# Body biasing fault injection: Enhancements, analysis, modeling, and simulation

PhD thesis defense

**Geoffrey Chancel** Jean-Marc Gallière Philippe Maurine

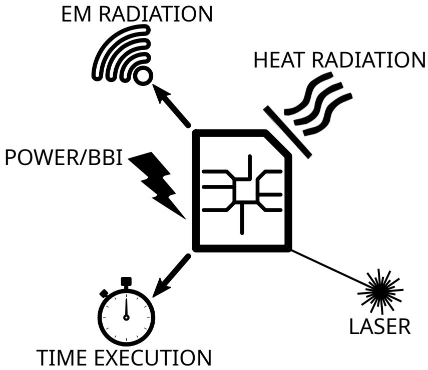
2024/01/29

Jean-Luc Danger Giorgio Di Natale Pascal Nouet Jean-Max Dutertre

# INTRODUCTION

# Context: hardware security

- Electronics are found in every economic sector;
- In IoT, CPS, debit cards, phones, bank systems;
- They embed cryptographic algorithms to ensure security;
- These algorithms are fallible, they leak data and can be disturbed.




Side-channel and fault injection.

# Fault injection attacks

Fault injection objectives:

- Denial of service (DoS) $\rightarrow$ Inject faults causing the circuit to stop;
- Verification bypass $\rightarrow$ Inject transient faults modifying data on the fly;
- Confidential data extraction $\rightarrow$ Inject transient faults at specific times.

Thanks to a fault injection platform:

- Power Glitch Fault Injection (PW-GFI);
- Clock Glitch Fault Injection (CK-GFI);
- Laser Fault Injection (LFI);
- Electromagnetic Fault Injection (EMFI);
- Body Biasing Fault Injection (BBI).

# Body biasing injection: state-of-the-art

Limited information in the literature at the beginning of my thesis:

- Philippe Maurine et al. Yet another fault injection technique : by forward body biasing injection;
- K. Tobich et al. Voltage spikes on the substrate to obtain timing faults;
- Noemie Beringuier-Boher et al. Body biasing injection attacks in practice.

A few days after the beginning:

- Colin O'Flynn. Low-cost body biasing injection (BBI) attacks on WLCSP devices.

# Body biasing injection: industrial and academic platforms

Langer EMV-Technik GmbH BBI platform

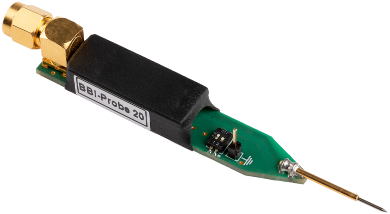
- All-in-one platform;
- A power supply and controller combo called "Burst Power Station";
- An active BBI probe: a current pulse generator, as shown on the right.


Active BBI probe by Langer EMV-Technik GmbH.

# Body biasing injection: industrial and academic platforms

Riscure BV BBI platform:

- All-in-one platform;
- A pulse generator;
- A BBI probe, as shown on the right.

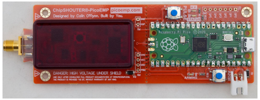



BBI probe proposed by Riscure BV.

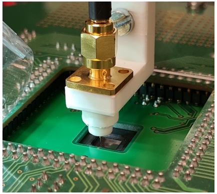
# Body biasing injection: industrial and academic platforms

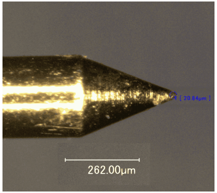
NewAE Technology Inc. BBI platform

- Combined EMFI/BBI pulse generator;




# Body biasing injection: LIRMM BBI platform







- Custom BBI probe;
  - Spring-loaded metal probe;
  - Custom 3D printed housing;
  - SMA connector;
- AVTECH AVRK-4-B high voltage pulse generator.

# Body Biasing Injection: thesis objectives

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

# Thesis agenda

- Body Biasing Injection platform enhancements;
- Integrated circuits modeling for BBI;
- Enhanced simulation flow;
- Substrate thinning analysis in a BBI context.
- Conclusion and perspectives

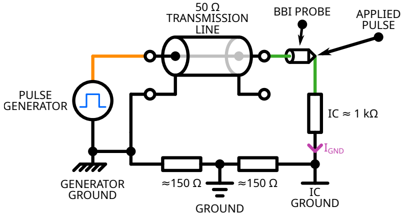
# BODY BIASING INJECTION PLATFORM ENHANCEMENTS

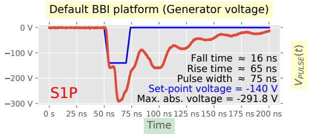
# Typical BBI platform

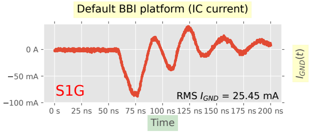
- BBI introduced to perform Bellcore attack;
- Demanding fault attacks difficult or impossible to perform;
- Low experiment repeatability.

## What are the limiting factors?

# Typical BBI platform

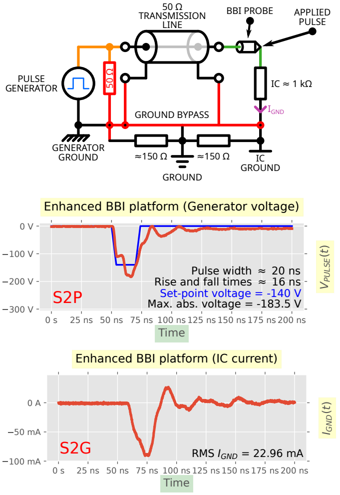


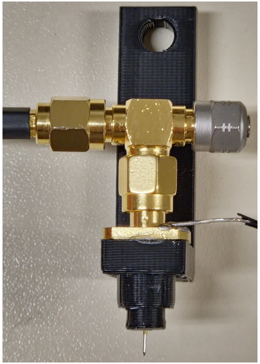




- Impedance mismatch;
- Floating grounds;
- Ringing;
- Set-point error.

# Enhanced BBI platform

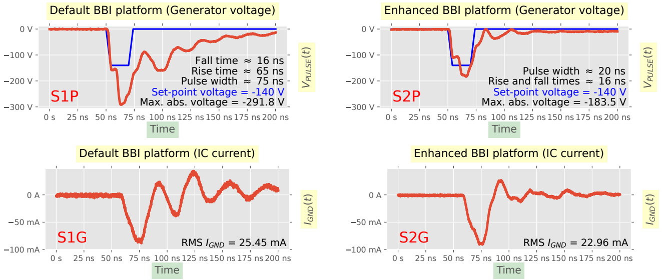






# Enhanced BBI platform

## Summary




Default platform:

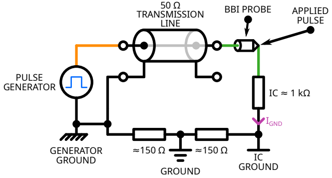
- -108 % pulse undershoot;
- 275 % pulse width overshoot;
- Obvious ringing.

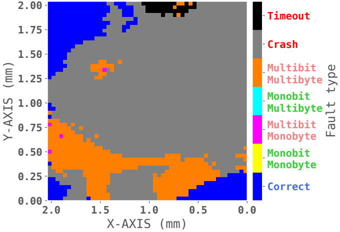
Enhanced platform:

- -31 % undershoot;
- Matched pulse width;
- Less ringing.

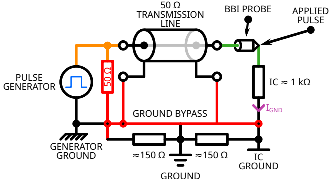
# Enhanced BBI platform benefits

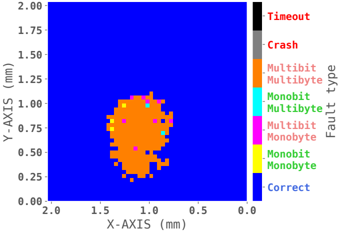
## Giraud's single bit fault attack




Unsuccessful Giraud's DFA




Successful Giraud's DFA

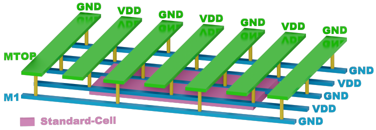
# Giraud's single bit fault attack

## Results

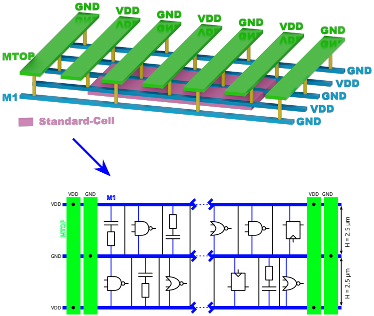
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K10 | 0xFF | 0x1F | 0x42 | 0xE8 | 0xEF | 0x44 | 0xA5 | 0x6A | 0xCA | 0xE7 | 0x55 | 0x3C | 0xFD | 0x65 | 0x39 | 0x26 |
| KEY | 0x01 | 0x23 | 0x45 | 0x67 | 0x89 | 0xAB | 0xCD | 0xEF | 0xDE | 0xAD | 0xBE | 0xEF | 0x12 | 0x34 | 0x43 | 0x21 |

- 14 bytes out of 16 found thanks to the Giraud's DFA;
- 2 remaining bytes found thanks to brute force.

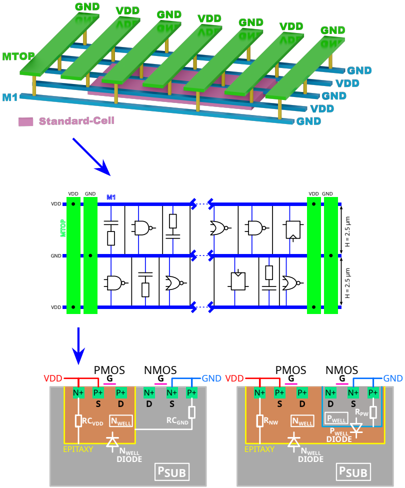
# Simulation models



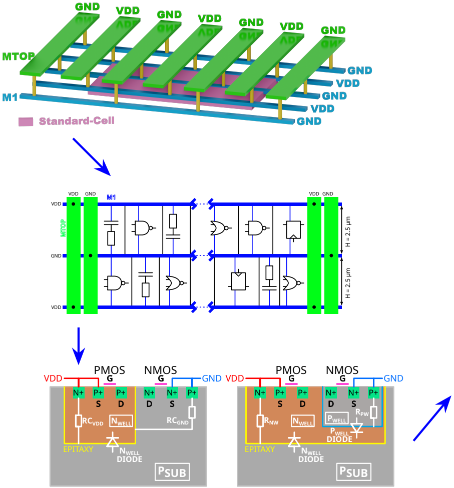
# Simulation models

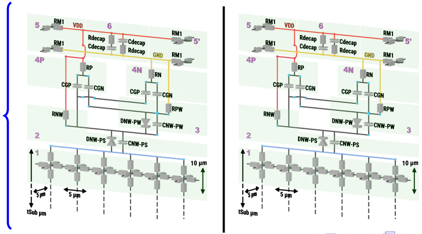


# Simulation models

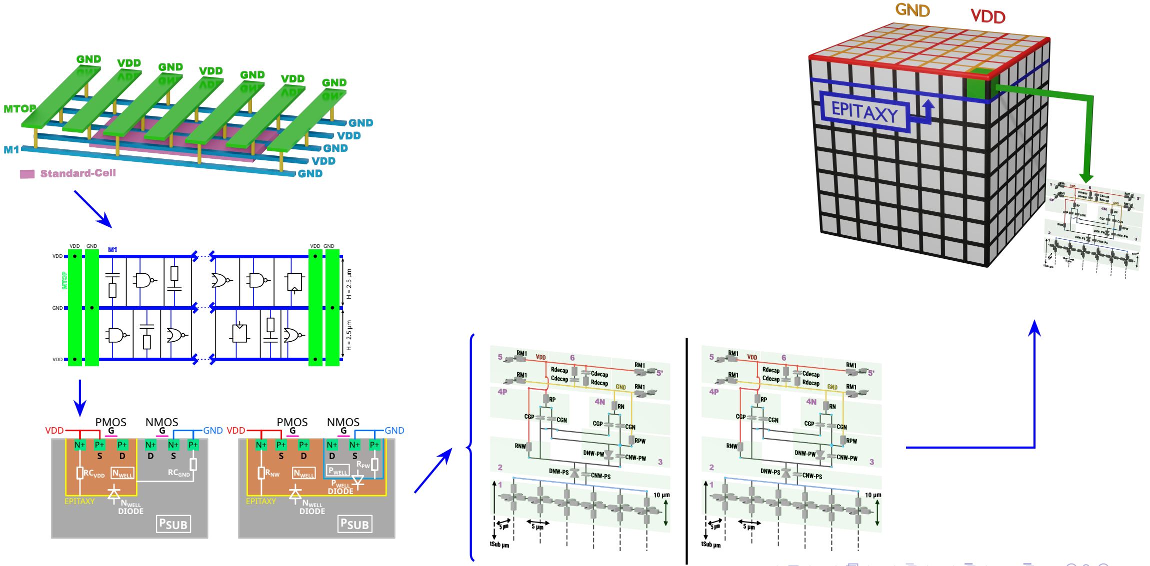


# Simulation models

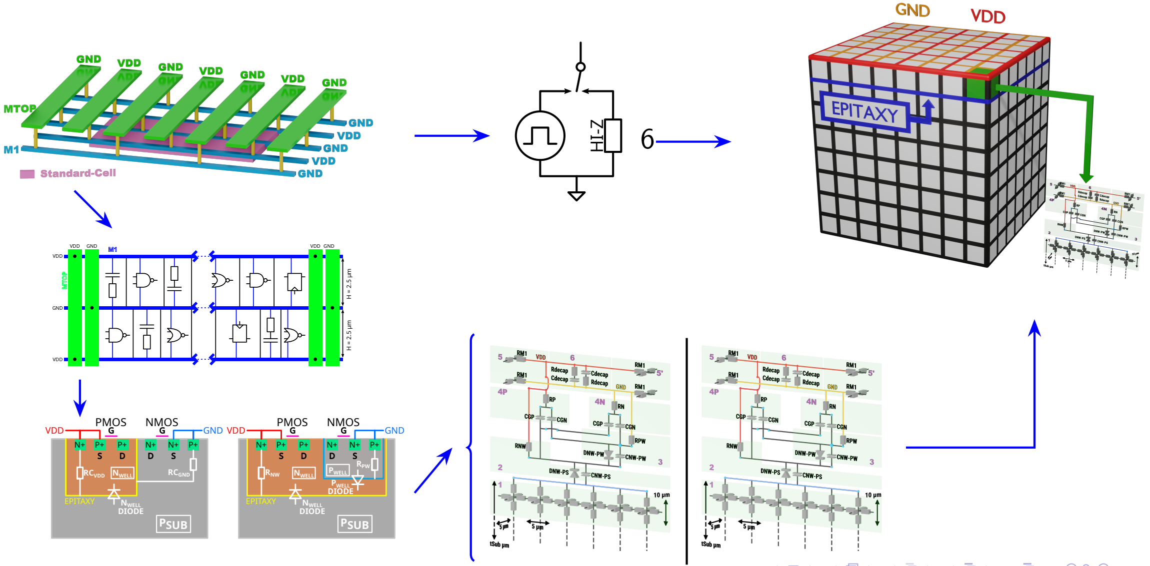


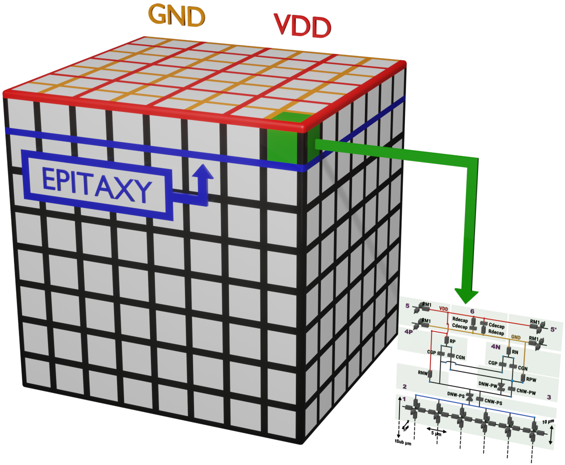
# Simulation models



# Simulation models



# Simulation models



# SIMULATION RESULTS

# Simulation results

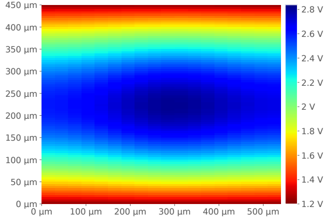
What we observe:

- Dual-well;
- Triple-well;
- Picture at the apex of the pulse;
- 550 $\mu m$ $(W)$ $\times$ 450 $\mu m$ $(D)$ $\times$ 140 $\mu m$ $(T)$: integrated circuit $\rightarrow$ 1620 SCS;

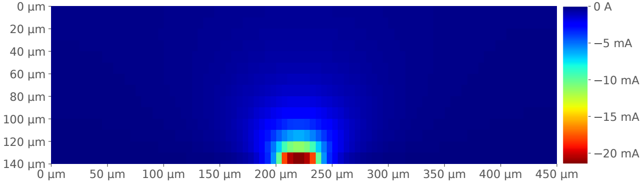
Simulation conditions:

- Voltage pulse amplitude: -300 V;
- Voltage pulse width: 20 ns;
- Rise and fall times: 8 ns;
- Approximate impedance matching.

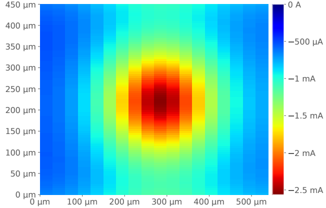
# Simulation results: Dual-Well



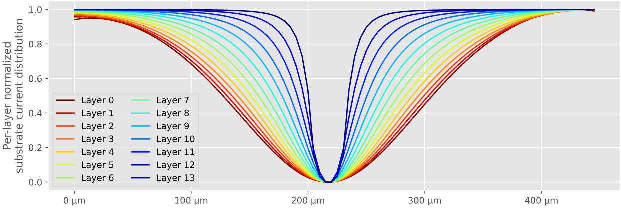

PS voltage distribution




Substrate current distribution

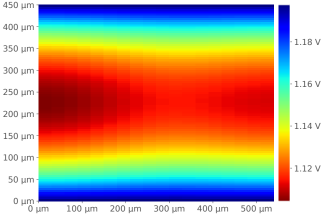



Epitaxy current distribution

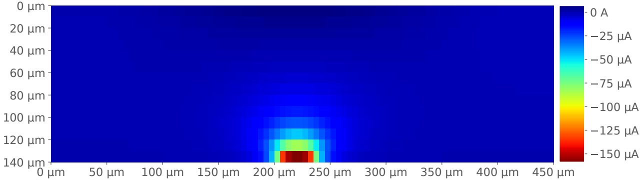



Per-layer normalized substrate current density

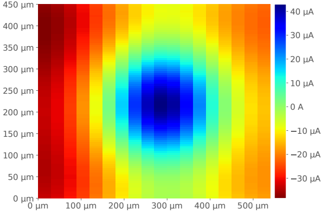
# Simulation results: Triple-Well



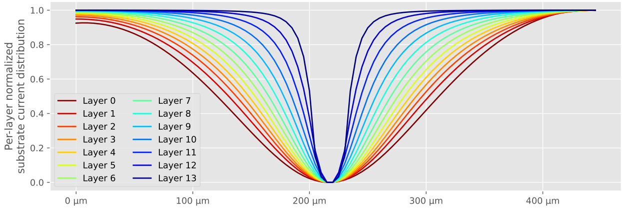

PS voltage distribution




Substrate current distribution




Epitaxy current distribution




Per-layer normalized substrate current density

# Dual-well vs Triple-well

Differences between Dual-well and Triple-well circuits:

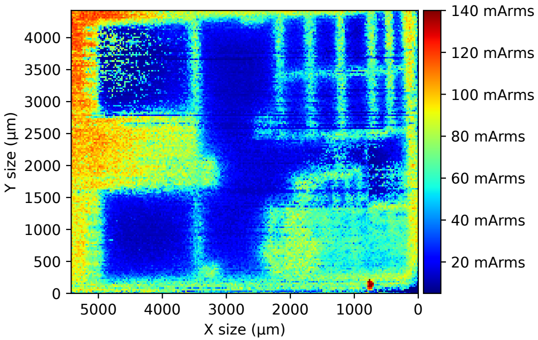
- Dual-well → NMOS are DC-coupled — PMOS are AC-coupled;
- Triple-well → entire IC is AC-coupled.

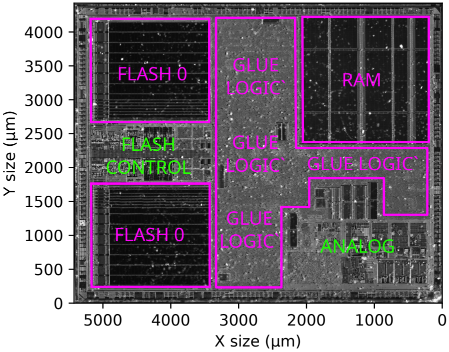
Implications:

- Dual-well → continuous energy flow during the pulse;
- Triple-well → energy flow confined to the pulse edges;

**For a given amount of time → less energy injected into TW compared to DW**
**→ less RMS current into TW compared to DW**

# Dual-Well and Triple-well ICs in practice



# SIMULATION FLOW FOLLOW-UP: HOW FAULTS OCCUR?

# SCS incomplete models: how faults occur?

To understand how faults occur

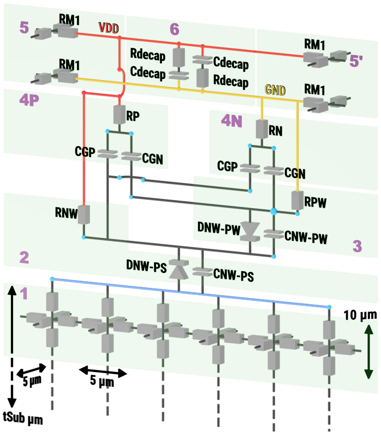
# SCS incomplete models: how faults occur?

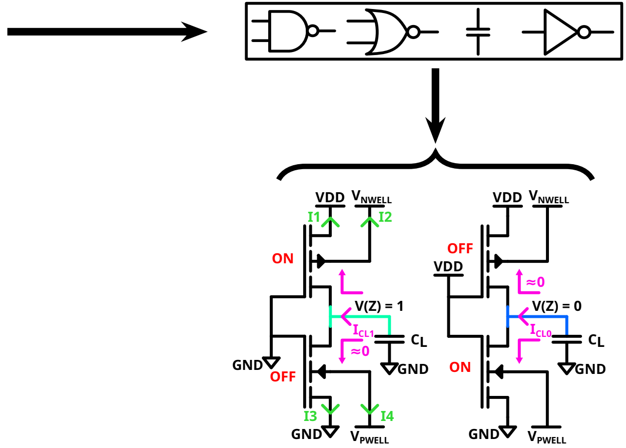
To understand how faults occur

$\downarrow$

We need to consider the logic inside the IC

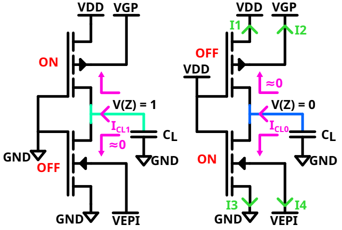
# SCS incomplete models: how to consider logic function?

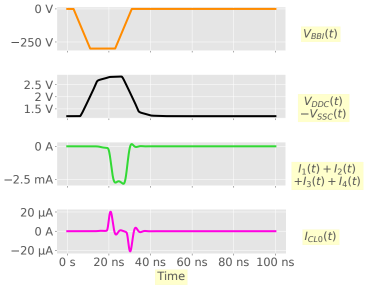


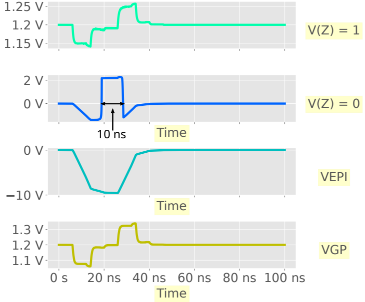



# How faults occur under BBI?

## Dual-well inverters

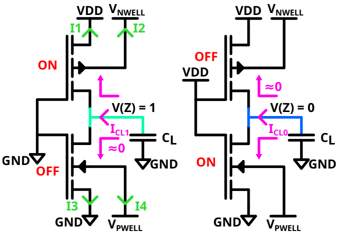


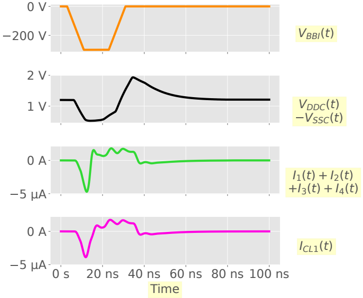



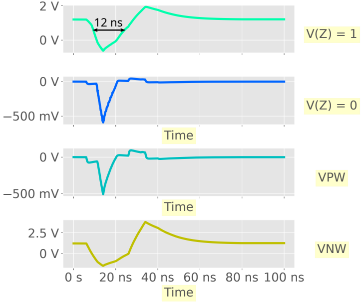



# How faults occur under BBI?

## Triple-well inverters



# How faults occur under BBI?

## Fault model

Data dependent faults:

- Circuits leaks more info;
- Can lead to safe-error attack.

# SUBSTRATE TINNING ANALYSIS

# Substrate thinning in a BBI context

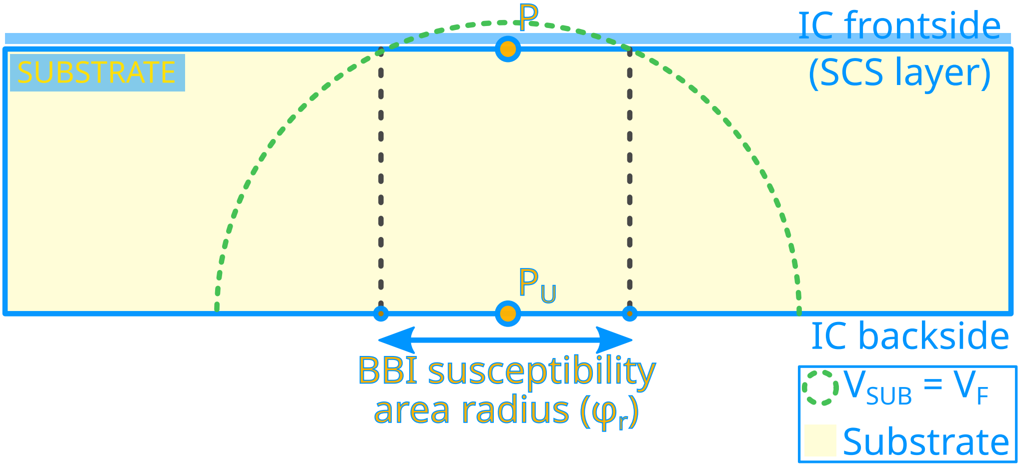
In Laser Fault Injection, substrate thinning has been proven useful
Is it the case concerning BBI?

Section agenda:

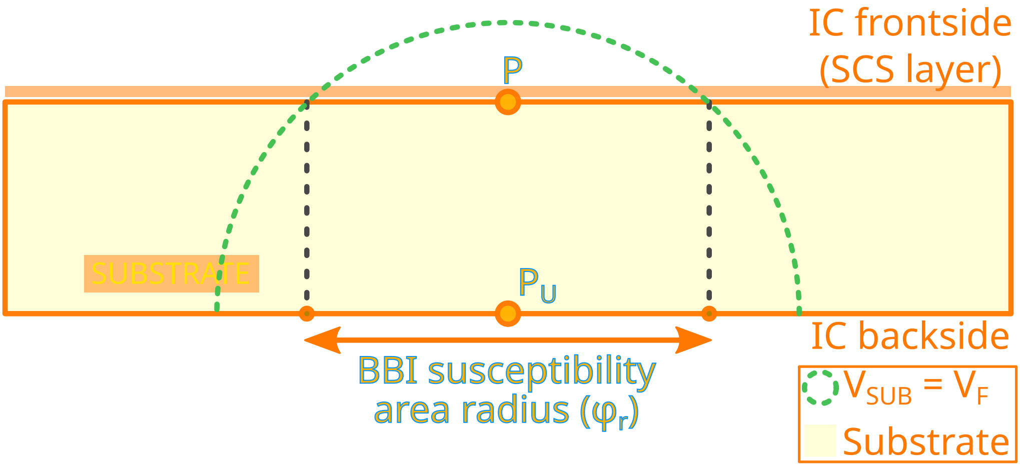
- Geometric approach
- Electrical simulation approach
- Experimental validation

# Geometric approach

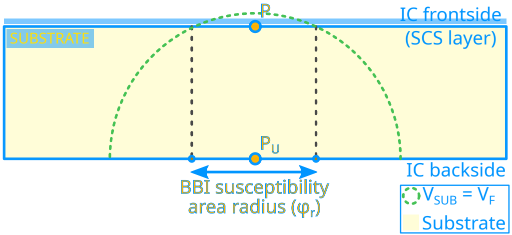
# Geometric approach

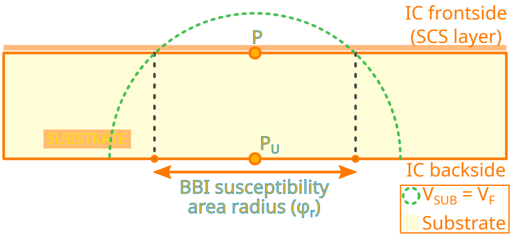


## Geometric approach

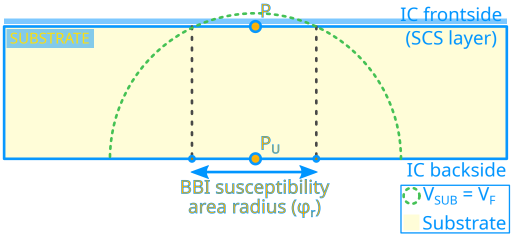


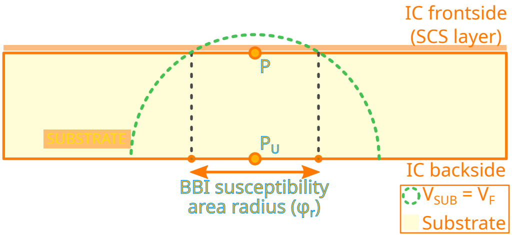
# Geometric approach



# Geometric approach



# Geometric approach outcomes

1. Thinning the substrate $\rightarrow$ Reduce the voltage pulse for a given susceptibility area;
2. Thinning the substrate $\rightarrow$ Susceptibility area increases at constant voltage;
3. Thinning the substrate $\rightarrow$ No improvement in resolution.

# Simulation approach

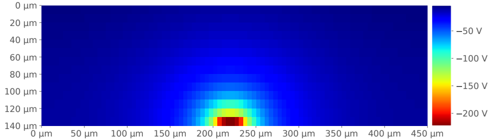
What we observe:

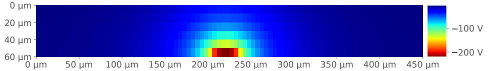
- Dual-well substrate IC;
- Picture at the apex of the pulse;
- 550 $\mu m$ ($W$) $\times$ 450 $\mu m$ ($D$): integrated circuit $\rightarrow$ 1620 SCS;
- 140 $\mu m$ ($T$) IC;
- 60 $\mu m$ ($T$) IC;

Simulation conditions:

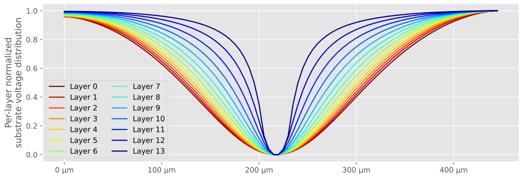
- Voltage pulse amplitude: -300 V;
- Voltage pulse width: 20 ns;
- Rise and fall times: 8 ns.

# Simulation approach

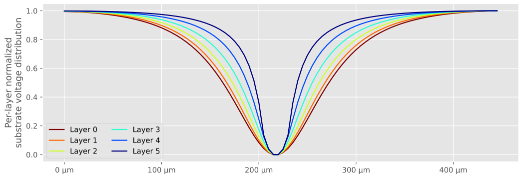



The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.




The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.



# A few words on substrate thinning techniques

AJOUTER IMAGES APPAREILS AMINCISSEMENT ET EXPLICATIONS

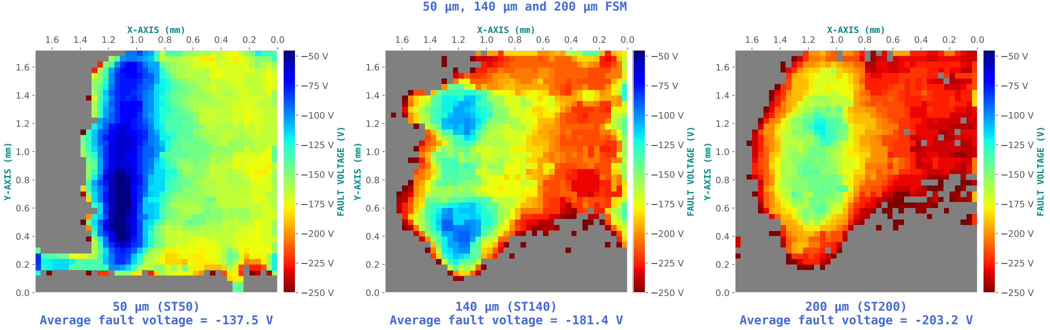
# Substrate thinning in practice

Three experiments to verify the soundness of the outcomes:

- Fault susceptibility maps;
- Susceptibility area spreading maps;
- Susceptibility area comparison.

# Substrate thinning in practice

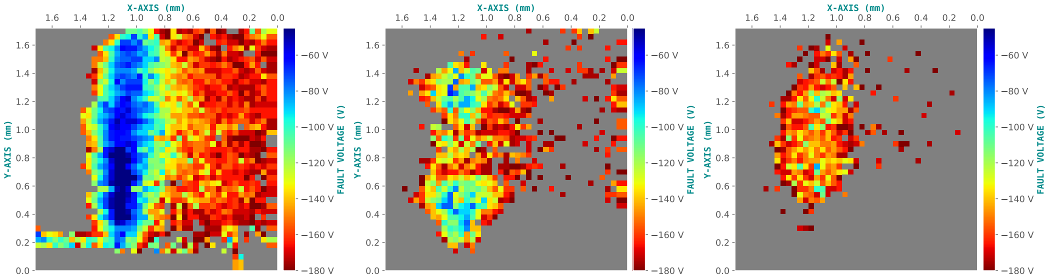
## Fault susceptibility maps



# Substrate thinning in practice

## Susceptibility area spreading

50 µm, 140 µm and 200 µm FSM




50 µm (ST50)
Average fault voltage = -132.3 V

140 µm (ST140)
Average fault voltage = -145.9 V

200 µm (ST200)
Average fault voltage = -154.7 V

# Substrate thinning in practice

## Fault susceptibility maps couples