

Body biasing injection: analysis, modeling and simulation (MAX 14 PAGES)

Geoffrey Chancel

Abstract—This is the abstract.
Orange text is for undecided wording/words.
Red text is for important messages.
Cyan text is for future bib references to add.

Index Terms—Article submission, IEEE, IEEEtran, journal, L^AT_EX, paper, template, typesetting.

I. INTRODUCTION

WHEN working with cybersecurity, specifically with hardware security, various fault injection methods are often considered. One can point out Electromagnetic Fault Injection (EMFI) [1], [2], Laser Fault Injection (LFI) [3], or Body Biasing Injection (BBI) [4], not to cite them all. The current work is dedicated in studying Body Biasing Injection.

Nowadays, electronic devices are found in every economic sector, and very often they manipulate sensitive data, such as in bank transactions, Internet of Things (IoT) devices, or smartphones. To ensure data authenticity, these devices embed cryptographic algorithms. While theoretically secure, once implemented on actual devices, these algorithms become fallible, leaking manipulated data, in addition to being sensitive to external disturbances.

A. Fault injection objectives

Fault injection methods are set up to perform various malicious manipulation on integrated circuits, such as:

- Denial of service (DoS) → Stop circuit operation and the related services;
- Verification bypass → Modify data on the fly to fake authenticity (e.g. to bypass bootloader security);
- Confidential data extraction → Modify data to perform differential fault analysis.

B. BBI in the state-of-the-art

When compared to EMFI, BBI has a smaller state-of-the-art, whether in the amount of scientific papers published or in the amount of industrial platforms proposed. Currently, there are ten main works lingering on BBI [4]–[13]. Each one of them made a unique contribution for a better understanding of BBI.

The first one [4] introduced the technique and presented a Bellcore attack on the targeted IC. Then, one year later, another work [5] further studied the method, followed by a third work three years later [6], introducing an advanced test bench to work and perform attacks with BBI.



Fig. 1: Langer and Riscure BBI probes. riscure_langer

However, there are still unanswered questions, and the current work aims at bringing more answers thanks to previous and new data.

Before introducing the present work, let us eventually analyze the industrial platforms proposed by various manufacturers and introduce our own test platform. We can distinguish three major actors proposing BBI related products:

- Langer EMV-Technik;
- Riscure;
- NewAE Technology.

1) *Langer EMV-Technik platform*: The German society Langer EMV-Technik proposes an all-in-one and ready-to-use BBI platform composed of two hardware tools:

- A current pulse generator with a metal needle, shown in left in Fig. 1;
- A general controller called "Burst Power Station", combining a power supply, control and monitor tool and a software.

C. BBI interrogations

With all the work in the state-of-the-art in mind, there are still remaining questions unanswered about BBI, such as:

- What is the spatial resolution of BBI?
- What is the time resolution of BBI?
- Is thinning the substrate useful in any way?
- How BBI induced faults occur?
- How to properly model BBI?

II. MODELING AND SIMULATING BBI

SIMULATING a fault injection method behavior is an important part in understanding its mechanisms. Whether it is EMFI, LFI or BBI, it allows to predict and understand the underlying phenomena at work to set up reliable experiments. In this paper, we are focusing solely on BBI.

Ideally, we would want to directly observe signals inside integrated circuits, allowing for fine measurements of power supply voltages, logic levels and power current not to cite

every physical quantity. However, embedding sensors into an already existing IC is not possible, and doing so on future IC is costly and takes time to fully implement. In addition to this, we do not have any guarantee that these sensors will not be disturbed too much by the fault injection. Therefore, we have decided to take the following approach:

Simulation → Conclusions → Verification

By doing so, we have freed ourselves from hardware limitations. However, other limitations remains. Indeed, modern ICs, even the smallest, embed millions of transistors, and with current technologies, it is impossible to evaluate with simulations entire circuits at a transistor level. Therefore, to tackle these limitations, we decided to adopt an hybrid approach, combining transistor-less models and local logic gates simulations. This approach is a compromise between accuracy and computational cost/time, and allows simulating relatively big circuits under BBI disturbances. Overall, it is similar to what has been done for EMFI in [2]. The resulting simulation flow is divided in three consecutive steps:

- The simulation of an IC under BBI using a transistor-less model, allowing for a purely electrical analysis;
- The extraction of significant disturbed signals from the previous simulation;
- The simulation of functional logic gates under BBI thanks to the previously extracted signals.

A. An hybrid simulation flow: building the models

Building the correct models for the simulation flow pass through multiple steps. As the goal of the hybrid flow is to reduce the computational power required to evaluate an IC, it is still important to maintain a certain accuracy concerning the IC physical structure. To do so, the models are designed around actual IC implementations. The main building blocks of the models are the power supply network, the standard-cells, and the substrate structure. In this work, we are only focusing on bulk substrates: specifically dual-well and triple-well substrates.

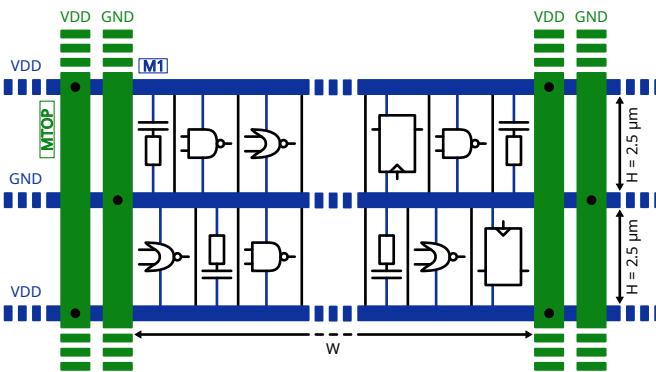


Fig. 2: A Standard-Cell Segment and its power delivery network.

fig_alim_std

1) Power supply rails and standard-cell segments: The power distribution inside an IC is typically made with a grid-like structure, composed of metal wires stacked on top of each

other on planes. In each layer, the metal wires are equally spaced and have a dedicated width, which becomes thinner the deeper they are. The lowest layer brings the power directly to the transistors. Fig. 2 presents a common power delivery network, designed with two metal levels for simplicity.

Within the metal lines are located standard-cell segments (SCS), composed of decoupling, logic and sequential elements, and are pre-characterized by foundries and categorized depending on their performance (mainly but not exclusively power consumption and speed). As illustrated in Fig. 2, SCS have a constant height, in our case of 2.5 μm , and a variable width depending on how much logic gates each one of them embed. As we have stated previously, the hybrid simulation flow use transistor-less models as basic IC building blocks. Therefore, the transistors, hence the standard-cell segments, are modeled with passive elements such as resistors and capacitors.

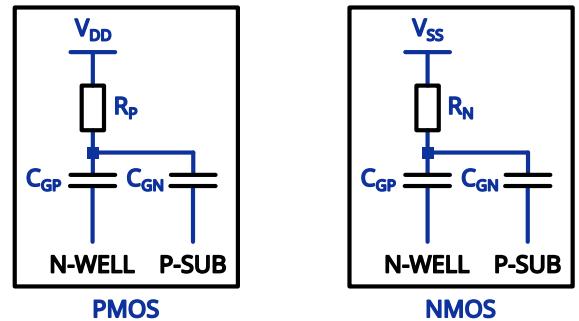


Fig. 3: aaa
mos_passive

To that end, the elementary SCS chosen measures 30 μm by 5 μm , representing two rows of logic cells. This represents about a hundred of logic gates, represented with four resistors and two capacitors, as shown in Fig. 3, with half of the transistors conducting, half not conducting. The conducting NMOS transistors, whose source is connected to V_{SS} , are equivalent to the passive resistor R_N . The conducting PMOS transistors, whose source is connected to V_{DD} , are equivalent to the passive resistor R_P . The resistors values depends on the considered technology, as well as the capacitors values, and can be adjusted and calculated according to one needs.

2) The substrate: Because BBI can be performed thanks to the silicon substrate as the main physical environment transferring energy from a generator to an IC, it is fundamental to elaborate a proper substrate model to precisely represent the various involved phenomena. As stated previously, our work focuses on bulk substrates, and in most cases, the substrate silicon is P-doped. There are two typical ways of lithographing the transistors in a bulk substrate, using dual-well or triple-well structures. Dual-well substrates are commonly found in moderately old circuits, while triple-well substrates are found in more recent circuits, while not bleeding-edge.

To properly understand how the differences between dual-well and triple-well substrates change the resulting model, let us analyze the cross-sectional schematics of an inverter created respectively in a triple-well and a dual-well substrate, as shown respectively in Fig. 4.a and Fig. 4.b:

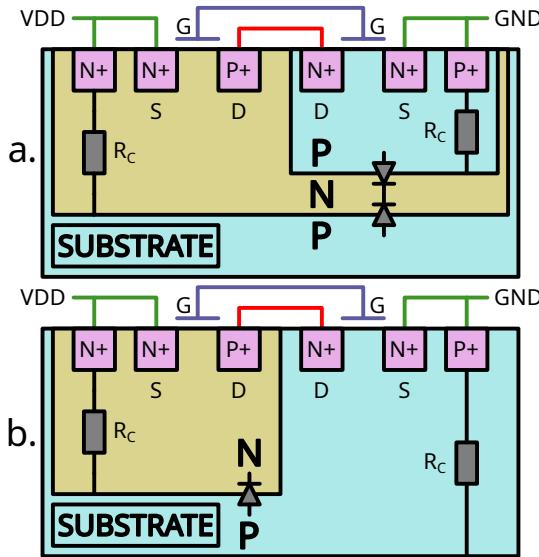


Fig. 4: Triple-well (a.) and Dual-well (b.) inverter cross-sectional view.

`fig_sub`

- In the triple-well substrate, the NMOS transistors are lithographed into a P-doped silicon well, itself lithographed inside a N-doped well, buried inside the P-doped substrate. The PMOS transistors are located inside the N-doped well;
- In the dual-well substrate, the PMOS transistors are still located inside the N-doped well, however, the NMOS are lithographed directly inside the P-doped substrate.

On the one hand, the triple-well substrate reveals two diodes:

- One formed between the P-well and the N-well;
- Another formed between the N-well and the P-substrate.

On the other hand, the dual-well substrate only reveals one diode between the N-well and the P-substrate.

3) *The resulting model*: Thanks to what we have introduced previously, we can now build the elementary building blocks for our hybrid simulation flow. It combines the power delivery network architecture, the equivalent logic gates models, and the substrate structure, all in an embedded model. This model represents an elementary section of the simulated IC, measuring 30 μm by 5 μm by t_{Sub} μm , the latter being the substrate thickness, a parameter which will vary depending on each considered IC.

As we consider both triple-well and dual-well substrate, there are two resulting elementary models, shown in Fig. 5. Each model is composed of various sub-regions, whose descriptions follow:

- 1 is the substrate network, divided into six sub-networks of six resistors for finer details;
- 2 is the first P-N silicon junction, common to both models;
- 3 is the access resistor (DW) or the second junction (TW);
- 4P is the PMOS equivalent section;
- 4N is the NMOS equivalent section;

- 5, 5' are the power supply metal layers (upper metal in green, first level in blue);
- 6 is the power supply decoupling.

As we have stated before, these models only represent a small portion of the modeled IC. To create an entire IC of a defined size, it is required to instantiate and interconnect as much as needed the elementary models. By doing so, we can create a bigger model of virtually any size. The language we have chosen to work with the simulation is the SPICE language. However, we created a custom Python script to interconnect the SCS together, place external power connections, and generate a SPICE file. For the current work, we decided to put the external power connections at the top and bottom of the IC (seen from above), and the BBI probe at the center of the IC (on the backside).

B. An hybrid simulation flow: performing simulations

Now that we set up the base models and their duplication, we can perform simulations with those models. To properly use these models, it is required, in the first place, to validate them through various steps to ensure their reliability. To that end, we generated an IC measuring 550 μm by 450 μm with a 140 μm substrate thickness, and performed an operating point to verify the correctness of the models for each substrate type.

Value	Triple-well	Dual-well
I_{GND}	2.88 nA	2.85 nA
I_{VDD}	-8.64 nA	-2.92 nA
GND_{drop}	1.83 nV	1.76 nV
VDD_{drop}	1.2 nV	1 nV

TABLE I: op point

`tab_op`

We should expect almost no voltage drop and zero current consumption from such a model. Otherwise, it indicates an underlying issue with the model.

Table I shows the operating point results for both a triple-well and a dual-well circuit, and indicates a correct operating point, with idle currents and voltage drops close to zero. However, verifying the bias point alone is not sufficient to consider the model validated. As these models are dedicated to be mainly used in transient simulations, it is required to perform one and evaluate the soundness of its results.

Therefore, we performed transient simulations with a triple-well and dual-well IC, with the following parameters:

- A nominal power supply voltage of 1.2 V;
- A voltage pulse amplitude of ± 300 V;
- A voltage pulse width of 15 ns;
- Rise and fall times of 8 ns;
- A simulation duration of 80 ns;
- A simulation time step: of 50 ps.

C. An hybrid simulation flow: analyzing the results

Analyzing the simulation results involves observing various internal IC signals, for each substrate type, the ones presented in this section being:

- The power supply voltage distribution;
- The epitaxial current;

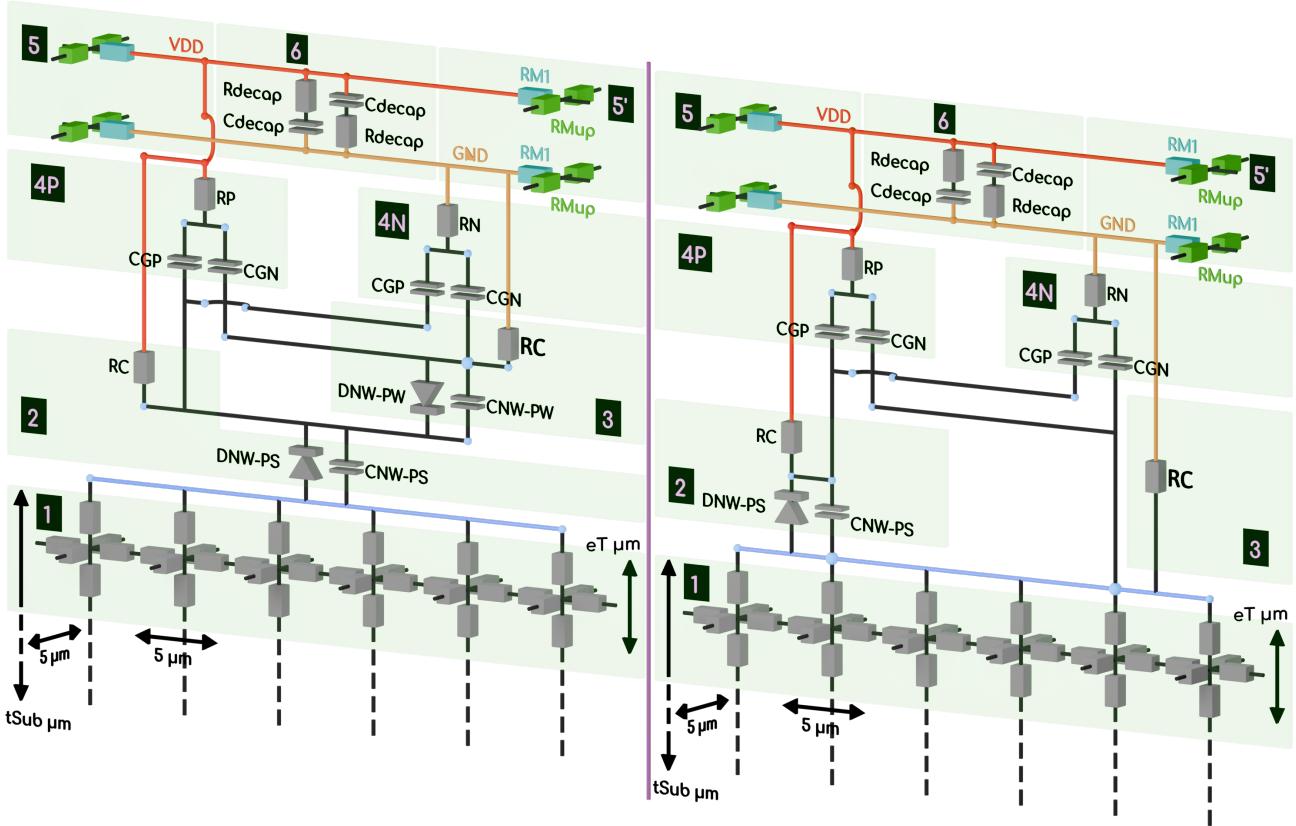


Fig. 5: Triple well (left) and dual well (right) std cell (PEUT ETRE FAIRE DES SOUS-FIGURES)
fig_triplewellstdcell

- The substrate current distribution;
- The substrate pre-layer current density.

The observed signals are displayed in two dimensions and at the apex of the BBI disturbance. Each signal brings some insights on what happens inside the circuits during a BBI pulse. We will first analyze the dual-well results, then the triple-well ones, to finally conclude with a comparison of both.

1) *Negative dual-well simulation results:* Fig. 6 shows the dual-well positive pulse results.

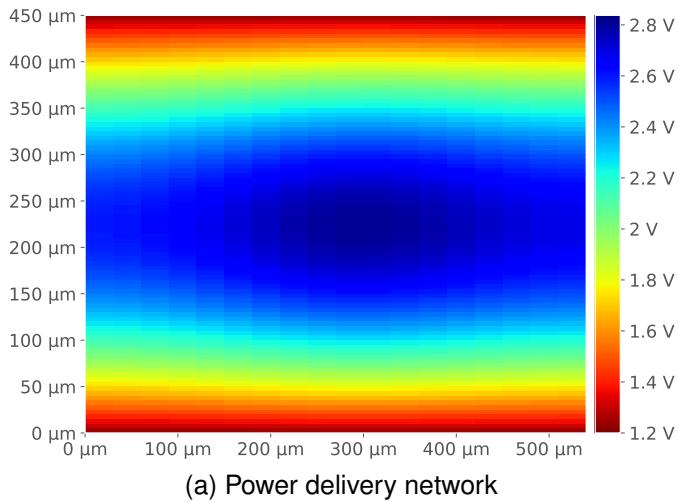
Sub-fig. 6(a) represents the power delivery network (PDN) voltage across the entire IC as seen from above. In other words, it is the supply voltage of the transistors. Expectedly, far from the external power connections, we observe some deviation from the nominal 1.2 V power supply voltage. However, at the center of the circuit, in other words under the BBI probe, the voltage goes up to 2.8 V, being a 33 % increase from the nominal value.

To put these values into perspective, let us look at sub-fig. 6(b), showing the epitaxial current distribution, representing the charges going from the substrate to the top of the SCS. According to the sub-figure, most of the charges are flowing at the center of the IC, under the BBI probe, as the current is the highest in that location. It is sound when comparing sub-fig. 6(a) and sub-fig. 6(b), as the voltage difference from the nominal value is higher where the epitaxial current is higher.

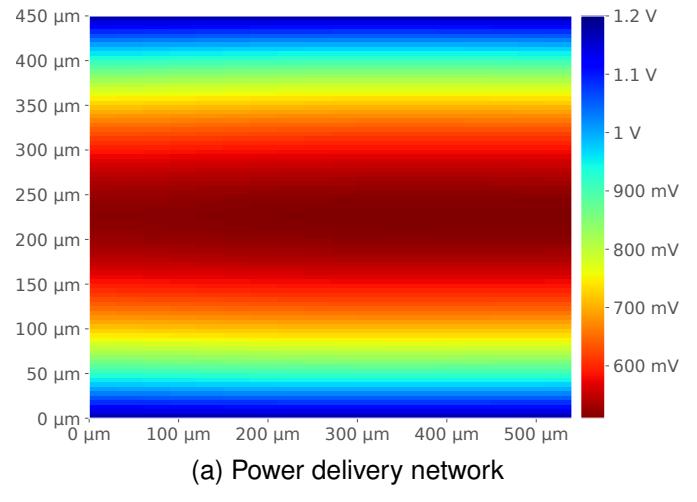
Sub-fig. 6(c) and sub-fig. 6(d) both represent the same physical quantity in two different ways. We have chosen this approach to extract as much information as possible from

these models and simulations. Sub-fig. 6(c) shows the cross-sectional view (from the Y-axis) of the current distribution inside the silicon substrate. The substrate being an isotropic environment, in other words, its resistivity is homogeneous in every spatial directions, we can observe a hemispheric current distribution in it. However, due to the large difference between the first layer (the farthest to the probe) and the last layer (the closest to the probe), it is difficult to do more observations. Therefore, we can look at sub-fig. 6(d), which represents the same data in a different perspective. To better illustrate the inter-layer differences, we have chosen to normalize the data in a per-layer basis. Thus, it allows us to compare the current density between layers. It is important to note that the normalized values are calculated in a way that the closer they are to zero, the denser the current is, and vice-versa. The layer 0 is the closest to the logic gates, while the layer 13 is the closest to the backside (the probe). What is interesting to note here is that for each substrate layer, the current is focused where the probe is located. It is to be expected, as the substrate is isotropic. However, the deeper we are into the substrate, the less focused the current is. Once again, it is quite logical as the charges diffuse homogeneously inside the substrate.

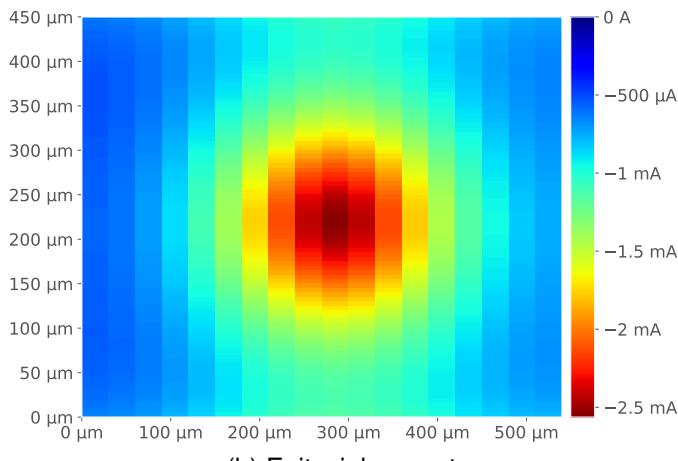
2) *Positive dual-well simulation results:* Concerning the positive pulse dual-well results, let us look at Fig. 7. Compared to the previous results, sub-fig. 7(a) shows that the PDN voltage exhibits not a voltage increase, but rather a voltage drop. Indeed, under the probe, the PDN voltage drops to 500 mV from 1.2 V. This is a substantial difference, which could



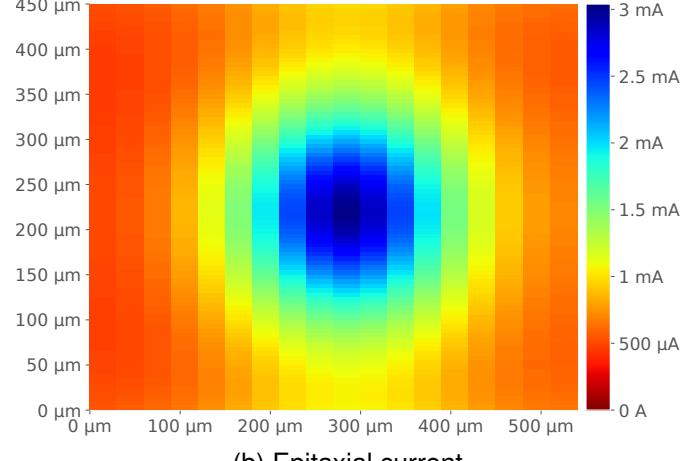
(a) Power delivery network



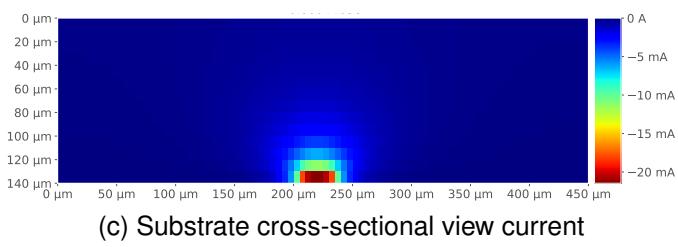
(a) Power delivery network



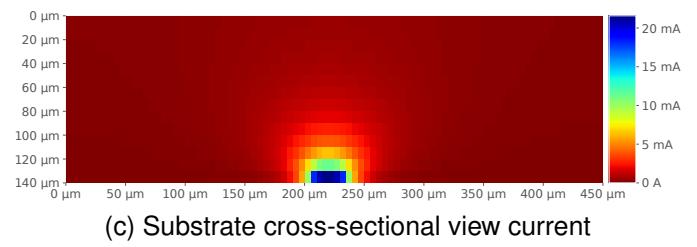
(b) Epitaxial current



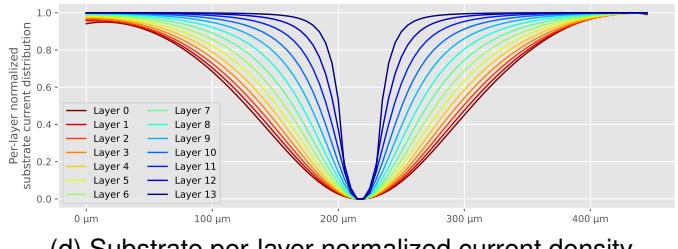
(b) Epitaxial current



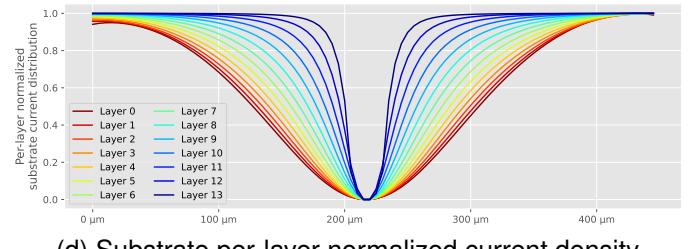
(c) Substrate cross-sectional view current



(c) Substrate cross-sectional view current

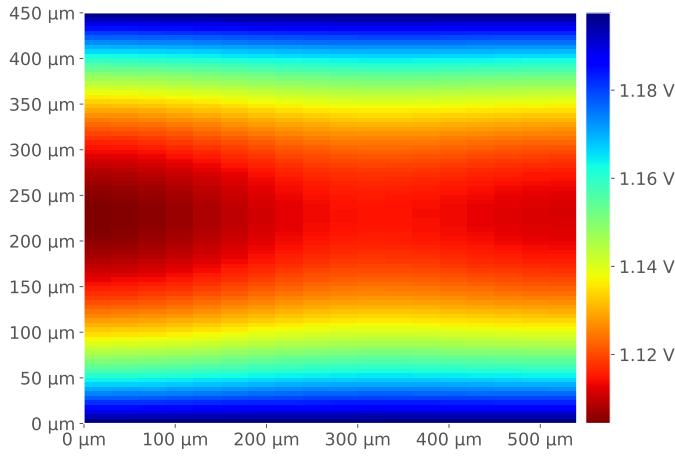


(d) Substrate per-layer normalized current density

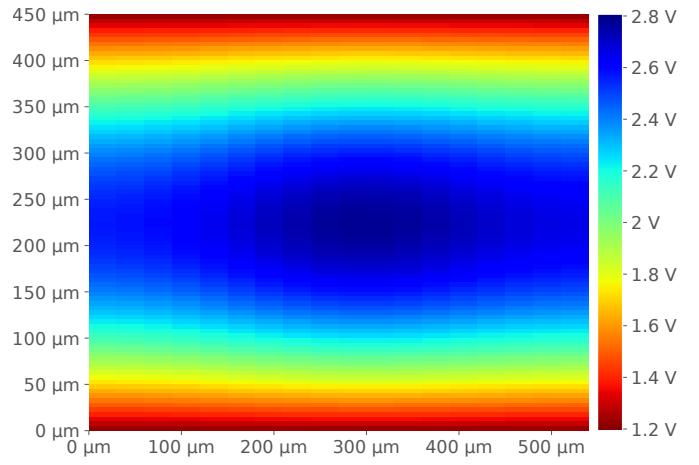
Fig. 6: Dual-well IC negative pulse simulation results_{sim_res_dw_neg}

(d) Substrate per-layer normalized current density

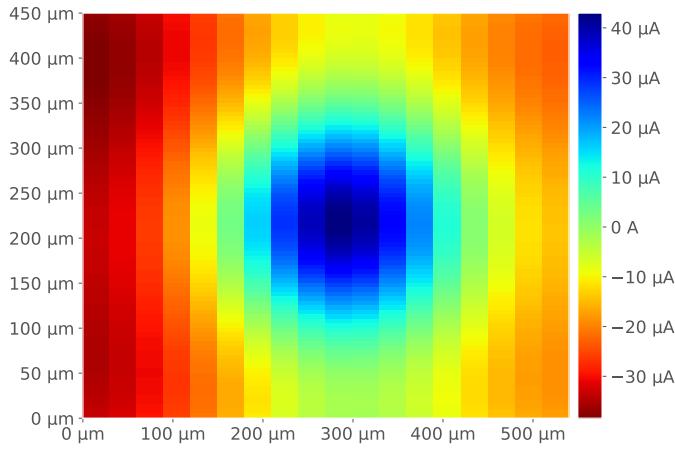
Fig. 7: Dual-well IC positive pulse simulation results_{sim_res_dw_pos}



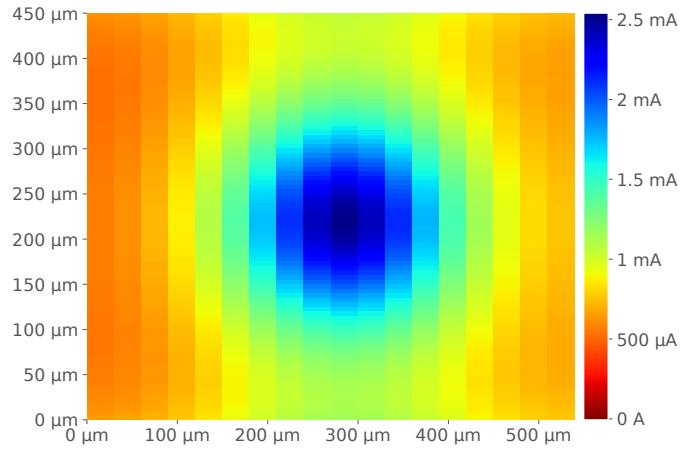
(a) Power delivery network



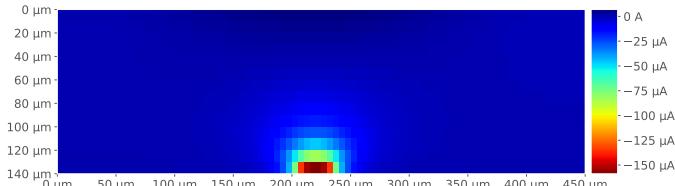
(a) Power delivery network



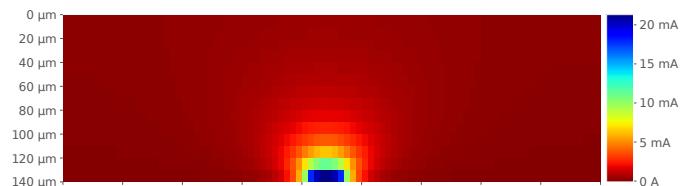
(b) Epitaxial current



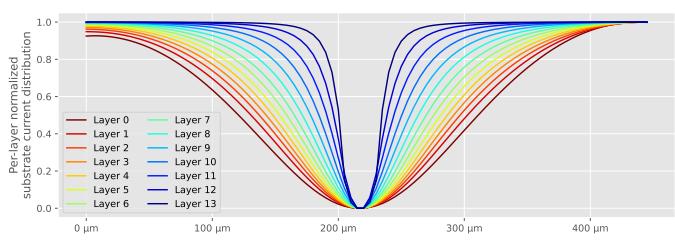
(b) Epitaxial current



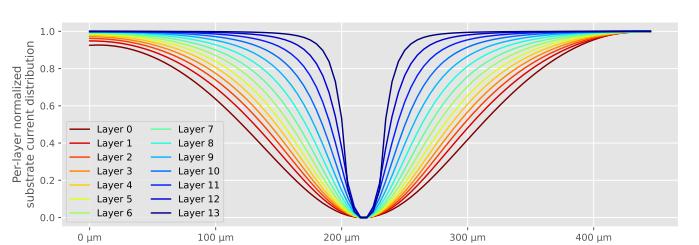
(c) Substrate cross-sectional view current



(c) Substrate cross-sectional view current



(d) Substrate per-layer normalized current density

Fig. 8: Triple-well IC negative pulse simulation results_{sim_res_tw_neg}

(d) Substrate per-layer normalized current density

Fig. 9: Triple-well IC positive pulse simulation results_{sim_res_tw_pos}

lead, if applied to actual transistors, a significant change in behavior such as an incorrect biasing.

Concerning the epitaxial current, shown in sub-fig. 7(b), we can notice two key changes. First, the current polarity has changed, from a negative to a positive one. Once again, it was to be expected, as the voltage pulse polarity has changed. Then, in absolute value, the maximal current is 500 mV higher than previously, which indicates that more energy has been injected into the circuit. Eventually, regarding the substrate current, there are no major differences except the current polarity, both for sub-fig. 7(c) and sub-fig. 7(d).

3) *Negative triple-well simulation results:* Let us take a closer look at Fig. 8. These results stand out all of the others, in many ways. First, if we take a look at sub-fig. 8(a) regarding the PDN voltage, we can see that there are very little variations from the nominal voltage. Indeed, the voltage drops only to 1.1 V. Then, concerning the epitaxial current shown in sub-fig. 8(b), we can see that it is almost a hundred times lower than on other results. It is then confirmed in sub-fig. 8(c) with the substrate current distribution. However, the current density stays consistent with the previous results. Before analyzing further these results and explaining them, let us analyze the last case.

4) *Positive triple-well simulation results:* Quite interestingly, with a triple-well substrate and a positive voltage pulse, as displayed in Fig. 9, we observe results that are very similar to the dual-well negative case (Fig. 6), whether it is on the PDN voltage or on the epitaxial current. Indeed, the PDN voltage disturbance is almost identical to sub-fig. 6(a), with an increase in voltage from 1.2 V to 2.8 V. Then, the epitaxial and substrate current maps are mirrors (in polarity) of sub-fig. 6(b) and 6(c). Eventually, the current density graph is very close to the other results.

5) *Differences between dual-well and triple-well (negative and positive pulses):* As we have seen through this section, we have four possible scenarios:

- A dual-well substrate and a negative voltage pulse;
- A dual-well substrate and a positive voltage pulse;
- A triple-well substrate and a negative voltage pulse;
- A triple-well substrate and a positive voltage pulse.

Each scenario behave differently than the others for one main reason: the electric coupling between the probe (substrate) and the SCS (logic). These differences in coupling are due to the substrate structure we encounter in dual-well and triple-well circuits.

As we have described before, the dual-well substrate embeds a P-N diode between the P-substrate and the N-well, and depending on the voltage pulse polarity, this diode is either blocking or conducting. This diode is interspersed between the substrate and the PMOS section. On the one hand, concerning the negative pulse scenario, the diode is blocking, thus creating an AC-coupling between the probe and the PMOS. On the other hand, the NMOS are DC-coupled to the probe as they are connected through a resistive path. Therefore, the circuit is globally DC-coupled to the probe, allowing the charges to flow all the time during the pulse. Then, concerning the positive pulse scenario, the diode conducts, creating another DC path to the transistors, reducing the effective circuit impedance seen

Substrate	Polarity	NMOS	Coupling	Circuit	Danger
		PMOS			
Dual-well	Negative	DC	AC	DC	
Dual-well	Positive	DC	DC	DC	
Triple-well	Negative	AC	AC	AC	
Triple-well	Positive	AC	DC	DC	

TABLE II: Caption

dw_tw_table

by the probe. It explains the greater observed currents, as the charges have an additional DC path to follow.

On the triple-well side, the top of the SCS is barred with a first P-N diode (P-substrate N-well), and the NMOS are behind another diode. When using negative pulses, the first diode is blocking, therefore creating a pure AC-coupling between the probe and the circuit. It means that the charges are able to flow in and out of the SCS only on the pulse edges. Consequently, for a given voltage pulse, less energy is transferred into the IC in that case.

Then, regarding the triple-well positive scenario, the first diode become conducting, while the second stays blocking. Therefore, the PMOS are DC-coupled, while the NMOS stay AC-coupled. We come back to a scenario similar to dual-well negative.

Eventually, the main outcomes these simulation results show are in Table II, alongside a qualitative dangerousness appreciation of each scenario.

III. VALIDATING AND COMPLETING THE MODELS

With the aim of verifying the soundness of the previous conclusions, we set up experiments using an actual IC composed of both triple-well and dual-well substrate on a monolithic die. These experiments consist in verifying if the difference in injected energy depending on the substrate type is actually significant or not.

The target used is a STM32F439 microcontroller, alongside the platform presented in the first chapter. We call these experiments "IC ground current mapping", and quite naturally, they consist in measuring in specific conditions the current at the target circuit external ground connection. The entirety of the IC is mapped, and a voltage pulse is injected at each location. Then, we measure the current at the circuit ground and calculate its RMS value to represent it into a two-dimensional cartography.

Knowing the coarse structure of the considered IC, in addition to having insights on the substrate type, we could draw the coarse structure picture shown in Fig. 10. The "glue logic" regions are known to be made with triple-well substrates, while the "flash control" and "analog" regions are made with dual-well substrates. The memories, however, are made of a mix of both.

REFERENCES

- [1] Mathieu Dumont, Philippe Maurine, and Mathieu Lisart. Modeling of electromagnetic fault injection. In *2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, pages 246–248, 2019.
- [2] M. Lisart M. Dumont and P. Maurine. Modeling and simulating electromagnetic fault injection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(4):680–693, 2021.

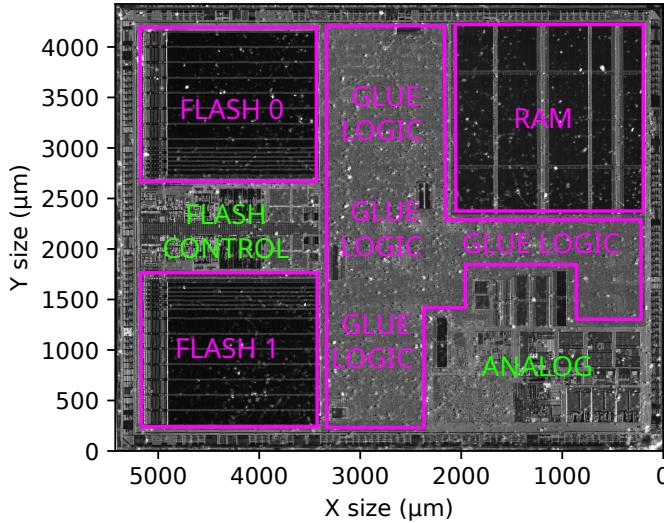


Fig. 10: Caption
stm_ir_photo

- [3] Jean-Max Dutertre, Vincent Berouille, Philippe Candelier, Stephan De Castro, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hély, Regis Leveugle, Paolo Maistri, Giorgio Di Natale, Athanasios Papadimitriou, and Bruno Rouzeyre. Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 1–6, 2018.
- [4] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre-Yvan Liardet. Yet another fault injection technique : by forward body biasing injection. "Yet Another Conference on Cryptography France (2012)", 09 2012.
- [5] K. Tobich, P. Maurine, P.-Y. Liardet, M. Lisart, and T. Ordas. Voltage spikes on the substrate to obtain timing faults. In *2013 Euromicro Conference on Digital System Design*, pages 483–486, 2013.
- [6] Noemie Beringuier-Boher, Marc Lacruche, David El-Baze, Jean-Max Dutertre, Jean-Baptiste Rigaud, and Philippe Maurine. Body biasing injection attacks in practice. In *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems, CS2 '16*, page 49–54, New York, NY, USA, 2016. Association for Computing Machinery.
- [7] Colin O'Flynn. Low-cost body biasing injection (BBI) attacks on WLCSP devices. In Pierre-Yvan Liardet and Nele Mentens, editors, *Smart Card Research and Advanced Applications*, pages 166–180, Cham, 2021. Springer International Publishing.
- [8] Takuya Wadatsumi, Kohei Kawai, Rikuu Hasegawa, Takuji Miki, Makoto Nagata, Kikuo Muramatsu, Hiromu Hasegawa, Takuya Sawada, Takahito Fukushima, and Hisashi Kondo. Voltage surges by backside esd impacts on ic chip in flip chip packaging. In *2022 IEEE International Reliability Physics Symposium (IRPS)*, pages P14–1–P14–6, 2022.
- [9] Takuya Wadatsumi, Kohei Kawai, Rikuu Hasegawa, Kazuki Monta, Takuji Miki, and Makoto Nagata. Characterization of backside esd impacts on integrated circuits. In *2023 IEEE International Reliability Physics Symposium (IRPS)*, pages 1–6, 2023.
- [10] G. Chancel, J.-M. Galliere, and P. Maurine. Body biasing injection: To thin or not to thin the substrate? In Josep Balasch and Colin O'Flynn, editors, *Constructive Side-Channel Analysis and Secure Design*, pages 125–139, Cham, 2022. Springer International Publishing.
- [11] G. Chancel, Jean-Marc Gallière, and P. Maurine. Body biasing injection: Impact of substrate types on the induced disturbances. In *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 50–60, 2022.
- [12] G. Chancel, J.-M. Galliere, and P. Maurine. A better practice for body biasing injection. In *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 48–59, 2023.
- [13] Colin O'Flynn. Picoemp: A low-cost emfi platform compared to bbi and voltage fault injection using tdc and external vcc measurements. Cryptology ePrint Archive, Paper 2023/1195, 2023. <https://eprint.iacr.org/2023/1195>.