

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

PhD thesis defense

Geoffrey Chancel

2024/01/29



Jean-Luc Danger

Giorgio Di Natale

Pascal Nouet

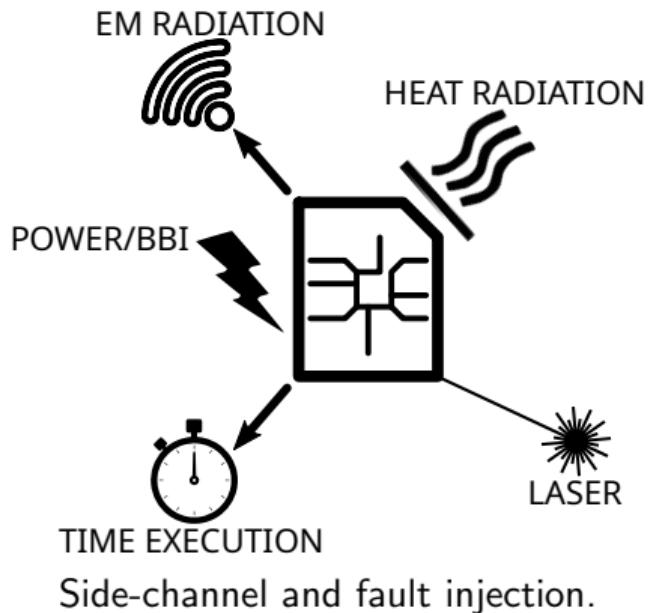
Jean-Max Dutertre

Jean-Marc Gallière

Philippe Maurine

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



Fault injection attacks

Fault injection objectives:

- Denial of service (DoS) → Stop circuit operations and the related services
- Verification bypass → Modify data on the fly to fake authenticity
- Confidential data extraction → Modify data to perform differential fault analysis

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

- "Yet another fault injection technique : by forward body biasing injection (2011)": Introducing the new technique and a Bellcore attack
- "Voltage spikes on the substrate to obtain timing faults (2012)": Timing faults
- "Body biasing injection attacks in practice (2016)": Lumped model for dual-well substrates

Six days after the beginning of my thesis:

- "Low-cost body biasing injection (BBI) attacks on WLCSP devices. (2020)": Low-cost tool, fault analysis, hardware attack

Limited information in the literature at the beginning of my thesis

Body biasing injection: industrial and academic platforms

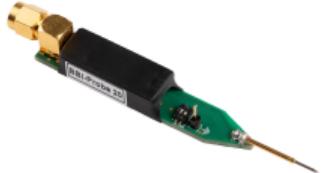
Langer



Current source:

- 4 A in 1Ω
- $\pm 1 \text{ ns}$ jitter
- 2 ns rise time

Riscure



Voltage source:

- Probe 64 A
- $450 \text{ V} \pm 45 \text{ V}$
- Max. PW 50 ns

ChipSHOUTER



Voltage source:

- 150 V to 450 V
- PW: 15 ns to 480 ns
- 220 ps jitter

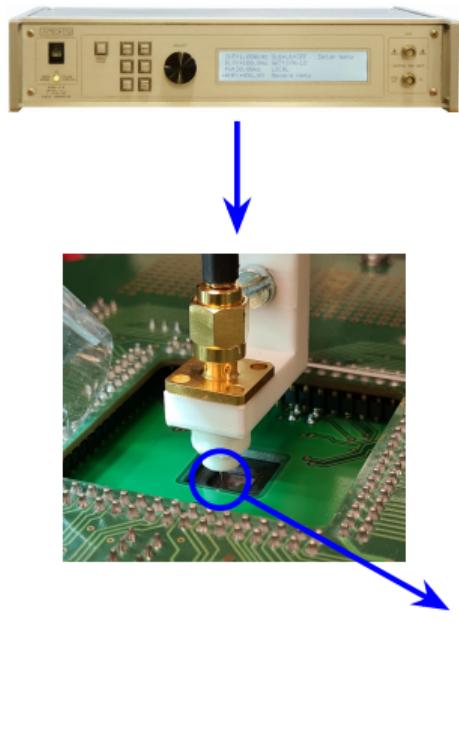
Pico-EMP



Voltage source (AC):

- Up to 250 V
- PW: 85 ns in 50Ω
- Up to 200 mW

Body biasing injection: LIRMM BBI platform



Main platform characteristics:

V_{PULSE}	[150 ; 750] V
P_W	[6 ; 20] ns
$T_R T_F$	4 ns
Recovery time	1 ms
Propagation delay	150 ns
Input jitter	$\pm 100 \text{ ps} \pm 0.03\%$
Output coupling	DC
Gen. I_{MAX} (50 Ω)	16 A
Probe I_{MAX}	3 A
Probe \varnothing	40 μm

Thesis objectives

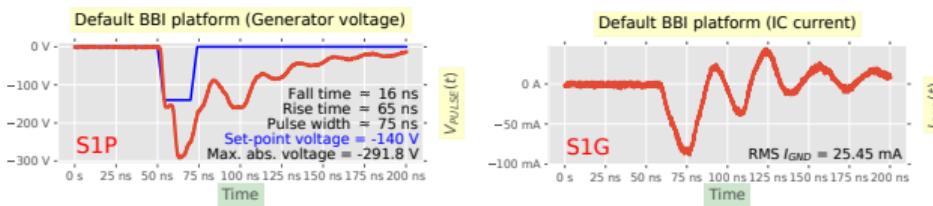
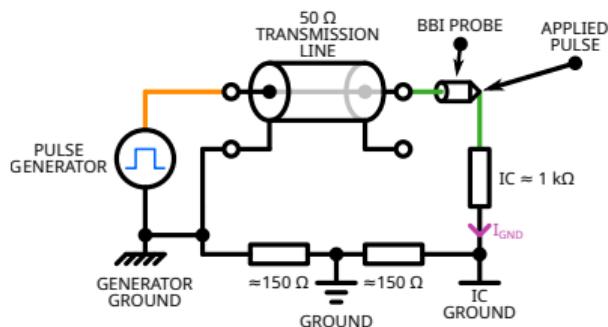
- What is the spatial resolution of BBI?
- What is the time resolution of BBI?
- Is thinning the substrate useful in any way?
- How BBI induced faults occur?
- How to model BBI?

Thesis agenda

- Enhancing the practice of Body Biasing Injection
- Integrated circuits modeling for BBI
- Enhanced simulation flow
- Substrate thinning analysis in a BBI context
- Conclusion and perspectives

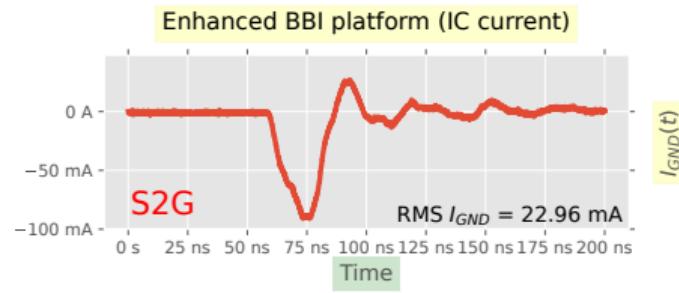
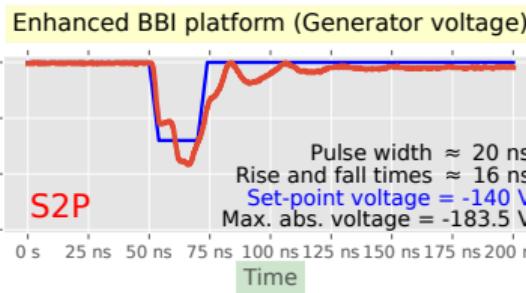
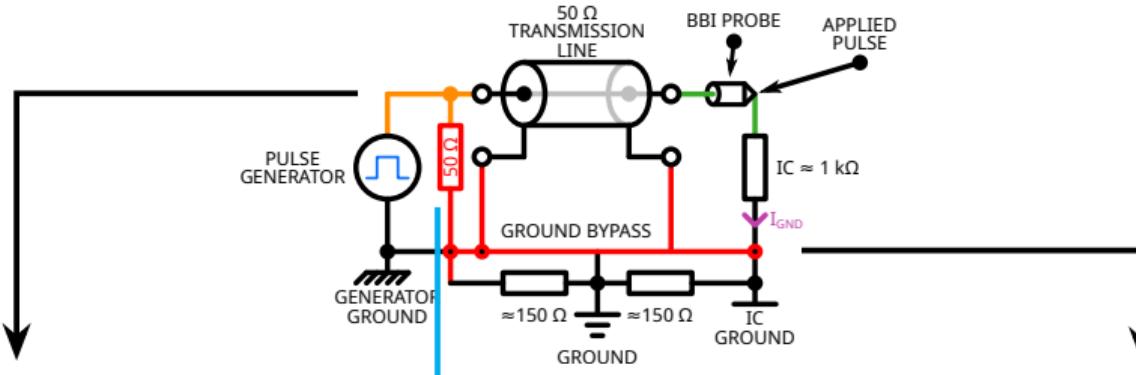
BETTER PRACTICES FOR BODY BIASING INJECTION

State-of-the-art BBI platform: limiting factors



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

Enhanced BBI platform

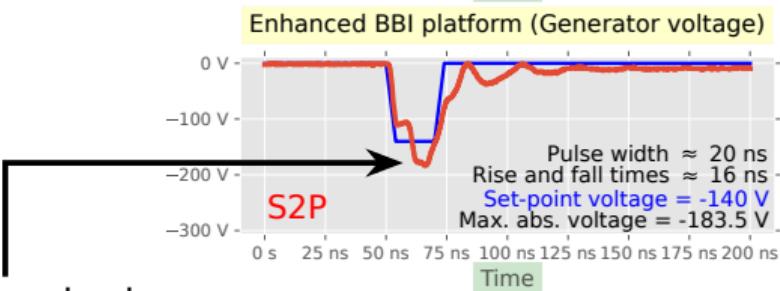
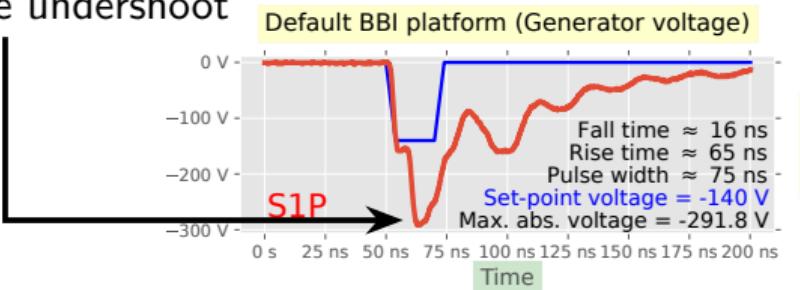


Enhanced BBI platform

Summary

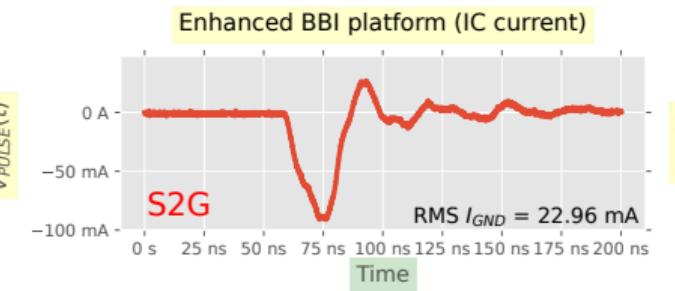
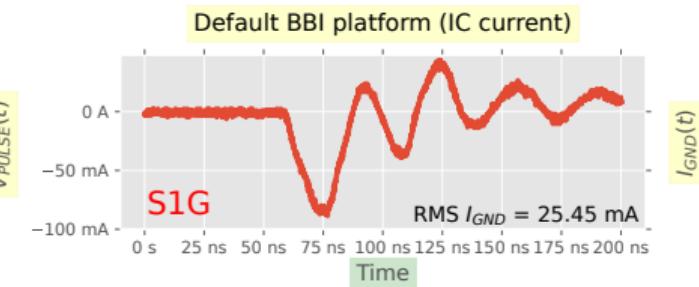
275 % PW overshoot

-108 % pulse undershoot



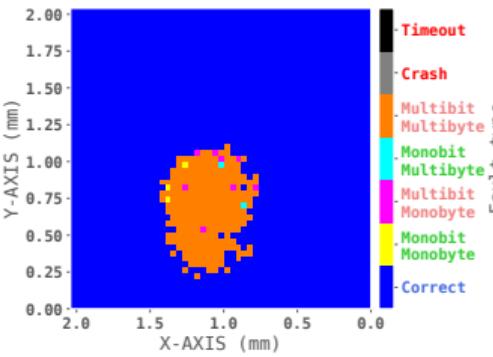
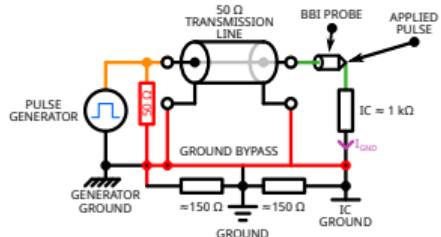
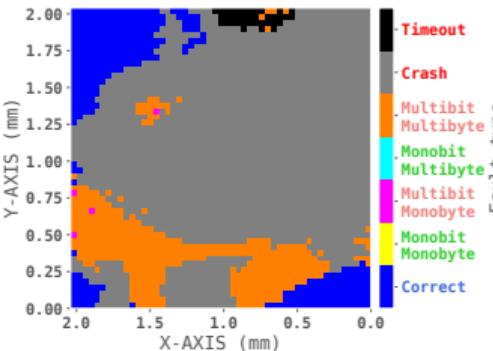
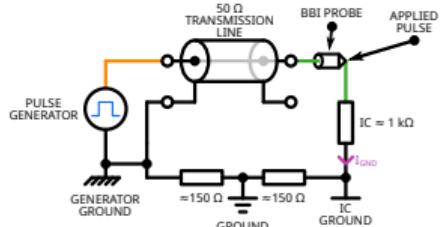
-31 % pulse undershoot

Matched pulse width



Enhanced BBI platform benefits

Giraud's single bit fault attack



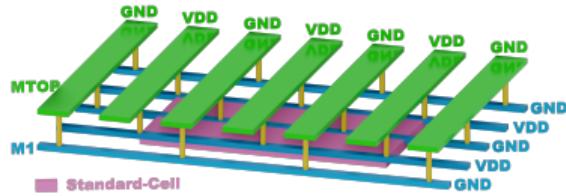
Impossibility to perform the
Giraud's DFA
No single bit faults after
2601 tested locations

5 locations → single bit faults
14 secret-key bytes out of 16
→ Giraud's DFA
2 remaining bytes
→ brute force

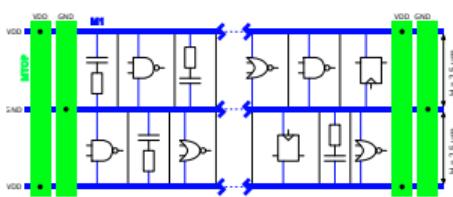
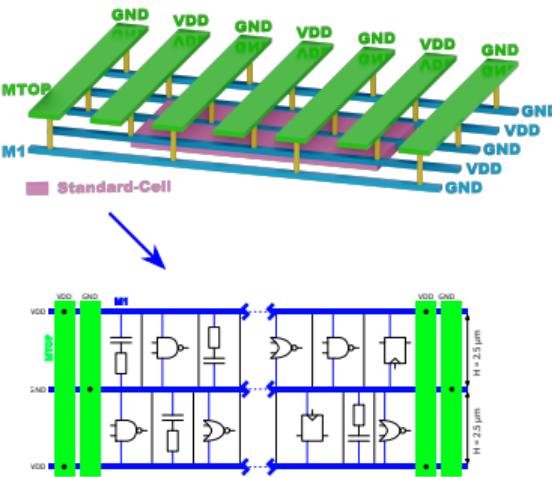
MODELING AND SIMULATING BODY BIASING INJECTION

Why modeling and simulating BBI?

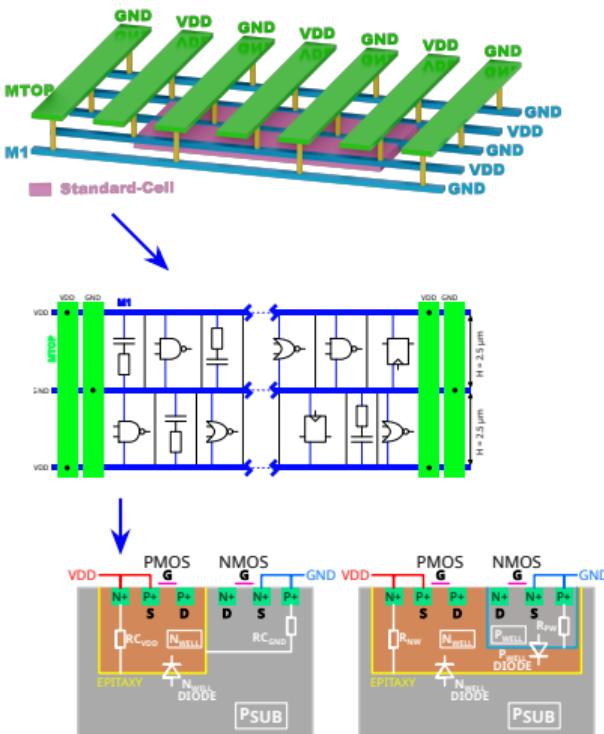
Simulation models



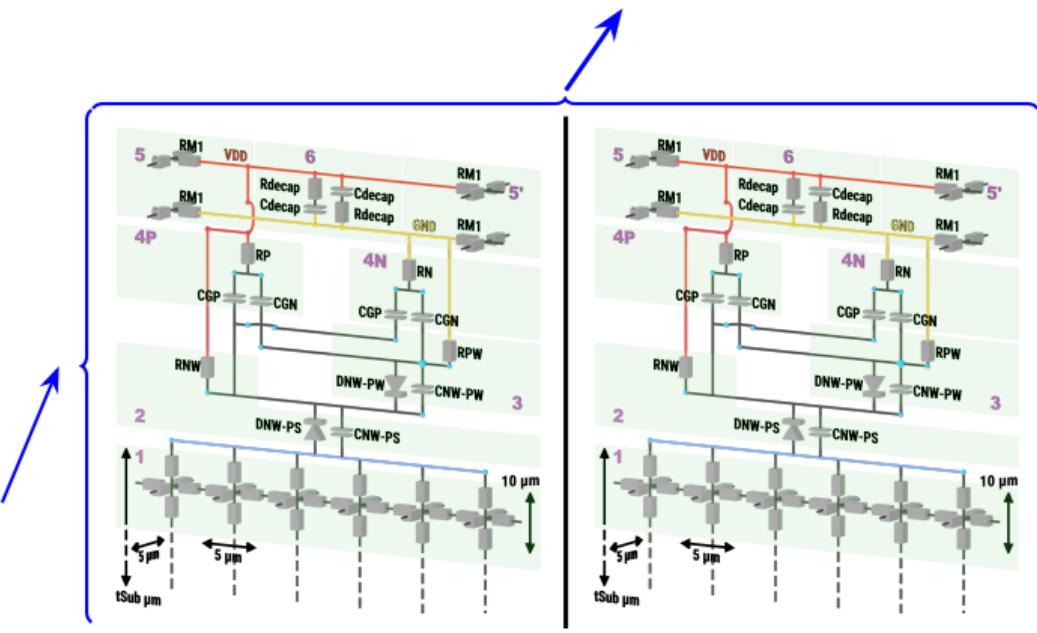
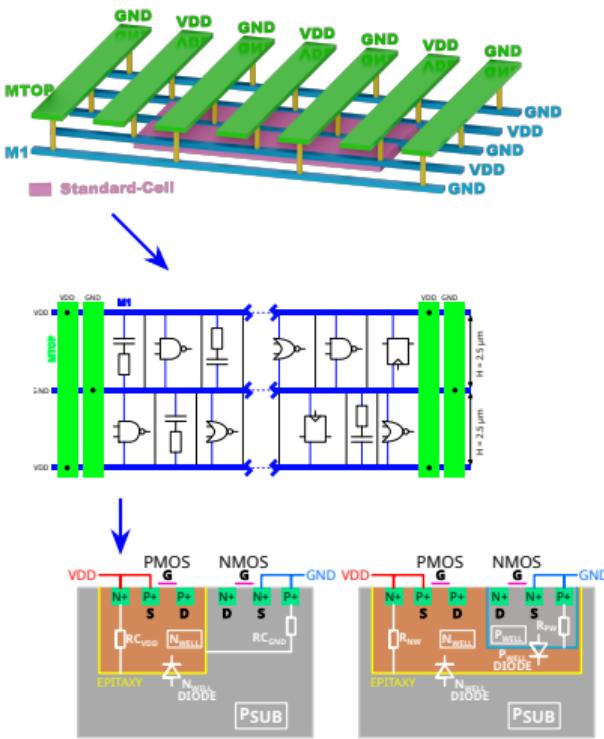
Simulation models



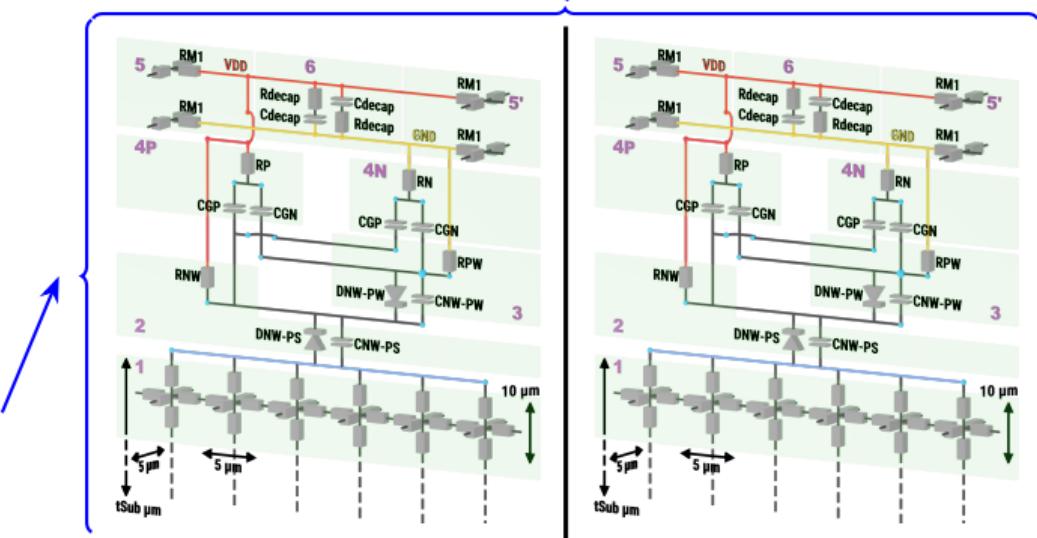
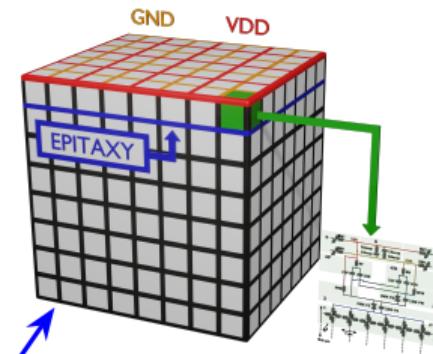
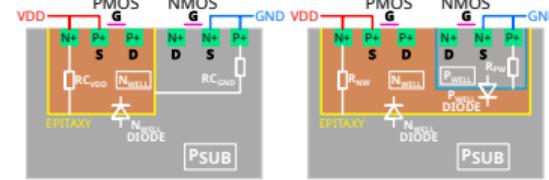
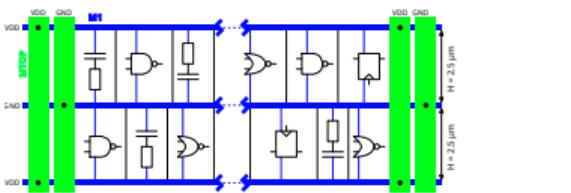
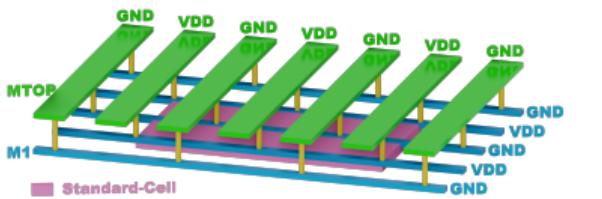
Simulation models



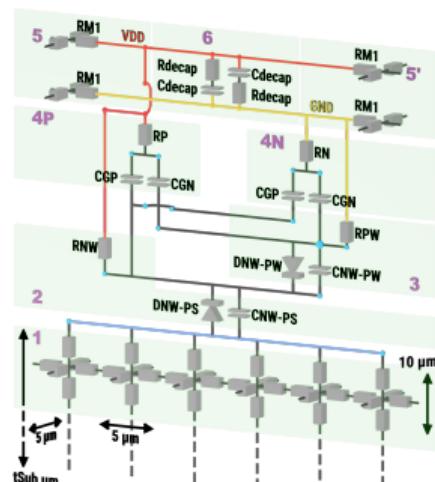
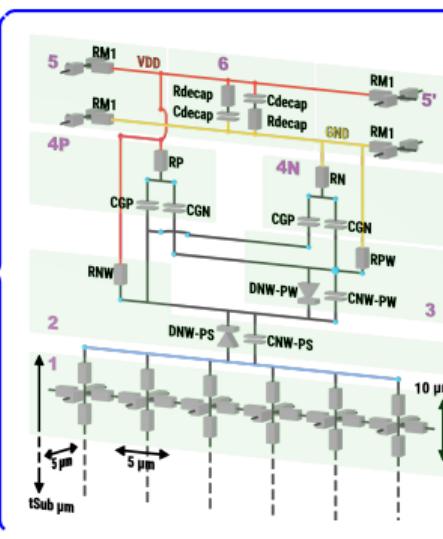
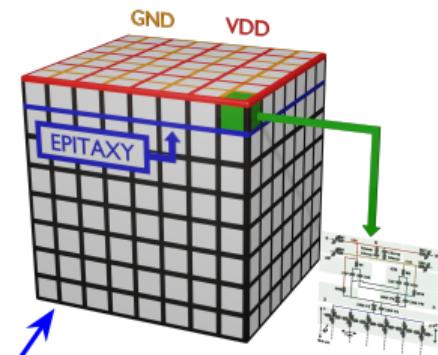
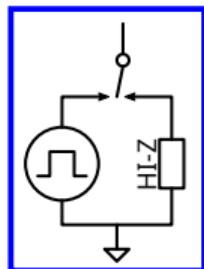
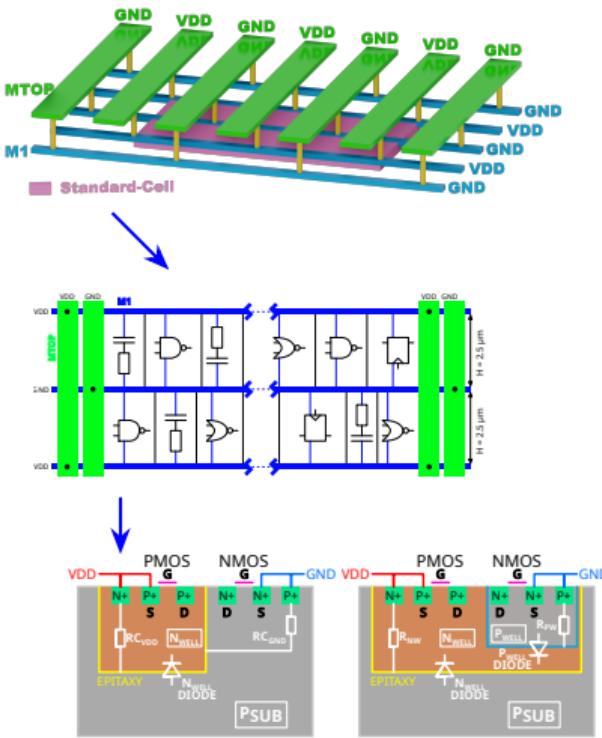
Simulation models



Simulation models



Simulation models



Simulation results

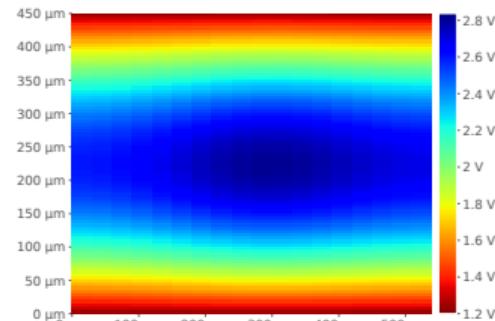
What we observe:

- 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;

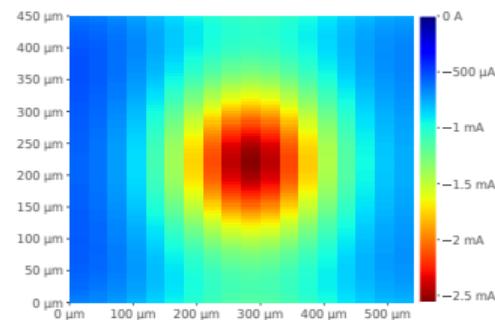
Simulation conditions:

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

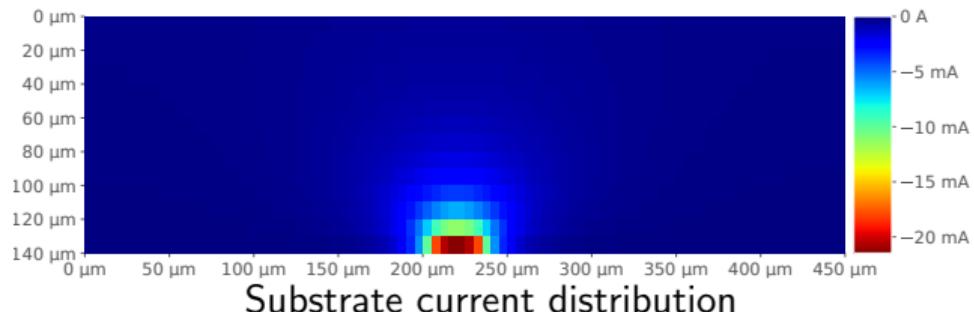
Simulation results: Dual-Well



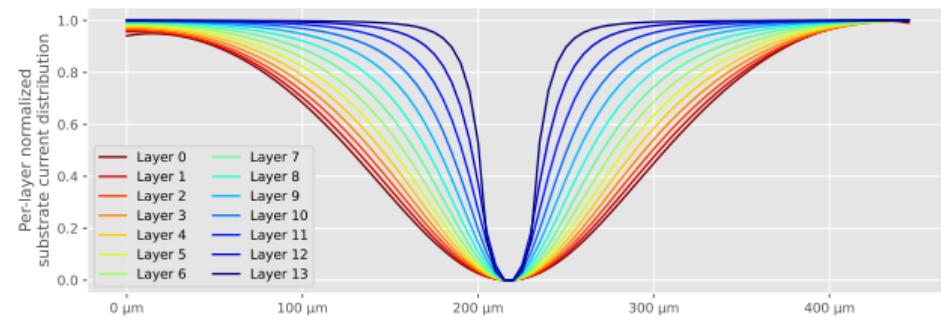
PDN voltage distribution



Epitaxy current distribution



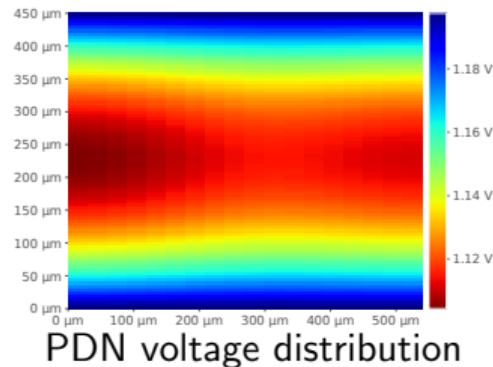
Substrate current distribution



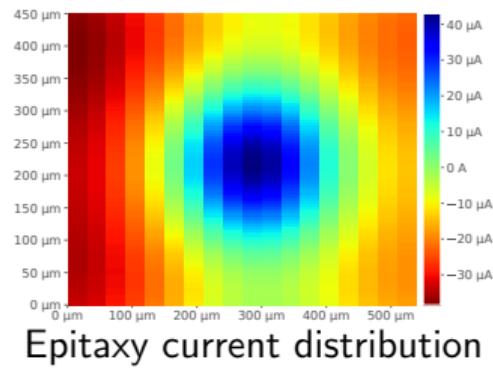
Per-layer normalized substrate current density

180 μm diameter mid-height

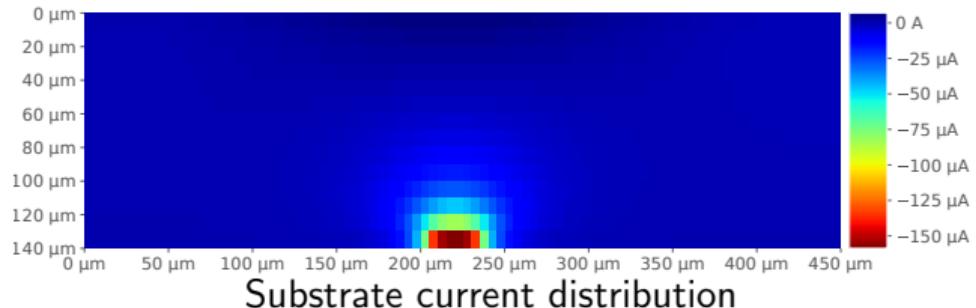
Simulation results: Triple-Well



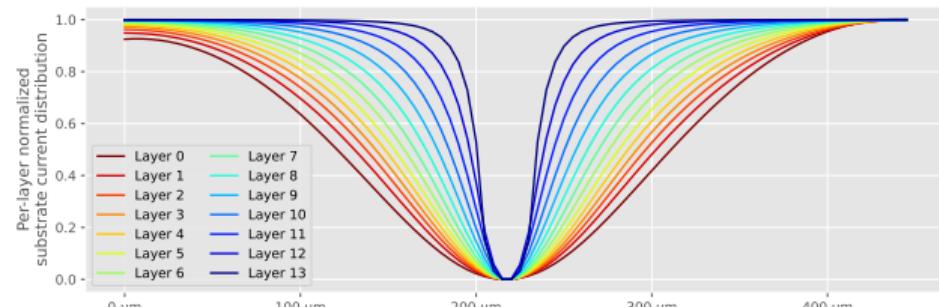
PDN voltage distribution



Epitaxy current distribution



Substrate current distribution



Per-layer normalized substrate current density:
186 μm diameter mid-height

Dual-well vs Triple-well

Differences between Dual-well and Triple-well circuits:

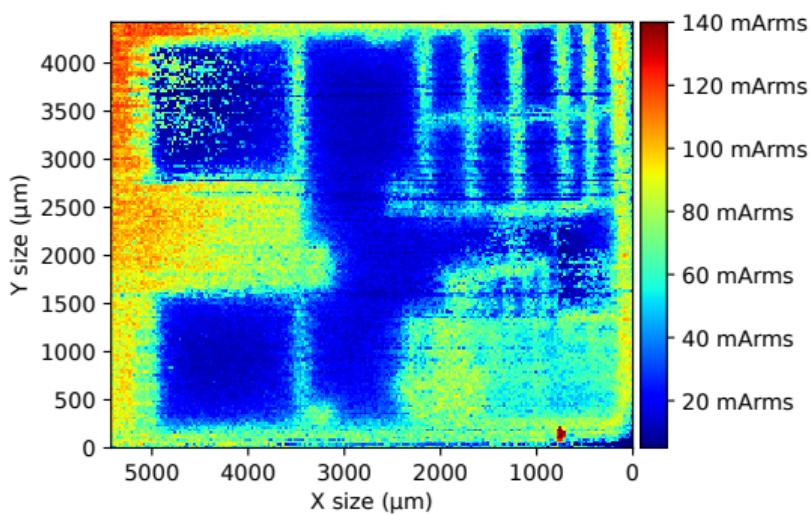
- Dual-well → NMOS are DC-coupled — PMOS are AC-coupled;
- Triple-well → entire IC is AC-coupled.

Implications:

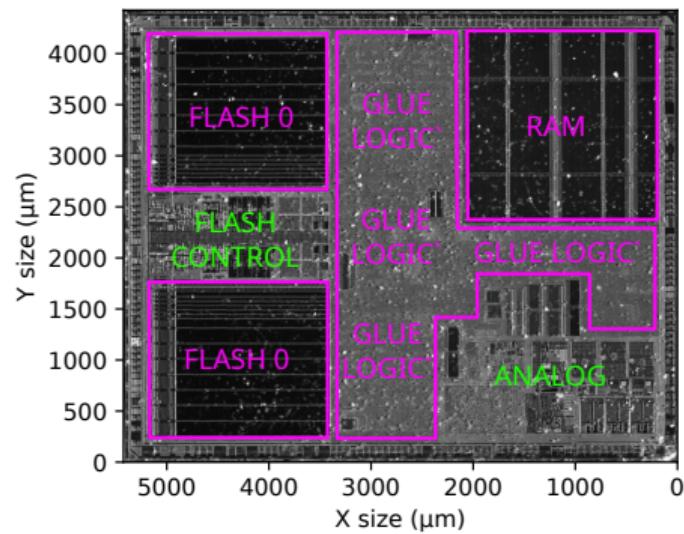
- Dual-well → continuous energy flow during the pulse;
- Triple-well → energy flow confined to the pulse edges;

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

Simulation results verification

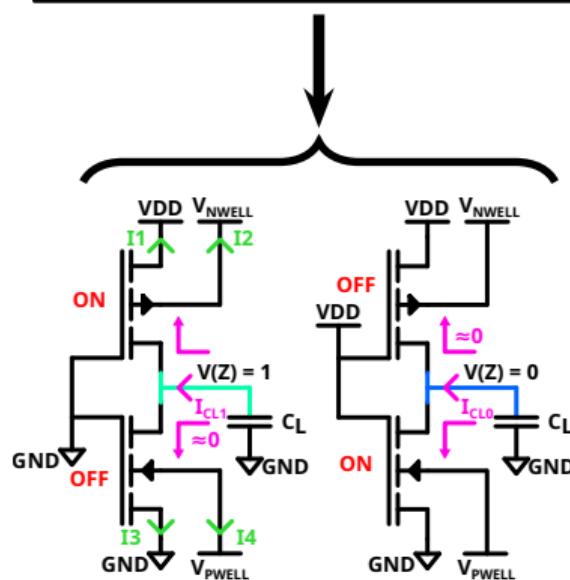
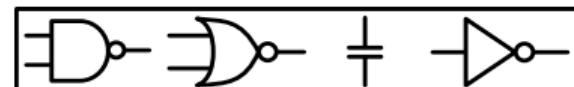
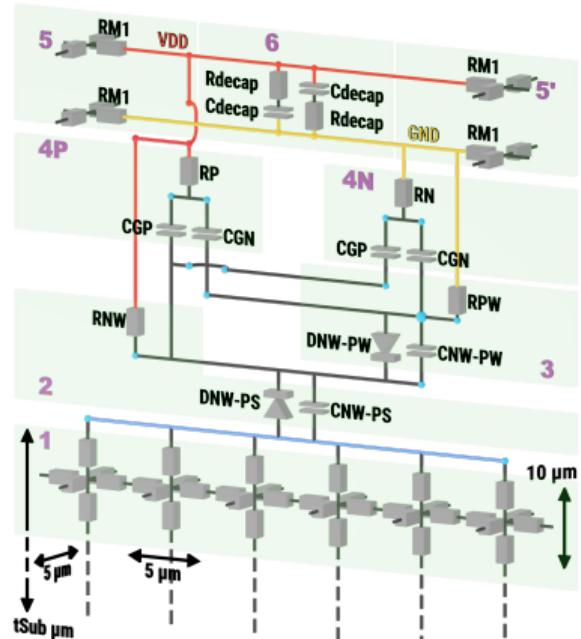


$V_{PULSE} = -70 \text{ V}; PW = 20 \text{ ns}$



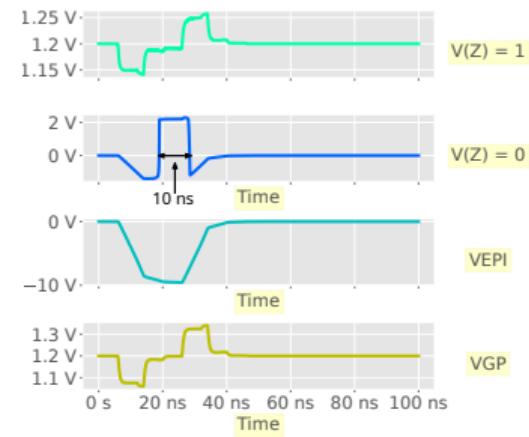
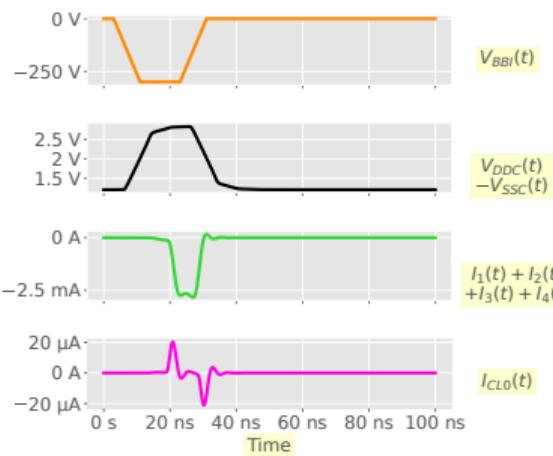
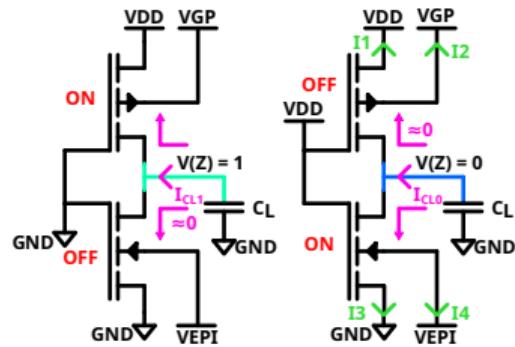
SIMULATION FLOW FOLLOW-UP: HOW FAULTS OCCUR?

SCS incomplete models: how to consider logic function?



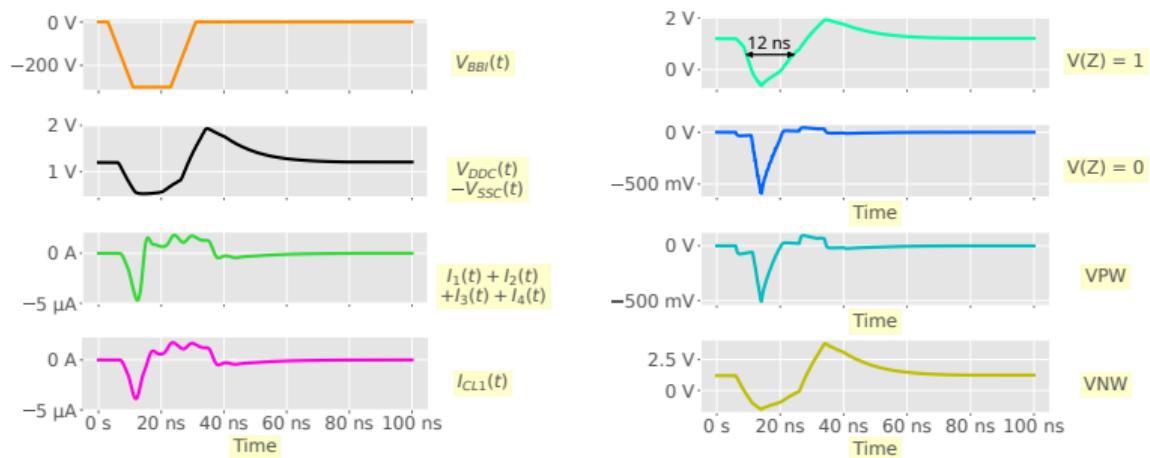
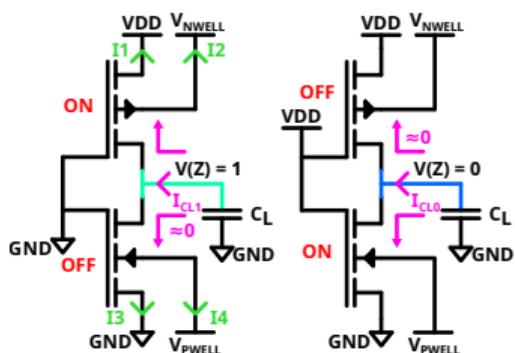
How faults occur under BBI?

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

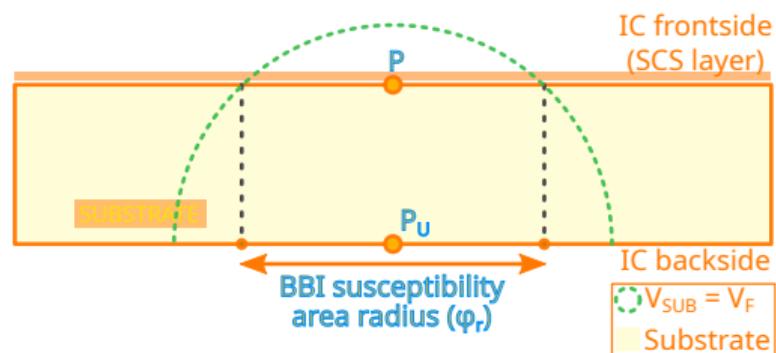
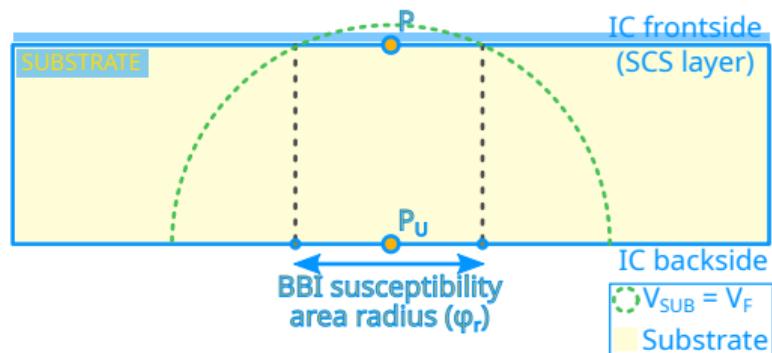
Substrate thinning in a BBI context

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

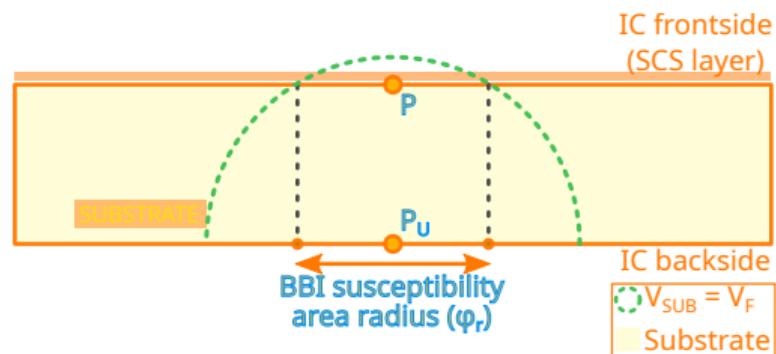
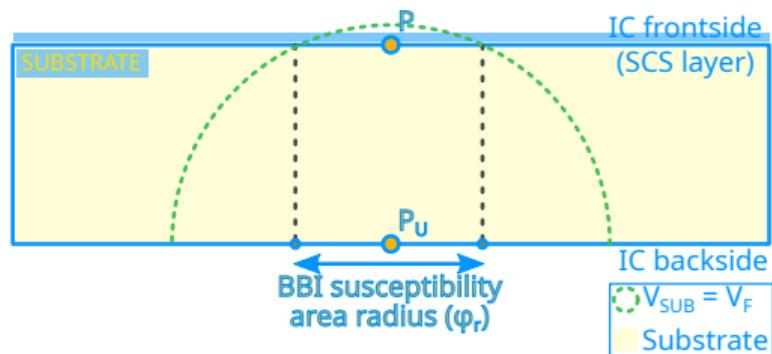


$$\phi_r(t) = 2 \cdot \sqrt{r(t)^2 - t_{SUB}^2} \quad (1)$$

$$\frac{\phi_r^{THIN}}{\phi_r^{THICK}} = \sqrt{\frac{r^2 - t_{THIN}^2}{r^2 - t_{THICK}^2}} > 1 \quad (2)$$

Higher susceptibility area \rightarrow greater current density

Geometric approach



$$V_{PU}^* = \frac{t_{THIN}}{t_{THICK}} \cdot V_{PU} + V_F \cdot \left(1 - \frac{t_{THIN}}{t_{THICK}}\right) \quad (3)$$

Geometric approach outcomes

- Thinning the substrate → Reduce the voltage pulse for a given susceptibility area;
- Thinning the substrate → Susceptibility area increases at constant voltage;
- Thinning the substrate → No improvement in resolution.

Simulation approach

What we observe:

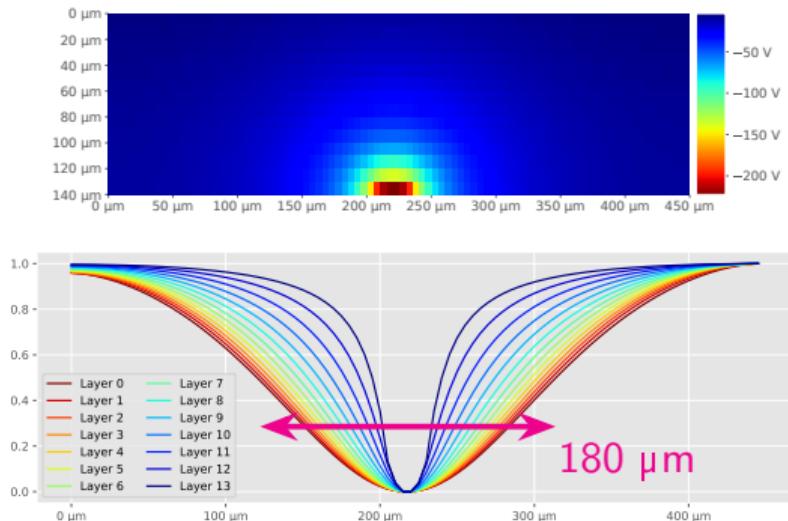
- Dual-well substrate IC;
- Picture at the apex of the pulse;
- $550 \mu\text{m} (W) \times 450 \mu\text{m} (D)$: integrated circuit $\rightarrow 1620$ SCS;
- $140 \mu\text{m} (T)$ IC;
- $60 \mu\text{m} (T)$ IC;

Simulation conditions:

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

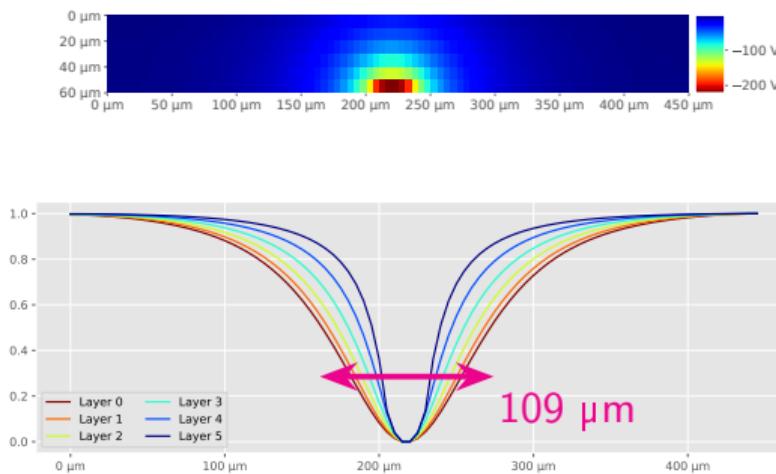
Simulation approach

Substrate voltage distribution (140 μm)



Substrate normalized current density (140 μm)
Highest layer @ 0.5 density diameter: 180 μm

Substrate voltage distribution (60 μm)



Substrate normalized current density (60 μm)
Highest layer @ 0.5 density diameter: 109 μm

For half of the normalized density \rightarrow lower diameter \rightarrow greater current density

Substrate thinning in practice

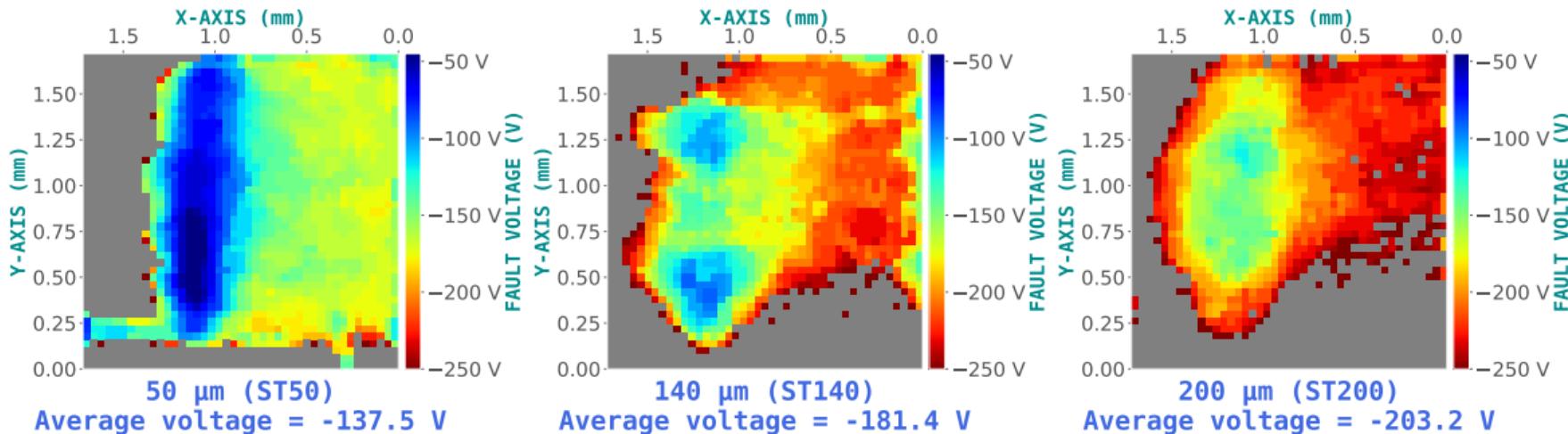
Three experiments to verify the soundness of the outcomes:

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

Substrate thinning in practice

Fault susceptibility maps

50 µm, 140 µm and 200 µm FSM

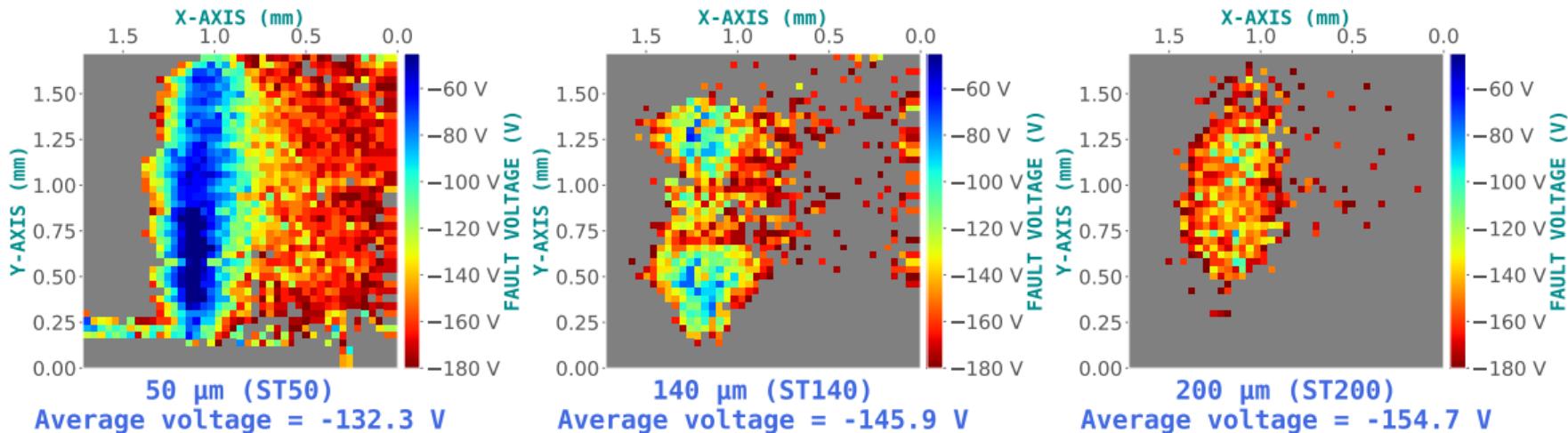


Thinning the substrate → reduces the voltage required to induce faults

Substrate thinning in practice

Susceptibility area spreading

50 μm , 140 μm and 200 μm FSM

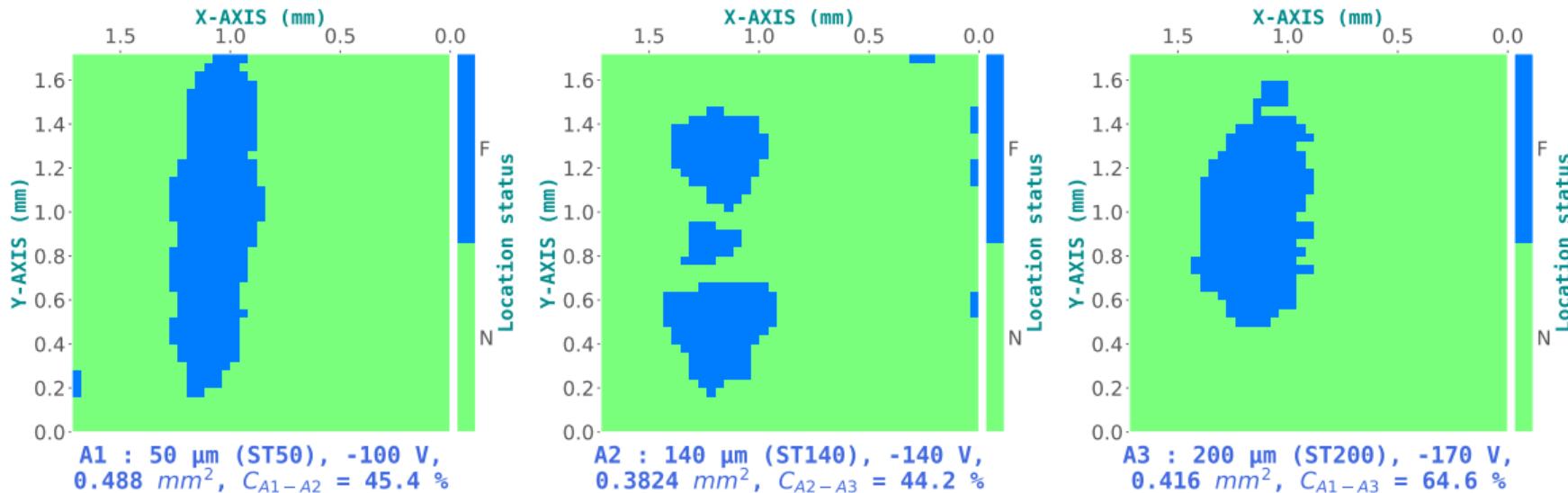


Thinning the substrate → increases the susceptibility for a given maximum voltage

Substrate thinning in practice

Fault susceptibility maps areas comparison

50 µm, 140 µm and 200 µm susceptibility areas comparison (F = FAULT, N = NO FAULT)



Same susceptibility areas with correct couple: (V_P, t_{SUB})
No change in spatial resolution

CONCLUSION AND OUTLOOKS

Conclusion

- Better practices for BBI → successful DFA:
 - Impedance matching
 - Low impedance grounding
- Modeling and simulating BBI:
 - Local effect on ICs → [100, 200] μm
 - Thanks to a DC or AC coupling with the probe
 - Data-dependent faults (bit set and bit reset)
 - DW substrate practice → dangerous
- Substrate thinning and BBI:
 - Lowers generator power requirements
 - Does not change spatial resolution → depends on (V_P , t_{SUB})

Outlooks

Further improvements:

- Adaptive impedance matching → increase repeatability
- Further study logic gates disturbance study → dynamic analysis
- Study memory elements and analog blocks (SRAM, FLASH, PLL)