Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault-Injection

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

https://doi.org/10.1109/TCAD.2019.2928972
IEEE TCAD: Transactions on Computer-Aided Design of Integrated Circuits and Ssytems

Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault-Injection

Raphael A. C. Viera*†‡, Philippe Maurine*, Jean-Max Dutertre†, and Rodrigo Possamai Bastos‡ * LIRMM, CNRS, UMR N5506 (Montpellier, France)
† Mines Saint-Etienne, CEA-Tech, Centre CMP, F - 13541 (Gardanne, France)
‡ Univ. Grenoble Alpes, Grenoble INP, CNRS, TIMA (Grenoble, France)
{raphael.viera, dutertre}@emse.fr, philippe.maurine@lirmm.fr, rodrigo.bastos@univ-grenoble-alpes.fr

***Abstract*—Laser fault injections induce transient faults into ICs by locally generating transient currents that temporarily flip the outputs of the illuminated gates. Laser fault injection can be anticipated or studied by using simulation tools at different abstraction levels: physical, electrical or logical. At the electrical level, the classical laser-fault injection model is based on the addition of current sources to the various sensitive nodes of CMOS transistors. However, this model does not take into account the large transient current components also induced between the VDD and GND of ICs designed with advanced CMOS technologies. These short-circuit currents provoke a significant IR-drop that contribute to the fault injection process. This paper describes our research on the assessment of this contribution. It shows through simulation and experiments that during laser fault injection campaigns, laser-induced IR-drop is always present when considering circuits designed with deep submicron technologies. It introduces an enhanced electrical fault model taking the laser-induced IR-drop into account. It also proposes a methodology that allows the use of the model to simulate laser-induced faults at the electrical level in large-scale circuits. On the basis of further simulations and experimental results, we found that, depending on the laser pulse characteristics, the number of injected faults may be underestimated by a factor of up to 2.4 if the laser-induced IR-drop is ignored. This could lead to incorrect estimations of the fault injection threshold, which is especially relevant to the design of countermeasure techniques for secure integrated systems.**

***Index Terms*—Laser fault injection, Hardware security implementation, Methodologies for EDA, Electrical simulation.**

I. Introduction

Fault injection attacks have become a common way to defeat the security mechanisms of embedded devices. There is a large and constantly growing number of known techniques for injecting faults into ICs [1], [2]. Among them one can find techniques that:

- disrupt the clock signal [3],
- induce sudden variations of the supply voltage [4] or of the substrate bias [5],
- inject parasitic currents into using powerful electromagnetic disturbances or intense light flashes [1], [6].

The efficiency of optical attacks was first demonstrated using a camera flash [7]. However, to be able to influence each logic cell independently, and thus to better control the injected faults, focusable sources of ionizing radiations are preferable. Laser sources are such sources. Indeed they allow to control the injected faults with precision thanks to their high spatial and temporal resolutions as highlighted in [7], which reported in the early 2000s the use of laser to induce a bit-flip in a SRAM cell. Following this pioneering work, the necessity for designing robust circuits, resistant to laser fault injection attacks soon became apparent in the hardware security community. Hence the need for models and methodologies allowing researchers to forecast the effects of laser based attacks on ICs.

Although fault simulations can be performed at different abstraction levels of design flows (transistor level, gate level, RTL level, and even software level), low abstraction levels provide the highest accuracy.

When a laser illuminates an IC, it generates a parasitic (photoelectric) current [8]. This current generates an undesired transient voltage that propagates through the logic toward the input of a register (D-type Flip Flops) and, if it is still present when the next rising clock edge occurs, a bit may be inverted, producing a soft error (SE). At the electrical level, it has been demonstrated [9], [10] that this transient current can be efficiently modeled with a current source delivering a current with a double exponential shape. This current source is added to the netlist of the cell illuminated by the laser beam. Then an electrical level simulation, which is expected to take into account the effects of the laser illumination, is performed.

If such an explanation was found relevant for old CMOS technologies, it has been put into question for advanced submicron technologies. Indeed, with increasing transistor density, laser illumination does not affect a single transistor (or CMOS gate) but rather illuminates multiple gates simultaneously. In this case, a laser shot also induces a current that flows from V_{DD} to G_{ND} causing a temporary power supply voltage drop (IR-drop) known by designers to be a source of timing failures. As the induced IR-drop may be of significant amplitude and duration [11], it has to be taken into account while simulating laser fault injection.

The above remark implies that the models [12]–[15] used so far for simulating the effects of laser shots on ICs designed with advanced technologies can lack accuracy. Furthermore, the joint effects of the photoelectric currents and of the related

IR-drop can only be accurately simulated at low abstraction levels (taking into account the layout topology to better represent the physical phenomenon) in the scope of a whole system. The simulation must thus be performed on complex circuits and not just in one (or few) CMOS cell.

To the best of our knowledge, among the formerly proposed fault simulators [12], [16]–[20], the most recent one is [21] which is based on open-source code [22]. The major issue with these fault simulators is that they rely on electrical models [13], [15], [23] that are technology dependent. For instance, in [24], the authors proposed a model that includes vertical parasitic bipolar junctions inherent to MOSFETs in the fault injection process that may lead to IR-drop effects. However, they did not extend their work beyond the scope of a single inverter. In fact, modeling 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. None of the aforementioned articles consider the effect of laser induced IR-drop.

Within this context, the contribution of this paper is three-fold. Firstly, it shows through simulation and experiment that during a laser shot, an additional current component causing an IR-drop with a significant effect on the target operation is always present when considering circuits designed in relatively new technologies. Secondly, the paper introduces an improved transient fault model that takes the laser-induced IR-drop into account for simulation purposes. Thirdly, it is derived, from the enhanced fault model, which uses an adequate simulation methodology based on standard CAD tools (taking the induced IR-drop into account) to forecast the effect of laser fault injections in large scale circuits.

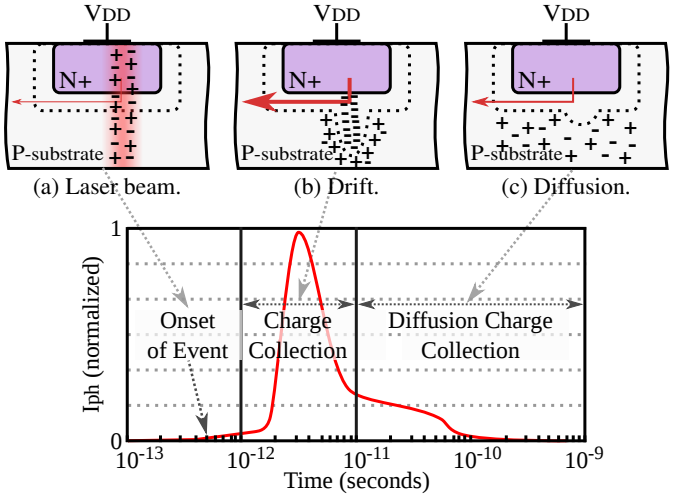
The rest of this paper is organized as follows. Section II recalls the background on the effects of laser illumination on ICs. Section III discusses the limitations of the classical fault model before introducing an enhanced fault model. Gate level simulations and experimental results of laser injections are given in Section IV in order to demonstrate the existence of laser-induced IR-drops and to validate the proposed enhanced fault model. Section V details the method used to simulate laser-induced faults in large-scale circuits, and Section VI analyzes simulation results provided by the proposed method. Additional evidence of the importance of laser-induced IR-drop at system level is provided in Section VII. Section VIII concludes the paper.

II. State of the Art of Laser Shot Effects on ICs

A. Effect of a Laser Shot at Transistor Level

ICs are known to be sensitive to induced transient currents. Such currents may be caused by a laser beam passing through the device, creating electron-hole pairs along the path of the laser beam [8]. These induced charge carriers generally recombine without any significant effect, unless they reach the strong electric field found in the vicinity of reverse biased PN junctions (the reverse biased junction is the most laser-sensitive part of circuits) [25]. In this case, the electrical field puts these charges into motion and a transient current flows. Each induced transient current has its proper characteristics such as polarity, amplitude and duration that depend on laser energy, laser shot location, device technology, device supply voltage and output load. The nature of these currents was first studied in the case of radioactive particles [26]–[30]. Laser illumination was first used as a way to emulate the effect of ionizing particles since the properties of the transient currents they both induce are similar.

Fig. 1 translates to the case of laser illumination the results of [25]. As shown in Fig. 1a, at the onset of an event caused by a laser shot, a track of electron hole pairs with high carrier concentration is formed along the path of the laser beam. When the resultant track traverses or comes close to the depletion region, carriers are rapidly collected by the electric field creating a current/voltage transient at that node. An interesting feature of the event is the distortion of the potential into a funnel shape [28], [31]. This funnel enhances the efficiency of the drift collection by extending the field depletion region deeper into the substrate (Fig. 1b). The profile of the funnel (size and distortion) depends on the substrate doping. This collection phase is completed in the picosecond range and followed by a phase where diffusion begins to dominate the collection process (Fig. 1c). An additional charge is collected as electrons diffuse into the depletion region on a longer time scale (nanosecond range) until all excess carriers have been collected, recombined, or diffused away from the junction area. A laser-induced transient current is thus called 'photocurrent' [9], [10]. The corresponding current pulse $I_{Photocurrent}$ (I_{Ph}) resulting from these three phases is shown in Fig. 1d. The red arrows in Fig. 1 represent the transient current flowing from the sensitive drain to the $P_{substrate}$ biasing contact tied at GND.



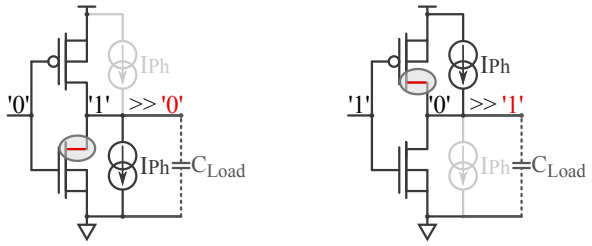
(d) Induced transient current.

Figure 1: Charge generation and collection phases in a reverse-biased PN junction and the resultant transient current caused by the passage of a laser beam [8], [25].

B. Effect of a Laser Shot at Gate Level

The effects of a laser shot are recalled in Fig. 2 which shows the case of an inverter where laser shots may generate photocurrents at gate level. When the inverter input is low (Fig.

2a), the most laser-sensitive part of the inverter is the NMOS transistor drain due to 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 (at G_{ND}). Similar reasoning can be made when the inverter input is high (Fig. 2b). In that case, the susceptible part of the inverter is the drain of the PMOS transistor. In Fig. 2a (resp. Fig. 2b), a part of the induced photocurrent (I_{Ph}) discharges (resp. charges) the inverter output capacitance. As a result the inverter output switches to low voltage (resp. high voltage), thus a so called voltage transient occurs.



(a) NMOS sensitive drain. (b) PMOS sensitive drain.

Figure 2: Electrical model of laser-induced transient currents applied to a CMOS inverter.

The beam diameter is one of the most important attributes 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 laser beam diameter is derived from the bivariate normal distribution of its intensity leading to measuring the beam diameter at 86.5% of its maximum value [32], or a drop of $\frac{1}{e^2}$ from its peak value.

The effects of a near infrared laser beam have been modeled in [33] and later in [23]. In the latter work, it is shown that the induced photocurrent (I_{Ph} in Fig. 1d), which is spatially distributed as a bivariate normal distribution, has a peak amplitude I_{ph_peak} that follows the empirical eq. (1):

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

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 used to take into account the laser pulse duration and S is the area of the PN junction (see [23] for additional details).

By way of illustration, Fig. 3 shows a three-dimensional view of the normalized amplitude of a laser spot. Beam intensity at a given (x,y) represents the amount of power delivered by the laser source at this specific coordinate.

C. Effect of a Laser Shot at Circuit Level

Fig. 2 illustrates where laser shots may generate an undesired transient current/voltage in a CMOS inverter. If this inverter is part of a larger combinational logic block (Fig. 4a), the transient voltage can propagate through the logic toward the input of memory cells (registers or latches). Depending on the transient voltage characteristics (width and amplitude)

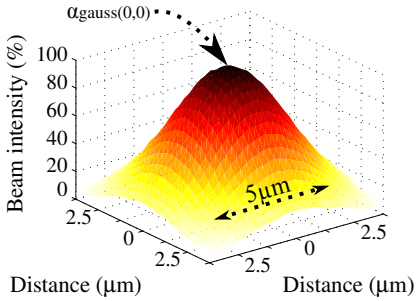
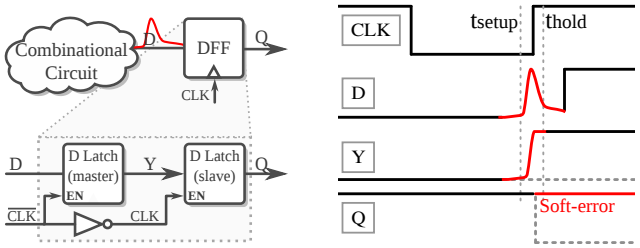


Figure 3: Three-dimensional view of a laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot.

the induced transient can still be present at the input of the Data-type Flip-Flop (DFF) when the rising clock edge occurs.

It is now not so rare to adopt a latch based design style. The main difference between latch based and DFF design styles is the insertion of a datapath between the master and slave latches of DFFs. Since SEs are due to the sampling of a wrong value by the master which is a latch, Fig. 4b is representative of what can happen in both design styles. This corresponds to the induction of a fault on the first phase of the clock signal ($\overline{CLK}$) in latch based ICs. The only remaining difference is that such SEs could also be directly induced by laser shots disrupting the datapath between the master and the slave during the second phase of the clock (CLK).



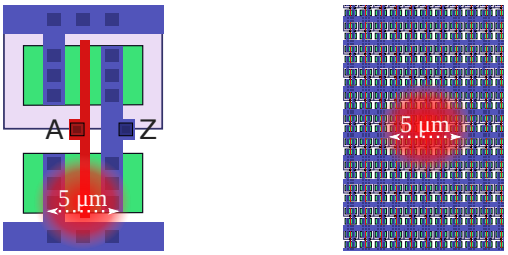
(a) Arbitrary datapath. (b) Waveforms of a datapath.

Figure 4: Propagation of a transient voltage through the combinational logic causing a soft error (in red).

III. Enhanced Laser Fault Model

1) Limits of the Classical Fault Model: The fault model in Fig. 2 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 a 1 μm to 5 μm spot diameter were able to target only one sensitive PN junction, as Fig. 5a illustrates. For advanced technologies this model is called into question. Looking at Fig. 5b, which shows 28 nm CMOS technology standard-cells being illuminated by a laser source with 5 μm spot diameter, it is clearly visible that the laser shot simultaneously illuminates at least 10 gates at a time and therefore not only one PN junction.

As a consequence, a transient current that flows directly from V_{DD} to G_{ND} is always induced. Fig. 6 illustrates the additional current component, named IPh_{Psub_nwell}. This



(a) 250 nm technology. Standard cell height: 12.5 μm

(b) 28 nm technology. Standard cell height: 1.2 μm

Figure 5: Standard cells being illuminated by a 5 μm laser spot diameter.

current is induced in the reversed biased $Psub$-$Nwell$ junction that surrounds every $Nwell$. Even if the laser beam is directed toward a sensitive NMOS, it also induces charge carriers that will be sufficiently close to a $Psub$-$Nwell$ junction to induce a transient current IPh_{Psub_nwell}. This current, which is not taken into consideration by the model in Fig. 2, can have a significant effect on the fault injection mechanism by inducing a supply voltage drop [34].

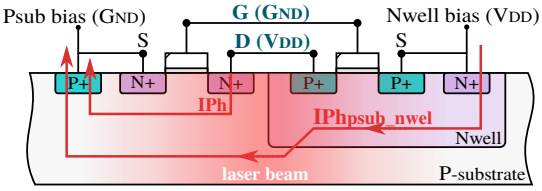


Figure 6: Laser-induced current components. Cross-section of a CMOS inverter.

2) Proposed Transient Fault Model of a Cell Under Laser Illumination: Fig. 7 shows, in the case of an inverter, the enhanced electrical model takes into account the laser-induced IPh_{Psub_nwell} current component. This current has no direct effect on the gate output as it draws current from the gate's power distribution network (PDN). As a result, the targeted gate power supply (V_{DD}) undergoes an IR-drop and its ground supply (G_{ND}) experiences a ground bounce. Furthermore, as neighboring cells are subject to similar transient currents, their effects add up and can propagate to distinct cells via the PDN.

However, the proposed electrical model (Fig. 7) is useless if the power supply grid is assumed ideal (i.e. V_{DD} and G_{ND} modeled by ideal supply sources and nets). It must thus be used in conjunction with the PDN. This explains why it is recommended to use the enhanced fault model in a simulation flow based on an Electromigration / IR-drop (EMIR) CAD tool. This kind of tool automatically provides the power-grid model for each cell in the design.

The current sources in Fig. 7 have a double exponential profile, such as the one illustrated in Fig. 1d. The currents have a peak amplitude defined by (1). The parameter S (area of the PN junction) corresponds to the PMOS drain area for I_{Ph}, while it is equal to the $Nwell$ area for the IPh_{Psub_nwell} component. IPh_{Psub_nwell} is usually larger than I_{Ph} since the drain area is significantly smaller than the $Nwell$'s area.

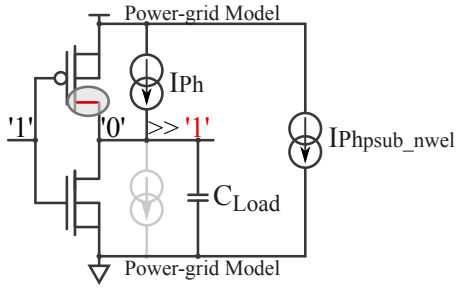


Figure 7: Proposed laser-induced transient fault model (applied to an inverter with input biased at V_{DD}) to take into account the supply voltage drop/bounce induced by the IPh_{Psub_nwell} parasitic current.

The IPh_{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 IPh_{Psub_nwell} currents add up and flow from V_{DD} to G_{ND} trough the power/ground networks of the device under illumination. Because the power grid is resistive and capacitive, local voltage drops and ground bounces occur thus reducing the voltage swing seen by standard cells in the close vicinity of the laser spot. This laser-induced voltage drop can by itself cause timing errors (timing constraint violations) or even data disruptions leading to sampling erroneous values by DFFs. This observation highlights the importance of considering the spatial distribution of the laser beam energy on the IC surface. It also highlights the importance of accurately modeling the power/ground network to simulate laser effects on ICs with accuracy.

IV. Simulation and Experimental Evidence of Laser-Induced IR-Drop

This section aims at giving evidence that a laser-induced IR-drop exists and should not be neglected during the design of secure systems. To achieve this, classical and enhanced models were applied on a ring oscillator (RO). The RO was also embedded in a FPGA for the purpose of backing up simulation results with experiments. Table I depicts in which order the results are presented: Section IV-B presents simulation and experimental results for both models in which the results were obtained by direct laser illumination of the RO's standard cells. Section IV-C also reports simulation and experimental results for both models, however the experiments were carried out with the laser aiming at regions near the RO (i.e. without direct laser illumination of its logic gates). In this case, the behavior of the RO remains unchanged if the classical fault model is correct. While, any change in its behavior shall indicate that the classical model is lacking representativity and accuracy.

A. Design Under Test (DUT)

A RO was chosen as DUT since its oscillation frequency varies linearly with the supply voltage over a wide range of V_{DD} [35]–[37]. This characteristic makes such a structure particularly interesting to experimentally monitor potential voltage drops caused by laser shots by measuring the evolution

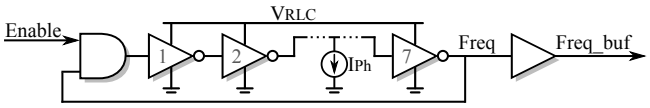
Table I: Presentation order of Section IV results

Laser illumination on a RO (Section IV-B)	**Laser illumination near a RO (Section IV-C)**
Simulation: classical model	Simulation: classical model
Simulation: enhanced model	Simulation: enhanced model
Experimental: laser shot on a RO	Experimental: laser shot near a RO

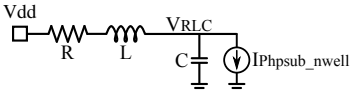
of their oscillation frequency [38]. The next paragraphs describe the RO electrical model used for simulation (IV-A1), its implementation details in FPGA (IV-A2), and the laser setup (IV-A3).

1) Electrical model of the RO used during simulations: The RO of Fig. 8a was designed using 65 nm technology. It features an AND2 gate, a BUFFER gate, and seven inverters. Its nominal oscillation frequency is equal to 148 MHz. The oscillation frequency was fixed in accordance with that of the RO considered during the experiments described in the following paragraphs to facilitate the joint analysis of experimental data and simulation results.

Fig. 8b shows a basic example of a series RLC distributed model [39] of V_{DD} between the supply pad and the inverters in Fig. 8a. The RLC network is used to consider the decoupling effect of the power grid as well as its inductance and resistance. This model therefore takes laser-induced IR-drops into account during simulations by setting $IPh_{Psub\_nwell} > 0$.



(a) RO block diagram including the IR-drop contribution (non-ideal V_{DD}) for a given power-grid model.

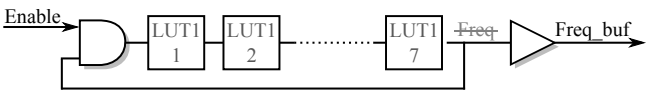


(b) Lumped elements of a series RLC network + IPh_{Psub_nwell} current component in parallel.

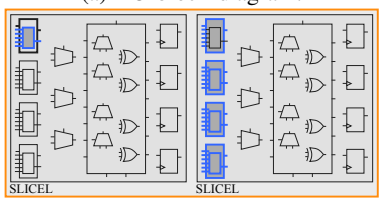
Figure 8: Single-ended ring oscillator used during simulations.

2) RO implemented on FPGA: A RO, similar to the one simulated, was implemented on a Virtex-5 FPGA [40] in order to launch experimental campaigns and also to ascertain the existence of a laser-induced IR-drop. This FPGA was chosen due to its flip-chip encapsulation allowing to perform laser shots from the backside (substrate).

The topology of the RO mapped onto the Virtex-5 is given in Fig. 9a. It is composed of five LUTs and has a nominal frequency equal to 148 MHz. Fig. 9b shows the placement of the LUTs in two different slices of the FPGA. The LUTs used to implement its seven inverters were placed in the same slice (the one on the right). The LUT used to implement the AND2 gate was placed in another slice to avoid disabling the RO during laser shots. The output buffer is associated with the IO port of the FPGA, thus having a fixed position (not shown in Fig. 9b).



(a) RO block diagram.



(b) Placement of the RO using the PlanAhead design tool [41].

Figure 9: RO implemented on a Virtex-5 FPGA.

3) Laser setup for the experimental fault injection: After implementing the RO on the Virtex-5, the board was mounted on a motorized XYZ stage in order to automatically perform laser-testing scans of its surface and thus to draw fault maps such as the ones reported in Section VII-A. These fault maps, as well as all other experimental results reported in the next sections were obtained using a laser source with 1,064 nm wavelength (infrared range). This source was used to generate laser pulses of a duration equal to 5 μs and of power equal to 1.04 W (considering 57.84% of the transmission coefficient of the lens). The size of the laser spot was set at 5 μm.

B. Simulation and experimental results for a laser shot applied on a RO

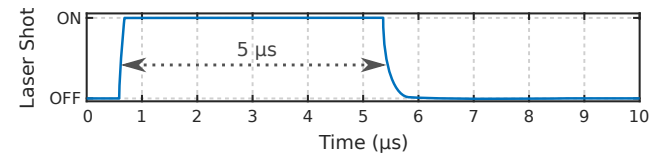
The next paragraphs give simulation and experimental results obtained for direct laser illumination of the RO.

1) Simulation result: classical fault model: As stated with the classical fault model, only the transient current I_{Ph} is induced by the laser illumination. In order to understand the effect of a laser shot on a RO according to this classical model, IPh_{Psub_nwell}, R, C and L were set to zero (Fig. 8b). Consequently the power supply is ideal (no IR-drop can occur) and all effects on the oscillation frequency are due to the increase in the illuminated inverters propagation delay.

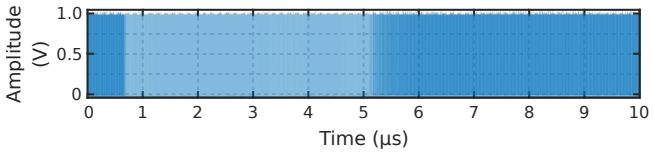
For this simulation, the I_{Ph} current source was tuned to provide current during $5\mu s$ as depicted in Fig. 10a. The resulting periodic signal Freq_buf is given in Fig. 10b in which the lighter blue region represents a time interval of roughly $5\mu s$ when Freq_buf has a frequency lower than 148 MHz. This lowering of the RO's output frequency is quantified in Fig. 10c. As illustrated, the frequency falls from 148 MHz to 100 MHz.

2) Simulation results: enhanced fault model: According to the enhanced fault model, a laser shot also induces a direct flow of current modeled by IPh_{Psub_nwell} (Fig. 8). By simply setting $I_{Ph} > 0$ (same current amplitude as in Fig. 10c), $IP_{Psub\_nwell} > 0$ and $(R, L, C) > 0$ (Fig. 8) it is thus possible to get an idea of the effect of a laser shot according to the enhanced model.

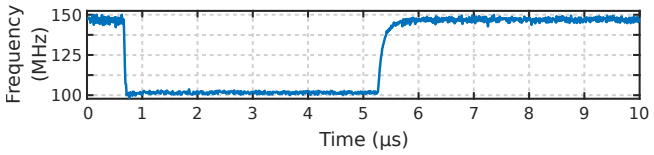
Fig. 11a depicts the shape of both I_{Ph} and IPh_{Psub_nwell} currents with duration of 5 μs and normalized amplitudes.



(a) Laser shot with pulse duration equal 5 μs.

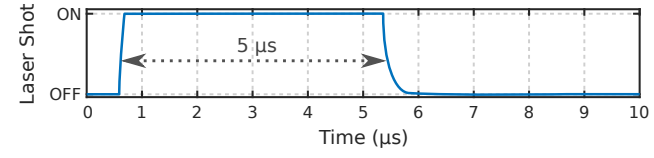


(b) Periodic signal $Freq\_buf$.

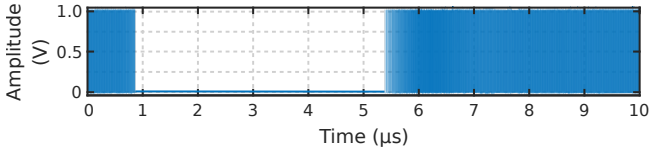


(c) Disturbance of the frequency over time.

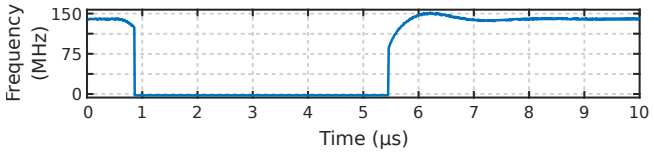
Figure 10: Simulation, according to the classical fault model, of the laser shot effect on the oscillation frequency of a RO.



(a) Laser shot with pulse duration equal 5 μs.



(b) Periodic signal $Freq\_buf$.



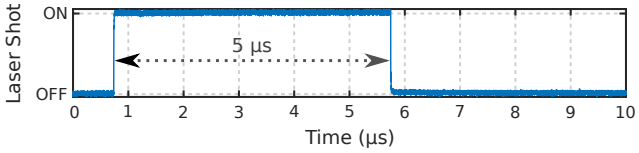
(c) Disturbance of the frequency over time.

Figure 11: Simulation, according to the enhanced fault model, of the laser shot effect on the oscillation frequency of a RO.

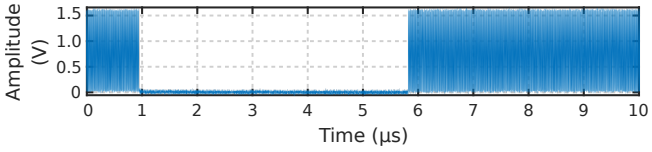
Fig. 11b shows the periodic signal $Freq\_buf$. In this figure a region where the signal $Freq\_buf$ if forced to zero appears. It is due to a cumulative effect between the laser-induced IR-drop provoked by IPh_{Psub_nwell} and I_{Ph}. As a result, this leads to the evolution of the $Freq\_buf$ frequency given by Fig. 11c. In this case, by considering the enhanced fault model, the RO stops oscillating for $5\mu s$. This indicates that the IR-drop induced by IPh_{Psub_nwell} amplifies the effect of I_{Ph} on the RO. This amplification effect will be further analyzed in Section VII-A.

3) Experimental results: laser shots on a RO: Experiments were carried out to measure the effects of laser shots on the RO oscillating frequency when targeting its logic gates.

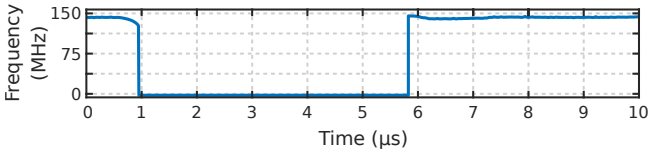
Fig. 12a depicts the laser shot with duration of 5 μs. The resulting periodic signal $Freq\_buf$ measured on the Virtex-5 is shown in Fig. 12b. In this case, during the laser shot, the $Freq\_buf$ signal stops oscillating. This experimental observation is in accordance with what has been simulated with the enhanced laser fault model. However, it is not a sufficient proof to conclude that the enhanced model is more accurate than the classical model. Additional evidence is reported in the next section.



(a) Laser shot with pulse duration equal 5 μs.



(b) Periodic signal $Freq\_buf$.



(c) Disturbance of the frequency over time.

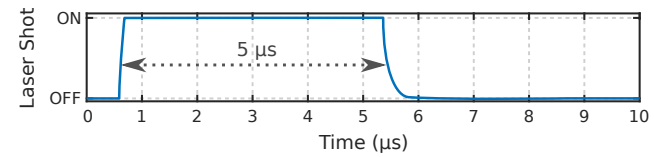
Figure 12: Measured effect (from the FPGA) on the RO oscillation frequency of a laser shot illuminating it directly.

C. Simulation and experimental results for a laser shot applied near a RO

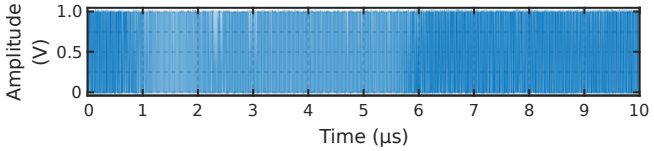
The next paragraphs discuss the effects of laser shots when they do not directly illuminate the RO but rather illuminate parts of the IC close to the RO. In this case, the only disturbance able to affect the RO is that of the induced IR-drop due to IPh_{Psub_nwell} if this transient current exists.

1) Simulation result: classical fault model: When applying the classical fault model in case of a laser shot striking the IC near the RO, no simulation is required because $I_{Ph} = 0$. Indeed, in this case the classical fault model predicts that there is no effect on the RO behavior as the PN junctions of the sensitive transistors drains will not be illuminated, therefore no current will be induced. If this prediction is not confirmed by experimental results, this means that the classical fault model is incomplete and underestimates the spatial distribution of the laser shot effects on ICs. This also indicates that the enhanced model is more appropriate.

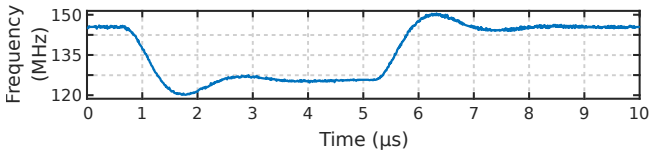
2) Simulation results: enhanced fault model: When choosing the enhanced model instead of the classical model, a simulation has to be run to get an insight into the effect of a



(a) Laser shot with pulse duration equal 5 μs.



(b) Periodic signal $Freq\_buf$.



(c) Disturbance of the frequency over time.

Figure 13: Simulation, according to the enhanced fault model, of a laser shot near the RO.

laser shot near the RO. Indeed, even if there is no photocurrent injected directly into the RO ($I_{Ph} = 0$ in the simulation), the IPh_{Psub_nwell} current flowing close to the RO alters its supply and thus its operations.

Fig. 13 shows the simulation results obtained in the case of a laser shot of duration equal to 5 μs as considered in former cases. The amplitude of IPh_{Psub_nwell} is such that it generated a maximum frequency drop of around 38 MHz. This drop can be observed in Fig. 13c that reports the complete evolution of the oscillation frequency. As shown, the evolution has a smoother profile than that observed in previous cases. This is due to the RC filtering effect of the supply voltage network. Frequency bounces are observed around the steady values, which are due to the inductance of the power network. Finally, the profile of Fig. 13c shows that the RLC network was designed to have an under-damped response [42].

3) Experimental results: laser shots near a RO: To experimentally observe the effect of a laser shot near a RO, several regions around it (but not over it) were illuminated. The $Psub$-$Nwell$ junctions, physically interconnected with the LUTs used to implement the RO, were located by monitoring the output of the RO directly. Laser shot positions, associated with an illumination of the PN junctions related to its design, were found in the same way.

Fig. 14a depicts the laser shot with a duration of 5 μs. Fig. 14b shows the periodic signal $Freq\_buf$ typically observed with the oscilloscope, when illuminating a region close to the RO. In this figure, a region in lighter blue is visible. It corresponds to an increase of the $Freq\_buf$ period. This behavior is similar to the one obtained by simulation in Fig. 10b.

Fig. 14c shows the evolution of $Freq\_buf$ frequency when the laser is active. As in the simulation, this evolution has a smooth profile due to the filtering effect (RC effect) of the supply voltage network. It is also possible to observe, as in the simulation in Fig. 13c, the bounces caused by the inductance.

D. Summary

Because we could identify (following the work described in [43]) the RO position with preliminary experiments we can be sure that Fig. 14c and Fig. 12c give the responses of the RO in two radically different situations (laser spot locations).

In the case associated to Fig. 14c the laser did not illuminate directly the RO, thus only activating IPh_{Psub_nwell}. On the contrary, in case of Fig. 12c, the laser beam directly illuminated the RO thus activating both I_{Ph} and IPh_{Psub_nwell}.

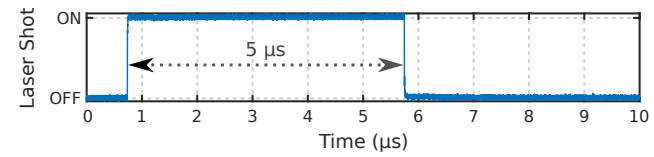
The comparison of the experimental results with the simulation results, especially the comparison of Fig. 14c and Fig. 13c showing a high level of correlation, demonstrates that laser induced IR-drops must not be neglected. This also highlights the superiority of the enhanced fault model proposed in this paper over the classical fault model. Despite this evidence of the existence and importance of the laser induced IR-drop, results suggest that these laser induced IR-drops amplify the effect of I_{Ph}. Indeed, instead of having a drop in frequency of 48 MHz (Fig. 10c) when considering only I_{Ph} (classical model), the frequency falls to zero (Fig. 11c and Fig. 12c) when the IR-drop is taken into account.

However, considering the laser-induced IR-drops could not be done by running simple electrical simulations in which the power/ground networks are assumed ideal. This explains why the next section presents a standard CAD tool-based method used to simulate laser-induced faults in large-scale circuits. Together with the simulation results provided by the proposed method, other experimental results will be used to emphasize the existence of the IPh_{Psub_nwell} current component. More importantly, the relevance of simulating this current will be shown by observing experimentally the phenomena highlighted by simulations and carried out with the proposed simulation flow, which is based on the enhanced fault model.

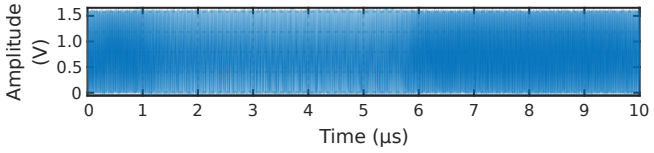
V. Proposed Methodology for Laser Fault Simulation Using Standard CAD Tools

A simulation flow taking laser-induced IR-drops into account during the simulation of large scale circuits is given in Fig. 15. This methodology is based on standard CAD tools: Cadence® Voltus^{TM} [44] for EMIR simulation and Cadence® Spectre® XPS [45] for the electrical/hybrid simulation. The proposed methodology provides: the ability to draw laser-induced IR-drop sensitivity maps and fault maps that can help the designer to decide how to harden designs against laser fault injection; and the ability to validate the efficiency of embedded countermeasures.

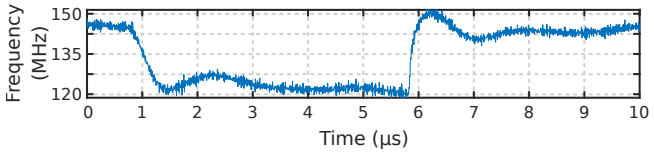
This methodology can be easily adapted to provide supplementary results to the ones reported in this work. To the best of our knowledge, this is the first methodology for simulating the effects of laser shots on ICs that simultaneously takes into account the design, the complete layout and the laser-induced IR-drops that have been proven to play a significant role in fault occurrence.



(a) Laser shot with pulse duration equal 5 μs.



(b) Periodic signal $Freq\_buf$.



(c) Disturbance of the frequency over time.

Figure 14: Measured typical effect on the RO oscillation frequency of a laser shot illuminating a region close to it.

Although Cadence tools were used, other tools able to perform IR-drop analysis and SPICE-like simulations can be used. Fig. 15 is subdivided into steps that are described in the following paragraphs.

Step 1: Defining simulation parameters

In the first step, a shell script file is completed by the user. It defines the parameters characterizing the laser parameters:

- the laser beam diameter,
- the laser power,
- the laser pulse duration,
- the time at which the laser illumination occurs with regard to the zero of the simulation,
- the (X, Y) displacement step of the laser spot when one aims at drawing a fault sensitivity map (details are given in Section VI-D),

This script is also used to choose the necessary tools and scripts for the correct execution of the simulation flow.

Step 2: Data preparation for the EMIR CAD tool

Most of the inputs that are inside the "EMIR CAD Tool" rectangle in Fig. 15 are files automatically generated by the CAD tool (Cadence® Innovus [46]). Other files were obtained from the design kit of the chosen CMOS 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 for modeling the RC network in the power/ground rails and to perform IR-drop analysis in Cadence® Voltus^{TM}, both necessary for the accomplishment of the proposed methodology.

Step 3: Spatial location of the laser spot

This step calculates the position of the laser shot with respect to the circuit layout. If the user decides (in step 1)

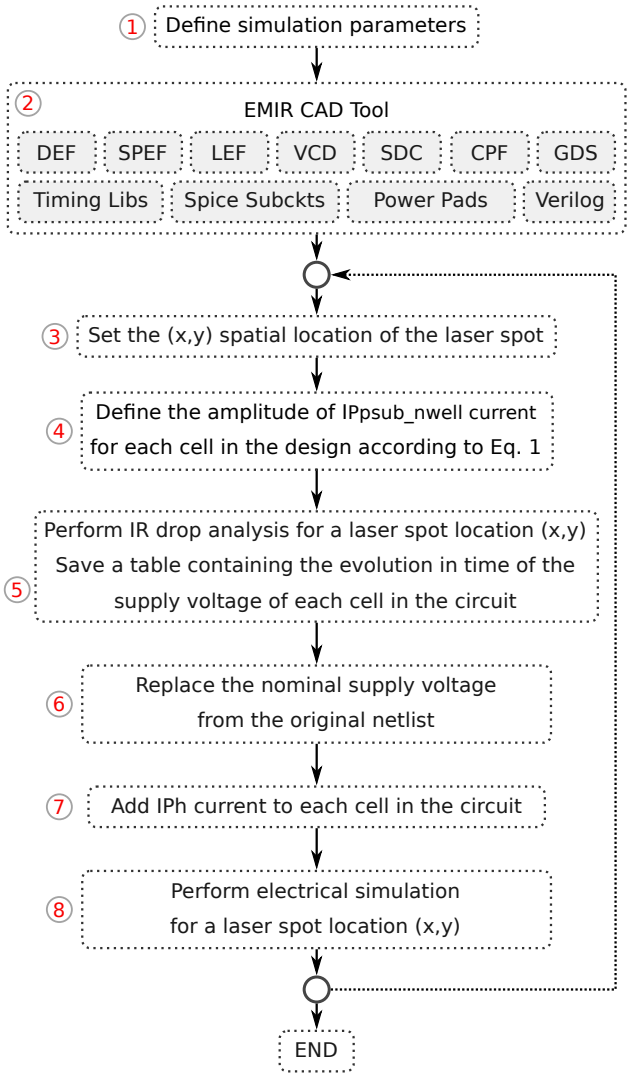


Figure 15: Proposed methodology to simulate the effects of laser shots on ICs using the enhanced fault model.

to draw a fault sensitivity map, then steps 3 (this one) to 8 are repeated n times, in which n is the number of simulations required to cover the whole IC surface according to the value of the laser spot displacement steps defined during step 1.

In the remainder of the paper, an implementation of the ARM 7 processor with an area of $110\,\mu m \times 70\,\mu m$ is considered (more details are provided in Section VI) as a test case. For this test case, choosing displacement steps $\Delta x = \Delta y = 5\mu m$ to sweep the whole design surface with the laser spot, beginning at $(x, y) = (0, 0)$ and ending at $(x, y) = (110, 70)$, implies the launching of $n = 345$ laser shot simulations as illustrated in Fig. 16.

Step 4: Definition of the IPh_{Psub_nwell} amplitude

The simulation of the effect of a laser shot starts by specifying the amplitude of the different current sources in the laser fault model (Fig. 7) applied to each standard cell in the circuit illuminated by the laser. Therefore it is necessary to know which instances of the DUT are affected by the laser.

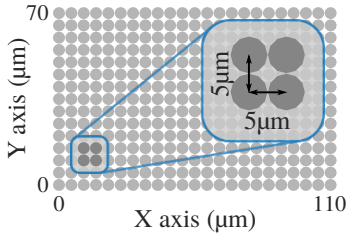


Figure 16: Illustration of the fault sensitivity map process: each point corresponds to a laser spot position, each position requires a simulation (steps 3 through 8).

Several ways can be adopted in order to fix the values of these current sources. The proposed methodology takes advantage of a Cadence® Voltus^{TM} feature. It 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 each region follows the spatial distribution of the laser-induced photocurrent defined by (1). Fig. 17 illustrates how the rectangular regions can be used to apply the laser power (i.e. the amount of current induced by the laser) to each rectangle.

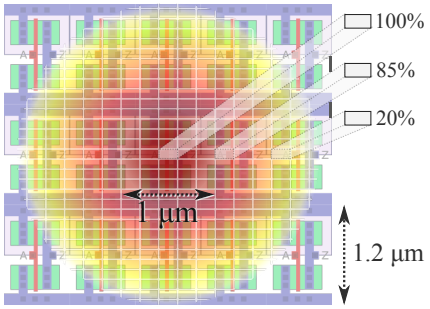


Figure 17: Laser-induced current regions applied over standard cells of a CMOS 28 nm technology. The current amplitude of each region is defined by (1).

The following code represents the characterization of the rectangle located at the center of the laser spot (Fig. 17).

```
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"
```

The above code describes piecewise linearly a current with a double exponential shape. In this example, the time step is equal to $5\,ps$, the peak value of the current (I_{Ph_peak}) which starts rising at $1.500\,ns$ occurs at $1.510\,ns$ and is equal to $1\,mA$. Other parameters such as capacitances are extracted from the .lib and .spi files of the technology for each illuminated instance. The resolution of each rectangle is $250\,nm$ as shown by the last parameter of the code: -region "x1 y1 x2 y2". The dimension of the rectangle can be changed according to the precision needed to model the laser spot.

Step 5: IR-drop analysis

In this step, Cadence® Voltus^{TM} is used to perform a laser-induced IR-drop simulation for the laser spot location defined during step 3. All other simulation parameters are kept constant (spot diameter, intensity, etc).

To clarify, 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 IPh_{Psub_nwell} will accumulate with the dynamic current of a cell, thus increasing its IR-drop while the laser is active ($IPh_{Psub\_nwell} \neq 0$).

For each iteration of this step, a table containing the evolution in time of voltage swing amplitude for each instance (V_{DD} - IR-drop - G_{ND} bounce) is saved for future analyses since different instances are affected by the laser shot. To illustrate, Table II gives the remaining voltage swing (with nominal V_{DD} = 1 V) of three different instances at the peak of the transient current (Fig. 1d) induced by three laser shots applied at three different locations.

Table II: Voltage swing of three instances of the DUT at the apex of three different laser shot locations.

Spot pos. 130 Voltage Swing	**Spot pos. 132 Voltage Swing**	**Spot pos. 139 Voltage Swing**
U205: 0.554 V	U205: 0.670 V	U205: 0.815 V
U1942: 0.554 V	U1942: 0.677 V	U1942: 0.818 V
U1088: 0.555 V	U1088: 0.669 V	U1088: 0.814 V

In this example, for laser spot position 130 (cf. Table II) the instances are more affected (lower voltage swing) as the epicenter of the laser spot is closer to these three instances. For laser spot positions 132 and 139, the instances are less affected since the laser spot is increasingly more distant.

Step 6: replace the supply voltage from the original netlist

After an estimation with Cadence® Voltus^{TM} of the IR-drops induced in the power/ground rails by the IPh_{Psub_nwell}, a shell script is used to replace the ideal V_{DD} and G_{ND} sources in the original SPICE netlist of the DUT by the IR-drop waveforms saved in step 5 for each instance in the circuit.

Step 7: inserting $\mathbf{I_{ph}}$

After inserting the effects of IPh_{Psub_nwell} (IR-drop and ground bounce) in the original spice netlist, a shell script is used in order to add current sources between the drain and the bulk of illuminated PMOS and NMOS transistors. They model the I_{ph} currents causing the transient voltage at the output of the illuminated gates. It should be noticed that only some of these current sources are activated depending on which drain's PN junction are reversely biased or not. To determine which of them should be turned ON, it is thus necessary to run a fault free electrical simulation and save a golden table with the inputs and outputs of each instance as a function of time.

Knowing that the IPh_{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 instance by analyzing the .lef and netlist files that contain information regarding each available standard cell. This leads to an estimation of the area of the affected PN junction of a particular transistor's drain as well as the area occupied by the $Nwell$.

Step 8: Electrical/hybrid fault simulation

This step consists in running an electrical simulation of the modified spice netlist for each laser shot position specified at step 3. However, because electrical simulations are time consuming, hybrid simulations are performed to decrease the overall simulation time.

In these hybrid simulations, run with the Cadence® Spectre® XPS simulator, solely the region of the circuit containing the most affected instances by the laser shot are simulated with SPECTRE accuracy. To delimit this region a threshold voltage, th, is defined based on all voltage swing values (V_{DD}-G_{ND}) provided by Table II. If the voltage swing value of an instance is higher than V_{DD}-th, it is considered as not affected by the laser shot. This is the case for instances which are far away from the laser spot epicenter (Table II). For example, if th is set equal to 5% of the nominal $V_{DD} = 1\,V$, then all instances with a residual voltage swing higher than $950\,mV$ are simulated at the logic abstraction level.

Table III gives the number of instances simulated at the logic abstraction level for different th values and different spot locations. The chosen spot locations were randomly selected with the purpose of showing that the number of affected instances changes depending on the laser spot location. As shown, increasing the th value facilitates (the management) of the trade off between speed (increasing the number of gates simulated at the abstraction level) and accuracy.

Table III: Number of instances simulated at the logic abstraction level for different th values at three spot locations. (5.21k instances in the circuit.)

th % of V_{DD}	No. of instances (spot loc. 130)	No. of instances (spot loc. 139)
10%	1676	1646
15%	4744	4866
20%	4878	5033

VI. Laser Fault Simulation Results

In order to simulate the effects of laser-induced faults on complex systems, simulations were performed for different circuits, however only the results obtained for an ARM 7 processor are shown in details. All circuits were synthesized using 28 nm CMOS technology.

1) Circuit Inventory: The nominal supply voltage of the DUT is 1 V and the clock period is $1\,ns$. The ARM 7 has an area equal to $110\,\mu m \times 70\,\mu m$ occupied by 5.21 k instances, 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.

2) Laser Spot Diameter: Laser sources used to produce faults can be characterized by their 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 optics) its effect area extends far beyond [47], [48]. 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 5 μm was chosen for the experiments reported below.

A. Simulation Performance

The performance of the simulation directly depends on the available computing resources and the complexity of the simulated circuit. The processor used to perform simulations was an Intel® Xeon® E5630@2.53 GHz with two cores and 16 GB of RAM. Table IV gives the simulation performance of the four assessed circuits. Note how the simulation time does not increase proportionally with the number of instances in the circuit. Since the proposed method deals with simulations of laser-induced fault injection, other factors such as the laser spot diameter, its power and the duration of the laser shot impact the simulation time. Indeed, these parameters directly:

- fix the number of instances with a supply voltage lower than V_{DD}-th and thus the number of instances that have to be simulated with Spectre accuracy,
- reduce the time step of simulations because V_{DD} and G_{ND} are no longer constant values.

Table IV: Simulation performances for different circuits regarding one laser shot.

Circuit	No. of instances	Simulation time
ARM 7	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

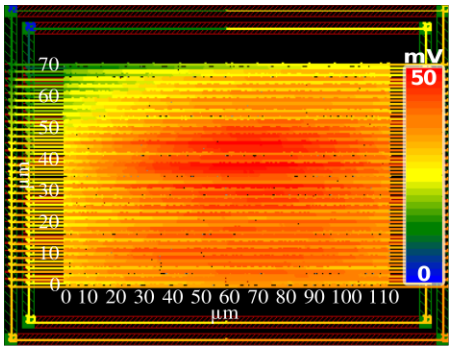
B. Spatial distribution of the laser-induced IR-drop

Laser illumination induces IR-drops, whose effect could spread over the IC surface. It is thus not limited as indicated by the classical fault model to the few transistors or logic gates directly illuminated by the beam. One can thus wonder how far and how the effect of a laser shot spread (the shape of its effect area). To give a first insight into this dissipation, Fig. 18b and Fig. 18a give the IR-drop maps obtained with Voltus for the considered test case with and without a laser shot, respectively.

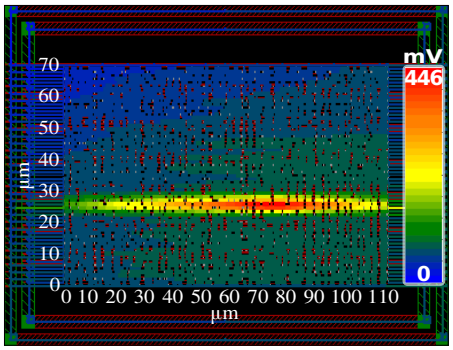
In Fig. 18a, the IR-drop across the power rails reaches a maximum value of $50\,mV$. This drop is due to the normal switching activity of the transistors. It seems to affect almost the entire circuit surface in a uniform way. There is indeed no specific spot at which the IR-drop is significantly stronger.

Fig. 18b (obtained at the end of step 5 of the proposed method) illustrates how the laser effect propagates on the circuit. In the presence of a single laser shot with a spot diameter of 5 μm at coordinates x=68 μm, y=25 μm, the effect area extends along the X axis of the power-grid main metal lines for more than 100 μm. It has a shape that is stretched horizontally along the power supply rails as they provide a propagation path for the laser-induced IR-drop and ground bounce. Whereas its extension along the Y axis is only approximately 7 μm. The peak value of the induced drop in the power lines is 446 mV (Fig. 18b). At this time, the voltage

swing is reduced to 554 mV, a value far below the nominal core voltage of 1 V.



(a) Maximum supply voltage drop of (V_{DD}-G_{ND}) in normal operation conditions.



(b) Maximum voltage drop in presence of a laser shot with a spot diameter equal to 5μm.

Figure 18: ARM 7 layout with 5k+ instances.

From the above observations, depending on the laser power, laser shots can induce faults in the circuit, such as timing errors or even data disruption quite far from the laser spot location. Indeed, dozens of standard cells are inside the laser effect area when considering 28 nm technology, and hundreds of them can experience a significant voltage drop.

C. Simulated Scenarios

The proposed methodology was used to simulate various scenarios. Among these scenarios, four are considered hereafter for the sake of simplicity. They are illustrated in Fig. 19, the first line showing the clock signal waveform used as a time reference. The two other lines give the typical evolutions observed during simulations, of the Q_x signal and the output of the cell 'x' of the design under illumination, in two different cases. These cases correspond to laser shots with a duration equal to $250\,ps$ applied at 1.5 ns and 1.7 ns respectively. They thus start closer and closer to the next rising clock edge that occurs at 2 ns.

The second line of Fig. 19 reports the results when the classical fault model (only I_{Ph}) is used during simulations while the third line reports results obtained with the enhanced model (I_{Ph} and IPh_{Psub_nwell}). In the third line, the curves have a higher amplitude due to the amplification effect (Section IV-B) as well as a smoother double exponential waveform when compared to that reported on the second line. This is due to the filtering effect (RC effect) of the supply voltage network.

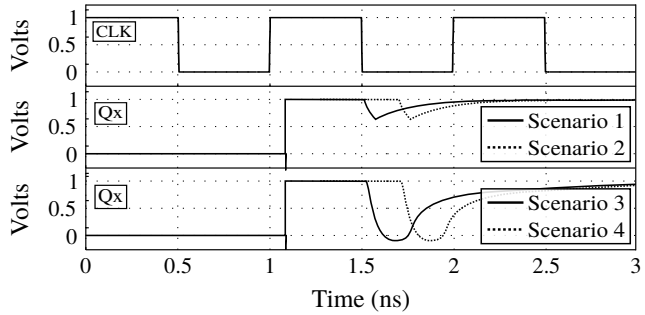


Figure 19: Typical waveforms observed during simulations at the output of an arbitrary gate illuminated by a laser beam. Line 1: clock signal. Line 2: waveforms observed when considering I_{Ph} contribution only. Line 3: waveforms observed when considering both I_{Ph} and IPh_{Psub_nwell} contributions.

D. Fault Injection Maps

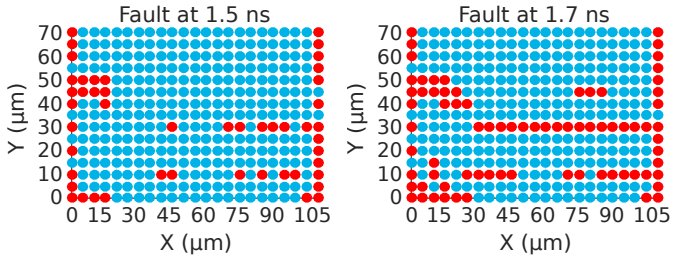
For the purpose of assessing the contribution of the laser-induced IR-drop to the fault injection mechanism, fault sensitivity maps were drawn based on simulation results using the proposed methodology. The simulations were done both with the classical and enhanced fault model. They were also performed 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 5 μm, resulting in 345 simulations for each figure (each dot corresponds to the location of a simulated laser shot).

Fig. 20 reports the fault maps obtained with both the classic electrical model (Fig. 2) and the enhanced model (Fig. 7). The red dots correspond to the occurrence of a fault (soft-error) and blue dots to 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.

1) Simulations with the classical fault model: Fig. 20a and Fig. 20b report simulations performed considering the classical fault model, in which only the I_{Ph} current component with a width of 250 ps is considered. The current begins to rise at 1.5 ns and 1.7 ns respectively. Note that more faults are induced when the laser shot is closer to the flip-flop sampling window (time window of width t_{setup} + t_{hold} centered on the rising edge).

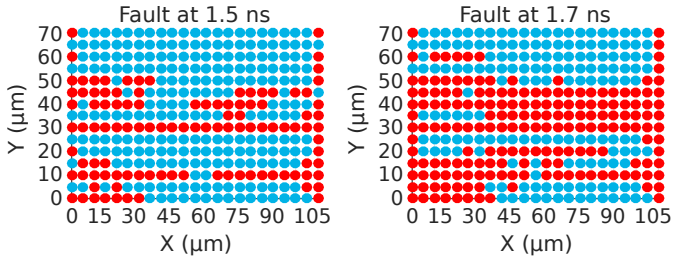
2) Simulations with the enhanced fault model: Fig. 20c and Fig. 20d report the fault maps obtained with the same settings, using the enhanced fault model instead of the classical one. The comparison of these maps with that of the first line reveals that the fault areas are wider. The IR-drop induced mainly by IPh_{Psub_nwell} amplifies the effect of the I_{Ph} current and thus the number of faults. It also revealed an extension of the laser sensitivity in time, in which the number of faults are increased respectively by a factor of 2.3 and 2.4 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 soft errors. Not taking the laser-induced IR-drop into account

leads to over optimistic results regarding the threshold of fault injection and the number of injected faults.



(a) I_{Ph} only - classical model. #faults: 48

(b) I_{Ph} only - classical model. #faults: 76



(c) I_{Ph} + IPh_{Psub_nwell} - enhanced model. #faults: 108

(d) I_{Ph} + IPh_{Psub_nwell} - enhanced model. #faults: 181

Figure 20: 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} and IPh_{Psub_nwell} contributions.

VII. Additional Evidences of the Importance of Laser-Induced IR-Drop

A. Lessons from Simulations

Fig. 13c, which reports simulation results related to a laser shot *near* the RO obtained by using the enhanced fault model, shows a frequency drop of 38 MHz. This frequency drop is due to the laser-induced IR-drop and to its propagation through the supply network. This propagation capability suggests that a laser shot can affect the behavior of a structure that it is not illuminating directly.

In the same way, Fig. 10c which gives simulation results related to a laser shot *over* the RO obtained considering the classical fault model shows a frequency drop of 48 MHz.

Considering the above two results, one can think that simulating a laser shot *over* the RO with the upgraded model would give a frequency drop equal to 38 MHz + 40 MHz=78 MHz. However, as shown in Fig. 11c that gives the result of such a simulation, this is not the case. Indeed, the frequency falls to zero during the laser shot. This reveals the existence of an amplification effect by the IR-drop (mainly due to IPh_{Psub_nwell}) of the amplitude of the transient fault generated by I_{Ph}.

We can thus conclude that the enhanced fault model shows the importance of the laser-induced IR-drop in the fault injection process. Indeed, according to the above simulation results, these IR-drops play an important role in the fault occurrence process by either amplifying the transients generated by I_{Ph} or by disrupting the behavior of gates far from the laser spot location because of their propagation capability.

This importance of the laser-induced IR-drops (and thus of the related amplification effect) has been highlighted by the results of Fig. 20 showing that the fault areas of the ARM7 surface are larger than expected from the classical fault model when considering IPh_{Psub_nwell} during simulations.

At this stage of the paper, one may wonder if the lessons related to laser shot effects (amplification and propagation effects) learned from simulations stand up in practice even if some experimental evidence of the validity of the enhanced model has been already given in Section IV.

B. Experimental Results - RO implemented on FPGA

To make meaningful comparisons of the results obtained with the proposed methodology in Fig. 20, fault maps of the Virtex-5 embedding a RO were also drawn. More precisely, two sets of laser scans were performed.

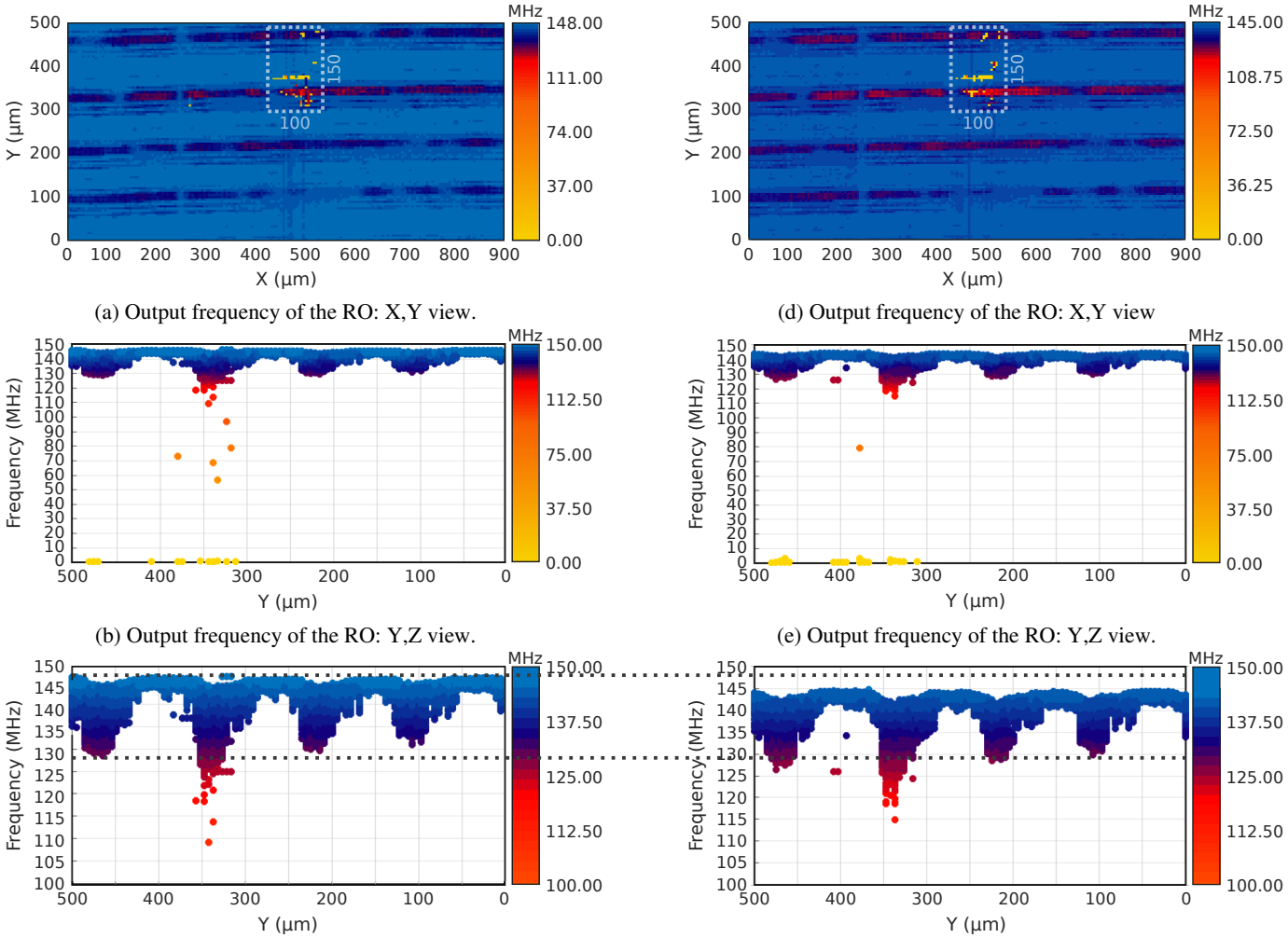
During the first scan, only a RO, placed as shown in Fig. 9b, was implemented. During the second scan the same implementation of the RO was considered. However, extra logic (a chain of inverters without any kind of logic connection with the RO) was placed around it. The additional logic uses an internal clock source of the FGPA as input which switches at a fixed frequency equal to 50 MHz. The role of this extra logic constantly switching is to generate a native IR-drop in the RO.

Fig. 21 combines all experimental results, validating the lessons learned from simulations, lessons related to the existence of an amplification effect and of a propagation effect.

Fig. 21a shows for each laser spot location the frequency drift induced by the shot. The scanned surface was equal to $900\,\mu m \times 500\,\mu m$ and enclosed the RO placed and routed, without surrounding logic, as shown by Fig. 9b. For this scan, the laser spot diameter was $5\,\mu m$ and the laser power was set to $1.04\,W$, a value which is near the minimum threshold to induce faults in the RO (fault means, in this case, a frequency equal to 0 MHz). The x and y displacement steps were set to $5\,\mu m$ resulting in a total of 18000 points. Each point of the scanned surface corresponds to a RO frequency measured over a time window of $10\,\mu s$, beginning shortly before the laser shot (c.f. Fig. 14a). The minimum frequency found over this window of $10\,\mu s$ was saved along with the corresponding (x, y) position of the laser shot. The color bar ranges from 148 MHz (the nominal frequency) down to 0 MHz. The dark/red stripes in Fig. 21a correspond to the areas with the $Psub$-$Nwell$ junctions (power rails).

Fig. 21b-c show the same results as in Fig. 21a after application of a rotation to only show the y and z axis, z being the frequency of the RO. Fig. 21c and Fig. 21b differ by their considered frequency range (color bar scale).

Fig. 21d-f give the same types of fault maps as Fig. 21a-c, but for the RO with its surrounding logic. In this case the nominal frequency of the RO dropped from 148 MHz to 145 MHz due to the IR-drop caused by the additional logic.



(a) Output frequency of the RO: X,Y view.

(d) Output frequency of the RO: X,Y view

(b) Output frequency of the RO: Y,Z view.

(e) Output frequency of the RO: Y,Z view.

(c) Output frequency of the RO (zoom): Y,Z view.

(f) Output frequency of the RO (zoom): Y,Z view.

Figure 21: Maps of laser-induced frequency drop of the RO implemented on FPGA: Each point corresponds to the output frequency of the RO observed on the oscilloscope. Laser pulse duration: 5 μs. Laser power: 1.04 W. Laser spot: 5 μm. (X,Y) displacement step: 5 μm. (a-c) RO implemented alone. (d-f) RO implemented with logic surrounding it causing additional IR-drop due to switching activity.

The two maps (Fig. 21a-c and Fig. 21d-f) experimentally demonstrate the existence of laser induced IR-drops. Indeed, on both maps, the frequency drops occur at many points of the scanned surface even if the RO occupies a small fraction of it ($100\,\mu m \times 150\,\mu m$). This gives experimental evidence that the effect of laser illumination is not as local as usually considered (the classical model is unable to predict these maps). This horizontal propagation of the frequency drop is similar to the voltage drop propagation shown in Fig. 18b. The laser effect of laser illumination is thus more global than previously thought. Additionally, the points in yellow corresponds to a laser shot completely stopping the operation of the RO (frequency equal to zero). The yellow points should correspond to the placement of the RO (Fig. 9b) or really close to it.

The amplification of the laser shot effect by the laser-induced IR-drop can be observed by comparing the first column of Fig. 21 (Fig. 21a-c) with its second column (Fig. 21d-f). Indeed, taking a closer look at Fig. 21a and Fig. 21d, it is possible to observe that the number of points in red and in yellow is larger in Fig. 21d. This means that in the case of Fig. 21d more points have a frequency value below a certain threshold (or a null frequency) as reported by Table V. This result demonstrates quantitatively that even a small additional IR-drop (of few mV) caused by the switchings of extra cells, increases the impact of laser shots. More precisely, it increases the frequency drop experienced by the RO when using the same laser power. Hence the amplification of the transient current I_{Ph} by the laser-induced IR-drop (IPh_{Psub_nwell}).

Table V: Number of points below or equal to a given frequency (nom. freq. = 148 MHz for Fig. 21a-c and nom. freq. = 145 MHz for Fig. 21d-f)

Frequency value (nom freq - x % of nom. freq.)	**No. of points Fig. 21a-c**	**No. of points Fig. 21d-f**
nom freq - 0 % of nom. freq.	18000	18000
nom freq - 5 % of nom. freq.	3363	3453
nom freq - 10 % of nom. freq.	468	563

VIII. Conclusions

This paper reported a methodology which allows the simulation of laser fault injection at the electrical level in large-scale circuits by using standard CAD tools. An enhanced electrical fault model that takes laser-induced IR-drop into account was proposed. The enhanced fault model was applied to each instance of a test-chip used in the methodology in order to demonstrate how the induced IR-drop facilitates the occurrence of SEs by amplifying laser-induced perturbations on logic signals.

This paper also revealed, based on simulation and experimental results that, when an IC —fabricated in a relatively old technology node (Virtex-5 FPGA - 65 nm)— is illuminated by a laser beam, it induces IR-drops. The induced IR-drops have a global effect spreading through the supply network. The paper gives experimental evidence that the effect of laser illumination is not as localised as previously thought.

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 increase in the number of faults by a factor of 2.4 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] A. Barenghi, L. Breveglieri, I. Koren *et al.*, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, Nov 2012.

[2] H. Bar-El, H. Choukri, D. Naccache *et al.*, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, Feb 2006.

[3] M. Agoyan, J.-M. Dutertre, D. Naccache *et al.*, "When clocks fail: On critical paths and clock faults," in *CARDIS*, 2010.

[4] R. Ahmadi and F. N. Najm, "Timing analysis in presence of power supply and ground voltage variations," in *ICCAD-2003. International Conference on Computer Aided Design*, Nov 2003, pp. 176–183.

[5] P. Maurine, K. Tobich, T. Ordas *et al.*, "Yet Another Fault Injection Technique: by Forward Body Biasing Injection," in *YACC'2012*.

[6] A. Dehbaoui, J.-M. Dutertre, B. Robisson *et al.*, "Electromagnetic Transient Faults Injection on a hardware and software implementations of AES," in *FDTC 2012*, Leuven, Belgium, Sep. 2012, p. 7.

[7] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *4th CHES*. London, UK: Springer-Verlag, 2002, pp. 2–12.

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

[9] A. G. Jordan and A. G. Milnes, "Photoeffect on diffused p-n junctions with integral field gradients," *IRE Trans. on Electron Devices*, 1960.

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

[11] R. A. C. Viera, J. M. Dutertre, R. P. Bastos *et al.*, "Role of laser-induced ir drops in the occurrence of faults: Assessment and simulation," in *2017 Euromicro Conference on Digital System Design (DSD)*, Aug 2017.

[12] F. Lu, G. D. Natale, M. L. Flottes *et al.*, "Laser-induced fault simulation," in *Euromicro Conference on Digital System Design*, 2013.

[13] A. Douin, V. Pouget, D. Lewis *et al.*, "Electrical modeling for laser testing with different pulse durations," in *11th IEEE IOLTS*, July 2005.

[14] H. M. Huang, Y. Lin, and C. H. P. Wen, "Fast-yet-accurate variation-aware current and voltage modelling of radiation-induced transient fault," in *DATE*, 2016.

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

[16] G. S. Greenstein and J. H. Patel, "E-proofs: A cmos bridging fault simulator," in *1992 IEEE/ACM ICCAD*, Nov 1992, pp. 268–271.

[17] H. Cha, E. M. Rudnick, J. H. Patel *et al.*, "A gate-level simulation environment for alpha-particle-induced transient faults," *IEEE Transactions on Computers*, vol. 45, no. 11, Nov 1996.

[18] W. Meyer and R. Camposano, "Active timing multilevel fault-simulation with switch-level accuracy," *IEEE TCAD*, vol. 14, no. 10, Oct 1995.

[19] M. B. Santos and J. P. Teixeira, "Defect-oriented mixed-level fault simulation of digital systems-on-a-chip using hdl," in *DATE, 1999*.

[20] G. Hubert, R. Velazco, and P. Peronnard, "A generic platform for remote accelerated tests and high altitude seu experiments on advanced ics: Correlation with musca sep3 calculations," in *2009 15th IOLTS*, 2009.

[21] F. Lu, G. D. Natale, M. L. Flottes *et al.*, "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)*, May 2014.

[22] A. Bosio and G. D. Natale, "Lifting: A flexible open-source fault simulator," in *2008 17th Asian Test Symposium*, Nov 2008, pp. 35–40.

[23] A. Sarafianos, O. Gagliano, V. Serradeil *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.

[24] L. Heriveaux, J. Clediere, and S. Anceau, "Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design," in *39th ISTFA ASM*, 2013.

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

[26] 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.

[27] T. C. May and M. H. Woods, "Alpha-particle-induced soft errors in dynamic memories," *IEEE Transactions on Electron Devices*, Jan 1979.

[28] C. M. Hsieh, P. C. Murley, and R. R. O'Brien, "A field-funneling effect on the collection of alpha-particle-generated carriers in silicon devices," *IEEE Electron Device Letters*, vol. 2, no. 4, pp. 103–105, April 1981.

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

[30] F. Wang and V. D. Agrawal, "Single event upset: An embedded tutorial," in *21st International Conference on VLSI Design*, Jan 2008.

[31] C.-M. Hsieh, P. C. Murley, and R. R. O'Brien, "Collection of charge from alpha-particle tracks in silicon devices," *IEEE Transactions on Electron Devices*, vol. 30, no. 6, pp. 686–693, Jun 1983.

[32] S. Buchner, F. Miller, V. Pouget *et al.*, "Pulsed-laser testing for single-event effects investigations," *IEEE Trans. on Nuclear Science*, 2013.

[33] E. W. Enlow and D. R. Alexander, "Photocurrent modeling of modern microcircuit pn junctions," *IEEE Transactions on Nuclear Science*, vol. 35, no. 6, pp. 1467–1474, Dec 1988.

[34] J.-M. Dutertre, R. Possamai Bastos, O. Potin *et al.*, "Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS," *Microelectronics Reliability*, Sep. 2014.

[35] J. A. McNeill, "Jitter in ring oscillators," *IEEE JSSC*, Jun 1997.

[36] A. Hajimiri, S. Limotyrakis, and T. H. Lee, "Jitter and phase noise in ring oscillators," *IEEE Journal of Solid-State Circuits*, vol. 34, no. 6, 1999.

[37] F. Herzel and B. Razavi, "A study of oscillator jitter due to supply and substrate noise," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 46, no. 1, pp. 56–62, Jan 1999.

[38] M. Lecomte, J. J. A. Fournier, and P. Maurine, "Thoroughly analyzing the use of ring oscillators for on-chip hardware trojan detection," in *2015 ReConFig*, Dec 2015, pp. 1–6.

[39] J. Rubinstein, P. Penfield, and M. A. Horowitz, "Signal delay in rc tree networks," *IEEE TCAD*, vol. 2, no. 3, pp. 202–211, July 1983.

[40] Xilinx. Virtex-5 overview. (December 3, 2017). [Online]. Available: https://www.xilinx.com/support/documentation/data_sheets/ds100.pdf

[41] Xilinx. Planahead design and analysis tool. (January 8, 2018). [Online]. Available: https://www.xilinx.com/products/design-tools/planahead.html

[42] C. Alexander and M. Sadiku, *Fundamentals of Electric Circuits*, 4th ed. McGraw Hill Higher Education, 2008.

[43] J. Breier, W. He, S. Bhasin *et al.*, "Extensive laser fault injection profiling of 65 nm fpga," *Journal of Hardware and Systems Security*, vol. 1, no. 3, pp. 237–251, Sep 2017. [Online]. Available: https://doi.org/10.1007/s41635-017-0016-z

[44] Cadence. Voltus IC power integrity solution. (December 3, 2017). [Online]. Available: https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/silicon-signoff/voltus-ic-power-integrity-solution.html

[45] Cadence. Spectre extensive partitioning simulator. (December 3, 2017). [Online]. Available: 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

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

[47] F. Darracq, H. Lapuyade, N. Buard *et al.*, "Backside seu laser testing for commercial off-the-shelf srams," *IEEE Trans. on Nuclear Science*, 2002.

[48] C. Roscian, A. Sarafianos, J. M. Dutertre *et al.*, "Fault model analysis of laser-induced faults in sram memory cells," in *FDTC, 2013*.