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

- Electronics systems are everywhere, from entertainment to business;
- They embed cryptographic algorithms to ensure secure operation;
- These implementations are fallible $\rightarrow$ they leak information.

Objectives

- Fault injection...;
- Side-channel attacks...;
- Main target $\rightarrow$ Modeling body biasing injection:
  - Characterize better practices for BBI;
  - Define electrical models for BBI simulation;
  - Understand the mechanisms at work;
  - Bring insights on substrate thinning and BBI.

State-of-the-art

Main flaws of algorithms implemented on actual circuits

LOCAL TITLE

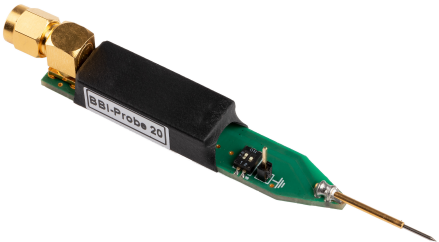
content...
content...
content...

LOCAL TITLE

content...
content...
content...

Body biasing injection: state-of-the-art

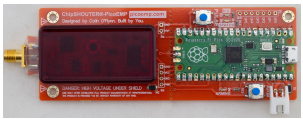
BBI probe proposed by Langer EMV-Technik GmbH.



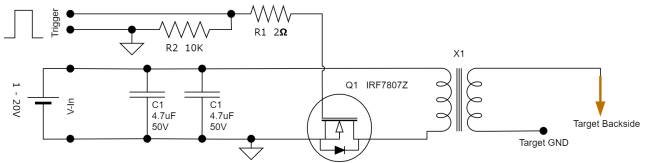
BBI probe proposed by Riscure BV.

Body biasing injection: state-of-the-art

ChipSHOUTER pulse generator

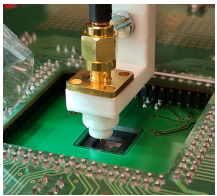


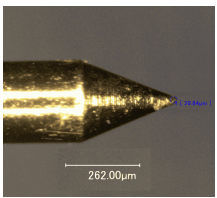
Pico-EMP: low-cost pulse generator



Pico-EMP architecture

Body biasing injection: our BBI platform

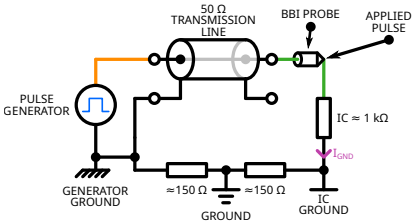


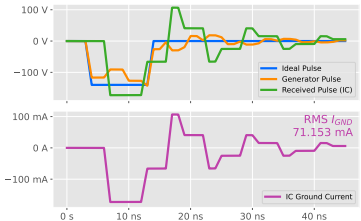


- Custom BBI probe;
  - Spring-loaded metal probe;
  - Custom 3D printed housing;
  - SMA connector;
- AVTECH AVRK-4-B high voltage pulse generator.

BBI IN PRACTICE

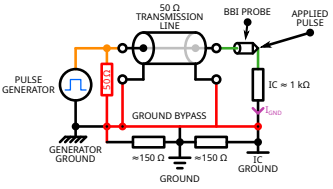
Typical BBI platform

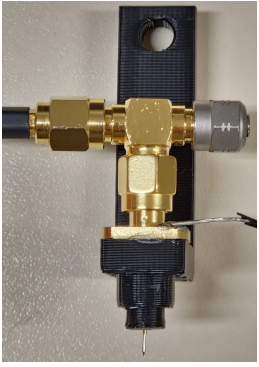




- Pulse generator;
- Transmission line;
- BBI probe;
- IC target;
- Platform ground.

Enhanced BBI platform





BBI in practice

Actual results: voltage pulse and IC ground current

Default platform:

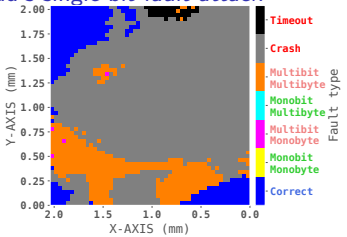
- -108 % pulse undershoot;
- 275 % pulse width overshoot;
- Obvious ringing.

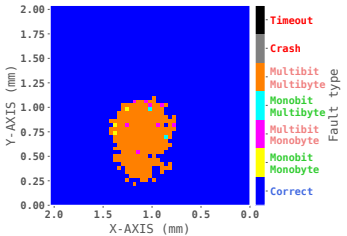
Enhanced platform:

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

Actual benefits of the improvements

Giraud's single bit fault attack





Giraud's single bit fault attack

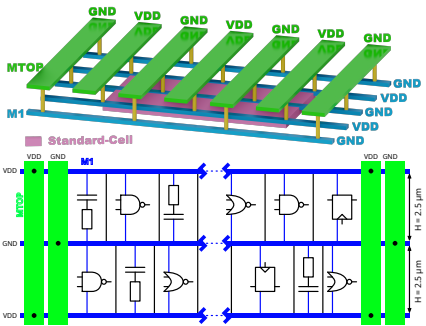
Results

	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.

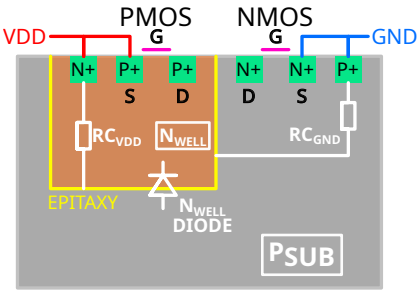
BBI IC SIMULATION FLOW

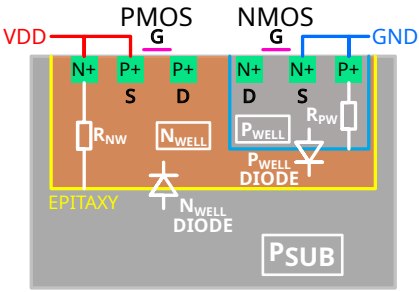
IC basic structure



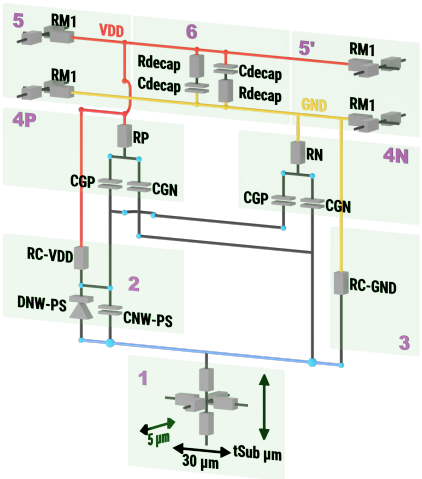
- Item1;
- Item1;
- Item1;
- Item1;

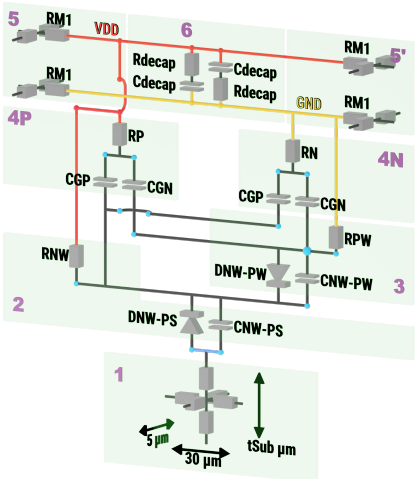
Bulk substrate types



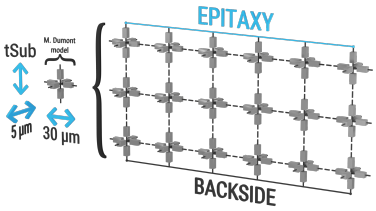


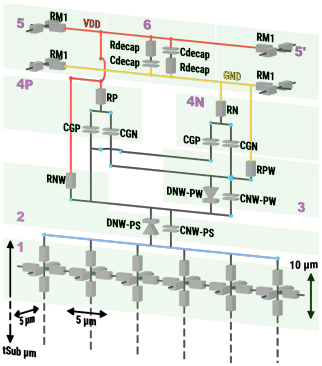
Standard-cell original models

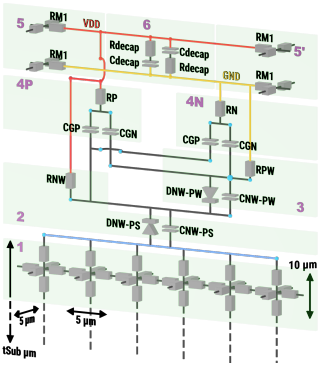




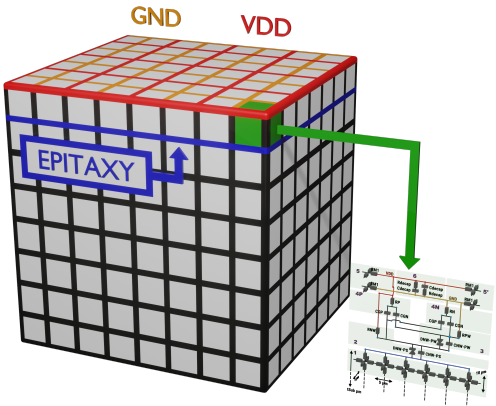
Standard-cell model substrate improvement







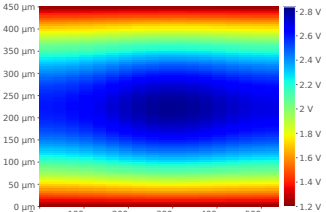
IC generation

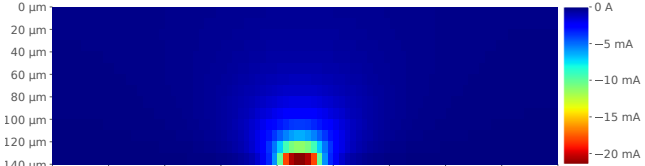


- Item
- Item
- Item
- Item
- Item

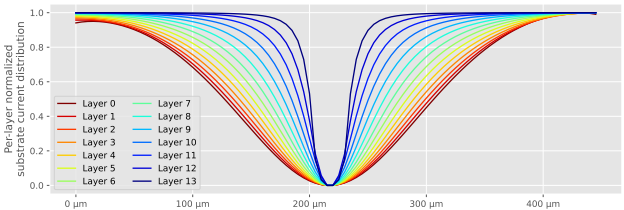
Generator model

Simulation results: Dual-Well

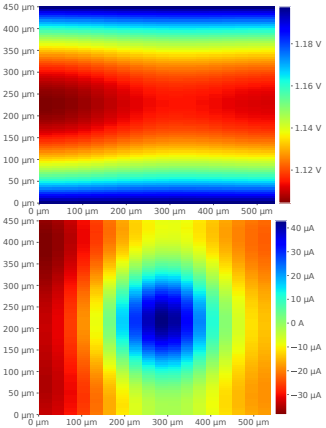


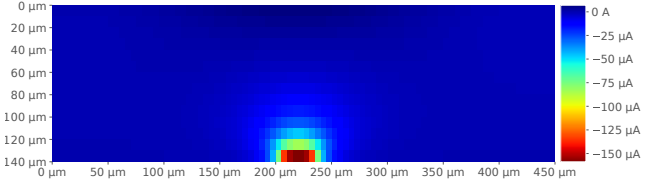


The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.

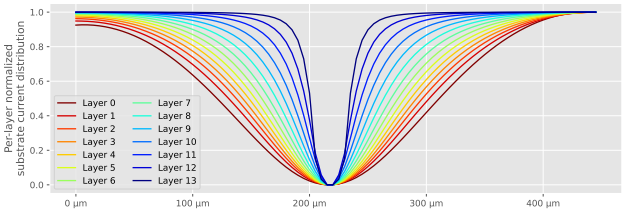


Simulation results: Triple-Well

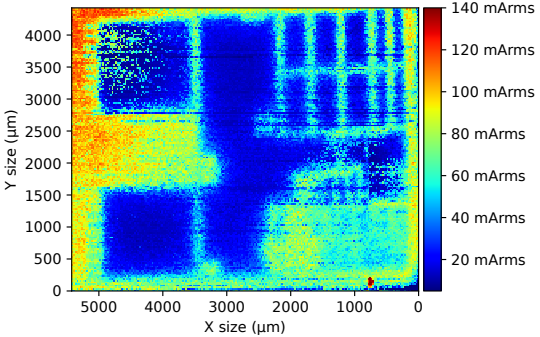


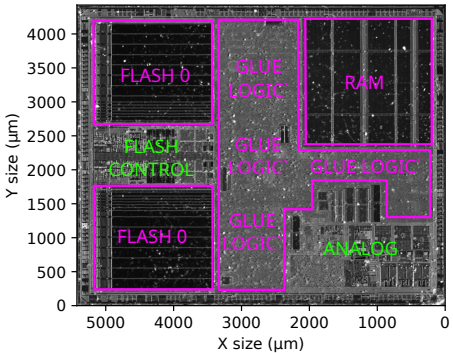


The higher the layer number, the closer to the probe.
The lower the normalized value, the higher the concentration.



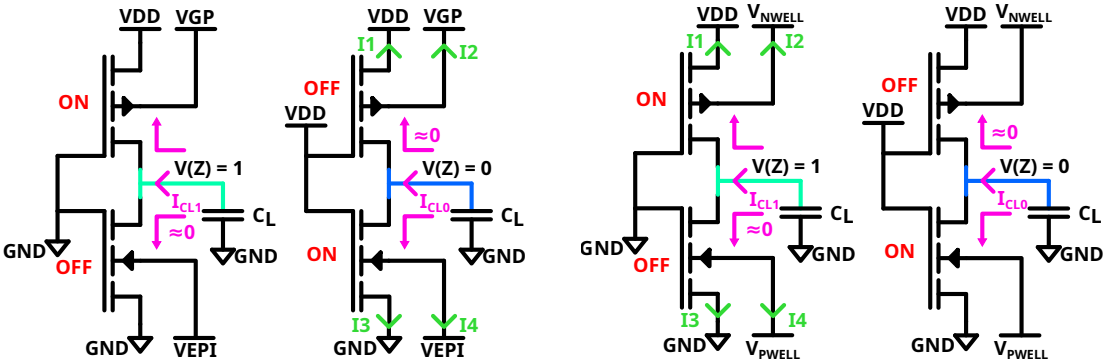
Dual-Well and Triple-well ICs in practice



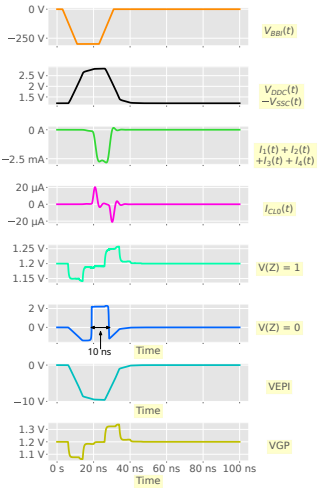


SIMULATION FLOW FOLLOW-UP

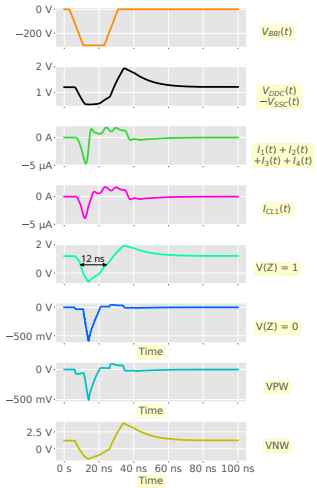
Logic gates simulations under BBI: models



Logic gates simulations under BBI: results



- Item 1
- Item 2
- Item 3

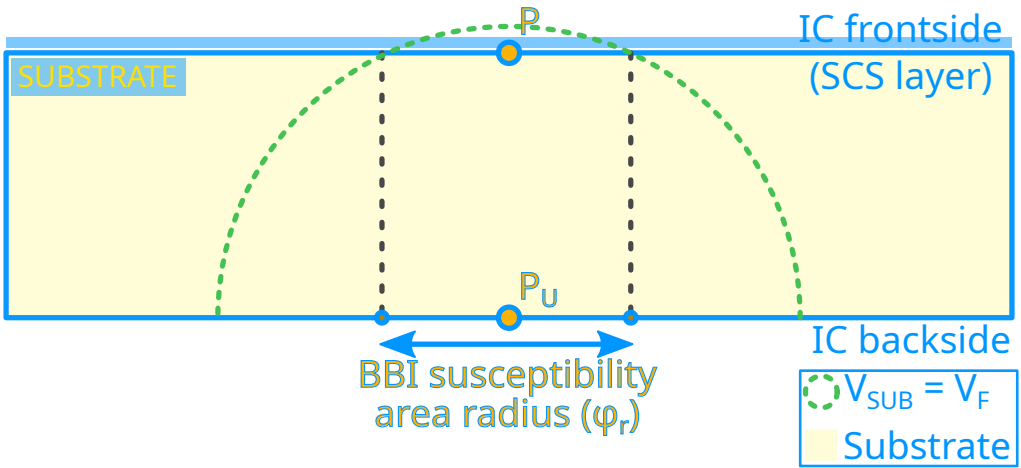


- Item 1
- Item 2
- Item 3

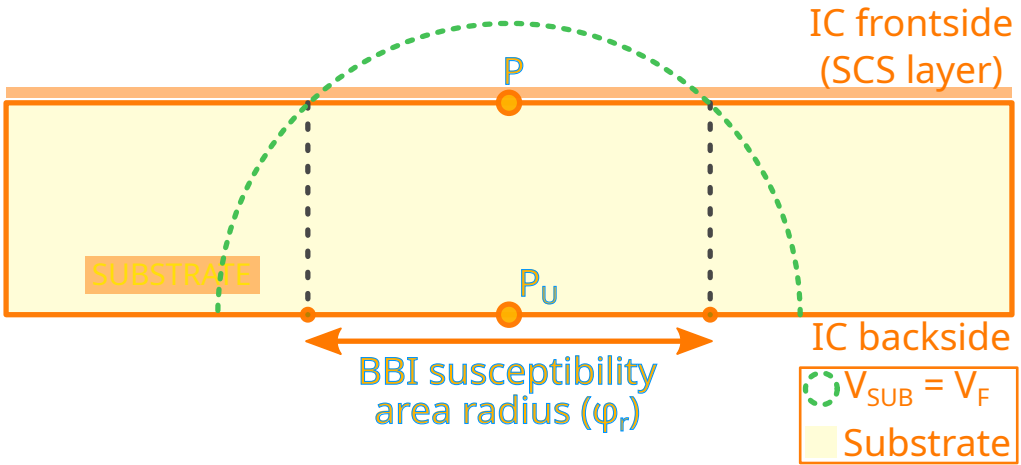
Local conclusion

SUBSTRATE TINNING ANALYSIS

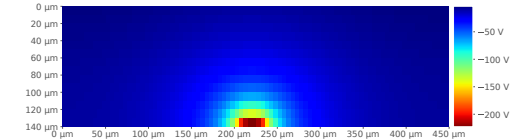
Geometric approach

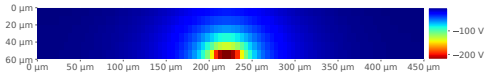


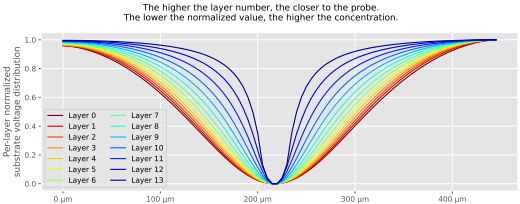
Geometric approach

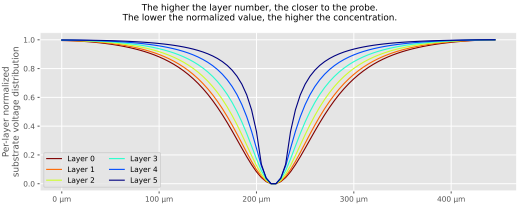


Simulation approach







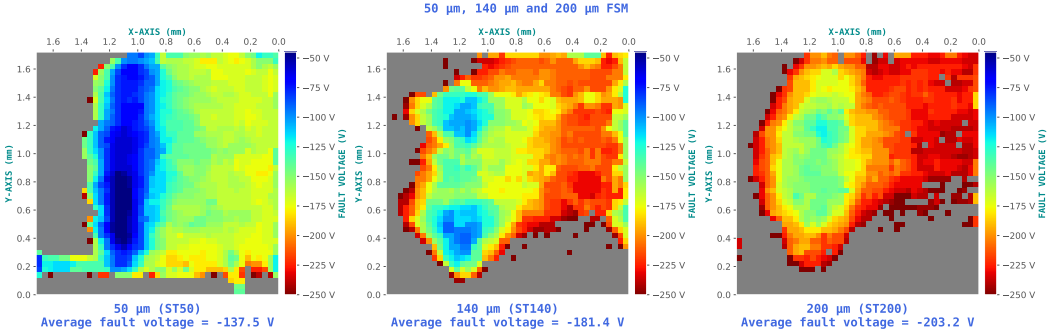


A few words on substrate thinning techniques

AJOUTER IMAGES APPAREILS AMINCISSEMENT ET EXPLICATIONS

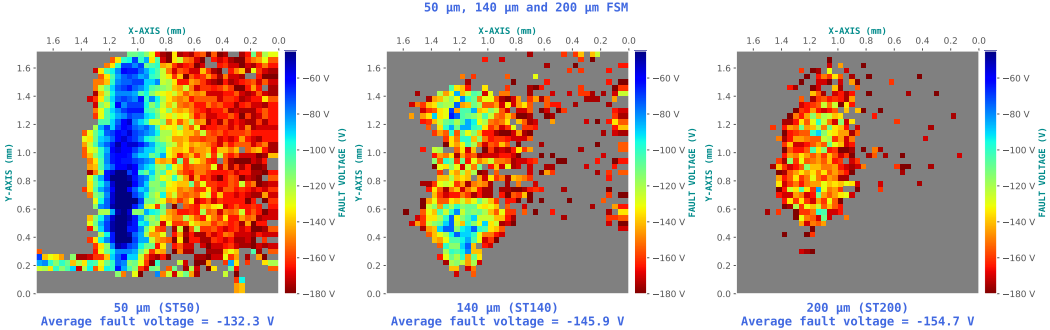
Substrate thinning in practice

Fault susceptibility maps



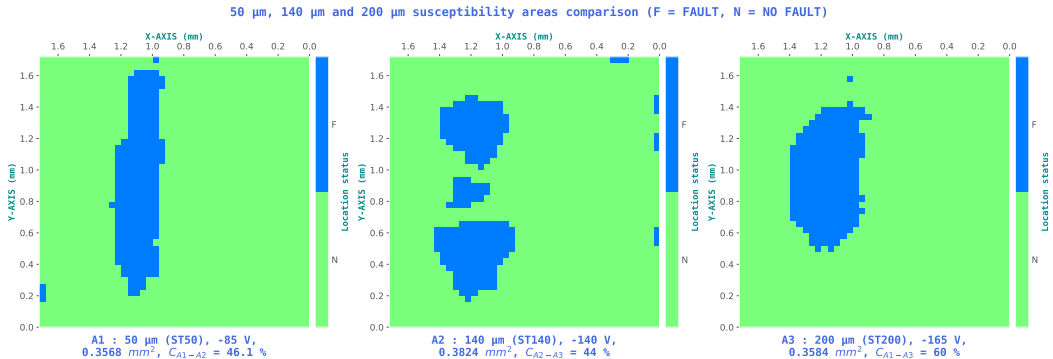
Substrate thinning in practice

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