Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation

Raphael Andreoni Camponogara-Viera, Jean-Max Dutertre, Rodrigo Possamai Bastos, Philippe Maurine

Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation

Raphael A. C. Viera*†‡, Jean-Max Dutertre*, Rodrigo Possamai Bastos†, and Philippe Maurine‡,
* Ecole Nat. Sup. des Mines de St-Etienne (Gardanne, France)
† Univ. Grenoble Alpes, CNRS, TIMA (Grenoble, France)
‡ LIRMM, CNRS, UMR N5506 (Montpellier, France)
{raphael.viera, dutertre}@emse.fr, rodrigo.bastos@univ-grenoble-alpes.fr, philippe.maurine@lirmm.fr

***Abstract*—Laser fault injection attacks induce transient faults into ICs by locally generating transient currents capable of temporarily flipping the outputs of logic gates. Laser fault injection may be anticipated or studied by using simulation tools at different abstraction levels: physical, electrical or logical. At the electrical level, the general laser-fault injection model is based on the addition of current sources to the various sensitive nodes of CMOS transistors. This type of electrical model does not take into account the large transient current components also induced between VDD and GND as a result of laser illumination. Such current components have no direct effect on the logic gate output nodes. Still, they provoke a significant IR-drop that may, in turn, contribute to the fault injection process. This paper describes our research on the assessment of this contribution. It introduces an upgraded electrical model taking the laser-induced IR-drop into account. It also proposes a methodology that allows the model's use to simulate laser-induced faults at electrical level in large-scale circuits. On the basis of simulations with a case-study circuit, we found that, depending on the parameters of the laser pulse, the number of injected faults may be underestimated by a factor as large as 48 if the 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.**

I. Introduction

Lasers have been used since the 1960s in order to simulate the effects caused by radiations on semiconductors [1]. In the early 2000s, [2] reported the use of laser illumination to induce faults into secure integrated circuits, e.g., a bit-flip into a SRAM cell. This created an urgent 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. At electrical-level, a double exponential current source has been demonstrated efficient for modeling at first order a laser shot [3], [4], [5]. These current sources are 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 [6]. These currents temporarily flip the outputs of few gates. This undesired state propagates through the logic toward the inputs of registers (flip-flops or latches) and, if it is still present when the clock edges occurs, memory bits may be inverted, producing soft errors (SE). However, the laser-induced current component responsible for flipping the output of a gate comes with other current components flowing from VDD to GND, which will produce a temporary power supply voltage drop (IR drop). Thus, a question, that will be later addressed in this paper, is raised: can this short-circuit creates significant IR drops and thus lead to a false estimation of the fault injection threshold? This is an important question since as technology scales, ICs become increasingly sensitive to IR drops [7], [8]. Furthermore, as experimentally observed in [9], this current may be more than an order of magnitude higher than the current flipping the outputs of logical gates. This implies that the models used so far (e.g., [5], [10], [11], [12]) for simulating the effects of laser shots on ICs designed in advanced technologies may lack accuracy.

To the best of our knowledge, there is only one investigation from [13] on the role of IR drop in the fault injection process related to laser illumination. This modeling work has 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. Furthermore, they did not extended their work beyond the scope of a single inverter.

In order to fill this gap, the contributions of this paper are:

- a transient fault model that takes into account the laser induced IR drop effects in the power and ground rails;
- a methodology, based on standard CAD tools and the proposed model, to simulate with the highest accuracy the effect of laser shots on complex circuits;
- an analysis providing some highlights on how soft errors are induced by the laser shots and the importance of laser-induced IR drops in the fault injection process.

II. State of the Art of laser fault injection and limits of the classical approach

A. Modeling laser effects on ICs

1) Laser Induced Transient Currents and Classical Transient Fault Model: 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 [6]. 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 [14].

Fig. 1 illustrates, on a basic example, the classical model explaining where laser shots generate a parasitic current. In case the inverter input is in low state 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 $P_{substrate}$. The effect of a laser is thus modeled by a current source as depicted in Fig. 1(a) placed between the drain and the source of the NMOS transistor. A similar reasoning can be made for Fig. 1(b) when the inverter input is high ('1'). In that case, the susceptible part of the inverter is the drain of the PMOS transistor.

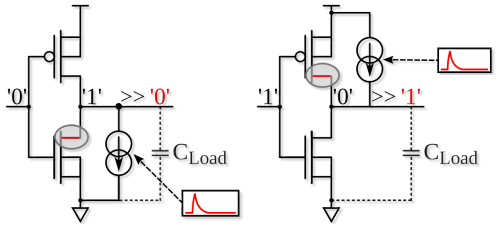


Fig. 1: Transient current modeled as a current source for: (a) the NMOS sensitive drain (b) the PMOS sensitive drain of an inverter.

In both cases, these transient currents have the shape of a double exponential and flow from the drain of the NMOS to the $P_{substrate}$ biasing contact as in Fig. 1(a) (resp. from the $Nwell$ biasing contact to the drain of the PMOS in Fig. 1(b)). In case of Fig. 1(a) (resp. Fig. 1(b)), a part of the induced current discharges (resp. charges) the inverter output capacitance. As a result the inverter output undergoes a voltage transient.

2) Spatial Distribution of Laser Beam Energy: The beam diameter is 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 [15], or a drop of $\frac{1}{e^2}$ from its peak value.

The effects of a Near Infra-Red laser beam have been modeled in [16] and later in [17]. 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} that follows the empirical equation:

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

where V is the reverse-biased voltage, 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 the area of the exposed PN junction. One can refer to [17] for additional details of the above parameters.

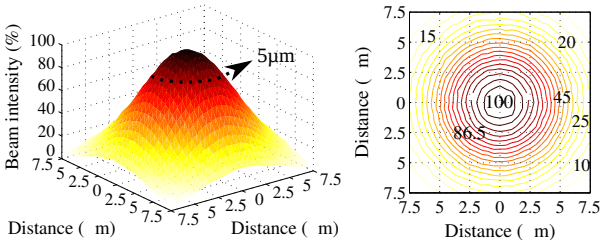


Fig. 2: Laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot: (a) Three-dimensional view (b) contour lines.

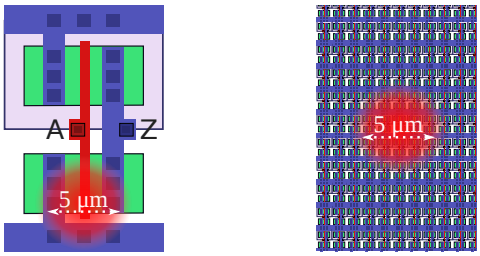
By way of illustration, Fig. 2(a) shows a three-dimensional view of the normalized amplitude of a laser spot. Beam intensity at a given coordinate (x,y) represents the amount of power delivered by the laser source at this specific point. Fig. 2(b) presents the contour lines of Fig. 2(a) in order to provide a topographic view of the laser beam intensity.

B. Limits of the Classical Transient Fault Model

The fault model of Fig. 1 uses current sources attached to the drain of laser sensitive transistors since these currents are the root cause of the transient fault injection mechanism. This 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, as illustrated in Fig. 3(a). For advanced technologies this model is questionable. Looking at Fig. 3(b), which shows standard cells of a 28 nm technology being illuminated by a laser source with 5 μm spot diameter, it is clearly visible that the laser shot simultaneously illuminates several gates at a time and probably not only one PN junction.

Another transient current component flowing from VDD to GND that may have a significant effect on the fault injection mechanism is not taken into consideration by the model of Fig. 1. This current transient is induced in the reversed biased $Psub$-$Nwell$ junction that surrounds every $Nwell$. If the sensitive transistor is a NMOS, the laser beam will induce charge carriers along its path that will be sufficiently close to a $Psub$-$Nwell$ junction to induce a transient current in it flowing from VDD to GND.

The $Psub$-$Nwell$ junction is always reversed biased and has an area larger than that of a transistor drain (the parameter S in (1)). Thus, it is no surprise that the authors of [9] reported on experimental basis that the transient current component flowing directly from VDD to GND (IP_{Psub_nwell} in Fig. 4) may be more than an order of magnitude greater than those flowing in the drains of the sensitive transistors (I_{Ph} in Fig. 4). This transient VDD to GND current may thus have a significant influence on the laser fault injection mechanism. This work aims at evaluating this influence and at offering a methodology to take it into account.



tech: 250nm - Hstd_cell: 12.5 µm (a) tech: 28nm - Hstd_cell: 1.2 µm (b)

Fig. 3: Standard cell(s) being illuminated by a 5μm laser spot diameter: (a) in 250nm technology. (b) in 28nm technology.

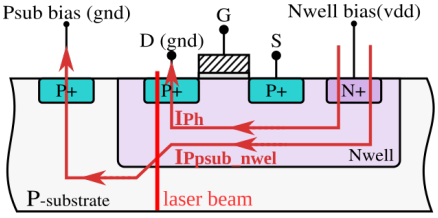


Fig. 4: Laser-induced current components. Cross-section of a PMOS transistor.

III. Upgraded Electrical Model and its Consequences on the Laser-Induced Fault Injection Mechanism

It is introduced in Fig. 5, as an example applied to the inverter case, an illustration of the upgraded electrical model designed to take into account the laser-induced VDD to GND current and its associated IR drop. For each standard cell in the effect range of the laser beam a current source, denoted IP_{Psub_nwell} in Fig. 5, is added to the netlist. This current has the classical shape of a double exponential and its peak amplitude is obtained from (1). In this case, the parameter S (area of the PN junction) corresponds to the cell's $Nwell$ area. This current is thus larger than that induced at a sensitive transistor drain because 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 VDD to GND trough the power and ground networks of the device under attack. Since the power grid exhibits both resistive and capacitive electrical behaviors, a voltage drop of the local VDD and also a ground bounce of the local GND delivered to the various std_cells is induced (the term IR drop is used throughout this paper to refer to this complex phenomenon). Since this paper provides a simulation flow using standard tools, it is considered that the power-grid model is automatically generated by the tool, thus facilitating the overall analysis and decreasing the simulation flow time.

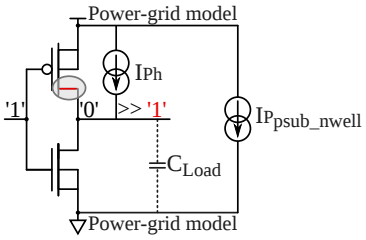


Fig. 5: Proposed laser-induced transient fault model applied to an inverter with input biased at VDD. Introducing the voltage drop/bounce contribution in the power rails by the current component IP_{Psub_nwell} for a given power-grid model.

A. Soft-error occurrence due to a laser shot

This section clarifies how a laser-induced transient fault can cause a soft error. The diagrams presented in Fig. 6(a)-8(a) show the timing paths to be analyzed. FF_i is the source register, FF_o is the destination register, and between, the combinational logic.

1) Influence of the I_{Ph} current component - Classical model: Laser shots generate parasitic currents that temporarily flip the output of few gates by means of a transient current modeled by I_{Ph} in Fig. 6(b). This undesired state propagates toward the input of FF_o (signal D_o in Fig. 6(c)) and, if still present when the clock edge occurs it is latched: a soft error appears as represented by the signal Q_o in Fig. 6(c).

2) Influence of the IP_{Psub_nwell} current component: Nowadays, IR drops can reach up to 20% of the power supply voltage [8]. However, when a laser illuminates the circuit, IR drops are even more accentuated in the affected cells. With the decrease of the power supply voltage, the speed of critical paths reduces by nearly the same ratio [18]; in particular, delays of some specific gates increase largely due to IR drops [19]. Therefore, IR drop can induce timing errors or even data disruption.

In case of timing errors, the timing constraints for a synchronous design are violated. These constraints require that the minimum clock period T_{CLK} (Fig. 7(c)), necessary for the circuit to operate correctly, must be superior or equal to:

$$T_{CLK} \geq t_{clk2Qi} + Q_i 2D_o + t_{setup}, \quad (2)$$

where t_{clk2Qi} is the FF_i clock-to-Q delay. $Q_i 2D_o$ is the maximum data path propagation delay and t_{setup} represents the setup time (minimum amount of time before the clock edge during which the signal D_o must be valid and stable).

Fig. 7 shows an example in which a voltage drop induced by the current IP_{Psub_nwell} causes a setup time violation in the data path.

3) Influence of I_{Ph} and IP_{Psub_nwell} current components: Until now, the influence of the current components I_{Ph} and IP_{Psub_nwell} have been considered separately. In Fig. 8(c) both components are taken into account. As a result, signal D_o shows a different profile of transient fault than the same signal in Fig. 6(c). The principle behind the observed amplification

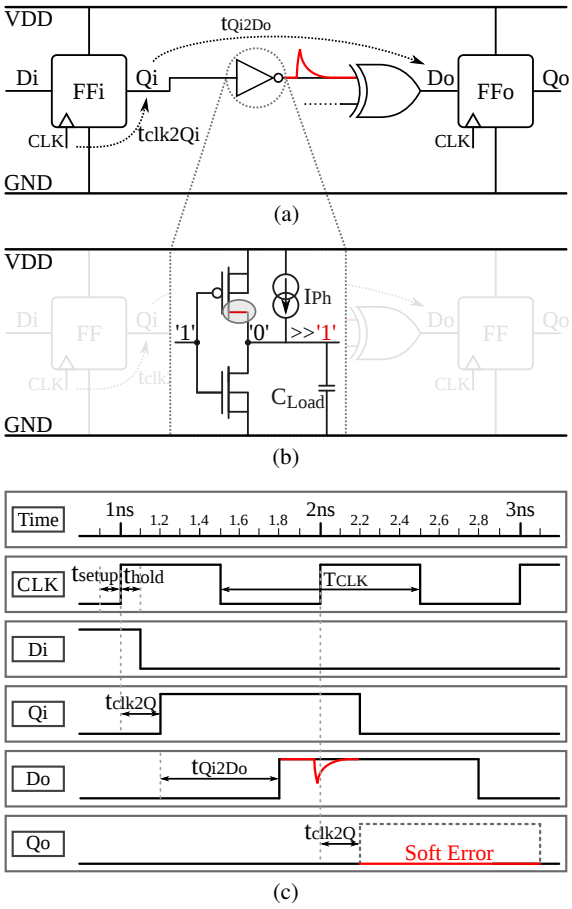


Fig. 6: Propagation of a corrupted signal along the data path and sampling of the signal at the next rising clock edge.

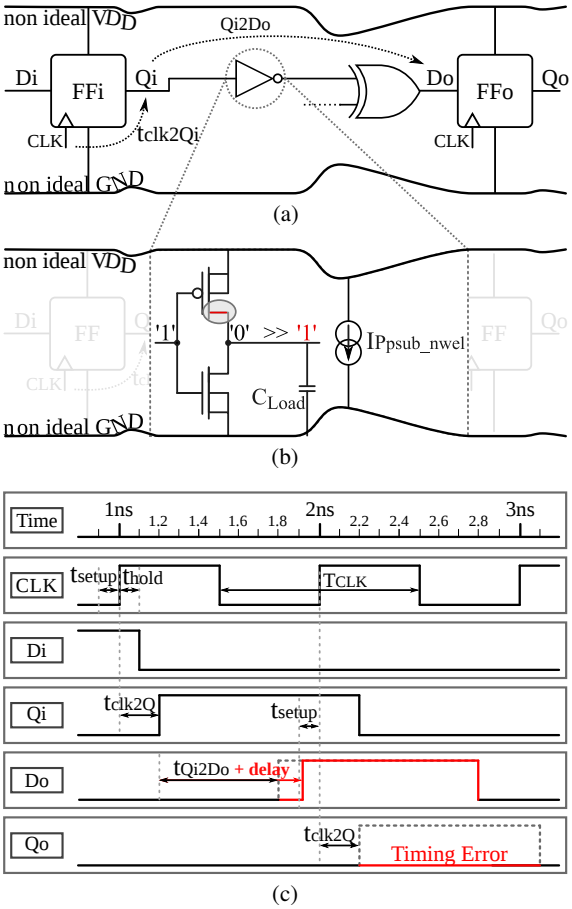


Fig. 7: Propagation of a signal along the data path and sampling of the signal at the next rising clock edge with increased delay leading to timing error due to IR drops.

of the amplitude and width of the transient fault profile will be addressed in the next section. However, Fig. 8(c) suggests that the contribution of both current components increase the total number of soft/timing errors observed in the circuit because the induced perturbations have higher amplitude and width.

4) Threshold for the Occurrence of Soft Errors: In the three models presented in Fig. 6-8, there is no fixed threshold on the laser shot characteristics (power, pulse width, etc.) indicating when a soft error occurs or not. In fact, the occurrence of a SE depends on the cell that has been illuminated by the laser beam and also on many design parameters such as the clock period, the timing slack, etc. A key parameter is the handled data which influences the data propagation time and the localization of the laser-sensitive areas. Particularly, in the models presented in Fig. 7-8, in which the influence of the current component IP_{Psub_nwell} is considered, the occurrence of SE also depends on the depth of the cell in its data path.

IV. Simulation Flow

With all former considerations, Fig. 9 proposes a non-exhaustive step by step simulation methodology. This methodology, which is based on standard CAD tools (Cadence® Voltus™ for EMIR simulation and Cadence® Voltus™-Fi using Cadence® Spectre® for the electrical simulation), allows to analyze the impact of IR drops induced by laser shots on complex circuits with the highest accuracy.

V. Evaluating by Simulation the Importance of IR Drops in the Fault Injection Mechanism

A. Testbench

1) Device Under Test: The device under test (DUT) shown in Fig. 10 is an ARM 7 processor with 5k+ cells designed in a 28 nm technology. The core voltage is 1 V and clock period of 1 ns. The circuit area is 110 μm x 70 μm. The cells highlighted in white are those of the critical path (made of 38 instances).

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 [20], [21]. Consequently, a laser spot does not induce a single transient current in a single gate, but several transient currents at different sensitive nodes of the target. Without loss of generality, a spot diameter of 5 μm, as illustrated in Fig. 10, has been chosen for the experiments reported below.

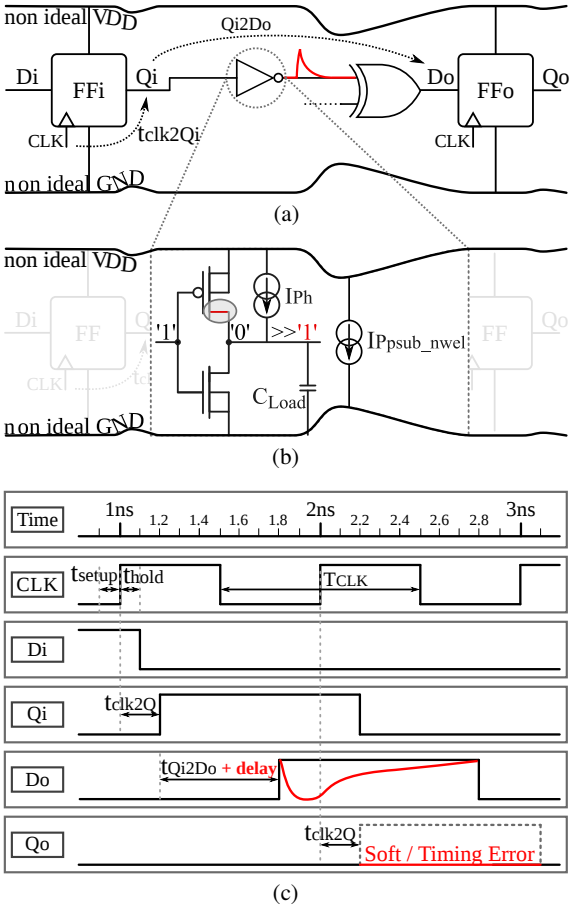


Fig. 8: Propagation of a corrupted signal along the data path and sampling of the signal at the next rising clock edge plus increased delay leading to soft/timing errors due to IR drops.

B. Laser Induced Currents and IR drop

IR-drop evaluation tools consider two types of currents: static and dynamic. The static IR drop is the average voltage drop for the design. The dynamic IR drop is evaluated when large amounts of circuitry switch simultaneously, causing peak current demand [7], thus, it depends on the switching activity of the logic, which is suited for simulating the dynamic behavior of a laser-induced current. Based on the dynamic current files generated in the power analysis flow, the total dynamic current of the DUT, in presence of a laser shot or not, is shown in Fig. 11. These currents were simulated on a 2 ns time slot (the clock period is 1 ns) in which there is a significant switching activity.

The model of Fig. 5 was used to simulate the dynamic current induced by a laser shot that contributes to the dynamic IR drop. Fig. 11(a) and 11(b) show the total dynamic current on VDD and GND rails respectively, in normal operation. Fig. 11(c) and 11(d) report the total dynamic current in presence of a laser pulse with a duration of 250 ps starting at 1.5 ns. The current peak is approximately ten times greater than in normal operation for this case-study.

Fig. 12 displays the same simulation results as the strength

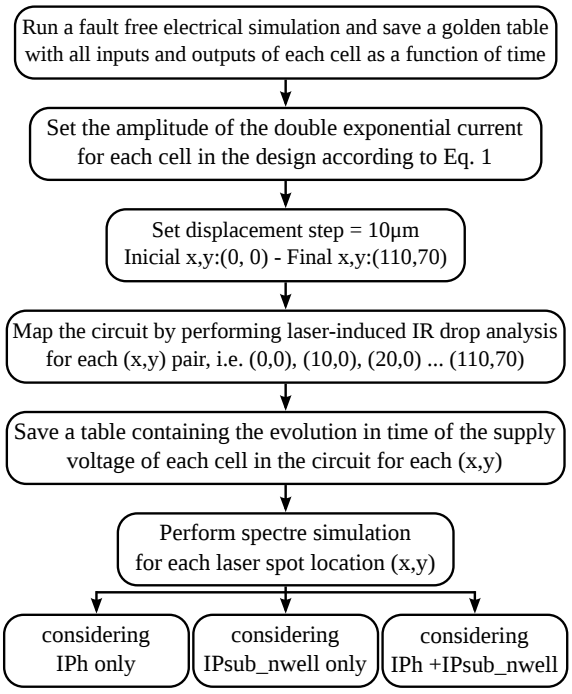


Fig. 9: Simulation flow.

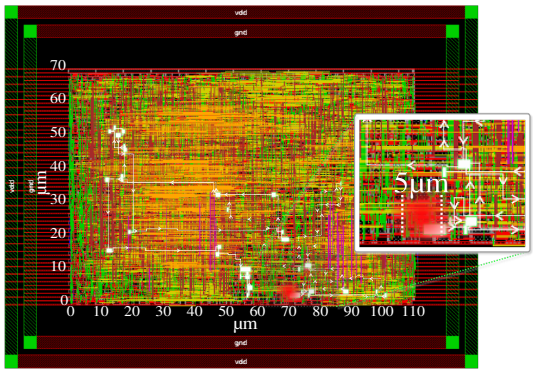


Fig. 10: Layout of the ARM7 DUT with its critical path and the 5μm laser spot diameter in evidence.

of the IR drop voltage (expressed in mV) depicted with a color scale on the DUT floorplan. With no laser illumination, the IR drop is distributed across the circuit's core with a peak value of 50 mV (Fig. 12(a)). In the presence of a laser shot at coordinates x=70 μm, y=5 μm, the IR drop effect area has an ellipsoidal shape stretched along the X axis, with a peak value of 791 mV (Fig. 12(b)). It extends along the the X axis of the power-grid main metal lines for over more than 60 μm. Whereas its extension along the Y axis is only approximately two times its 5 μm diameter. There are hundreds of standard cells inside the laser-induced IR drop area that accounts for the additional 25 mA of current, meaning that a few hundreds of μA are distributed to each affected cell in this area.

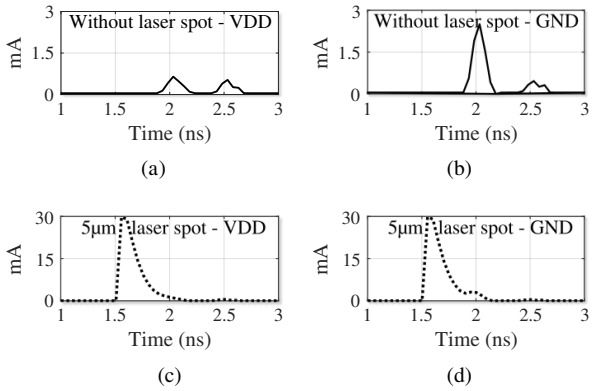


Fig. 11: ARM7 maximum total dynamic current flowing in: (a) VDD rail without laser shot, (b) GND rail without laser shot, (c) VDD rail in presence of a 5μm laser shot, (d) GND rail in presence of a 5μm laser shot.

C. Voltage Drop Propagation

To illustrate how the IR drop propagates in the circuit, refer to Fig. 12(a) and 12(b). In Fig. 12(a), 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. Now refer to Fig. 12(b) in which the laser shot is considered. The effect area of the 5 μm laser spot 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. Fig. 12(b) reports the IR drop at its apex: an amplitude of 791 mV is observed. At this time, the voltage swing is reduced to 209 mV. This value is far below the nominal core voltage of 1 V.

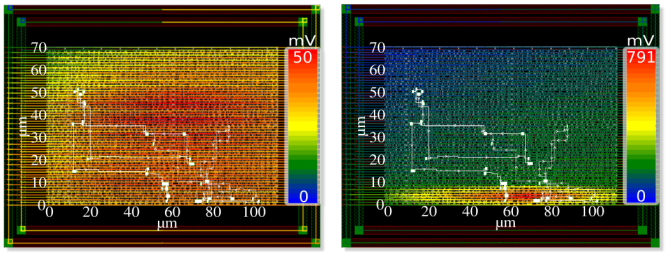


Fig. 12: ARM 7 Layout with 5k+ instances (critical-path with 38 instances in evidence): (a) Maximum voltage drop (IR-Drop + Bounce) in normal operation condition. (b) Maximum voltage drop in presence of a 5μm laser shot.

D. Simulated Scenarios

We report a total of 9 simulated scenarios among the studied. They are illustrated in Fig. 13(a) that shows in the first line the clock signal waveform used as a time reference. The three other lines give the typical evolutions observed during our simulations, of the signal Q_x, the output of the cell 'x' of the design under illumination, in three different situations. These three situations represent the behavior when a laser pulse with 250 ps of duration starts at 1.5 ns, 1.7 ns and 1.9 ns respectively. These times are progressively closer to the next rising clock edge that occurs at 2 ns.

The 2^{nd} line of Fig. 13(a) gives these evolutions when only the I_{Ph} current sources with a double exponential shape are considered to model the laser effects. The 3^{rd} line gives these evolutions when only the IP_{Psub_nwell} current sources with the power-grid model are considered. The 4^{th} line gives the evolutions when both the current sources I_{Ph} and IP_{Psub_nwell} plus the power-grid model are considered.

In the 2^{nd} line, the curves have a double exponential waveforms. In the 3^{rd} line, they have also a double exponential waveform but the latter are smoother. This is due to the filtering effect (RC effect) of the supply voltage network that also reduces their amplitude with respect to line 2. The shape of the curves is similar in the 4^{th} line to that of lines 2 and 3. However their amplitude is much more important and are even greater than the sum of the amplitude of the corresponding curves in lines 2 and 3.

E. Fault Injection Maps

For the purpose of assessing the contribution of the laser-induced IR drop to the fault injection phenomenon we drew fault sensitivity maps on simulation basis for different areas: 1^{st} by considering only the laser-induced transient currents between the drains and the substrates of the sensitive transistors (I_{Ph}), which are used as a reference for the classical electrical model; 2^{nd} by considering only the laser-induced IR-drop (IP_{Psub_nwell} with power-grid model); 3^{rd} by considering both phenomena. These simulations were performed for locations of the laser spot sweeping the whole circuit area ($110\,\mu m$ x $70\,\mu m$) with X and Y displacement steps of 10 μm. For each location, the various scenarios of Fig. 13(a) were used. Figs. 13(b-j) reports the obtained fault maps, where red dots correspond to the occurrence of a fault and blue dots the absence of faults (each dot location is that of a simulated laser shot). Note that we considered only bit-flip faults, i.e. faults corresponding to the flipping (with reference to normal operation) of the output state of one or more flip-flops.

The first line of Fig. 13(b-j) (Fig. 13(b), (c) and (d)) represents the simulations performed considering only the I_{Ph} influence, i.e., laser-induced IR-drop is ignored. Since the transient current profile has a width of 250 ps, when this current is applied closer to the flip-flop sampling window (time window of width t_{setup} + t_{hold} centered on the rising edge), more faults are observed from left to right, which corresponds to scenarios 1, 2 and 3.

In the second line of Fig. 13(b-j), only the IR-drop effects are taken into account (i.e. IP_{Psub_nwell} with power-grid model). One may observe that laser induced IR-drop can cause by itself faults in the circuit due to many factors such as timing errors or even data disruption.

The third line of Fig. 13(b-j) reports the fault maps for which both the I_{Ph} and IP_{Psub_nwell} with power-grid model are considered. By comparison to the 1^{st} line, it reveals that

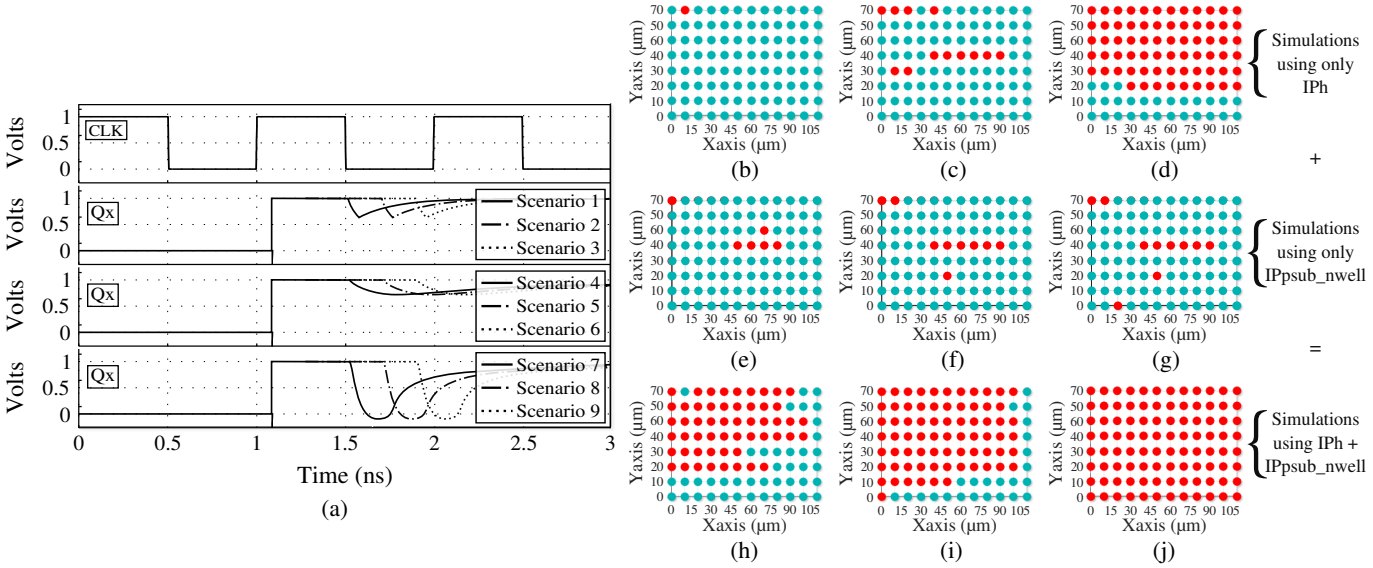


Fig. 13: (a) Typical waveforms observed during simulations at the output of gates illuminated by a laser beam. Line 1: clock signal. Line 2: waveforms observed when considering I_{Ph} contribution only. Line 3: waveforms observed when considering IP_{Psub_nwell} contribution only. Line 4: waveforms observed when considering I_{Ph} + IP_{Psub_nwell} contributions. (b-j) Maps of laser-induced faults for the simulated scenarios.

the fault areas are larger than expected for all considered laser shot times. It also unveiled an extension of the laser sensitivity in time, particularly at 1.7 ns and 1.5 ns, the number of faults are increased respectively by a factor of 5.4 and 48. This demonstrates that IR drops induced by laser shots play an important role in the occurrence of faults, thus, not taking this effect into account leads to over optimistic results regarding the threshold of fault injection.

F. First-order approximation of the IR drop contribution to the fault injection mechanism

To understand how the superposition of the effects of IR drop and the current sources connected to the drains of transistors creates the strong effect depicted in the 4^{th} quadrant of Fig. 13(a) and in Fig. 13(h-j), consider the inverter case as depicted in Fig. 14. In normal operation with its input at zero, the current flowing in the PMOS transistor during the steady state, which is in its linear mode of operation, is equal to zero. For the sake of simplicity, consider that the laser-induced photocurrent has a constant amplitude $I_{Ph_{NMOS}}$ (as described by (1)). Thus, this current will flow through the ON PMOS transistor and a voltage ΔV_{out} will appear across the PMOS as expressed by (3):

$$\Delta V_{out}(withoutIR) = \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}, \quad (3)$$

in which $I_{Ph_{NMOS}}$ is the photocurrent amplitude, W and L the width and the length of the PMOS transistor, μ the hole mobility, C_{ox} the oxide thickness and V_T the threshold voltage.

In the above simple calculation, the supply voltage is considered unaffected by the laser shot and thus equal to VDD. Considering now that the laser shot simultaneously generates

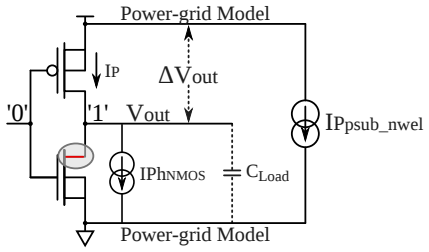


Fig. 14: Inverter with a low input signal under laser illumination.

an IR drop affecting VDD with an amplitude denoted V_{drop}. It will in turn affect ΔV_{out} the voltage across the PMOS according to:

$$\Delta V_{out}(withIR) = V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}, \quad (4)$$

As shown by (4), the effect of the IR drop on the ΔV_{out} is hyperbolic. Voltage drops induced by laser shots have thus an important effect and cannot be neglected. This is especially true for ICs designed in advanced technologies for which the supply voltage is low with respect to the threshold voltages, as shown by:

$$\frac{\Delta V_{out}(withIR)}{\Delta V_{out}(withoutIR)} = \frac{1}{1 - \frac{V_{drop}}{V_{DD} - V_T}} \quad (5)$$

that gives the amplification by the IR drop of the laser induced perturbation at the gate output.

By way of illustration, Fig. 15(a) gives some simulated V_{out} values for different V_{drop} in case of a basic 28nm CMOS

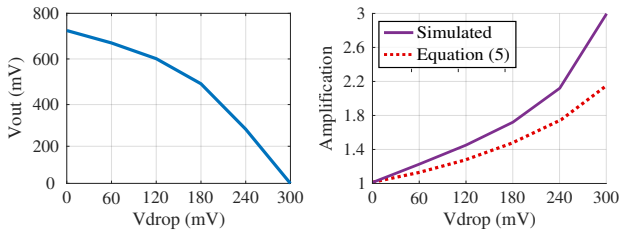


Fig. 15: (a) Simulated V_{out} values with regard to V_{drop} (b) IR drop amplification according to (5) and electrically simulated.

inverter. As expected from the above equation, the higher the V_{drop}, the lower V_{out} is. Similarly, Fig. 15(b) gives, for the same inverter, the simulated and calculated IR drop induced amplification of the perturbations. The obtained trend is in accordance with (5) even if the modeling of the IR drop effect remains of first order.

G. Probability of soft error occurrence

The occurrence of SEs due to a laser shot basically depends on the following: the laser spot diameter, the transient fault profile, the time when the laser shot is applied in the circuit with regard to the clock signal, the position of the affected cells in the circuit and the handled data. Considering these parameters fixed, the probability of a SE occurrence depends on the data path propagation delay of a particular signal.

On simulation basis, Fig. 16 shows the probability of SE occurrence on two signals affected by a laser shot at position (x,y). The output of the observed signals were saved with a time step of 50 ps in a range of two clock cycles, i.e. 2 ns. Note in the fourth line of Fig. 16 how the probability of soft/timing error occurrence due to the contribution of I_{Ph} + IP_{Psub_nwell} (proposed model) is always higher than the contribution of I_{Ph} alone (classical model). Furthermore, the time when the laser shot is applied causing a SE is more unpredictable due to the delay caused by the IP_{Psub_nwell} current component that induces IR drops in the power rails.

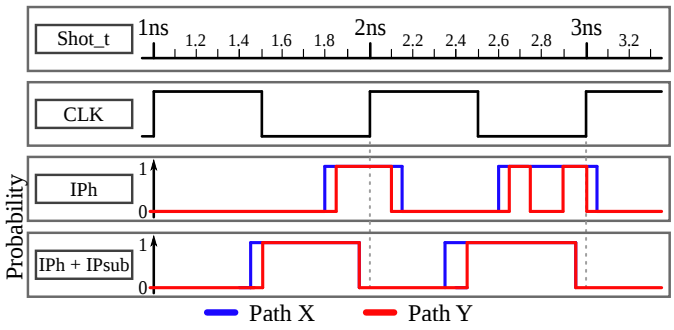


Fig. 16: Probability of SE occurrence. $Shot_t$: Laser shot time. I_{Ph}: I_{Ph} contribution only. IP_{Psub}: IP_{Psub_nwell} contribution only. I_{Ph} + IP_{Psub}: I_{Ph} + IP_{Psub_nwell} contribution.

VI. Conclusions

This paper highlighted how laser-induced IR drop effects significantly contribute to fault injection. A model that takes into account the voltage drop effects in the power and ground rails has been presented. The model was used in a methodology which allows the simulation of laser-induced IR-drop at circuit scale. This methodology was applied to a test-chip in order to demonstrate how IR drop facilitate the occurrence of SEs by amplifying laser induced perturbations on logic signals.

The results reveal that ignoring the laser-induced IR drop may result in underestimating the risk of fault injection, not to mention the incorrect estimation of the fault injection threshold. Indeed, for the test-chip assessed, an impressive increase in the number of faults by a factor of 48 has been observed when IR drops are taken into account. This result is especially relevant for the design of countermeasure techniques for secure integrated systems.

References

[1] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, Oct 1965.

[2] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *4th International Workshop on Cryptographic Hardware and Embedded Systems*. London, UK: Springer-Verlag, 2002, pp. 2–12.

[3] A. G. Jordan and A. G. Milnes, "Photoeffect on diffused p-n junctions with integral field gradients," *IRE Transactions on Electron Devices*, vol. 7, no. 4, pp. 242–251, Oct 1960.

[4] J. L. Wirth and S. C. Rogers, "The transient response of transistors and diodes to ionizing radiation," *IEEE Transactions on Nuclear Science*, vol. 11, 1964.

[5] F. Lu *et al.*, "Laser-induced fault simulation," in *2013 Euromicro Conference on Digital System Design*, 2013.

[6] A. H. Johnston, "Charge generation and collection in p-n junctions excited with pulsed infrared lasers," *IEEE Trans. Nucl. Sci.*, 1993.

[7] J. Ma *et al.*, "Identification of ir-drop hot-spots in defective power distribution network using tdf atpg," in *2010 5th IDTW*, Dec 2010.

[8] S. Zhao and K. Roy, "Estimation of switching noise on power supply lines in deep sub-micron cmos circuits," in *VLSI Design, 2000. Thirteenth International Conference on*, 2000, pp. 168–173.

[9] J.-M. Dutertre *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, Sep. 2014.

[10] A. Douin *et al.*, "Electrical modeling for laser testing with different pulse durations," in *11th IEEE IOLTS*, July 2005, pp. 9–13.

[11] H. M. Huang *et al.*, "Fast-yet-accurate variation-aware current and voltage modelling of radiation-induced transient fault," in *DATE*, 2016.

[12] C. Godlewski *et al.*, "Electrical modeling of the effect of beam profile for pulsed laser fault injection," *Microelectronics Reliability*, Aug. 2009.

[13] L. Hériveaux *et al.*, "Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design," in *39th ISTFA ASM*, 2013.

[14] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, Oct 1965.

[15] S. Buchner *et al.*, "Pulsed-laser testing for single-event effects investigations," *IEEE Transactions on Nuclear Science*, 2013.

[16] G. C. Messenger, "Collection of charge on junction nodes from ion tracks," *IEEE Transactions on Nuclear Science*, 1982.

[17] A. Sarafianos *et al.*, "Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology," in *IRPS, 2013 IEEE International*, April 2013, pp. 5B.5.1–5B.5.9.

[18] X. Wang and D. Su, "On-chip emi monitoring for integrated circuits of 55nm and below technologies," in *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI*, Aug 2014, pp. 1–4.

[19] K. Peng *et al.*, "Emulating and diagnosing ir-drop by using dynamic sdf," in *2010 15th ASP-DAC*, Jan 2010, pp. 511–516.

[20] F. Darracq *et al.*, "Backside seu laser testing for commercial off-the-shelf srams," *IEEE Transactions on Nuclear Science*, 2002.

[21] C. Roscian *et al.*, "Fault model analysis of laser-induced faults in sram memory cells," in *FDTC, 2013 Workshop on*, Aug 2013, pp. 89–98.