THESIS TO OBTAIN THE DEGREE OF DOCTOR
OF THE UNIVERSITY OF MONTPELLIER

In SyAM - Automatic and Microelectronic Systems

Doctoral school: Information, Structures and Systems sciences

Research Unit: LIRMM

Body biasing fault injection: modeling

Presented by Geoffrey Chancel

COMPILATION DATE: COMPILATION DATE: 2023-07-19 13:44:45+02:00

Under the supervision of TO BE COMPLETED

Thesis Committee:

Philippe Maurine , Associate Professor ?? , University of Montpellier	**Thesis Director**
Jean-Marc Gallière, Associate Professor ?? , University of Montpellier	**Thesis Supervisor**

UNIVERSITÉ DE MONTPELLIER

Abstract COMPILATION DATE: 2023-07-19 13:44:45+02:00

Résumé de la thèse COMPILATION DATE: 2023-07-19 13:44:45+02:00

Acknowledgements COMPILATION DATE: 2023-07-19 13:44:45+02:00

The authors acknowledge the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-19-CE39-0008 (project ARCHI-SEC). They also acknowledge the French Ministère des Armées – Agence de l'innovation de défense (AID) under grant ID-UM-2019 65 0036.

Contents

List of Figures

List of Tables

List of Algorithms

List of Acronyms

BBI	**B**ody **B**iasing **I**njection
EMFI	**E**lectro-**M**agnetic **F**ault **I**njection
LFI	**L**aser **F**ault **I**njection
SCS	**S**tandard **C**ell **S**egment
BSIM	**B**erkeley **S**hort-channel **I**GFET **M**odel
RAM	**R**andom **A**ccess **M**emory

I

Introduction COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap:1intro

Contents

1.1 Context COMPILATION DATE: 2023-07-19 13:44:45+02:00

1.2 Contribution COMPILATION DATE: 2023-07-19 13:44:45+02:00

II

Body Biasing Injection platforms and good practices COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap:2goodPractices

Contents

2.1 Summary COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:summary

This chapter first introduces multiple concepts, hardware and tools which are used and mentioned all along the work. Afterward, as its name implies, it brings forward better practices for Body Biasing Injection. It aims at introducing them with theoretical examples in addition to practical demonstrations. To that end, we propose to analyze different BBI platform scenarios thanks to coarse electrical models, allowing us to analyze their drawbacks and advantages in order to introduce the proposed enhancements. Eventually, we will present a real differential fault attack on a hardware AES co-processor in order to illustrate the soundness of the proposed improvements.

2.2 Introduction COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:intro

2.2.1 Platform equipment COMPILATION DATE: 2023-07-19 13:44:45+02:00

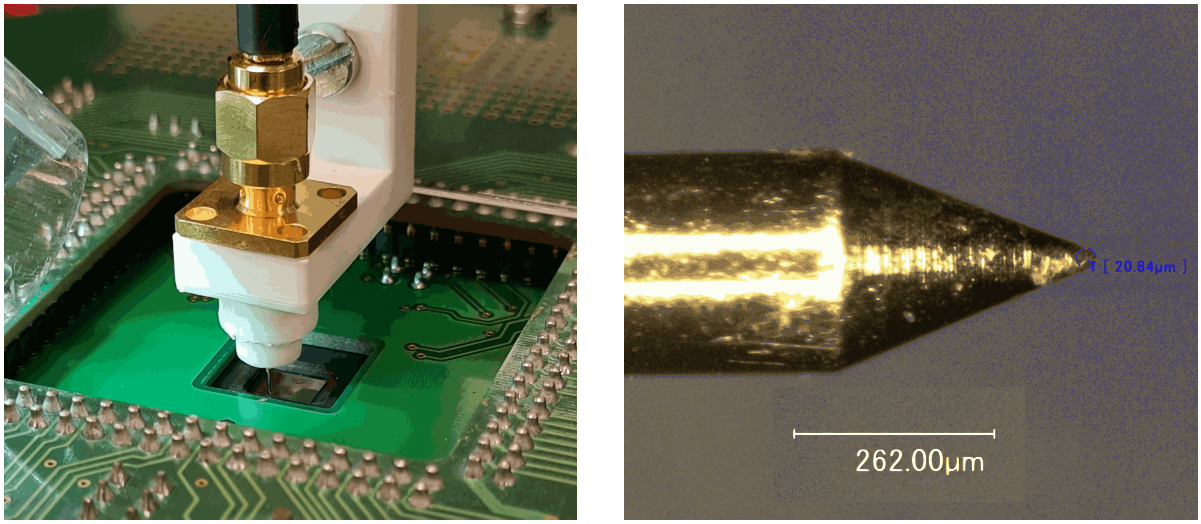
chap2:intro:platEquip

This section is dedicated in presenting the different piece of equipment which allowed us to perform this work. The hardware platform, as well as the different software used are introduced.

2.2.2 The hardware COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:intro:platEquip:hardware

The main piece of equipment when working with BBI is the electrical probe. It is commonly made with a metal tip, a connector of any sort and a mechanical support to hold everything together. For the purpose of this work, a custom probe was designed around three simple parts, an SMA connector, in order to have a low-cost, small and standard interconnection, a spring-loaded metallic probe soldered onto the SMA connector, and a custom 3D printed support to hold the structure together. Fig. 2.1 shows detailed pictures of the designed BBI metallic probe, with a global view in operation on Fig.2.1a, and a photograph under a microscope of the probe's tip-end on Fig. 2.1b, allowing to measure its actual size before the first usage. The metallic probe used has



(a) *BBI metallic probe in mechanical contact with IC target.* `subfig:sondeBBI`

(b) *BBI metallic probe measurement closer look* `subfig:pointeBBI`

Figure 2.1: *Dual-well and triple-well inverter silicon sectional view ARRANGER MISE EN PAGE FIGURES* `fig:sondePointeBBI`

a 0.635 mm diameter and is 16.35 mm long. The specified maximum nominal current of the probe is of 1.5 A, and the electrical contact resistance measures 70 mΩ.

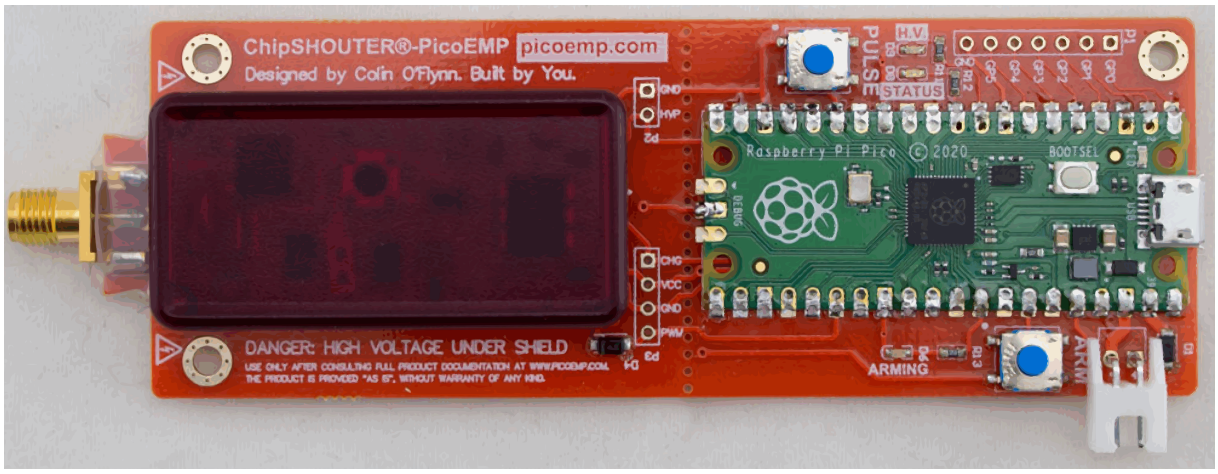


Figure 2.2: *ChipSHOUTER®-PicoEMP from NewAE Technology Inc.* `fig:newAeChipShouter`

Another fundamental piece of equipment for the practice of BBI is the voltage pulse generator. It is, generally, the most expensive hardware tool required. However, nowadays, cheap solutions are easily available, like the NewAE Technology Inc. ChipSHOUTER®-PicoEMP for example, illustrated in Fig. 2.2. In addition to being cheaper than most industrial solutions, its design sources are available online, making it a future-proof solution. In contrast to more expensive solutions, it has inevitably some drawbacks:

- The output transformer is low-power, around up to 200 mW
- Its recovery time is slow, from 1 to 4 seconds between pulses
- It can generate maximum voltage pulses of approximately 250 V
- There is no pre-calibration
- The pulse width control is not as reliable as other solutions

Figure 2.3: *Front side of the Avtech Electrosystems Ltd. AVRK-4-B High Voltage Pulser.* fig:avrk4b

Nevertheless, for this work, the generator used in all experiments is from the company Avtech Electrosystems Ltd., specifically the model AVRK-4-B, shown in Fig. 2.3. It is a high-speed and high-voltage generator, specified to work with 50 Ωloads. Its main specifications are the following:

- Voltage pulse amplitude from 150 V to 750 V with positive and negative polarities
- Pulse width ranging from 6 ns to 20 ns
- Rise time (resp. fall-time) for positive (resp. negative) pulses of 4 ns
- Up to 1000 pulses per second
- GPIB remote control
- Propagation delay under 150 ns
- DC-coupled output

Then, the central piece of equipment of any fault injection method is the IC target. In our work, the focus was made on an STM32F439VIT6 LQFP100 micro-controller. It is

a moderately modern IC commonly used nowadays. It was chosen because it embeds a dedicated cryptographic core, able to do DES or AES not to cite them all. The IC is manufactured with a bulk 90 nm process. Its core clock frequency goes up to 180 MHz, and it embeds 256 kB of RAM and 2 MB of Flash memory in two separate banks.

2.2.3 The software COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:intro:platEquip:software

Because several simulations are performed for the purpose of this work, different piece of software are used. In order to perform every electrical simulations, we used Synopsys®'s PrimeSim HSPICE. It allows fast simulations with parallel calculation of large netlists. The computer used for these simulations is made around a 48 cores, 96 threads CPU, alongside 420 GB of usable system memory. As we will study further in Chapter 3, the considered netlists are procedurally generated. To that end, we developed an algorithm, implemented in Python. It allows automatic generation of every netlist, minimizing user intervention, therefore drastically reducing errors, especially when considering the size of the simulated netlists. Indeed, they are not complex in their structure, as they are composed of resistors, capacitors and diodes, but the amount of components ranges from one million for the smallest, to 4.7 millions for the biggest. The main limitation in simulating these netlists lies in the available system memory, as it is the first bottleneck to appear. In fact, simulating the smallest ICs takes up to 76 GB of memory during the transient simulation. As the memory usage scales linearly with the number of components, and because when doubling the width and height, the IC surface quadruples, the same applies for the components count. Therefore, simulating the biggest ones takes up to 420 GB of system memory, which represents an IC size of 1.1 mm by 1.2 mm. In addition to the memory consumption, the time required is also an important factor. Effectively, the smallest ICs take up to four hours and ten minutes with 8 CPU threads (which is close to the maximum HSPICE can do for our netlists). Then, because simulation time scales linearly with components count, the biggest IC takes up to 17 hours to be completed.

2.3 Body Biasing Injection enhanced practice COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:goodPractices

With the platform thoroughly introduced,we can now discuss the BBI practice in the state of the art compared to the enhancements we propose.

2.3.1 BBI practice in the state of the art COMPILATION DATE: 2023-07-19 13:44:45+02:00

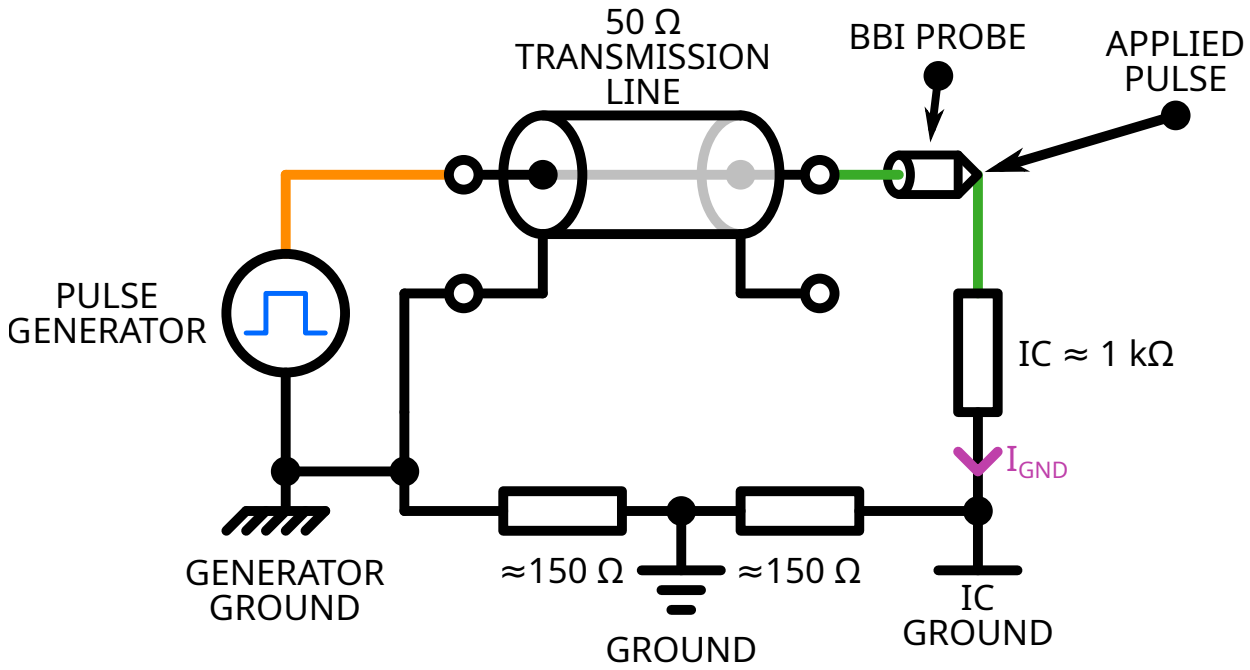


Figure 2.4: *BBI platform example in the state of the art*

fig:bbiPracticeBadGnd

First and foremost, in order to introduce the proposed enhancements, we will explain the limitations of state of the art BBI practices.

2.4 Giraud's differential fault attack COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap2:dfaGiraud

III

Integrated circuits modeling COMPILATION DATE:

2023-07-19 13:44:45+02:00

chap:3icModeling

Contents

3.1 Summary COMPILATION DATE: 2023-07-19 13:44:45+02:00

This chapter presents the work carried out concerning the modeling and simulation of integrated circuits and platforms in a body biasing fault injection context. The presented work focused on elaborating electrical models allowing to evaluate with simulations the behaviors of ICs subjected to BBI. The chapter introduces the elaborated models and the algorithms used to create them, and then goes on to present various validation steps to check the meaningfulness of the models. Parts of this work have been published both in [1] and [2].

3.2 Introduction COMPILATION DATE: 2023-07-19 13:44:45+02:00

When evaluating and studying ICs under BBI, it is important to be able to fully predict and understand the underlying mechanisms at work in order to set up reproducible and reliable experiments, as well as being able to set up efficient countermeasures. However, to model and simulate integrated circuit behavior subject to fault injection is not an easy task. Specifically, simulating an entire IC at a transistor level under fault injection is unrealistic with current resources and technology. It is especially true when considering time cost, as current digital ICs are composed of about a million of transistors for standard microcontrollers. Furthermore, no software nor algorithm is currently dedicated to simulate the functional, electrical behavior of millions of transistors at the same time while some of them are disrupted by strong and transient disturbances. In addition to that, to be able to set up a reliable model, one should have access to the detailed architecture of each considered IC, which is almost never the case, as most studied architectures are proprietary. Therefore, it is required to find alternative workarounds in order to be able to study IC behavior and their various responses to fault injection techniques.

This has been first proposed in 2019 concerning Electromagnetic Fault Injection (EMFI) [3], and further extended in 2021 [4]. Especially in the latest work [4], the proposed solution consisted in establishing an equivalent non-logical model of the section of an IC. Instead of modeling each logic gate with as many transistors as required,

in addition to the power delivery network and the silicon substrate, it was chosen to represent a hundred of logic gates in an average way, solely with a few resistors and capacitors. This results in a transistor-less model, achieved using manufacturing data for the studied IC. The authors assumed that the first half of the transistors are conducting while the other half are blocking. Then, two levels of power delivery network were added, simply modeled with electrical resistances. Eventually, and because the modeled IC was manufactured using a dual-well substrate type, the silicon substrate and the P-N junction respectively are modeled by six resistors going in every direction in addition to a diode and its capacitance respectively. This clever design allows to drastically reduce the computing work required to analyze and predict behaviors of ICs subject to EMFI. Indeed, simulating the average behavior of a hundred of logic gates only with four resistors and four capacitors is immensely lighter than simulating the equivalent with BSIM (Berkeley Short-channel IGFET Model) transistors. However, the main shortcoming being the lack of functionality with the produced ICs, it is therefore impossible to evaluate their functional or logical behavior.

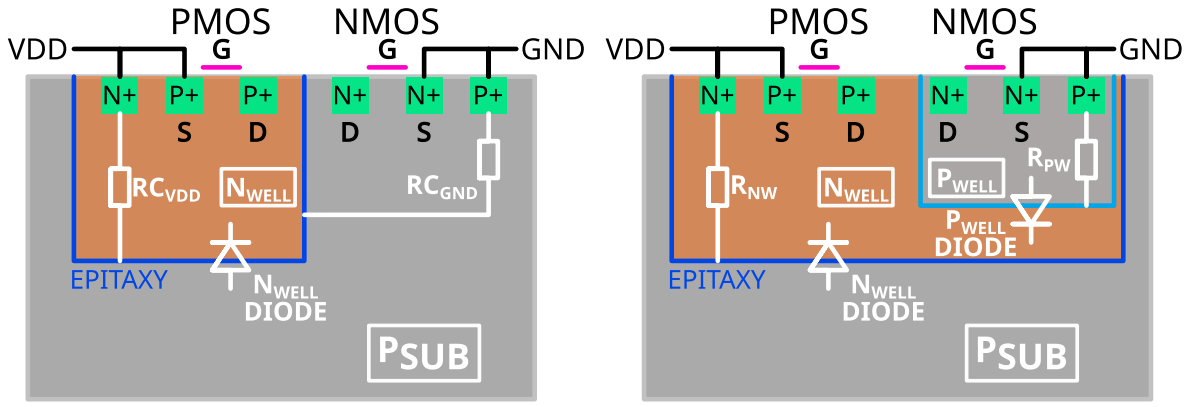
Body biasing injection being less documented than EMFI, no distributed model has yet been proposed to simulate ICs under BBI. In this context, our motivations were to set up and evaluate electrical models being able to reliably predict both in time and space IC behavior in order to understand how BBI induced disturbances propagate and create faults inside ICs. The current work main goal being to model and simulate BBI similarly to EMFI, we decided to start from the model proposed in [4], to improve and adapt it in order to be able to implement it in a BBI context.

This chapter begins with a general presentation of the enhanced models, followed by a closer look at each model and its specific features. Eventually, various model validation are studied in order to verify their soundness.

3.3 Electrical models COMPILATION DATE: 2023-07-19 13:44:45+02:00

sect:elecModels

On one hand, when performing EMFI (usually on the front side of the IC), air is the physical support to convey energy through electromagnetic waves. It is achieved



(a) *Dual-Well* `subfig:dualIvx` **(b)** *Triple-Well* `subfig:tripleIvx`

Figure 3.1: *Dual-well and triple-well inverter silicon sectional view.* `fig:dualTripleIvx`

by coupling the loop wire probe to the power delivery network loops. On the other hand, when working with BBI, the context is different. Indeed, the energy is conveyed through electrical charges through the silicon substrate. Therefore, the carriers have to go through the metallic probe and the whole substrate to reach the logic gates and the power delivery network in order to disturb the IC operation. Thus, the substrate type and design could have a significant impact on BBI efficiency. As a result, we explored and studied BBI in two specific scenarios depending on the substrate types: dual-well and triple-well. Fig. 3.1 shows the sectional views of two inverters manufactured in a dual-well and a triple-well substrate respectively. These simple schematics are helpful in understanding the reasoning behind the design of the electrical models.

Fig. 3.1a depicts the cross-sectional view of a dual-well CMOS inverter. The P-doped silicon substrate is colored in gray, with RC_{GND} being the access resistance from the epitaxy layer to the NMOS bulk. This physical environment is the conducting support of electrical charges which flow up to the NMOS transistor. The orange region is the N-doped silicon well, located inside the P-substrate to manufacture the PMOS transistors. RC_{VDD} is the access resistance from the epitaxy to the PMOS bulk inside the N_{WELL}. In addition to the P-substrate, the N-well is the last environment electrical charges have to go through before reaching the PMOS transistor.

Fig. 3.1b shows the cross-sectional view of a triple-well CMOS inverter. As before, gray areas represent P-doped silicon, and orange areas N-doped silicon. R_{NW} is the N_{WELL} access resistance from the epitaxy to the PMOS bulk, and R_{PW} is the P_{WELL} access resistance from the $N_{WELL} - P_{WELL}$ junction to the NMOS bulk. In this case,

two silicon junctions are present, represented by two independent diodes. In order to reach the PMOS transistors, charges have to go through the exact same environments as before. However, concerning NMOS transistors, they have to pass through two silicon junctions instead of none. As discussed in Chapter 5, this has a significant impact on BBI induced effects. However, these schematics are incomplete and do not allow simulating ICs behaviors under BBI.

Therefore, as it has been done in [4], ICs are spatially split in elementary sections called standard-cells segments (SCS). However, in addition to the improvement of the dual-well proposed model proposed in [4], we also introduce a triple-well model in order to fully appreciate the behavioral differences of BBI applied to both substrate types.

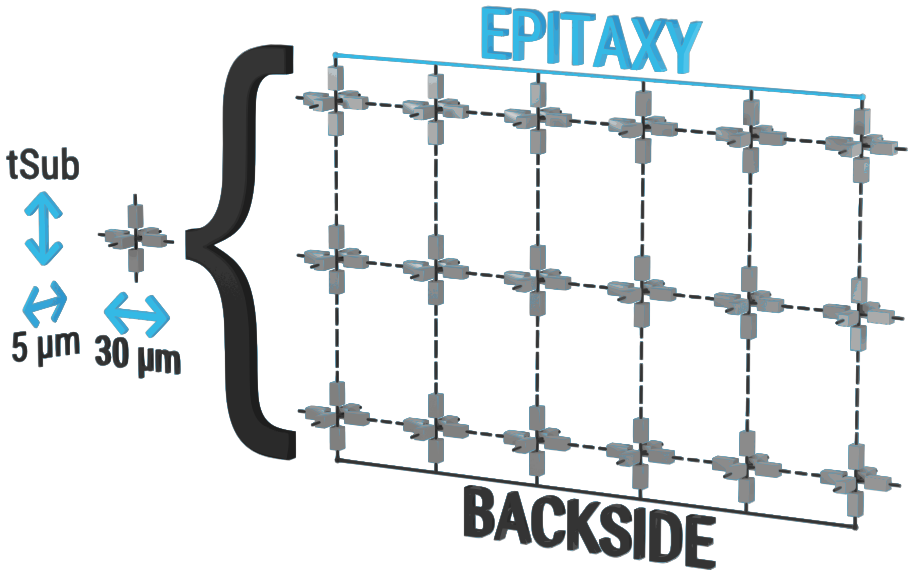
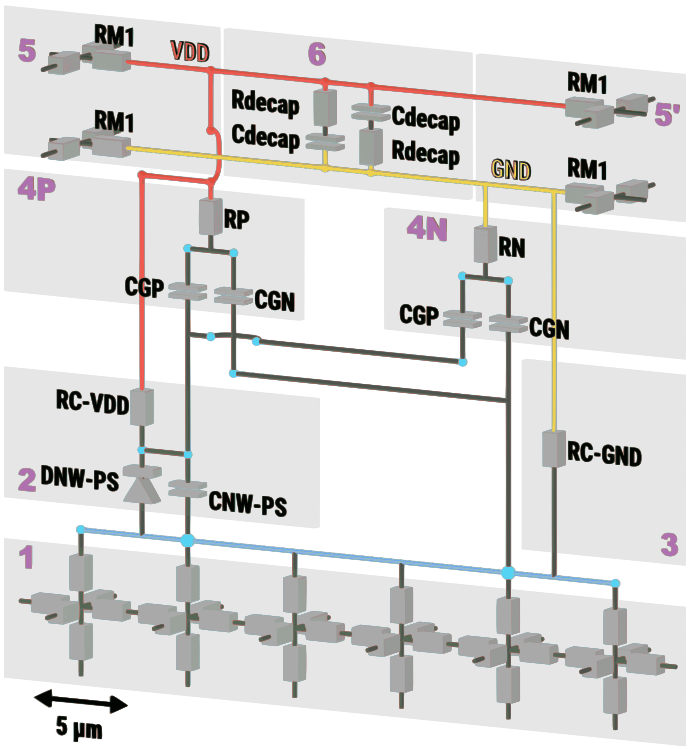
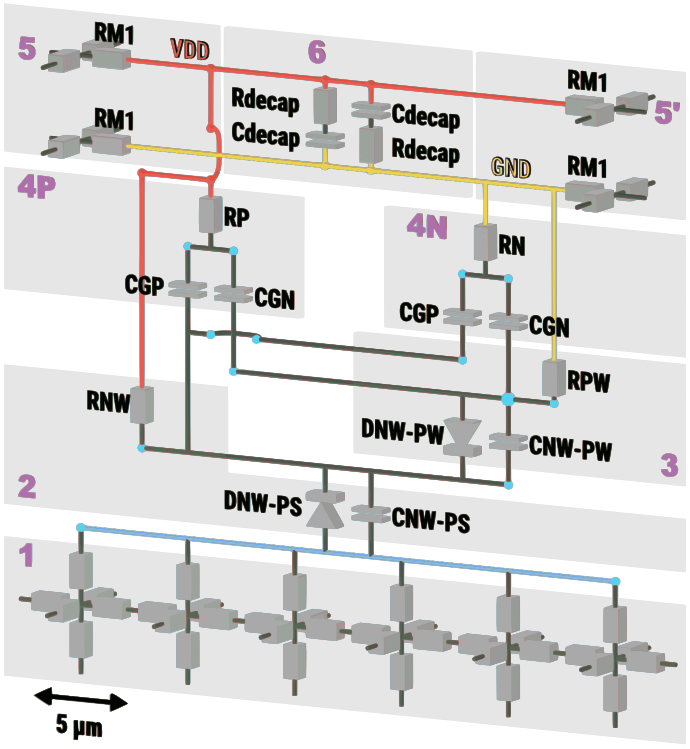


Figure 3.2: *Surface subdivision improvement.* `fig:surfaceSubDivid`

The main improvement over the dual-well model proposed in [4] concerns the substrate resistive network, as shown in Fig. 3.2. In [4], the substrate network is coarse and only consists of six electrical resistances for each SCS. It means that they represent the entire SCS substrate thickness, width, and height (on the left in Fig 3.2). Even though it is sufficient to appreciate the injection method effects while studying EMFI, mainly because the substrate is almost transparent when it comes to electromagnetic waves, but also because EMFI is mostly performed at the IC front side, it is not precise enough to model the spreading of he voltage pulse from the IC backside to the transistors.



(a) *Dual-Well* `subfig:dualScs`



(b) *Triple-Well* `subfig:tripleScs`

Figure 3.3: *Three-dimensional Dual-Well and Triple-Well IC comprehensive standard-cell electrical schematic.* `fig:dualTripleScs`

To that end, we decided to split as much as possible these resistors, as shown in Fig. 3.2, to provide a precise enough substrate sub-model while keeping realistic computational workload. For the final models, it was decided to use an editable elementary thickness of $10\ \mu m$, and fixed width and depth of $5\ \mu m$ for each elementary six-resistors substrate models, according to the footprint of an SCS on the XY plane ($5\ \mu m\ \times\ (6\ \mu m\ \times\ 5\ \mu m)$), resulting in a $30\ \mu m$ wide and $5\ \mu m$ deep SCS. One can remark that in Fig 3.3, no number is given concerning the substrate thickness, as similar to LFI, it is an important parameter which does not have a fixed value. Indeed, an attacker may want to thin the substrate or not before performing BBI.

Furthermore, as shown in Fig. 3.3, both SCS models contain various electrical components describing the IC structure, roughly composed of:

- Its substrate
- Its silicon junction(s)
- Its logic gates
- Its power supply rails

These two models, while being close to each other, allow, thanks to their subtle differences, to properly consider the different behaviors each substrate type exhibits. In the next section, dual-well SCS model and triple-well SCS model are consecutively considered and analyzed.

3.3.1 Standard-cell segment models COMPILATION DATE: 2023-07-19 13:44:45+02:00

`subSect:dualTripleWellScs`

Historically, IC substrate was manufactured using an exclusive dual-well structure. However, nowadays, it is common to find on relatively modern ICs a mix of dual-well and triple-well structures on a monolithic die. Triple-well substrate structures bring significant advantages over dual-well substrates. In digital ICs, it is mainly used to body bias transistors to optimize their performance under power constraints. When used in analog or mixed designs, it gives two main advantages: substrate cross-talk

and noise reduction, in addition to power supply decoupling thanks to the additional P-N junction capacitance [5]. This is why we decided to cover dual-well and triple-well structures in our models.

Fig. 3.3a depicts an SCS dual-well model. Each significant section of the SCS is gray-framed and numbered:

- The section 1 represents the substrate environment: resistive and isotropic.
- The section 2 is the $P - N$ silicon junction between the P-substrate and the N-well, represented by a diode and its junction capacitance, in addition to an access resistance $RC - VDD$, being the N-well electrical resistance.
- The section 3 is the substrate access resistance.
- The sections 4P and 4N contain the average non-logical model of a hundred of logic gates.
- The sections 5 and 5′ are the two levels of the power delivery network, which are low resistive metals.
- The section 6 is the decoupling between both GND and V_{DD} power networks.

Fig. 3.3b depicts the SCS triple-well model as follows:

- The section 2 is the $P - N$ silicon junction between the P-substrate and the N-well, represented by a diode and its junction capacitance, in addition to an access resistance R_{NW}, being the N-well electrical resistance.
- The section 3 is the $N - P$ silicon junction between the N-well and the P-well, represented once again by a diode and its junction capacitance, in addition to an access resistance R_{PW}, being the P-well electrical resistance.
- The sections 1, 4P, 4N, 5′ and 6 being the same as before.

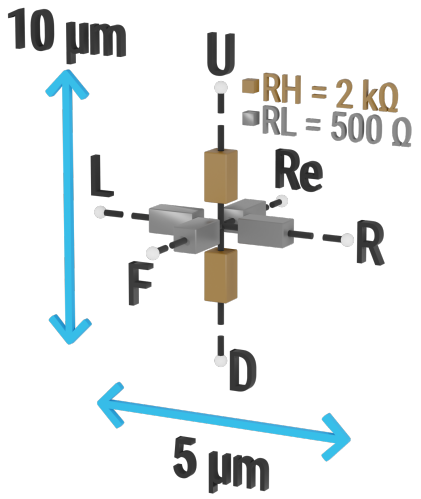


Figure 3.4: *Elementary substrate 3D netlist* fig:algo

```
.subckt elementary_bloc D F L R Re U
R1 U N001 RH
R2 N001 D RH
R3 Re N001 RL
R4 N001 F RL
R5 N001 L RL
R6 R N001 RL
.ends elementary_bloc
```

Figure 3.5: *Elementary substrate SPICE netlist* fig:subSpiceNetlist

```
.subckt elementary_blocx6 D1 D2 D3 D4 D5 D6
+F1 F2 F3 F4 F5 F6 L R RE1 RE2 RE3 RE4 RE5 RE6
+U1 U2 U3 U4 U5 U6 VSUBCintC
XX1 D1 F1 L VSUBCintL2 RE1 U1 elementary_bloc
XX2 D2 F2 VSUBCintL2 VSUBCintL1 RE2 U2 elementary_bloc
XX3 D3 F3 VSUBCintL1 VSUBCintC RE3 U3 elementary_bloc
XX4 D4 F4 VSUBCintC VSUBCintR1 RE4 U4 elementary_bloc
XX5 D5 F5 VSUBCintR1 VSUBCintR2 RE5 U5 elementary_bloc
XX6 D6 F6 VSUBCintR2 R RE6 U6 elementary_bloc
.ends elementary_blocx6
```

Figure 3.6: *SCS substrate layer SPICE netlist* fig:subSpiceSCS

Algorithm 1 Generation algorithm classes and function `alg:genFuncClass`

class NETLISTTEXTFILE ▷ Object defining the netlist to be generated

text: String content of the class

$write(value : String)$: Write characters into the parent class "**text**" attribute

end class

class DUALWELLSCS ▷ Dual-well standard-cell netlist

text: String content of the class

$read()$: Read characters into the parent class "**text**" attribute

end class

class TRIPLEWELLSCS ▷ Triple-well standard-cell netlist

text: String content of the class

$read()$: Read characters into the parent class "**text**" attribute

end class

function CREATENETS(X : float, Y : float, NET : String)

▷ Create nets to connect SCS together

$NetArray \leftarrow ???$

return NetArray

end function

function WRITEINMAINNETLIST(value : String)

▷ Write generated results into main netlist

NetlistTextFile.write(value)

end function

function SUBRHCALC(ESUB : int, RH : float, RL : float)

▷ Calculate elementary substrate resistors

$RH \leftarrow RH \times (ESUB \div 10)$

$RL \leftarrow RL \times (ESUB \div 10)$

return RH, RL

end function

function SCSELEMGEN(SUBTYPE) ▷ Generate Standard Cell Segment Model

Algorithm 2 Integrated circuit SPICE netlist generation algorithm. alg:icGen

Require: SUBTYPE ▷ IC substrate type: Dual-well, Triple-well, Mixed
Require: TSUB ▷ IC substrate thickness
Require: ESUB ▷ Elementary substrate block thickness
Require: VPUU ▷ Voltage pulse amplitude
Require: PW ▷ Voltage pulse width
Require: TFR ▷ Voltage pulse rise and fall times
Require: SIMTIME ▷ Simulation duration
Require: SIMSTEP ▷ Simulation time step
Require: TEX ▷ Desired X size (µm)
Require: TEY ▷ Desired Y size (µm)
$RH \leftarrow 2000$
$RL \leftarrow 500$
$nC \leftarrow TEX \div 30$ ▷ Number of column
$nL \leftarrow TEY \div 5$ ▷ Number of lines
$nH \leftarrow TSUB \div ESUB$ ▷ Number of substrate layers
Ensure: nC, nL and nH are integers
$RH, RL \leftarrow$ SUBRHCALC$(ESUB, RH, RL)$
for all cX in **do**
end for
TO FINISH.

Each area of the elementary SCS models were automatically generated using a custom algorithm, shown in Alg. 2. It was mainly designed in order to reduce as much as possible any human intervention to limit difficult to debug errors and inconsistencies. Ce qui suit doit être revu.In addition to that, it offers flexibility thanks to easy user modifications directly into the generation algorithm parameters instead of netlist editing, which further reduces errors. Furthermore, because these models only represent a section of an integrated circuit, it is required, in order to use and verify these models effectively, to replicate and interconnect them spatially as much as needed. This was achieved using custom Python scripts with procedural generation. The IC generation algorithm allows multiple settings to be modified in order to produce the

required results, while also having some intrinsic structural limitations. The two main limitations are the fixed width and depth of the elementary SCS models, and the fixed number of metal levels of the power delivery network. On the other hand, next is a non-exhaustive list of user modifiable settings:

- Global IC size.
- Probe position.
- IC global substrate thickness.
- IC elementary substrate thickness.
- Substrate type (dual-well, triple-well, or mixed).
- Voltage pulse amplitude.
- Voltage pulse width.
- Voltage pulse rise and fall times.
- Simulation time and step.

Eventually, the generator script incorporates a visual inspection tool in order to quickly verify the correctness of the generated netlist.

3.4 Preliminary model validation COMPILATION DATE: 2023-07-19 13:44:45+02:00

Because validating such models is a complex task, we chose to trim validation into elementary steps. As these models aim at modeling and report back average IC behaviors, it is required to verify their soundness in trivial scenarios. Specifically, two class of measurements are going to be discussed in this section:

- Global quiescent leakage current evaluation
- Quiescent power network IR drop verification

These are important parameters to verify before going any further because any inconsistent or unrealistic value would result in meaningless models and simulations.

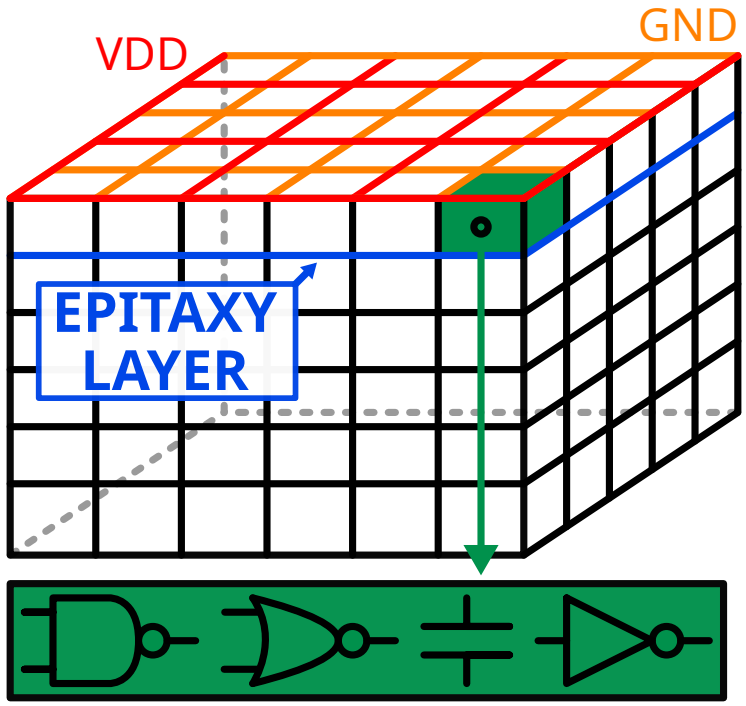


Figure 3.7: *Three-dimensional standard-cell segments interconnection example.* fig:surfaceSplitScs

To that end, we decided, as stated previously, to create an IC composed of several SCS. Fig. 3.7 depicts in a general way how the various SCS required are spatially connected to each other. In blue is indicated the epitaxy layer, which is the junction between the highest substrate level and the top of the SCS. All SCS share the power delivery network at their top and the silicon substrate at their bottom. As mentioned earlier, each SCS represent the average behavior of about a hundred of logic gates. The resulting IC measurements are the following: a width of $550\ \mu m$, a depth of $450\ \mu m$, and a thickness of $140\ \mu m$. First, we will present the global leakage current, then, we will analyze mappings of the simulated ICs power distribution networks. Dual-well, triple-well and mixed substrates models are analyzed, and most importantly, the simulated circuits do not include the voltage pulse generator nor any other external component required to work with BBI as what we present here is the first validation step. They are proposed as is, and Table 3.1 presents the operating point results for each substrate type.

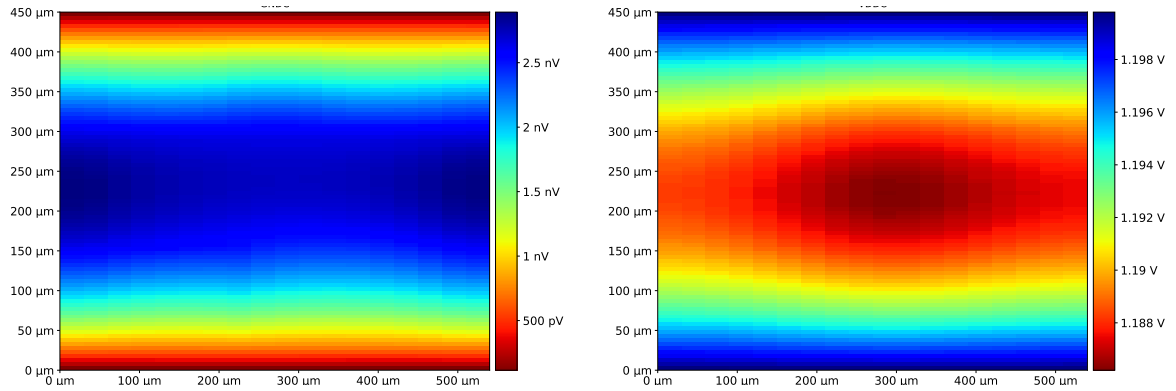
Looking at Table 3.1 indicates the absence of any significant leakage current and power supply voltage drop. However, to check the models relevance further and in a

Table 3.1: *Dual-well, triple-well and mixed substrates SCS operating point.*

tab:basicOpPointScs

Measurement	Description	Dual-well	Triple-well	Mixed substrates
I_{GND}	IC global ground current	1.92 nA	1.94 nA	3.4 nA
I_{VDD}	IC global VDD current	-1.96 nA	-5.8 nA	-3.5 nA
GND_{AVG}	Average GND voltage	1 nV	1 nV	1.75 nV
VDD_{AVG}	Average VDD Voltage	1.2 V	1.2 V	1.2 V

more reliable way, it is interesting to look at voltage mappings of the power delivery networks (VDD and GND), as shown in Fig. 3.8. Concerning both GND and VDD



(a) *GND* subfig:opMixedGnd **(b)** *VDD* subfig:opMixedVdd

Figure 3.8: *Mixed substrates operating point.* fig:opMixed

operating point maps, there is no significant voltage drop across both maps, which indicates further the absence of significant leakage current in the simulated IC. With this in mind, we then introduced the generator into the model.

3.5 Voltage pulse generator model and further validation

COMPILATION DATE: 2023-07-19 13:44:45+02:00

section:genModel

Introducing the generator did not come without major problems. Indeed, the latter inevitably interacts with the target IC, and depending on the real generator output stage architecture, this interaction can drastically vary from one to another.

For example, when using ESD guns as in [6, 7], their output stages are usually AC-coupled, while on our works, we mostly use DC-coupled generators. These subtle differences in practice become major issues in simulation when not treated correctly. Indeed, even considering the transmission line as it has been recommended in Chapter

2, most DC-coupled high voltage generators use a high-impedance mode to disconnect the load from the generator before and after the generated pulses. Therefore, one has to consider this specific aspect when designing a proper BBI electrical model, as we will explain in this section.

3.5.1 Early generator models COMPILATION DATE: 2023-07-19 13:44:45+02:00

subsection:earlyGenModel

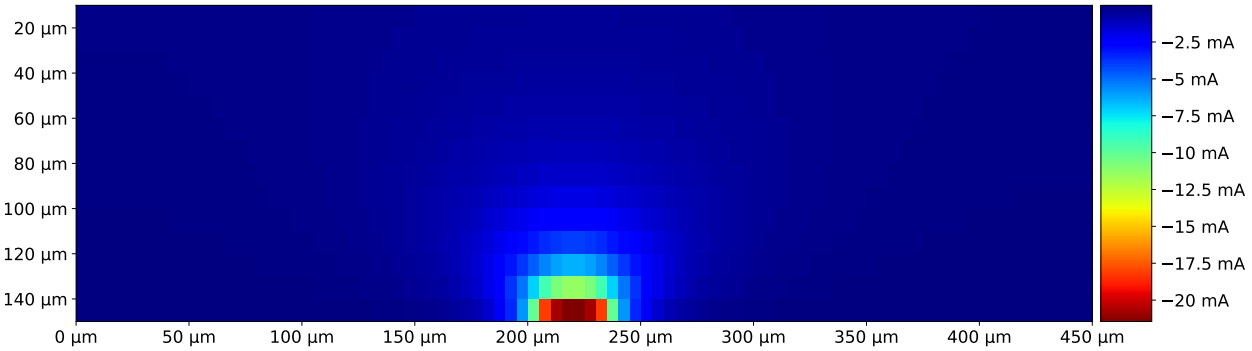
The first models consisted in a PWL voltage source directly connected to the substrate of the IC, and we quickly observed abnormal operating point values. Je dois rajouter des valeurs chiffrées. Indeed, in this setup, at rest, the generator is equivalent a DC voltage source applying 0 V to the backside of the simulated IC. Therefore, it applies an undesired bias to the substrate and thus changes the operating point, inducing a high amount of charges flowing between power sources, thus disturbing the power delivery network. To circumvent this issue, we chose to mimic the behavior of an actual high voltage pulse generator and to switch between a high impedance mode and a voltage pulse mode as a function of the pulse time. This allowed to observe correct operating points with the generator connected, as it is the case in a real experiment. Je rajouterai les figures.

3.5.2 Further generator models and verification COMPILATION DATE: 2023-07-19 13:44:45+02:00

subsection:furtherGenModel

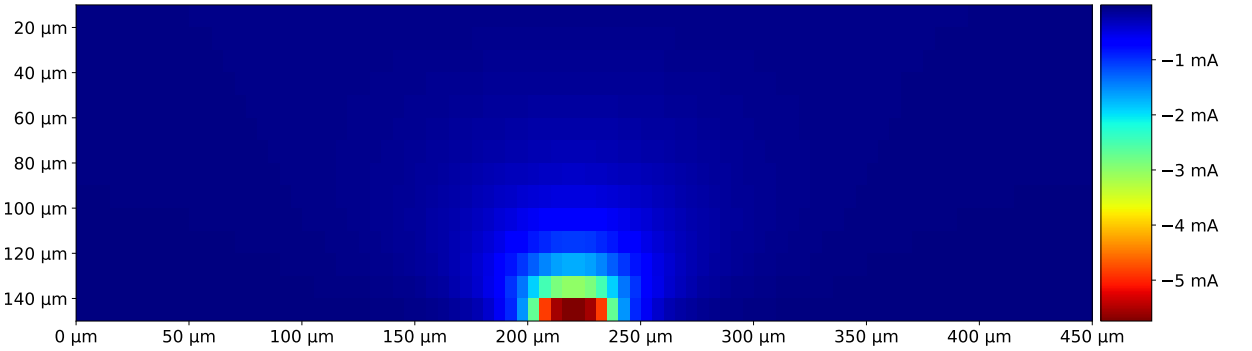
Because the previously explained generator model is electrically perfect and does not include any impedance mismatching effects, we extended the model to include the generator output impedance and the transmission line. Peut-être faire un schéma ? It allowed us to observe impedance mismatch effects, which are of great importance when performing BBI (Chapter 1), as the injected pulses are very fast and of high amplitude. Thus, impedance mismatch greatly changes the effective applied voltage pulse and injected currents, while also modifying unpredictably the induced disturbances, as we will observe further in this manuscript.

In order to verify more thoroughly the soundness of the proposed models, a circuit



(a) *Dual-well*

subfig:coupeCourantDw



(b) *Triple-well*

subfig:coupeCourantTw

Figure 3.9: *Dual-well and triple-well cross-sectional current distribution view at the apex of the voltage pulse*

fig:coupeCourantDwTw

under BBI is simulated in order to analyze the current distribution and amplitude, specifically at the peak of the voltage pulse. Fig. 3.9 presents the results for both dual-well and triple-well ICs. The substrate being a resistive environment, it is natural to observe isotropic hemispheric current distributions. However, it is interesting to notice that the results show a lower amount of current concerning the triple-well IC compared to the dual-well one. It can be explained thanks to the coupling between the probe/substrate and the logic gates. On one hand, as shown in Fig. 3.1, in the dual-well IC, the charges do not have to cross any silicon junction in order to reach the NMOS transistors, while there is one junction between the probe and the PMOS transistors. On the other hand, concerning the triple-well IC, there is always at least one silicon junction to cross in order to reach the transistors. Because of this, and because the voltage pulse will inevitably bias the diode, it will change the coupling whether the diode is conducting or blocking. When the diode is conducting, the transistors are DC-coupled to the probe, whereas when the diode is blocking, the transistors are AC-

coupled. In the second case, it means that charges can flow only on the edge of the pulse. Thus, during the pulse's plateau, there is no charge flow.

3.6 Experimental comparisons COMPILATION DATE: 2023-07-19 13:44:45+02:00

CREUSER PLUS EN DÉTAILS DANS LES SECTIONS PRÉCÉDENTES LES DIFFÉRENCES DUAL/TRIPLE, PARCE QUE C'EST IMPORTANT DANS LE MODÈLE ! In order to complete this chapter, we are going to analyze, in this last section, experimental results highlighting the differences between dual-well and triple-well substrates.

3.7 Conclusion COMPILATION DATE: 2023-07-19 13:44:45+02:00

In this chapter, we presented enhanced electrical models which can be utilized to simulate integrated circuits under body biasing fault injection. These models, supported by older ones originally designed for ICs under EMFI, cover two substrate types commonly found in commercial ICs: dual-well and triple-well substrates. The substrate type is of great importance when considering BBI as it is the only physical environment where charges can circulate. Each sub-models contain:

- The power delivery network
- The average electrical model of a hundred of logic gates
- The various silicon junctions
- The silicon substrate

Standard-cells segments models representing a portion of an IC, they need to be replicated and connected with each other in order to be meaningful. In addition to this, they propose refined substrate sub-models in order to improve the model spatial accuracy over their predecessors. The main advantage of these models is their relative lightness, computationally speaking. Indeed, they are only composed of passives

components, in order to be able to simulate large resulting ICs. However, their main advantage is also their main shortcoming, they do not represent any function of the modeled IC, but its average electrical behavior.

IV

Substrate thinning analysis COMPILATION DATE:

2023-07-19 13:44:45+02:00

chap:4thinning

Contents

4.1 Summary COMPILATION DATE: 2023-07-19 13:44:45+02:00

This chapter proposes to study the interests of thinning the substrate of integrated circuits with the aim to enhance Body Biasing Injection efficiency. First, we are going to present a geometrical approach in order to appreciate the effects of substrate thinning on ICs behaviors. Second, thanks to the models presented in Chapter 3, we are going to analyze theoretically the effects of substrate thinning. Eventually, in order to verify the soundness of the geometric approach and the simulation results, experiments are going to be studied thanks to the analysis of the same IC with different substrate thicknesses.

4.2 Introduction COMPILATION DATE: 2023-07-19 13:44:45+02:00

When working with integrated circuits in a fault injection context, several physical parameters of the considered IC are of great importance. For example, as we have seen in the previous Chapter, the type of substrate used to manufacture the IC has a significant impact on BBI efficiency and behavior. In addition to this, the transistor's size, power supply voltage, the IC package or the IC substrate thickness can drastically change fault injections results. Among these examples, one of great interest in this chapter is the substrate thickness.

Indeed, as there are different manufacturing processes depending on the purpose of ICs, it is common to find various substrate thicknesses depending on ICs targeted application. On one hand, it is not rare to find 700 µm thick wafers with 300 mm diameters for generic applications. On the other hand, in other specific applications like SoCs, where vertical stacking is commonly used, or in Smart-cards and ID cards, typical substrate thicknesses value are lower, around 200 µm. In addition to these differences one can find in commercial products, the practice of thinning the substrate of ICs is widespread in a context of fault injection. Specifically, substrate thinning has been widely studied concerning Laser Fault Injection (LFI) [8], and has proven to greatly enhance LFI efficiency in terms of fault creation, in addition to drastically reducing the power required to create faults. However, it had not been studied for Body Biasing Injection at the beginning of this work.

In this context, this work was first done in order to assess whether substrate thinning has similar effects as LFI. Second, because thin ICs commonly found in Smartcards have unavoidable security constraints, third because BBI is performed using the silicon substrate as the physical environment to carry energy through electrical charges. Therefore, this Chapter will evaluate the interests of substrate thinning on BBI efficiency. In other words, we will analyze the electrical and behavioral differences between identical ICs with different substrate thicknesses. This analysis will take place using multiple approaches. In the first place, we will address the question using a geometric approach to appreciate the effects of substrate thinning on voltage propagation inside the substrate. Then, the geometric approach will be completed with an electrical simulation analysis of two identical ICs with different substrate thickness thanks to the models proposed in Chapter 3. Eventually, experimental results will be analyzed in order to verify the correctness of the previous approaches, in addition to studying the actual effects of substrate thinning concerning faults creation.

4.3 Geometric and electrical modeling COMPILATION DATE: 2023-07-19 13:44:45+02:00

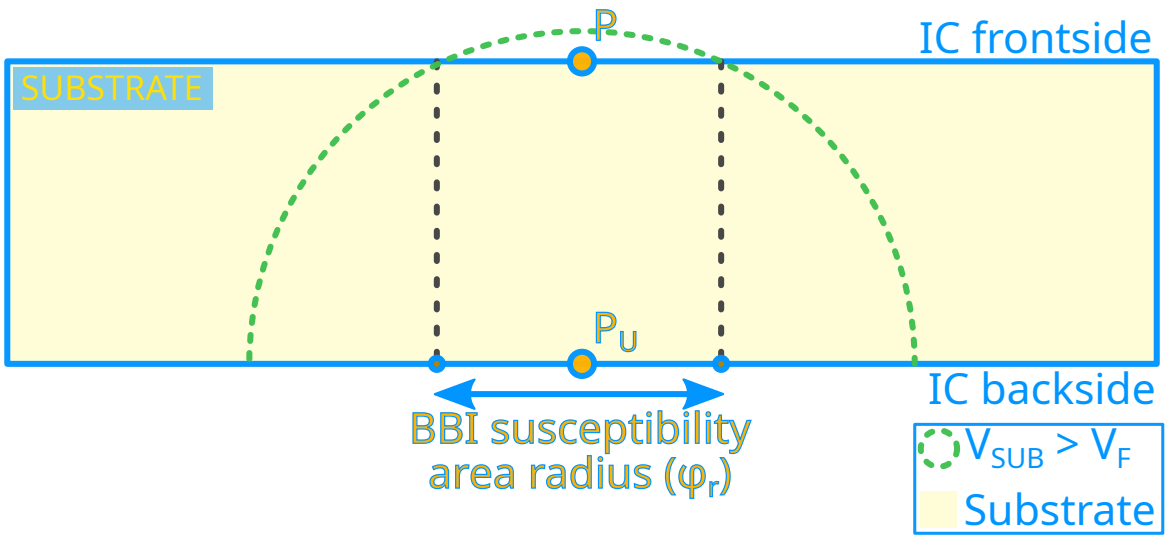
chap4:sect:geomModel

To begin with, we will address the geometric approach. It has been chosen thanks to the advantages it brings forward, such as the abstraction from electronics it enables, thus allowing easier and faster modeling. However, because this approach alone is insufficient, we will then study an analogous electrical one.

4.3.1 Geometric modeling COMPILATION DATE: 2023-07-19 13:44:45+02:00

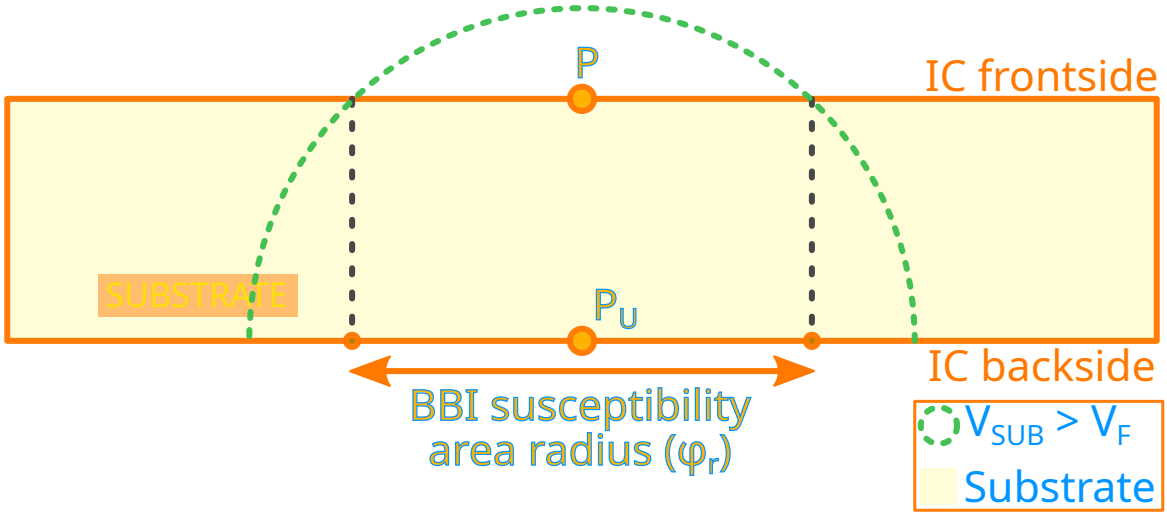
chap4:sect:geomModel:subsect:geomModel

For the purpose of geometric modeling, let us consider two identical ICs. A commercial one, with an arbitrary standard substrate thickness, and another one with its substrate thinned by a certain amount in order to perform fault injection. Fig. 4.1 illustrates the two-dimensional cross-sectional views of the considered ICs substrates during an arbitrary BBI voltage pulse. The silicon substrate being an isotropic resistive envi-



(a) *Normal IC*

fig:geomCrossView;subfig:geomThick



(b) *Thinned IC*

fig:geomCrossView;subfig:geomThin

Figure 4.1: *BBI susceptibility area cross-sectional 2D view.*

fig:geomCrossView

ronment, it is quite natural to expect the electrical charges to flow and spread evenly when injected into it at any given time. Therefore, equipotentials form half-sphere surfaces inside the substrate volume. These surfaces are highlighted in two-dimensions as green half-circles in Fig. 4.1.

In this scenario, an attacker wants to induce a fault in the logic gates, located at the top of each IC. To that end, they need to change the voltage enough at point P, called V_P, in order to disturb the transistors and change the logic gates behavior. In addition to that, and for the sake of simplicity, let us assume that P is the only location in the considered IC where faults can be injected. However, in order to observe faults at point

P, V_P needs to reach a minimal threshold voltage, called V_F. Because the attacker is working with BBI, a metallic probe is connected onto the backside of the IC, at point P_U, in order to inject energy into the IC. Depending on the amount of injected energy, in other words, the maximum amplitude of the voltage pulse because the substrate effective resistance is static, the voltage at P might never reach V_F, therefore, no faults will be observed. Let us consider that the attacker chose an amplitude V_{PU} big enough such that at a moment in the injection, V_P reaches V_F or more in each considered IC. In that scenario, the area on the IC front side where $V > V_F$ is a disk of radius ϕ, centered in P, called the BBI susceptibility area radius. It means that the attacker can position the probe anywhere on the backside within this disk to reach V_F at P, and therefore induce a fault at P.

The half-sphere equipotential radius relative to time can be determined thanks to the following formula:

$$r(t) = \frac{\rho_{SUB}}{\sqrt{2}} \cdot \frac{|I_G(t)|}{|V_{PU}(t) + V_F|} \tag{4.1}$$

with ρ_{SUB} the resistivity of the silicon substrate, $I_G(t)$ the instantaneous sum of the current distribution contained in the half-sphere, and $V_{PU}(t)$ the instantaneous voltage pulse applied on the backside of the IC. Then, logically, the BBI susceptibility area radius, denoted ϕ_r, is described by:

$$\phi_r(t) = 2 \cdot \sqrt{r(t)^2 - t_{SUB}^2} \tag{4.2}$$

with t_{SUB} being the IC substrate thickness.

As it is illustrated in Fig. 4.1, thinning the substrate inevitably increases the size of the susceptibility area if the experimental conditions are constant. It means that the susceptibility evolution ratio is always greater than 1 when thinning the substrate:

$$\frac{\phi_r^{THIN}}{\phi_r^{THICK}} = \sqrt{\frac{r^2 - t_{THIN}^2}{r^2 - t_{THICK}^2}} > 1 \tag{4.3}$$

Therefore, in order to obtain the same susceptibility area with a thinner IC, it is

required to reduce the voltage pulse amplitude, thanks to the following relation:

$$V_{PU}^{*} = \frac{t_{THIN}}{t_{THICK}} \cdot V_{PU} + V_F \cdot (1 - \frac{t_{THIN}}{t_{THICK}}) \quad (4.4)$$

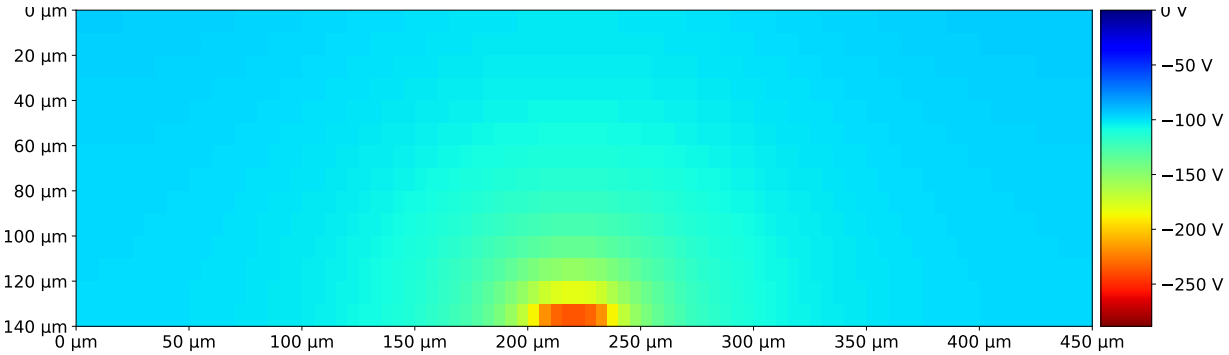
chap4:sect:geomModel:eqnVpu*

Eventually, this geometrical approach allows deducing three conclusions:

1. Thinning the substrate allows reducing the minimal voltage pulse amplitude required to induce a fault while keeping a constant susceptibility area.
2. The BBI susceptibility area increases while the substrate thickness decreases while working at a constant voltage pulse V_{PU}.
3. Thinning the substrate alone does not have an influence on BBI spatial resolution, as the susceptibility area depends on the couple (t_{SUB}, V_{PU}). Thus, similar spatial resolution could be obtained with different substrate thicknesses by changing V_{PU}.

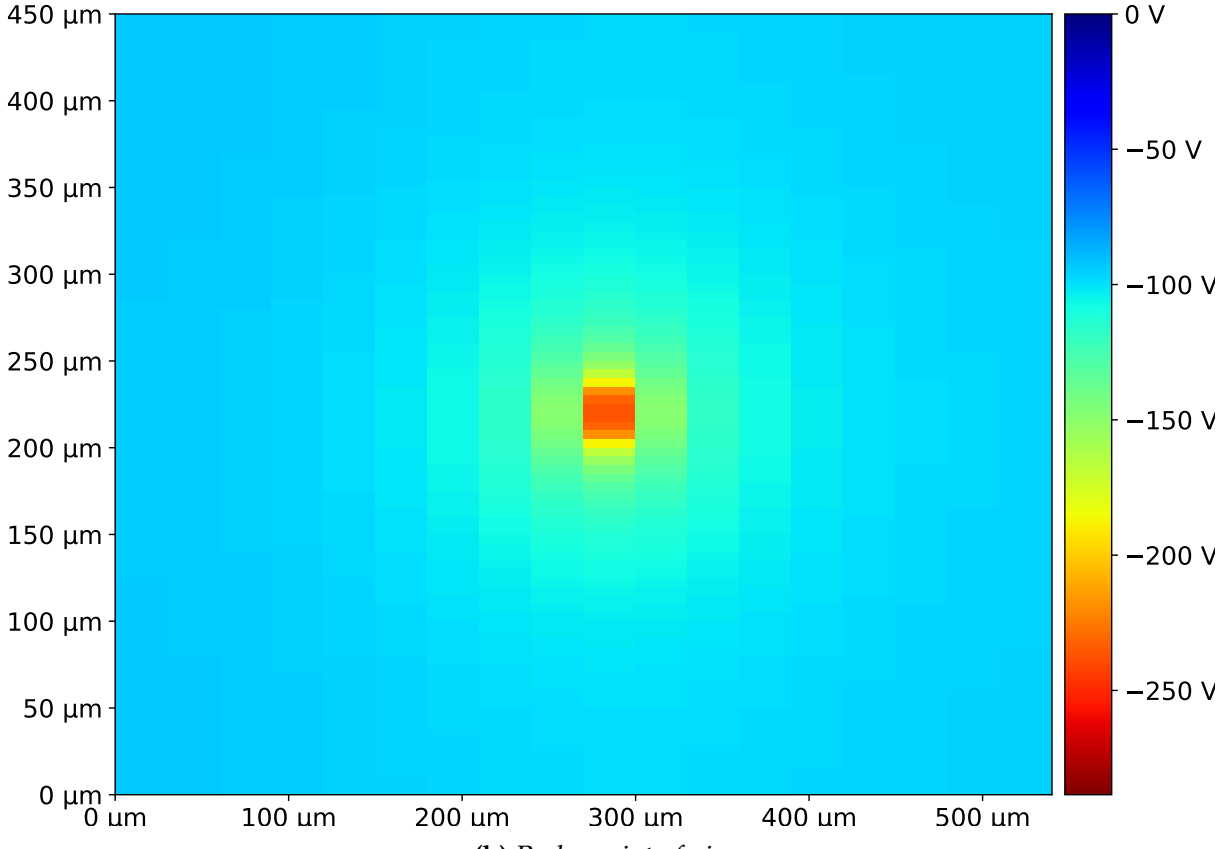
4.3.2 Electrical approach COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap4:sect:geomModel:subsect:elecApproach



(a) *Cross-sectional view (Y-axis)*

fig:simuSubCoupeThick;subfig:yaxis

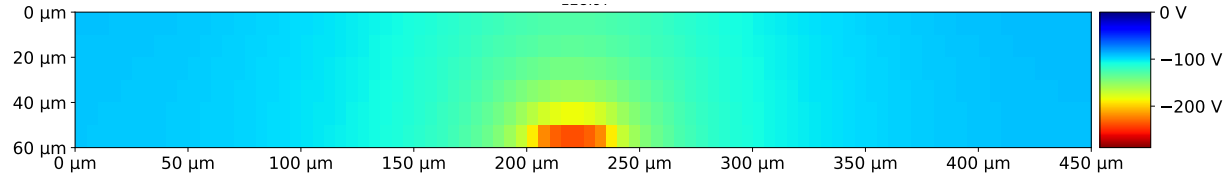


(b) *Probe point of view*

fig:simuSubCoupeThick;subfig:bottom

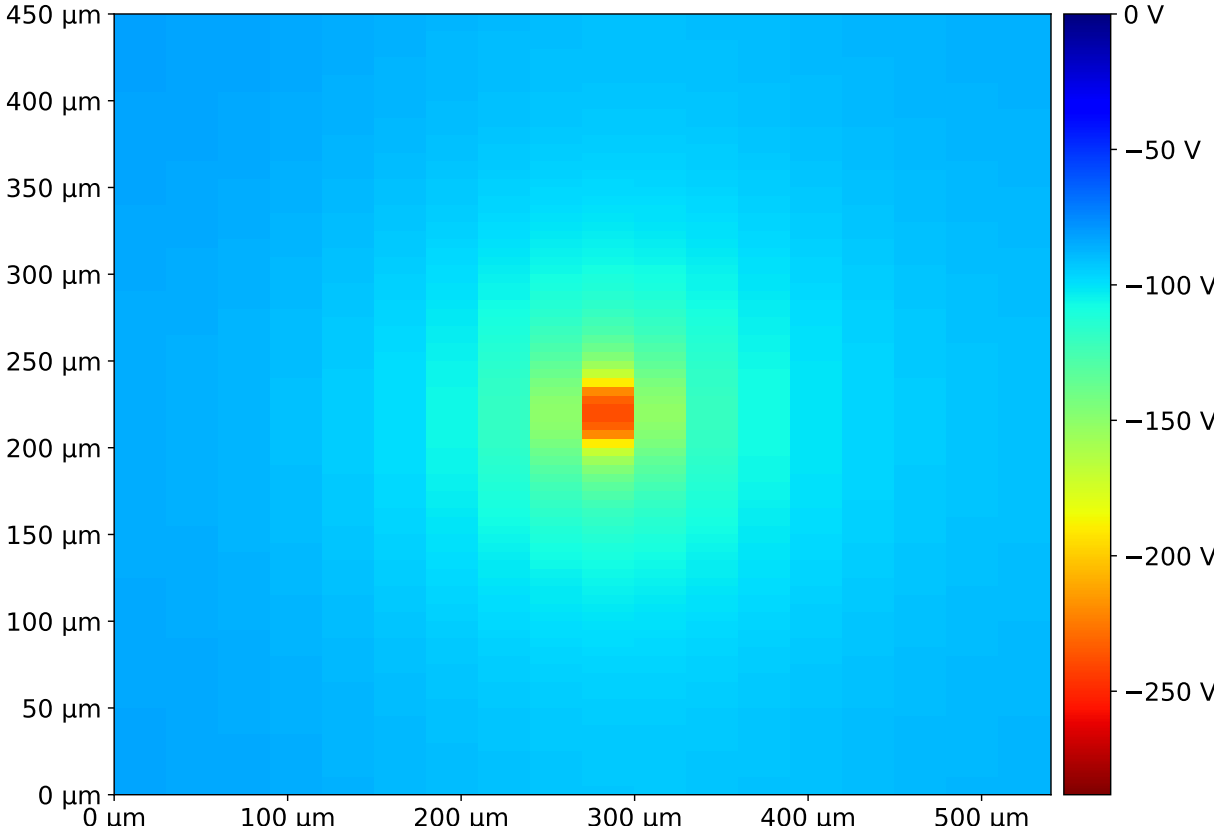
Figure 4.2: *Simulated non-thinned IC (140 µm) substrate voltage distribution: peak of the first voltage pulse edge*

fig:simuSubCoupeThick



(a) *Cross-sectional view (Y-axis)*

fig:simuSubCoupeThin;subfig:yaxis



(b) *Probe point of view*

fig:simuSubCoupeThin;subfig:bottom

Figure 4.3: *Simulated thinned IC (60 µm) substrate voltage distribution: peak of the first voltage pulse edge*

fig:simuSubCoupeThin

As stated previously, in order to verify the meaningfulness of the geometrical approach, we will complete it with an electrical modeling approach. For this purpose, the models introduced in Chapter 3 are reused. The electrical approach consists in generating ICs with different substrate thicknesses and simulating them during BBI. The considered ICs are 550 µm wide and 450 µm deep. Two substrate thicknesses are analyzed, 60 µm and 140 µm. The simulation parameters are the following:

- Triple-well substrate
- Required voltage pulse: -300 V
- Required pulse width: 20 ns

- Required rise and fall times: 8 ns

Fig. 4.2 and Fig. 4.3 show, for each simulated IC, the voltage bias across the substrate through different point of view at the apex of the voltage pulse first edge. For the sake of simplicity, results are shown in two dimensions and from two point of views. A cross-sectional view and a bottom view are displayed. The first interesting thing to note is that, as predicted thanks to the geometric model and as shown in Fig. 4.2 and 4.3, equipotentials effectively form half-circles (half-spheres in 3D). They can be observed thanks to both point of views. IL Y A BEAUCOUP DE CHOSES À DIRE MAIS JE MANQUE D'INSPIRATION POUR CETTE PARTIE, JE REVIENDRAI PLUS TARD DESSUS.

4.4 Models validation COMPILATION DATE: 2023-07-19 13:44:45+02:00

`chap4:sect:modelValid`

4.4.1 IC substrate thinning quick look COMPILATION DATE: 2023-07-19 13:44:45+02:00

`chap4:sect:modelValid:subsect:thinQuick`

As substrate thinning is quite widespread when performing fault injection, let us have a quick look on how it is performed. Commonly, It is done using Selected Area Preparation (SAP) or Focused Ion Beams (FIB) milling. SAP milling consists in a very precise mechanical milling tool, generally able to remove material with a precision down to a few micrometers. However, it can often lead to uneven surfaces. FIB milling consists in a physical milling which does not imply a mechanical contact with the material to be removed, and allows nanometer-level precision. For that purpose, FIB is commonly used in combination with SAP [9] to produce even substrate surfaces. In addition to substrate thinning, SAP milling machines allow removing the plastic package and eventual internal metallic heat-sinks of ICs prior to substrate thinning. It has the advantage of providing low damage to thinned ICs, thanks to low spindle speed and low temperature rise compared to traditional high speed milling.

4.4.2 Experiments with thinned circuits COMPILATION DATE: 2023-07-19 13:44:45+02:00

chap4:sect:modelValid:subsect:XPthinning

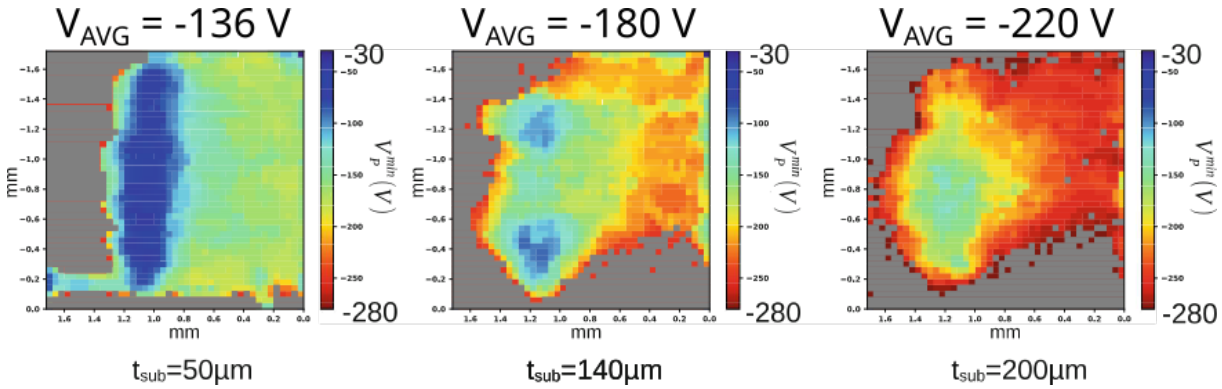


Figure 4.4: *Fault susceptibility maps*

fig:fsm1

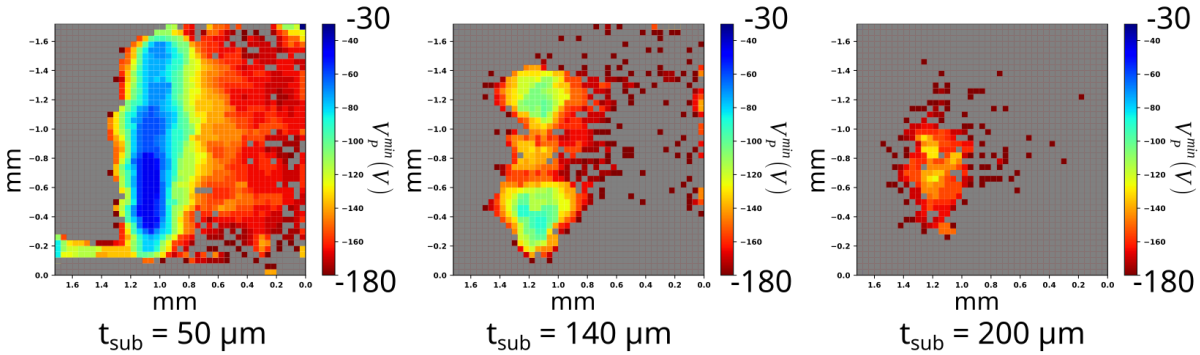


Figure 4.5: *Susceptibility area spreading*

fig:fsm1spread

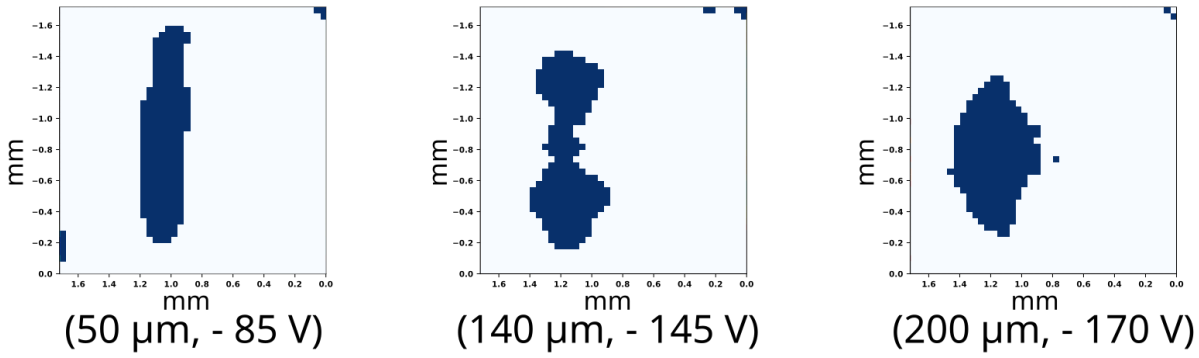


Figure 4.6: *Fault susceptibility maps couples*

fig:fsm1couple

With geometric and electrical modeling complete, it is now possible to conduct actual experiments in order to verify the meaningfulness of the previous approaches. In this context, three an STM32F439VIT6 LQFP100 identical targets were thinned to three different levels, from 750 µm to respectively 200 µm, 140 µm and 50 µm, respectively named ST200, ST140 and ST50 for the rest of this Chapter. In order to verify the three

conclusions extracted from the modeling section, three experiments are conducted for each target.

The first experiment aims at measuring the minimal voltage pulse amplitude V_{PU}^{MIN} required to induce a faulty behavior on an IC performing computations. These experiments are called Fault Susceptibility Maps (FSM). They allow spotting the region where the IC is sensitive to BBI, no matter which type of induced fault. Therefore, when mapping an entire IC, it is common to spot various areas not directly involved in the targeted calculation, like the analog voltage regulator or the FLASH memory logic control logic not to cite them all. As a result, and because in a fault injection context the cryptographic core is very often targeted, it was decided to focus the maps above the STM32 AES core only. Fig. 4.4 presents the three performed FSM. From left to right, t_{SUB} goes from 50 µm, then to 140 µm, finally to 200 µm. As stated before, the maps are performed above the hardware AES core of the IC, temporally aiming the penultimate AES round. The scanned area measures 1.7 mm by 1.7 mm, with a displacement step of 40 µm between each point. V_{PU} was limited to the following range: [30 V ; 280 V], with 5 V steps and a negative polarity. The pulse width was fixed at 6 ns. The first important thing to note here is that, as predicted with the geometric and electrical modelings, a thinner substrate allows a lower fault induction threshold. It is mainly shown thanks to the measurement of the average voltage required to induce a fault across the entire map, annotated at the top of each map. All of this sustains the first conclusion made in section 4.3.

Then, the second experiment, whose results are shown in Fig. 4.5, consist in analyzing the spreading of the BBI susceptibility area. The core of the experiment is identical as before. However, in order to highlight the spreading effect, it was required to set a lower maximum voltage amplitude (in absolute value). The value of 180 V was chosen as it is the average voltage of the medium-thinned IC. What is interesting here is that, for the ST200 target, because the voltage at the epitaxy level cannot reach the threshold value V_F in most cases, the fault area is tiny compared to the other targets, and focused on the AES core. Then, concerning the ST140 target, thanks to the thinner substrate, the voltage at the epitaxy level can reach a higher value, and thus can cause more logic gates or further logic gates from the probe to have a faulty behavior. Eventually, the

ST50 target shows the largest fault area. These experiments help to sustain the second conclusion of section 4.3.

Eventually, the last experiment consisted in finding, whenever possible, (t_{SUB}, V_{PU}) couples for which the susceptibility area is identical across all targets. The search for the couples of values was done by first choosing an arbitrary couple for ST200 target, and then calculating the correlation for each couple between the other two susceptibility areas and finding the highest correlation. Then, to confront the geometric modeling predictions, we calculated, thanks to equation 4.4, couples corresponding to

4.5 Conclusion COMPILATION DATE: 2023-07-19 13:44:45+02:00

This chapter introduced the interest of thinning the substrate of integrated circuits on Body Biasing Injection efficiency. In the first place, we studied thanks to a geometrical approach the potential benefits of this practice, further completed with electrical simulations. The geometric approach brought mathematical relations allowing to evaluate preliminary the effects of thinning the substrate of a target IC.

À FINIR.

V

Fault model

chap:5faultModel

Contents

5.1 Summary

chap5:sect:summary

This last chapter introduces a fault model for BBI, explaining how and why faults occur in ICs subject to body biasing injection. Thanks to the electrical models proposed in Chapter 3 and to further logic gates simulation, it is possible to present a physical understanding of fault creation.

5.2 Introduction

chap5:sect:intro

To further complete the understanding of BBI, in addition to having a reliable model to predict IC behavior, it is of great importance of having a precise fault model, in order to be able to set up countermeasures. Indeed, the main objective of studying fault injection techniques is to protect secured ICs. As it has been said in Chapter 3, simulating at a transistor level an entire IC is unrealistic computationally speaking. Therefore, and because the previous models do not represent the logical functions of ICs, we propose an additional step to the simulation workflow proposed in Chapter 3. It allows appreciating logic gates behavior under BBI disturbances in order to get a deeper and more precise understanding of both electrical and functional fault creation.

5.3 Charge extortion

chap5:sect:chargeExtortion

5.3.1 Logic considerations

chap5:sect:chargeExtortion:subsect:logicConsiderations

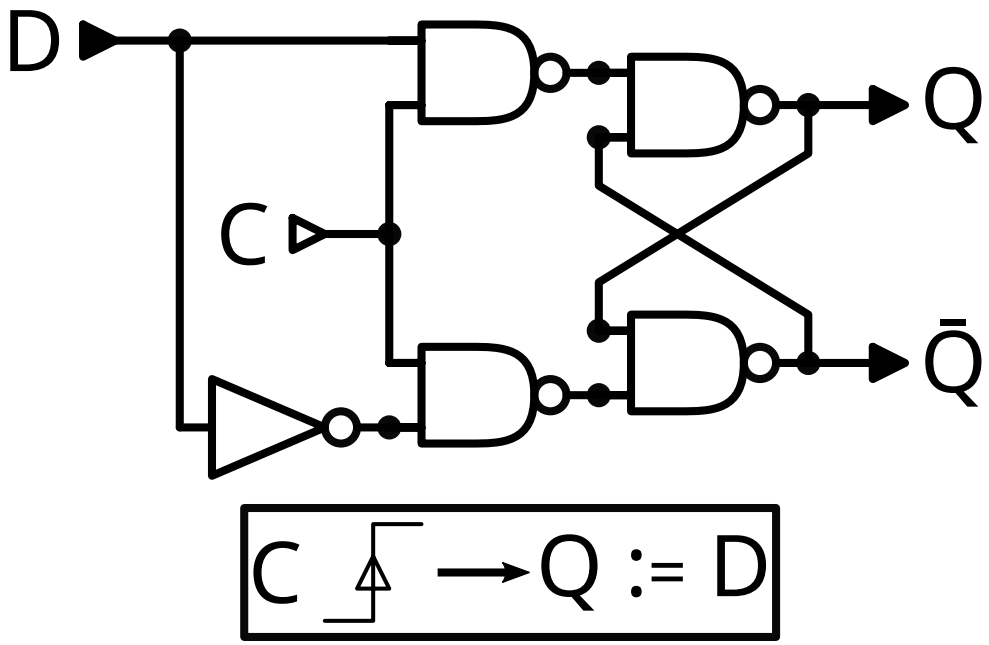


Figure 5.1: *D Flip-Flop logic schematic* chap:5;fig:dffLogic

In order to understand electrically why faults occur, it is important to begin with logic considerations. Nowadays, the vast majority of commercial ICs are sequential. The main building block of a sequential IC is the Edge-Triggered D Flip-Flop (DFF). Fig. 5.1 presents the logic schematic of a DFF. Because DFFs work on clock edges, it is interesting to target them at specific times when performing fault injection. Paragraphe à terminer, compléTer, revoir... This fault model has been proposed in [10] for EMFI.

Parler du fait que les circuits séquentiels échantillonnent périodiquement les valeurs des DFFs (registres). Du coup, si on change un niveau logique suffisamment longtemps pour qu'il perdure pendant l'échantillonnage, c'est gagné ! Faute !, sinon Non.

5.3.2 Charge extortion

chap5:sect:chargeExtortion:subsect:chargeExtortion

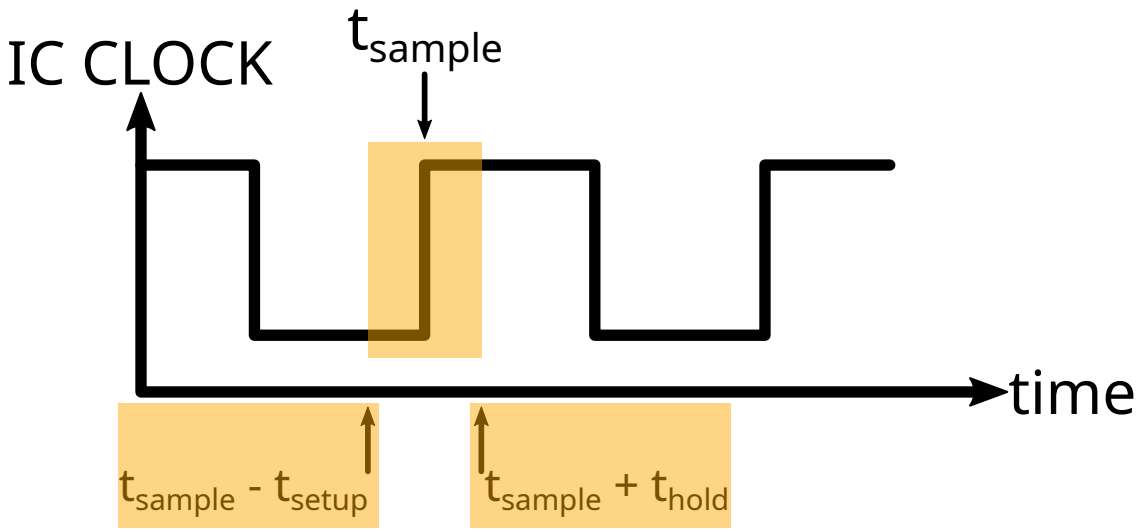


Figure 5.2: *BBI sampling fault susceptibility* chap:5;fig:bbiSusc

With the previous fault model in mind, let's have deeper look at it. Fig. 5.2 presents the sampling fault model we are going to discuss. It states that to maximize fault creation, faults have to be injected during a specific period of time. It is precisely located before and after every clock rising edge.

VI

Conclusion

chap:6conclusion

Bibliography

[1] 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. 10

[2] G. Chancel, Jean-Marc Gallière, and P. Maurine. Body biasing injection: Impact of substrate types on the induced disturbances$f$. In *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 50–60, 2022. 10

[3] 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. 10

[4] 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. 10, 11, 13

[5] Yasuhiro Ogasahara, Masanori Hashimoto, Toshiki Kanamoto, and Takao Onoye. Supply noise suppression by triple-well structure. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 21(4):781–785, 2013. 16

[6] 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. 23

[7] 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. 23

[8] Breier et al. Extensive laser fault injection profiling of 65 nm fpga. *J Hardw Syst Secur 1*, pages 237–251, 2017. 30

[9] C. Boit, R. Schlangen, A. Glowacki, U. Kindereit, T. Kiyan, U. Kerst, T. Lundquist, S. Kasapi, and H. Suzuki. Physical ic debug and - backside approach and nanoscale challenge. *Advances in Radio Science*, 6:265–272, 2008. 37

[10] S. Ordas, L. Guillaume-Sage, and P. Maurine. Electromagnetic fault injection: the curse of flip-flops. *Journal of Cryptographic Engineering*, 7(3):183–197, Sep 2017. 43