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

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

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

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

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

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

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

ABSTRACT

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

ACM Reference Format:
Raphael A. C. Viera, Jean-Max Dutertre, Philippe Maurine, and Rodrigo Possamai Bastos. 2018. Standard CAD Tool-Based Method for Simulation of Laser-Induced Faults in Large-Scale Circuits. In *ISPD '18: 2018 International Symposium on Physical Design, March 25–28, 2018, Monterey, CA, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3177540.3178243

1 INTRODUCTION

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

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

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

The issue being that, as far as we know, there is no tool capable to simulate laser-induced IR drop and its propagation in a large circuit. Thus, the first and main objective of this work is to introduce the

devised methodology to simulate at the electrical level the effect of IR drop on the fault injection sensitivity using standard CAD tools; the second objective is to illustrate, on simulation grounds, that laser-induced IR drop has to be considered since it may result in underestimating the risk of fault injection.

2 STATE OF THE ART

2.1 Modeling laser effects on ICs

2.1.1 Laser Induced Transient Currents. ICs are known to be sensitive to induced transient currents. These currents may be caused by laser shots passing through the device, creating electron-hole pairs along the path of the laser beam [15]. The induced charge carriers recombine without any significant effect, unless they reach the strong electric field found in the vicinity of reverse biased PN junctions. In this case, the electrical field puts these charges into motion and a transient current appears as well as a transient fault. The nature of this fault is similar to the ionization effect generated by energetic particles [13].

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

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

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

2.1.2 Spatial Distribution of Laser Beam Energy. The beam diameter is one of the most important propagation attribute of a laser beam in a class of commonly measured parameters (beam diameter, spatial intensity distribution, beam quality factor etc.). A commonly used definition of the laser beam diameter is derived from the bivariate normal distribution of its intensity leading to

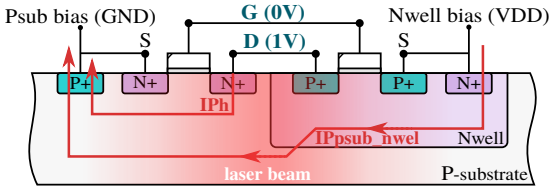


Figure 1: Laser-induced current components. Cross-section of a CMOS inverter.

measure the beam diameter at 86.5% of its maximum value [2], or a drop of $\frac{1}{e^2}$ from its peak value.

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

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

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

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

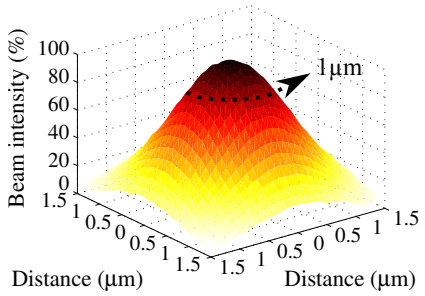


Figure 2: Three-dimensional view of a laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot.

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

Electromigration/IR drop (EMIR) CAD tool to automatically provide the power-grid model for each cell in the circuit.

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

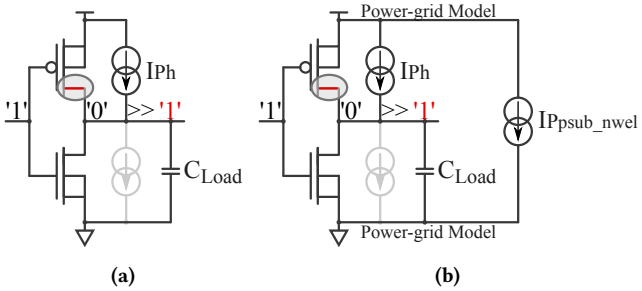


Figure 3: Laser-induced transient fault model applied to an inverter with its input biased at V_{DD}. (a) Classical model. (b) Improved model including the IR drop and ground bounce contribution induced by IP_{Psub_nwell} for a given power-grid model [27].

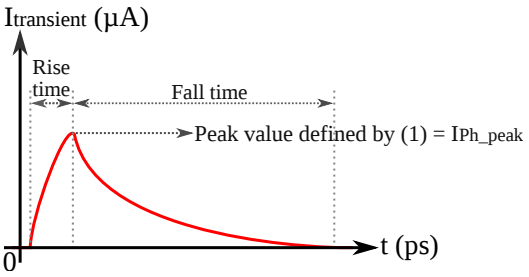


Figure 4: Double exponential profile with current peak defined by (1).

The IP_{Psub_nwell} current source is attached to the biasing contacts of the *Nwell* and the $P_{substrate}$ (for standard cells without embedded biasing contacts, the current source is connected to the closest). The various IP_{Psub_nwell} currents add up and flow from V_{DD} to G_{ND} trough the power and ground networks of the device under attack. Because the power grid exhibits both resistive and capacitive electrical behaviors, a local voltage drop and ground bounce occurs thus reducing the voltage swing seen by standard cells in the close vicinity of the laser spot. Considering the above, this paper provides a method based on standard CAD tools to take at chip level the effect of laser-induced IR drops into account.

2.2 Previous Works on Laser Fault Simulation

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

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

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

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

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

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

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

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

3 PROPOSED METHODOLOGY FOR LASER FAULT SIMULATION

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

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

3.1 Step 1: defining simulation parameters

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

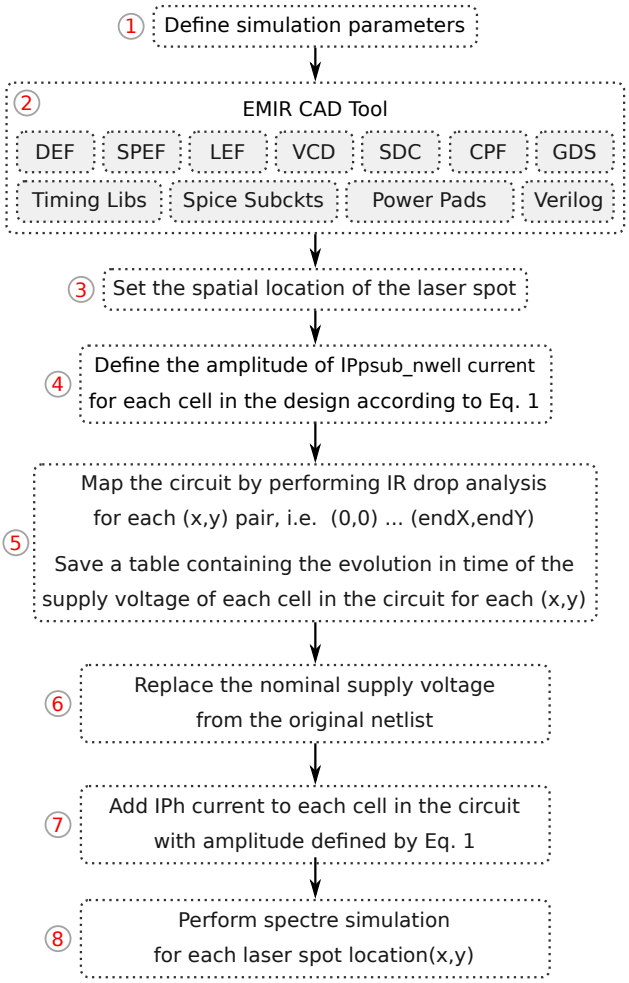


Figure 5: Procedure used to draw laser-induced fault sensitivity maps using the proposed methodology.

3.2 Step 2: data preparation for the EMIR CAD tool

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

3.3 Step 3: spatial location of the laser spot

In this step it is necessary to know the dimension of the design and the number of simulated laser shots that are going to be applied over the circuit. For this work, an ARM 7 with a 110 $\mu m \times$ 70 μm area was used (more details are provided in Section 4). If a displacement step of x, y: 5μm is set, then, in order to sweep the

whole circuit, beginning at x, y: (0, 0) and ending at x, y: (110, 70), it would demand 345 laser shots as illustrate in Fig. 6.

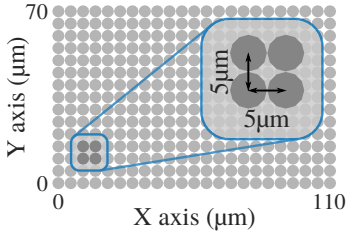


Figure 6: Spatial location of the laser spots. Each point corresponds to a laser shot at different positions (each point corresponds to a simulation).

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

3.4 Step 4: laser-induced fault injection

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

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

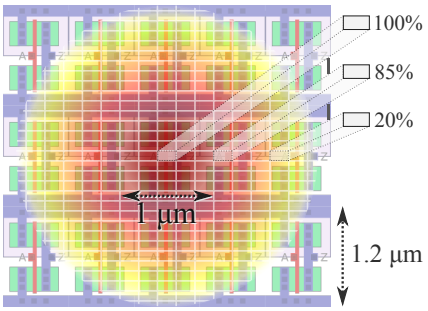


Figure 7: Laser-induced current regions applied over standard cells of a CMOS 28 nm technology. The current amplitude of each region is defined by (1).

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

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

3.5 Step 5: mapping the circuit

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

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

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

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

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

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

3.6 Step 6: inserting IP$_{\text{Psub_nwell}}$

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

3.7 Step 7: inserting I_{ph}

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

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

3.8 Step 8: electrical/hybrid fault simulation

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

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

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

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

4 LASER FAULT SIMULATION RESULTS

4.1 Testbench

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

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

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

4.2 Simulation Performance

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

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

4.3 Laser Propagation on the Circuit Surface

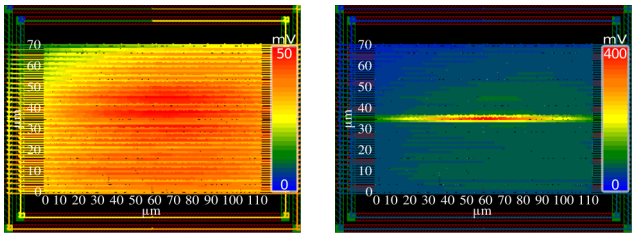
To illustrate how the IR drop propagates in the circuit, refer to Fig. 8a and Fig. 8b. In Fig. 8a, for which no laser effect is considered, the IR drop across the rails reach the maximum of 50 mV. In this figure, the voltage drop is uniquely due to normal switching activity. Even though not fully uniform,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

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

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

y=35 μm, the effect area extends along the X axis of the power-grid main metal lines for more than 100 μm (the effect area has a shape that is stretched horizontally along the power supply rails as they provide a propagation path to the laser-induced IR drop and ground bounce). Whereas its extension along the Y axis is only approximately 3 μm, i.e., three times the laser spot diameter. The peak value of the induced voltage transient in the power lines is 400 mV (Fig. 8b). At this time, the voltage swing is reduced to 600 mV. This value is far below the nominal core voltage of 1 V. Thus laser-induced IR drop may induce faults in the circuit, such as timing errors or even data disruption.

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



(a) (b)

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

4.4 Simulated Scenarios

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

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

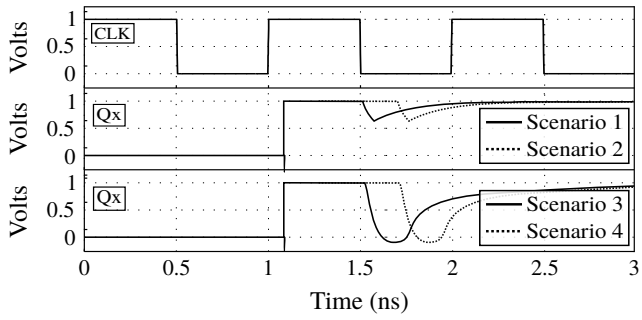


Figure 9: Typical waveforms observed during simulations at the output of gates illuminated by a laser beam. Line 1: clock signal. Line 2: waveforms observed when considering I_{Ph} contribution only. Line 3: waveforms observed when considering I_{Ph} + IP_{Psub_nwell} contributions.

4.5 Fault Injection Maps

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

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

4.5.2 Contribution of $\mathbf{I_{ph}}$ *and* $\mathbf{IP_{Psub\_nwell}}$. Fig. 10c and Fig. 10d report fault maps for which I_{Ph}, IP_{Psub_nwell} and the power-grid model are considered (scenarios 3 and 4). By comparison to the first line, it reveals that the fault areas are larger than expected for the considered laser shot times. It also unveiled an extension of the laser sensitivity in time, in which the number of faults are increased respectively by a factor of 2.6 and 3.1 for the laser applied at 1.5 ns and 1.7 ns. This demonstrates that IR drops induced by laser shots

play an important role in the occurrence of faults. Not taking this effect into account leads to over optimistic results regarding the threshold of fault injection.

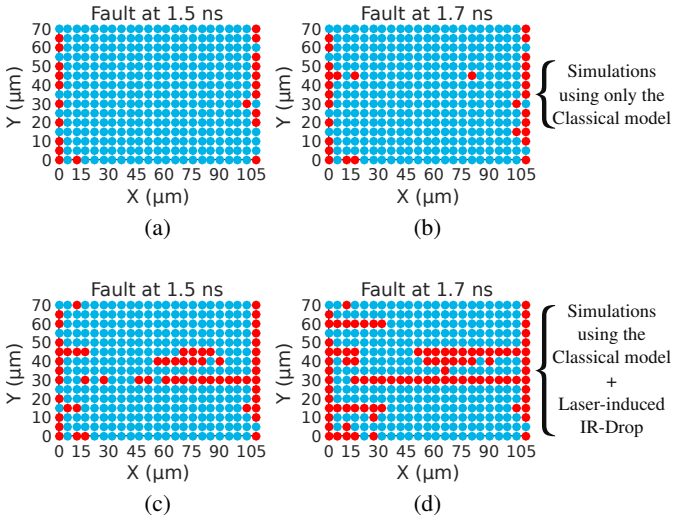


Figure 10: Maps of laser-induced faults for the simulated scenarios: (a-b) laser applied at 1.5 ns and 1.7 ns respectively, considering I_{Ph} contribution only. (c-d) laser applied at 1.5 ns and 1.7 ns respectively, considering I_{Ph} + IP_{Psub_nwell} contributions.

5 CONCLUSIONS

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

REFERENCES

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

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

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

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

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

[6] Hungse Cha, E. M. Rudnick, J. H. Patel, R. K. Iyer, and G. S. Choi. 1996. A gate-level simulation environment for alpha-particle-induced transient faults. *IEEE Trans. Comput.* 45, 11 (Nov 1996), 1248–1256. https://doi.org/10.1109/12.544481

[7] F. Darracq, H. Lapuyade, N. Buard, F. Mounsi, B. Foucher, P. Fouillat, M. C. Calvet, and R. Dufayel. 2002. Backside SEU laser testing for commercial off-the-shelf SRAMs. *IEEE Transactions on Nuclear Science* (2002). https://doi.org/10.1109/TNS.2002.805393

[8] A. Douin, V. Pouget, D. Lewis, P. Fouillat, and P. Perdu. 2005. Electrical modeling for laser testing with different pulse durations. In *11th IEEE IOLTS*. 9–13. https://doi.org/10.1109/IOLTS.2005.27

[9] Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre, Giorgio Di Natale, and Alexandre Sarafianos. 2014. Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS. *Microelectronics Reliability* 54 (Sept. 2014), 2289 – 2294. https://doi.org/10.1016/j.microrel.2014.07.151

[10] Z. E. Fleetwood, N. E. Lourenco, A. Ildefonso, J. H. Warner, M. T. Wachter, J. M. Hales, G. N. Tzintzarov, N. J. H. Roche, A. Khachatrian, S. P. Buchner, D. McMorrow, P. Paki, and J. D. Cressler. 2017. Using TCAD Modeling to Compare Heavy-Ion and Laser-Induced Single Event Transients in SiGe HBTs. *IEEE Transactions on Nuclear Science* 64, 1 (Jan 2017), 398–405. https://doi.org/10.1109/TNS.2016.2637322

[11] C. Godlewski, V. Pouget, D. Lewis, and Mathieu Lisart. 2009. Electrical modeling of the effect of beam profile for pulsed laser fault injection. *Microelectronics Reliability* (Aug. 2009).

[12] G. S. Greenstein and J. H. Patel. 1992. E-PROOFS: A CMOS bridging fault simulator. In *1992 IEEE/ACM International Conference on Computer-Aided Design*. 268–271. https://doi.org/10.1109/ICCAD.1992.279362

[13] D. H. Habing. 1965. The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits. *IEEE Transactions on Nuclear Science* 12, 5 (Oct 1965), 91–100. https://doi.org/10.1109/TNS.1965.4323904

[14] Laurent Hériveaux, Jessy Clédière, and Stéphanie Anceau. 2013. Electrical Modeling of the Effect of Photoelectric Laser Fault Injection on Bulk CMOS Design. In *39th ISTFA ASM*.

[15] A. H. Johnston. 1993. Charge generation and collection in p-n junctions excited with pulsed infrared lasers. *IEEE Trans. Nucl. Sci.* (1993). https://doi.org/10.1109/23.273491

[16] A. G. Jordan and A. G. Milnes. 1960. Photoeffect on diffused P-N junctions with integral field gradients. *IRE Transactions on Electron Devices* 7, 4 (Oct 1960), 242–251. https://doi.org/10.1109/T-ED.1960.14688

[17] R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, G. Haller, V. Pouget, D. Lewis, J. M. Dutertre, and A. Tria. 2012. Characterization and TCAD simulation of 90 nm technology transistors under continous photoelectric laser stimulation for failure analysis improvement. In *2012 19th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits*. 1–6. https://doi.org/10.1109/IPFA.2012.6306298

[18] F. Lu, G. Di Natale, M. L. Flottes, and B. Rouzeyre. 2013. Laser-Induced Fault Simulation. In *2013 Euromicro Conference on Digital System Design*.

[19] F. Lu, G. D. Natale, M. L. Flottes, B. Rouzeyre, and G. Hubert. 2014. Layout-aware laser fault injection simulation and modeling: From physical level to gate level. In *2014 9th IEEE International Conference on Design Technology of Integrated Systems in Nanoscale Era (DTIS)*. 1–6. https://doi.org/10.1109/DTIS.2014.6850665

[20] G. C. Messenger. 1982. Collection of Charge on Junction Nodes from Ion Tracks. *IEEE Transactions on Nuclear Science* (1982). https://doi.org/10.1109/TNS.1982.4336490

[21] W. Meyer and R. Camposano. 1995. Active timing multilevel fault-simulation with switch-level accuracy. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 14, 10 (Oct 1995). https://doi.org/10.1109/43.466340

[22] A. Papadimitriou, D. Hély, V. Beroulle, P. Maistri, and R. Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*. 1–4. https://doi.org/10.7873/DATE.2014.219

[23] C. Roscian, A. Sarafianos, J. M. Dutertre, and A. Tria. 2013. Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells. In *FDTC, 2013 Workshop on*. 89–98. https://doi.org/10.1109/FDTC.2013.17

[24] M. B. Santos and J. P. Teixeira. 1999. Defect-oriented mixed-level fault simulation of digital systems-on-a-chip using HDL. In *Design, Automation and Test in Europe Conference and Exhibition, 1999. Proceedings (Cat. No. PR00078)*. 549–553. https://doi.org/10.1109/DATE.1999.761181

[25] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J. M. Dutertre, and A. Tria. 2013. Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology. In *IRPS, 2013 IEEE International*. 5B.5.1–5B.5.9. https://doi.org/10.1109/IRPS.2013.6532028

[26] Sergei P. Skorobogatov and Ross J. Anderson. 2002. Optical Fault Induction Attacks. In *4th International Workshop on Cryptographic Hardware and Embedded Systems*. Springer-Verlag, London, UK, 2–12.

[27] R. A. C. Viera, J. M. Dutertre, R. P. Bastos, and P. Maurine. 2017. Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation. In *2017 Euromicro Conference on Digital System Design (DSD)*. 252–259. https://doi.org/10.1109/DSD.2017.43

[28] J. L. Wirth and S. C. Rogers. 1964. The Transient Response of Transistors and Diodes to Ionizing Radiation. *IEEE Transactions on Nuclear Science* 11 (1964).