTT were gathered, producing a distribution of the sensor efficiency with 250 samples.

Afterwards, Trojan-infected DUTTs were also simulated under the same conditions, delivering a distribution of the sensor efficiency with 250 samples. Finally, with the two sets of data (Trojan-free and Trojan-infected DUTT distributions), KS test was performed by taking Trojan-free DUTT samples as the reference distribution and calculating the p-value for each one of the 250 samples.

4.3.2 Target HT implanted in DUTTs

To ensure that our HT detection method is effective for tracking different types of Trojans, the technique was tested under worst case scenarios. For this reason, small Trojans were chosen to be implemented in this analysis since they induce negligible modifications on the side-channel parameters of DUTTs and even so, being able to provoke critical consequences in security systems, as stated in [6, 41, 62]. On the other hand, bigger HTs induce more variations on the side-channel parameters and they are naturally more noticeable. Therefore, the success on tracking small hardware modifications indicates that this technique is also able to identify other more sophisticated HTs. Hence, three different minimalist HTs were applied on DUTTs to evaluate our method: (1) a minimum-sized inverter as the technology's smallest gate (minimum drive capability) that emulates the worst gate-level Trojan case; (2) a single PMOS transistor with minimum width and length as a layout-level Trojan in which the detection is more difficult to be achieved than the previous mentioned gate-level Trojan due to its smaller dimensions; (3) a reduction by a factor of 1000 on the channel doping concentration of a PMOS transistor as another layout-level Trojan, emulating the HTs presented in [6, 62], able to make cryptographic systems more vulnerable to leak information. The detection of these 3 HTs indicates that the proposed method is able to detect any HT type composed of one or more gates (1); one or more transistors (2); or parametric HT making modifications on the channel doping concentration (3).

4.3.3 DUTTs used to generate simulation results

Table 4.1 summarizes the set of performed simulations and obtained results. The first case study was a DUTT composed of a chain of 10 inverters with one minimum-sized PMOS transistor inserted as HT. This DUTT is monitored by one sensor that produces an estimated area

overhead of 28.5%. Fig. 4.5 presents the progress of p-value in relation to the number of tested devices. As high as the number of DUTT samples was increased, the p-value was calculated. The analysis of the p-value results leads to the conclusion that a few DUTT samples are needed to detect the Trojan. The HT insertion upsets the original sensor efficiency distribution in such a way it is possible to conclude with a probability of 99% (p-value < 0.01) that approximately 11 DUTT samples are needed to classify the DUTT as Trojan-infected. This case-study DUTT can be even interpreted as a subcircuit of the DUTT in the second line of Table 4.1, composed of 10 chains of 10 inverters monitored by 10 sensors. If the same HT is inserted in one of their 10 subcircuits, the performance of the method remains unchanged since each individual sensor works independently. Consequently, the ratio between HT and DUTT size is substantially reduced if DUTT is composed of several subcircuits. Therefore, all DUTTs in Table 4.1 could be interpreted as subcircuits of a system.

Results obtained from chains of 50 inverters, considering a transistor and an inverter as HT, illustrate the method effectiveness, even if the amount of gates monitored by the same sensor is considerably increased. Benchmarks b01 and c17 are also considered in the analysis to generate results for DUTTs composed of other gates than inverters. At last, a chain of 10 inverters with a reduced doping concentration (dopant Trojan) is analyzed to emulate the HT presented in [6,62], showing that our method is also suitable for this type of threat.

4.3.4 DUTT area overhead and number of required samples

The area overhead and the number of required samples are two balanced parameters chosen by the designers. As the overhead area is directly derived from the number of sensors implemented in the circuit, it is defined during the design phase. The designer can reduce this area offset if a large number of DUTT samples are taken for testing. In order to illustrate it, results in Tab. 4.1 show that in a chain of 10 inverters only 11 DUTT samples are required to detect a HT. However, the sensor used to monitor this circuit increases the total area of 28.5%. By enhancing the number of inverters to 50, the overhead area is reduced to 5.7% whereas 136

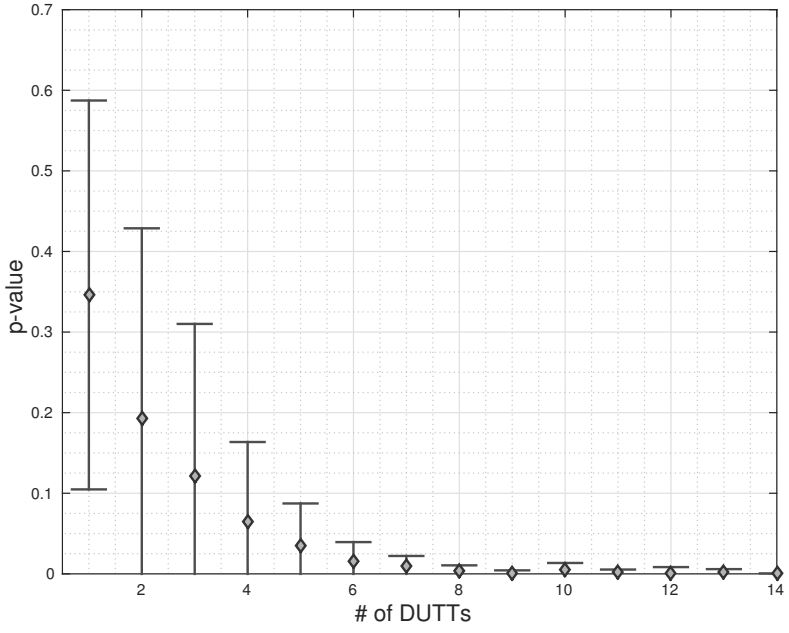


Fig. 4.5: Progress of p-value (with accuracy of $\pm\sigma$) in function of the number of DUTTs.

Table 4.1: Monte Carlo simulation results with confidence level of 99 % over 250 samples of the Trojan-free DUTT. The percentages in column "DUTT Area Overhead" represent the extra area required by the sensors regarding the total cell area of the Trojan-free DUTT with no sensors.

DUTT	Number of Gates	Number of Transistors	Number of Built-in Sensors	DUTT Area Overhead	Implanted HT	Number of Required DUTT samples
Chain of 10 Inverters	10	20	1	28.5%	1 PMOS	11
10 Chains of 10 Inverters	100	200	10	28.5%	1 PMOS	12
Chain of 50 Inverters	50	100	1	5.7%	1 PMOS	136
Chain of 50 Inverters	50	100	1	5.7%	1 Inverter	101
c17	6	24	1	25%	1 Inverter	8
b01	28	306	4	20%	1 Inverter	93
Chain of 10 Inverters	10	10	1	28.5%	Dopant HT in all Inverters	16

samples are needed. The other results in Tab. 4.1 show that no more than 150 DUTT samples are needed if the overhead is larger than 5%. Moreover, if the circuit already features this sensor to its original purpose (transient current detection) the area overhead needed for HT detection is negligible since it uses the same preexisting sensor.

4.4 Conclusions

This chapter proposes a new post-fabrication testing method able to detect gate- and layout-level Trojans inducing negligible variations on the classical side-channel signals (i.e. power, Iddq, delay, thermal, and radiation). The impacts caused by a HT on the impedance of the DUTT substrate allows the detection of minimal alterations. Moreover, the effectiveness of the method on detecting stealth and small HT can be improved whether the whole DUTT is split into smaller subcircuits, making the identification of the HT location possible too. Area overhead is negligible if the same sensor are reused as online-testing mechanisms for detecting transient currents and if some standard filler cells are replaced by BBICS cells. One could argue that attackers may implant HTs on the sensor circuit, however the method offers the possibility of being self-monitored. For this purpose, besides monitoring its subcircuit, each sensor would also monitor the circuit of the sensor that protects other subcircuit on the side. The method is still applicable in combination with other side-channel technique such as path delays and current leaks in order to further increase the HT detection coverage.

Chapter 5

Level shifter for dynamically biasing ultra-low voltage subcircuits of systems

Classical power management strategies based on dynamic voltage scaling (DVS) reduce, on the fly, the operation voltage (V_{DD}) of circuits to save energy during idle periods [63, 96]. In addition, traditional low-power techniques insert mechanisms to turn off power supplies of inactive networks of gates [54]. Complementarily, body biasing (BB) schemes or adaptive body-bias generators are able to modify the body bias (V_B) of transistors for tuning threshold voltages (V_{th}) and, thus, dynamically compensating V_{th} alterations induced by aging, process, voltage, and temperature variations as well as minimizing sub-threshold leakage [10, 37, 44, 53, 77, 128]. BB schemes are, moreover, effective for run-time optimization of system power and speed [31, 124], especially in technologies featuring efficient control of the BB effects on transistor channels, such as the process UTBB FD-SOI (ultra thin body and buried oxide fully depleted silicon on insulator) [101, 103]: increasing V_{th} of transistors saves energy, decreasing it speeds up performance of circuits.

In all mentioned techniques the integrated systems are split into subcircuits, at design time, to individually manage them with fine granularity at run time, better controlling V_{th} variations, power, and speed. Each subcircuit operates such as an island [28, 37, 61] having its own V_B or even its own V_{DD}, both locally adapted with the help of specific built-in cells able to dynamically shift them to different voltage levels. Depending on the size of the target subcircuit, the so-called level shifter (LS) cell is designed to output voltage levels either with a fine resolution or only two levels. Wide resolutions require, in addition to the LS function, analog circuitry and control logic for smoothly generating and tuning distinct voltage levels [10, 53, 77]. For minimizing area overheads, therefore, systems that are fine-grained with small subcircuits, on the order of hundreds of gates, have to use simpler architectures of LS cells [14, 20, 23, 26, 40, 43, 47, 50, 57, 59, 60, 64, 66, 70, 71, 76, 98, 110, 116, 117, 125, 127, 129, 135, 140, 141, 147, 148], which feature only modifying subcircuit voltages from/to nominal value to/from another lower or higher voltage levels.

LS cells need, moreover, to properly function with: (1) ultra-low V_{DD} levels for dynamically scaling down the V_{DD} of subcircuits to near/sub-threshold regions in which minimum energy operations are reachable [132]; (2) positive and negative body-to-source voltage (V_{BS}) levels for fully benefiting from the effective BB properties of today's technologies [101, 103], i.e. the reverse BB that reduces leakage of subcircuits, and the forward BB that makes them faster.

Different LS architectures have been proposed [14, 20, 23, 26, 40, 43, 47, 50, 57, 59, 60, 64, 66, 70, 71, 76, 98, 110, 116, 117, 125, 127, 129, 135, 140, 141, 147, 148] with the aim of dynamically

scaling down V_{DD} of subcircuits from a low V_{DD} (V_{DDL}) to a high V_{DD} (V_{DDH}). Additionally to DVS purposes, this chapter presents a new LS architecture featuring ultra-low voltage operation, quick time response, and low power and area penalties, which enable its application also on modern BB schemes [44] requiring LS transitions as fast as the data throughput of high performance systems. Typical state-of-the-art LS issue in terms of delay and power – which are degraded due to the current contention during LS transitions – is mitigated by simply returning output buffer signals to the internal LS structure responsible to switch the voltage levels. The proposed return signals play to isolate the pull-up networks from the pull-down networks of the LS, further weakening the competition between the currents coming from pull-up transistors and the currents going to pull-down transistors. The works of this chapter are within the thesis context of my Ph.D. student Otto Rolloff, it will be presented in the international conference ISCAS 2018.

The contents of this chapter are organized as follows: section 5.1 classifies state-of-the-art LS architectures, section 5.2 presents the new LS architecture, and section 5.3 and 5.4, respectively, analyzes simulation results and concludes this work.

5.1 State-of-the-art level shifter architectures

The fundamental operation of a LS architecture consists in switching its primary output (named as $\overline{V_X}$ in this paper) from Gnd to V_{DDH} whenever a voltage level (on the order of V_{DDL}) is applied at its primary input (herein EV_{DDH} in Fig. 5.1 and Fig. 5.2). The function of EV_{DDH} is, therefore, to enable a transition of $\overline{V_X}$ from Gnd to V_{DDH}. If the goal is to use the LS architecture in a forward BB scheme, $\overline{V_X}$ is connected to V_B of a n-well island (subcircuit designed with flip-well configuration [101, 103]); otherwise if the target is a DVS scheme, V_X and $\overline{V_X}$ are separately connected to the gate terminals of two PMOS transistors that operate to switch the V_{DD} of a subcircuit from V_{DDH} to V_{DDL} (or from V_{DDL} to V_{DDH}).

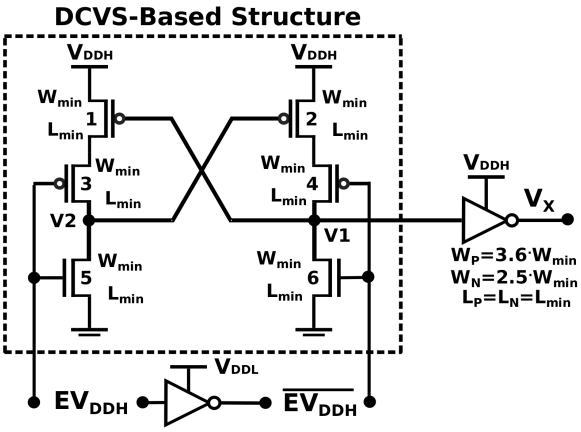
State-of-the-art LS architectures are classified in this section into five categories defined according to the presence of the following particular internal structures: (1) cross-coupled PMOS transistors; (2) diode-connected transistors; (3) current mirrors; (4) pass transistors; and (5) dynamic logic.

Cross-type LS architectures

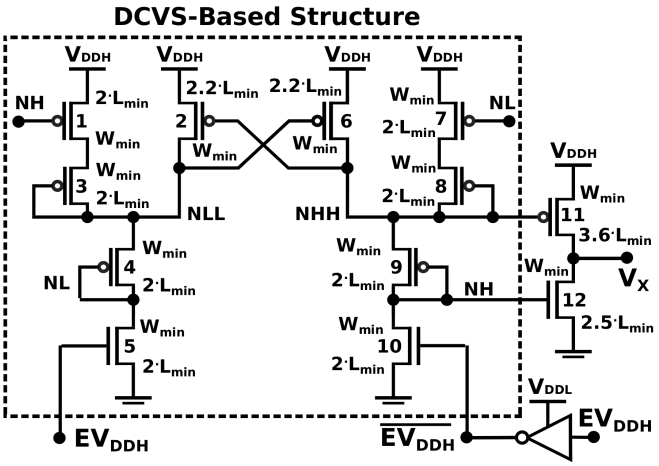
Several state-of-the-art LS architectures [127, 129, 135, 141] have been proposed using the principles of the differential cascode voltage switch (DCVS) CMOS logic [46] to mitigate static current overheads. Fig. 5.1 illustrates DCVS structures (inside dashed boxes), which are cross-coupled PMOS pairs forming two pull-up networks (PUNs) complemented by two pull-down networks (PDNs). A basic DCVS-based LS architecture [127] is shown in Fig. 5.1a.

Diode-type LS architectures

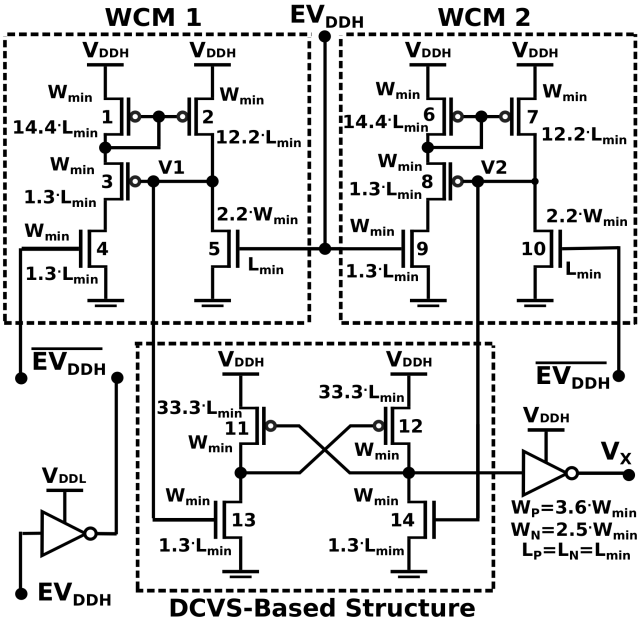
Diode-connected transistors have been used in state-of-the-art LS architectures [26, 40, 57, 64, 66, 110, 116, 140, 147] as current limiters to attenuate the typical LS issue of current contention (mentioned in the introduction of this chapter). Recently, Lanuzza et al. [64] have proposed the LS architecture in Fig. 5.1b. In addition to to the classic DCVS-based structure and diode-connected transistors, a self-adapting boost circuit increases the strength of each LS branch during their charging phase, and weakening them in the discharging phase.



(a)



(b)



(c)

Fig. 5.1: State-of-the-art LS architectures and their names used in this paper: (a) a cross-type LS (CMLS [127]); (b) a diode-type LS (LANLS [64]); (c) a mirror-type LS (CAOLS [14]).

Mirror-type LS architectures

LS-architectures based on current mirrors have been proposed [14, 23, 47, 59, 70, 71, 76, 98, 148] to feature wider input voltage range at EV_{DDH}. Fig. 5.1c illustrates a LS architecture [14] using two Wilson current mirrors connected to a conventional LS structure.

Pass-type LS architectures

In the early 2000s, LS architectures employing pass transistors and other complementary structures were presented in [110] and [43, 60, 117, 125] to improve classic LS structures.

Dynamic-type LS architectures

Another type of LS architecture was proposed in [50] and [20] by exploiting dynamic logic to operate at lower voltage levels. The dynamic-type LS architectures require a circuitry for the precharge phase of the dynamic logic.

5.2 Proposed level shifter architecture

The proposed architecture baptized herein as the weak contention level shifter (WCLS) is composed of a DCVS-based structure (dashed box in Fig. 5.2). WCLS is quite similar to CMLS in Fig. 5.1a, however a fundamental difference exists at gate terminals of transistors 3 and 4 (cf. Fig. 5.2) that are connected, respectively, to the signals $\overline{FB}$ and FB of the output buffers.

$\overline{FB}$ and FB, which are generated after the DCVS-based structure output, ensure that transistors 3 and 4 change their voltage levels only after the output V_{X} has changed. The delay of this feedback signals has to be controlled to certify that $V2$ and $V1$ nodes has fully switch to Gnd or V_{DDH} before these signals affect transistors 3 and 4. To reduce the leakage of this LS architecture, even under ultra-low voltage operation, every branch of the DCVS-based structure must switch completely after an input transition arrives at EV_{DDH}.

When $\overline{EV_{\text{DDH}}}$ switches from Gnd to V_{DDL}, the node $V2$, already charged to V_{DDH}, will discharge to Gnd. Transistor 3 was already cut by the signal $\overline{FB}$, previously settled to V_{DDH}. When discharging, the signal $V2$ will activate transistor 2, enabling the node $V1$ to charge, if considered that transistor 4 was already activated by the signal FB, previously set to Gnd. Once $V1$

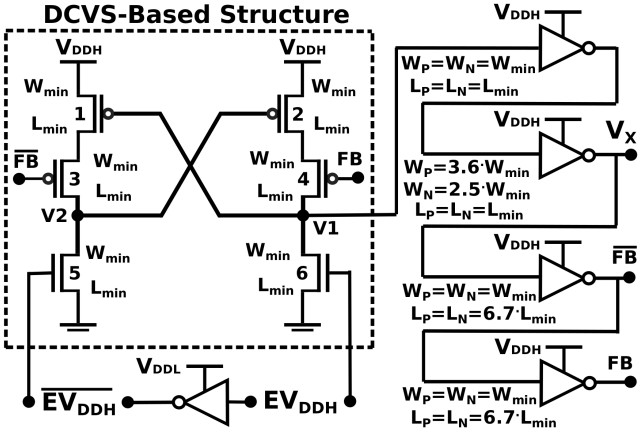


Fig. 5.2: The proposed LS architecture baptized WCLS.

has been set to V_{DDH}, forcing $\overline{FB}$ to Gnd, transistor 3 will be activated, and the signal FB will deactivate transistor 4, preparing each branch of the DCVS-based structure for the next input transition at EV_{DDH}. As transistor 4 is open, in the next transition of $\overline{EV_{\text{DDH}}}$ to Gnd, the node $V1$ will discharge to Gnd, fast and free of the contention normally imposed by the PUN in other state-of-the-art LS architectures.

5.3 Simulation results and analysis

This section describes simulation experiments, analyzes, and compares results of recent and effective state-of-the-art LS architectures (CMLS [127], LANLS [64], and CAOLS [14]) shown in Fig. 5.1 with our proposition WCLS in Fig. 5.2.

5.3.1 Description of simulation experiments

Electrical-level simulations were done using low threshold voltage (LVT) transistors from a commercial technology UTBB FD-SOI 28 nm. For the sake of fair comparison, the W/L ratios of each transistor in the DCVS-based structures of CAOLS and LANLS were firstly reproduced from the paper references and optimized with the minimum size that makes them functional. A periodic pulse was applied at EV_{DDH} with a frequency of 50 MHz and an amplitude of V_{DDL}, while the output V_{X} was loaded by 20 minimum-sized inverters of the technology. In the case of CMLS and WCLS circuits, the transistors were set to the technology's minimum sizes W_{min} and L_{min}. The performance of both these LS architectures could be enhanced thanks to higher W/L ratio of the transistors in the PDNs of the DCVS-based structure.

A parametric analysis simulation was performed varying V_{DDL} of each LS architecture, and keeping V_{DDH} at 1 V. For each simulation, the following three figures of merit were considered: delay, static power, and transition energy, as shown in Fig. 5.3. Moreover, a Monte Carlo simulation has been done to evaluate the reliability of the proposed architecture against process variations. Scattering plots for 2000 runs are presented in Fig. 5.4.

5.3.2 Comparison of LS architectures

Fig. 5.3 shows three graphics describing on their axis y average results of delay (a), static power (b), and transition energy (c); all of them in function of V_{DDL}. The minimum V_{DDL} reachable by each LS architecture are approximately:

- CAOLS [14] (gray): 0.37 V;
- LANLS [64] (green): 0.32 V;
- WCLS [this work] (red): 0.19 V;
- CMLS [127] (blue): 0.37 V.

The best results in terms of delay, static power, and transition energy are for CMLS and WCLS, showing similar trends within the V_{DDL} range between 0.4 V and 1 V. In fact, the explanation is that both LS architectures have the same DCVS-based structure. Moreover, for this V_{DDL} range, the PDN is strong enough if compared to the PUN, allowing to quickly discharge the nodes $V2$ ($V1$) when the transistor 3 (and 4) are activated by $\overline{EV_{\text{DDH}}}$ (EV_{DDH}). For V_{DDL} lower than 0.37 V, the PDN current of the CMLS architecture is lower than the PUN current, then $V2$

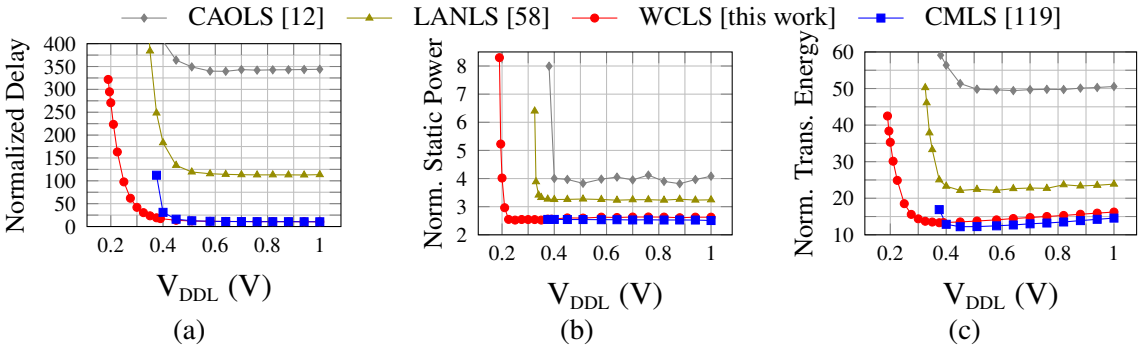


Fig. 5.3: Normalized average results of delay, static power, and transition energy for each LS architecture with fixed nominal V_{DDH} = 1 V and EV_{DDH} switching from Gnd to V_{DDL} as well as from V_{DDL} to Gnd. All points of these graphics and those in Fig. 5.4 are normalized to the results of the technology's standard LVT inverter cell with minimum drive capability. The average delay, static power, and transition energy of this reference inverter are 4.88 ps, 4.35 nW, and 0.43 fJ under the same conditions: typical corner, nominal V_{DD} = 1 V, and T = 27 °C.

and $V1$ nodes are not discharged when required, making it impossible to switch. Otherwise, for the same V_{DDL} range, WCLS continues operating because transistor 3 (and 4) were cut-off by the signal $\overline{FB}$ (FB) after the occurrence of the last transition of $\overline{EV_{DDH}}$, and before the next transition of $\overline{EV_{DDH}}$ (EV_{DDH}) arrives (from Gnd to V_{DDL}), letting node $V2$ ($V1$) discharging almost without any opposition of the PUNs.

For V_{DDL} of 0.4 V, and applying transitions at EV_{DDH} from Gnd to V_{DDL} and from V_{DDL} to Gnd, we notice the average delay of LANLS exceeds the WCLS's average delay by a factor of at least 11. CAOLS and LANLS consume also significantly higher static power than WCLS. In terms of average transition energy, the CAOLS and LANLS overheads are, respectively, 4 and 2 times higher than WCLS costs. For CAOLS, as the ratios W/L of the transistors 1, 2, 6, and 7 are low, the PUNs of the WCM structures are very weak, enabling the PDNs effectively discharging through the branches of the transistors 4 and 9, for a wider V_{DDL} range. Nevertheless, CAOLS is not effective for V_{DDL} lower than 0.37 V. Similar effects are observed for LANLS that operates up to 0.32 V. The technique that dynamically weakens the PUN is not effective if V_{DDL} is lower than 0.32 V as the PDN drive gets weaker than the PUN drive under this ultra-low voltage condition. The same argument is used to justify how the LS delay is longer for CAOLS and LANLS than for WCLS. WCLS is the only studied option that isolates almost completely the PUNs and the PDNs, allowing the already charged branch of the DCVS-based structure to discharge practically without opposition of the PUNs. Even under ultra-low V_{DD} condition, the PDNs of WCLS are able to discharge the nodes $V1$ and $V2$.

Fig. 5.4 details measures of the transition energy and static power in function of the delay of each LS. As this work has looked for the lowest power consumption and the shortest delay, the best LS results within the simulated conditions is the ones closest to the lower-left corner of the scatter plot. According to this aspect, the most stable LS architecture is the CMLS because their points are more concentrated and closer to the lower-left corner. On the other hand, the most stable LS architecture in terms of delay is the WCLS as their points are the least spread on the axis x. It is due to the absence of PUN contention, which leads to a stabler discharge of each branch, even under process variations. If the transition energy is analyzed, the CMLS is the most stable solution. Finally, for a static power analysis, LANLS and CMLS are the stablest, presenting almost the same behavior under process variations.

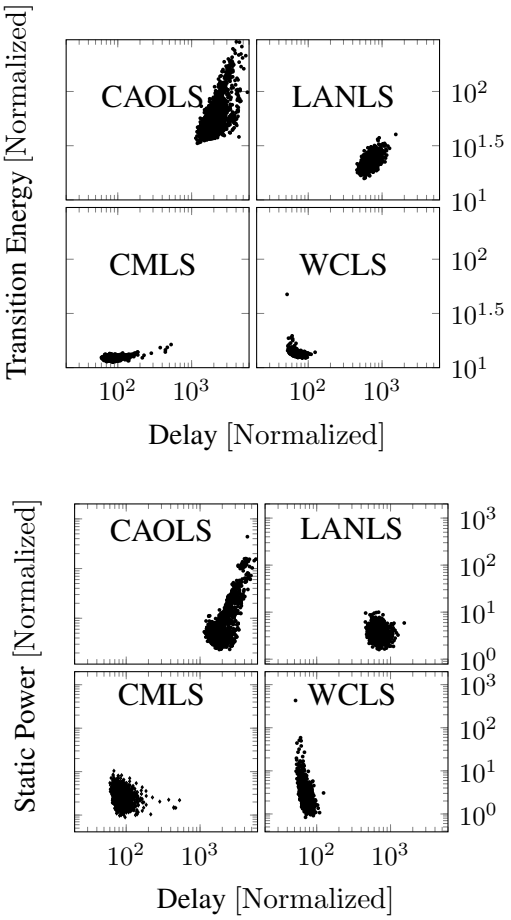


Fig. 5.4: Monte Carlo simulation for 2000 runs (V_{DDH} = 1 V, V_{DDL} = 0.45 V, frequency of 50 MHz and T = 27 °C)

5.4 Conclusions

This chapter presents a novel LS architecture able to provide V_{DDH} from ultra-low V_{DD} at expense of low delay, static power, and transition energy. Thanks to feedback signals coming from the buffers connected at the LS output, the current contention issue is efficiently mitigated, leading to an almost total isolation between PUN and PDN (of a DCVS-based structure branch) before the discharge of it.

The proposed WCLS is suitable for implementations at the interface between multiple V_{DD} domains, transferring data at sub-threshold V_{DD} to above V_{th}. As it is controllable by a circuitry operating at ultra-low V_{DD}, WCLS is also convenient for controlling BB schemes that use ultra-low V_{DD} in UTBB FD-SOI systems. Both DVS and BB techniques operating at ultra-low V_{DD} are fundamental in the today's low-power demand for IoT devices.

A future work is to devise a complementary WCLS architecture able to shift V_{BS} to negative voltage levels. A complete ultra-low voltage solution will be thus proposed for performing reverse and forward BB in complex integrated systems.

Chapter 6

Ultra-low voltage asynchronous circuits in FD-SOI technology

Among state-of-the-art power management techniques, reducing the operation voltage (Vdd) of circuits is a traditional method to decrease power consumption. However, low Vdd makes circuits more vulnerable to process, voltage, and temperature (PVT) variations [142], causing timing uncertainties that can lead to clock assumption violations in synchronous circuits.

In this context, asynchronous circuits appear as an alternative solution for addressing power consumption issues and ensuring high system reliability at lower Vdd levels. As their own data flow is used to locally synchronize information between parts of the system, delay variations are much more tolerable. Thus, asynchronous circuits are intrinsically more robust to PVT variations, especially the quasi-delay insensitive (QDI) class that enables operation at ultra-low Vdd.

The data driven processing between asynchronous blocks makes the system more modular, and the inclusion of local voltage scaling techniques is much easier. In addition, extended low-power features are exploitable from the recent Fully-Depleted Silicon On Insulator (FD-SOI) process. Thanks to a more efficient control of the body biasing effects on the transistor channel [9], the FD-SOI technology provides the option of setting different threshold voltages (Vth) even during system operation. Therefore, local synchronization signals can be used to control biasing of asynchronous blocks' substrates, which enables power reductions or speed improvements [45].

Automatic power reduction strategy on QDI asynchronous circuits with body biasing features in FD-SOI technology has been proposed and analyzed in [45]. Furthermore, power behavior of an asynchronous architecture have been compared with its synchronous counterpart in a classic bulk CMOS 130 nm technology [21]. In order to apply voltage scaling techniques to decrease Vdd of integrated systems and to profit the full low-power potential of the FD-SOI body biasing features [30, 72], additional studies and analysis are still required, especially to define and compare the minimum operation voltages of asynchronous case-study circuits in FD-SOI technology. In this chapter, we present a comparison of an asynchronous arithmetic logic unit (ALU) with its synchronous version, both designed in FD-SOI 28 nm. Results in terms of data throughput, power consumption, and energy per bit are analyzed at different Vdd levels. The works of this chapter are within the thesis context of my Ph.D. student Thiago Leite, it was presented in the international conference PATMOS 2016.

Section 6.1 of this chapter presents fundamental concepts of asynchronous circuits and FD-SOI technology, and section 6.2 discusses how QDI features are exploitable for saving power. Section 6.3 describes the case-study circuits analyzed in this work, and in sections 6.4 and 6.5 comparative results and final conclusions are highlighted.

6.1 Asynchronous circuits and FD-SOI technology

6.1.1 Synchronous vs. asynchronous circuits

Synchronous circuits are architectures with data flow governed by a global signal: the clock. Therefore, it determines circuit's performance and strongly influences its power consumption. A classical representation of a clocked system is shown in Fig.6.1a.

The synchronous design approach has been dominant and widely used by the industry, however reliability and security issues of today's complex integrated systems push researches for seeking alternative solutions.

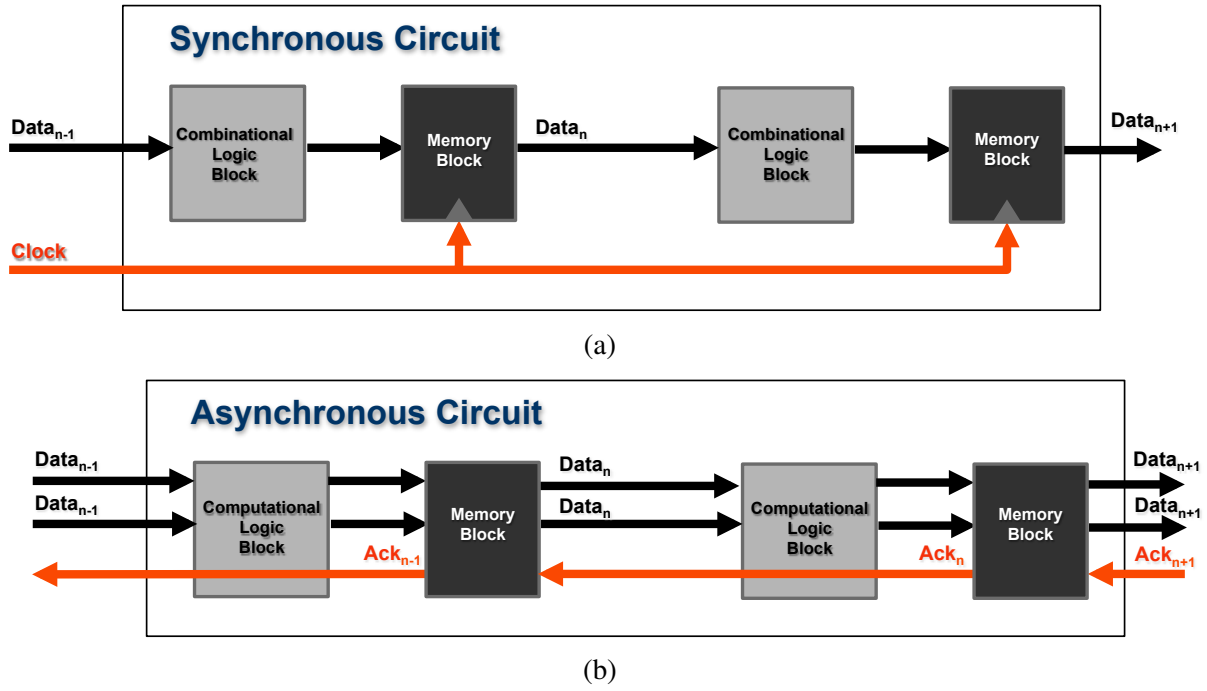


Fig. 6.1: Typical representations of synchronous (a) and asynchronous (b) systems.

A different technique to synchronize data is used by asynchronous circuits. They have the global clock replaced by a local communication protocol. Consequently, data flows from a pipeline stage of the system (sender) to the following one (receiver) as soon as the latter finishes processing previous inputs. A typical representation of an asynchronous system is shown in Fig.6.1b. When the leftmost logic block finishes the computation of a result, the leftmost memory block responds with an acknowledgment signal, allowing the acquisition of new input data. The same synchronization procedure is executed in every pipeline stage of the architecture.

The absence of a global synchronizing signal in asynchronous circuits gives them certain advantages if compared to its synchronous equivalent, namely: lower power consumption, robustness toward PVT variations, less electromagnetic noise emission, better modularity, no clock distribution and skew issues [95].

6.1.2 QDI asynchronous circuits

There are different methods to conceive asynchronous circuits that differ from each other in the number of timing assumptions used to implement sequencing [74]. The class of Quasi-Delay Insensitive (QDI) asynchronous circuits, which is the design approach used in this work, can operate correctly with only a few assumptions on certain forks [73]. The reduced number of timing assumptions makes QDI asynchronous circuits very robust and appropriate for low-power operation.

The logic blocks depicted in Fig.6.1b were designed in this work by using Delay Insensitive Min-terms Synthesis (DIMS) [123]. This design method allows to generate robust architectures, which are suitable for low Vdd operation. Furthermore, the memory blocks, represented in Fig.6.1b, were designed as half buffers. They memorize data between pipeline stages and implement the 4-phase Weak-Conditioned Half-Buffer (WCHB) communication protocol [67].

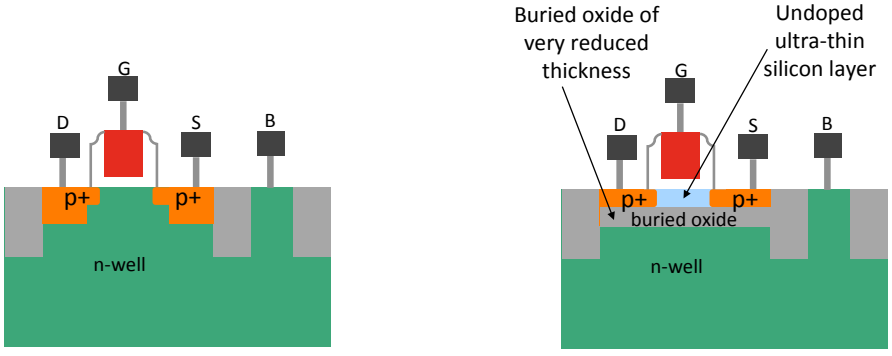
6.1.3 FD-SOI technology

The continuous scale down of transistors to nodes beyond 40 nm brought to the spotlight some phenomena previously neglected: short channel effects and random dopant fluctuation, for example. Therefore, manufacturing technologies different than classical Bulk started been indicated as possible solutions to overcome these issues and allow progression of performance and scale enhancements in the deep sub-micron era.

In this context, the Fully Depleted Silicon on Insulator (FD-SOI) technology has been indicated as one of the candidates for designing circuits that enable low voltage operation and yet achieve a much better performance than bulk could provide in CMOS advanced nodes [8]. A comparison of classical bulk and FD-SOI PMOS transistors is illustrated in Fig. 6.2.

In the FD-SOI technology, a buried oxide (BOX) layer is added to the substrate, electrically isolating the body, also known as back plane, from the source, drain and channel. The latter is undoped, significantly reducing the random dopant fluctuation issues. Additionally, source and drain are raised, causing a decrease in the contact resistance [102].

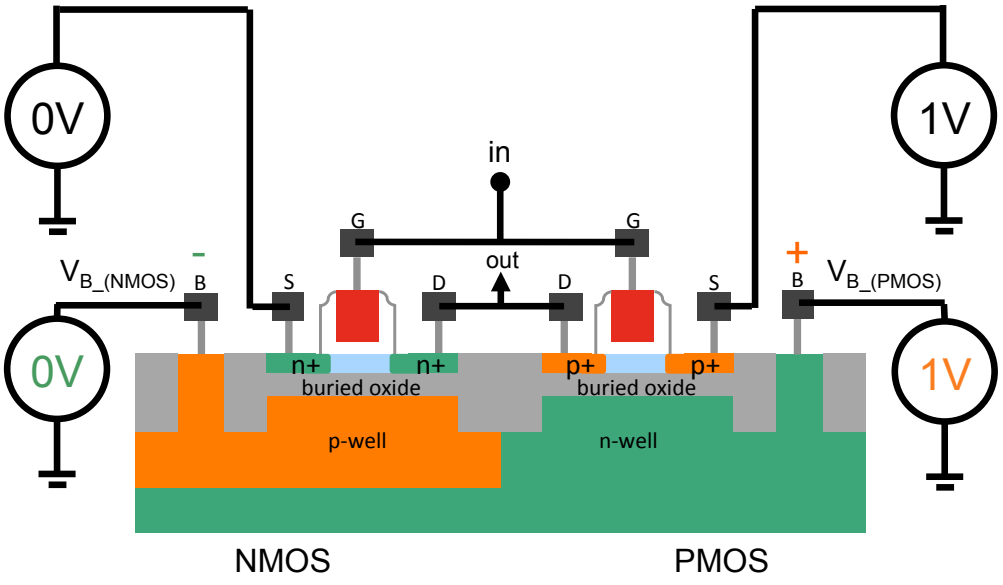
Well taps connected to the back plane enable coupling it to a body bias (V_B), which allows fine grain tuning of transistors threshold voltage (Vth) [102]. A wide V_B range is achievable as result of electrical isolation between back plane and source/drain provided by the BOX. Hence, it is possible to decrease Vth to boost operating speed, at the cost of high dynamic and static power consumption, or on the contrary, it is possible to increase Vth in order to reduce power consumption, at the cost of performance degradation.



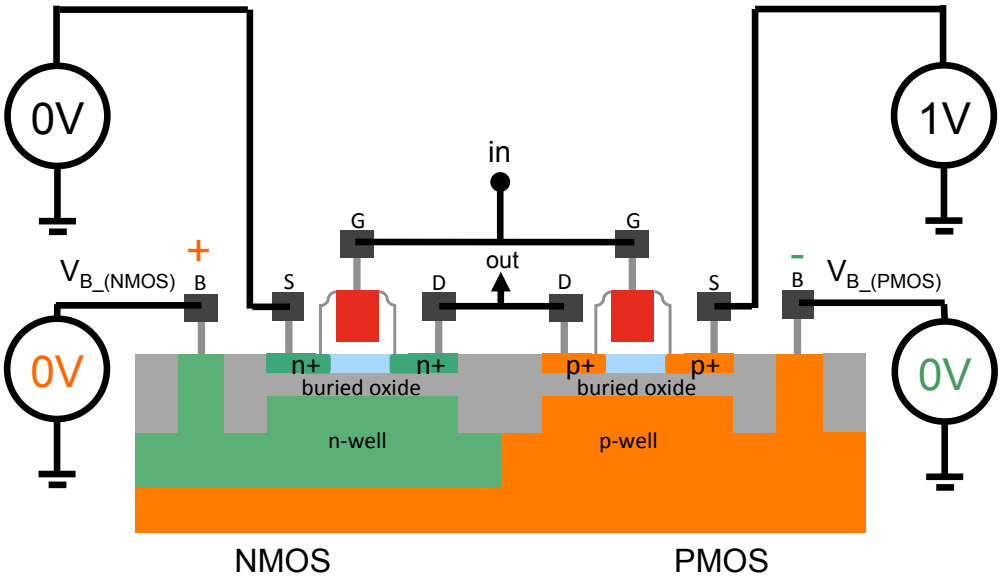
(a) (b)

Fig. 6.2: Layout cross section of classical bulk (a) and FD-SOI (b) PMOS transistors.

Designers have the option of using either Low Vth (LVT) transistors or Regular Vth (RVT) transistors depending on their needs. If RVT transistors are chosen, the gates have a conventional well configuration, see Fig. 6.3a. In this case, transistors can have their Vth further increased to reduce leakage by applying a Reverse Body Biasing (RBB) technique. Conversely, if LVT transistors (flip well configuration) are chosen (Fig. 6.3b), their Vth can be further reduced by applying a Forward Body Biasing (FBB) technique. This type of transistor is generally used for high performance applications. In both cases (conventional or flip well), the limit of body bias ($V_{B\_(NMOS)}$ or $V_{B\_(PMOS)}$) that can be applied is the breakdown voltage between p-well and n-well.



(a)



(b)

Fig. 6.3: Layout cross section of a FD-SOI CMOS inverter by using conventional well (RVT transistors) (a) and flip well (LVT transistors) (b) configurations.

6.2 Exploiting intrinsic features of QDI asynchronous circuits for saving power

Traditional power saving strategy for integrated systems simply applies lower operation voltages rather than the nominal one. Low voltages, however, increase the delay of system components, making timing violations more probable in clock-based circuits like the synchronous ones.

Asynchronous circuits, otherwise, are well suited for operating in a wide Vdd range, especially QDI asynchronous circuits that present three intrinsic features enabling ultra-low voltage operation and on-the-fly power management of integrated systems:

1. the absence of a clock eliminates several related timing assumptions;

2. the tolerance to any delay variation on their gates and on majority of their wires;

3. the modularity and operation by using data-based request and acknowledgement signals between blocks.

At the expense of a delay increase on their gates, QDI circuits are, therefore, able to operate with low voltages for saving power. Furthermore, as low voltage operation has been demonstrated in FD-SOI synchronous circuits [30, 72], previously mentioned properties of QDI circuits in association with body biasing FD-SOI advantages are fully exploitable to optimize speed and power of asynchronous components operating at low voltages [45].

Design strategies for controlling the body bias of system's blocks have been exploited the modularity of asynchronous pipeline stages [45]. Fig. 6.4 abstracts one of the strategies proposed by Hamon and Beigne. Note that special elements, named boost cells, play such as voltage-level shifters (further details in chapter 5) for biasing the system's blocks. In addition, simple logic circuits responsible for detecting switching activity in asynchronous system's blocks are required, enabling, consequently, the boost cells.

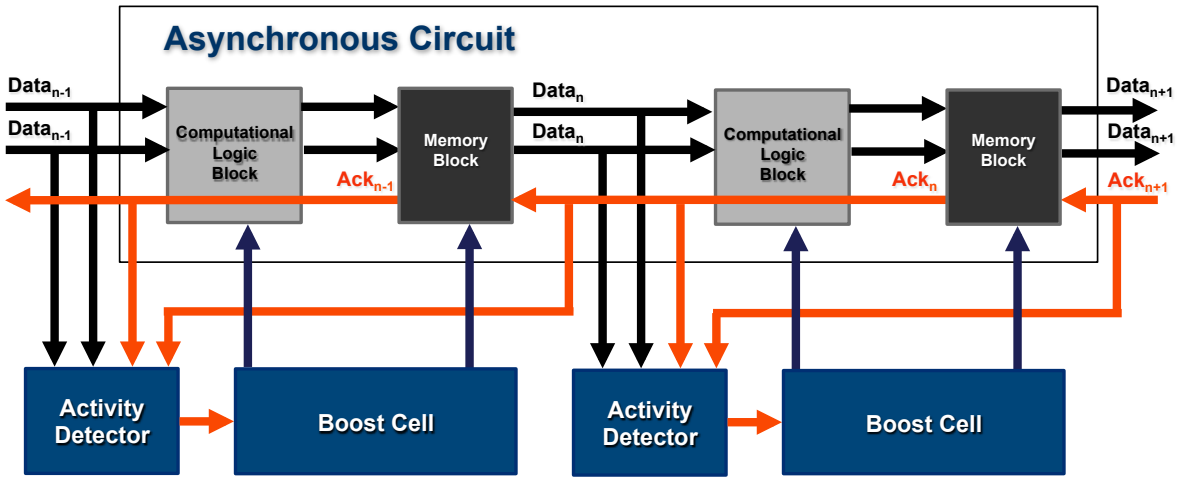


Fig. 6.4: Body biasing strategy applied on an asynchronous circuit [45].

6.3 Case-study circuits: synchronous and asynchronous ALU

As previously mentioned in the introduction, an 8-bit ALU was used in this work as a case-study. This circuit has been specifically chosen since it is one of the most important blocks in modern processors. The designed architecture can compute either addition, subtraction, or bitwise logic operations. Fig. 6.5 depicts the proposed ALU architecture. It is composed of three stages of pipeline. The first one is the input stage, with de-multiplexers for either arithmetic or logic operation; the second stage is the execution stage, in which the logic and arithmetic units compute their corresponding output; and the third stage of pipeline is the output selection stage. Both synchronous and asynchronous circuits were equally pipelined and have logic blocks with the same functionality. Thus, both circuits are composed of:

- One 8-bit Sklansky Adder, which computes the operations of addition and subtraction;
- One 8-bit Logic Unit for computing AND, OR and XOR logic operations;
- Several multiplexers and de-multiplexers necessary to correctly select the required operations.

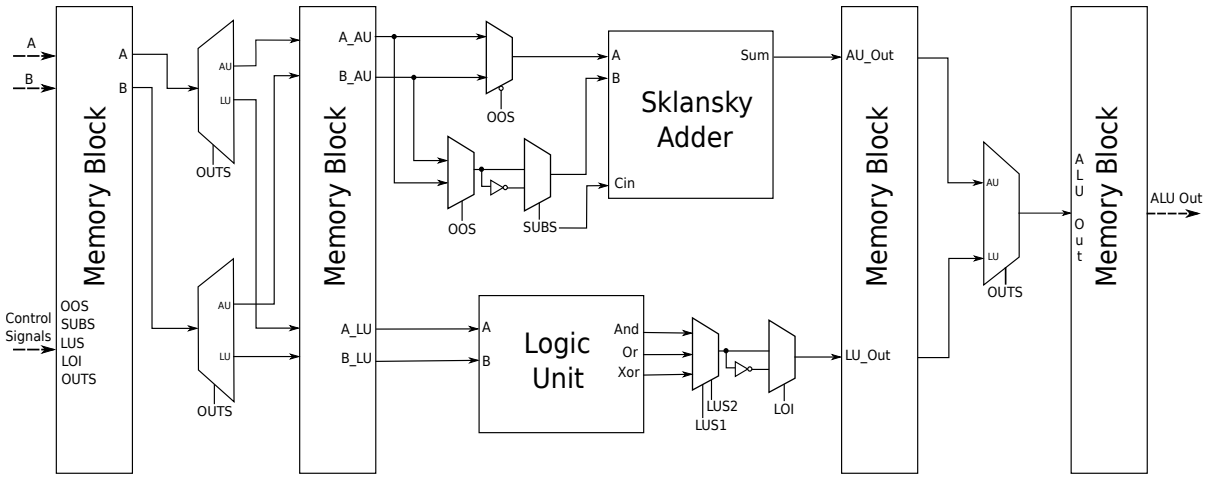


Fig. 6.5: ALU general architecture, designed in synchronous and asynchronous versions.

The difference between the synchronous and asynchronous implementation of the proposed architecture is that the former has registers as memory blocks and is entirely composed of standard cells. The latter, on the other hand, has half-buffers as memory blocks and was designed by using standard cells and some asynchronous dedicated circuits, i.e., C-elements. Moreover, the asynchronous logic blocks were built by using DIMS, as detailed in section 6.1.

The synchronous ALU was described in VHDL, at structural level, with the same blocks used in the asynchronous circuit. The hardware description was then synthesized for a target voltage of 1 V. Subsequently, the generated verilog gate level netlist was converted to a SPICE netlist, so that electrical simulations could be performed. On the other hand, for the asynchronous design, the same blocks previously described were directly designed at spice level, using a QDI dual-rail 4 phase asynchronous encoding. Details on the simulation environment will be given in section 6.4.

It is widely known that QDI designs present a considerable area overhead if compared to a synchronous equivalent, as reported by [21]. In fact, to cope with the extra robustness, the

asynchronous ALU present a significant area overhead compared to the synchronous circuit. In this study-case, the functional blocks of the asynchronous circuit are 1.8x to 2.5x larger than the synchronous functional blocks, which leads to a total of approximately 2.3x area overhead in the asynchronous ALU.

6.4 Synchronous and asynchronous ALU results

6.4.1 Simulation environment

The synchronous and asynchronous ALU spice netlists, obtained as detailed in section 6.3, were simulated with Regular Threshold Voltage (RVT) transistors of FD-SOI 28nm technology. Each netlist was connected to a Linear Feedback Shift Register (LFSR) so that it could generate the input vectors. Afterwards, electrical simulations were performed with the circuit, ALU and LFSR, for a fixed amount of time with different levels of Vdd, ranging from nominal 1.0 V down to 0.4 V. This procedure was the same for both circuits, synchronous and asynchronous. Some precautions needed to be taken into account in simulations with the synchronous design though. For each simulation scenario, it was necessary to adjust the clock frequency to prevent timing violations. Moreover, to allow a fair comparison with the asynchronous counterpart, the clock frequency was adjusted to the fastest possible for each Vdd, ensuring maximum performance of the synchronous ALU through all simulations. A script was used to automatically tune the clock frequency for each simulation.

With the asynchronous design, however, no special adjustment needed to be done to ensure correct behavior and maximum performance at each Vdd. In fact, as previously mentioned in section 6.2, QDI circuits are intrinsically robust to voltage variation. Furthermore, the local handshake protocol, used by the asynchronous counterpart, ensures that it will always operate at its maximum speed.

6.4.2 Results and comparative analysis

After performing the simulations described in subsection 6.4.1, results in terms of power consumption, data throughput and energy efficiency were obtained. Fig. 6.6 shows the average power consumption of the synchronous and asynchronous designs, for different Vdd levels under three corner conditions: TT, FF and SS. Fig. 6.8 illustrates the measured throughput of both circuits at the same Vdd levels. The throughput has been chosen as figure of merit for performance comparison between the designs since it can be easily measured in both synchronous and asynchronous designs. One can remark that the throughput of the synchronous circuit is directly determined by the clock frequency. Hence the importance of implementing a clock frequency scaling mechanism, as section 6.4.1 describes.

Fig. 6.7 depicts the results of energy per bit for synchronous and asynchronous designs. A lower value of energy per bit represents a better efficiency.

It is important to highlight that a zoom of the graphics was added in Fig. 6.6 and 6.8, in order to increase the visibility and details of the curves when reaching low voltages (between 0.5V and 0.4V, for instance).

The figures illustrate the trade-off between power and performance in FD-SOI technology. Comparing Fig. 6.6 and 6.8, it can be noticed that as Vdd is reduced, so does the throughput. For example, when Vdd is decreased from 1 V to 0.8 V, there is a reduction of approximately 30% and 44% in the synchronous and asynchronous architectures performance, respectively.

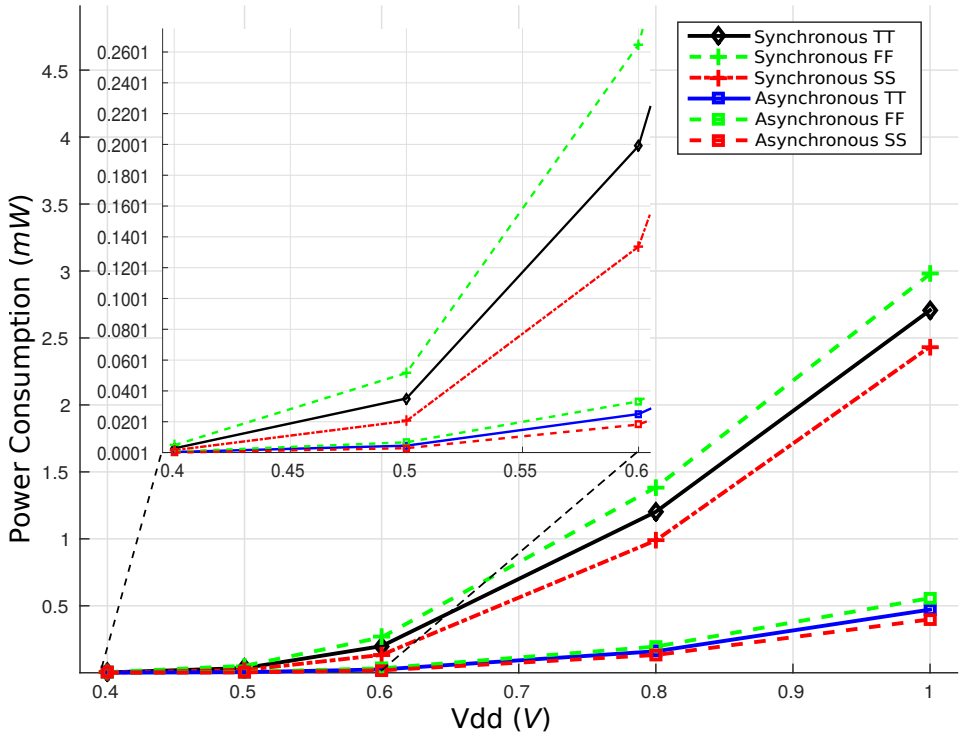


Fig. 6.6: Average power consumption of synchronous and asynchronous ALU in different Vdd conditions and corners.

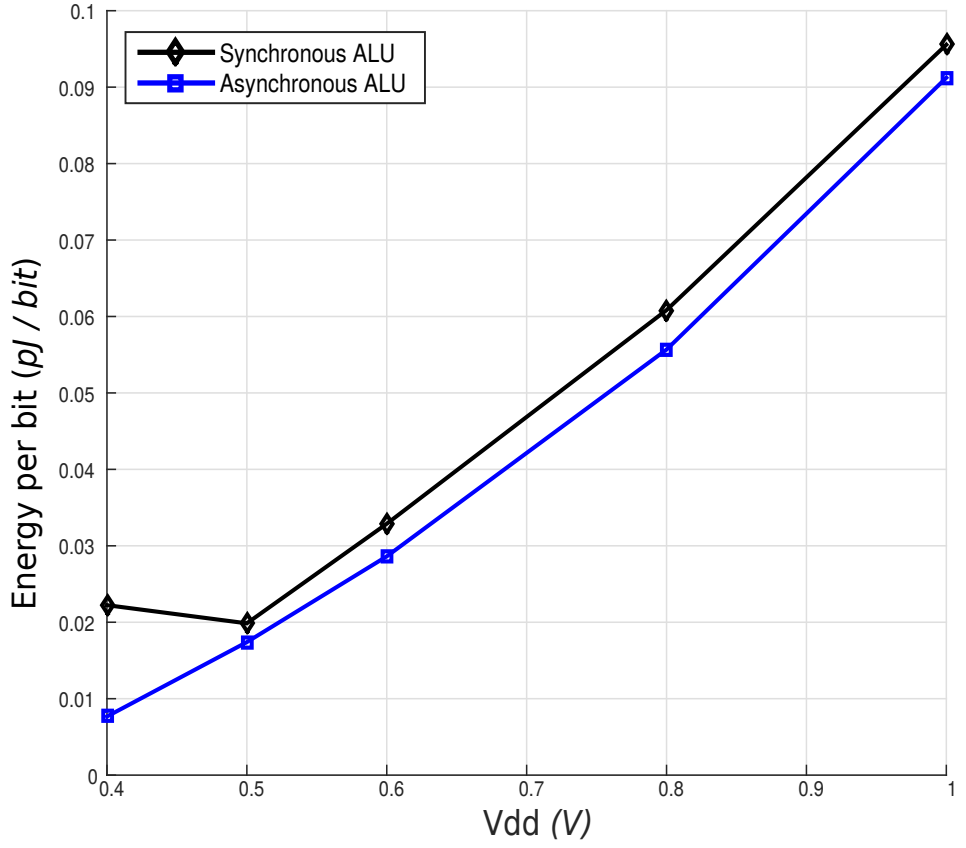


Fig. 6.7: Energy per bit of the synchronous and asynchronous ALU in different Vdd conditions.

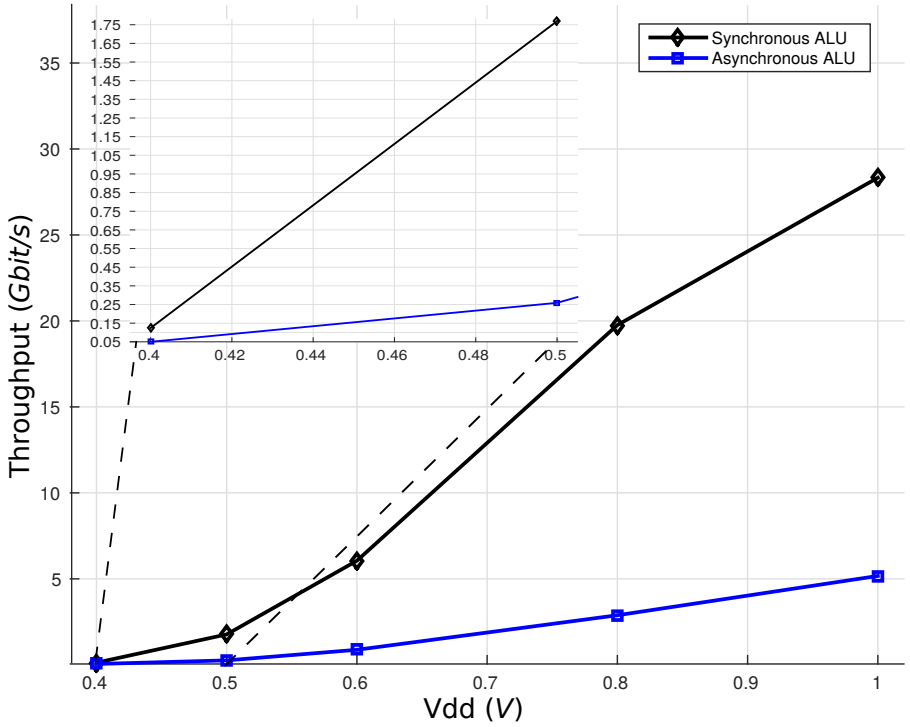


Fig. 6.8: Data throughput of synchronous and asynchronous ALU in different Vdd conditions.

Fig. 6.6 points out that the asynchronous ALU has a lower average power consumption – if compared to the synchronous one – in every simulated operation voltage. This result is explained by the intrinsic QDI asynchronous properties, which ensure switching activity only in blocks that are processing some data. In synchronous designs, otherwise, inadvertent transistors also switch, which increases the dynamic power consumption. Moreover, corner curves in Fig. 6.6 for typical (TT), slow (SS), and fast (FF) synchronous circuit are steeper than the asynchronous ones. This confirms that the synchronous design is much more sensitive to voltage variations than the asynchronous design. Additionally, SS and FF corner curves for synchronous design are more widely spaced than asynchronous ones, which indicates that the synchronous circuit is also more sensitive to process variations.

On the contrary, Fig. 6.8 shows that the performance of the synchronous ALU is better for values close to the nominal voltage, however it gets closer to asynchronous performance if Vdd decreases. Again, synchronous performance is more sensitive to Vdd changes – if compared to its asynchronous counterpart – because it has higher slope in the throughput curve in Fig. 6.8. Finally, if energy efficiency is analyzed, Fig. 6.7 shows that the energy per bit ratio is lower in the asynchronous circuit. In the case of operation voltage bellow 0.5 V, the throughput degradation becomes quite severe in the synchronous design. Its energy per bit ratio thus starts growing, indicating that the throughput degradation overcomes the power consumption reduction trade-off. The main reason for that is the enormous amount of timing margin that has to be added to the clock at very low Vdd, which makes the synchronous circuit spends leakage power for much longer interval. The same behavior is not observed in the asynchronous counterpart for Vdd equals to 0.4 V. Hence, for Vdd levels lower than 0.5 V, the usage of QDI asynchronous instead of classical synchronous architectures is more suitable.

6.5 Conclusions

A synchronous and an asynchronous ALU circuits in FD-SOI 28 nm have been designed in this work. The goal was to compare and analyze the behavior of these circuits operating at low voltages and in FD-SOI technology. Thanks to natural asynchronous properties, the asynchronous ALU presents a better energy efficiency in all simulated Vdd conditions. Furthermore, with Vdd lower than 0.5 V, the asynchronous architecture becomes predominantly much more power efficient. Although QDI asynchronous design leads to almost the double of area than its synchronous counterpart, it has been noticed that it is intrinsically robust, and thus suitable for applications requiring high reliability and security. The synchronous design, otherwise, has to be adapted by receiving extra circuitry that may make it robust to situations in which asynchronous design is already prepared to face. Results of this work allows to define new voltage scaling strategies for FD-SOI 28-nm asynchronous circuits, and in addition with the body biasing features of this technology, more power savings can be envisioned. Ongoing works analyze the synchronous and asynchronous ALU circuits with different body biasing voltages.

Chapter 7

Conclusions and perspectives

A post-fabrication testing method for detecting hardware Trojans (HT), a run-time testing mechanism for detecting transient faults (TF), and a bias scheme for adaptively compensating voltage threshold (Vth) variations, as well as optimizing power and speed of integrated systems, are presented and discussed in this work. All proposed techniques monitor the body terminals of transistors, fully exploiting modern advanced fabrication processes, such as the UTBB FD-SOI technology, which efficiently control the body biasing effects on transistor channels, allowing the application of wider ranges of body-to-source voltage (V_{BS}) levels without risks of collateral consequences like CMOS latch-ups.

State-of-the-art run-time testing mechanisms for detecting TF have been evaluated in this work by using a simulation-based method proposed in chapter 2. Results provide a rank in terms of their effectivenesses in detecting TF, revealing the bulk built-in current sensors (BBICS) as the most efficient solution. BBICS integrates the high concurrent error detection efficiency of costly techniques (duplication with comparison) with the low area and power overheads of less efficient run-time testing mechanisms (time redundancy schemes). Moreover, unlike most existing TF-detection techniques, the BBICS is also able to detect long-duration and multiple TF, a major problem in intentional fault-based attacks targeting to break the security of integrated systems. For this reason, available BBICS architectures in literature have been studied and compared in this work with regard to their sensitivities in detecting TF. Chapter 3 presents such comparison results and a novel BBICS architecture with enhanced TF-detection sensitivity, negligible power consumption, and lower area penalty than its antecedents.

Furthermore, we have discovered a second function for the BBICS: the detection of HT. Chapter 4 details our post-fabrication testing method that takes advantage of the BBICS as an offline-testing mechanism for detecting HT. As this type of sensor monitors body terminals of system's subcircuits, the proposed method is capable to identify any slight HT-induced variations on the electrical impedance of subcircuits by simply injecting a short train of current pulses into body terminals, and analyzing digital signatures provided by the BBICS. At run time, the same BBICS operates as an online-testing mechanism for detecting TF. This method adds a new category to the classical taxonomy of side-channel analysis-based techniques, it is indeed the first work that analyzes as a side channel the digital signatures related to the impedance of subcircuit's n-well or p-well regions.

Partitioning integrated systems into subcircuits having single n-well or p-well regions allows, in addition to individually manage them at run time, better controlling Vth variations, power, and speed. Chapter 5 of this work presents a new architecture of a specific built-in cell that is mandatory to dynamically adapt the body bias of small subcircuits: a level shifter (LS). With reasonable area, power, and delay penalties, the proposed LS cell is fully suitable for fine-grained systems such as circuits designed with asynchronous logic, which is intrinsically

modular due to the absence of a clock. For this purpose, chapter 6 discusses advantages of applying body biasing schemes on asynchronous circuits designed in UTBB FD-SOI technology, besides underlining the better energy efficiency of an asynchronous 8-bit ALU – compared with its synchronous counterpart – and its lower voltage operation thanks to its reduced number of timing assumptions.

7.1 Short-term perspectives

Putting into perspective the works proposed and discussed herein, we immediately note all them exploit the body terminals of transistors, and hence, in the near future, the first major insight is to merge their main actors (BBICS and LS), promoting the creation of a never seen before unique cell having quintuple function: (1) detection of big or slight stealthy HT; (2) detection of single, multiple, short-duration, or long-duration TF; (3) compensation of Vth alterations induced by aging, PVT variations, or body bias modifications; (4) optimization of the system's trade-off between low power and high speed; and (5) operating alike with the classical filler cells of typical integrated circuit design flows, i.e. filling intra-core spaces that are intentionally left between regular standard logic cells for a successful place and route of all them, moreover connecting, evidently, body terminals of transistors to power rails. The envisioned quintuple function cells could, therefore, replace the classical filler cells, or some of them, helping to mitigate the already low area overhead imposed by the elements of the BBICS and LS circuitry.

Complementary to the development of such a unique cell, our ongoing works are studying optimal hardware schemes able to identify switching activities in subcircuits of asynchronous pipelines and, shortly afterward, drive LS cells for adaptively biasing body terminals of subsequent subcircuits in asynchronously-pipelined systems. This envisioned body bias schemes could thus play to automatically control the system power and speed, applying low-power body bias conditions on inactive subcircuits, and high-speed body bias conditions on active subcircuits. In case of quasi-delay insensitive (QDI) asynchronous systems, the circuitry of body bias schemes would analyze request and acknowledgement signals between subcircuits and their input data, which are normally encoded, for instance, through dual rails that allow to represent four states: 01 (valid data 1), 10 (valid data 0), 00 (invalid data), and 11 (forbidden state appearing only in error situations). Accordingly, the same logic gates of the body bias schemes could be exploited to also provide alarm signals indicating the occurrence of forbidden states, empowering asynchronous properties of detecting soft errors – i.e. bit flips induced in memory elements by radiation or malicious sources.

Behind the adaptive body bias aspects of the envisioned cells, an additional function operating like human eyes is required to identify Vth alterations and appropriately inform LS cells in the actions of compensating it. For that purpose, the astute properties of the asynchronous logic can help us again with the design of high-resolution time-to-digital converters (TDC) that are potentially able to measure delay deviations induced by Vth alterations in subcircuit elements. TIMA laboratory has been studied asynchronous TDC architectures since 2016, getting preliminary insights in calibrating high resolutions by using a method based on self-timed rings (STR) or, alternatively, a hybrid solution having, for instance, a more stable oscillator with a coarse grain resolution and a fine–grain resolution STR. A radiation hardness high-resolution TDC will also be devised and qualified under radiation effects in the context of the project NanoBob of the CSUG (Centre Spatial Universitaire de Grenoble). The works will start in 2018 with the goal of lunching a nanosatellite in 2020. The devised TDC will have the role to sample photon arrivals from the quantum communication between ground stations and the nanosatellite.

7.2 Medium-term perspectives

Most our works exploit asynchronous circuits that have by nature several well-known advantages in terms of security, reliability, and power, perfectly fitting with today's demands of related applications requiring such features. Even though asynchronous design style has been more regularly demanded by the microelectronics industry to improve, mainly, the security of systems, the lack of steady and commercial tools for the specification, verification, and design of them has oriented most of the research efforts to the that direction. Only a few works, however, have paid attention in seeking solutions dedicated to test asynchronous circuits after fabrication, and even less whether we take into account specific issues of advanced nanometer technology processes. Relevant reference papers date back to 1995 [49], 2002 [7], 2004 [58], and more recently 2010 [35], 2011 [24], 2013 [99], and 2015 [112, 143].

The challenge for the testing of asynchronous circuits is directly associated to the breadth of manners we can design them. Two known classes of asynchronous circuits are especially attractive for the design of security systems in advanced technologies: (1) the micropipeline circuits, which are quite similar to the classic synchronous architectures, operate with a local-synchronization structure based on handshake that completely replaces the use of a clock network. The data path is kept exactly such as in synchronous pipelines, requiring design efforts close to the practices we find today in the industry; and (2) the QDI asynchronous circuits, otherwise, have only a few timing assumptions on wires of critical forks. All other wires and gates use an unbounded-delay model, making QDI circuits very robust to delay variations, and a relevant option for applications that need high levels of security.

The reuse of traditional design for testing (DfT) mechanisms devised initially to synchronous circuits, such as functional testing, built-in self test (BIST), scan chains, and automatic test pattern generation (ATPG), is certainly a natural start point to derive new techniques able to efficiently test asynchronous circuits. Nevertheless, the presence of an unbounded-delay model in QDI circuits, and in the control part of micropipeline circuits, produces nondeterministic conditions, and consequent difficulties for testing them with conventional DfT mechanisms and commercial testers, all expecting circuit's responses by clock cycle. As asynchronous circuits have no determined time to conclude computations of input logic stimuli, testing methods have to consider and define a suitable bounded-delay model in order to check if the asynchronous device under test (ADUT) properly operates below a certain upper limit. The non-existence of a clock cadence, moreover, complicates the controllability of the testing as well as the adaptation of efficient step-based techniques that increase the fault coverage by scanning internal flip-flops.

A project beginning in October 2017 goals to propose new testing solutions that circumvent nondeterminism and controllability issues of micropipeline and QDI asynchronous circuits. We plan to take advantage of existing testing methods and tester equipment dedicated to synchronous circuits in order to limit costs and make the solution applicable by the industry. The innovative aspects of this work are directly related to the testing of asynchronous circuits in advanced technologies. To the best of our knowledge, there are no works in literature that answer such a question within the context of today's complex technology processes. For that, we have some insights to solve it by exploiting fault-induced deadlocks in asynchronous circuits, and built-in current sensors to increase the fault coverage in delay-sensitive parts of the ADUT. Additional challenge will be dealing with the reliability questions of advanced technologies, even though asynchronous design paradigm is able to compensate them with its inherent robustness properties.

7.3 Long-term perspectives

Closing the perspective circle of near-future works related to the fields of the post-fabrication test, run-time test, and adaptive body bias in asynchronous integrated circuits, we have incoming fresh ideas to explore and devise new artificial intelligence (AI) features that would operate to learn, memorize, and take decisions based on the history of the system behavior. For that, our new challenges will be to search suitable neural networks capable to deal with local power and data throughput of system subcircuits for smartly acting on the control of the body bias, and thus eventually compensating Vth alterations provoked by aging and PVT variations. Towards the addition of AI aspects in adaptive body bias schemes applied on asynchronous circuits, we expect to research and invent built-in components that will transform adaptive asynchronous systems into self-adaptive. Moreover, profiting from our background, expertise, and international collaborations, we goal to evaluate how self-adaptive asynchronous systems react under radiation-induced effects, qualify them, and propose more efficient countermeasures.

In the advent of AI systems, new design solutions will have to be devised, verified, and tested, qualifying them under unprecedented situations of which we will have to predict as well. Today's and future many applications of integrated systems through autonomous electronics mechanisms to tiny IoT devices will demand more and more the attention of researchers and engineers. The society and industry's dependence on such smart systems will further push the research to find answers for issues related to the reliability, security, and power optimization, opening to us new opportunities and perspectives.

References

[1] AARESTAD, J., ACHARYYA, D., RAD, R., AND PLUSQUELLIC, J. Detecting Trojans Through Leakage Current Analysis Using Multiple Supply Pad $I_rm DDQ$s. *IEEE Transactions on Information Forensics and Security 5*, 4 (Dec. 2010), 893–904.

[2] AGRAWAL, D., BAKTIR, S., KARAKOYUNLU, D., ROHATGI, P., AND SUNAR, B. Trojan Detection using IC Fingerprinting. In *2007 IEEE Symposium on Security and Privacy (SP '07)* (May 2007), pp. 296–310.

[3] ANGHEL, L., AND NICOLAIDIS, M. Cost reduction and evaluation of a temporary faults detecting technique. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition 2000 (Cat. No. PR00537)* (2000), pp. 591–598.

[4] ATHAN, S. P., ET AL. A novel built-in current sensor for iddq testing of deep submicron cmos ics. In *Proc. IEEE (VTS'96)* (1996), pp. 118–123.

[5] BARENGHI, A., BREVEGLIERI, L., KOREN, I., AND NACCACHE, D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. *Proceedings of the IEEE 100*, 11 (Nov. 2012), 3056–3076.

[6] BECKER, G., REGAZZONI, F., PAAR, C., AND BURLESON, W. Stealthy dopant-level hardware trojans. In *CHES* (2013), pp. 197–214.

[7] BEEST, F. T., PEETERS, A., VERRA, M., BERKEL, K. V., AND KERKHOFF, H. Automatic scan insertion and test generation for asynchronous circuits. In *Proceedings. International Test Conference* (2002), pp. 804–813.

[8] BEIGNÉ, E., VALENTIAN, A., GIRAUD, B., THOMAS, O., BENOIST, T., THONNART, Y., BERNARD, S., MORITZ, G., BILLOINT, O., MANEGLIA, Y., ET AL. Ultra-wide voltage range designs in fully-depleted silicon-on-insulator FETs. In *Conference on Design, Automation and Test in Europe (DATE)* (2013), EDA Consortium, pp. 613–618.

[9] BEN-AKKEZ, I., FENOUILLET-BERANGER, C., CROS, A., BALESTRA, F., AND GHIBAUDO, G. Impact of back biasing on the effective mobility in UTBB FDSOI CMOS technology. In *Semiconductor Conference Dresden-Grenoble (ISCDG), 2013 International* (Sept 2013), pp. 1–3.

[10] BLAGOJEVIĆ, M., COCHET, M., KELLER, B., FLATRESSE, P., VLADIMIRESCU, A., AND NIKOLIĆ, B. A fast, flexible, positive and negative adaptive body-bias generator in 28nm FDSOI. In *2016 IEEE Symposium on VLSI Circuits (VLSI-Circuits)* (June 2016), pp. 1–2.

[11] BORREL, N., CHAMPEIX, C., KUSSENER, E., RAHAJANDRAIBE, W., LISART, M., SARAFIANOS, A., AND DUTERTRE, J. M. Influence of triple-well technology on laser fault injection and laser sensor efficiency. In *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)* (Oct. 2015), pp. 85–90.

[12] BOWMAN, K. A., TSCHANZ, J. W., KIM, N. S., LEE, J. C., WILKERSON, C. B., LU, S. L. L., KARNIK, T., AND DE, V. K. Energy-Efficient and Metastability-Immune Resilient Circuits for Dynamic Variation Tolerance. *IEEE Journal of Solid-State Circuits 44*, 1 (Jan. 2009), 49–63.

[13] CAO, Y., CHANG, C. H., AND CHEN, S. A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection. *IEEE Transactions on Information Forensics and Security 9*, 12 (Dec. 2014), 2220–2231.

[14] CAO, Y., YE, W., ZHAO, X., AND DENG, P. An energy-efficient subthreshold level shifter with a wide input voltage range. In *2016 IEEE International Symposium on Circuits and Systems (ISCAS)* (May 2016), pp. 726–729.

[15] CASTRO, S. D., NATALE, G. D., FLOTTES, M. L., ROUZEYRE, B., AND DUTERTRE, J. M. Figure of Merits of 28nm Si Technologies for Implementing Laser Attack Resistant Security Dedicated Circuits. In *2015 IEEE Computer Society Annual Symposium on VLSI* (July 2015), pp. 362–367.

[16] CHA, B., AND GUPTA, S. K. Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost. In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)* (Mar. 2013), pp. 1265–1270.

[17] CHA, H., AND PATEL, J. A logic-level model for alpha-particle hits in cmos circuits. In *Proc. IEEE International Conference on Computer Design (ICCD'93)* (1993), pp. 538–542.

[18] CHAKRABORTY, R., PAUL, S., AND BHUNIA, S. On-demand transparency for improving hardware trojan detectability. In *HOST* (2008), pp. 48–50.

[19] CHAMPEIX, C., ET AL. Experimental validation of a bulk built-in current sensor for detecting laser-induced currents. In *Proc. IEEE (IOLTS'15)* (2015), pp. 150–155.

[20] CHANG, I. J., KIM, J. J., KIM, K., AND ROY, K. Robust Level Converter for Sub-Threshold/Super-Threshold Operation:100 mV to 2.5 V. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 19*, 8 (Aug. 2011), 1429–1437.

[21] CHANG, K.-L., CHANG, J., GWEE, B.-H., AND CHONG, K.-S. Synchronous-logic and asynchronous-logic 8051 microcontroller cores for realizing the Internet of Things: A comparative study on dynamic voltage scaling and variation effects. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems 3*, 1 (2013), 23–34.

[22] CHEN, L., ET AL. Methods and devices for detecting single-event transients. In *U.S. patent no. 8,451,028.* (2013).

[23] CHEN, T.-H., CHEN, J., AND CLARK, L. T. Subthreshold to Above Threshold Level Shifter Design. *Journal of Low Power Electronics 2*, 2 (Aug. 2006), 251–258.

[24] CHENG, C.-H., AND LI, J. C.-M. An Asynchronous Design for Testability and Implementation in Thin-film Transistor Technology. *Journal of Electronic Testing 27*, 2 (Apr. 2011), 193–201.

[25] COOK, G., LEE, J., TSAI, T., KONG, A., DEANS, J., JOHNSON, B., AND JARDIM, E. Clicking Clean: Who is Winning the Race to Build A Green Internet? Tech. rep., Greenpeace Inc., Jan. 2017.

[26] CORSONELLO, P., FRUSTACI, F., AND PERRI, S. A layout strategy for low-power voltage level shifters in 28nm UTBB FDSOI technology. In *2015 AEIT International Annual Conference (AEIT)* (Oct. 2015), pp. 1–5.

[27] COURBON, F., LOUBET-MOUNDI, P., FOURNIER, J. J. A., AND TRIA, A. A high efficiency hardware trojan detection technique based on fast sem imaging. In *DATE* (2015), pp. 788–793.

[28] DAL, D., NUNEZ, A., AND MANSOURI, N. Power islands: a high-level technique for counteracting leakage in deep sub-micron. In *7th International Symposium on Quality Electronic Design (ISQED'06)* (Mar. 2006), pp. 6 pp.–170.

[29] DAS, S., TOKUNAGA, C., PANT, S., MA, W. H., KALAISELVAN, S., LAI, K., BULL, D. M., AND BLAAUW, D. T. RazorII: In Situ Error Detection and Correction for PVT and SER Tolerance. *IEEE Journal of Solid-State Circuits 44*, 1 (Jan. 2009), 32–48.

[30] DE STREEL, G., AND BOL, D. Impact of back gate biasing schemes on energy and robustness of ULV logic in 28nm UTBB FDSOI technology. In *IEEE International Symposium on Low Power Electronics and Design (ISLPED)* (Sept 2013), pp. 255–260.

[31] DE STREEL, G., AND BOL, D. Study of Back Biasing Schemes for ULV Logic from the Gate Level to the IP Level. *Journal of Low Power Electronics and Applications 4*, 3 (July 2014), 168–187.

[32] DODD, P., ET AL. Production and propagation of single-event transients in high-speed digital logic ics. *IEEE Trans. Nuclear Science 51*, 6 (2004), 3278–3284.

[33] DUTERTRE, J.-M., ET AL. Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection. *Microelectronics Reliability 53*, 9 (2013), 1320–1324.

[34] DUTERTRE, J.-M., ET AL. Improving the ability of bulk built-in current sensors to detect single event effects by using triple-well cmos. *Microelectronics Reliability 54*, 9-10 (2014), 2289–2294.

[35] EFTHYMIOU, A. Initialization-Based Test Pattern Generation for Asynchronous Circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 18*, 4 (Apr. 2010), 591–601.

[36] FERLET-CABROIS, V., ET AL. Statistical analysis of the charge collected in soi and bulk devices under heavy ion and proton irradiation—implications for digital sets. *IEEE Trans. Nuclear Science 53*, 6 (2006), 3242–3252.

[37] GARG, S., AND MARCULESCU, D. System-Level Leakage Variability Mitigation for MPSoC Platforms Using Body-Bias Islands. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 20*, 12 (Dec. 2012), 2289–2301.

[38] GILL, B., ET AL. An efficient bics design for seus detection and correction in semiconductor memories. In *Proc. IEEE (DATE'05)* (2005), pp. 592–597.

[39] GODLEWSKI, C., POUGET, V., LEWIS, D., AND LISART, M. Electrical modeling of the effect of beam profile for pulsed laser fault injection. *Microelectronics Reliability 49*, 9 (Sept. 2009), 1143–1147.

[40] GOSATWAR, P., AND GHODESWAR, U. Design of voltage level shifter for multi-supply voltage design. In *2016 International Conference on Communication and Signal Processing (ICCSP)* (Apr. 2016), pp. 0853–0857.

[41] GUIMARÃES, L. A., POSSAMAI BASTOS, R., LEITE, T. F. P., AND FESQUET, L. Simple tri-state logic trojans able to upset properties of ring oscillators. In *Proc. Design Technology of Integrated Systems in Nanoscale Era (DTIS), 2016 11th International Conference on* (April 2016), pp. 1–6.

[42] GUIMARÃES, M. V., AND TORRES, F. S. Automatic layout integration of bulk built-in current sensors for detection of soft errors. In *Proc. Symposium on Integrated Circuits and Systems Design (SBCCI'16)* (2016), pp. 1–6.

[43] HAMADA, M., TAKAHASHI, M., ARAKIDA, H., CHIBA, A., TERAZAWA, T., ISHIKAWA, T., KANAZAWA, M., IGARASHI, M., USAMI, K., AND KURODA, T. A top-down low power design technique using clustered voltage scaling with variable supply-voltage scheme. In *Proceedings of the IEEE 1998 Custom Integrated Circuits Conference (Cat. No.98CH36143)* (May 1998), pp. 495–498.

[44] HAMON, J., AND BEIGNE, E. Automatic Leakage Control for Wide Range Performance QDI Asynchronous Circuits in FD-SOI Technology. In *2013 IEEE 19th International Symposium on Asynchronous Circuits and Systems* (May 2013), pp. 142–149.

[45] HAMON, J., AND BEIGNE, E. Automatic leakage control for wide range performance QDI asynchronous circuits in FD-SOI technology. In *19th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)* (May 2013), pp. 142–149.

[46] HELLER, L., GRIFFIN, W., DAVIS, J., AND THOMA, N. Cascode voltage switch logic: A differential CMOS logic family. In *1984 IEEE International Solid-State Circuits Conference. Digest of Technical Papers* (Feb. 1984), vol. XXVII, pp. 16–17.

[47] HOSSEINI, S. R., SABERI, M., AND LOTFI, R. An energy-efficient level shifter for low-power applications. In *2015 IEEE International Symposium on Circuits and Systems (ISCAS)* (May 2015), pp. 2241–2244.

[48] HU, K., NOWROZ, A. N., REDA, S., AND KOUSHANFAR, F. High-sensitivity hardware trojan detection using multimodal characterization. In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)* (March 2013), pp. 1271–1276.

[49] HULGAARD, H., BURNS, S. M., AND BORRIELLO, G. Testing asynchronous circuits: A survey. *Integration, the VLSI Journal 19*, 3 (Nov. 1995), 111–131.

[50] ISHIHARA, F., SHEIKH, F., AND NIKOLIC, B. Level conversion for dual-supply systems. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 12*, 2 (Feb. 2004), 185–195.

[51] JHA, S., AND JHA, S. Randomization based probabilistic approach to detect trojan circuits. In *HASE* (2008), pp. 117–124.

[52] JIN, Y., AND MAKRIS, Y. Hardware Trojan detection using path delay fingerprint. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (June 2008), pp. 51–57.

[53] KAMAE, N., ISLAM, A. K. M. M., TSUCHIYA, A., AND ONODERA, H. A body bias generator with wide supply-range down to threshold voltage for within-die variability compensation. In *2014 IEEE Asian Solid-State Circuits Conference (A-SSCC)* (Nov. 2014), pp. 53–56.

[54] KAO, J. T., AND CHANDRAKASAN, A. P. Dual-threshold voltage techniques for low-power digital circuits. *IEEE Journal of Solid-State Circuits 35*, 7 (July 2000), 1009–1018.

[55] KARNIK, T., AND HAZUCHA, P. Characterization of soft errors caused by single event upsets in CMOS processes. *IEEE Transactions on Dependable and Secure Computing 1*, 2 (Apr. 2004), 128–143.

[56] KIM, C. H., AND QUISQUATER, J. J. Faults, Injection Methods, and Fault Attacks. *IEEE Design Test of Computers 24*, 6 (Nov. 2007), 544–545.

[57] KIM, Y., LEE, Y., SYLVESTER, D., AND BLAAUW, D. SLC: Split-control Level Converter for dense and stable wide-range voltage conversion. In *2012 Proceedings of the ESSCIRC (ESSCIRC)* (Sept. 2012), pp. 478–481.

[58] KING, M. L., AND SALUJA, K. K. Testing micropipelined asynchronous circuits. In *2004 International Conference on Test* (Oct. 2004), pp. 329–338.

[59] KOO, K.-H., SEO, J.-H., KO, M.-L., AND KIM, J.-W. A new level-up shifter for high speed and wide range interface in ultra deep sub-micron. In *2005 IEEE International Symposium on Circuits and Systems* (May 2005), pp. 1063–1065 Vol. 2.

[60] KULKARNI, S. H., AND SYLVESTER, D. High performance level conversion for dual V/sub DD/ design. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 12*, 9 (Sept. 2004), 926–936.

[61] KULKARNI, S. H., SYLVESTER, D., AND BLAAUW, D. A Statistical Framework for Post-Silicon Tuning through Body Bias Clustering. In *2006 IEEE/ACM International Conference on Computer Aided Design* (Nov. 2006), pp. 39–46.

[62] KUMAR, R., JOVANOVIC, P., BURLESON, W., AND POLIAN, I. Parametric trojans for fault-injection attacks on cryptographic hardware. In *FDTC* (2014), pp. 18–28.

[63] KURSUN, V., AND FRIEDMAN, E. G. Supply and Threshold Voltage Scaling Techniques. In *Multi-Voltage CMOS Circuit Design*. John Wiley & Sons, Ltd, 2006, pp. 45–84.

[64] LANUZZA, M., CRUPI, F., RAO, S., ROSE, R. D., STRANGIO, S., AND IANNACCONE, G. An Ultralow-Voltage Energy-Efficient Level Shifter. *IEEE Transactions on Circuits and Systems II: Express Briefs 64*, 1 (Jan. 2017), 61–65.

[65] LEITE, F., ET AL. Using bulk built-in current sensors and recomputing techniques to mitigate transient faults in microprocessors. In *Proc. Latin American Test Workshop (LATW'09)* (2009), pp. 1–6.

[66] LIN, Y. S., AND SYLVESTER, D. M. Single stage static level shifter design for sub-threshold to I/O voltage conversion. In *2008 ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED)* (Aug. 2008), pp. 197–200.

[67] LINES, A. M. Pipelined asynchronous circuits. Tech. rep., California Institute of Technology, 1998.

[68] LISBOA, C., ET AL. Using built-in sensors to cope with long duration transient faults in future technologies. In *Proc. IEEE International Test Conference (ITC'07)* (2007), pp. 1–10.

[69] LO, J., ET AL. Design of static cmos self-checking circuits using built-in current sensing. In *Proc. IEEE (FTCS'92)* (1992), pp. 104–111.

[70] LUO, S. C., HUANG, C. J., AND CHU, Y. H. A Wide-Range Level Shifter Using a Modified Wilson Current Mirror Hybrid Buffer. *IEEE Transactions on Circuits and Systems I: Regular Papers 61*, 6 (June 2014), 1656–1665.

[71] LUTKEMEIER, S., AND RUCKERT, U. A Subthreshold to Above-Threshold Level Shifter Comprising a Wilson Current Mirror. *IEEE Transactions on Circuits and Systems II: Express Briefs 57*, 9 (Sept. 2010), 721–724.

[72] MAKIPAA, J., AND BILLOINT, O. FDSOI versus BULK CMOS at 28 nm node which technology for ultra-low power design? In *IEEE International Symposium on Circuits and Systems (ISCAS)* (May 2013), pp. 554–557.

[73] MANOHAR, R., AND MARTIN, A. J. Quasi-delay-insensitive circuits are turing-complete. Tech. rep., California Institute of Technology, Pasadena, CA, USA, 1995.

[74] MARTIN, A., AND NYSTROM, M. Asynchronous techniques for system-on-chip design. *Proceedings of the IEEE 94*, 6 (2006), 1089–1120.

[75] MASSEY JR, F. J. The kolmogorov-smirnov test for goodness of fit. *Journal of the American statistical Association 46*, 253 (1951), 68–78.

[76] MATSUZUKA, R., HIROSE, T., SHIZUKU, Y., KUROKI, N., AND NUMA, M. A 0.19-V minimum input low energy level shifter for extremely low-voltage VLSIs. In *2015 IEEE International Symposium on Circuits and Systems (ISCAS)* (May 2015), pp. 2948–2951.

[77] MAURICIO, J., AND MOLL, F. Local variations compensation with DLL-based Body Bias Generator for UTBB FD-SOI technology. In *2015 IEEE 13th International New Circuits and Systems Conference (NEWCAS)* (June 2015), pp. 1–4.

[78] MELO, J. G. M., AND SILL TORRES, F. Exploration of noise impact on integrated bulk current sensors. *Journal of Electronic Testing, Theory and Applications (JETTA) 32*, 2 (2016), 163–173.

[79] MELO, J. G. M., SILL TORRES, F., AND POSSAMAI BASTOS, R. Exploration of noise robustness and sensitivity of bulk current sensors for soft error detection. In *Proc. CMOS Variability (VARI), 2015 6th European Workshop on* (2015), pp. 13–18.

[80] MESSENGER, G. C. Collection of charge on junction nodes from ion tracks. *IEEE Transactions on Nuclear Science 29*, 6 (Dec 1982), 2024–2031.

[81] MITRA, S., ET AL. Which concurrent error detection scheme to choose ? In *ITC* (2000), pp. 985–994.

[82] MITRA, S., ZHANG, M., WAQAS, S., SEIFERT, N., GILL, B., AND KIM, K. S. Combinational Logic Soft Error Correction. In *2006 IEEE International Test Conference* (Oct. 2006), pp. 1–9.

[83] MOEIN, S., ET AL. Classification of hardware trojan detection techniques. In *ICCES* (2015).

[84] MUKHERJEE, S. *Architecture Design for Soft Errors*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008.

[85] NARASIMHAN, S., AND BHUNIA, S. *Hardware Trojan Detection*. Springer New York, New York, NY, 2012, pp. 339–364.

[86] NARASIMHAN, S., DU, D., CHAKRABORTY, R. S., PAUL, S., WOLFF1, F., PAPACHRISTOU, C., ROY, K., AND BHUNIA, S. Multiple-parameter side-channel analysis: A non-invasive hardware Trojan detection approach. In *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (June 2010), pp. 13–18.

[87] NARSALE, A., AND M. C. HUANG, M. C. Variation-tolerant hierarchical voltage monitoring circuit for soft error detection. In *Proc. IEEE (ISQED'09)* (2009), pp. 799–805.

[88] NDAI, P., ET AL. A soft error monitor using switching current detection. In *Proc. IEEE (ICCD'05)* (2005), pp. 185–190.

[89] NETO, E. H., ET AL. Evaluating fault coverage of bulk built-in current sensor for soft errors in combinational and sequential logic. In *Proc. Symposium on Integrated Circuits and Systems Design (SBCCI'12)* (2005), pp. 62–67.

[90] NETO, E. H., KASTENSMIDT, F. L., AND WIRTH, G. Tbulk-bics: A built-in current sensor robust to process and temperature variations for soft error detection. *IEEE Trans. Nuclear Science 55*, 4 (2008), 2281–2288.

[91] NETO, E. H., RIBEIRO, I., VIEIRA, M., WIRTH, G., AND KASTENSMIDT, F. L. Using Bulk Built-in Current Sensors to Detect Soft Errors. *IEEE Micro 26*, 5 (Sept. 2006), 10–18.

[92] NGO, X. T., EXURVILLE, I., BHASIN, S., DANGER, J. L., GUILLEY, S., NAJM, Z., RIGAUD, J. B., AND ROBISSON, B. Hardware Trojan detection by delay and electromagnetic measurements. In *2015 Design, Automation Test in Europe Conference Exhibition (DATE)* (Mar. 2015), pp. 782–787.

[93] NICOLAIDIS, M. Time redundancy based soft-error tolerance to rescue nanometer technologies. In *Proceedings 17th IEEE VLSI Test Symposium (Cat. No.PR00146)* (1999), pp. 86–94.

[94] NICOLAIDIS, M. Design for soft error mitigation. *IEEE Transactions on Device and Materials Reliability 5*, 3 (Sept. 2005), 405–418.

[95] NIELSEN, L., AND SPARSØ, J. Designing asynchronous circuits for low power: an IFIR filter bank for a digital hearing aid. *Proceedings of the IEEE 87*, 2 (1999), 268–281.

[96] NIELSEN, L. S., NIESSEN, C., SPARSO, J., AND BERKEL, K. V. Low-power operation using self-timed circuits and adaptive scaling of the supply voltage. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2*, 4 (Dec. 1994), 391–397.

[97] NOWROZ, A. N., HU, K., KOUSHANFAR, F., AND REDA, S. Novel Techniques for High-Sensitivity Hardware Trojan Detection Using Thermal and Power Maps. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33*, 12 (Dec. 2014), 1792–1805.

[98] OSAKI, Y., HIROSE, T., KUROKI, N., AND NUMA, M. A Low-Power Level Shifter With Logic Error Correction for Extremely Low-Voltage Digital CMOS LSIs. *IEEE Journal of Solid-State Circuits 47*, 7 (July 2012), 1776–1783.

[99] PAKBAZ, F., SMITH, J. R., AND VENTRONE, S. T. Asynchronous circuit with an at-speed built-in self-test (BIST) architecture, Dec. 2013.

[100] PALFRAMAN, D. J., KIM, N. S., AND LIPASTI, M. H. Time redundant parity for low-cost transient error detection. In *2011 Design, Automation Test in Europe* (Mar. 2011), pp. 1–6.

[101] PELLOUX-PRAYER, B., BLAGOJEVIĆ, M., THOMAS, O., AMARA, A., VLADIMIRESCU, A., NIKOLIĆ, B., CESANA, G., AND FLATRESSE, P. Planar fully depleted SOI technology: The convergence of high performance and low power towards multimedia mobile applications. In *2012 IEEE Faible Tension Faible Consommation* (June 2012), pp. 1–4.

[102] PELLOUX-PRAYER, B., VALENTIAN, A., GIRAUD, B., THONNART, Y., NOEL, J. P., FLATRESSE, P., AND BEIGN, E. Fine grain multi-v<inf>t</inf> co-integration methodology in UTBB FD-SOI technology. In *IFIP/IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC)* (2013), pp. 168–173.

[103] PELLOUX-PRAYER, B., VALENTIAN, A., GIRAUD, B., THONNART, Y., NOEL, J. P., FLATRESSE, P., AND BEIGNÉ, E. Fine grain multi-VT co-integration methodology in UTBB FD-SOI technology. In *2013 IFIP/IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC)* (Oct. 2013), pp. 168–173.

[104] POSSAMAI BASTOS, R., DUTERTRE, J.-M., AND SILL TORRES, F. Comparison of bulk built-in current sensors in terms of transient-fault detection sensitivity. In *Proc. CMOS Variability (VARI), 2014 5th European Workshop on* (2014), pp. 1–6.

[105] POSSAMAI BASTOS, R., ET AL. A new bulk built-in current sensor-based strategy for dealing with long-duration transient faults in deep-submicron technologies. In *Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT'11)* (2011), pp. 302–308.

[106] POSSAMAI BASTOS, R., ET AL. Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode. *Microelectronics Reliability 52*, 9-10 (2012), 1781–1786.

[107] POSSAMAI BASTOS, R., ET AL. A bulk built-in sensor for detection of fault attacks. In *Proc. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'13)* (2013), pp. 51–54.

[108] POSSAMAI BASTOS, R., ET AL. A single built-in sensor to check pull-up and pull-down cmos networks against transient faults. In *Proc. International Workshop on Power and Timing Modeling, Optimization, and Simulation (PATMOS'13)* (2013), pp. 157–163.

[109] POSSAMAI BASTOS, R., NATALE, G. D., FLOTTES, M.-L., LU, F., AND ROUZEYRE, B. A New Recovery Scheme Against Short-to-Long Duration Transient Faults in Combinational Logic. *Journal of Electronic Testing 29*, 3 (June 2013), 331–340.

[110] PURI, R., STOK, L., COHN, J., KUNG, D., PAN, D., SYLVESTER, D., SRIVASTAVA, A., AND KULKARNI, S. Pushing ASIC performance in a power envelope. In *Proceedings 2003. Design Automation Conference (IEEE Cat. No.03CH37451)* (June 2003), pp. 788–793.

[111] RAJALAKSHMI, T. R., AND SUDHAKAR, R. A novel carbon nanotubefet based bulk built-in current sensor for single event upset detection. *Sadhana 41*, 5 (2016), 489–495.

[112] RONCKEN, M., GILLA, S. M., PARK, H., JAMADAGNI, N., COWAN, C., AND SUTHERLAND, I. Naturalized Communication and Testing. In *2015 21st IEEE International Symposium on Asynchronous Circuits and Systems* (May 2015), pp. 77–84.

[113] ROSSI, D., OMANA, M., AND METRA, C. Transient Fault and Soft Error On-die Monitoring Scheme. In *2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems* (Oct. 2010), pp. 391–398.

[114] SALMANI, H., TEHRANIPOOR, M., AND KARRI, R. On design vulnerability analysis and trust benchmark development. In *ICCD* (2013).

[115] SELLERS, F., ET AL. *Error detecting logic for digital computers*. McGraw-Hill, 1968.

[116] SHAO, H., AND TSUI, C.-Y. A robust, input voltage adaptive and low energy consumption level converter for sub-threshold logic. In *ESSCIRC 2007 - 33rd European Solid-State Circuits Conference* (Sept. 2007), pp. 312–315.

[117] SHOR, J. S., AFEK, Y., AND ENGEL, E. IO buffer for high performance, low-power application. In *Proceedings of CICC 97 - Custom Integrated Circuits Conference* (May 1997), pp. 595–598.

[118] SILL TORRES, F., AND POSSAMAI BASTOS, R. Robust modular bulk built-in current sensors for detection of transient faults. In *Proc. Symposium on Integrated Circuits and Systems Design (SBCCI'12)* (2012), pp. 1–6.

[119] SILL TORRES, F., AND POSSAMAI BASTOS, R. Detection of transient faults in nanometer technologies by using modular built-in current sensors. *Journal of Integrated Circuits and Systems (JICS) 8*, 2 (2013), 89–97.

[120] SIMIONOVSKI, A., AND WIRTH, G. A bulk built-in current sensor for set detection with dynamic memory cell. In *Proc. IEEE Latin American Symposium on Circuits and Systems (LASCAS'12)* (2012), pp. 1–4.

[121] SIMIONOVSKI, A., AND WIRTH, G. Simulation Evaluation of an Implemented Set of Complementary Bulk Built-In Current Sensors With Dynamic Storage Cell. *IEEE Transactions on Device and Materials Reliability 14*, 1 (Mar. 2014), 255–261.

[122] SIMIONOVSKI, A., AND WIRTH, G. Adding a self-reset feature to the bulk-bics with dynamic storage cell. *Microelectronics Reliability 55*, 12 (2015), 2748–2753.

[123] SPARSØ, J., AND FURBER, S. *Principles of Asynchronous Circuit Design*. Springer, 2002.

[124] TACO, R., LEVI, I., FISH, A., AND LANUZZA, M. Exploring back biasing opportunities in 28nm UTBB FD-SOI technology for subthreshold digital design. In *2014 IEEE 28th Convention of Electrical Electronics Engineers in Israel (IEEEI)* (Dec. 2014), pp. 1–4.

[125] TAWFIK, S. A., AND KURSUN, V. Multi-Vth Level Conversion Circuits for Multi-VDD Systems. In *2007 IEEE International Symposium on Circuits and Systems* (May 2007), pp. 1397–1400.

[126] TEHRANIPOOR, M., AND KOUSHANFAR, F. A Survey of Hardware Trojan Taxonomy and Detection. *IEEE Design Test of Computers 27*, 1 (Jan. 2010), 10–25.

[127] TRAN, C. Q., KAWAGUCHI, H., AND SAKURAI, T. Low-power high-speed level shifter design for block-level dynamic voltage scaling environment. In *2005 International Conference on Integrated Circuit Design and Technology, 2005. ICICDT 2005.* (May 2005), pp. 229–232.

[128] TSCHANZ, J. W., KAO, J. T., NARENDRA, S. G., NAIR, R., ANTONIADIS, D. A., CHANDRAKASAN, A. P., AND DE, V. Adaptive body bias for reducing impacts of die-to-die and within-die parameter variations on microprocessor frequency and leakage. *IEEE Journal of Solid-State Circuits 37*, 11 (Nov. 2002), 1396–1402.

[129] USAMI, K., IGARASHI, M., MINAMI, F., ISHIKAWA, T., KANZAWA, M., ICHIDA, M., AND NOGAMI, K. Automated low-power technique exploiting multiple supply voltages applied to a media processor. *IEEE Journal of Solid-State Circuits 33*, 3 (Mar. 1998), 463–472.

[130] VARGAS, F., AND NICOLAIDIS, M. Seu-tolerant sram design based on current monitoring. In *Proc. IEEE (FTCS'94)* (1994), pp. 106–115.

[131] VIERA, R. A. C., ET AL. Validation of single bbics architecture in detecting multiple faults. In *Digest of Papers, IEEE Asian Test Symposium (ATS'15)* (2015), pp. 1–6.

[132] WANG, A., AND CHANDRAKASAN, A. A 180-mV subthreshold FFT processor using a minimum energy design methodology. *IEEE Journal of Solid-State Circuits 40*, 1 (Jan. 2005), 310–319.

[133] WANG, H. B., ET AL. A novel built-in current sensor for n-well set detection. *Journal of Electronic Testing, Theory and Applications (JETTA) 31*, 4 (2015), 395–401.

[134] WANG, L., XIE, H., AND LUO, H. Malicious circuitry detection using transient power analysis for IC security. In *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)* (July 2013), pp. 1164–1167.

[135] WANG, W.-T., KER, M.-D., CHIANG, M.-C., AND CHEN, C.-H. Level shifters for high-speed 1 V to 3.3 V interfaces in a 0.13 mu;m Cu-interconnection/low-k CMOS technology. In *2001 International Symposium on VLSI Technology, Systems, and Applications. Proceedings of Technical Papers (Cat. No.01TH8517)* (2001), pp. 307–310.

[136] WANG, X., TEHRANIPOOR, M., AND PLUSQUELLIC, J. Detecting malicious inclusions in secure hardware: Challenges and solutions. In *HOST* (2008), pp. 15–19.

[137] WIRTH, AND ROGERS. The Transient Response of Transistors and Diodes to Ionizing Radiation. *IEEE Transactions on Nuclear Science 11*, 5 (Nov. 1964), 24–38.

[138] WIRTH, G. Bulk built in current sensors for single event transient detection in deep-submicron technologies. *Microelectronics Reliability 48*, 5 (2008), 710–715.

[139] WIRTH, G., AND FAYOMI, C. The bulk built in current sensor approach for single event transient detection. In *Proc. International Symposium on System-on-Chip (ISSOC'07)* (2007), pp. 1–4.

[140] WOOTERS, S. N., CALHOUN, B. H., AND BLALOCK, T. N. An Energy-Efficient Subthreshold Level Converter in 130-nm CMOS. *IEEE Transactions on Circuits and Systems II: Express Briefs 57*, 4 (Apr. 2010), 290–294.

[141] YU, C.-C., WANG, W.-P., AND LIU, B.-D. A new level converter for low-power applications. In *ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No.01CH37196)* (May 2001), vol. 1, pp. 113–116 vol. 1.

[142] ZAKARIA, H., AND FESQUET, L. Designing a process variability robust energy-efficient control for complex SOCs. *IEEE J. Emerg. Sel. Top. Circuits Syst (JETCAS)*, 1 (2011), 160 – 171.

[143] ZEIDLER, S., AND KRSTIĆ, M. A survey about testing asynchronous circuits. In *2015 European Conference on Circuit Theory and Design (ECCTD)* (Aug. 2015), pp. 1–4.

[144] ZHANG, X., AND TEHRANIPOOR, M. RON: An on-chip ring oscillator network for hardware Trojan detection. In *2011 Design, Automation Test in Europe* (Mar. 2011), pp. 1–6.

[145] ZHANG, Z., ET AL. A new bulk built-in current sensing circuit for single-event transient detection. In *Proc. Canadian Conference on Electrical and Computer Engineering (CCECE'10)* (2010), pp. 1–4.

[146] ZHANG, Z., ET AL. A bulk built-in voltage sensor to detect physical location of single-event transients. *Journal of Electronic Testing, Theory and Applications (JETTA) 29*, 2 (2013), 249–253.

[147] ZHAO, W., ALVAREZ, A. B., AND HA, Y. A 65-nm 25.1-ns 30.7-fJ Robust Subthreshold Level Shifter With Wide Conversion Range. *IEEE Transactions on Circuits and Systems II: Express Briefs 62*, 7 (July 2015), 671–675.

[148] ZHOU, J., WANG, C., LIU, X., ZHANG, X., AND JE, M. An Ultra-Low Voltage Level Shifter Using Revised Wilson Current Mirror for Fast and Energy-Efficient Wide-Range Voltage Conversion from Sub-Threshold to I/O Voltage. *IEEE Transactions on Circuits and Systems I: Regular Papers 62*, 3 (Mar. 2015), 697–706.

Part II

Curriculum vitae

Chapter 1

Identification et parcours professionnel

M. **POSSAMAI BASTOS** Rodrigo, 37 ans (22/04/1980).
Maître de Conférences à l'Université Grenoble Alpes (UGA) depuis **septembre 2012**.
Chercheur au laboratoire CNRS TIMA.
Enseignant au DLST, UFR IM2AG et PhiTEM.
Prime d'encadrement doctoral et de recherche (**PEDR**) de 2016 à 2020.
Publications : **11 revues internationales et 37 conférences internationales**.

Sep. 2011 – Août 2012 :
Attaché Temporaire d'Enseignement et de Recherche (**ATER**) :
Laboratoire CNRS LIRMM (Montpellier, France) et Université Montpellier 2 (UM2).

Sep. 2010 – Dec. 2011 :
Postdoctorat en Sécurité des Circuits Intégrés :
Laboratoire CNRS LIRMM (Montpellier, France).

Sep. 2006 – Août 2010 :
Doctorat en Micro et Nano Électronique « Ph.D. in Nano and Microelectronics » :
Équivalent bac + 11 en France.
Thèse soutenu le 9 juillet 2010 en Cotutelle Internationale :
Laboratoire TIMA, Grenoble INP (France) et
Institut d'Informatique, Univ. Fédérale du Rio Grande do Sul (UFRGS, Porto Alegre, Brésil).

Nov. 2004 – Août 2006 :
Master en Génie Informatique « M.Sc. in Computer Science » :
Équivalent bac + 7 en France.
Institut d'Informatique, Univ. Fédérale du Rio Grande do Sul (UFRGS, Porto Alegre, Brésil).

Nov. 2002 – Oct. 2004 :
Ingénieur de Recherche et Développement de Syst. Embarqués pour la Télécommunication :
DataCom Telemática à Porto Alegre (Brésil).

Mars 1998 – Oct. 2002 :
Diplôme d'Ingénieur en Électronique « Electrical Engineer's Degree » :
Équivalent bac + 5 en France.
École d'Ingénieurs, Univ. Fédérale du Rio Grande do Sul (UFRGS, Porto Alegre, Brésil) :
Équivalente à une grande école en France.
Moy. Harm. (Index I3 UFRGS) = 9,0 / 10.

NOTE : particularités de l'enseignement supérieur et de la recherche au Brésil :

Bac + 11 : par défaut, le doctorat au Brésil s'est fait en 4 ans dont la troisième année est constituée de la rédaction d'un manuscrit préalable de thèse et une pré-soutenance devant un jury d'experts. Pour soutenir la thèse à la fin de la quatrième année, le candidat doit avoir au moins une publication ou acceptation d'article en revue internationale. Le candidat ayant soutenu sa thèse atteint un niveau équivalent bac + 11 en France ;

Bac + 7 : différemment des masters en France, les programmes de master au Brésil n'admettent que les étudiants ayant un diplôme de niveau équivalent bac + 5 en France. Par ailleurs, le master s'est fait en 2 ans, et pour qu'un étudiant soutienne son travail, au moins une publication en conférence internationale est normalement requis. A la fin du master, un étudiant atteint ainsi un niveau équivalent bac + 7 en France ;

Bac + 5 : les grandes écoles d'ingénieurs appartient aux universités et délivrent des diplômes aux étudiants ayant réussi 5 ans d'études supérieurs, c'est l'équivalent au niveau bac + 5 en France. Pour entrer dans une grande école, les candidats doivent passer des examens écrits dans le cadre des concours publiques ayant un nombre assez limité de places. Les grandes écoles des universités fédérales (publiques) attirent les meilleurs étudiants car elles sont gratuites et ont généralement les enseignants-chercheurs les plus qualifiés.

Chapter 2

Publications et production scientifique

2.1 Travaux soutenus devant un jury

(4) POSSAMAI BASTOS, R. P. Transient-Fault Robust Systems Exploiting Quasi-Delay Insensitive Asynchronous Circuits. July 2010. 142 p. Thesis (Ph.D.) – EDEEATS, TIMA, INP, Grenoble & PGMicro, Instituto de Informática, UFRGS, Porto Alegre.

(3) POSSAMAI BASTOS, R. P. Circuitos Assíncronos QDI: Uma Alternativa Naturalmente Robusta a Desafios das Tecnologias Submicrônicas. November 2009. 98 p. Thesis Proposal (Ph.D.) – PGMicro, Instituto de Informática, UFRGS, Porto Alegre.

(2) POSSAMAI BASTOS, R. P. Design of a Soft-Error Robust Microprocessor. August 2006. 120 p. Thesis (Master) – PPGC, Instituto de Informática, UFRGS, Porto Alegre.

(1) POSSAMAI BASTOS, R. P. Sistemas Embarcados de Equipamentos de Telecomunicação. September 2002. 40 p. Report (Supervised Training in DataCom Telemática) – Departamento de Engenharia Elétrica, UFRGS, Porto Alegre.

2.2 Articles dans des revues d'audience internationale

(11) POSSAMAI BASTOS, R. P.; GUIMARÃES, L. A.; TORRES, F. S.; FESQUET, L.; Architectures of Bulk Built-In Current Sensors for Detection of Transient Faults in Integrated Circuits. Elsevier Microelectronics Journal, 2017.

(10) ROCHA, R. O.; TORRES, F. S.; POSSAMAI BASTOS, R. P.; Towards high-sensitive built-in current sensors enabling detection of radiation-induced soft errors. Elsevier Microelectronics Reliability Journal, 2017.

(9) VIERA, R. A. C.; POSSAMAI BASTOS, R. P.; DUTERTRE, J. M.; MAURINE, P.; JADUE, R. I.; Method for evaluation of transient-fault detection techniques. Elsevier Microelectronics Reliability Journal, 2017.

(8) ROLLOFF, O.A.; POSSAMAI BASTOS, R. P.; FESQUET, L.; Exploiting Reliable Features of Asynchronous Circuits for Designing Low-Voltage Components in FD-SOI Technology. Elsevier Microelectronics Reliability Journal, 2015.

(7) DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; POTIN, O.; FLOTTES, M.L.; ROUZEYRE, B.; DI NATALE, G.; SARAFIANOS, A.; Improving the ability of Bulk Built-In Current Sen-

sors to detect SEEs by using triple-well CMOS. Elsevier Microelectronics Reliability Journal, 2014.

(6) DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; POTIN, O.; FLOTTES, M.L.; ROUZEYRE, B.; DI NATALE, G. Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection. Elsevier Microelectronics Reliability Journal, 2013.

(5) TORRES, F. S.; POSSAMAI BASTOS, R. P. Detection of Transient Faults in Nanometer Technologies by using Modular Built-In Current Sensors. SBC Journal of Integrated Circuits and Systems, JICS, 2013. This work is an **extended version of an IEEE/ACM SBCCI 2012's paper thanks to a best paper award nominee**.

(4) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; LU, F.; ROUZEYRE, B. A New Recovery Scheme against Short-to-Long Duration Transient Faults in Combinational Logic. Springer Journal of Electronic Testing: Theory and Applications, JETTA, 2013.

(3) POSSAMAI BASTOS, R. P.; TORRES, F. S.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode. Elsevier Microelectronics Reliability Journal, 2012.

(2) POSSAMAI BASTOS, R. P.; SICARD, G.; KASTENSMIDT, F. L.; RENAUDIN, M.; REIS, R. Asynchronous Circuits as Alternative for Mitigation of Long-Duration Transient Faults in Deep-Submicron Technologies. Elsevier Microelectronics Reliability Journal, 2010-c.

(1) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F.; REIS, R. Design of a Soft-Error Robust Microprocessor. Elsevier Microelectronics Journal, 2008.

2.3 Conférences internationales avec comité de lecture et actes

(37) JADUE, A. R. I; POSSAMAI BASTOS, R. P.; LEITE, T. F. P.; ROLLOF, O. A.; MAMADOU, D.; FESQUET, L. Level Shifter Architecture for Dynamically Biasing Ultra-Low Voltage Subcircuits of Integrated Systems. In: IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS, ISCAS, 2018, Florence, Italy... Proceedings.. [S.l.:s.n], 2018.

(36) GUIMARÃES, L. A.; LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; FESQUET, L.; Non-Intrusive Testing Technique for Detection of Trojans in Asynchronous Circuits. In: IEEE DESIGN, AUTOMATION, AND TEST IN EUROPE, DATE, 2018, Dresden, Germany... Proceedings.. [S.l.:s.n], 2018.

(35) VIERA, R. A. C.; DUTERTRE, J.M.; MAURINE, P.; POSSAMAI BASTOS, R. P.; Standard CAD tool-based method for simulation of laser-induced faults in large-scale circuits. In: ACM INTERNATIONAL SYMPOSIUM ON PHYSICAL DESIGN, ISPD, 2018, Monterey, USA... Proceedings.. [S.l.:s.n], 2018.

(34) GUIMARÃES, L. A.; POSSAMAI BASTOS, R. P.; FESQUET, L. Detection of Layout-Level Trojans by Monitoring Substrate with Preexisting Built-in Sensors. In: IEEE SYMPOSIUM ON VLSI, ISVLSI, 2017, Bochum, Germany... Proceedings.. [S.l.:s.n], 2017.

(33) VIERA, R. A. C.; DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; MAURINE, P.; Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation. In: EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, DSD, 2017. Proceedings...

[S.l.]: IEEE, 2017.

(32) VIERA, R. A. C.; MAURINE, P.; DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; Importance of IR Drops on the Modeling of Laser-Induced Transient Faults. In: INTERNATIONAL CONFERENCE ON SYNTHESIS, MODELING, ANALYSIS AND SIMULATION METHODS, AND APPLICATIONS TO CIRCUIT DESIGN, SMACD, 2017. Proceedings... [S.l.]: IEEE, 2017. **Best paper award nominee in the conference**.

(31) SIMATIC, J.; CHERKAOUI, A.; POSSAMAI BASTOS, R. P.; FESQUET, L. A practical framework for specification, verification, and design of self-timed pipelines. In: INTERNATIONAL SYMPOSIUM ON ASYNCHRONOUS CIRCUITS AND SYSTEMS, ASYNC, 2017. Proceedings... [S.l.]: IEEE, 2017.

(30) SIMATIC, J.; CHERKAOUI, A.; POSSAMAI BASTOS, R. P.; FESQUET, L. New Asynchronous Protocols for Enhancing Area and Throughput in Bundled-Data Pipelines. In: SYMPOSIUM ON INTEGRATED CIRCUITS AND SYSTEMS DESIGN, SBCCI, 2016. Proceedings... [S.l.]: IEEE/ACM, 2016. **Runner-up best paper award in the conference**.

(29) LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; IGA, R.; FESQUET, L. Comparison of Low-Voltage Scaling in Synchronous and Asynchronous FD-SOI Circuits. In: INTERNATIONAL WORKSHOP ON POWER AND TIMING MODELING, OPTIMIZATION AND SIMULATION, PATMOS, 2016. Proceedings... [S.l.]: IEEE, 2016.

(28) SIMATIC, J.; POSSAMAI BASTOS, R. P.; FESQUET, L. High-Level Synthesis for Event-Based Systems. In: INTERNATIONAL CONFERENCE ON EVENT-BASED CONTROL, COMMUNICATION AND SIGNAL PROCESSING, EBCCSP, 2016. Proceedings... [S.l.]: IEEE, 2016.

(27) GUIMARÃES, L. A.; POSSAMAI BASTOS, R. P.; LEITE, T. F. P.; FESQUET, L. Simple Tri-State Logic Trojans Able to Upset Properties of Ring Oscillators. In: INTERNATIONAL CONFERENCE ON DESIGN & TECHNOLOGY OF INTEGRATED SYSTEMS IN NANOSCALE ERA, DTIS, 2016. Proceedings... [S.l.]: IEEE, 2016.

(26) MELO, J. G. M.; TORRES, F. S.; POSSAMAI BASTOS, R. P. Exploration of Noise Robustness and Sensitivity of Bulk Current Sensors for Soft Error Detection. In: EUROPEAN WORKSHOP ON CMOS VARIABILITY, VARI, 2015. Proceedings... [S.l.]: IEEE, 2015.

(25) POSSAMAI BASTOS, R. P.; DUTERTRE, J.M.; TORRES, F. S. Comparison of Bulk Built-In Current Sensors in terms of Transient-Fault Detection Sensitivity. In: EUROPEAN WORKSHOP ON CMOS VARIABILITY, VARI, 2014. Proceedings... [S.l.]: IEEE, 2014.

(24) POSSAMAI BASTOS, R. P.; TORRES, F. S.; DUTERTRE, J.M.; FLOTTES, M.L.; DI NATALE, G.; ROUZEYRE, B. A Single Built-in Sensor to Check Pull-up and Pull-down CMOS Networks against Transient Faults. In: INTERNATIONAL WORKSHOP ON POWER AND TIMING MODELING, OPTIMIZATION AND SIMULATION, PATMOS, 2013. Proceedings... [S.l.]: IEEE, 2013.

(23) POSSAMAI BASTOS, R. P.; TORRES, F. S.; DUTERTRE, J.M.; FLOTTES, M.L.; DI NATALE, G.; ROUZEYRE, B. A Bulk Built-in Sensor for Detection of Fault Attacks. In: IEEE International Symposium on Hardware Oriented Security and Trust, HOST, 2013. Proceedings... [S.l.]: IEEE, 2013.

(22) TORRES, F. S.; POSSAMAI BASTOS, R. P. Robust Modular Bulk Built-In Current Sensors for Detection of Transient Faults. In: SYMPOSIUM ON INTEGRATED CIRCUITS AND

SYSTEMS DESIGN, SBCCI, 2012. Proceedings... [S.l.]: IEEE/ACM, 2012. **Best paper award nominee in the conference**.

(21) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. A New Bulk Built-in Current Sensor-Based Strategy for Dealing with Long-Duration Transient Faults in Deep-Submicron Technologies. In: IEEE INTERNATIONAL SYMPOSIUM ON DEFECT AND FAULT TOLERANCE IN VLSI AND NANOTECHNOLOGY SYSTEMS, DFT, 26., 2011, Vancouver, Canada. Proceedings... [S.l.]: IEEE, 2011. p. 302-308.

(20) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. How to Register Transient Error Signals of Concurrent Error Detection Schemes?. In: CONFERENCE ON RADIATION EFFECTS ON COMPONENTS AND SYSTEMS, RADECS, 2011, Seville, Spain. Proceedings... [S.l.]: IEEE, 2011.

(19) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. Timing Issues for an Efficient Use of Concurrent Error Detection Codes. In: LATIN AMERICAN TEST WORKSHOP, LATW, 12., 2011, Porto de Galinhas, Brazil. Proceedings... [S.l.]: IEEE, 2011-a. p. 1-6.

(18) POSSAMAI BASTOS, R. P.; SICARD, G.; KASTENSMIDT, F.; RENAUDIN, M.; REIS, R. Evaluating Transient-Fault Effects on Traditional C-element‘s Implementations. In: INTERNATIONAL ON-LINE TESTING SYMPOSIUM, IOLTS, 16., 2010, Corfu Island, Greece. Proceedings... [S.l.]: IEEE Computer Society, 2010-b. p. 35-40.

(17) POSSAMAI BASTOS, R. P.; MONNET, Y.; SICARD, G.; KASTENSMIDT, F.; RENAUDIN, M.; REIS, R. Comparing Transient-Fault Effects on Asynchronous and on Synchronous Circuits. In: INTERNATIONAL ON-LINE TESTING SYMPOSIUM, IOLTS, 15., 2009, Sesimbra-Lisbon, Portugal. Proceedings... [S.l.]: IEEE, 2009-b. p. 29-34.

(16) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Design at High Level of a Robust 8-Bit Microprocessor to Soft Errors by Using Only Standard Gates. In: SYMPOSIUM ON INTEGRATED CIRCUITS AND SYSTEMS DESIGN, SBCCI, 19., 2006, Ouro Preto, Brazil. Proceedings... [S.l.]: ACM, 2006-d. p. 196-201.

(15) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Design of a Robust 8-Bit Microprocessor to Soft Errors. In: INTERNATIONAL ON-LINE TESTING SYMPOSIUM, IOLTS, 12., 2006, Lake of Como, Italy. Proceedings... [S.l.]: IEEE Computer Society, 2006-c. p. 195-196.

(14) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Designing Low Power Embedded Software for Mass-Produced Microprocessor by Using a Loop Table in On-Chip Memory. In: INTERNATIONAL WORKSHOP ON POWER AND TIMING MODELING, OPTIMIZATION AND SIMULATION, PATMOS, 15., 2005, Leuven, Belgium. Proceedings... Berlin, Germany: Springer, 2005-b. p. 59-68. (Lecture Notes in Computer Science, LNCS, v. 3728).

2.4 Conférences internationales avec comité de lecture

(13) VIERA, R. A. C.; POSSAMAI BASTOS, R. P.; DUTERTRE, J. M.; MAURINE, P.; JADUE, R. I.; Method for evaluation of transient-fault detection techniques. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND

ANALYSIS, ESREF, 2017.

(12) GUIMARÃES, L. A.; POSSAMAI BASTOS, R. P.; FESQUET, L. Detection of Layout-Level Trojans by Injecting Current into Substrate and Digitally Monitoring Built-In Sensors. In: DESIGN AUTOMATION CONFERENCE, DAC, 2017, Austin, USA. Work-In-Progress Poster Session... [S.l.:s.n], 2017.

(11) SIMATIC, J.; POSSAMAI BASTOS, R. P.; FESQUET, L. Desynchonization Tool for High-Level Synthesis of Asynchronous Circuits. UNIVERSITY BOOTH at DESIGN, AUTOMATION, AND TEST IN EUROPE, DATE, 2016. Digest of Papers... [S.l.] : IEEE, 2016.

(10) VIERA, R. A. C.; POSSAMAI BASTOS, R. P.; DUTERTRE, J.M.; POTIN, O.; FLOTTES, M.L.; DI NATALE, G.; ROUZEYRE, B. Validation of Single BBICS Architecture in Detecting Multiple Faults. In: IEEE Asian Test Symposium, ATS, 2015. Digest of Papers... [S.l.]: IEEE, 2015.

(9) ROLLOFF, O.A.; POSSAMAI BASTOS, R. P.; FESQUET, L.; Exploiting Reliable Features of Asynchronous Circuits for Designing Low-Voltage Components in FD-SOI Technology. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND ANALYSIS, ESREF, 2015.

(8) DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; POTIN, O.; FLOTTES, M.L.; ROUZEYRE, B.; DI NATALE, G. Design of Bulk Built-In Current Sensors to Detect Single Event Effects and Laser-Induced Fault Injection Attempts. In: OPEN FORUM ON TRUSTWORTHY MANUFACTURING AND UTILIZATION OF SECURE DEVICES, TRUDEVICE, 2014.

(7) DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; POTIN, O.; FLOTTES, M.L.; ROUZEYRE, B.; DI NATALE, G.; SARAFIANOS, A.; Improving the ability of Bulk Built-In Current Sensors to detect SEEs by using triple-well CMOS. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND ANALYSIS, ESREF, 2014.

(6) DUTERTRE, J.M.; POSSAMAI BASTOS, R. P.; POTIN, O.; FLOTTES, M.L.; ROUZEYRE, B.; DI NATALE, G. Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND ANALYSIS, ESREF, 2013.

(5) POSSAMAI BASTOS, R. P.; TORRES, F. S.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND ANALYSIS, ESREF, 2012.

(4) POSSAMAI BASTOS, R. P.; SICARD, G.; KASTENSMIDT, F. L.; RENAUDIN, M.; REIS, R. Asynchronous Circuits as Alternative for Mitigation of Long-Duration Transient Faults in Deep-Submicron Technologies. In: EUROPEAN SYMPOSIUM ON RELIABILITY OF ELECTRON DEVICES, FAILURE PHYSICS AND ANALYSIS, ESREF, 2010-c.

(3) POSSAMAI BASTOS, R. P.; SICARD, G.; KASTENSMIDT, F. L.; RENAUDIN, M.; REIS, R. Asynchronous Circuits as Alternative for Mitigation of Long-Duration Transient Faults in Deep-Submicron Technologies. In: EUROPEAN TEST SYMPOSIUM, ETS, 15., 2010, Prague, Czech Republic. Digest of Papers... [S.l.]: IEEE Computer Society, 2010-a.

(2) POSSAMAI BASTOS, R. P.; MONNET, Y.; SICARD, G.; KASTENSMIDT, F. L.; RENAUDIN, M.; REIS, R. A Methodology to Evaluate Transient-Fault Effects on Asynchronous and Synchronous Circuits. In: EUROPEAN TEST SYMPOSIUM, ETS, 14., 2009, Seville,

Spain. Digest of Papers... [S.l.] : IEEE Computer Society, 2009-a.

(1) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Design of a Robust 8-Bit Microprocessor to Soft Single Event Effects. In: LATIN AMERICAN TEST WORKSHOP, LATW, 7., 2006, Buenos Aires, Argentina. Digest of Papers... [S.l.]: IEEE Computer Society, 2006-a. p. 137-142.

2.5 Colloques nationaux

(9) ROLLOFF, O.A.; JADUE, A. R. I; LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; FESQUET, L. Body Bias Control Cells based on Negative- and Positive-Level Shifter Architectures in Technology FD-SOI 28 nm. In: JOURNEES NATIONALES DU RESEAU DOCTORAL EN MICRO-NANOELECTRONIQUE, JNRDM, 20., 2017, Strasbourg, France. Digest of Papers... [S.l.:s.n], 2017.

(8) ROLLOFF, O.A.; LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; FESQUET, L. Analysis of granularity for automatic biasing control in FDSOI technology with low-voltage supply. In: JOURNEES NATIONALES DU RESEAU DOCTORAL EN MICRO-NANOELECTRONIQUE, JNRDM, 19., 2016, Toulouse, France. Digest of Papers... [S.l.:s.n], 2016.

(7) LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; FESQUET, L. Low-Power Asynchronous Arithmetic Logic Unit in Technology FD-SOI 28 nm. In: JOURNEES NATIONALES DU RESEAU DOCTORAL EN MICRO NANOELECTRONIQUE, JNRDM, 19., 2016, Toulouse, France. Digest of Papers... [S.l.:s.n], 2016.

(6) GUIMARÃES, L. A.; POSSAMAI BASTOS, R. P.; FESQUET, L. A New Proposition on Hardware Trojan Activation. In: JOURNEES NATIONALES DU RESEAU DOCTORAL EN MICRO-NANOELECTRONIQUE, JNRDM, 18., 2015, Bordeaux, France. Digest of Papers... [S.l.:s.n], 2015.

(5) SIMATIC, J.; POSSAMAI BASTOS, R. P.; FESQUET, L. Flot de conception pour l'ultra-faible consommation : échantillonnage non-uniforme et électronique asynchrone. In: JOURNEES NATIONALES DU RESEAU DOCTORAL EN MICRO-NANOELECTRONIQUE, JNRDM, 18., 2015, Bordeaux, France. Digest of Papers... [S.l.:s.n], 2015.

(4) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. Calibrating Bulk Built-in Current Sensors for Detecting Transient Faults. In: COLOQUE DU GROUPEMENT DE RECHERCHE SYSTEM-ON-CHIP ET SYSTEM-IN-PACKAGE, GDR-SOC-SIC, 2012, Paris, France. Digest of Papers... [S.l.:s.n], 2012.

(3) POSSAMAI BASTOS, R. P.; DI NATALE, G.; FLOTTES, M.L.; ROUZEYRE, B. Timing Issues of Transient Faults in Concurrent Error Detection Schemes. In: COLOQUE DU GROUPEMENT DE RECHERCHE SYSTEM-ON-CHIP ET SYSTEM-IN-PACKAGE, GDR-SOC-SIC, 2011, Lyon, France. Digest of Papers... [S.l.:s.n], 2011.

(2) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Design of a Robust 8-Bit Microprocessor to Soft Single Event Effects. In: SOUTH SYMPOSIUM ON MICROELECTRONICS, SIM, 21., May 8, 2006, Porto Alegre, RS, Brazil. Proceedings... Porto Alegre, RS, Brazil: Universidade de Federal do Rio Grande do Sul, UFRGS, 2006-b. p. 151-155.

(1) POSSAMAI BASTOS, R. P.; KASTENSMIDT, F. L.; REIS, R. Designing Low Power Em-

bedded Software for Mass-Produced Microprocessor by Using a Loop Table in On-Chip Memory. In: SOUTH SYMPOSIUM ON MICROELECTRONICS, SIM, 20., May 6-7, 2005, Santa Cruz do Sul, RS, Brazil. Proceedings... Porto Alegre, RS, Brazil: Universidade de Santa Cruz do Sul, UNISC, 2005-a. p. 137-140.

2.6 Colloques régionaux

(5) CENTENO, P. C. ; POSSAMAI BASTOS, R. P. ; REIS, R. . Simulação de Circuitos Assíncronos QDI no Nível de Transistores sob o Efeito de Injeção de Falhas. In: SALÃO DE INICIAÇÃO CIENTÍFICA, SIC, 18., 2007, Porto Alegre, RS. Livro de Resumos.... Porto Alegre, RS : Universidade Federal do Rio Grande do Sul, UFRGS: Resumo, 2007.

(4) MANITO, R. ; POSSAMAI BASTOS, R. P. ; REIS, R. . Simulação de Circuitos Robustos através de Injeção de Falhas no Nível de Portas Lógicas.. In: SALÃO DE INICIAÇÃO CIENTÍFICA, SIC, 17, 2006, Porto Alegre, RS. Livro de Resumos.... Porto Alegre, RS : Universidade Federal do Rio Grande do Sul, UFRGS: Resumo, 2006.

(3) PIAZZA, A. ; POSSAMAI BASTOS, R. P. ; PALUDO, L. H. ; LOUREIRO, L. T. R. . Acionamento Microcontrolado de Motor de Passo Através de Sinais Infravermelho Padrão RC5. In: SALÃO DE INICIAÇÃO CIENTÍFICA, SIC, 13., 2001, Porto Alegre, RS. Livro de Resumos.... Porto Alegre, RS : Universidade Federal do Rio Grande do Sul, UFRGS: Resumo 002, 2001. p. 649.

(2) POSSAMAI BASTOS, R. P. ; SUSIN, A. A. . Sistema Microprocessado de Medição de Vibração para Aquisição em Tempo Real. In: SALÃO DE INICIAÇÃO CIENTÍFICA, SIC, 13., 2001, Porto Alegre, RS. Livro de Resumos.... Porto Alegre, RS : Universidade Federal do Rio Grande do Sul, UFRGS: Resumo 191, 2001. p. 223.

(1) POSSAMAI BASTOS, R. P. ; NEGREIROS, M. ; SUSIN, A. A. ; PARDI JUNIOR, W. ; MARCAL, R. F. M. Sistema de Medição de Vibração com Acelerômetro de Estado Sólido.. In: SALÃO DE INICIAÇÃO CIENTÍFICA, SIC, 12., 2000, Porto Alegre, RS. Livro de Resumos.... Porto Alegre, RS : Universidade Federal do Rio Grande do Sul, UFRGS: Resumo 011, 2000. p. 539.

Chapter 3

Encadrements scientifiques

3.1 Thèses de doctorat (soutenances en début décembre 2017)

(2) **Jean Simatic** :
Titre de la thèse : Flot de Conception pour l'Ultra-Faible Consommation : Échantillonnage Non-Uniforme et Électronique Asynchrone.
Université : UGA et Grenoble INP.
École Doctorale : Electronique, Electrotechnique, Automatique et Traitement du Signal (EEATS).
Spécialité : Nano Electronique et Nano Technologies (NENT).
Début : 01/12/2014.
Soutenance : 07/12/2017.
Direction : Laurent Fesquet (70 %).
Co-encadrement : Rodrigo Possamai Bastos (30 %).
Conférences internationales : ASYNC 2017, SBCCI 2016, EBCCSP 2016 et DATE 2016.
Distinction : Runner-up best paper award in SBCCI 2016.

(1) **Leonel Acunha Guimarães** :
Titre de la thèse : Testing Techniques for Detection of Hardware Trojans in Integrated Circuits of Trusted Systems.
Université : UGA et Grenoble INP.
École Doctorale : Electronique, Electrotechnique, Automatique et Traitement du Signal (EEATS).
Spécialité : Nano Electronique et Nano Technologies (NENT).
Début : 01/10/2014.
Soutenance : 01/12/2017.
Direction : Laurent Fesquet (30 %).
Co-encadrement : Rodrigo Possamai Bastos (70 %).
Conférences internationales : DATE 2018, ISVLSI 2017, DAC 2017 et DTIS 2016.
Revue internationale : MEJ 2017.

3.2 Thèses de doctorat en cours

(4) **Ricardo Aquino Guazzelli** :
Titre de la thèse : Test of Asynchronous Circuits for Security Systems in Advanced Technologies.

Université : UGA et Grenoble INP.
École Doctorale : Electronique, Electrotechnique, Automatique et Traitement du Signal (EEATS).
Spécialité : Nano Electronique et Nano Technologies (NENT).
Début : 03/10/2017.
Soutenance prévue : 30/09/2020.
Direction : Laurent Fesquet (50 %).
Co-direction : Rodrigo Possamai Bastos (50 %)

(3) **Raphael Andreoni Camponogara Viera** :
Titre de la thèse : Evaluating the efficiency of New Transient-Fault Detection Techniques for Integrated Circuits under Laser-Induced Fault Sources.
Université : Université Montpellier 2.
École Doctorale : Information, Structures, Systèmes (I2S).
Spécialité : Systèmes Automatiques et Microélectroniques (SyAM).
Début : 01/10/2015.
Soutenance prévue : 30/09/2018.
Direction : Philippe Maurine (33.3 %).
Co-encadrement : Rodrigo Possamai Bastos (33.3 %), Jean-Max Dutertre (33.3 %).
Conférences internationales : ISPD 2018, ESREF 2017, DSD 2017, SMACD 2017 et ATS 2015.
Revue internationale : MER 2017.
Distinction : Best paper award nominee in SMACD 2017.

(2) **Thiago Ferreira de Paiva Leite** :
Titre de la thèse : Méthodes et Flot de Conception pour l'Intégration de Logique Asynchrone avec les Technologies FD-SOI.
Université : UGA et Grenoble INP.
École Doctorale : Electronique, Electrotechnique, Automatique et Traitement du Signal (EEATS).
Spécialité : Nano Electronique et Nano Technologies (NENT).
Début : 01/11/2015.
Soutenance prévue : 31/10/2018.
Direction : Laurent Fesquet (40 %).
Co-encadrement : Rodrigo Possamai Bastos (60 %).
Conférences internationales : ISCAS 2018, DATE 2018, PATMOS 2016 et DTIS 2016.

(1) **Otto Aureliano Rolloff** :
Titre de la thèse : Cellules et Structures de Contrôle pour la Gestion de Performances des Circuits Asynchrones dans les Technologies FD-SOI.
Université : UGA et Grenoble INP.
École Doctorale : Electronique, Electrotechnique, Automatique et Traitement du Signal (EEATS).
Spécialité : Nano Electronique et Nano Technologies (NENT).
Début : 01/02/2015.
Soutenance prévue : 31/10/2018.
Direction : Laurent Fesquet (50 %).
Co-encadrement : Rodrigo Possamai Bastos (50 %).
Conférence internationale : ISCAS 2018 et ESREF 2015.
Revue internationale : MER 2015.

3.3 Stages de fin d'études en niveau master 2 ou 3ème année d'écoles d'ingénieurs

(5) **Matheus Garay Trindade** :
Titre du travail : Qualification of Supervised Learning Models under Radiation-Induced Effects.
Début : septembre 2017.
Fin : juillet 2018.
Encadrement : Rodrigo Possamai Bastos (100 %).

(4) **Raphael Andreoni Camponogara Viera** :
Titre du travail : Evaluation of New FD-SOI Standard Cells under the Effects of Malicious Laser-Induced Transient Faults.
Début : avril 2015.
Fin : juillet 2015.
Encadrement : Rodrigo Possamai Bastos (100 %).

(3) **Thiago Ferreira de Paiva Leite** :
Titre du travail : Design of New Digital Signal Processing Subsystems by using FD-SOI technology and Asynchronous Features.
Début : avril 2015.
Fin : juillet 2015.
Encadrement : Rodrigo Possamai Bastos (100 %).

(2) **Otto Aureliano Rolloff** :
Titre du travail : Design and Evaluation of Standard Cells for Asynchronous Integrated Circuits in Low Power Nanotechnology.
Début : février 2014.
Fin : octobre 2014.
Encadrement : Rodrigo Possamai Bastos (100 %).

(1) **Ahmad Al Youssef** :
Titre du travail : Évaluation de l'Efficacité de Techniques de Détection des Fautes Transitoires.
Début : février 2013.
Fin : juin 2013.
Encadrement : Rodrigo Possamai Bastos (100 %).

Chapter 4

Diffusion des travaux (rayonnement et vulgarisation)

4.1 Distinctions

(4) Prime d'Encadrement Doctoral et de Recherche (PEDR) de 01/10/2016 au 30/09/2020.

(3) Best paper award nominee in IEEE SMACD 2017. Importance of IR Drops on the Modeling of Laser-Induced Transient Faults. VIERA, R. A. C.; MAURINE, P.; DUTERTRE, J.M.; and POSSAMAI BASTOS, R. P.

(2) Runner-up best paper award in IEEE/ACM SBCCI 2016. New Asynchronous Protocols for Enhancing Area and Throughput in Bundled-Data Pipelines. SIMATIC, J.; CHERKAOUI, A.; POSSAMAI BASTOS, R. P.; and FESQUET, L.

(1) Best paper award nominee in IEEE/ACM SBCCI 2012. Robust Modular Bulk Built-In Current Sensors for Detection of Transient Faults. TORRES, F. S.; and POSSAMAI BASTOS, R. P.

4.2 Membre de jury en soutenances de doctorat, master et travail de fin d'études

(13) 2018 : TELECOM ParisTech : rapporteur de la thèse de doctorat de Benjamin COËFFIC : Flot Expérimental d'Injection de Fautes Statistiques pour la Certification de Circuits Orientés Sécurité et Applications Critiques.

(12) 2018 : UGA : examinateur en jury de master 2 MIAGE.

(11) 2018 : UGA : examinateur en jury de master 2 MISTRE.

(10) 2017 : UGA : examinateur en jury de master 2 MIAGE.

(9) 2017 : UGA : examinateur en jury de master 2 MISTRE.

(8) 2016 : UGA : examinateur en jury de master 2 MIAGE.

(7) 2016 : UGA : examinateur en jury de master 2 NENT.

(6) 2015 : UGA : examinateur en jury de master 2 MIAGE.

(5) 2014 : UFRGS : examinateur en jury de travail de fin d'études en école d'ingénieurs.

(4) 2014 : TELECOM Bretagne : examinateur en jury de travail de fin d'études.

(3) 2014 : UGA : examinateur en jury de master 2 MIAGE.

(2) 2013 : UGA : examinateur en jury de master 2 MIAGE.

(1) 2013 : UGA : examinateur en jury de master 2 NENT.

4.3 Implication en comités de conférences

(15) Chair of technical track in the international conference IEEE/ACM SBCCI 2018:
31st International Symposium on Integrated Circuits and Systems Design (Bento Gonçalves).

(14) Program committee member of the international conference IEEE/ACM SBCCI 2018:
31st International Symposium on Integrated Circuits and Systems Design (Bento Gonçalves).

(13) Program committee member of the international conference IEEE LATS 2018:
19th Latin-American Test Symposium (São Paulo).

(12) Program committee member of the international conference IEEE LASCAS 2018:
9th Latin-American Symposium on Circuits and Systems (Puerto Vallarta).

(11) Chair of technical track in the international conference IEEE/ACM SBCCI 2017:
30th International Symposium on Integrated Circuits and Systems Design (Fortaleza).

(10) Program committee member of the international conference IEEE/ACM SBCCI 2017:
30th International Symposium on Integrated Circuits and Systems Design (Fortaleza).

(9) Program committee member of the international conference IEEE ICCDCS 2017:
10th International Caribbean Conference on Devices, Circuits, and Systems (Cozumel).

(8) Chair of technical track in the international conference IEEE/ACM SBCCI 2016:
29th International Symposium on Integrated Circuits and Systems Design (Belo Horizonte).

(7) Program committee member of the international conference IEEE/ACM SBCCI 2016:
29th International Symposium on Integrated Circuits and Systems Design (Belo Horizonte).

(6) Section chair in the international conference IEEE NEWCAS 2015:
13th International NEW Circuits And Systems (Grenoble).

(5) Publicity chair in the international conference IEEE NEWCAS 2015:
13th International NEW Circuits And Systems (Grenoble).

(4) Program committee member of the national conference SIM 2013:
28th South Symposium on Microelectronics (Porto Alegre).

(3) Program committee member of the national conference SIM 2007:
22nd South Symposium on Microelectronics (Porto Alegre).

(2) Program committee member of the national conference SIM 2006:
21st South Symposium on Microelectronics (Porto Alegre).

(1) Program committee member of the national conference SIM 2005:
20th South Symposium on Microelectronics (Santa Cruz).

4.4 Rapporteur d'articles de revues et conférences

(16) Elsevier Computers and Electrical Engineering Journal (COMPELECENG 2018)

(15) Elsevier Microprocessors and Microsystems Journal (MICRO 2018)

(14) Elsevier Microelectronics Reliability Journal (MER 2018)

(13) Elsevier Microprocessors and Microsystems Journal (MICRO 2017)

(12) Elsevier Microelectronics Reliability Journal (MER 2016)

(11) IEEE International Conference on Electronics, Circuits and Systems (ICECS 2016)

(10) IEEE International Conference on Electronics, Circuits and Systems (ICECS 2016)

(9) IEEE International Symposium on Circuits and Systems (ISCAS 2016)

(8) IEEE International Computer Society Annual Symposium on VLSI (ISVLSI 2015)

(7) Elsevier Microelectronics Reliability Journal (MER 2015)

(6) ASP Journal of Low Power Electronics (JOLPE 2013)

(5) IEEE Southeastern Symposium on System Theory (SSST 2012)

(4) IEEE European Test Symposium (ETS 2012)

(3) Springer Journal of Analog Integrated Circuits and Signal Processing (JAICSP 2011)

(2) IEEE International Conference on Electronics, Circuits and Systems (ICECS 2008)

(1) IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2008)

4.5 Institutions et entreprises ayant des projets en coopérations directement établies

(8) PUCRS (Pontifícia Universidade Católica do Rio Grande do Sul) à Porto Alegre (Brésil)

(7) UFSM (Université Fédérale de Santa Maria) à Santa Maria (Brésil)

(6) ST Microelectronics à Crolles

(5) Tiempo Secure à Montbonnot Saint Martin

(4) Centre Microélectronique de Provence (Campus G. Charpak) à Gardanne

(3) UFMG (Université Fédérale de Minas Gerais) à Belo Horizonte (Brésil)

(2) LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier)

(1) UFRGS (Université Fédérale du Rio Grande do Sul) à Porto Alegre (Brésil)

4.6 Communications sur invitation (séminaires)

(5) JADUE, A. R. I; LEITE, T. F. P.; POSSAMAI BASTOS, R. P.; ROLLOF, O. A.; MAMADOU, D.; FESQUET, L. Layout Strategies for Body Bias Islands in FD-SOI Systems. 20th

International IP-SoC Conference and Exhibition, 2017, Grenoble, France.

(4) POSSAMAI BASTOS, R. P.; Dynamisant les Cours en Amphi avec les Smartphones des Etudiants et les Boîtiers de Vote de l'Université : Activités en Groupe et Classement par Etudiant. Talk presented in Rencontre Boitiers de Vote à l'Université Grenoble Alpes (Grenoble, France) on June 17th 2016.

(3) POSSAMAI BASTOS, R. P.; The World of the Hardware Trojans. Talk presented in Federal University of Rio Grande do Sul (UFRGS, Porto Alegre, Brazil) on April 26th 2013.

(2) POSSAMAI BASTOS, R. P.; Systèmes Intégrés Tolérants aux Fautes, Fiables et Sécurisés. Talk presented in TIMA Laboratory (Grenoble, France) on April 17th 2012.

(1) POSSAMAI BASTOS, R. P.; Asynchronous Circuits as an Alternative for Mitigation of Long-Duration Transient Faults in Deep-Submicron Technologies. Talk presented in Federal University of Rio Grande do Sul (UFRGS, Porto Alegre, Brazil) on April 1st 2011.

Chapter 5

Responsabilités scientifiques et pédagogiques

5.1 Responsable de projets scientifiques

(6) 2017-2018 : projet LabEx PERSYVAL-Lab : « Qualification of Supervised Learning Models under Radiation-Induced Effects ». Idéalisation et responsabilité scientifique des activités de l'étudiant de master 2 Matheus Garay Trindade qui a obtenu une bourse d'excellence PERSYVAL-Lab grâce à sa performance académique de haut niveau au Brésil et notre proposition de projet au LabEx. Matheus a été très bien recommandé par mes partenaires de l'UFSM (Brésil) ;

(5) 2017-2020 : projet de thèse de doctorat financé par le gouvernement français : « Testing of Asynchronous Circuits for Security Systems in Advanced Technologies ». Idéalisation et responsabilité scientifique des activités de l'étudiant de doctorat Ricardo Aquino Guazzelli qui a obtenu une bourse ministérielle grâce à sa performance lors de son master niveau bac + 7 au Brésil et notre proposition de projet à l'École Doctorale EEATS. Ricardo a été très bien recommandé par mes partenaires de la PUCRS (Brésil) ;

(4) 2018-2021 : projet soumis en mai 2017 à l'appel CAPES-COFECUB : « SUNRISE : SecUre aNd Reliable computIng SystEms » en partenariat avec le LIRMM (Montpellier), IES (Montpellier), UFRGS (Brésil) et PUCRS (Brésil). Idéalisation et responsabilité scientifique au TIMA des activités de notre groupe de recherche. Si accepté, ce projet financera des missions d'échanges scientifiques à 6 chercheurs permanents français et 5 brésiliens. De plus, il permettra à nos doctorants français et brésiliens de réaliser des stages scientifique à l'extérieur ;

(3) 2015-2019 : projet de thèse de doctorat financé par l'agence brésilienne CNPq : « Evaluating the efficiency of New Transient-Fault Detection Techniques for Integrated Circuits under Laser-Induced Fault Sources ». Idéalisation et responsabilité scientifique des activités de l'étudiant de doctorat Raphael Andreoni Camponogara Viera qui a obtenu une bourse brésilienne grâce à sa performance académique et notre proposition de projet au CNPq. Raphael a été très bien recommandé par mes partenaires de l'UFSM (Brésil) ; Ce projet finance complètement la thèse du doctorant pendant une période de 4 ans ainsi que les billets d'avion aller-retour pour sa famille, une aide d'installation et sécurité sociale ;

(2) 2014-2017 : projet de thèse de doctorat financé par le gouvernement français : « Testing Techniques for Detection of Hardware Trojans in Integrated Circuits of Trusted Systems ».

Idéalisation et responsabilité scientifique des activités de l'étudiant de doctorat Leonel Acunha Guimarães qui a obtenu une bourse ministérielle dans le cadre d'un projet de sujet fléché dont nous avons proposé à l'École Doctorale EEATS. Leonel a été recommandé par mes partenaires de l'UFRGS (Brésil) ;

(1) 2014-2016 : projet financé par le programme brésilien UNIVERSAL MCT/CNPq : « Making a transient-fault detection technique feasible in integrated circuits ». Idéalisation et responsabilité scientifique au TIMA de ce projet de coopération avec le groupe de l'enseignant-chercheur Frank Sill Torres de l'UFMG (Brésil). Ce projet a financé un test chip contenant des capteurs de courant innovants ainsi que deux stagiaires de niveau bac + 4 dans le contexte d'une formation brésilien appelée d'initiation à la recherche. Par ailleurs, en août 2016 une mission scientifique à Belo Horizonte (Brésil) a été partiellement financée dans le cadre des visites d'échanges scientifiques prévues dans le projet.

5.2 Co-responsable de projets scientifiques

(3) 2018-2020 : projet de coopération internationale financé par l'université brésilienne PUCRS : « Secure and Self-Aware Multi-core Systems (SSAMS) International Cooperation Project » en partenariat avec le TUWien (Autriche) et Université Bretagne Sud (France). Co-responsabilité scientifique au TIMA des activités de notre groupe de recherche. Ce projet financera 8 missions internationales d'échanges scientifiques de 15 jours au Brésil, France et Autriche ;

(2) 2018-2021 : projet soumis en septembre 2017 à l'appel IDEX UGA : « NanoBob : Quantum Physics with a Nanosatellite » en partenariat avec le Centre Spatial Universitaire de Grenoble (CSUG). Co-leader du « Work Package 3B: Payload Time Stamping Unit » avec l'enseignant-chercheur Laurent FESQUET, idéalisation et responsabilité scientifique des activités de notre groupe de recherche. Si accepté, ce projet financera : 3 ans de thèse d'un doctorant et 1 ans d'ingénieur de recherche ;

(1) 2014-2018 : projet européen ENIAC « THIN but Great Silicon 2 Design Objects (Things2Do) ». Co-gestion avec l'enseignant-chercheur Laurent FESQUET, idéalisation et responsabilité scientifique des activités de notre groupe de recherche. Ce projet finance : 3 ans de thèse des doctorants Otto Aureliano Rolloff et Thiago Ferreira de Paiva Leite ; 2 ans de l'ingénieur de recherche Rodrigo Iga Jadue ; et un test chip en technologie FD-SOI 28 nm au coût de 25 k€.

5.3 Membre de conseil de laboratoire

(1) 2016-2020 : membre élu du conseil du laboratoire TIMA.

5.4 Responsable d'activités pédagogiques

(12) 2016-2018 : tuteur universitaire : suivi de 6 étudiants en alternance université et entreprise dans le cadre du master 2 UGA MISTRE (Microélectronique Intégration des Systèmes Temps Réels Embarqués) de l'UFR PhiTEM. Suivi pendant l'année universitaire : 8 heures par étudiant.

(11) 2016-2018 : enseignant responsable de l'UE « Projet et Conception de Systèmes Intégrés

» du programme de master 2 UGA MISTRE de l'UFR PhiTEM. Encadrement de 8 étudiants réalisant des projets pratiques de 60 heures de travail personnel : 6 heures d'encadrement par étudiant.

(10) Responsable de la création et animation d'activités innovantes d'enseignement en utilisant formulaires Google en ligne, smartphones et méthodes de pédagogie inversée, enseignement collaboratif, atelier de débat et évaluation par les pairs. Ces méthodes sont adaptées et utilisées dans tous les enseignements dont je suis le responsable (cf. les points ci-après). Un séminaire décrivant ces méthodes a été fait en juin 2016 sur invitation du Service d'Accompag-nement des Pédagogies, des Initiatives Enseignantes et du Numérique dans le Supérieur (SAPIENS) de l'UGA.

(9) 2016-2018 : enseignant responsable de l'unité d'enseignement (UE) « Formation Bureautique et Informatique (FBI) » : création en 2016, gestion d'une équipe de 8 vacataires et encadrement de travaux pratiques. L'équipe de la FBI assurent environ 400 heures des travaux pratiques à plus de 1400 étudiants de licence 1 du Département Licence Sciences et Technologies (DLST) de l'UGA.

(8) 2016-2018 : suivi de 12 étudiants sportifs de haut niveau (SHN) dans le cadre de l'UE FBI du DLST de l'UGA. Suivi pendant l'année universitaire : 0,5 heure par étudiant.

(7) 2015-2018 : enseignant responsable de l'UE « Architectures de Systèmes à Base de Processeurs ». Appartenant au programme de master 2 UGA MISTRE de l'UFR PhiTEM, l'UE propose 24 heures de cours magistraux et 18 heures de travaux dirigés à environ 30 étudiants.

(6) 2012-2018 : tuteur universitaire : suivi de 12 étudiants en alternance université et entreprise dans le cadre du master 2 UGA MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises) de l'UFR IM2AG. Suivi pendant l'année universitaire : 14 heures par étudiant.

(5) 2014-2017 : enseignant responsable de l'UE « Introduction aux Architectures Logicielles et Matérielles » du DLST de l'UGA : gestion, réalisation de cours magistraux, travaux dirigés et pratiques. Cette UE de niveau licence 2 a une équipe de 5 enseignants qui encadrent 42 heures de travaux dirigés et pratiques par groupe. Les 18 heures de cours magistraux sont dispensés en amphithéâtre à environ 140 étudiants.

(4) 2013-2017 : enseignant référent au DLST pour le Certificat Informatique et Internet (C2i). Environ 200 étudiants de licence 2 passaient les épreuves du C2i qui a été remplacé en 2017-2018 par la certification PIX.

(3) 2016 : tuteur universitaire : suivi d'un étudiant en stage entreprise dans le cadre du master 2 UGA NENT (Nano Electronique et Nano Technologies) de l'UFR PhiTEM. Suivi pendant le semestre du stage : 3 heures.

(2) 2013-2016 : enseignant responsable de l'UE « Sécurité des Architecture Matérielles » du programme de master 2 UGA en Sécurité, Audit, inFormatique légalE (SAFE) de l'UFR IM2AG. L'UE proposait 12 heures de cours magistraux à environ 20 étudiants.

(1) 2012-2015 : enseignant responsable de l'UE « Projet de Méthodologie et Outils de Conception » du programme de master 2 UGA NENT de l'UFR PhiTEM. L'UE proposait 32 heures de travaux pratiques à environ 15 étudiants.

Chapter 6

Résumé d'activités de recherche

Mes principales activités de recherche depuis mon doctorat sont résumées ci-après en anglais.

6.1 Introduction

In the advent of self-adaptive systems like geolocation satellites, aircraft, drones, autonomous cars, nuclear power plant robots, in-body-implanted medical devices – which are all applications of high risk in case of failure – embedded circuits must be sufficiently reliable, safely operating within a specified range of low-power performance even in harsh environments. Furthermore, circuits embedded in such critical applications must also be conveniently secure, hiding confidential data, restricting access to private information, and defending themselves from intentional attacks that aim to hack into systems for maliciously carrying out illegal actions or inducing catastrophic situations.

My research works are specifically interested to deal with three important issues related to the security, reliability, and power of integrated systems in complementary metal–oxide–semiconductor (CMOS) technologies:

(a) hardware Trojans (HT), which are malicious slight layout alterations or furtive mechanisms included in outsourced IC design, fabrication, or manufacturing phases by third-party suppliers willing to hack, disturb, or intentionally disable, at run time, the Trojan-infected circuits;

(b) transient faults (TF), as voltage glitches induced by radiation or malicious sources of perturbation, can provoke bit flips in memory elements – i.e. soft errors that may lead entire systems to fail, compromising critical applications or even providing relevant information for cryptanalysis methods that exploit results of fault-injection attacks over secure circuits; and

(c) transistor threshold voltage (Vth) alterations – induced by aging, process, voltage, and temperature (PVT) variations as well as by body bias modifications – are able not only to slow down gates of circuits, violating critical timing constraints, but also speed up them at the expense of static power consumption increase.

6.2 Main research activities and scientific contributions

Since the begin of my researcher career, I have developed scientific works related to the fields of the design, run-time test, and post-fabrication test of reliable, secure, and low-power integrated systems.

State-of-the-art run-time testing mechanisms for detecting TF have been evaluated by using a simulation-based method that we have recently published. Obtained results provide a rank in terms of their efficiencies in detecting TF, revealing the bulk built-in current sensors (BBICS) as the most efficient solution. BBICS integrates the high concurrent error detection efficiency of costly techniques (duplication with comparison) with the low area and power overheads of less efficient run-time testing mechanisms (time redundancy schemes). Moreover, unlike most existing TF-detection techniques, the BBICS is also able to detect long-duration and multiple TF, a major problem in intentional fault-based attacks targeting to break the security of integrated systems. For this reason, available BBICS architectures in literature have also been studied and compared with regard to their sensitivities in detecting TF. Novel BBICS architectures with enhanced TF-detection sensitivity, negligible power consumption, and lower area penalty than its antecedents have been devised and published.

Furthermore, we have discovered a second function for the BBICS: the detection of HT. We have invented a post-fabrication testing method that takes advantage of the BBICS as an offline-testing mechanism for detecting HT. As this type of sensor monitors body terminals of system's subcircuits, the proposed method is capable to identify any slight HT-induced variations on the electrical impedance of subcircuits by simply injecting a short train of current pulses into body terminals, and analyzing digital signatures provided by the BBICS. At run time, the same BBICS operates as an online-testing mechanism for detecting TF. This method adds a new category to the classical taxonomy of side-channel analysis-based techniques, it is indeed the first work that analyzes as a side channel the digital signatures related to the impedance of subcircuit's n-well or p-well layers.

Partitioning integrated systems into subcircuits having single n-well or p-well layers allows, in addition to individually manage them at run time, better controlling Vth variations, power, and speed. We have studied and devised a new architecture of a specific built-in cell that is mandatory to dynamically adapt the body bias of small subcircuits: a level shifter (LS). With reasonable area, power, and delay penalties, the proposed LS cell is fully suitable for fine-grained systems such as circuits designed with asynchronous logic, which is intrinsically modular due to the absence of a clock. For this purpose, we have analyzed and evaluated the advantages of applying body biasing schemes on asynchronous circuits designed in UTBB FD-SOI technology, besides underlining the better energy efficiency of case-study asynchronous circuits – compared with its synchronous counterpart – and its lower voltage operation thanks to its reduced number of timing assumptions.

In the field of the asynchronous logic, we have also studied and discovered another new benefit of the quasi-delay insensitive (QDI) asynchronous circuits: their strong natural ability for mitigation of single long-duration transient faults in advanced technologies. Novel logical and electrical-level simulation methods dedicated for injecting transient faults into asynchronous circuits have also been proposed. Furthermore, we have devised a complete framework named ALPS: Architectural tools for ultra-Low Power (event-driven) Systems that allows choosing and simulating a signal-specific sampling scheme, and to synthesize a dedicated event-driven circuit to process the resulting sampled data.

Part III

Appendix: some complementary works

Appendix A

Article in international IEEE conference: DATE 2018

Non-Intrusive Testing Technique for Detection of Trojans in Asynchronous Circuits

Leonel Acunha Guimarães, Thiago Ferreira de Paiva Leite, Rodrigo Possamai Bastos, and Laurent Fesquet
Univ. Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000 Grenoble, France
* Institute of Engineering Univ. Grenoble Alpes
{leonel.guimaraes|thiago.leite|rodrigo.bastos|laurent.fesquet}@univ-grenoble-alpes.fr

***Abstract*—Asynchronous circuits, as any IC, are vulnerable to hardware Trojans (HTs), which might be maliciously implanted in IC designs during outsourced fabrication phases. In this paper, a new testing technique to detect HTs by exploiting the regular side-channel properties of quasi-delay insensitive (QDI) asynchronous circuits is proposed. The technique does not need neither additional circuitry nor significant adjustments in the post-fabrication testing phase. Simulation results show that the proposed technique is able to detect HTs with dimensions smaller than 1% of the original circuit.**

I. Introduction

Nowadays IC architectures demand matching robustness against attacks and faults with low power and performance. Clockless circuits, also known as asynchronous circuits are an interesting alternative to deal with power consumption without compromising system's performance [1]. Those architectures employ local communication protocols instead of a global clock for data synchronization, avoiding unnecessary dynamic power consumption in parts of the circuit that have no data to process at a certain point in time. The robustness of Quasi-Delay-Insensitive (QDI) asynchronous circuits against Differential Power Analysis (DPA) [2], transient-faults [3] and EM emissions [1] makes them also a good solution from a security point a view.

Hardware Trojans (HT) are a security issue that currently draws attention of many researchers and engineers. A HT can be a simple layout modification made by an attacker in an untrusted foundry that enables security-oriented systems to leak keys to an adversary [4]. Furthermore, a Trojan can be designed to remain inactive until being triggered by a rare event, leading it to be almost undetectable during regular testing phase. Since a HT, even inactive, causes impacts on side-channel signals, several techniques exploit them for detecting HTs [5]–[9].

Nevertheless, process variations (PV) affect side-channel signals, masking Trojan effects in the circuit. Thus, side-channel analysis detection methods require considerable efforts at design- or test-level to compensate PV. A widely used design-level approach consists of splitting the original circuit in several measurement domains in order to isolate the Trojan impacts to a specific area [6], [7]. This strategy require extra on-chip circuitry or pads to separate the sub-circuits signals and additional post-manufacture tests or dedicated set-ups to generate all required signals, which increases the project cost.

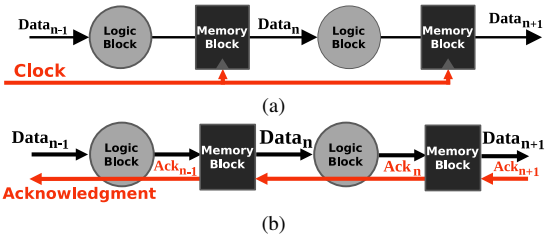


Figure 1. Typical representations of synchronous (a) and asynchronous (b) systems.

Some works were recently published showing that it is possible to implement Trojans in asynchronous circuits [10], [11], while others [12], [13] present strategies to detect threats in mixed macro synchronous micro asynchronous systems. However, for the best of our knowledge, none have ever proposed methods devoted for detecting Trojans inserted in QDI asynchronous circuits.

In this paper, we propose a testing technique for Trojan detection dedicated to QDI asynchronous circuits exploiting the transient current (I_{DDT}) and path delay (Δt) to compare patterns from genuine ICs and devices under Trojan test (DUTT) without adding any extra circuitry nor modifying the original post-silicon test set-up. The proposed technique takes advantage of intrinsic aspects of asynchronous circuits' supply current, which produces separate traces from different blocks that compose the system. We show that it is only required measuring global supply current I_{DD} from the V_{DD} pin to obtain isolated side-channel signals from each block of the circuit.

II. Fundamentals of QDI Asynchronous Systems

Circuits that use a local communication protocol for data synchronization, instead of a global clock, are known as clockless or asynchronous circuits. In such architectures, a certain block (sender) only outputs a signal to the following one (receiver) if all its output channels are empty. The receiver, in turn, will only start processing new data when all the necessary inputs are available. These two directives are the basis of a local communication protocol. Respecting them is thus crucial for a correct functioning of asynchronous circuits.

A typical representation of an asynchronous system is shown in Fig.1b. If compared to its synchronous equivalent, the basic difference noted is the absence of a clock signal and the addition of an acknowledgement signal. The latter

is part of the local protocol that enables synchronization in asynchronous systems. It signalizes the previous stage that the calculation is completed and new data can be processed.

QDI is a class of asynchronous circuits that can operate correctly with only a few timing constraints [1]. They require a robust data encoding, one that allows data validity to be signaled by the information being propagated itself, hence dual-rail encoding is used for this purpose. In this case, the protocol validity signal (request) is merged into data signals. Thus, there is no physical difference between data and the communication protocol signal. This type of encoding is particularly robust against DPA based attacks, due to its power balance property which masks internal states [2]. Moreover, this class of circuits also features robustness against fault attacks, as discussed in [3]. Consequently, QDI asynchronous architectures are an attractive solution in terms of security.

III. Side Channel Analysis Applied to QDI Asynchronous Circuits

A. Trojan Detection Through Side-Channel Analysis

Several methods have been proposed in literature comparing side-channel signals patterns of DUTTs with golden results from genuine ICs [4]. If the patterns obtained from a DUTT deviate from the golden IC references, a Trojan is detected. Different side-channel signals such as transient current (I_{DDT}) [5], quiescent current (I_{DDQ}) [6], path delay [7] and EM [8] can be exploited.

Despite the multiple options of side-channel signals that can be exploited, dealing with variability is one of the biggest challenges faced by the referred studies. In fact, PV alters circuit parameters such as threshold voltages (V_{th}), channel lengths (L), and oxide thickness (T_{ox}). The detection of slight Trojans relies on alternatives to compensate for parameter fluctuations that could mask HT effects. Several methods [5], [6] propose using multiple power pins in the circuit to highlight the side-channel patterns from a specific regions of the chip, isolating their effects in a smaller region consequently increasing detectability.

Although reliable results are presented covering most of circuit designs against Trojans, such techniques impose substantial area overhead or considerable addition in cost and duration of the testing phase. For instance, the method in [7] proposes using a secondary clock signal to control a set of shadow registers to measure the path delay of logic blocks. The approach in [9] evaluates a pair of parameters (maximal frequency and transient current) to detect Trojans, measuring the signals from multiple power supply pins in order to isolate the Trojan and applying power gating to enhance the detection rate. The methodology in [8] is able to detect Trojans by mapping thermal characteristics with no extra hardware in the original design. However, it requires the use of high resolution devices to generate thermal maps, which increases time-to-market and costs at testing phase, besides the challenging procedures for nanoscale technology nodes.

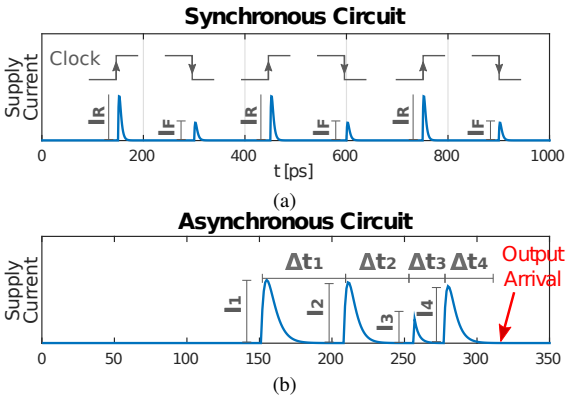


Figure 2. Abstraction of the supply current from synchronous (a) and asynchronous (b) circuits.

B. Side-Channel Signals in QDI Asynchronous Circuits

As presented in section II, locally derived handshake pulses control data propagation in asynchronous circuits. Their generation, which can occur at any moment, are governed by the latency of the successor and the predecessor blocks. Therefore, these pulses tend to be randomized over time, resulting in smoother supply current curves [1], without the large di/dt spikes as in synchronous circuits, as shown in Fig. 2a.

The asynchronous protocol results in a current trace as the one depicted in Fig. 2b. This example represents the current response of a single input vector passing through a 4-stage pipelined asynchronous circuit measured from the global power supply. In case of a single input vector test, whenever the first stage outputs data to be processed by the second stage, the former will no longer have new calculations to do, and will become idle. The same behavior will be observed in every following stage of the asynchronous pipeline until all stages turn inactive. Therefore, only one stage of the pipeline is in fact active at a certain moment, while the other stages stand idle, waiting for new data to process. Thus, each peak in Fig. 2b corresponds to the operation of a single pipeline stage. For this reason, a Trojan inserted in an asynchronous circuit directly impacts the current peak that corresponds to the stage in which it has been inserted. Conversely, in synchronous circuits the global clock governs the switching activity of all pipeline stages simultaneously. Hence, the current peaks depicted in 2a represent the sum of the individual contribution of all elements that composes the circuit. The insertion of a Trojan in this case would impact the supply current response of the system as a whole, not only the pipeline stage in which it has been inserted. Consequently, it is possible to obtain the transient current of each separate pipeline stage and the path delay only with the global supply current trace.

1) Global Path Delay (Δt): In QDI asynchronous circuits, the delay of a pipeline stage can be measured by the difference Δt_i between two current peaks (see Fig. 2b). As the global delay is given by $\Delta t = \sum_{i=1}^{n} \Delta t_i$, the deviation caused by a Trojan in one of its n pipeline stages is propagated to others subsequent blocks, delaying the output. Therefore, measuring the delay Δt between the primary inputs and its arrival at the

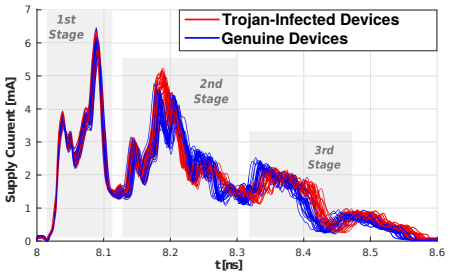


Figure 3. Current curves in a 3-stage pipelined QDI asynchronous circuit obtained with 50-run Monte Carlo simulations. Blue traces were generated by genuine and red by Trojan-infected devices.

system output, is sufficient for malicious circuitry tracking. Obtaining path delay in asynchronous circuit, thus, requires only non-intrusive current measures on the power supply pin, seamlessly fitting in the regular testing phase with no extra cost in terms of design. Additionally, as gate delays is inversely proportional to power supplies levels, two simple actions can increase feasibility of path delay measurements: (1) reduction of the power supply level V_{DD} and; (2) reduction of the substrate voltage V_{DDS}.

2) Transient Current (I_{DDT}): Since only the gates from a specific pipeline stage switches simultaneously, if a Trojan is inserted in a certain stage, its relative current peak is increased, highlighting the Trojan impact. Therefore, a HT insertion in a given stage can be recognized by the variation in its current amplitude.

Path delays and transient currents are correlated and mutually affected by PV. If the variation increases the current, it decreases the delay and vice-versa. The measurement of one variable allows deducing the range of the other, thus reducing the range of possible values of the other one. Therefore, the evaluation of the variables I_{DDT} and Δt allows reducing the impact of PV effects, as similarly demonstrated in [9].

C. Trojan Impacts on Side-Channel Signals

We propose to illustrate the Trojan effects on the current trace by a preliminary test considering PV effects in FD-SOI 28nm technology. Fig. 3 show an example of supply current traces obtained from 3-stage pipelined devices with and without a Trojan implanted in its second stage. The result figure depicts the impacts caused by Trojans (of approximately 1.3% of the original circuit area) in the current trace. It illustrates the motivation for the Trojan detection technique presented in this work. Note that the current in the first stage remains unadulterated, whereas the current peaks in the second stage are clearly increased, and delayed in the third due to the Trojan effects. The necessary steps to perform Trojan detection are thus discussed in the following section.

IV. Proposed HT-Detection Technique for QDI Asynchronous Circuits

A. Test Procedure: Collecting I_{DDT} and Δt

Initially, the proposed test procedure requires collecting side-channel signatures from genuine devices (golden data) as in other methods. Subsequently, the same procedure is applied on each DUTT in order to produce results that will be statistically compared to the golden data.

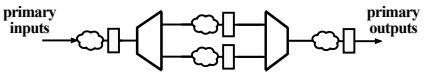


Figure 4. Representation of the pipeline stages from the ALU in [14].

As explained in Section III-B, the supply current trace is enough to obtain I_{DDT} and Δt, which are the necessary parameters for the proposed analysis. Thus, the current trace is directly measured from the global V_{DD} pin of each golden device using a test input vector X, from which the I_{DDT} peaks of each pipeline stage (I_{DDT1}, I_{DDT2}, I_{DDT3}) are extracted and stored. The Δt is obtained with the same test, however using a reduced V_{DD} level to facilitate the delay measurement, as discussed in III-B1. This test is repeated for each available genuine device. By the end, due to the PV effects, the collected parameters form a statistical distribution. Defining limits to such a distribution results in a data range in which measurements from genuine devices are expected to lay on. By performing the same test in each DUTT, it is possible to verify if its parameters belong to the generated distribution, thus classifying it as Trojan-free if the assumption is true, otherwise the DUTT is classified as Trojan-infected.

V. Experiments, Results, and Analysis

The QDI asynchronous 8-bit ALU proposed in [14] is the case-study circuit chosen for this study. It has 3 stages of pipeline and a total of 506 logic gates. Fig. 4 depicts an abstraction of it.

The Trojan model is a gate-level trigger that alters data flow whenever the input is set to a specific value, which is never tested during our simulations to make the detection more challenging. Therefore, the Trojan remains inactivated during all performed tests, which implies that its architecture is not pertinent for the detection. Simulations were done with Trojans representing 1.7%, 1.3% 1%, and 0.8% area of the original design. Both case-study and Trojan were synthesized with low threshold voltage transistors in FD-SOI 28nm technology. Results were obtained by using 400-run Monte Carlo (MC) simulations performed at a reference temperature of 25^oC. Intra- and inter-die PV have been considered.

Two simulations are performed in order to generate results for the technique proposed in IV: one to obtain I_{DDT} with supply voltage V_{DD} of 1V, and the second one to obtain global Δt, with V_{DD} of 0.6V. Data collected from Trojan-free devices produce the signature of golden ICs by following the procedure explained in section IV. Afterwards, the same design is infected with different Trojans, to produce results that are statistically compared with the golden data. The parameter used to evaluate the results is the detection rate, defined as the percentage of Trojan data not pertaining to the Trojan-free distribution.

A. Results and Analysis

Results from MC simulations performed with genuine and Trojan-infected devices are shown in Fig. 5. In these simu-

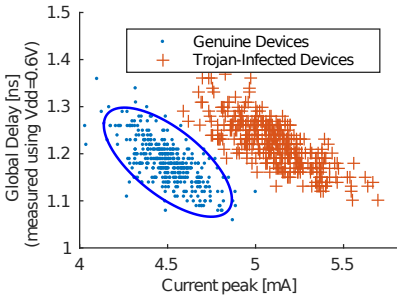


Figure 5. Current peak in the second stage and the global delay obtained from 400-run MC in the Trojan-free and Trojan-infected ALU. The ellipse surrounds the data from genuine devices with a confidence level of 95%.

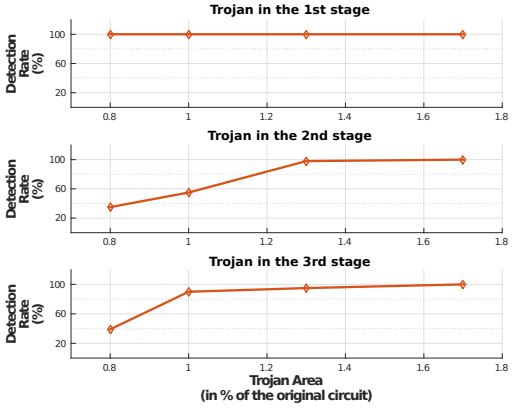


Figure 6. Detection rate obtained considering Trojan infection in different pipeline stages.

lations, the Trojans have a total area of 1.6% of the original circuit area and were inserted in the second pipeline stage. An error ellipse with 95% of confidence level surrounds the golden data, indicating a region in the parameters space where a circuit is accepted as Trojan-free. Note that the impact of the Trojan shifts the data from its original value to a greater current peak and global delay, as previously signaled in Fig. 3. As no point from the Trojan-infected circuit is enclosed by the Trojan-free ellipse, the detection rate is 100%.

The same study is extended to cases in which the HT size and location vary. Fig. 6 depicts the curves of detection rate versus Trojan size. The graphs represent the results for HTs inserted in the first, second, and third stages respectively.

Results in Fig. 6 show that it is possible to detect Trojans representing 1.3% of the original circuit area with a detection rate of 100% if the Trojan is inserted in the first pipeline stage, 98% in the second one, and 95% in the third stage. The curves in different stages are different, since the total number of gates vary in each stage. If the stages were equality balanced, the total dynamic consumption would be divided equally in all stages and, thus the curves would be more homogeneous. Furthermore, systems with more pipeline stages would present its dynamic power divided in more stages, enhancing the relative Trojan overhead in one of their stages. In order to enhance the detection rate, modifications in the original circuit could be made to increase the number of pipeline stages.

VI. Conclusions

We presented an efficient Trojan detection technique dedicated to QDI asynchronous circuits exploiting its inherent transient current and path delay characteristics. The evenly distributed current peaks, intrinsic of asynchronous circuits, make them more sensitive to side-channel deviations than synchronous circuits, thus enhancing HT detection potential. Thus, it is possible to detect modifications smaller than 1.3% of original circuit with a detection rate of 95% without requiring any extra-circuitry. Moreover, the testbench set-up employed in the regular post-silicon testing phase can be reused for this purpose. Still, this technique can also be employed combined with any other methods proposed in the literature in order to enhance the obtained results, thus allowing the detection of even smaller Trojans. Future works will include adapting the proposed detection technique to other classes of asynchronous circuits, e.g. micropipeline.

References

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design: A Systems Perspective*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[2] W. G. Ho *et al.*, "Security analysis of asynchronous-logic qdi cell approach for differential power analysis attack," in *2016 International Symposium on Integrated Circuits (ISIC)*, Dec 2016, pp. 1–4.

[3] Y. Monnet *et al.*, "Designing resistant circuits against malicious faults injection using asynchronous logic," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1104–1115, Sept 2006.

[4] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, Jan 2010.

[5] R. Rad *et al.*, "Sensitivity analysis to hardware trojans using power supply transient signals," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, June 2008, pp. 3–7.

[6] J. Aarestad *et al.*, "Detecting trojans through leakage current analysis using multiple supply pad I_{ddq} s," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 893–904, Dec 2010.

[7] B. Cha and S. K. Gupta, "Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost," in *DATE*, 2013.

[8] K. Hu *et al.*, "High-sensitivity hardware trojan detection using multimodal characterization," in *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2013, pp. 1271–1276.

[9] S. Narasimhan *et al.*, "Hardware trojan detection by multiple-parameter side-channel analysis," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183–2195, Nov 2013.

[10] T. Y. Koutaro Inaba and M. Imai, "Hardware trojan asynchronous noc router," in *Asynchronous Circuits and Systems (ASYNC), 2017 IEEE 24th International Symposium on*, May 2017, to be published.

[11] S. R. Hasan *et al.*, "Hardware trojans in asynchronous fifo-buffers: From clock domain crossing perspective," in *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug 2015, pp. 1–4.

[12] F. K. Lodhi *et al.*, "Hardware trojan detection in soft error tolerant macro synchronous micro asynchronous (msma) pipeline," in *2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug 2014, pp. 659–662.

[13] ——, "Formal analysis of macro synchronous micro asychronous pipeline for hardware trojan detection," in *2015 Nordic Circuits and Systems Conference (NORCAS): NORCHIP International Symposium on System-on-Chip (SoC)*, Oct 2015, pp. 1–4.

[14] T. F. de Paiva Leite *et al.*, "Comparison of low-voltage scaling in synchronous and asynchronous fd-soi circuits," in *2016 26th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, Sept 2016, pp. 229–234.

Appendix B

Article in international ACM conference: ISPD 2018

Standard CAD Tool-Based Method for Simulation of Laser-Induced Faults in Large-Scale Circuits

Raphael A. C. Viera
Ecole Nat. Sup. des Mines de St-Etienne
LIRMM, CNRS, UMR N5506
Univ. Grenoble Alpes, CNRS, TIMA
raphael.viera@emse.fr

Jean-Max Dutertre
Ecole Nat. Sup. des Mines de St-Etienne
Gardanne, France
dutertre@emse.fr

Philippe Maurine
LIRMM, CNRS, UMR N5506
Montpellier, France
philippe.maurine@lirmm.fr

Rodrigo Possamai Bastos
Univ. Grenoble Alpes, CNRS, TIMA
Grenoble, France
rodrigo.bastos@univ-grenoble-alpes.fr

ABSTRACT

Designing secure integrated systems requires methods and tools dedicated to simulating —at early design stages— the effects of laser-induced transient faults maliciously injected by attackers. Existing methods for simulation of laser-induced transient faults do not take into account IR drop effects that are able to cause timing failures, abnormal reset, and SRAM flipping. This paper proposes a novel standard CAD tool-based method allowing to simulate laser-induced faults in large-scale circuits. Thanks to a power-grid network modeled by a commercial IR drop CAD tool, an additional transient current component causing laser-induced IR drop is taken into consideration. This current component flows from V_{DD} to G_{ND} and may have a significant effect on the fault injection process. The method provides fault sensitivity maps that enable a quick assessment of laser-induced fault effects on the circuit under analysis. As shown in the results, the number of induced faults is underestimated by a factor as large as 3.1 if laser-induced IR drop is ignored. This may lead to incorrect estimations of the fault injection threshold, which is especially relevant for the design of countermeasure techniques for secure integrated systems. Simulation times regarding four different circuits are also presented in the results section.

1 INTRODUCTION

Lasers have been used since the 1960s in order to emulate the effects caused by radiation on semiconductors [13]. In the early 2000s, [26] reported the use of laser illumination to induce faults into secure integrated circuits, e.g., a bit-flip into a SRAM cell. This created a need for designing robust circuits against laser fault injection, consequently generating a demand for simulation tools capable of simulating the effects of laser shots on ICs. Although fault simulations can be performed at different abstraction levels of the design flow, i.e. transistor, gate, RTL and software, low abstraction levels provide the highest accuracy. At the electrical level, a double exponential current source has been demonstrated efficient for modeling a laser shot [16, 28]. This current source is added to the netlists of cells illuminated by the laser. Then an electrical level simulation, which takes into account the effects of the laser attack, can be performed.

The idea commonly accepted is that a laser shot generates parasitic currents [15]. These currents generate an undesired transient voltage that propagates through the logic toward the inputs of registers (D-type Flip Flops) and, if it is still present when the clock edge occurs, bits may be inverted, producing soft errors (SE). Due to the increasing transistor density, a laser shot will affect multiple gates at the same time. Thus, laser illumination also induces, in addition to the well known photoelectric effect, an IR drop phenomenon with a significant effect on the fault injection process that has to be taken into account while simulating laser fault injection [27]. These effects must be simulated at low abstraction levels taking into account the layout topology to better represent physical phenomenon in the scope of a whole system, i.e., the simulation must be performed in complex circuits and not just in one (or few) cells.

To the best of our knowledge, among the existent fault simulators [6, 12, 18, 21, 24], the most recent one is [19], which is based on the open-source Lifting [1]. The major issue with these fault simulators is that they rely on electrical models [8, 11, 25] that are technology dependent. For instance, in [14], the authors proposed a model that includes the vertical parasitic bipolar junctions inherent to MOSFETs in the fault injection process that may lead to IR drop effects. However, they did not extended their work beyond the scope of a single inverter. In fact, dimensioning the RC network of power/ground rails is a difficult task, since the RC values depend on the technology, the size of cells, the position of voltage taps on the rails, the RC parasitics, etc.

The issue being that, as far as we know, there is no tool capable to simulate laser-induced IR drop and its propagation in a large circuit. Thus, the first and main objective of this work is to introduce the devised methodology to simulate at the electrical level the effect of IR drop on the fault injection sensitivity using standard CAD tools; the second objective is to illustrate, on simulation grounds, that laser-induced IR drop has to be considered since it may result in underestimating the risk of fault injection.

2 STATE OF THE ART

2.1 Modeling laser effects on ICs

2.1.1 Laser Induced Transient Currents. ICs are known to be sensitive to induced transient currents. These currents may be caused by laser shots passing through the device, creating electron-hole pairs along the path of the laser beam [15]. The induced charge carriers recombine without any significant effect, unless they reach

the strong electric field found in the vicinity of reverse biased PN junctions. In this case, the electrical field puts these charges into motion and a transient current appears as well as a transient fault. The nature of this fault is similar to the ionization effect generated by energetic particles [13].

As an example (the cross section of an inverter), Fig. 1 illustrates where laser shots may generate parasitic currents. In case the inverter input is in low state ('0') the most laser-sensitive part of the inverter is the drain of the NMOS transistor since there is a reverse biased PN junction between the drain and the $P_{substrate}$. Thus, an induced transient current (I_{Ph}) flows from the drain of the NMOS to the $P_{substrate}$ biasing contact. A similar reasoning can be made when the inverter input is high ('1'). In that case, the susceptible part of the inverter is the drain of the PMOS transistor. In case of Fig. 1, a part of the induced photocurrent (I_{Ph}) charges the inverter output capacitance. As a result the inverter output undergoes a voltage transient.

Another transient current component flowing from V_{DD} to G_{ND} that may have a significant effect on the fault injection mechanism is taken into consideration by the model of Fig. 1 [27]. This transient current is induced in the reversed biased *Psub-Nwell* junction that surrounds every *Nwell*. Even if the laser beam is directed towards a sensitive NMOS, the laser beam also induces charge carriers that will be sufficiently close to a *Psub-Nwell* junction to induce a transient current in it flowing from V_{DD} to G_{ND}.

The *Psub-Nwell* junction is always reversed biased and has a larger area than that of a transistor drain (the parameter S in (1)). Thus, it is no surprising that the authors of [9] reported on experimental basis that the transient current component flowing directly from V_{DD} to G_{ND} (IP_{Psub_nwell} in Fig. 1) may be more than an order of magnitude greater than those flowing in the drains of the sensitive transistors (I_{Ph} in Fig. 1). This transient V_{DD} to G_{ND} current may thus have a significant influence on the laser fault injection mechanism since it will produce a temporary supply voltage drop (IR drop) [9, 14, 27].

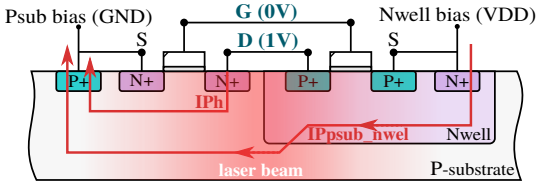


Figure 1: Laser-induced current components. Cross-section of a CMOS inverter.

2.1.2 Spatial Distribution of Laser Beam Energy. The beam diameter is one of the most important propagation attribute of a laser beam in a class of commonly measured parameters (beam diameter, spatial intensity distribution, beam quality factor etc.). A commonly used definition of the laser beam diameter is derived from the bivariate normal distribution of its intensity leading to measure the beam diameter at 86.5% of its maximum value [2], or a drop of $\frac{1}{e^2}$ from its peak value.

The effects of a Near Infrared laser beam have been modeled in [20] and later in [25]. In the latter work, it is shown that the induced photocurrent, which is spatially distributed as a bivariate normal distribution, has a peak amplitude I_{ph_peak} that follows the empirical equation:

$$I_{Ph\_peak} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \qquad (1)$$

where V is the reverse-biased voltage of the exposed PN junction, a and b are constants that depend on the laser power, $\alpha_{gauss(x,y)}$ is a term related to the bivariate distribution of the laser beam amplitude in space, $Pulse_w$ is a term allowing to take into account the laser pulse duration and S is the area of the PN junction. One can refer to [25] for additional details of the above parameters.

By way of illustration, Fig. 2 shows a three-dimensional view of the normalized amplitude of a laser spot. Beam intensity at a given coordinate (x,y) represents the amount of power delivered by the laser source at this specific point.

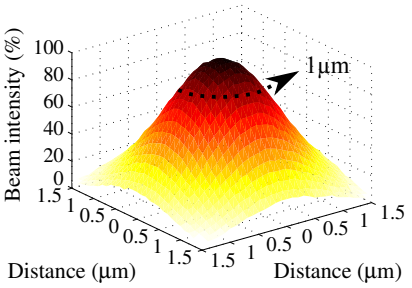


Figure 2: Three-dimensional view of a laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot.

2.1.3 Electrical Model of a Cell Under Laser Illumination. Fig. 3a introduces, in case of an inverter, the classical model showing that the effect of a laser is modeled by a current source placed between the drain and the source of the laser-sensitive transistor (PMOS transistor in this example). Fig. 3b shows, in case of an inverter, the enhanced electrical model taking into account the laser-induced IP_{Psub_nwell} current. Without the power-grid model (i.e., considering V_{DD} and G_{ND} ideals), it would be impossible to take the current IP_{Psub_nwell} into account. Consequently, the laser-induced IR drop contribution also would not be taken into account during simulations. This work proposes in its flow the use of an Electromigration/IR drop (EMIR) CAD tool to automatically provide the power-grid model for each cell in the circuit.

The current sources in Fig. 3a and Fig. 3b have a profile of a double exponential, such as the one illustrated in Fig. 4. The currents have a peak amplitude defined by (1). Since the parameter S (area of the PN junction) corresponds to the cell's *Nwell* area, thus, the current component IP_{Psub_nwell} is larger than that induced at a sensitive transistor drain (*IPh*) since the drain area is smaller than the *Nwell*'s area (see [9] for an experimental assessment).

The IP_{Psub_nwell} current source is attached to the biasing contacts of the *Nwell* and the $P_{substrate}$ (for standard cells without embedded biasing contacts, the current source is connected to the closest). The various IP_{Psub_nwell} currents add up and flow from V_{DD} to G_{ND} trough the power and ground networks of the device

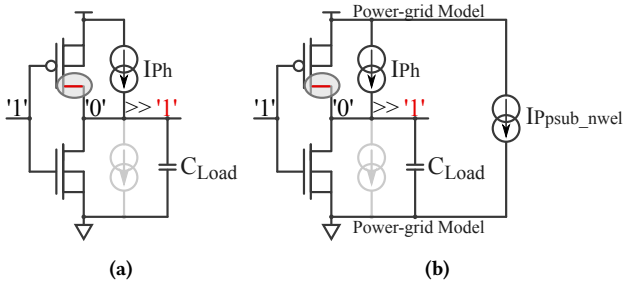


Figure 3: Laser-induced transient fault model applied to an inverter with its input biased at V_{DD}. (a) Classical model. (b) Improved model including the IR drop and ground bounce contribution induced by IP_{Psub_nwell} for a given power-grid model [27].

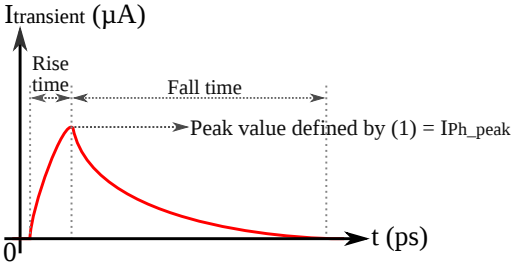


Figure 4: Double exponential profile with current peak defined by (1).

under attack. Because the power grid exhibits both resistive and capacitive electrical behaviors, a local voltage drop and ground bounce occurs thus reducing the voltage swing seen by standard cells in the close vicinity of the laser spot. Considering the above, this paper provides a method based on standard CAD tools to take at chip level the effect of laser-induced IR drops into account.

2.2 Previous Works on Laser Fault Simulation

Laser fault injection may be anticipated or studied by using simulation tools at different abstraction levels: physical, electrical or logical. In this section, previous works that proposed laser fault simulation tools are reviewed in order to justify the need for the methodology presented in this work.

2.2.1 Physical Level. Based on Technology Computer Aided Design (TCAD), the authors in [17] characterize and analyze photoelectric effects induced by static 1064 nm wavelength laser on a 90 nm technology NMOS transistor. In [10], Silicon-Germanium Heterojunction Bipolar Transistor (SiGe HBT) models are used in TCAD to investigate single event transients induced by heavy-ion broadbeam and pulsed-laser sources. Although TCAD is the ultimate tool to simulate laser effects on ICs, this simulator is extremely CPU consuming and can only be applied to individual transistors or small circuit areas.

2.2.2 Logic Level. The authors of [22] proposed a methodology for multiple fault injection at the Register Transfer Level (RTL). The methodology would reduce the fault space of laser fault injection campaigns by using the locality characteristic of laser fault, and through a partitioning of the RTL description of the circuit. Their efforts involve the development of an RTL fault injection approach more representative of laser attacks than random multi bits fault injection. Unfortunately, as a RTL fault simulator, the fault model is defined as a logic pulse with different widths, which is not sufficient to take into account neither the laser parameters nor IR drop effects.

2.2.3 Electrical Level. Laser fault simulation at the electrical level is a good tradeoff between speed (logic level) and accuracy (physical level). Therefore, it is possible to represent the laser physical phenomenon in the scope of a whole system. Although the simulation time might be an issue, today's electrical simulators are up to 100x faster than baseline SPICE simulators without loss of accuracy. Furthermore when large circuits are simulated, it is possible to profit by the use of hybrid simulation in which only the affected zone of the IC is simulated with SPICE accuracy while the non affected cells are simulated with gate level accuracy.

To the extent of our knowledge, the most recent fault simulator at the electrical level was proposed by [19]. Their simulator is based on the open-source Lifting [1], which allows both 0-delay and delay-annotated simulations of digital circuits using layout information to derive the laser spot location. They also use multi-level simulation, trading of speed for accuracy. The major issue with these fault simulators is that they to rely on electrical models [8, 11, 25] that are technology dependent. Even though it is possible to dimension these models, it is hard to obtain accurate results when dealing with new technologies.

For instance, the contribution of IR drop effects play a significant role in the fault injection process as reported in [27]. The authors of [14] modeled a RC network in the power/ground rails to demonstrated the significant contribution of the current induced by vertical parasitic bipolar junctions inherent to MOSFETs in the fault injection process. However, they did not study the effect of the IR drop induced by laser shots, i.e., its impact in the fault injection mechanism. They also did not extended their work beyond the scope of a single inverter since they manually dimensioned the values of the RC components, which would be a difficult task to do for a whole circuit.

2.2.4 Summary. What has been observed so far is that there is a great improvement of laser fault models. However the models were developed at the level of a single gate, ignoring thus the effects of laser-induced IR drops at chip level. Regarding laser fault simulators, they usually use the simple fault model in which current sources are attached to the drain and bulk of laser sensitive transistors [16, 28]. Unfortunately, this fault model was created at a time when laser sources with 1 μm to 5 μm spot diameter were used to target only one sensitive PN junction at the same time. For advanced technologies this model is questionable. For a 28 nm technology, the standard cells have a height value of about 1.2μm, meaning that even lasers with 1 μm spot diameter will also illuminate the *Psub-Nwell* junction (see Fig. 1) and thus induce significant IR drop in the area surrounding the laser spot.

In order to use a fault model that takes into account the IR drop contribution induced by the current component created between the *Psub-Nwell* junction, it is necessary to model by a RC network

the power/ground rails. Modeling the RC network of a large circuit is not a task to be performed manually. In view of this limitation, i.e., that current laser fault simulators do not use complete and accurate fault models, we propose a fault simulation methodology that uses an EMIR CAD tool to automatically provide the RC network of the power/ground rails for a given design. It also provides the transient voltage that propagates along the power rails as a result of the IP_{Psub_nwell} current. The methodology can be used for any circuit designed in any technology supported by the standard CAD tools. Next section presents in details the proposed methodology.

3 PROPOSED METHODOLOGY FOR LASER FAULT SIMULATION

The diagram presented in Fig. 5 proposes a step by step simulation methodology that makes it possible to simulate laser fault injection in large scale circuits. This methodology, which is based on standard CAD tools (Cadence Voltus^{TM} [5] for EMIR simulation and Cadence Spectre XPS [4] for the electrical and hybrid simulation), allows to analyze the impact of laser shots on complex circuits by drawing laser-induced fault sensitivity maps.

The methodology can be easily adapted to provide other set of results besides the ones reported in this work. As far as we know, this is the first methodology able to simulate laser effects on ICs that takes into account laser-induced IR drop effects. Although Cadence tools were used, any other tools that are able to perform IR drop analysis and SPICE like simulations can be used. Fig. 5 is subdivided in numbers that represent each step described in the following sections.

3.1 Step 1: defining simulation parameters

In the first step, a shell script file (main.scr) defines parameters characterizing the laser shot. Among them, one can find: the laser beam diameter, the duration of the laser shot, the time at which begins the laser shot with regard to the operation of the IC, the (X,Y) displacement step of the laser spot when one aims to draw fault sensitivity maps (detailed in step 5), etc. This file is also responsible for calling the necessary tools and scripts for the correct execution of the simulation flow.

3.2 Step 2: data preparation for the EMIR CAD tool

Most of the inputs that are inside the dashed rectangle "EMIR CAD Tool" of Fig. 5 are files that were automatically generated by the design CAD tool (Cadence Innovus [3]). Other files were obtained from the design kit of the technology. It is out of scope of this work to explain each of these files in detail. It suffices to say that they are necessary to model the RC network in the power/ground rails and perform IR drop analysis in Cadence Voltus^{TM}, both necessary for the accomplishment of the proposed methodology.

3.3 Step 3: spatial location of the laser spot

In this step it is necessary to know the dimension of the design and the number of simulated laser shots that are going to be applied over the circuit. For this work, an ARM 7 with a 110 μm × 70 μm area was used (more details are provided in Section 4). If a

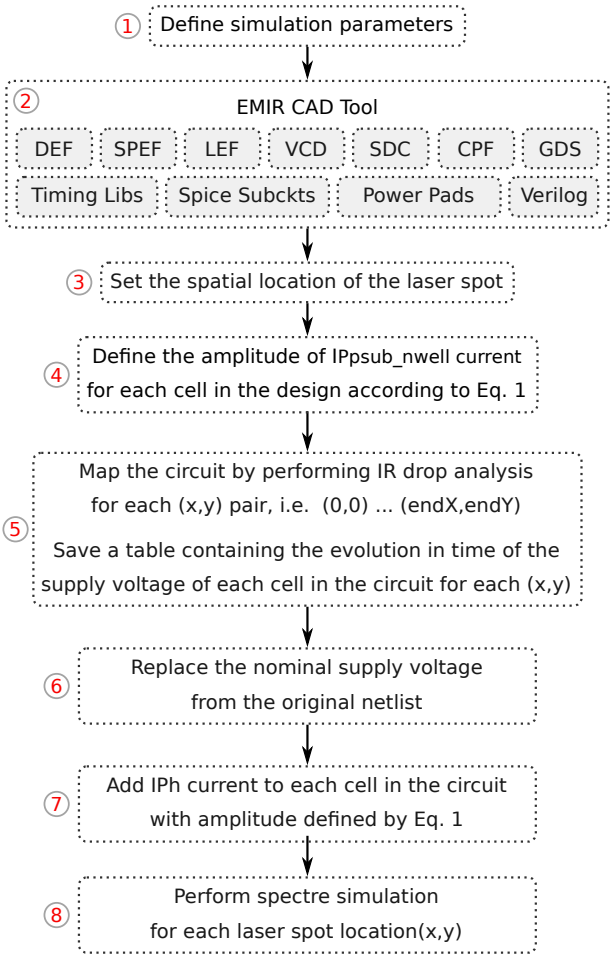


Figure 5: Procedure used to draw laser-induced fault sensitivity maps using the proposed methodology.

displacement step of x, y: 5μm is set, then, in order to sweep the whole circuit, beginning at x, y: $(0, 0)$ and ending at x, y: $(110, 70)$, it would demand 345 laser shots as illustrate in Fig. 6.

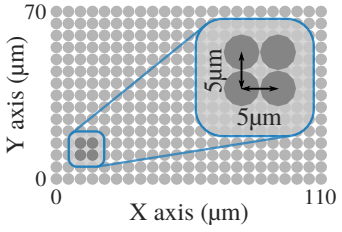


Figure 6: Spatial location of the laser spots. Each point corresponds to a laser shot at different positions (each point corresponds to a simulation).

This step allows to know where the laser spot illuminates the IC during each simulation. Next step shows which cells are illuminated by the laser spot for each x, y position and at which intensity.

3.4 Step 4: laser-induced fault injection

Faults induced by laser illumination can be simulated by specifying the current amplitude of the current sources that compose the laser-induced transient fault model (Fig. 3) of each standard cell in the circuit. Therefore, to simulate a circuit being attacked by means of laser fault injection it is necessary to know which cells will be affected by the laser.

Several ways can be adopted in order to discover the values to be assigned to the current sources in the fault model (Fig. 3). This methodology benefits from a feature present in Cadence Voltus^{TM}. This tool allows to apply an amount of current to a defined region, in this way, several small rectangular regions are defined and the current amplitude of that region follows the spatial distribution of the laser-induced photocurrent defined by (1). Fig. 7 illustrates how the rectangular regions can be used in order to apply the laser power (current induced by the laser) to each rectangle.

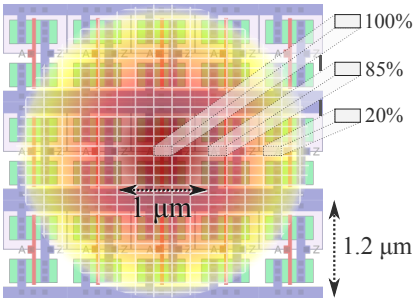


Figure 7: Laser-induced current regions applied over standard cells of a CMOS 28 nm technology. The current amplitude of each region is defined by (1).

The following code example represents the characterization of a rectangle (current region) located at the center of the laser spot (Fig. 7). Therefore its I_{ph_peak} is maximum, 100% or 1 mA for this example. The double exponential has a step size of 5 ps, the peak is thus found at it apex, i.e., 1.510ns, considering 10 ps of rise time and fault starting at 1.500 ns. Other parameters such as capacitances are extracted from .lib and .spi files of the technology for each affected cell. The resolution of each rectangle is 250 nm as shown by the last parameter: -region "x1 y1 x2 y2". The dimension of the rectangle can be changed according to the precision needed to model the laser spot.

```
create_current_region -current {1.500ns 0.000mA
1.505ns 0.820mA 1.510ns 1.000mA 1.515ns 0.950mA
... 1.800ns 0.000mA} -layer M2 -intrinsic_cap C
-loading_cap C -region "1.50 1.50 1.75 1.75"
```

3.5 Step 5: mapping the circuit

In this step, Cadence Voltus^{TM} is used with the purpose to perform laser-induced IR drop simulations for the different laser spot locations calculated during step 3. All other simulation parameters being kept constant (spot diameter, intensity, etc.).

Clarifying, IR drop can be defined as the power supply noise induced by currents flowing through the resistive parasitic elements of the power distribution network. In this work, the laser-induced IR drop is also considered, meaning that the laser-induced current will accumulate with the dynamic current of a cell, thus increasing its IR drop while the laser is active ($IP_{Psub\_nwell} \neq \emptyset$).

For each iteration of this step, a table containing the evolution in time of each cell's voltage swing amplitude (V_{DD}-G_{ND}) is saved for future analysis since different cells are affected by the laser shot. It is also possible to save a table with the dynamic current in time, which translates directly to the amplitude of the current IP_{Psub_nwell} for each cell in the circuit. Table 1 illustrates for three different cells the remaining voltage swing when the laser effect reaches its apex (peak of the double exponential transient current from Fig. 4).

Table 1: List of cells of the circuit with their voltage swing at the apex of the laser shot.

Spot pos. 1 Voltage Swing	Spot pos. 2 Voltage Swing	Spot pos. 10 Voltage Swing
U232 0.619 V	U232 0.689 V	U232 0.926 V
U132 0.620 V	U132 0.678 V	U132 0.905 V
U271 0.621 V	U271 0.695 V	U271 0.932 V

Note in this example that, for the laser spot position 1 (cf. Table 1) the cells are more affected (lower voltage swing) as the epicenter of the laser spot is closer to these three cells. For laser spot positions 2 and 10, the cells are less affected since the epicenter of the laser spot is far away from the cells listed in the table.

3.6 Step 6: inserting IP_{Psub_nwell}

The IP_{Psub_nwell} current component induces voltage drops in the power/ground rails. This effect is captured thanks to Cadence Voltus^{TM} in the previous steps. In this step a shell script replaces the ideal V_{DD} and G_{ND} in the original SPICE netlist by waveforms saved in step 5 for each cell in the circuit.

3.7 Step 7: inserting I_{ph}

A shell script is used in order to add a current source between the drain and bulk of PMOS and NMOS transistors. It models the laser-induced currents that may turn into faults. Note that only one of these current sources are activated depending on which drain's PN junction is reversely polarized. For this, it was necessary to run a fault free electrical simulation and save a golden table with all inputs and outputs of each cell as a function of time.

Knowing that the IP_{Psub_nwell} current is defined as a $factor \times I_{ph}$ because of the parameter S in (1), it is possible to compute the $factor$ value to be applied to each cell by analyzing the .lef file of each cell and to estimate the area of the affected PN junction of the transistor's drain as well as the $Nwell$ of the same cell.

3.8 Step 8: electrical/hybrid fault simulation

At this point, electrical simulations are performed for each laser shot with different locations as defined on step 3. Electrical simulations are time consuming depending mainly on the circuit's size and available computing resources. To circumvent this drawback, a hybrid simulation has to be performed. This simulation defines a region of the circuit where only the most affected cells are simulated with SPICE accuracy. For the hybrid simulation, Cadence Spectre XPS simulator is used. To define the cells that are going to be simulated at logical level, a threshold voltage is defined based on the V_{DD}-G_{ND} (IR drop + ground bounce) values provided by Table 2. If a cell's power/ground voltage is close to the nominal V_{DD} and G_{ND}, it is considered that this cell is not affected by the laser shot, since it is far away from the epicenter of the laser spot. For example, if a threshold voltage of 10% of the nominal V_{DD} = 1 V is defined, then all cells with IR drop + ground bounce lower than 100 mV are simulated at the logic abstraction level.

Table 2 shows the number of cells simulated with the logic abstraction level for different threshold voltages and different spot locations. The spot locations were selected by chance with the purpose to show that the number of affected cells changed depending on the location where the laser shot was applied.

Table 2: Number of cells simulated with the logic abstraction level for different threshold voltages and different spot locations. (5.21k cells in the circuit.)

Threshold (IR drop + bounce)	No. of cells (spot loc. 1)	No. of cells (spot loc. 2)
10%	2535	2625
15%	4510	4585
20%	4641	4620

4 LASER FAULT SIMULATION RESULTS

4.1 Testbench

In order to simulate the effects of laser-induced faults on complex systems, simulations were performed for different circuits, however only results for an ARM 7 processor (DUT) are shown in details. All circuits were synthesized using a 28 nm technology. The core nominal voltage of the DUT is 1 V and the clock period is 1 ns. The DUT has an area equal to 110 $\mu m \times 70\ \mu m$.

4.1.1 Circuit Inventory. The evaluated design is composed by 5.21 k cells, 5.34 k nets and 90 k nodes. The power-grid model generated by Cadence Voltus^{TM} has 100 k resistors and 90 k capacitors.

4.1.2 Laser Spot Diameter. Typical laser sources used to produce faults are characterized by a beam diameter equal to 1 μm, 5 μm or 20 μm and a wavelength of 1064 nm. Although the minimum diameter of a laser spot is 1 μm, given the laws of optic its effect area extends far beyond [7, 23]. Consequently, a laser spot does not induce a single transient current in a single cell, but several transient currents at different sensitive nodes of the target. Without loss of generality, a spot diameter of 1 μm has been chosen for the experiments reported below.

4.2 Simulation Performance

The performance of the simulation depends directly on the available computing resources and the complexity of the simulated circuit. The available processor used to perform simulations was an Intel Xeon E5630 @ 2.53 GHz with two cores and 16 GB of RAM. Since the proposed method deals with the simulation of laser-induced fault injection, other factors should be also taken into account, such as the laser spot diameter, its power and the duration of the laser shot. Considering the simulation performed using only Spectre accuracy, the simulation takes more time to be performed when comparing to the simulation of the same circuit in a fault free scenario. This happens as the cells no longer have ideal V_{DD} and G_{ND}, thus the simulator has to decrease the simulation step to account with laser-induced transient currents, which are in the ps range. Therefore, since the diameter of the laser spot determines how many cells are affected, it influences on the time required by the simulator to perform necessary calculations. When using hybrid simulation, it is possible to decrease the amount of cells simulated with Spectre accuracy, thus reducing simulation time.

Table 3 shows simulation times for different circuits using Spectre XPS (hybrid simulation). Simulation times for other simulators (Spectre accuracy only) are not shown as they take at least 22 times more to simulate. Simulations were also performed using Spectre and Spectre APS with the intention to compare results regarding the accuracy of Spectre XPS. In all cases the results were the same, i.e., the same sensitivity maps presented in the next section were obtained. In fact, for this kind of analysis there is no need to have the same precision as simulations for RF designs, in which the Spectre RF simulator is recommended.

Table 3: Simulation performance for different circuits regarding one point of the fault sensitivity map (1 simulation out of 345 simulations to create a complete map).

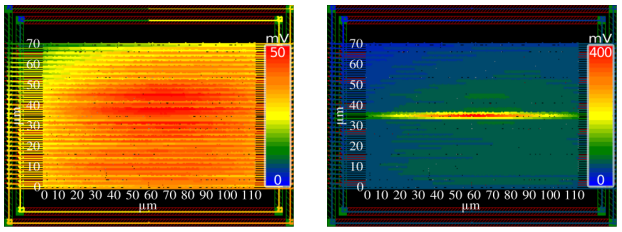
Circuit	No. of cells	Simulation time
Arm7	5.210	1min 02s
S38584 (ISCAS'89)	20.705	1min 20s
B18 (ITC'99)	52.601	3min 05s
B19 (ITC'99)	105.344	6min 35s

4.3 Laser Propagation on the Circuit Surface

To illustrate how the IR drop propagates in the circuit, refer to Fig. 8a and Fig. 8b. In Fig. 8a, for which no laser effect is considered, the IR drop across the rails reach the maximum of 50 mV. In this figure, the voltage drop is uniquely due to normal switching activity. Even though not fully uniform, the IR drop affects almost the whole circuit. Fig. 8b (obtained in step 5 of the proposed method) illustrates how the laser effect propagates in the circuit. In presence of a single laser shot with a spot diameter of 1 μm at coordinates x=60 μm, y=35 μm, the effect area extends along the X axis of the power-grid main metal lines for more than 100 μm (the effect area has a

shape that is stretched horizontally along the power supply rails as they provide a propagation path to the laser-induced IR drop and ground bounce). Whereas its extension along the Y axis is only approximately 3 μm, i.e., three times the laser spot diameter. The peak value of the induced voltage transient in the power lines is 400 mV (Fig. 8b). At this time, the voltage swing is reduced to 600 mV. This value is far below the nominal core voltage of 1 V. Thus laser-induced IR drop may induce faults in the circuit, such as timing errors or even data disruption.

There are hundreds of standard cells inside the area affected by the laser when considering a 28 nm technology, meaning that the cells inside the affected area will absorb the laser-induced current according to the surface distribution of the laser beam given by 1.



(a) (b)

Figure 8: ARM 7 layout with 5k+ instances: (a) Maximum voltage drop (IR-Drop + ground bounce) in normal operation condition. (b) Maximum voltage drop in presence of a laser shot with spot diameter equal 1μm.

4.4 Simulated Scenarios

We report a total of 4 simulated scenarios among the ones studied. They are illustrated in Fig. 9 that shows in the first line the clock signal waveform used as a time reference. The two other lines give the typical evolutions observed during simulations, of the signal Q_x, the output of the cell 'x' of the design under illumination, in two different situations. These two situations represent the behavior when a laser pulse with 250 ps duration starts at 1.5 ns and 1.7 ns respectively. These times are thus closer and closer to the next rising clock edge that occurs at 2 ns.

The second line of Fig. 9 gives these evolutions when only the I_{Ph} current sources with a double exponential shape are considered to model laser effects. In the third line, the curve has a smoother double exponential waveform when comparing with the profile of double exponential current pulse (c.f. second line) proposed by [20] due to the filtering effect (RC effect) of the supply voltage network. In fact, the profile proposed by [20] aims to model alpha-particle hits, which does not exactly correspond to charge generation and collection in PN junctions excited with pulsed infrared lasers as analyzed in [15].

4.5 Fault Injection Maps

For the purpose of assessing the contribution of laser-induced faults into the circuit, we drew fault sensitivity maps on simulation basis for different areas (considering the model presented in Section 2.1.3). These simulations were performed for locations of the laser spot

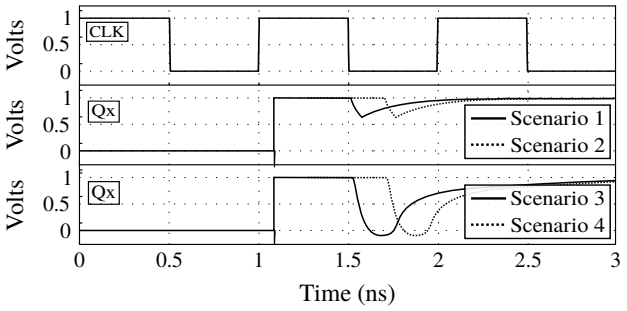


Figure 9: Typical waveforms observed during simulations at the output of gates illuminated by a laser beam. Line 1: clock signal. Line 2: waveforms observed when considering I_{Ph} contribution only. Line 3: waveforms observed when considering I_{Ph} + IP_{Psub_nwell} contributions.

sweeping the whole circuit area (110 μm x 70 μm) with X and Y displacement steps of 5 μm, resulting in 345 simulations for each figure (each dot location is that of a simulated laser shot). Fig. 10 reports the fault maps for which the model presented in Section 2.1.3 is used (i.e. with the power-grid model provided by the EMIR CAD tool). The red dots correspond to the occurrence of a fault (soft-error) and blue dots the absence of faults. Only bit-flip faults were considered, i.e. faults corresponding to the flipping (with reference to normal operation) of the output state of one or more flip-flops.

4.5.1 Contribution of $\mathbf{I_{ph}}$. Fig. 10a and Fig. 10b report simulations performed considering only the influence of I_{Ph} (laser-induced IR-drops are ignored). Having the transient current profile a width of 250 ps, when this current is applied at 1.5 ns and 1.7 ns, i.e., closer to the flip-flop sampling window (time window of width $t_{setup} + t_{hold}$ centered on the rising edge), more faults are observed.

4.5.2 Contribution of $\mathbf{I_{ph}}$ *and* $\mathbf{IP_{Psub\_nwell}}$. Fig. 10c and Fig. 10d report fault maps for which I_{Ph}, IP_{Psub_nwell} and the power-grid model are considered (scenarios 3 and 4). By comparison to the first line, it reveals that the fault areas are larger than expected for the considered laser shot times. It also unveiled an extension of the laser sensitivity in time, in which the number of faults are increased respectively by a factor of 2.6 and 3.1 for the laser applied at 1.5 ns and 1.7 ns. This demonstrates that IR drops induced by laser shots play an important role in the occurrence of faults. Not taking this effect into account leads to over optimistic results regarding the threshold of fault injection.

5 CONCLUSIONS

This paper presented a new method that allows to simulate laser-induced faults at the electrical level in large-scale circuits by using standard CAD tools. Its main intent is to take into account the IR drop effects induced by laser shots: a key parameter in the fault injection process. For each cell in the circuit, a high accuracy electrical fault model that includes the voltage drop effects in the power and ground rails was used thanks to the use of an EMIR CAD tool. The method was applied to a test-chip in order to demonstrate how

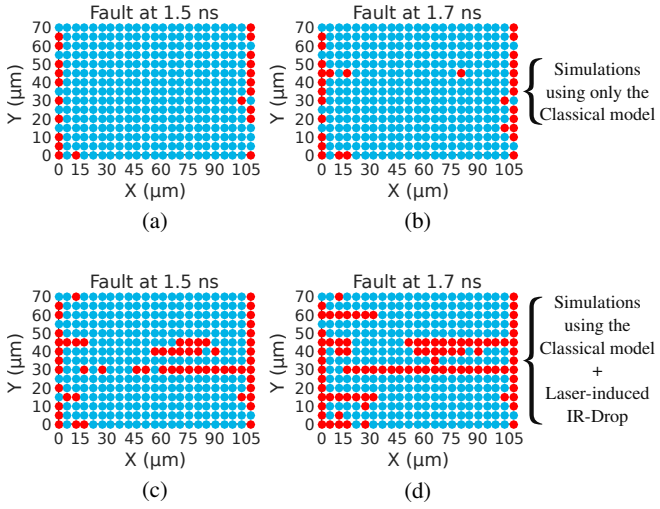


Figure 10: Maps of laser-induced faults for the simulated scenarios: (a-b) laser applied at 1.5 ns and 1.7 ns respectively, considering I_{Ph} contribution only. (c-d) laser applied at 1.5 ns and 1.7 ns respectively, considering I_{Ph} + IP_{Psub_nwell} contributions.

fault sensitivity maps can be drawn with the purpose of assessing the contribution of laser-induced faults into the circuit.

REFERENCES

[1] A. Bosio and G. D. Natale. 2008. LIFTING: A Flexible Open-Source Fault Simulator. In *2008 17th Asian Test Symposium*. 35–40. https://doi.org/10.1109/ATS.2008.17

[2] S.P. Buchner, F. Miller, V. Pouget, and D.P. McMorrow. 2013. Pulsed-Laser Testing for Single-Event Effects Investigations. *IEEE Transactions on Nuclear Science* (2013). https://doi.org/10.1109/TNS.2013.2255312

[3] Cadence. 2017. Innovus Implementation System. (2017). Retrieved December 3, 2017 from https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/hierarchical-design-and-floorplanning/innovus-implementation-system.html

[4] Cadence. 2017. Spectre eXtensive Partitioning Simulator. (2017). Retrieved December 3, 2017 from https://www.cadence.com/content/cadence-www/global/en_US/home/tools/custom-ic-analog-rf-design/circuit-simulation/spectre-extensive-partitioning-simulator-xps.html

[5] Cadence. 2017. Voltus IC Power Integrity Solution. (2017). Retrieved December 3, 2017 from https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/silicon-signoff/voltus-ic-power-integrity-solution.html

[6] Hungse Cha, E. M. Rudnick, J. H. Patel, R. K. Iyer, and G. S. Choi. 1996. A gate-level simulation environment for alpha-particle-induced transient faults. *IEEE Trans. Comput.* 45, 11 (Nov 1996), 1248–1256. https://doi.org/10.1109/12.544481

[7] F. Darracq, H. Lapuyade, N. Buard, F. Mounsi, B. Foucher, P. Fouillat, M. C. Calvet, and R. Dufayel. 2002. Backside SEU laser testing for commercial off-the-shelf SRAMs. *IEEE Transactions on Nuclear Science* (2002). https://doi.org/10.1109/TNS.2002.805393

[8] A. Douin, V. Pouget, D. Lewis, P. Fouillat, and P. Perdu. 2005. Electrical modeling for laser testing with different pulse durations. In *11th IEEE IOLTS*. 9–13. https://doi.org/10.1109/IOLTS.2005.27

[9] Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre, Giorgio Di Natale, and Alexandre Sarafianos. 2014. Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS. *Microelectronics Reliability* 54 (Sept. 2014), 2289 – 2294. https://doi.org/10.1016/j.microrel.2014.07.151

[10] Z. E. Fleetwood, N. E. Lourenco, A. Ildefonso, J. H. Warner, M. T. Wachter, J. M. Hales, G. N. Tzintzarov, N. J. H. Roche, A. Khachatrian, S. P. Buchner, D. McMorrow, P. Paki, and J. D. Cressler. 2017. Using TCAD Modeling to Compare Heavy-Ion and Laser-Induced Single Event Transients in SiGe HBTs. *IEEE Transactions on Nuclear Science* 64, 1 (Jan 2017), 398–405. https://doi.org/10.1109/TNS.2016.2637322

[11] C. Godlewski, V. Pouget, D. Lewis, and Mathieu Lisart. 2009. Electrical modeling of the effect of beam profile for pulsed laser fault injection. *Microelectronics Reliability* (Aug. 2009).

[12] G. S. Greenstein and J. H. Patel. 1992. E-PROOFS: A CMOS bridging fault simulator. In *1992 IEEE/ACM International Conference on Computer-Aided Design*. 268–271. https://doi.org/10.1109/ICCAD.1992.279362

[13] D. H. Habing. 1965. The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits. *IEEE Transactions on Nuclear Science* 12, 5 (Oct 1965), 91–100. https://doi.org/10.1109/TNS.1965.4323904

[14] Laurent Hériveaux, Jessy Clédière, and Stéphanie Anceau. 2013. Electrical Modeling of the Effect of Photoelectric Laser Fault Injection on Bulk CMOS Design. In *39th ISTFA ASM*.

[15] A. H. Johnston. 1993. Charge generation and collection in p-n junctions excited with pulsed infrared lasers. *IEEE Trans. Nucl. Sci.* (1993). https://doi.org/10.1109/23.273491

[16] A. G. Jordan and A. G. Milnes. 1960. Photoeffect on diffused P-N junctions with integral field gradients. *IRE Transactions on Electron Devices* 7, 4 (Oct 1960), 242–251. https://doi.org/10.1109/T-ED.1960.14688

[17] R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, G. Haller, V. Pouget, D. Lewis, J. M. Dutertre, and A. Tria. 2012. Characterization and TCAD simulation of 90 nm technology transistors under continous photoelectric laser stimulation for failure analysis improvement. In *2012 19th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits*. 1–6. https://doi.org/10.1109/IPFA.2012.6306298

[18] F. Lu, G. Di Natale, M. L. Flottes, and B. Rouzeyre. 2013. Laser-Induced Fault Simulation. In *2013 Euromicro Conference on Digital System Design*.

[19] F. Lu, G. D. Natale, M. L. Flottes, B. Rouzeyre, and G. Hubert. 2014. Layout-aware laser fault injection simulation and modeling: From physical level to gate level. In *2014 9th IEEE International Conference on Design Technology of Integrated Systems in Nanoscale Era (DTIS)*. 1–6. https://doi.org/10.1109/DTIS.2014.6850665

[20] G. C. Messenger. 1982. Collection of Charge on Junction Nodes from Ion Tracks. *IEEE Transactions on Nuclear Science* (1982). https://doi.org/10.1109/TNS.1982.4336490

[21] W. Meyer and R. Camposano. 1995. Active timing multilevel fault-simulation with switch-level accuracy. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 14, 10 (Oct 1995). https://doi.org/10.1109/43.466340

[22] A. Papadimitriou, D. Hély, V. Beroulle, P. Maistri, and R. Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*. 1–4. https://doi.org/10.7873/DATE.2014.219

[23] C. Roscian, A. Sarafianos, J. M. Dutertre, and A. Tria. 2013. Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells. In *FDTC, 2013 Workshop on*. 89–98. https://doi.org/10.1109/FDTC.2013.17

[24] M. B. Santos and J. P. Teixeira. 1999. Defect-oriented mixed-level fault simulation of digital systems-on-a-chip using HDL. In *Design, Automation and Test in Europe Conference and Exhibition, 1999. Proceedings (Cat. No. PR00078)*. 549–553. https://doi.org/10.1109/DATE.1999.761181

[25] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J. M. Dutertre, and A. Tria. 2013. Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology. In *IRPS, 2013 IEEE International*. 5B.5.1–5B.5.9. https://doi.org/10.1109/IRPS.2013.6532028

[26] Sergei P. Skorobogatov and Ross J. Anderson. 2002. Optical Fault Induction Attacks. In *4th International Workshop on Cryptographic Hardware and Embedded Systems*. Springer-Verlag, London, UK, 2–12.

[27] R. A. C. Viera, J. M. Dutertre, R. P. Bastos, and P. Maurine. 2017. Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation. In *2017 Euromicro Conference on Digital System Design (DSD)*. 252–259. https://doi.org/10.1109/DSD.2017.43

[28] J. L. Wirth and S. C. Rogers. 1964. The Transient Response of Transistors and Diodes to Ionizing Radiation. *IEEE Transactions on Nuclear Science* 11 (1964).

Appendix C

Article in international journal: Elsevier Microelectronics Reliability 2017

Towards High-Sensitive Built-In Current Sensors Enabling Detection of Radiation-Induced Soft Errors

Raphael de Oliveira Rocha, Frank Sill Torres
Federal University of Minas Gerais
Belo Horizonte, Brazil
franksill@ufmg.br

Rodrigo Possamai Bastos
Univ. Grenoble Alpes, CNRS, TIMA
Grenoble, France
rodrigo.bastos@univ-grenoble-alpes.fr

***Abstract*— Soft error resilience is an increasingly important requirement of integrated circuits realized in CMOS nanometer technologies. Among the several approaches, Bulk Built-in Current Sensors (BBICS) offer a promising solution able to detect particle strikes immediately after its occurrence. Principal challenges for its wide application in common designs are area costs and robustness, both directly related to the sensor's sensitivity. Following this requirement, this work presents strategies enabling the design of high-sensitive BBICS. In detail, we are proposing three approaches based on gate voltage control, body biasing, and stack forcing that can be integrated in all *state-of-the-art* BBICS architectures. In order to verify the feasibility of this approaches, the proposed techniques have been integrated in a modular BBICS realized in a comercial 65 nm technology. Simulation results indicate an increase of the detection sensitivity by up to factor 6, leading to 17 % area overhead, response times around 1 ns, a negligible power penalty, and high robustness against wide variations of temperature and process parameters.**

Keywords*— Built-in current sensors, soft errors, transient faults, reliability

I. Introduction

CMOS remains the dominating technology for integrated circuits, mainly due to its miniaturization capability and high integrability. However, the continuously reduction of technology sizes results in designs that are susceptible to several fault sources like parameter variations [1], oxide breakdown [2], and radiation [3]. In case of the latter, energetic particles inject electrical charge into sensitive regions of the semiconductor devices, creating transient currents that can result in soft errors. For years, researches on radiation-induced soft errors concentrated mainly on memories and application intended for avionics and aerospace environment. However, as current technologies reached nanometer scale, soft error resilience is also required for applications on ground level as well as the combinational parts of the circuits. Several concurrent error detection and/or correction techniques have been presented to circumvent the effects of soft errors. This includes the application of multiple clocking schemes [4], checker-based arithmetic units [5], and selective redundancy [6]. In contrast to gate and system level techniques, Bulk Built-In Current Sensors (BBICS) are a promising approach on transistor level, which enables the detection of radiation-induced particle strikes immediately after its occurrence [7-10]. BBICS offer fast error detection and low cost in terms of power. On the downside, BBICS design is a challenging task, as these sensors tend to be prone to parameter and temperature variations and/or require a considerable amount of area [11-13]. Previous works introduced several different kinds of BBICS architectures, including the single BBICS [14], the modular BBICS [15, 16], the dynamic BBICS [17], a low-leakage BBICS [18], as well as an architecture based on transistors with different threshold voltages [19]. Despite the diversity of BBICS architectures, there is still a demand for further improvements. Principal requirements are reduction of area costs and robustness.

This work presents several new concepts leading to considerable enhanced sensitivity, and thus, to notably improved area costs, response time, and robustness. The proposed techniques can be employed by all reported BBICS architectures turning the results of this work into an important step towards the consolidation of the BBICS approach.

The rest of the paper is organized as follows. Section 2 introduces basic information and the BBICS method, while Section 3 details the new strategies. Section 4 is related to simulation results. Finally, section 5 draws the conclusion.

II. Preliminaries

This section discusses the generation of transient faults induced by radiation on integrated circuits and introduces the BBICS approach.

A. Transient Faults and Soft Errors

Unintentional transient signal variations in integrated circuits are defined as transient faults. A transient fault can turn into a soft error when it propagates to the input of a sampling element or affects directly a node within the sampling element, for example a latch or flip-flop.

There are several sources for transient faults like cross-talk, ground bounce, or radiation-induced energetic particles [20]. The latter are critical for reversed-biased p-n junctions, as it is the case for drain or source regions of transistors in cut-off state. In the event of a particle strike, the electron-hole pair track formed in the path of the energetic particle affects the electrical field in the depletion region to shortly adopt the shape of a funnel towards the substrate [21]. This starts the so-called carrier collection that is observed as transient voltage on the affected node. The subsequent phase of carrier collection is defined by a slower phenomenon in which carriers are conducted through the depletion region due to diffusion. The corresponding current pulse is traditionally modeled by a double-exponential function I_{coll} by following equation [22]:

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

Hereby, Q_{coll} is the total collected charge, and t_r and t_f represent the time constants for the funnel collection and he second phase of carrier collection.

B. BBICS Detecting Transient Faults

The idea behind BBICS is to monitor anomalous currents in the transistor bulk in case of a particle strike [7, 12]. Consequently, it enables the detection of radiation-induced currents that might lead to soft errors.

The principal idea of BBICS shall be introduced with the aid of the modular BBICS (mBBICS) reported in [15]. It consists of functional blocks named as heads and tail (see Fig. 1). The head circuits are connected to the bulk of the monitored devices, *i.e.*, the Block Under Test (BUT) in Fig. 1, and act as sensing elements. The outputs of several heads (wire $\text{head}_{\text{NMOS}}$) are latched by the tail circuit. As most of *state-of-the-art* BBICS, the mBBICS approach comprises a NMOS type able to detect transient faults in NMOS devices and a complementary PMOS version.

Fig. 1 illustrates an NMOS-mBBICS in which the gate of transistor Nh1 is connected to VDD and the drain to the NMOS bulk of the monitored transistors in the BUT. In normal operation, the drain of Nh1 acts as a virtual GND, while the head output (*i.e.*, drain of Nh2) is at VDD level. In case of a particle strike, the fault current in the bulk is conducted through Nh1, resulting in a voltage drop over Nh1 that increases the gate voltage of Nh2. If this voltage exceeds the threshold voltage $v_{th,Nh2}$ of Nh2, this device is switched on and the signal $\text{head}_{\text{NMOS}}$ is pulled down, leading the tail circuit to latch this signal and set an error flag. The circuit remains in this logic state until the reset transistor Pt3 is activated, turning the sensor ready for another detection [15].

The PMOS-mBBICS, which permits the detection of transient faults in PMOS devices, has a complementary behavior and structure and is omitted herein for the sake of simplicity.

The sensitivity of a BBICS relates to the amplitude of a radiation-induced bulk current that can be detected. The amplitude of this current correlates with the collected charge and the capacitive load of the sensor's input [23]. The latter is directly related to the number of monitored devices. Hence, the higher the BBICS's sensitivity the greater the number of devices a single BBICS can monitor and, consequently, the less the area penalty [24].

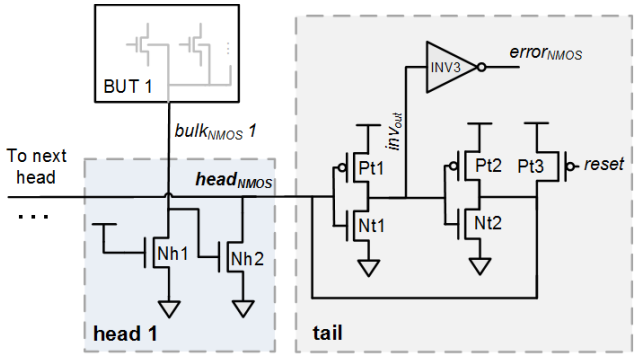


Fig. 1. mBBICS architecture (head + tail, NMOS type) able to detect transient faults in the monitored blocks defined as BUT

Note that the processing of the generated error flag in case of a transient fault is realized on higher abstraction layers and is not discussed in this work. Further information can be found in [25-28].

III. Strategies for Improving BBICS

This section presents the strategies for improving the sensitivity of BBICS architectures, leading to enhanced response time, area costs, and robustness. All techniques are applied exemplarily for the mBBICS architecture. Nevertheless, we would like to emphasize the universality of the approaches for different types of BBICS architectures.

For the sake of simplicity, the discussions relate solely to the NMOS version, but it can be carried over directly to the complementary PMOS type.

A. Adjustable Gate Voltage on Sensing Transistor

A common element of BBICS architectures is the sensing device that converts the bulk current into a voltage signal [12, 17, 18, 29]. In case of the mBBICS, transistor Nh1 is this element (see Fig. 1 and section II.B). At the onset of a particle strike and a resulting bulk current, the voltage drop at the drain of Nh1 must be sufficient to activate Nh2, and thus switching the signal $\text{head}_{\text{NMOS}}$. It is, therefore, desired that the current through Nh1 results into a high voltage drop over Nh1. On the other side, it has to be assured that the bulk voltage must be kept at GND level in fault-free operation mode. Previous BBICS [8, 11, 15, 18] achieved these goals by using a transistor with small W/L ratio that operates in linear mode, *i.e.*, a gate-source voltage equal to VDD. Consequently, the sensor sensitivity can be calibrated by adjusting the gate length of Nh1. This parameter is directly related to the channel resistance, and thus, the voltage drop over Nh1 in case of a fault current. However, this solution turns out to be costly in terms of area.

We propose the application of a minimum sized transistor and adjustable gate voltage as illustrated in Fig. 2. Here, the voltage drop over Nh1 is controlled by the gate-source voltage V_{gs_Nh1} of Nh1, which controls the channel resistance. This solution proved to be area efficient, since it permits the application of a transistor with minimum length and width. Moreover, it also enables sensitivity adjustments during runtime.

It is mandatory to assure that the bulk stays at GND level during normal operation in order to avoid variations of the threshold voltage of the monitored devices due to the body-effect [30]. Hence, it must be ensured that the chosen gate-source voltage allows the passing of noise and bulk leakage currents.

Further, during physical design of the chip, distribution of voltages with values below the supply voltage has to be

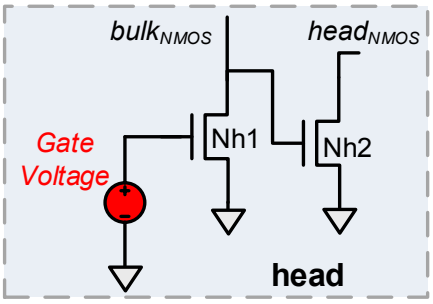


Fig. 2. Adjustable gate voltage applied on sensing transistor

considered. However, this is a common problem and has been tackled in several related work [31, 32].

B. Threshold Voltage Modification via Body-biasing

A further element of the sensing part of BBICS is the transistor that works as a trigger and whose gate input is connected to the bulk [8, 11, 15, 18]. In the event of a particle strike, the voltage drop on the bulk caused by the bulk current that passes the sensing transistor activates the trigger device. In case of the mBBICS, the transistor Nh2 assumes this function (see Fig. 1 and section II.B). It is activated as soon as the bulk voltage crosses Nh2's threshold voltage $v_{th,Nh2}$. In order to achieve high sensitivity it is desired to have a low value for $v_{th,Nh2}$.

The threshold voltage v_{th} of a CMOS device can be modeled with [33]:

$$v_{th} = v_{th0} + \gamma a_1 V_{sb} - \eta a_2 V_{ds} \qquad (2)$$

with v_{th0} is the zero-bias threshold voltage, γ is the body-bias coefficient, a_1 and a_2 label technology constants, η corresponds to the Drain Induced Barrier Lowering (DIBL) coefficient, V_{sb} labels the source-body voltage, and V_{ds} is the drain-source voltage. From equation (2) follows that the threshold voltage also depends on the body voltage, which is known as the aforementioned body-effect [30]. We propose to increase the sensor's sensitivity by biasing the body of Nh2. Thereby, the body terminal is connected to a positive voltage source as illustrated in Fig. 3. Consequently, V_{sb} turns negative leading to reduction of v_{th_Nh2}.

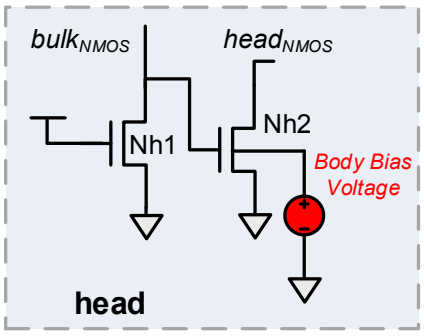


Fig. 3. Body-biasing of the trigger device Nh2

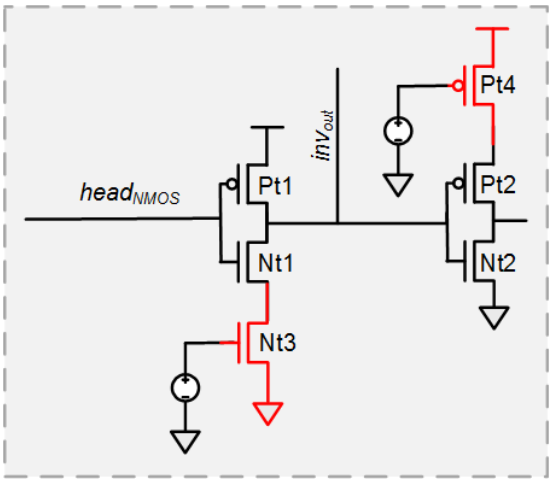


Fig. 4. Stack-forcing in the tail circuits

The downside of this approach is an increasing sub-threshold leakage current I_{sub} due to lower threshold voltage [33]. Also, in order to separate the bulk from the other transistors, Nh2 has to be placed in a separated N-well, leading to higher area costs.

C. Stack-forcing

Most of the reported BBICS architectures apply feedback inverter structures to latch the signal that this generated via the sensing part [11, 12, 18]. Consequently, the performance of this structure is critical for the response time t_{resp} of the sensor.

In case of the mBBICS, the latching is executed in the tail circuits (see Fig. 1 and section II.B). Hence, in order to lower t_{resp}, the signal inv$_{out}$ must perform a fast state transition (0→1) when a particle strike is detected. This way, both inverters INV1 and INV2 created by the transistors Nt1/Pt1 and Nt2/Pt2 should have switching voltages that favor a 0→1 transition of inv$_{out}$ as well as a 1→0 transition of head$_{NMOS}$ (see Fig. 1). Consequently, the channel resistances of Nt1 and Pt2 should be higher than their counterparts in the inverters. This goal can be achieved by decreasing the W/L ratio of both devices. However, this leads to higher input capacitances that, consequently, increase the capacitive load of both inverters resulting in higher t_{resp}.

We propose the addition of a stacked device in row with Nt1 and Pt2, respectively (see Fig. 4). The gate of both stacked transistors is connected to a voltage source, which assures that both devices operate in linear mode. This configuration leads to higher resistance of the pull-down path in INV1 and the pull-up paths in INV2 at constant input capacitances. Hereby, the increase of the path resistance follows on the one hand from the additional channel resistance due to the stacked device. Additionally, the increased potential of the source of Nt1 as well as Pt2 results in higher threshold voltages due to elevated source-body voltage V_{sb}, which increases the body-effect (see equation 2).

IV. Analysis

This section presents the simulation results of the proposed improvement strategies. All techniques have been applied exemplarily for the mBBICS architecture [15].

A. Test Environment

The tests were based on a commercial 65 nm technology, with triple-well option and a supply voltage of 1.2 V. Chains of ten minimum sized inverters consisting of low threshold transistors (L_{drawn} = 60 nm, W_{drawn_NMOS} = 200 nm, W_{drawn_PMOS} = 280 nm) implemented in a triple-well form the circuits to be monitored. The bulks of all devices of an inverter chain are connected to one head circuit. Hereby, NMOS devices are connected to a NMOS type mBBICS and PMOS devices to a PMOS type mBBICS. Moreover, several chains can be connected to a single head circuit. Each tail block is connected to six head blocks, following the results of previous works [15, 16]. It should be noted that the sensors circuits are located outside the well regions of the monitored devices.

B. Sizing and Voltage levels

Following discussions relate to the NMOS type mBBICS but can easily be adopted for the complementary PMOS type.

Table I lists the results of the sizing process, which was executed based on an iterative method similar to the one proposed in [34]. Notable outcomes of this step are the minimum sizes of Nh1 and the high W/L ratio of Nh2 in the head circuits (see Fig. 2). The first results from the proposed reduced gate voltage, while the latter follows from the requirement to have a high discharge current of the $head_{NMOS}$ in case of a detection.

Further, the devices in the tail circuits have been sized to favor a 0→1 transition of the signal inv_{out} (Fig. 4). Consequently, Pt1 received a high W/L ratio, while Nt1 is minimum sized. Likewise, the devices Pt2/Nt2 should provide a fast 1→0 transition of $head_{NMOS}$, *i.e.*, Pt2 should be minimum sized and Nt2 should have a high W/L ratio. However, during our analysis we could observe that the leakage through Nt2 is critical as it discharges the node $head_{NMOS}$. Therefore, Nt2 is minimum sized, leading to lower leakage. Alternatively, high-V_{th} devices could be applied [29]. Further, the devices utilized for stack-forcing, *i.e.*, Nt3 and Pt4 (see Fig. 4 and III.C), are sized with very low W/L ratio leading to high channel resistances. Finally, the reset device Pt3 possesses a slightly increased width in order to restore the $head_{NMOS}$ to VDD in reasonable time. Also, the inverter INV3 is minimum sized.

TABLE I. Transistor sizes in nm for the applied mBBICS whereas the 1st number indicates the width and the 2nd the length

NMOS		PMOS	
Name	**Size**	**Name**	**Size**
Nh1	135/65	Ph1	135/65
Nh2	810/65	Ph2	945/65
Pt1	540/65	Pt1	135/65
Nt1	135/65	Nt1	675/65
Nt3	135/325	Pt3	135/650
Pt2	135/65	Pt2	135/65
Nt2	135/260	Nt2	135/65
Pt4	135/1300	Nt4	135/1300
Pt3	270/65	Nt3	200/65

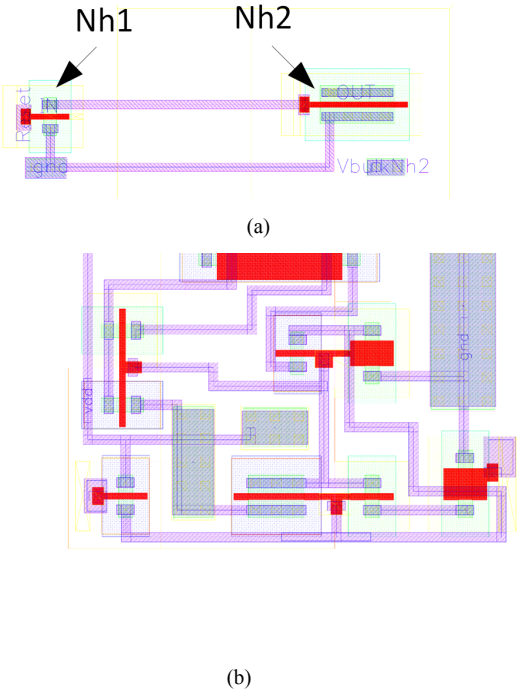


Fig. 5. Layouts of NMOS type mBBICS (a) head and (b) tail

TABLE II. Voltage levels applied to the mBBICS circuits

NMOS		PMOS	
Voltage	**Value**	**Voltage**	**Value**
V_{gate_Nh1}	0 mV	V_{gate_Ph1}	1.2 V
V_{body_Nh2}	700 mV	V_{body_Ph2}	500 mV
V_{gate_Pt4}	700 mV	V_{gate_Pt3}	500 mV
V_{gate_Nt3}	500 mV	V_{gate_Nt4}	400 mV

Table II lists the results of the determination of the voltage levels. It includes the gate voltages V_{gate} of Nh1 in the head circuit (see Fig. 2) and the stacked transistors in the tails (see Fig. 4), as well as the voltage V_{body_Nh2} of the bulk terminal of Nh2 (see Fig. 3). With exception of V_{gate_Nh1} and V_{gate_Ph1} all voltages have been defined via an iterative method similar to the one proposed in [34].

As detailed in sub-section III.A, the gate voltage V_{gate_Nh1} of Nh1 should be as small as possible, but must be high enough to assure that the bulk remains at GND level. Therefore, the design was operated for 1 s in normal mode, *i.e.*, no strike current was applied, while the bulk was monitored. It could be determined that even for V_{gate_Nh1} = GND the bulk continuously staid at GND level.

In order to determine the exact area costs for each sensor, all blocks have been implemented as layout (see Fig. 5). Table III lists the sizes of the head and tail blocks of each

TABLE III. LAYOUT SIZES OF MBBICS BLOCKS AND INVERTER (DESIGEND IN 65 NM TECHNOLOGY)

	NMOS	PMOS	INV
Head	13.4 µm²	5.9 µm²	-
Tail	14.3 µm²	15.7 µm²	-
Head + 6 tails	94.7 µm²	51.4 µm²	-
Cell area	-	-	3.5 µm²

types, the area of a set of six heads and a tail and the cell area of a minimum sized inverter.

C. Characterization

The proposed sensor was submitted to simulations in order to analyze its detection sensitivity and response time for typical conditions, *i.e.*, temperature Temp = 25 °C and typical process corners.

In a first attempt, we determined the minimum charge that leads to a transient fault at the output of the inverter chain. Therefore, a particle strike was simulated by a current pulse based on equation (1) with adjustable Q_{coll} at the output node of the 9th inverter of the chain. All injected transient currents were defined with t_r = 1 ps and t_f = 10 ps to keep the typical shapes of transient faults: short rise time and longer fall time [35, 36]. A transition fault was registered when the output voltage of the chain crossed VDD/2.

The estimated values are Q_{coll} = 3.15 fC for particle strikes in a NMOS device and Q_{coll} = 3.5 fC in case of a PMOS transistor. Next, the response time for increasing amount of monitored inverter chains per head was analyzed. This analysis considers that the voltage peak on the bulk, which activates the device Nh2 in case of a particle strike, depends on the amount of monitored transistors [23]. The simulations had been realized for NMOS and PMOS type mBBICS with the Q_{coll} that results in a transition fault in the corresponding circuit.

The results shown in Table III indicate that the NMOS type mBBICS has a response time lower than 1 ns for up to 50 monitored inverters, while the PMOS type mBBICS achieves a similar response time for only 40 inverters. This difference can be explained by the greater width of the PMOS transistors ($W_{drawn\_NMOS}/W_{drawn\_PMOS}$ = 200 nm / 280 nm), which leads to higher capacitive load on the bulk.

TABLE IV. NUMBER OF MONITORED INVS VS. RESPONSE TIME

NMOS (Q_{coll} = 3.15 fC)		**PMOS** (Q_{coll} = 3.5 fC)	
N° INV	t_{resp} [ns]	N° INV	t_{resp} [ns]
10	0.24	10	0.45
20	0.27	20	0.50
30	0.35	30	0.66
40	0.54	40	1.04
50	0.94	50	2.08
60	1.74	60	9.56
70	3.35		
80	8.10		

TABLE V. DETECTION CAPABILITY OF THE PROPOSED BBICS. TF INDICATES THE OCCURRENCE OF A TRANSIENT FAULT, DTCN INDICATES WHETHER THE ERROR FLAG WAS SET.

	NMOS (50 INV)			PMOS (40 INV)		
Q_{coll} (fC)	TF	DTCN	t_{resp} [ns]	TF	DTCN	t_{resp} (ns)
1.8	No	×	-	No	×	-
2.0	No	✓	6.2	No	×	-
2.3	No	✓	3.14	No	×	-
2.5	No	✓	2.03	No	✓	11.64
2.7	No	✓	1.44	No	✓	3.15
3	No	✓	1.09	No	✓	2.03
3.2	**Yes**	✓	**0.86**	No	✓	1.49
3.4	**Yes**	✓	**0.71**	No	✓	1.20
3.6	**Yes**	✓	**0.60**	**Yes**	✓	**1.06**
3.8	**Yes**	✓	**0.53**	**Yes**	✓	**0.88**
4.0	**Yes**	✓	**0.47**	**Yes**	✓	**0.80**
4.3	**Yes**	✓	**0.43**	**Yes**	✓	**0.72**
4.5	**Yes**	✓	**0.40**	**Yes**	✓	**0.67**

Next, it was analyzed the sensitivity of the proposed mBBICS for different values of the collected charge Q_{coll}. Therefore, the NMOS type mBBICS was monitoring 50 inverters, while the PMOS version was connected to 40 inverters. As can be concluded from Table IV, an increase of Q_{coll} leads to a reduction of the response time t_{resp}. This is an expected result, as larger collected charges result in higher bulk currents (see also equation 1).

However, the results in Table V also reveal that the proposed mBBICS is more sensitive than required, *i.e.*, it indicates a transition fault even if the collected charge is not sufficient for changing the output signal of the inverter chain. Depending on high layer processing, this false detection might lead to a performance penalty of the integrated design. It is up to the designer to trade-off the sensitivity with the sensor's robustness against variations.

Fig. 6 depicts the area penalty and maximum response time in relation to the number of inverters monitored by a NMOS and PMOS type mBBICS pair. It had been considered that a tail connects to six heads [15]. The results indicate that the monitoring of 40 to 60 inverters per head leads to an area penalty between 10 to 20 %, while the related maximum response time is between 1 to 2 ns.

TABLE VI. RESPONSE TIME VERSUS TEMPERATURE

	NMOS type mBBICS *(Q_{coll} = 3.2 fC, 50 INV)*	**PMOS** type mBBICS *(Q_{coll} = 3.6 fC, 40 INV)*
Temp [°C]	**t_{resp} [ns]**	**t_{resp} [ns]**
-55	No detection	1.50
-20	1.26	1.26
0	1.05	1.16
25	0.86	1.06
50	0.80	0.98
75	0.67	0.91
90	0.60	0.87
125	no detection	0.76

Finally, the cost in power consumption was estimated for a configuration of 40 monitored inverters per NMOS/PMOS mBBICS pair. Therefore, the chains were simulated for a frequency of 1 GHz and an activity of 20 %. The increase of the power dissipation due to the application of mBBICS was estimated with 0.3 %.

D. Robustness Analysis

In this work, we define robustness as resilience against environmental influences, e.g., temperature fluctuations, and technological factors, e.g., process variations.

In order to determine the impact of environmental factors, we studied the impact of the temperature on the response time t_{resp} of the proposed sensor. Therefore, the NMOS type mBBICS was simulated with 50 inverters and Q_{coll} = 3.2 fC, while the PMOS version was simulated with 40 inverters and Q_{coll} = 3.6 fC. The devices sizes of each sensor are taken from Table I.

The results listed in Table VI indicate that the NMOS type mBBICS could not detect transient faults for temperatures lower than -20 ºC and higher than 90 ºC. In contrast, the PMOS type mBBICS proved to work over the complete analyzed temperature range of -55 ºC to 125 ºC. The reduction of t_{resp} with increasing temperature follows mainly from the inverse

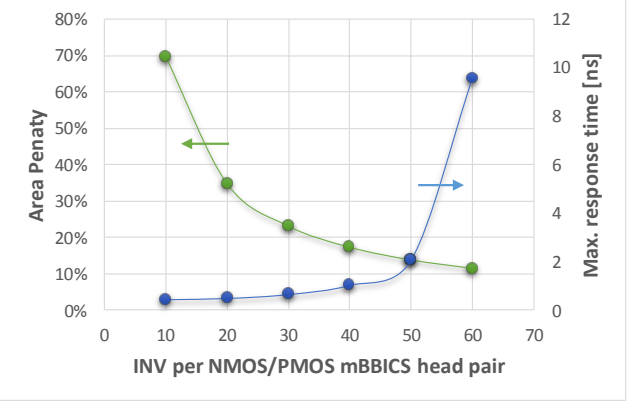


Fig. 6. Area penalty and maximum response time versus number of monitored inverters per NMOS/PMOS mBBICS pair (one tail per six heads)

TABLE VII. RESPONSE TIME FOR DIFFERENT PROCESS CORNERS AND MONTE-CARLO SIMULATIONS

	t_{resp} [ns] of **NMOS** type *(Q_{coll} = 3.2 fC, 50 INV)*	t_{resp} [ns] of **PMOS** type *(Q_{coll} = 3.6 fC, 40 INV)*
FF	0.33	0.55
FS	0.50	1.57
SF	1.85	0.76
SS	4.20	2.24
MC (3σ)	3.75	2.01

relation between temperature and transistors threshold voltage [37]. Thus, at higher temperatures $v_{th,Nh2}$ decreases, which results in lower t_{resp} (see also sections II and III).

Next, the impact of process variations on the response time was analyzed. Therefore, following corner cases, which are offered by the chosen technology, had been selected: fast-fast (FF), slow-slow (SS), fast-slow (FS) and slow-fast (SF), whereas the first term relates to the NMOS devices and the second to the PMOS ones. Further, for each sensor 1000 Monte-Carlo simulations have been executed and the 3σ-delay was determined [38]. The latter refers to the maximum delay over 99.86 % of all simulations. In call cases, the temperature was set to 25 ºC.

The results are listed in Table VII. It follows that in all cases the sensors could detect a transient fault. Although, it was only in FF and FS process corners (for NMOS type mBBICS) and FF and SF (for PMOS type mBBICS) that the fault could be detected in less than 1 ns. The higher response times for the corners SF (NMOS) and FS (PMOS) as well as for the Monte-Carlo simulations follow from the impact of Nh2 and Ph2 on t_{resp} (see also III.B).

E. Comparsion with related works

In a final step, the proposed mBBICS was compared to its unmodified version, similar to the one presented in [15]. Therefore, the sensor was implemented with the recommended parameters reported in [15] and the values for Q_{coll} were set such that a transient fault occurred in the monitored inverter chains. The simulation results indicated that the unmodified sensor could solely monitor 10 inverters per head (NMOS and PMOS type). Hence, the proposed modifications increased the sensor's sensitivity by factor 6, in case of the PMOS type, and factor 8 for the NMOS type sensors. The response times are with 0.36 ns for the NMOS and 0.67 ns for the PMOS type roughly 50 % lower than for the modified version. Differences to the results in [15] follow from the applied technologies, as a predictive 16 nm technology was chosen.

Table VIII compares the results of the proposed sensor to reported BBICS. The table list the area and power penalty to the monitored circuits, the minimum collected charge Q_{coll} that could be detected and the related rise time t_r, as well as the applied technology. It should be noted that, following from equation (1), the smaller Q_{coll} and the pulse width the lower the detection capability of the sensor. The comparison indicates that the proposed sensor offers an auspicious relation between detection sensitivity and area offset in comparison to the applied technology.

TABLE IX. COMPARISON OF HARDWARE APPROACHES FOR SOFT ERROR DETECTION (SED)

Name / Ref.	Area penalty	Delay penalty	SED Capability
Transient detection on Flip-Flops [40, 41]	44 %	25 %	Partial
Time redundancy [39]	0 %	96 %	Partial
Duplication with comparison [42]	112 %	0 %	Full
This work	17 %	0 %	Full

Table IX compares the presented sensor with hardware approaches for soft error detection in terms of area and delay penalty as well as the capability to detect all soft errors. The techniques Transient detection on Flip-Flops and Time redundancy are not able to detect all soft errors, as both do not consider soft errors that last longer than a clock period [39, 40]. It can be noted, that the proposed sensor has, compared to related approaches, a considerable area overhead and stands out with the absence of any delay penalty.

V. CONCLUSIONS

The application of Bulk Built-In Current Sensors (BBICS) is a promising solution to cope with increasing problems due to soft errors in nanometer technologies. However, these sensors demand high detection sensitivity in order to detect required level of collected charges, fast response times, high robustness against variations and reasonable area penalty. The proposed modification for BBICS include adjustable voltage of the sensing transistors, body-biasing, and stack forcing to mitigate these problems. Simulations of a modified sensor in a comercial 65 nm technology indicated that the proposed sensor could detect all injected transition faults with response times close to 1 ns for the nominal case, and near 4 ns under wide process and temperature variations. This could be achieved with a reasonable area offset of 17 % and very low increase in power dissipation. Further, in comparison to the unmodified version of the sensor, the sensitivity could be increased by up to factor 6, while the response time decreased by more than 50 %. It should be noted, that the proposed design strategies are applicable on all *state-of-the-art* BBICS architectures.

VI. ACKNOWLEDGMENTS

We gratefully thank CAPES, CNPq, and FAPEMIG for the financial support.

TABLE VIII. COMPARISON TO STATE-OF-THE-ART BBICS ARCHITECTURES

Name / Ref.	Area penalty	Power penalty	Min Q_{coll}	t_r / t_f	Technology
BBICS [7]	29 %	Not reported	3.4 fC	5 / 10 ps	100 nm
S-BBICS [11]	23 %	+26 %	7.5 fC	50 / 150 ps	32 nm
DynBBICS [8]	18 %	Not reported	55 fC	2 / 50 ps	130 nm
mBBICS_16nm [15]	25 %	4 %	2 fC	1 / 5 ps	16 nm
mBBICS_65nm (this work)	70 %	2 %	3.2 fC	1 / 10 ps	65 nm
This work	17 %	0.3%	2 fC	1 / 10 ps	65 nm

VII. REFERENCES

[1] O. S. Unsal, J. W. Tschanz, K. Bowman, V. De, X. Vera, A. Gonzalez, *et al.*, "Impact of parameter variations on circuits and microarchitecture," *IEEE Micro,* vol. 26, pp. 30-39, Nov-Dec 2006.

[2] J. Srinivasan, S. V. Adve, P. Bose, and J. A. Rivers, "The impact of technology scaling on lifetime reliability," in *Dependable Systems and Networks, 2004 International Conference on*, 2004, pp. 177-186.

[3] 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,* vol. 1, pp. 128-143, Apr-Jun 2004.

[4] N. D. P. Avirneni and A. K. Somani, "Low Overhead Soft Error Mitigation Techniques for High-Performance and Aggressive Designs," *Ieee Transactions on Computers,* vol. 61, pp. 488-501, Apr 2012.

[5] S. Pontarelli, P. Reviriego, C. J. Bleakley, and J. A. Maestro, "Low Complexity Concurrent Error Detection for Complex Multiplication," *Ieee Transactions on Computers,* vol. 62, pp. 1899-1903, Sep 2013.

[6] S. N. Pagliarini, G. G. dos Santos, L. A. D. Naviner, and J. F. Naviner, "Exploring the feasibility of selective hardening for combinational logic," *Microelectronics Reliability,* vol. 52, pp. 1843-1847, Sep-Oct 2012.

[7] E. H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. L. Kastensmidt, "Using bulk built-in current sensors to detect soft errors," *IEEE Micro,* vol. 26, pp. 10-18, Sep-Oct 2006.

[8] A. Simionovski and G. Wirth, "Simulation Evaluation of an Implemented Set of Complementary Bulk Built-In Current Sensors With Dynamic Storage Cell," *IEEE Transactions on Device and Materials Reliability,* vol. 14, pp. 255-261, Mar 2014.

[9] G. Wirth, "Bulk built in current sensors for single event transient detection in deep-submicron technologies," *Microelectronics Reliability,* vol. 48, pp. 710-715, May 2008.

[10] F. Vargas and M. Nicolaidis, "SEU-tolerant SRAM design based on current monitoring," in *Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., Twenty-Fourth International Symposium on*, 1994, pp. 106-115.

[11] R. P. Bastos, F. S. Torres, J. M. Dutertre, M. L. Flottes, G. Di Natale, and B. Rouzeyre, "A Single Built-in Sensor to Check Pull-up and Pull-down CMOS Networks against Transient Faults," presented at the 23rd International Workshop on Power and Timing Modeling, Optimization and Simulation (Patmos), 2013.

[12] E. H. Neto, F. L. Kastensmidt, and G. Wirth, "Tbulk-BICS: A Built-In Current Sensor Robust to Process and Temperature Variations for Soft Error Detection," *IEEE Transactions on Nuclear Science,* vol. 55, pp. 2281-2288, Aug 2008.

[13] Z. Zhang, T. Wang, L. Chen, and J. Yang, "A new Bulk Built-In Current Sensing circuit for single-event transient detection," in *Electrical and Computer Engineering (CCECE), 2010 23rd Canadian Conference on*, 2010, pp. 1-4.

[14] R. P. Bastos, J. M. Dutertre, and F. S. Torres, "Comparison of bulk built-in current sensors in terms of transient-fault detection sensitivity," in *CMOS Variability (VARI), 2014 5th European Workshop on*, 2014, pp. 1-6.

[15] F. Sill Torres and R. Possamai Bastos, "Detection of Transient Faults in Nanometer Technologies by using Modular Built-In Current Sensors," *Integrated Circuits and Systems, Journal of* vol. 8, pp. 89-97, 2013.

[16] F. Sill Torres and R. P. Bastos, "Robust modular Bulk Built-in Current Sensors for detection of transient faults," in *Integrated Circuits and Systems Design (SBCCI), 2012 25th Symposium on*, 2012, pp. 1-6.

[17] A. Simionovski and G. Wirth, "Adding a self-reset feature to the Bulk-BICS with dynamic storage cell," *Microelectronics Reliability,* vol. 55, pp. 2748-2753, 12// 2015.

[18] Z. Zhang, Y. Ren, L. Chen, N. J. Gaspard, A. F. Witulski, T. W. Holman, *et al.*, "A Bulk Built-In Voltage Sensor to Detect Physical Location of Single-Event Transients," *Journal of Electronic Testing,* vol. 29, pp. 249-253, 2013// 2013.

[19] J. M. Dutertre, R. Possamai Bastos, O. Potin, M. L. Flottes, B. Rouzeyre, and G. Di Natale, "Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection," *Microelectronics Reliability,* vol. 53, pp. 1320-1324, 9// 2013.

[20] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolić, *Digital integrated circuits : a design perspective*, 2nd ed. Upper Saddle River, N.J.: Pearson Education, 2003.
[21] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," *IEEE Transactions on Device and Materials Reliability,* vol. 5, pp. 305-316, Sep 2005.
[22] G. C. Messenger, "Collection of Charge on Junction Nodes from Ion Tracks," *IEEE Transactions on Nuclear Science,* vol. 29, pp. 2024-2031, 1982.
[23] J. G. M. Melo and F. Sill Torres, "Exploration of Noise Impact on Integrated Bulk Current Sensors," *Journal of Electronic Testing,* vol. 32, pp. 163-173, 2016.
[24] M. V. Guimarães and F. S. Torres, "Automatic layout integration of Bulk Built-In Current Sensors for detection of soft errors," in *2016 29th Symposium on Integrated Circuits and Systems Design (SBCCI)*, 2016, pp. 1-6.
[25] M. Nicolaidis, *Soft errors in modern electronic systems*. New York: Springer, 2011.
[26] R. P. Bastos, G. Di Natale, M. L. Flottes, and B. Rouzeyre, "How to sample results of concurrent error detection schemes in transient fault scenarios?," in *Radiation and Its Effects on Components and Systems (RADECS), 2011 12th European Conference on*, 2011, pp. 635-642.
[27] I. Wagner and V. Bertacco, *Post-Silicon and Runtime Verification for Modern Processors*: Springer Publishing Company, Incorporated, 2010.
[28] F. Leite, T. Balen, M. Herve, M. Lubaszewski, and G. Wirth, "Using Bulk Built-In Current Sensors and Recomputing Techniques to Mitigate Transient Faults in Microprocessors," *Latw: 2009 10th Latin American Test Workshop,* pp. 147-152, 2009.
[29] J. M. Dutertre, R. Possamai Bastos, O. Potin, M. L. Flottes, B. Rouzeyre, G. Di Natale*, et al.*, "Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS," *Microelectronics Reliability,* vol. 54, pp. 2289-2294, 9// 2014.
[30] S. M. Sze and K. K. Ng, *Physics of semiconductor devices*, 3rd ed. Hoboken, N.J.: Wiley-Interscience, 2007.
[31] M. Blagojević, M. Cochet, B. Keller, P. Flatresse, A. Vladimirescu, and B. Nikolić, "A fast, flexible, positive and negative adaptive body-bias generator in 28nm FDSOI," in *2016 IEEE Symposium on VLSI Circuits (VLSI-Circuits)*, 2016, pp. 1-2.
[32] D. Jacquet, F. Hasbani, P. Flatresse, R. Wilson, F. Arnaud, G. Cesana*, et al.*, "A 3 GHz Dual Core Processor ARM Cortex TM -A9 in 28 nm UTBB FD-SOI CMOS With Ultra-Wide Voltage Range and Energy Efficiency Optimization," *IEEE Journal of Solid-State Circuits,* vol. 49, pp. 812-826, 2014.
[33] S. Hu, et. al., "Berkeley short channel IGFET model," Dpt. of EECS, University of California, Berkeley2005.
[34] R. Possamai Bastos, F. Sill Torres, G. Di Natale, M. Flottes, and B. Rouzeyre, "Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode," *Microelectronics Reliability,* vol. 52, pp. 1781-1786, 9// 2012.
[35] P. E. Dodd, M. R. Shaneyfelt, J. A. Felix, and J. R. Schwank, "Production and propagation of single-event transients in high-speed digital logic ICs," *IEEE Transactions on Nuclear Science,* vol. 51, pp. 3278-3284, 2004.
[36] V. Ferlet-Cavrois, P. Paillet, M. Gaillardin, D. Lambert, J. Baggio, J. R. Schwank*, 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,* vol. 53, pp. 3242-3252, 2006.
[37] F. Sill, J. You, and D. Timmermann, "Design of mixed gates for leakage reduction," presented at the Proceedings of the 17th ACM Great Lakes symposium on VLSI, Stresa-Lago Maggiore, Italy, 2007.
[38] T. McConaghy, K. Breen, J. Dyck, and A. Gupta, "3-Sigma Verification and Design," in *Variation-Aware Design of Custom Integrated Circuits: A Hands-on Field Guide: A Hands-on Field Guide*, ed New York, NY: Springer New York, 2013, pp. 65-114.
[39] D. Sabena, M. S. Reorda, L. Sterpone, P. Rech, and L. Carro, "On the evaluation of soft-errors detection techniques for GPGPUs," in *2013 8th IEEE Design and Test Symposium*, 2013, pp. 1-6.
[40] D. Ernst, S. Das, S. Lee, D. Blaauw, T. Austin, T. Mudge*, et al.*, "Razor: Circuit-level correction of timing errors for low-power operation," *IEEE Micro,* vol. 24, pp. 10-20, Nov-Dec 2004.
[41] B. Liu, "Error-detecting/correcting-code-based self-checked/corrected/timed circuits," in *2010 NASA/ESA Conference on Adaptive Hardware and Systems*, 2010, pp. 66-72.
[42] C. Frenkel, J. D. Legat, and D. Bol, "Comparative analysis of redundancy schemes for soft-error detection in low-cost space applications," in *2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, 2016, pp. 1-6.

Appendix D

Article awarded in international IEEE/ACM conference: SBCCI 2016

Late Protocols for Smaller, Faster, and Energy-Efficient Asynchronous Pipelines

Jean Simatic, Abdelkarim Cherkaoui, Rodrigo Possamai Bastos, and Laurent Fesquet
Univ. Grenoble Alpes, Grenoble INP, CNRS, TIMA Laboratory, F-38031 Grenoble, France
Email: {*First name*}.{*Last name*}@univ-grenoble-alpes.fr

***Abstract*—Asynchronous design is an interesting alternative for low-power digital systems. To improve the performances of bundled-data asynchronous circuits, this paper investigates the class of asynchronous protocols that use the falling edge of the request wire to indicate data validity, also called late protocols. We show that late protocols gains in area and energy increase with the length of the critical path. The throughput of the protocol Maximus, one of the two new protocols presented, remains remarkably high even when the pipeline is almost full.**

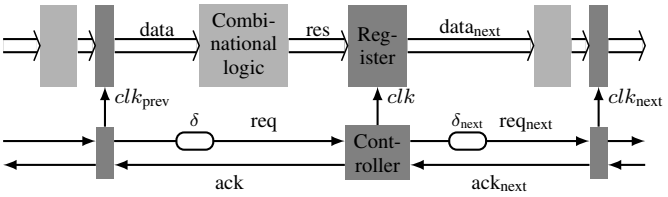
I. Introduction

Asynchronous circuits are a promising solution to design modular circuits with low electromagnetic emissions and high tolerance to variations [1]. These characteristics come from each data transfer being a local transaction between registers. Asynchronous registers communicate through channels that explicitly notifies the destination register of the arrival of new data (requests) and the source register of the liberation of the channel (acknowledgments). In bundled-data (BD) circuits (Figure 1a), each channel consists in data wires, which are similar to synchronous ones, and two handshake wires for the requests and acknowledgments.

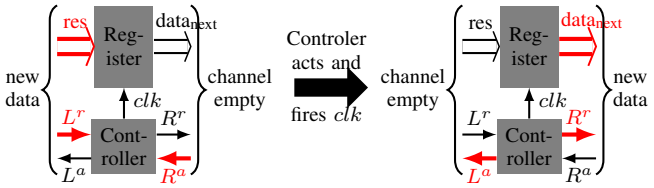
At the interface of channels, each register is associated with an asynchronous controller. As Figure 1b shows, the controller waits until there are new data on the input channel (L for left) and no data on the output channel (R for right). Then, the controller fires the local clock clk, thus filling the R channel and emptying the L one.

In practice, the state of the channel (full or empty) is coded by the handshake wires. The asynchronous controllers order the transitions (rising or falling edges) of these wires so that the channel state follows correctly the data movements, hence the name 'bundled-data'. These relative ordering constraints of the transitions on the handshake wires is called protocol.

When using flip-flops as registers, there are three kinds of protocols (Figure 2), called signaling conventions [2]. Firstly, in the 2-phase protocol, the data is considered valid after both the rising and falling edges of the request. A controller implementing the 2-phase protocol is simple but requires dual-edge triggered flip-flops. Secondly, the early (and broad) protocols use the rising edge of the request wire to notify new data arrivals. All 137 early protocols [3], [4] are penalized by the return-to-zero (RZ) phase, during which the channel needs to return to its idle state without transmitting any data. Finally, the late protocols, three of which are known [5]–[7], use the falling edge of the request wire to notify new data. By having a working phase instead of a RZ, late protocols allow higher throughput at the cost of more complex controllers [6], [7].



(a) Structure of an asynchronous bundled-data pipeline. Local handshake signals (requests and acknowledgments) manage data transfers.



(b) Action of an asynchronous controller. It acts when there are new data from the previous stage (request on L^r) and the next stage is ready to receive new data (acknowledgment on R^a). Then, the controller fires the local clock clk to capture data, notifies the next controller for incoming data (request on R^r) and to the preceding one for its readiness to receive new data (acknowledgment on L^a).

Figure 1. Bundled-data 3-stage pipeline.

This paper highlights the improvements of the area, and energy efficiency of BD pipelines brought by late protocols, and the caveats of existing ones (Section II). Section IV proposes the two new late protocols, Late-capture and Maximus, that increase the decoupling of previously proposed ones. Sections V and VI compare the proposed protocols and present a performance metric to rank controllers depending on the operation conditions. To the best of our knowledge, Maximus is also the first late protocol which could not be used with an early convention. Thus, asynchronous protocols is proven still to be an open question.

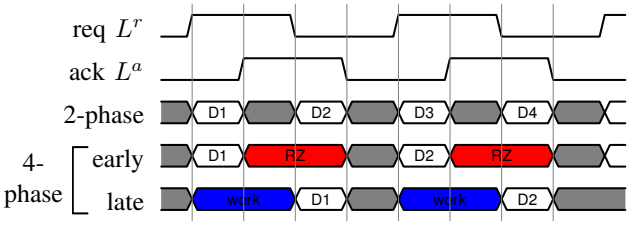
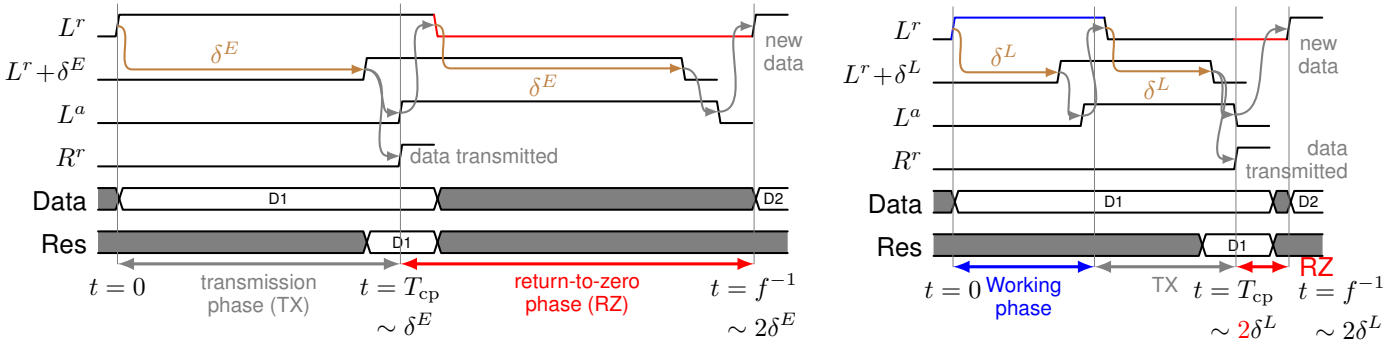


Figure 2. Possible signaling conventions [2]. Channels are empty in the grey zones.



(a) Early protocols. The long RZ phase is due to the propagation of the fall of the request wire through the DE δ^E. This RZ time is a synchronization overhead hindering the pipeline throughput.

(b) Late protocols. The RZ is shorter as the falling edge $L^r\searrow$ has already gone through the DE.

Figure 3. Timing of the transmisssion of one data item. T_{cp} is the length of the critical path of the current stage. Arrows indicate ordering constraints.

II. Asymptotic evaluation of the interest of late protocols : area, energy, and throughput

In order to meet the setup constraints, delay elements (DEs) (denoted δ in Figure 1a) have to be inserted on the request wires. The request has indeed to reach the destination controller *after* the data has reached the destination register (BD constraint). This sections shows that, as the length of the critical path T_{cp} increases, the required size of DE δ is smaller for late protocols than for early ones (resulting in better surface and energy consumption). Also, the throughput of the stage (denoted f) decreases less in the case of late protocols.

For the sake of clarity, delays in the controller are considered negligible compared to δ in this section. Simulation results in Section VI however take into account all delays.

A. Performance of early protocols : the return-to-zero burden

As Figure 3a shows, 'Data' start propagating from the previous stage when L^r rises. After a time δ^E, the rising edge has gone through the DE and reaches the current controller. With an early protocol, this rising edge notifies the arrival of the data. Hence, the BD constraint imposes $\delta^E > T_{\text{cp}}$.

After the transmission is done, the channel must returns to zero before accepting new data : the transmission is acknowledged ($L^a\nearrow$), the request wire falls ($L^r\searrow$ and then $L^r+\delta^E\searrow$). Therefore, $T_{\text{rz}} > \delta^E$. As a result, the throughput f^E of the stage verifies (1).

$$f^E < f^E_{\max} = \frac{1}{2\delta^E} \sim \frac{1}{2T_{\text{cp}}} \tag{1}$$

The best case scenario, $T_{\text{rz}} = \delta^E$, is achieved when the left channel (L) is decoupled from the right channel (R), i.e. when L can return to zero without waiting for R. In non-decoupled protocols (*e.g.* the 'simple' protocol [8]), $T_{\text{rz}} = \max(\delta^E, \delta^E_{\text{next}})$, where δ^E_{next} is the length of the next stage's DE.

This means that for a critical path of $T_{\text{cp}} = 2\,\text{ns}$, the maximum achievable throughput is $250\,\text{MHz}$. The throughput can be improved by using decoupled controllers *and* asymmetric DEs, which allow the falling edge of the request to go through the DE faster than the rising edge. However, both decoupled controllers and asymmetric DEs lead to larger circuits and higher energy consumption.

B. Performance of late protocols: putting return-to-zero to work

As for the early protocols, 'Data' starts propagating when L^r rises (Figure 3b). Also similarly, after a time δ^L, the rising edge has gone through the DE and reaches the destination controller. Unlike the early case, the data 'Res' do not need to be arrived yet at the end of this working phase.

Then the rising edge of the request wire ($L^r + \delta^L\nearrow$) is acknowledged by $L^a\nearrow$. The request wire goes down ($L^r\searrow$). After a time δ^L, this falling edge reaches the controller. With a late protocol, this falling edge notifies the arrival of the data. Hence, the BD constraint imposes $2\delta^L > T_{\text{cp}}$.

After the transmission is done, the channel returns to zero before accepting new data. The RZ is nevertheless shorter than for an early protocol : the transmission is acknowledged by a single falling edge ($L^a\searrow$). Therefore, $T_{\text{rz}} > 0$. As a result, the throughput f^L verifies (2).

$$f^L < f^L_{\max} = \frac{1}{2\delta^L} \sim \frac{1}{T_{\text{cp}}} \tag{2}$$

As for early protocols, the best case scenario, $T_{\text{rz}} = 0$, is achieved with decoupled protocols. In non-decoupled protocols such as CUSA [5], $T_{\text{rz}} = \delta^L_{\text{prev}} + \delta^L_{\text{next}}$, where δ^L_{prev} and δ^L_{next} are respectively the lengths of the DEs of the previous and next stages.

In conclusion, the shortening the RZ phase allows late protocols to have higher throughput ($f^L_{\max} \sim 2f^E_{\max}$). Also, thanks to the working phase, late protocols also requires inserting smaller DEs ($\delta^L \sim \delta^E/2$). These smaller DEs save area and energy.

III. Decoupling-based classification of existing late protocols

Decoupling is a key factor of the controller throughput. Therefore, decoupling is at the base of all generic classifications of protocols.

Most frameworks are dedicated to early protocols. Either the works propose constraints to ensure functional early protocols, list the possible compliant protocols and order them by decoupling [8], [9]. Or the early protocol offering a maximal concurrency (the least coupling) serves as a seed from which

all others protocols are exhaustively obtained by successive transformations that reduce the concurrency [3], [4].

To the best of our knowledge, only three late protocols have been proposed: CUSA by David [5], Burst-mode by Yun, Beerel and Arceo [6], and Early-ack by Mannakkara and Yoneda [7]. All three protocols have a common operating mode shown in Figure 4, but have different decoupling. Figure 5 shows the relationships between their respective decoupling: CUSA is less decoupled than Burst-mode, which is itself less decoupled than Early-ack. Note that Early-ack requires additional timing assumptions to operate correctly.

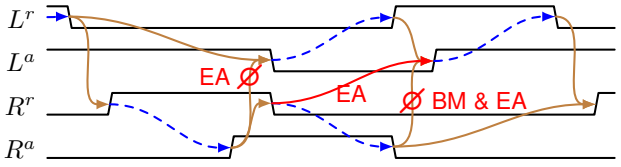


Figure 4. Ordering of transitions for controllers implementing existing late protocols. Arrows represent ordering constraints between the transitions. In particular, dotted arrows are responses of the rest of the pipeline to the controllers actions (solid arrows).

The waveform of Figure 4 specify a protocol by using arrows that define relative ordering constraints between the transitions: the transition at the arrow head must occur after the transition at its tail. For the sake of readability, this formalism is prefered to the usual STG specification [10]. We used the latter to get the formal expression of the RZ times.

1) CUSA: The protocol represented by Figure 4 is CUSA, the least decoupled of the three existing late protocols. After the request arrives ($L^r\searrow$), a new handshake is initiated on the R channel ($R^r\nearrow$). Then, the controller waits for a rising edge on the acknowledgment wire ($R^a\nearrow$) to acknowledge the data on the L channel ($L^a\searrow$) and send the request on the R channel ($R^r\searrow$), and so on.

2) Burst-mode: The Burst-mode protocol decouples the $L^a\nearrow$ transition by removing the $R^a\searrow\rightarrow L^a\nearrow$ dependency of CUSA.

3) Early-ack: The Early-ack protocol decouples the $L^a\searrow$ transition (by removing the $R^a\nearrow\rightarrow L^a\searrow$ dependency) and increases concurrency (by replacing $R^a\searrow\rightarrow L^a\nearrow$ by $R^r\searrow\rightarrow L^a\nearrow$). This data sequence requires however a fast propagation of the request falling edge ($R^r\searrow\overset{\delta_{\text{next}}}{\rightarrow} L^r_{\text{next}}\searrow\rightarrow R^r_{\text{next}}\nearrow$), otherwise new data could be accepted ($R^r\searrow\rightarrow L^a\nearrow\rightarrow L^r\searrow\rightarrow R^r\nearrow$) before the next stage reads the current one. As the latter path goes through no DE, the DE δ_{next} on the former path must be asymmetric and have a short falling delay.

IV. Proposed late protocols and positioning with respect to the existing ones

Due to their couplings, the existing protocols CUSA and Burs-mode do not reach the minimum RZ time ($T_{\text{rz}} = \delta_{\text{prev}} + \delta_{\text{next}}$ for CUSA and $T_{\text{rz}} = \delta_{\text{next}}$ for Burst-mode). Although, the protocol Early-ack has a negligible RZ time, Early-ack requires asymmetric DEs which prevent from halving the length of the DEs. To solve these issues, we add two new protocols to the existing family of late protocols (Figure 5).

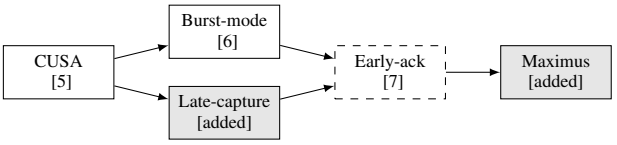


Figure 5. Relative ordering of existing an proposed late protocols. Arrows indicate a strict increase in decoupling.

A. Late-capture

Late-capture is the late protocol that follows the same synchronization principle as Early-ack, but reduces decoupling in order to allow using symmetrical delays. As Figure 6 shows, the $L^a\nearrow$ transition waits for $R^a\searrow$ (instead of $R^r\searrow$ for Early-ack).

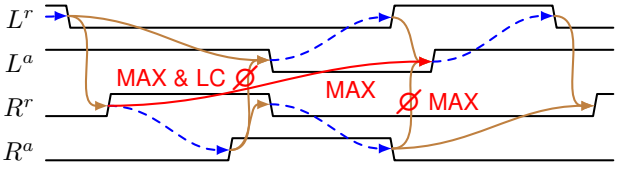


Figure 6. Ordering of transitions for controllers implementing the proposed late protocols.

However, this decoupling reduction requires the previous stage to stop without having sent the request. When the current stage has finished its data transfer ($R^a\searrow$ after a time $T_{\text{cp}} = 2\delta$) the previous stage can send the request, which goes through the previous DE δ_{prev}. Therefore, $T_{\text{rz}} = \delta_{\text{prev}}$.

B. Maximus

The protocol Maximus targets the optimal RZ time while not requiring asymmetrical DEs as Early-ack does. As Early-ack (Figure 4), Maximus removes the same dependencies as Burs-mode ($R^a\searrow\rightarrow L^a\nearrow$) and Late-capture ($R^a\nearrow\rightarrow L^a\searrow$) (Figure 6).

The dependency $R\nearrow\rightarrow L^a\nearrow$ is added to obtain a smaller circuit. With this dependency, only one internal state variable is needed to complete the state encoding. Moreover, this formal concurrency reduction does not degrade the actual performance. Indeed, the internal transitions $L^r\searrow\rightarrow R^r\nearrow\rightarrow L^a\nearrow$ takes less time than $L^r\searrow\rightarrow L^a\searrow\overset{\delta}{\rightarrow} L^r\nearrow\rightarrow L^a\nearrow$.

Of all presented late protocols, Maximus is the first that has early equivalent in existing frameworks dedicated to early protocols [3], [4]. The concurrency reduction on the L channel of the late protocols actually allows increasing the decoupling of the R channel.

C. Expected performances of new protocols compared to existing ones

Figure 7 shows how the proposed protocols (in red) are expected to perform compared to the existing protocol. In terms of surface (asymptotically proportional to the size of the DE), Late-capture and Maximus will have reduced DEs as typical late controllers (Section II-B). Early-ack is an exception as it requires using asymmetric DEs.

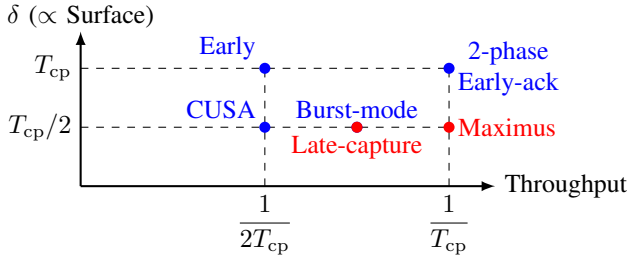


Figure 7. Summary of asymptotic performances of the existing and proposed protocols depending on the critical path length T_{cp}.

In terms of throughput, Maximus reaches the ideal throughput, along with Early-ack and 2-phase protocols. For Late-capture, there is one DE toggle during the RZ phase. However, as the DEs are shorter than for early protocols, the toggle has less impact on the throughput.

V. Benchmark

We compare the proposed Late-capture and Maximus to three of the classical early protocols of [8] (Simple, Semi-decoupled, and Fully-decoupled) and to Burst-mode [6]. The controllers are mapped on a TSMC 40 nm CMOS library by Dolphin Integration. The simulations at gate-level with retro-annotated delays aim at refining the properties of late protocols summarized in Figure 7.

A. Implementation of the controllers

The controller implementation uses symmetric and asymmetric C-elements. Figures 8a and 8b show their respective gate symbols and conventional transistor-level implementations. Since the target technology library had only symmetric C-elements, Figure 8c shows the used gate-level implementation of the asymmetric C-element.

Figure 8 shows the controller speed-independent gate-level netlists synthesized using the tool Petrify [11]. The input of Petrify is the STG specification of the protocol. The tool generates the state graph, eventually inserts state variables to complete the state coding, and return the required hardware.

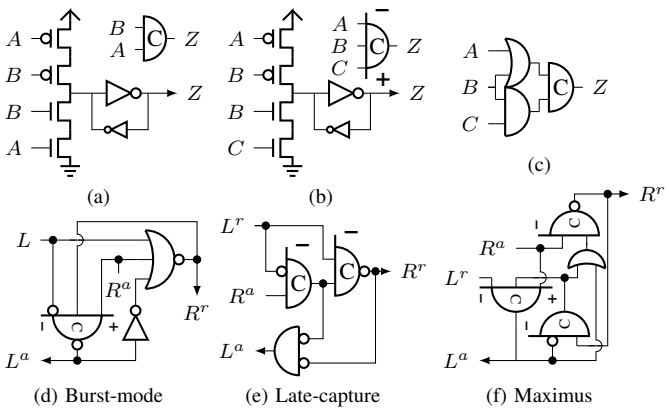


Figure 8. C-element and controller implementations. a) Conventional symmetric C-element. b) 3-input asymmetric C-element. c) 3-input asymmetric standard cell C-element. d-f) Late controllers.

B. Circular pipeline configuration

For each controller, we simulate a ring of 20 identical stages. The circular configuration allows keeping a constant number of data items in the pipeline. At most $20 - 1 = 19$ data items can circulate in the pipeline. This corresponds to a ratio of data items to the number of stages, namely *occupancy*, of 95%. To contain 19 data items, we must put two simple controllers per pipeline stage (half-buffer). Other protocols only need one controllers per pipeline stage (full-buffers).

We simulate the pipelines with different DE lengths δ, identical for all stages. The benchmark uses inverter-based delays: chains of minimal-size inverters. The propagation delays of rising and falling edges are similar.

VI. Analysis of Simulation Results

To abstract the result from the used technology and pipeline data widths, the delay unit is the gate delay (GD). It corresponds to the switching time of one minimum-size inverter connected to three identical ones (FO3). Also, one data item (DI) is the number of bits of the output stage of the pipeline. In the used technology, $1\,\mathrm{GD} = 420\,\mathrm{ps}$. Then, the throughput is expressed milli-data item per gate delay (mDI/GD). If the pipeline output is 32-bit wide, then $1\,\mathrm{mDI/GD} = 76\,\mathrm{Mbit/s}$. The pipeline with simple controllers and delay lines of null size is the reference for normalization of area and performance metric.

A. Benefits of halving the delay elements: area and energy gains

As expected from Figure 7, late protocols requires half as many inverters as early protocols to cover the same critical path (Figure 9a).

As a first result (Figure 9b), for longer critical paths, the area of the asynchronous control (controllers and DEs) using late protocols becomes smaller than if it used early protocols. The area gain on the DEs compensates the added logic in the controller. Note that in our test setup, gate implementation of the asymmetric C-elements are much larger than what direct transistor implementation could yield.

In term of consumed energy, being more complex, late controllers consume more energy than early controllers. Nevertheless, the efficient use of the DEs mitigates this energy overhead for long critical paths (Figure 9c). Note that the dynamic energy increases linearly with T_{cp} and the leaked energy linearly with ${T_{cp}}^2$. Among the late controllers, Burst-mode uses less energy.

B. Benefits of reducing the RZ phase: throughput gain

Figure 9d shows the minimum frequency of the pipeline (inverse of the maximum throughput) in function of critical path length. Consistently with Figure 7, the slopes of the lines are 2 for the early protocols, 3/2 for Burst-mode and Late-capture, and 1 for Maximus. Due to the computation overhead of the late protocols, only early protocols allow having propagation times and cycle times smaller than 7 GD.

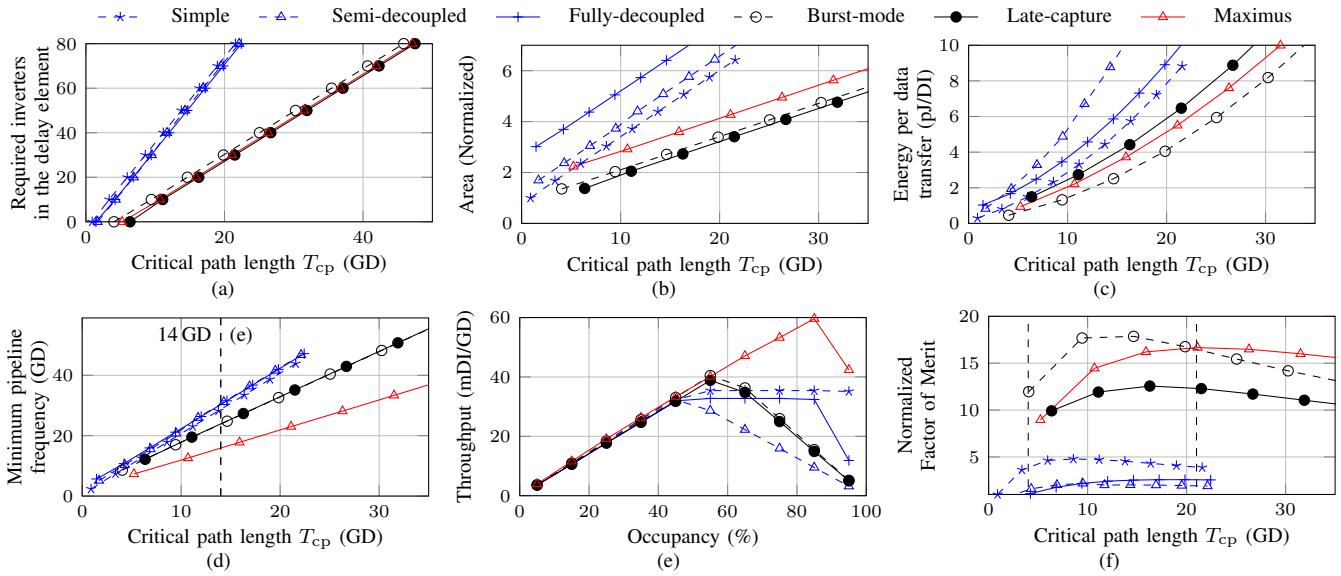


Figure 9. Comparison of early and late protocols. a) Required size of delay elements versus critical path length T_{cp}. b) Area and c) Consumed energy per data transfer versus T_{cp}. d) Pipeline frequency versus critical T_{cp}. e) Throughput versus occupancy for a fixed $T_{cp} = 14\,\text{GD}$. f) Figure of merit versus T_{cp}.

For fair comparison, we compare the protocols with delay elements matching at best a critical path length T_{cp} of 14 GD. Thus, all protocols have similar throughputs on the left part of Figure 9e, where the throughput is limited by the requests, themselves limited by the propagation of few data in the pipeline. On the right hand side, the throughput is limited by the propagation speed of the acknowledgments. For Maximus, this speed is independent on the delay element length, leading to high throughput even at high occupancy.

C. Figure of merit

In order to choose among the protocols, we define the following figure of merit (FOM):

$$\text{FOM} = \frac{\text{Throughput}}{\text{Area} \times \text{Energy}} \times {T_{cp}}^3 \tag{3}$$

Where the ${T_{cp}}^3$ factor would lead to strictly positive asymptotic values in the absence of leakage.

Figure 9f plots the normalized FOM of each controller versus the critical path length. For short critical paths (less than 4 GD), late protocols are too slow to efficiently match the paths. For medium length path (between 4 and 21 GD), Burst-mode stands out because it is low energy consumption. It appears that the Late-capture, which we introduced as a logical complement of the rest of the family, has no particular interest compared to Burst-mode. Finally, for long critical path (more than 21 GD), Maximus provides the best results because of its capacity to maintain a high throughput.

VII. Discussion

A. Of the use of asymmetric delay elements

Asymmetric DEs would shorten the RZ phase of early protocols at the cost of increased area and power consumption. Therefore, they may become faster than semi-decoupled late protocols such as Burst-mode and Late-capture. For pipelines with high occupancy however, Maximus should still be faster as the RZ phase only consist in one transition on the acknowledgment wire instead of two (plus one on the request wire) for the early protocols.

B. Of the search for all late protocols

The existing framework exploring extensively asynchronous protocols are dedicated to early protocols [3], [4]. They are based on a protocol of maximum decoupling from which all protocols are deduced by successive decoupling reduction. Late protocols such as Maximus actually that take advantage of the coupling on the left channel to increase the coupling of the right channel beyond what is possible for early protocols. Therefore, such late protocols are out of the existing frameworks.

Nevertheless, the existing strategies for exploring early protocols can be transposed to late ones. Maximus without its optimization decoupling reduction ($R^r\nearrow \rightarrow L^a\nearrow$) seems a good candidate for the most decoupled late protocols.

VIII. Conclusions

Late protocols are interesting design opportunities to improve the area, throughput and energy efficiency of bundled-data pipelines. The decoupling added in the Maximus protocol allows maintaining high throughput even in pipelines with high occupancy. Maximus also pushes the frontier of known protocols. New frameworks should be developed to finish exploring the protocol design space.

Asynchronous pipelines can be improved by using several protocols in the same circuit [12]. Therefore, the new protocols empower the designers in selecting the controllers fitting best their applications and architectures. Versatility may be a key property to make asynchronous design a more competitive solution in terms of area and performance.

ACKNOWLEDGEMENT

This work has been partially supported by the LabEx PERSYVAL-Lab (ANR-11-LABX-0025-01).

REFERENCES

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design*. Springer, 2002.

[2] A. Peeters and K. van Berkel, "Single-rail handshake circuits," in *2nd Working Conference on Asynchronous Design Methodologies*, 1995, pp. 53–62.

[3] P. B. McGee and S. M. Nowick, "A lattice-based framework for the classification and design of asynchronous pipelines," in *42nd annual Design Automation Conference (DAC)*. ACM, 2005, pp. 491–496.

[4] G. Birtwistle and K. S. Stevens, "The family of 4-phase latch protocols," in *14th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)*, 2008, pp. 71–82.

[5] R. David, "Modular design of asynchronous circuits defined by graphs," *IEEE Transactions on Computers*, vol. C-26, no. 8, pp. 727–737, 1977.

[6] K. Yun, P. Beerel, and J. Arceo, "High-performance asynchronous pipeline circuits," in *2nd International Symposium on Advanced Research in Asynchronous Circuits and Systems (ASYNC)*, 1996, pp. 17–28.

[7] C. Mannakkara and T. Yoneda, "Asynchronous pipeline controller based on early acknowledgement protocol," *IEICE Transactions on Information and Systems*, vol. 93, no. 8, pp. 2145–2161, 2010.

[8] S. Furber and P. Day, "Four-phase micropipeline latch control circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 4, no. 2, pp. 247–253, 1996.

[9] I. Blunno, J. Cortadella, A. Kondratyev, L. Lavagno, K. Lwin, and C. Sotiriou, "Handshake protocols for de-synchronization," in *10th International Symposium on Asynchronous Circuits and Systems (ASYNC)*, 2004, pp. 149–158.

[10] T.-A. Chu, "On the models for designing VLSI asynchronous digital systems," *INTEGRATION, the VLSI journal*, vol. 4, no. 2, pp. 99–113, 1986.

[11] J. Cortadella, M. Kishinevsky, A. Kondratyev, L. Lavagno, E. Pastor, and A. Yakovlev, "Petrify: a tool for synthesis of Petri nets and asynchronous circuits," Software, http://www.cs.upc.edu/~jordicf/petrify/ [accessed 2016-04-11].

[12] E. Yahya, "Performace modeling, analysis and optimization of multi-protocol asynchronous circuits," Ph.D. dissertation, Institut National Polytechnique de Grenoble - INPG, Dec 2009.

Appendix E

Article in international journal: Springer JETTA 2013

A New Recovery Scheme against Short-to-Long Duration Transient Faults in Combinational Logic

Rodrigo Possamai Bastos[1,2], Giorgio Di Natale[2], Marie-Lise Flottes[2], Feng Lu[2], and Bruno Rouzeyre[2]
[1]TIMA Laboratory (Grenoble INP, UJF, CNRS), Grenoble, France
[2]LIRMM (Université Montpellier II / CNRS UMR 5506), Montpellier, France
bastos@imag.fr, {bastos, dinatale, flottes, lu, rouzeyre}@lirmm.fr

Abstract – **This paper presents a new recovery scheme for dealing with short-to-long duration transient faults in combinational logic. The new scheme takes earlier into account results of concurrent error detection (CED) mechanisms, and then it is able to perform shorter recovery latencies than existing similar strategy. The proposed scheme also requires less memory resources to save input contexts of combinational logic blocks. In addition, this work also proposes a taxonomy of CED techniques. It allows pointing out which are the necessary recovery resources as well as identifying which are the types of CED mechanisms that can be used with the new recovery scheme of this paper. The effectiveness of the proposed scheme was evaluated through electrical-level simulations. For all short-to-long duration transient-fault injections, it was never slower than state-of-art similar strategy, and indeed its recovery latency was faster for 34% of the simulated faulty scenarios.**

Keywords – transient faults; soft errors; concurrent error detection; and recovery schemes

I. INTRODUCTION

Higher resilience is expected from an increasing number of integrated systems while, in the same time, ultra-deep submicron technologies make these systems prone to misbehaviors induced by the natural aging processes or the environment (radiations from cosmic origin or every day material). In addition to these natural phenomena, malicious fault-based attacks can be used for leading secure systems to misbehavior, bypassing security mechanisms or providing information on confidential data [1][2]. For both these environmental or malicious phenomena many applications require fast recovery.

Until the early 2000's, researches on transient faults and soft errors 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 in terms of digital security 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.

In addition, some transient fault phenomena considered as short in the past (much less than one clock cycle) can be now considered as long duration transient faults (reaching the clock period) due to the possibility of higher operating frequencies in recent ultra-deep-submicron technology-based circuits [3][4]. In fact, the effects of long-duration transient faults have clearly a much higher probability of not being masked, and so they also stand a greater chance of producing system failures. In addition, we may expect that maliciously induced transients could be better monitored whether they last several clock cycles. This emerging issue on long-duration transients introduces therefore supplementary difficulties to design optimized protections for the circuits.

The current trend in solutions to cope with transient-fault effects is applying protection techniques at different abstraction levels of the design [3][4][5][6]. The idea is thus to prevent the use of costly fault-tolerance mechanisms like the tripe modular redundancy, taking advantage of cheaper mitigation techniques that ensure satisfactory soft-error coverage for the system's most recurrent operations. This modern strategy is exemplified through recovery schemes based on concurrent error detection (CED).

CED mechanisms designed at transistor or gate level guarantee an early detection, as soon as the faults happens, 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 misbehavior, an error flag is generated and the scheme can activate recovery mechanisms already implemented in modern systems for dealing with branch misprediction [4][6]. After the transient fault disappearing, earlier faulty operation is thus repeated and the system returns to perform its normal computational sequence.

This work proposes a new recovery scheme based on CED that can be also used to improve already existing solutions. More precisely, the contributions of this paper are:

- Section II presents a new taxonomy of CED techniques that allows understanding the requirements for implementing their associated recovery schemes against short-to-long duration transient faults as well as evaluating qualitatively their costs and efficiencies;
- Section III discusses recovery schemes at micro-architectural level in function of the CED types defined in section II. Furthermore, we show a transient-fault scenario that proves for existing recovery schemes the exigency of saving two input contexts of logic blocks;

- Section IV presents the new recovery scheme and, unlike our work in [7], its generic applicability for any CED technique classified in II as asynchronous due to its transient result in function of the fault behavior;
- Section V evaluates the effectiveness of our scheme and compares it with another existing similar strategy. We show the benefits of the new recovery scheme based on experimental results issued from transient-fault injection simulations.

II. TYPES OF CED TECHNIQUES

In the following, CED (Concurrent Error Detection) is a misuse of language because we consider error detection and fault detection schemes as well. As mentioned before, transient faults do not necessarily produce a soft error; however detection of masked transient faults is also of importance for secure applications.

Classic CED solutions to face transient-fault effects are adding spatial, information, or time redundancy to the circuit. These three approaches can be implemented at different abstraction levels of the design. Fig. 1 presents basic example of such techniques at micro-architectural level. They essentially compare two redundant results of which at least one must be safe to permit the detection of errors. If for instance one result fails, the comparison provides an error flag. Furthermore, Fig. 1 also illustrates another type of CED that is based on built-in current sensors (BICS). BICS are connected either to V_{dd} and Gnd (VGBICS in [8]) or to Bulks of transistors (BBICS in [9]) in order to detect anomalous transient currents that can become (or not) soft errors. BICS-based schemes therefore are able to generate an error flag in case of occurrence of transient faults within a range defined by the calibration of the BICS.

Fig.2 generalizes the components of a CED with recovery to protect a target circuit. The CED circuitry is responsible to deliver an error flag if a transient misbehaviour is detected (i.e. a transient fault in the combinational logic of the target circuit or a soft error in a storage element). However, as such an error flag can have behaviours as transient and asynchronous as the transient fault that induces it, mechanisms for sampling this CED's result have to be implemented. These sampling mechanisms ensure the error flags in a steady state enough time to activate correctly the recovery procedure.

If we come back to the columns of Fig. 1, we can even classify the CED techniques into two types according to the features of their error flags:

- Synchronous CED schemes: classic CED approaches that compare their redundant parts after the data register (e.g. [10][11][12][13][14]). Hence, they inherently guarantee their results in steady conditions during the cycle following the cycle on which the transient fault appears. The error flag is generated already in synchronization with the system since the mechanisms for sampling such a CED's result are indeed parts of the CED scheme. Therefore, there is no need for registering this result if its value is directly used for starting the recovery procedure during the cycle following the first faulty cycle. On the other hand, only transient faults that reach data registers (causing soft errors) are detected in this case. As discussed before, it is correct for applications in which the recovery must be launch only in case of soft errors, but this is not sufficient when transient faults must be detected even if they do not induce any error. Synchronous CED schemes can be very expensive since they require the storage of all redundant data bits (N or C additional redundant registers in Fig. 1's examples) [15];

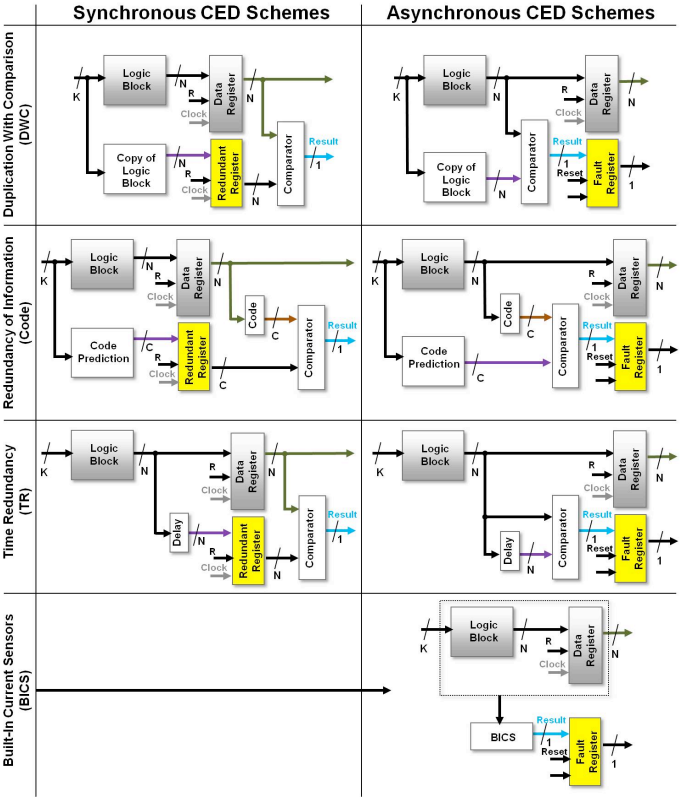


Figure 1. Examples of synchronous and asynchronous CED schemes

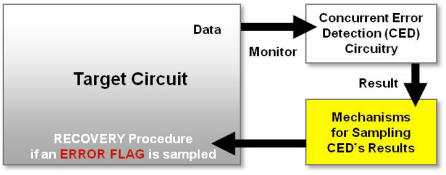


Figure 2. A target circuit protected by using CED with recovery

- Asynchronous CED schemes: CED techniques that generate asynchronously their error flags in function of the transient-fault features (e.g. [4][6][8][9][16][17][18][19][20]). Hence, asynchronous CED schemes must include another extra 1-bit register dedicated only to sample their error flags, and so ensuring results at steady state during the necessary time for starting the recovery procedures. Conversely to synchronous CED schemes, there is no need to register the redundant data bits but only the flag, and thus these solutions are less expensive [15].

III. Recovery Schemes for Dealing with Short and Long-Duration Transient Faults in Logic

CED techniques dedicated to identify transient-fault effects require recovery schemes in order to correct soft errors. The recovery machine acts in function of the CED's result to thus in fault-free conditions repeat the affected cycles whether an error flag is generated.

The recovery scheme, therefore, initially works to save fault-free input status of the target circuit, such as input values of logic blocks. Then, in case of an error flag, the system is able to later reload such good input values (after the transient fault vanishing), and so recomputing the first cycle at which the fault has affected the logic block's operations.

We highlight that there is a latency of extra clock cycles only if a transient fault is detected, and thus the target circuit normally operates without penalty in fault-free scenarios. About the area overheads added by recovery schemes we remind that they can be minimal whether the target circuit's architecture has already a machine to repeat operations in branch-misprediction situations. In addition, microprocessor-based systems can take advantage of their instruction/data memory resources in order to save the input context of logic blocks.

Fig. 3, 4, and 5 illustrate a system compounded of a register IN, a register OUT, and a logic block that is protected by three different recovery schemes for dealing with short and long duration transient faults. The other grey blocks (i.e. except CED schemes, Redundant, Fault and Recovery Registers, and Reset multiplexer) are resources that might be already present in certain modern architectures to recompute previous operations, and so they can be reused in conjunction with CED schemes to mitigate transient faults. Note in Fig. 3, 4, and 5 that the communications between the CED blocks and the recovery circuits are slightly different. More precisely, the type of CED scheme (Synchronous or Asynchronous, as section II defines) and the strategy for sampling its results (e.g. by using a Flip-Flop or a Latch) determine the recovery efficiency and which minimum memory resources are necessary to properly save input contexts of logic blocks during the fault-free cycles that precede the first faulty cycle "First_Faulty_Cycle".

The costly synchronous CED techniques discussed in II require at least a recovery scheme similar to Fig. 3's illustration. This classic machine saves the logic block's inputs during each clock's low phase by using a memory that, in this example, is represented by K latches, and we call it in this paper as a backup file. Then, when the CED scheme indicates an error flag in the cycle posterior to "First_Faulty_Cycle", the machine is able to restore the saved logic block's inputs (Fig. 3's "saved_logic_inputs") of one cycle ago the instant at which the error flag is set (i.e. the logic block's inputs of "First_Faulty_Cycle"). This process of restoring and recomputing is done in the first following fault-free cycle "Repeated_Cycle" on which the transient fault has already vanished.

Asynchronous CED techniques that use a flip-flop for sampling its results demand a recovery scheme like the schematic in Fig. 4 (e.g. [6]'s Checksum-based scheme). This simple strategy is not so efficient to sample the CED's results [15][21], and then its recovery efficiency is moderate.

On the other hand, Asynchronous CED techniques that use a latch require more elaborate recovery architecture such as Fig. 5 shows, but they allow high recovery efficiency (e.g. [4]'s BBICS-based scheme). In fact, the fault register's output from Fig. 5's scheme has a steady condition but it can be achieved at any instant, in function of the moment at which the transient fault happens as well as the duration it takes. This fault register's output is, therefore, an asynchronous signal that must be synchronized in order to be correctly dealt by the recovery scheme. Hence, another flip-flop, illustrated in Fig. 5 as recovery register, is mandatory to prevent metastability problems. This flip-flop also ensures enough time to reset the fault register before the recomputation as well as it allows to deal with cases in which the response time "RT" of the asynchronous CED is longer than the clock's high pulse width. Note that if the fault register is a latch, we define RT as the delay between the beginning of the transient fault and the fault register's output. On the other hand, if the fault register is a flip-flop, it already makes the synchronization with the recovery scheme, and then RT is defined as the delay between the beginning of the transient fault and the Asynchronous CED scheme's output.

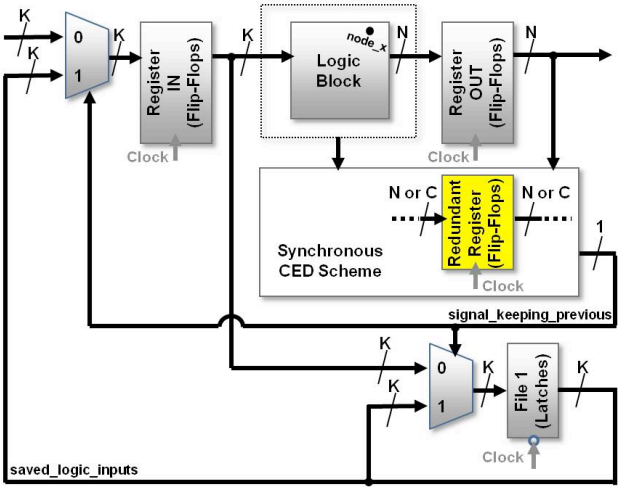


Figure 3. Classic recovery scheme for Synchronous CED techniques

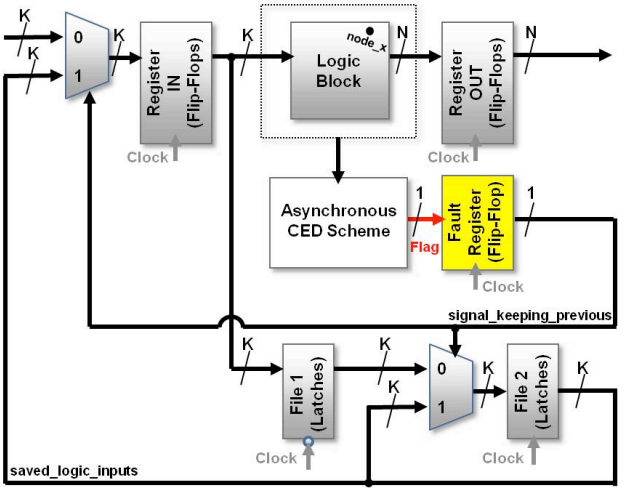


Figure 4. Recovery scheme based on a flip-flop to sample results of asynchronous CED mechanisms

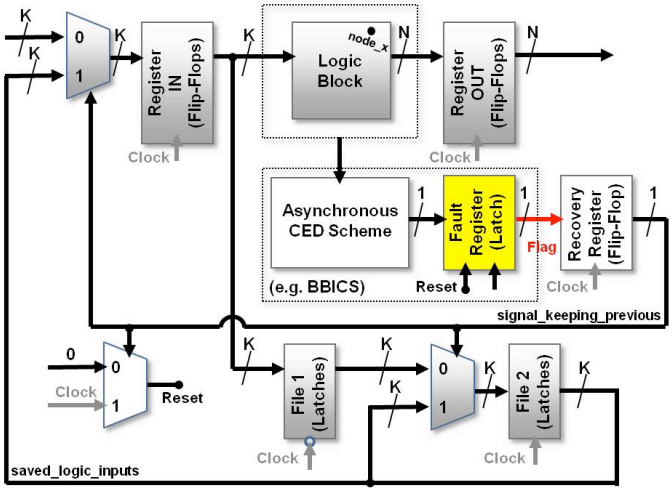


Figure 5. Recovery scheme based on a latch and a flip-flop to sample results of asynchronous CED mechanisms

Both types of machine in Fig. 4 and 5 save logic block's inputs of two clock cycles by using two backup files with K latches each one. Thereby, if CED scheme indicates an error flag, the recovery circuit is able to restore in "Repeated_Cycle" the saved logic block's inputs (Fig. 4 and Fig 5.'s "saved_logic_inputs") of two cycles ago the instant at which the error flag is identified and registered at "signal_keeping_previous". Observe in Fig. 4 and 5 that this signal is used to keep in the backup files the logic block's inputs of the previous cycles.

We notice in this paper that recovery strategies such as Fig. 4 and Fig. 5's schemes necessarily need at least two backup files with K latches to save logic block's inputs of two clock cycles. In fact, as Fig. 6 highlights, there are chances of transient faults "TF" starting in cycle 1 not to raise "signal_keeping_previous" in cycle 2, and then the logic block's inputs saved in file 1 during cycle 1 must be transferred to file 2 during cycle 2 in order to be available in cycle 3. Furthermore, if the response time "RT" is greater than the clock period "T" (e.g. [4]'s BBICS calibrated with slower RT), more than two files are required. Therefore, the slower the RT the greater can be the number of required files.

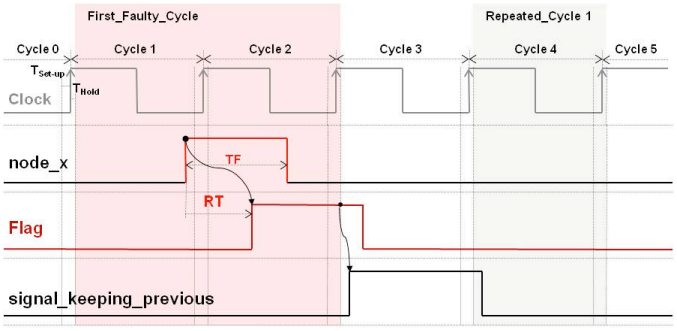


Figure 6. Transient fault's case that proves the exigency of at least two backup files for Fig. 4 and Fig. 5's recovery schemes

Let us now in Fig. 7 take another example like Fig. 6's case but with a transient fault of longer duration "TF1". It starts on a "node_x" of Fig. 5's logic block during cycle 1. The asynchronous CED's scheme thus raises in cycle 2 an error flag at signal "Flag" after a maximum response time "RT" equals to 50 % of the circuit's clock period "T". However, this error flag is only registered at recovery register during cycle 3. Then, as "signal_keeping_previous" achieves steady logical level "1" in cycle 3, logic block's inputs from cycle 1 (which are kept at "saved_logic_inputs") are restored in register IN at the beginning of cycle 4. Nevertheless, as TF1 spans up to cycle 3, the asynchronous CED's scheme raises again an error flag that keeps the recovery register at "1" during cycle 4. Thus, logic block's inputs from cycle 1 are restored once more in register IN but now at beginning of cycle 5 in order to recompute such an operation without faults. TF1, therefore, penalizes the system with a recovery latency of four extra cycles by using Fig. 5's scheme.

Furthermore, Fig. 7 also shows a fault "TF2" that makes the recovery register's flip-flop metastable. Then, "signal_keeping_previous" results in an unknown value that may be, for instance, "0", and so TF2 would penalize the system with a latency of three extra cycles instead of two whether the resultant value was "1".

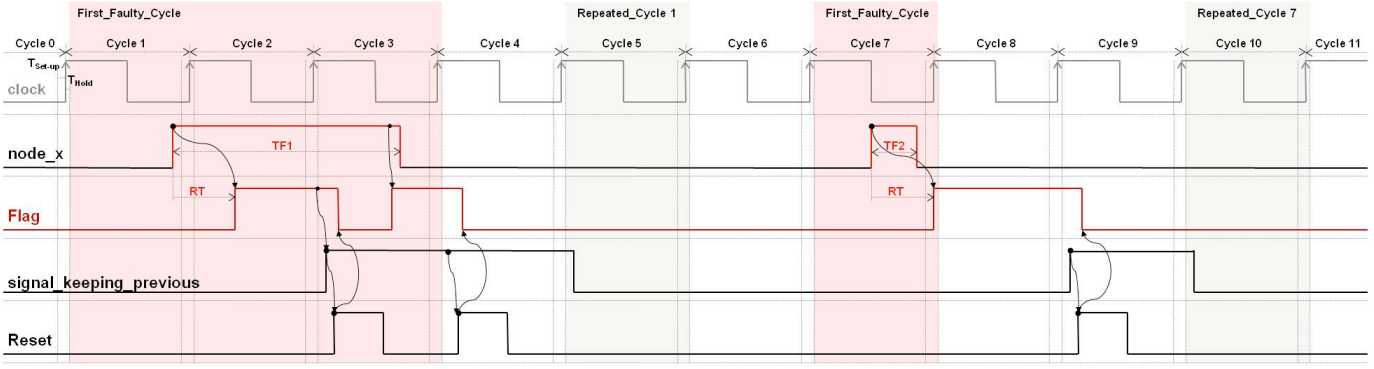


Figure 7. Functional behavior of Fig. 5's recovery scheme to cope with transient faults "TF1" and "TF2"

IV. A New Recovery Schemes for Dealing with Short and Long-Duration Transient Faults in Logic

We propose in this section a considerable improvement of Fig. 5's scheme discussed in III. Our improved scheme, which is illustrated in Fig. 8, requires a smaller number of memory resources. In fact, only a backup file is necessary since our approach need to save the logic block's inputs of just one cycle ago the instant at which an error flag is identified and registered at recovery register. This optimization is made by using a latch as recovery register instead of a flip-flop. It allows starting to sample the signal "Flag" at clock's falling edge, and so the scheme can deal earlier with error flags coming from asynchronous CED schemes.

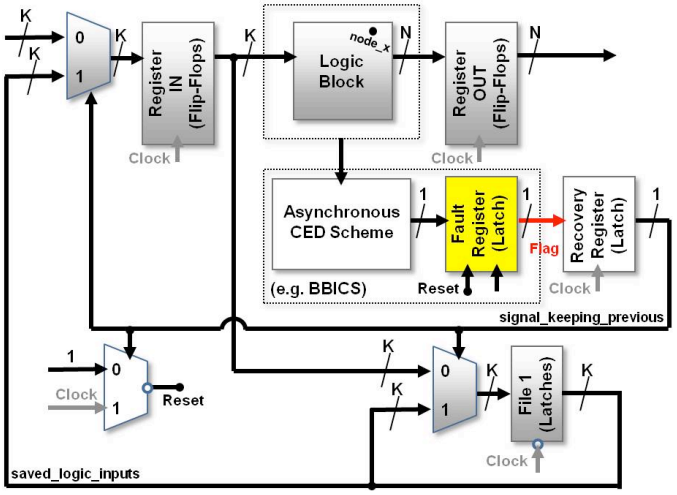


Figure 8. Our new recovery scheme based on a two latches to sample results of asynchronous CED mechanisms

Fig. 9 gives further details about our recovery scheme by showing the mitigation of the transient faults "TF1", "TF3", "TF2", and "TF4". Note that the same faults "TF1" and "TF2" analyzed in Fig. 7 for Fig. 5's scheme are also discussed for our approach.

Let us firstly analyze TF1 and TF2. Unlike the reactions of Fig. 7's "signal_keeping_previous", this signal in Fig. 9 raises earlier during cycle 2 and cycle 8 instead of respectively cycle 3 and cycle 9 in Fig. 7. In fact, Fig. 9's "signal_keeping_previous" gets steady logical level "1" after clock's falling edge in cycle 2 and cycle 8, then logic block's inputs of "First_Faulty_Cycle" are restored earlier in register IN, at the beginning of cycle 3 and cycle 9. As TF1 lasts until cycle 3, the logic block's inputs from cycle 1 are restored again in register IN at the beginning of cycle 4, and so the faulty operation is now properly re-executed without the fault presence. Therefore, TF1 and TF2 penalizes the system respectively with three and two extra cycles instead of four and three taken by using Fig. 5's scheme. Our improved scheme shows thus requiring smaller latencies to complete the recovery due to short or long-duration transient faults. In fact, our approach advances the recomputation by anticipating the identification of error flags at the clock's falling edge instead of the rising edge used by Fig. 5's scheme.

Note however that there are two simple design constraints which are modified to ensure the anticipation of the recomputation as well as the use of only one backup file to save previous logic block's inputs.

In order to explain the first constraint, let us initially take Fig. 9's limit fault scenario in cycle 5. TF3 starts on the border on which cycle 4 leaves of being perturbed, and so from such an instant, which is defined as hold time "T_{Hold}" after clock's rising edge, cycle 4 is not necessary to be recomputed later. Clock's high Pulse Width "hPW" has to be thus ensured sufficiently longer than RT for clock's falling edge sampling correctly this last TF3-induced error flag that requires logic block's inputs from cycle 4. If it is accomplished, all transient faults started from the beginning of cycle 4 (after hold time "T_{Hold}") until the instant of the TF3's startup have their resultant error flags certainly sampled in cycle 5, and so only the logic block's inputs from cycle 4 has to be saved.

Equation (1) below defines this first constraint by using a $T_{MarginFall}$ as additional time margin for variations in clock's falling edge operations (jitter and skew), and manufacturing and environmental variabilities:

$$hPW > RT + T_{Hold\_RegIN} + T_{Set-up\_File1} + T_{Margin Fall} \quad (1)$$

The second design constraint is related to the low Pulse Width "lPW" that complements hPW to make a clock period "T". In fact, by taking similar TF3 scenario but with TF starting a little after, lPW must last enough time in cycle 5 to ensure the worst case (after clock's edge falling) when an error flag at signal "Flag" causes metastability in recovery register's latch and "signal_keeping_previous" stabilizes at logical level "1". In this situation, the condition below in (2) must be respected in order to the scheme works properly to recompute in cycle 6 the logic block's inputs from cycle 4. $T_{MarginRise}$ is similar to $T_{MarginFall}$ but for clock's rising edge, D_{Mux2x1}, and D_{Latch} are respectively the delays of the multiplexer at the register IN's inputs, and of the recovery register's latch.

By using the fact that T = hPW + lPW, (2) results in (3). And taking (1) and (3), we have (4). Note that RT and T are adjustable whether equations (5) (derived from (1)) and (6) are respected. D_{Logic} is the Logic Block's longest delay.

$$lPW = (T - hPW) > T_{Hold\_RecoverReg} + T_{Margin Fall} + D_{Latch} + D_{Mux2x1} + T_{Margin Rise} + T_{Set-up\_RegIN} \quad (2)$$

$$hPW < T - (T_{Hold\_RecoverReg} + T_{Margin Fall} + D_{Latch} + D_{Mux2x1} + T_{Margin Rise} + T_{Set-up\_RegIN}) \quad (3)$$

$$RT + T_{Hold\_RegIN} + T_{Set-up\_File1} + T_{Margin Fall} < hPW < T - (T_{Hold\_RecoveryReg} + T_{Margin Fall} + D_{Latch} + D_{Mux2x1} + T_{Margin Rise} + T_{Set-up\_RegIN}) \quad (4)$$

$$RT < hPW - (T_{Hold\_RegIN} + T_{Set-up\_File1} + T_{Margin Fall}) \quad (5)$$

$$T > T_{Hold\_RegIN} + D_{Logic} + T_{Margin Rise} + T_{Set-up\_RegOUT} \quad (6)$$

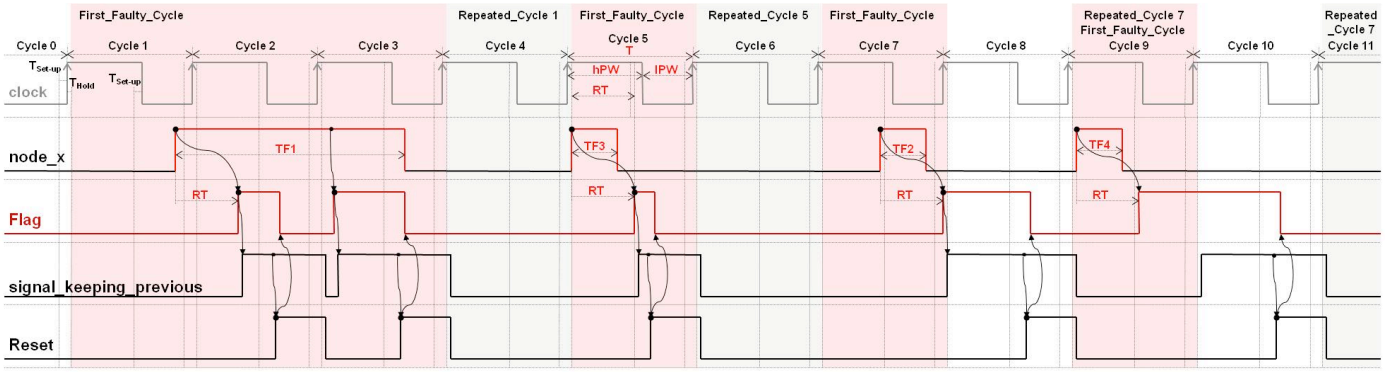


Figure 9. Functional behavior of our new recovery scheme to cope with transient faults "TF1", "TF3", "TF2", and "TF4"

V. Experimental Results Comparing Recovery Schemes

In this section we present some experimental results that show the effectiveness of our proposed approach. We compare the recovery latency required for the schemes presented in Fig. 5 and Fig. 8 (our proposed solution). Fig. 3 and Fig. 4's schemes are not considered because the first one is very costly in terms of area and power consumption while Fig. 4's approach is not so effective in identifying many transient-fault scenarios and requires at least two backup files (see discussions in sections II and III). Furthermore, in theory these schemes in Fig. 3 and Fig. 4 have higher recovery latencies or, at the best, equivalent since they sample the error flags by using the same clock's edge used by register IN and OUT.

Experimental results were obtained using transistor-level simulation of circuits with the recovery schemes and of the injected single transient fault. The asynchronous CED scheme and the fault register's latch from Fig. 5 and Fig. 8 were emulated such as the behavior of BBICS. The following parameters were considered:

- The circuits were designed using a commercial 65-nm standard-cell library, V_{dd} 1.2V, nominal conditions, and SVT transistors;
- The clock period is 1ns, 50 % duty cycle;
- The transient fault was simulated by using a double-exponential current source. Then, transient pulses with several durations (50ps, 250ps, 500ps, 750ps, and 1ns) were parameterized in such a way that the voltage amplitude achieves V_{dd}. It prevents the electrical masking effects of the transient faults. In fact, as the goal is to analyze the efficiency of the recovery mechanisms and not of the CED techniques, we were not interested in any type of transient-fault masking effect;
- Considered RT (asynchronous CED's response time defined in III) are 200ps, 250ps, 300ps, and 400ps;
- Initial instant of injection were simulated from 0 to 1000 ps of "First_Faulty_Cycle". We have therefore supposed a range of different logic block's nodes on which single transient faults are injected and propagated up to make a soft error in register OUT. Logical and latching-window masking effects of the transient faults are thus not taken into account. As a step of 1ps is used, 1000 simulations were performed for each value of RT and fault duration;
- Recovery latency is expressed in number of clock cycles required for the scheme to recompute the logic block's inputs of "First_Faulty_Cycle".

For each RT values and transient fault durations, we have counted how many injections (over 1000) were recovered in 1, 2, 3, and 4 clock cycles. Results of all simulations are summarized in Fig. 10. As it can be seen, our proposed scheme allows recovering from short and long transient faults in less clock cycles than the other solution. For instance, for RT 400ps and fault duration 1000ps, our Fig. 8's approach has a recovery latency of 4 cycles in 21% of the injected faults and of 3 cycles in the remainder 79%, while Fig. 5's scheme requires 4 cycles in 73% of the injected faults and of 3 cycles in 27% of the scenarios.

Finally, taking into account all transient fault durations for RT 200ps, 250ps, 300ps, and 400ps, the circuit with our scheme returned to its normal operation one cycle earlier respectively in 31%, 33%, 35%, and 37% of the injected transient-fault scenarios. Note therefore that the slower the RT the better is our solution. Evidently, in the remainder of the scenarios both schemes have the same recovery latency.

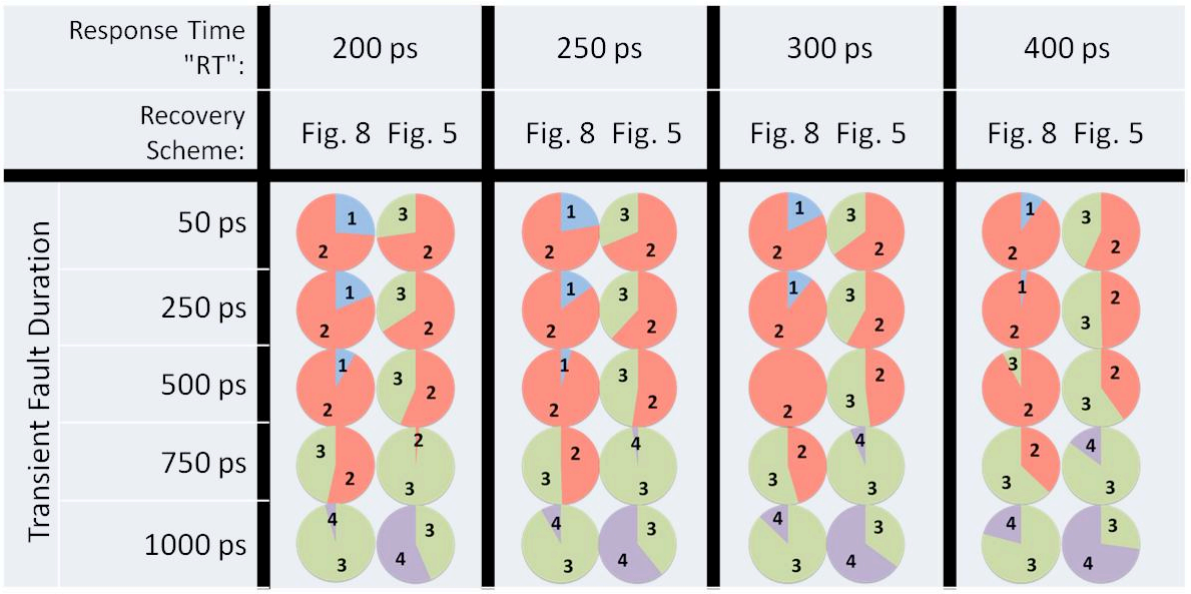


Figure 10. Distribution of recovery latencies (1, 2, 3, or 4 clock cycles) for Fig. 8 and Fig. 5's recovery schemes in function of the asynchronous CED's response time "RT" (200ps, 250ps, 300ps, and 400ps) and the transient fault duration (50ps, 250ps, 500ps, 750ps, and 1ns). For instance, let us take RT 200ps and fault duration 50ps, our Fig. 8's approach has a recovery latency of 1 cycle in 26% of the injected faults and of 2 cycles in the remainder 74%, while Fig. 5's scheme requires 3 cycles in 27% of the injected faults and of 2 cycles in 73% of the scenarios.

VI. Final Conclusions

In this paper we have proposed the classification of the CED techniques into synchronous and asynchronous in order to identify which are the necessary recovery resources. In addition, we have proposed a new recovery scheme based on asynchronous CED schemes for dealing with short-to-long transient faults. Our approach uses the clock's falling edges (in case of data registers use clock's rising edges) for starting to sample error flags from transient faults. It allows reducing the recovery latency by one cycle. Moreover, the new recovery scheme also permits to use only a backup file to save input contexts of logic blocks. Our solution therefore requires much smaller recovery resources and lower latency than existing similar strategy.

References

[1] C.N. Chen, and S.M. Yen, "Differential Fault Analysis on AES Key Schedule and Some Countermeasures," in Proc. ACISP, v. 2727 of LNCS, 2003, pp. 118-129.

[2] P. Dusart, G. Letourneux, and O. Vivolo, "Differential Fault Analysis on A.E.S," in Proc. ACNS, v. 2846 of LNCS, 2003, pp. 293-306.

[3] C. Lisboa, M. Erigson, and L. Carro, "System level approaches for mitigation of long duration transient faults in future technologies," in Proc. ETS, IEEE, 2007, pp. 165-170.

[4] 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.

[5] C. Albrecht et al., "Towards a Flexible Fault-Tolerant System-on-Chip," in Proc. ARC, VDE Verlag GMBH, 2009, pp. 83-90.

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

[7] R.P. Bastos, G.D. Natale, M. Flottes, and B. Rouzeyre, "A New Bulk Built-In Current Sensor-Based Strategy for Dealing with Long-Duration Transient Faults in Deep-Submicron Technologies," in Proc. DFT, IEEE, 2011, pp. 302-308.

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

[9] 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.

[10] S. Mitra and E. McCluskey, "Which concurrent error detection scheme to choose?," in Proc. ITC, IEEE, 2000, pp. 985–994.

[11] M. Nicolaidis, "Time redundancy based soft-error tolerance to rescue nanometer technologies," in Proc. VTS, IEEE, 1999, pp. 86-94.

[12] Anghel, L., and M. Nicolaidis, "Cost Reduction and Evaluation of a Temporary Faults Detecting Technique," in Proc. DATE, IEEE, 2000, pp. 591-598.

[13] D. Ernst et al., "Razor: A low-power pipeline based on circuit-level timing speculation," in Proc. MICRO, IEEE/ACM, 2003, pp. 7-18.

[14] K. Bowman et al., "Energy-efficient and metastability-immune resilient circuits for dynamic variation tolerance," IEEE JSSC, v. 44, n. 1, pp. 49–63, Jan. 2009.

[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] S. Das et al., "RazorII: In situ error detection and correction for PVT and SER Tolerance," IEEE JSSC, vol. 44, no. 1, pp. 32–48, Jan. 2009.

[17] M. M. Kermani, A. R. Masoleh, "Parity-Based Fault Detection Architecture of S-box for Advanced Encryption Standard," in Proc. DFT', IEEE, 2006, pp. 572-580.

[18] C. Lisboa, and L. Carro, "XOR-based low cost checkers for combinational logic," in Proc. DFT, IEEE, 2008, pp. 281-289.

[19] D. Rossi, M. Omanã, and C. Metra, "Transient fault and soft error on-die monitoring scheme," in Proc. DFT, IEEE, 2010, pp. 391–398.

[20] D. J. Palframan, N. S. Kim, M. H. Lipasti, "Time Redundant Parity for Low-Cost Transient Error Detection," in Proc. DATE, IEEE, 2011.

[21] R. P. Bastos et al., "Timing Issues for an Efficient Use of Concurrent Error Detection Codes," in Proc. LATW, IEEE, 2011, pp. 1-6.

Exploiting Body Terminals of Transistors for Performing Post-Fabrication Tests, Run-Time Tests, and Self-Adaptive Bias in Integrated Circuits

Abstract – Ubiquitous integrated circuit applications help the humanity to rapidly evolve by supporting electronics systems that are more and more assuming autonomous functions and decisions of important responsibility for the society. In this context, dealing with security, reliability, and power issues of integrated circuits is fundamental to ensure the operation of systems within reasonable levels of privacy, safety, and energy consumption. Exploiting body terminals of transistors in CMOS technology-based systems, this work contributes with new techniques dedicated to: (a) test circuits – just after fabrication – for detecting possible hardware Trojans inserted to maliciously compromise systems; (b) test circuits on the fly for detecting transient faults provoked by radiation effects or malicious attacks; and (c) perform body bias adaptation in systems aiming to optimize speed and power but also compensate threshold voltage alterations induced by aging, process, voltage, and temperature variations. Moreover, herein, ongoing and near-future related activities and insights are discussed as potential perspectives of this work.

Keywords – Integrated circuit, design, test, run-time test, body biasing, low power, built-in current sensor, asynchronous circuit, level shifter, concurrent error detection, fault simulation, hardware Trojan, transient fault, soft error.

Thèse préparée au laboratoire TIMA (Techniques de l'Informatique et de la Microélectronique pour l'Architecture des ordinateurs), 46 Avenue Félix Viallet, 38031, Grenoble Cedex, France

ISBN: 978-2-11-129239-0