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

PhD thesis defense

Geoffrey Chancel Jean-Marc Gallière Philippe Maurine

2024/01/29

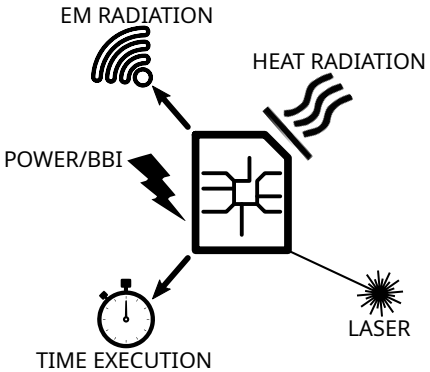
LIRMM

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) → Inject faults causing the circuit to stop;
- Verification bypass → Inject transient faults modifying data on the fly;
- Confidential data extraction → Inject transient faults at specific times.

Thanks to a fault injection platform:

- Thanks to Power Glitch Fault Injection (PW-GFI);
- Thanks to Clock Glitch Fault Injection (CK-GFI);
- Thanks to Laser Fault Injection (LFI);
- Thanks to Electromagnetic Fault Injection (EMFI);
- Thanks to 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

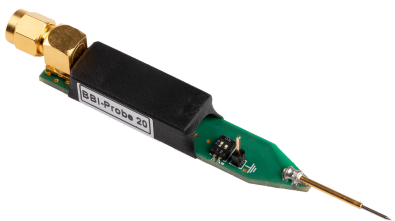
- All-in-one platform;
- A power supply and controller combo called "Burst Power Station";
- An active BBI probe: a current pulse generator, as shown on the right.

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.

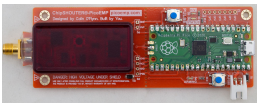


BBI probe proposed by Riscure BV.

Body biasing injection: industrial and academic platforms

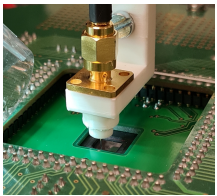
NewAE Technology Inc. BBI platform

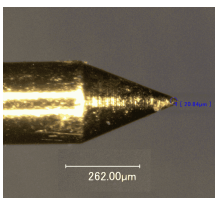
- Combined EMFI/BBI pulse generator;



NewAE PicoEMP low-cost 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

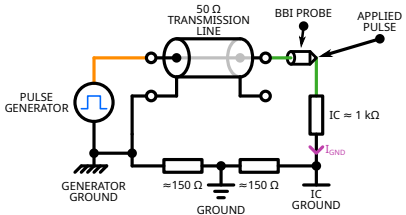
BODY BIASING INJECTION PLATFORM ENHANCEMENTS

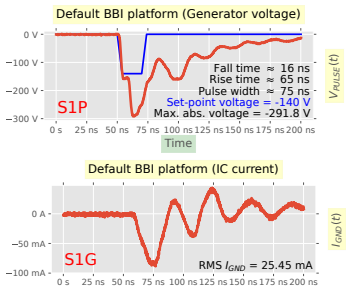
Typical BBI platform

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

What are the limiting factors?

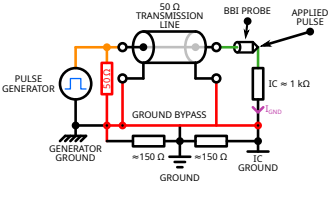
Typical BBI platform

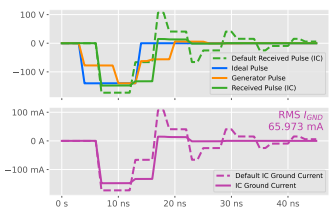


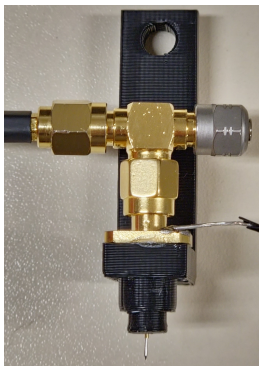


- Impedance mismatch;
- Floating grounds;
- Ringing;
- Set-point error.

Enhanced BBI platform







BBI in practice

Actual results: voltage pulse and IC ground current

Default platform:

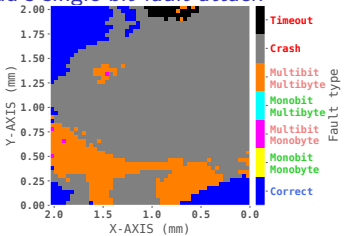
- -108 % pulse undershoot;
- 275 % pulse width overshoot;
- Obvious ringing.

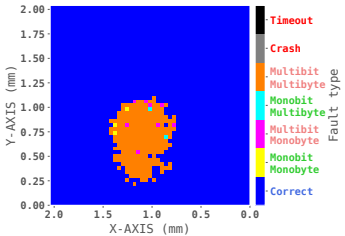
Enhanced platform:

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

Actual benefits of the improvements

Giraud's single bit fault attack





Giraud's single bit fault attack

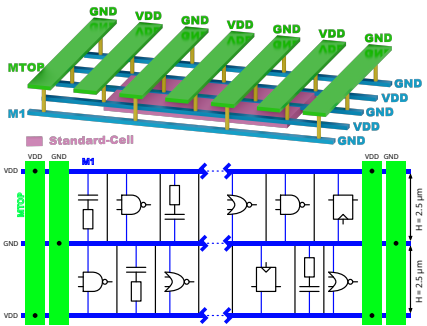
Results

	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

Text content.

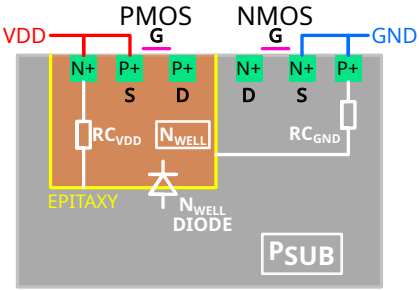
BBI IC SIMULATION FLOW

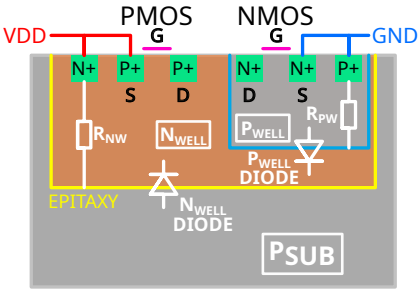
IC basic structure



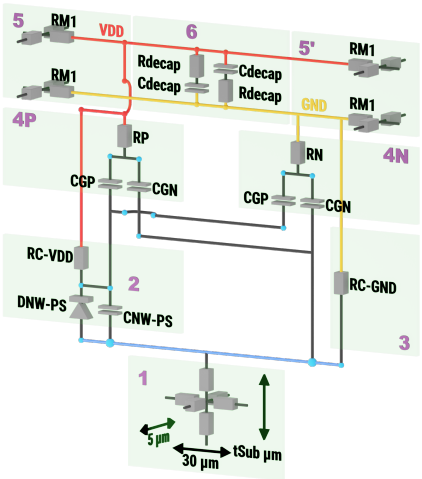
- Item1;
- Item1;
- Item1;
- Item1;

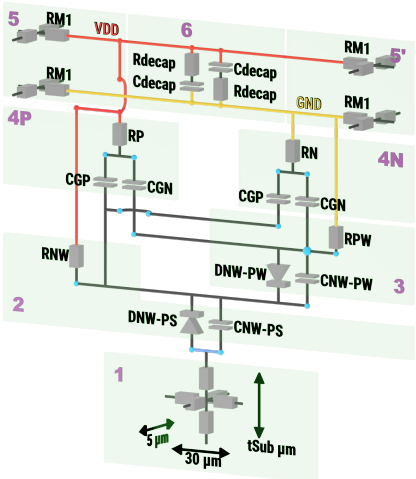
Bulk substrate types



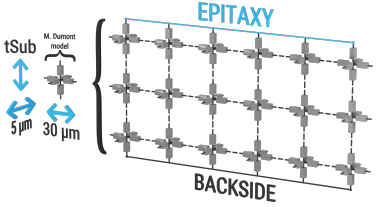


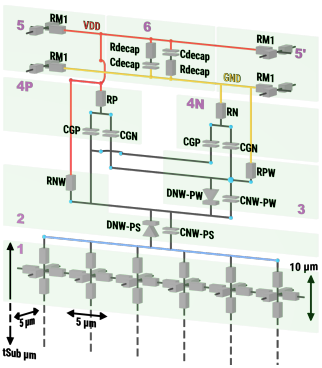
Standard-cell original models

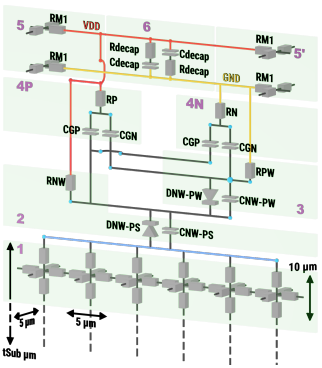




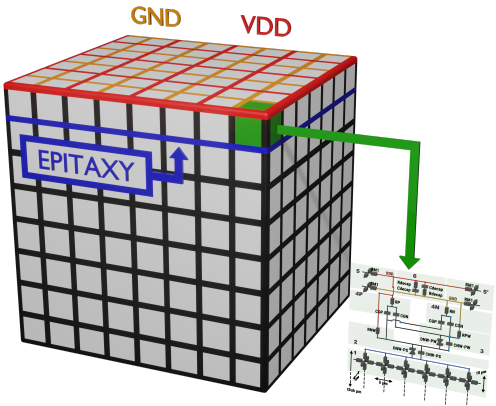
Standard-cell model substrate improvement







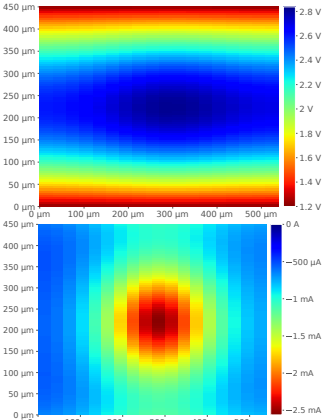
IC generation

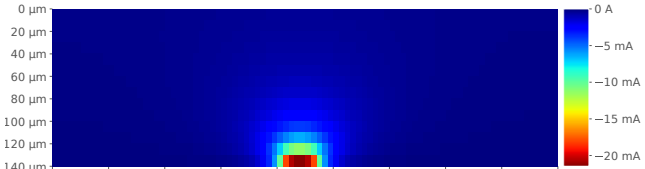


- Item
- Item
- Item
- Item
- Item

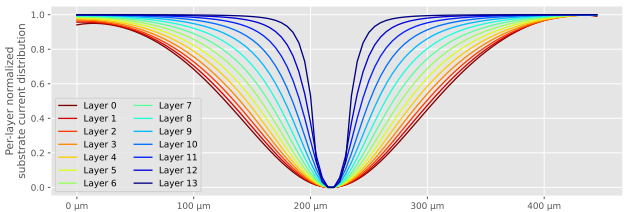
Generator model

Simulation results: Dual-Well

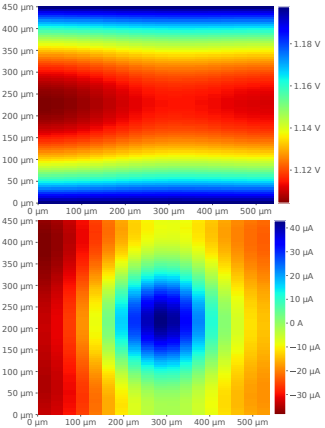


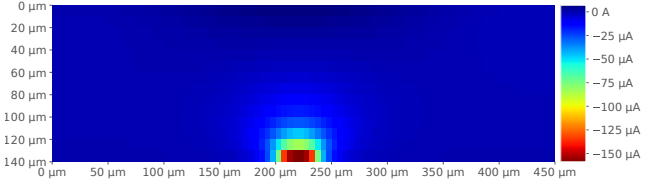


The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.

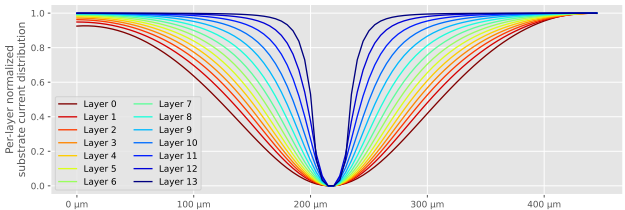


Simulation results: Triple-Well

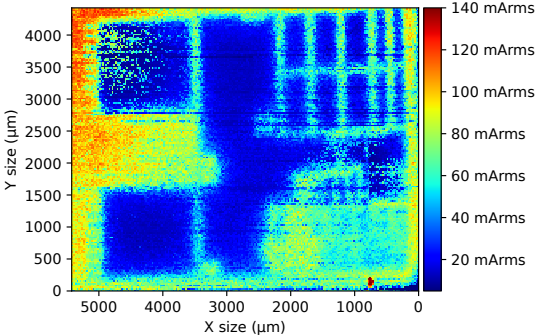


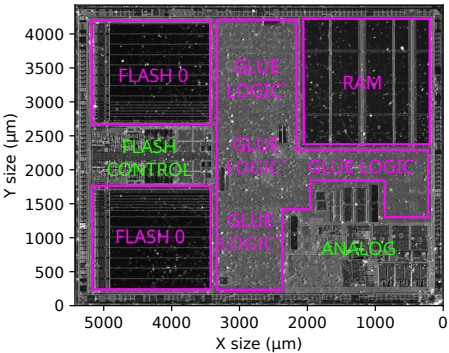


The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.



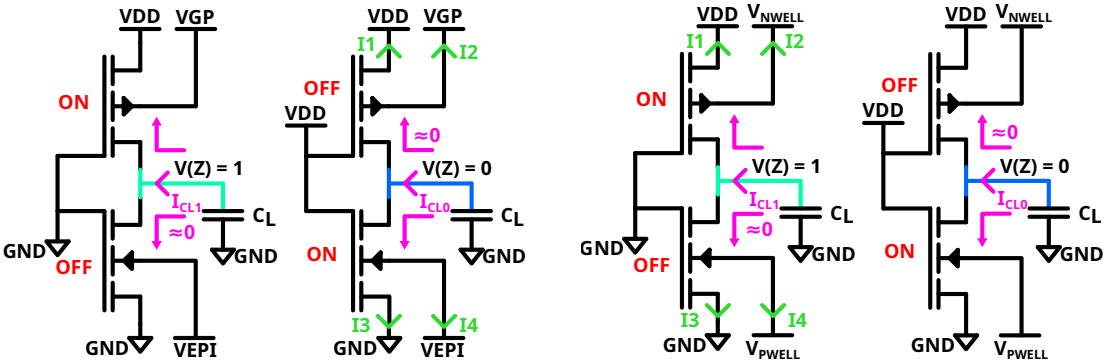
Dual-Well and Triple-well ICs in practice



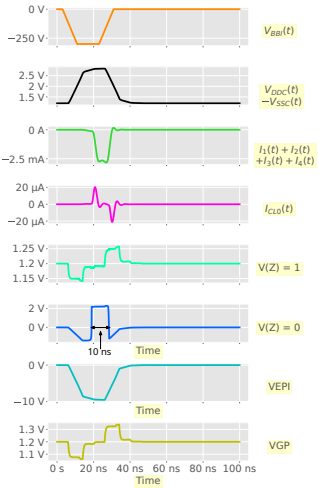


SIMULATION FLOW FOLLOW-UP

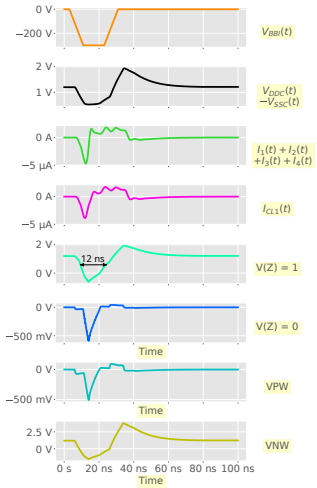
Logic gates simulations under BBI: models



Logic gates simulations under BBI: results



- Item 1
- Item 2
- Item 3

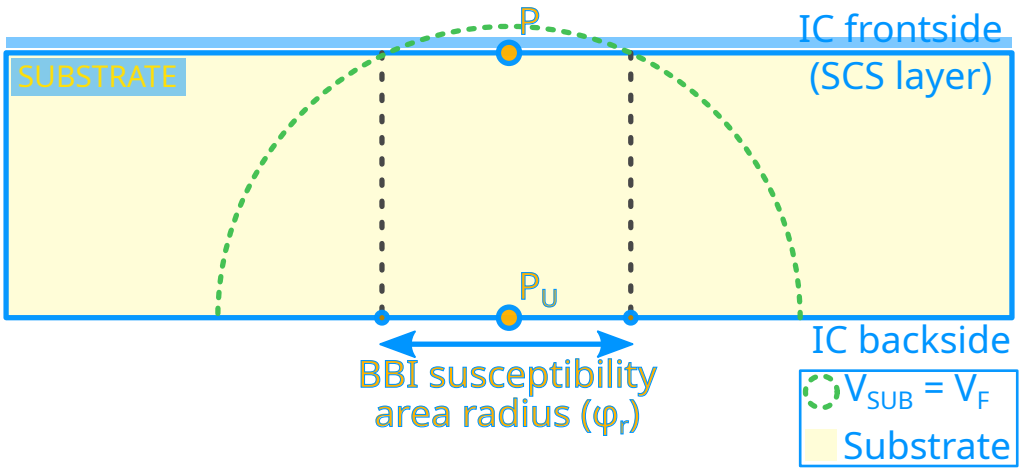


- Item 1
- Item 2
- Item 3

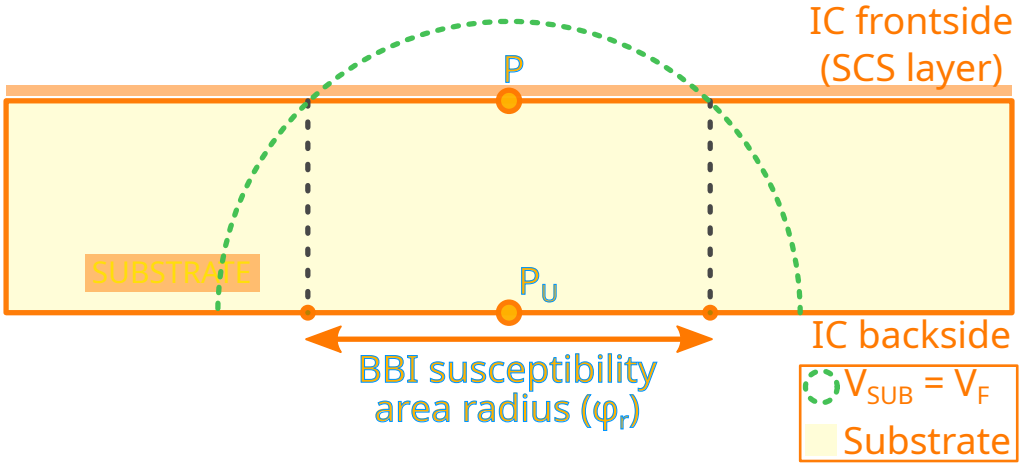
Local conclusion

SUBSTRATE TINNING ANALYSIS

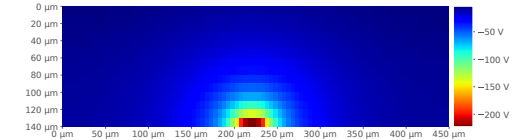
Geometric approach

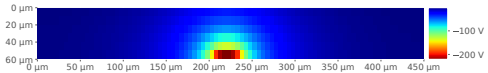


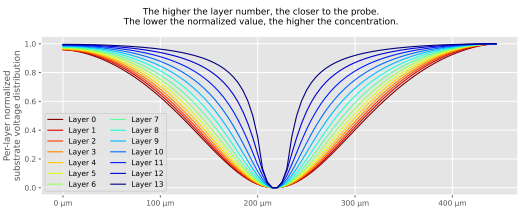
Geometric approach

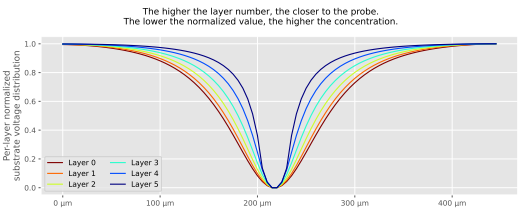


Simulation approach







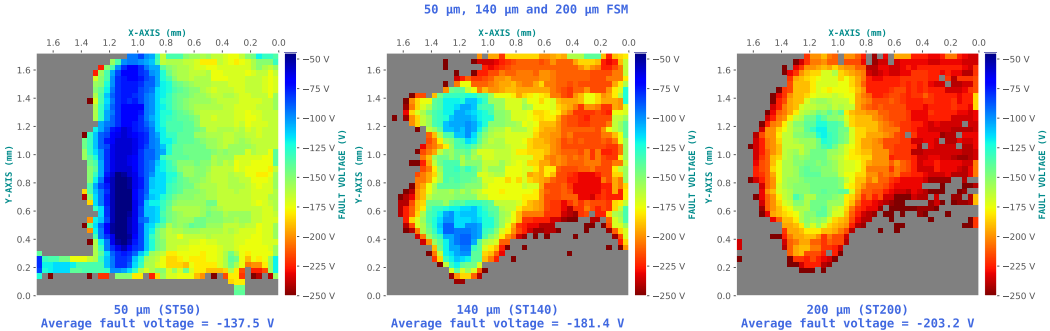


A few words on substrate thinning techniques

AJOUTER IMAGES APPAREILS AMINCISSEMENT ET EXPLICATIONS

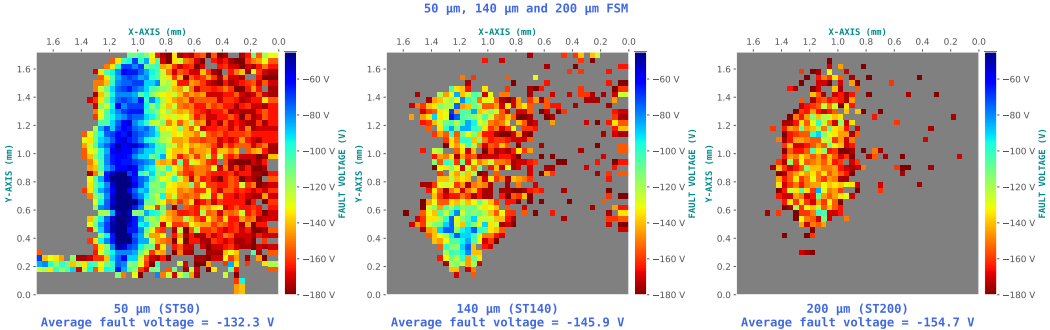
Substrate thinning in practice

Fault susceptibility maps



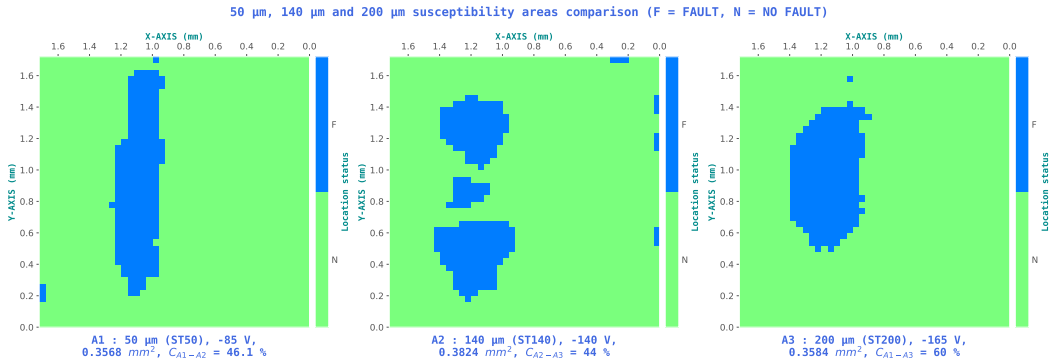
Substrate thinning in practice

Susceptibility area spreading



Substrate thinning in practice

Fault susceptibility maps couples



CONCLUSION

TITLE

SUBTITLE

OUTLOOKS

TITLE

SUBTITLE

PUBLICATIONS

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE