A better practice for Body Biasing Injection

Geoffrey CHANCEL

Jean-Marc GALLIERE

Philippe MAURINE

CONTEXT & STATE OF THE ART

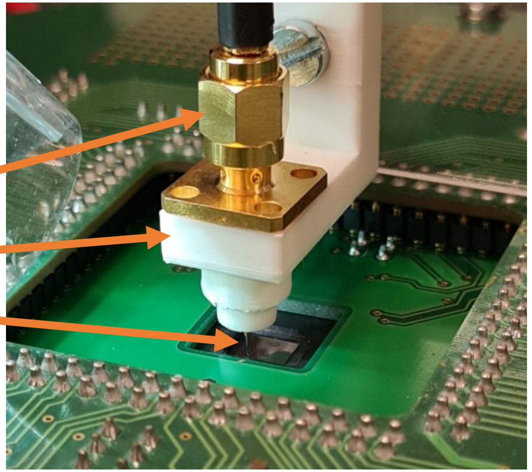
- Fault injection techniques: EMFI, LFI, BBI
- State of the art:
  - *P. Maurine et al., "Yet Another Fault Injection Technique: by Forward Body Biasing Injection"*, 2012
  - *K. Tobich et al., "Voltage Spikes on the Substrate to Obtain Timing Faults", 2013*
  - *N. Beringuier-Boher et al., "Body Biasing Injection Attacks in Practice", 2016*
  - *O'Flynn Colin, "Low-Cost Body Biasing Injection (BBI) Attacks on WLCSP Devices", 2020*
  - *G.Chancel et al., "Body Biasing Injection: To Thin or Not to Thin the Substrate?", 2022*
  - *T. Wadatsumi et al., "Voltage Surges by Backside ESD Impacts on IC Chip in Flip Chip Packaging", 2022*
  - *G. Chancel et al., "Body Biasing Injection: Impact of substrate types on the induced disturbances" 2022*

OBJECTIVES

- Introduce enhanced BBI platforms:
  - Better efficiency
  - More reproducible results
- Differential fault attack:
  - Hardware AES
  - Giraud's DFA
- BBI fault model:
  - Charge extortion

Test platform

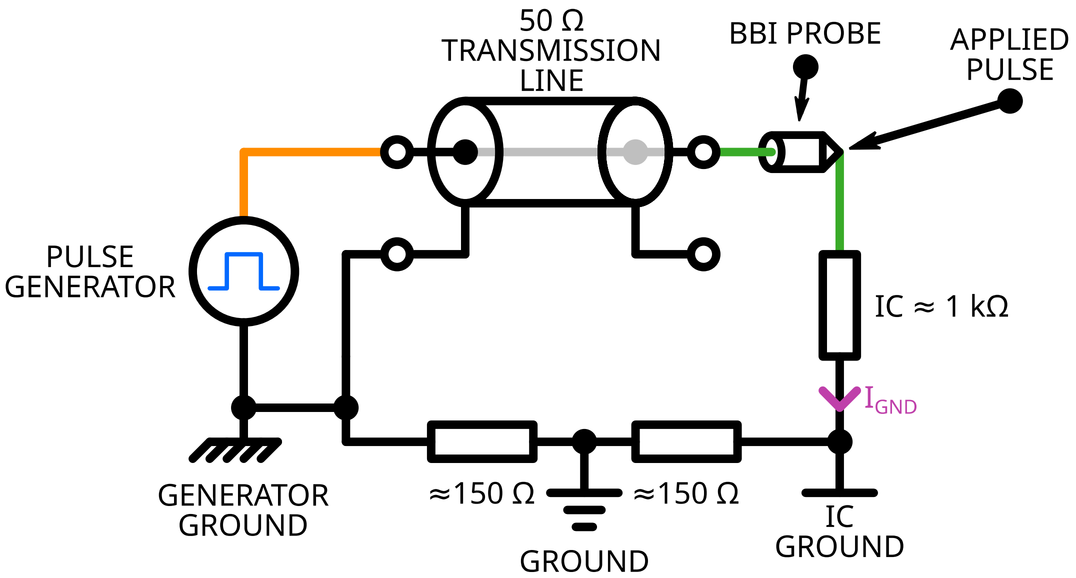
- AVTECH AVRK-4-B voltage pulse generator:
  - Amplitudes: ± 50 V to ± 750 V
  - Pulse widths: 6 ns to 20 ns
- Custom made BBI probes and support:
  - 3D-printed support
  - SMA connector
  - Pogo-pin

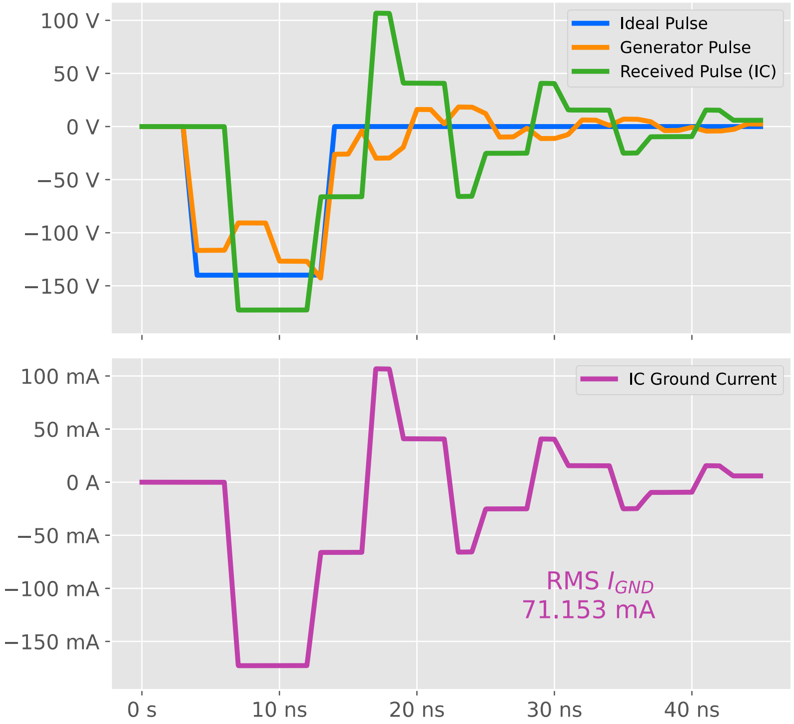


- STM32F439 32-bits microcontroller → hardware AES co-processor

BBI enhanced platforms

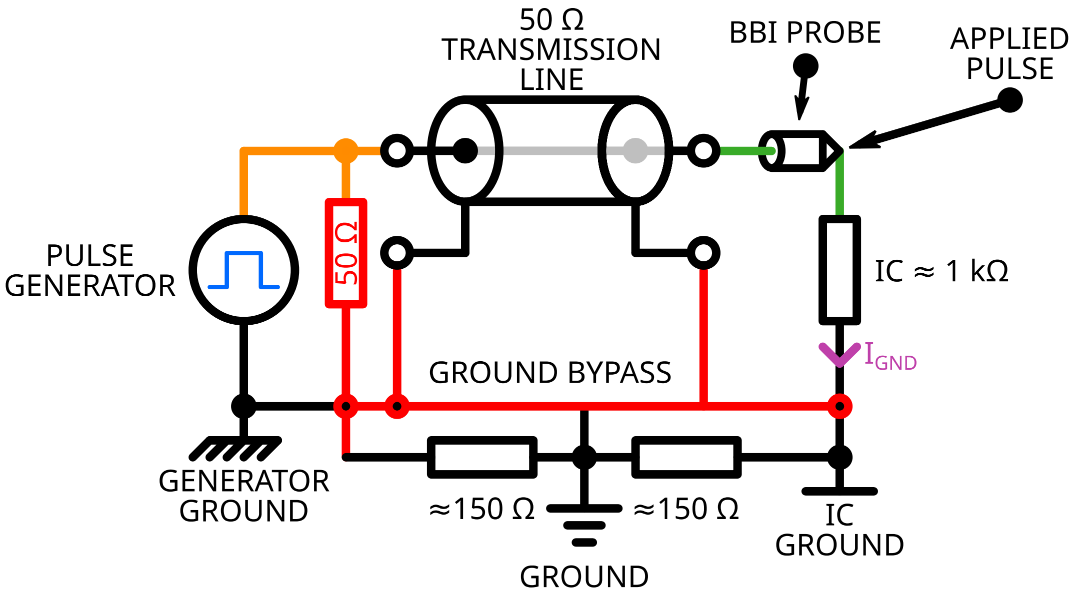
BBI in the state-of-the-art

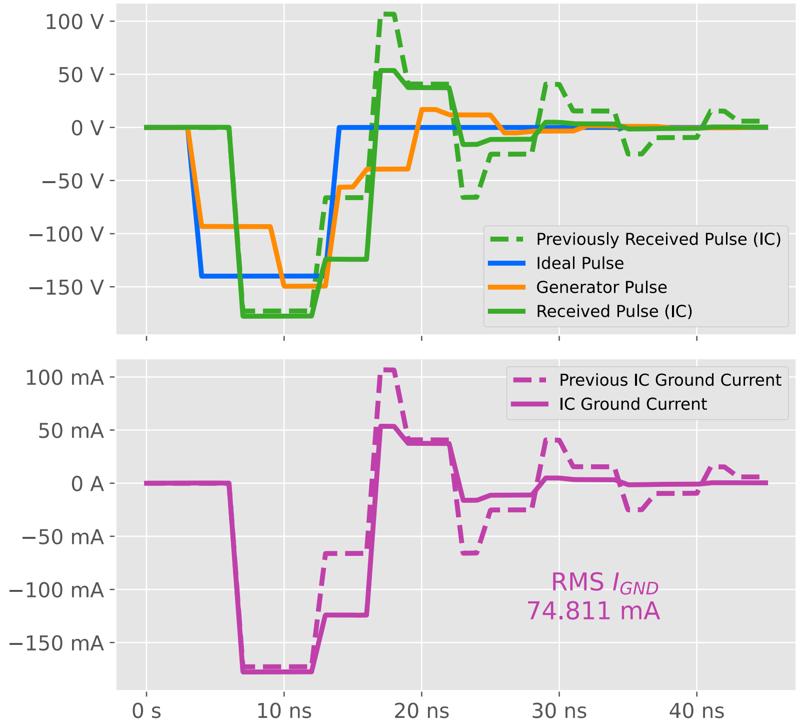




- Voltage setpoint not met:
  - Lot of ringing → impedance mismatch
  - Low-quality equipment grounding

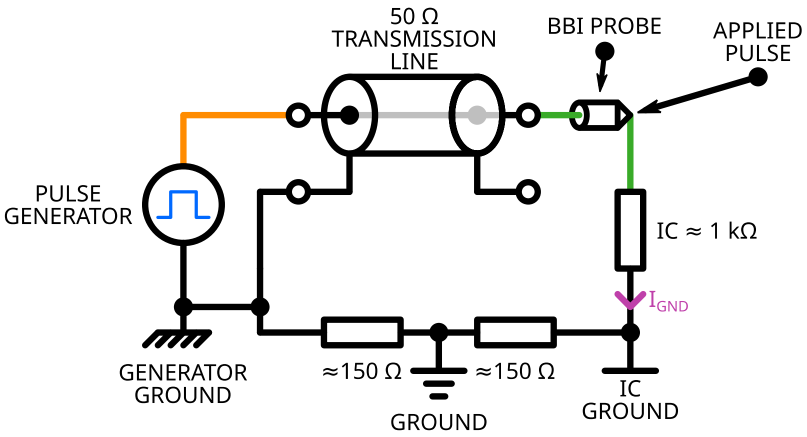
BBI enhanced platform

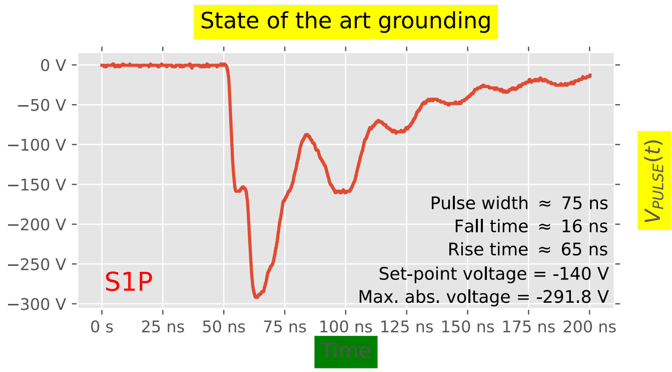


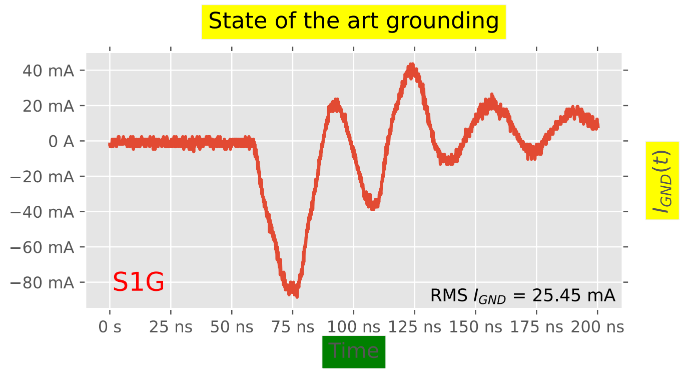


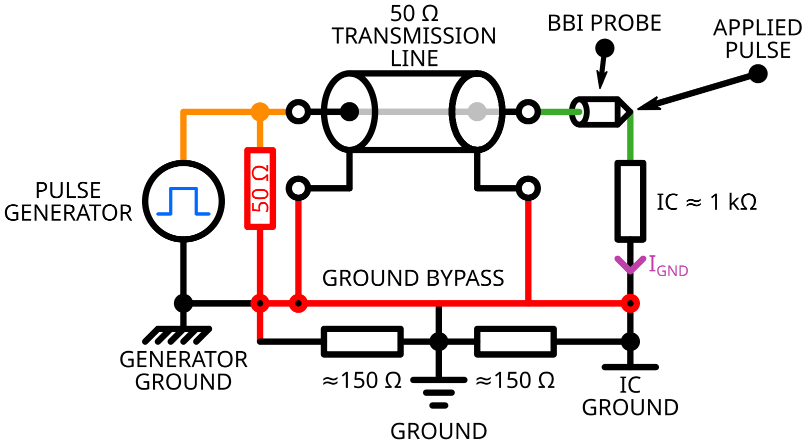
- Voltage setpoint closer to expectations
- Less ringing

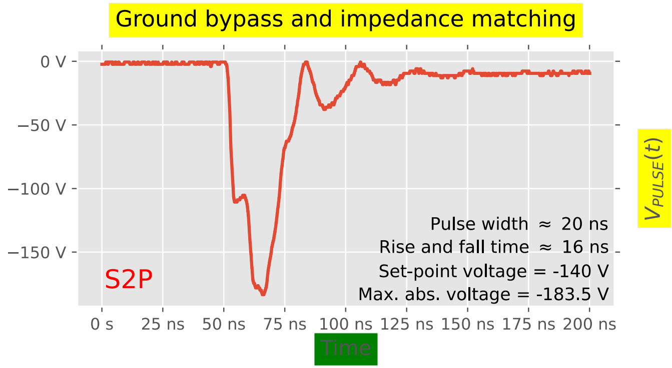
Experimental measurements

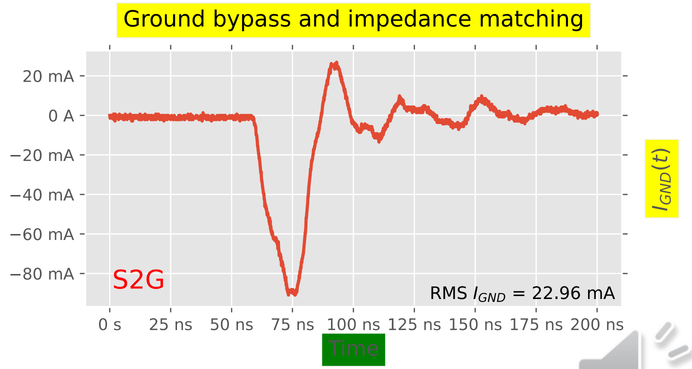










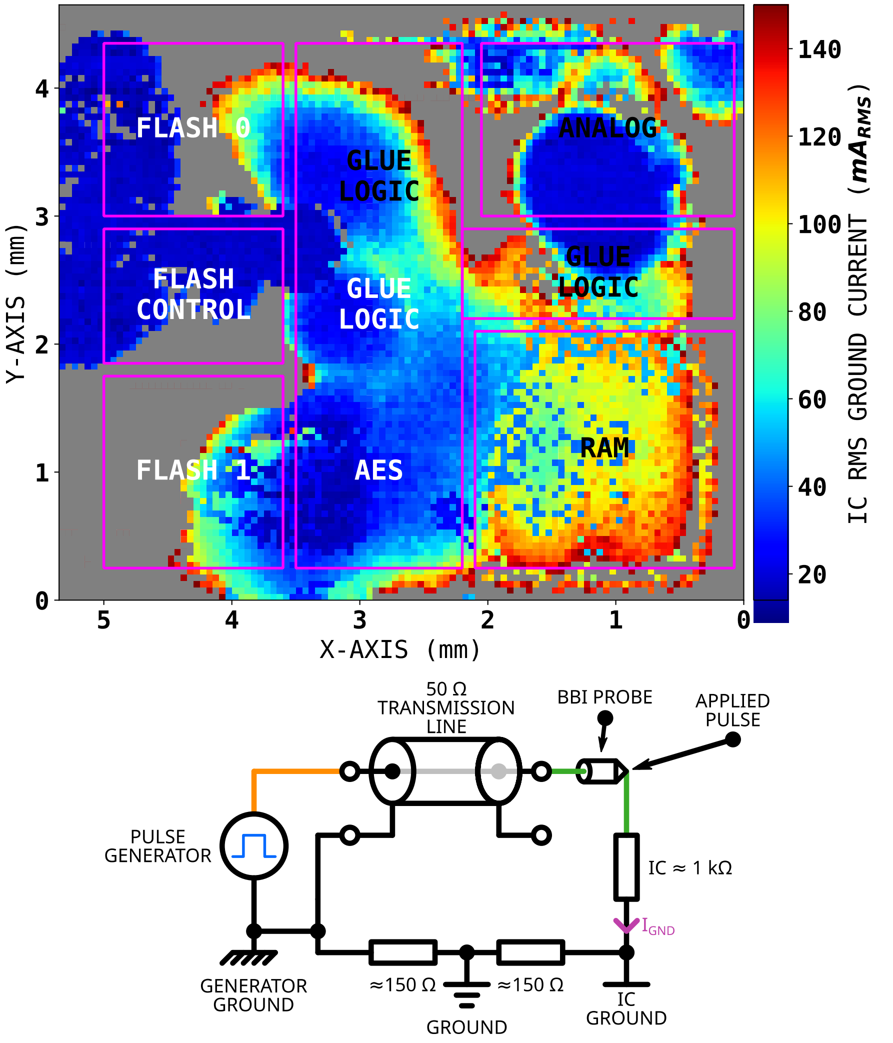


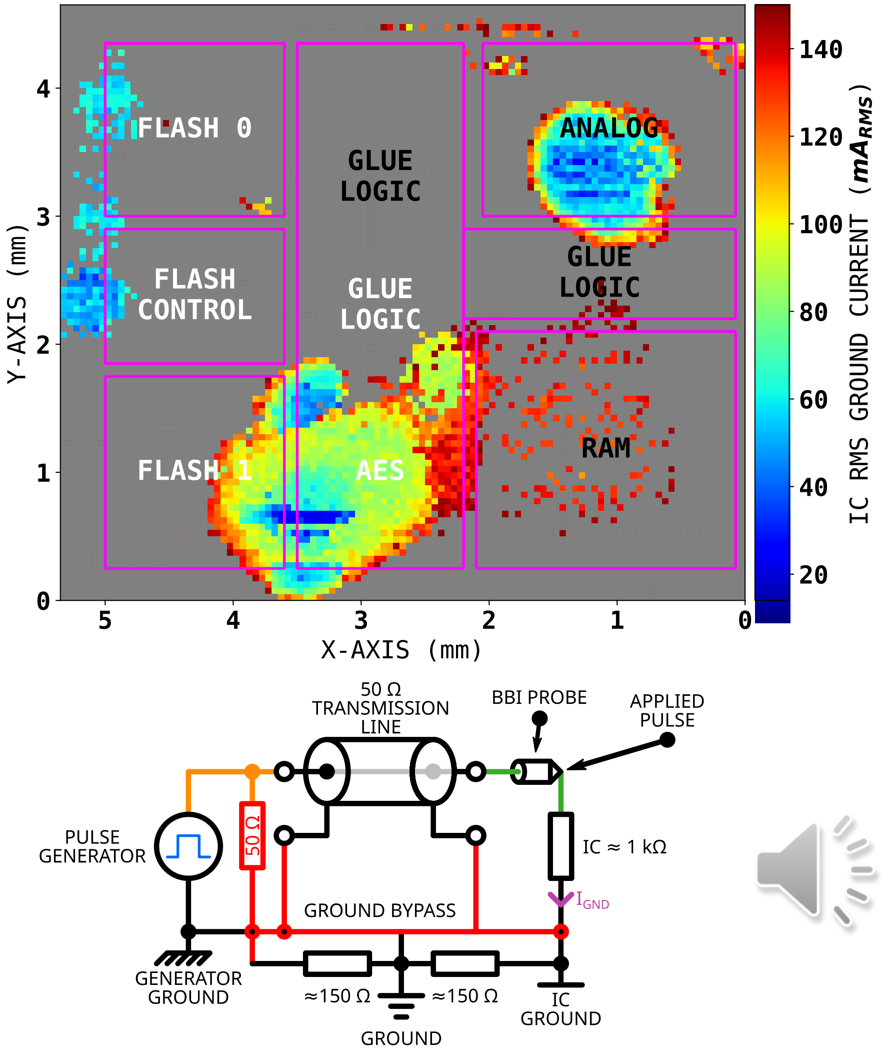
Voltage pulse generator output:
Setpoint: -140 V ; 20 ns

IC ground current

Enhancements in practice

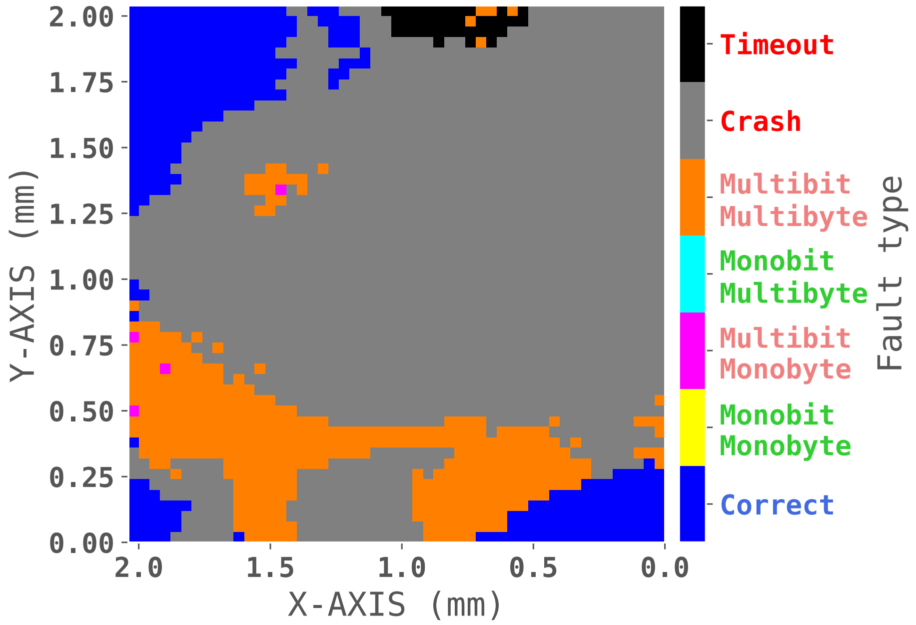
IC fault susceptibility analysis

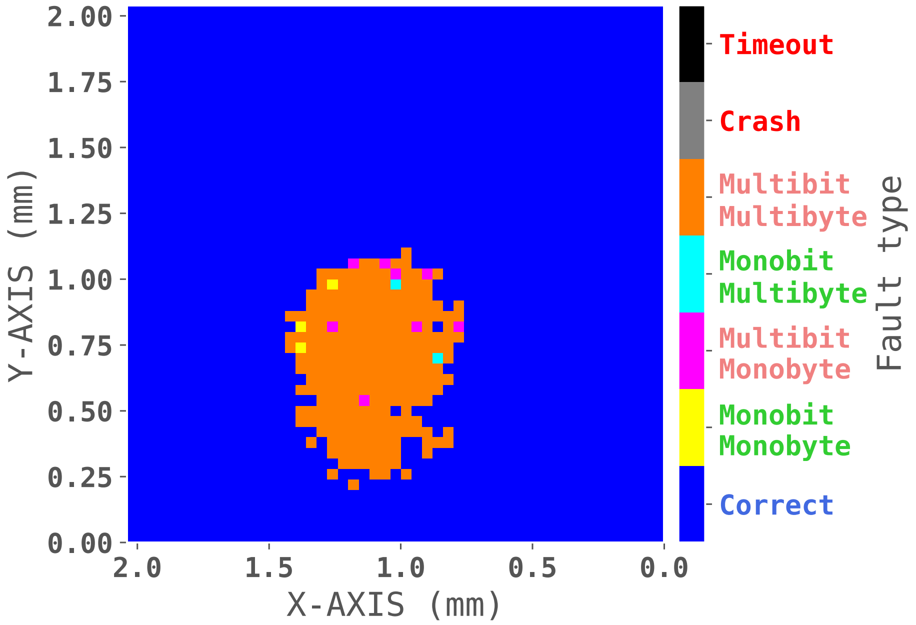


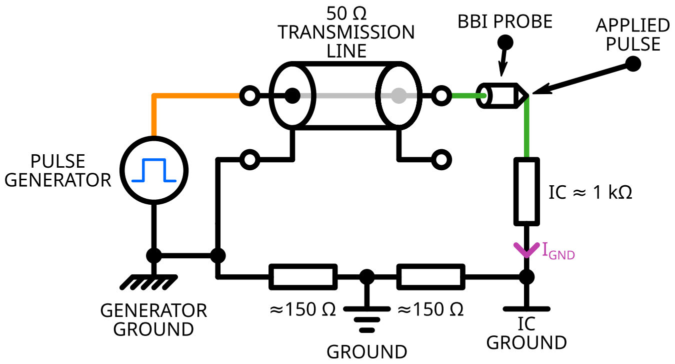


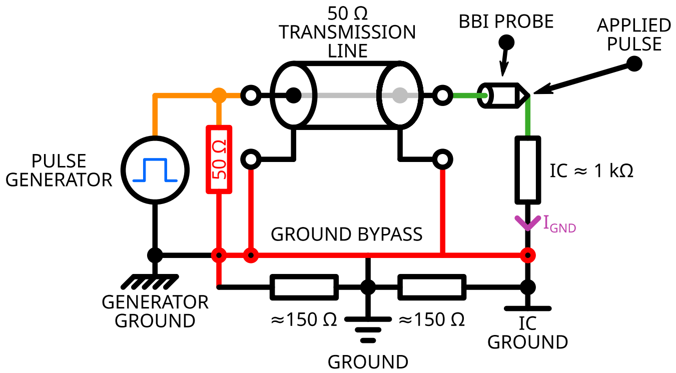
Differential fault attack in practice

Bit-fault attack on AES-128 → Giraud, 2002

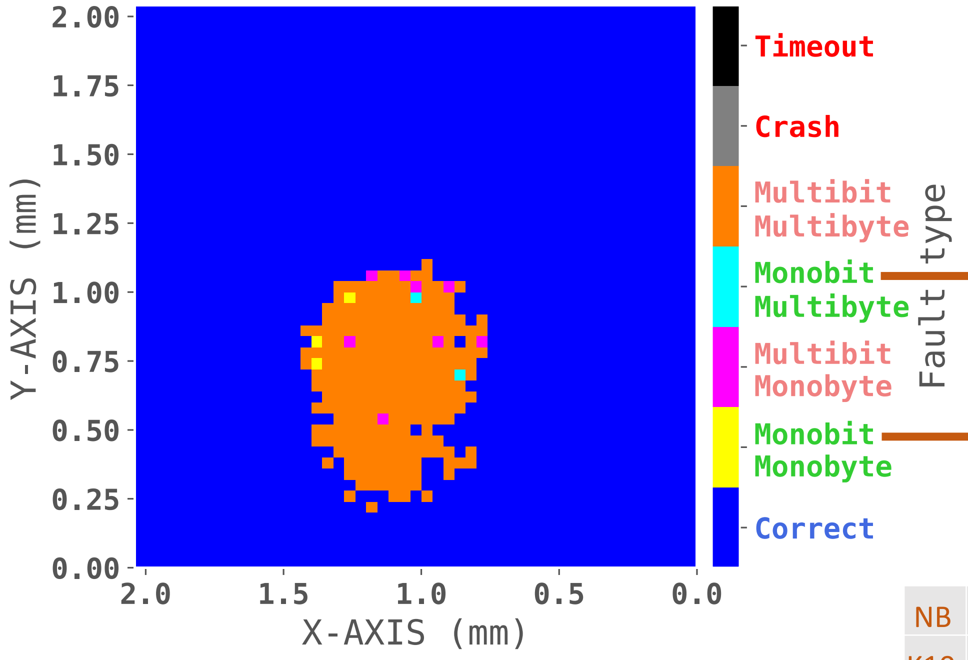








Differential fault attack in practice

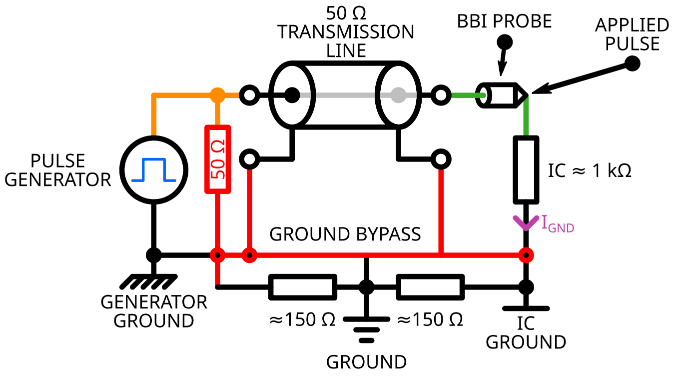


Valid faults for Giraud's monobit DFA

- Monobit faults on single bytes
- Monobit faults on multiple bytes
- Successful Giraud attack

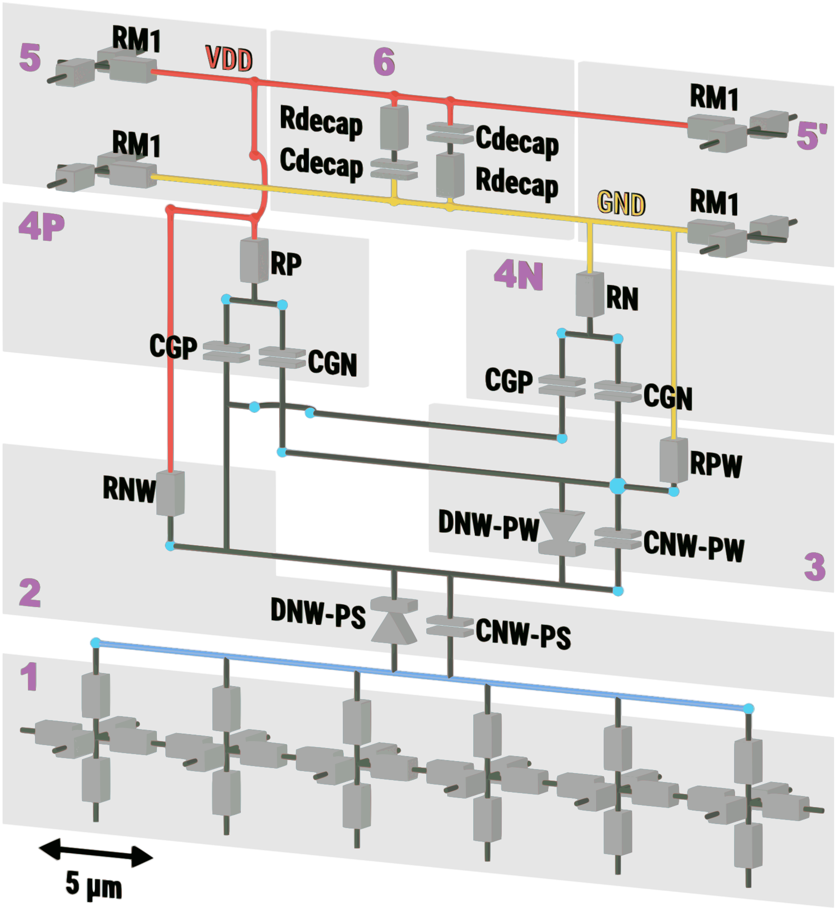
NB	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K10	0xFF	0x1F	XX	0xE8	0xEF	XX	0xA5	0x6A	0xCA	0xE7	0x55	0x3C	0xFD	0x65	0x39	0x26
KEY	0x01	0x23	0x45	0x67	0x89	0xAB	0xCD	0xEF	0xDE	0xAD	0xBE	0xEF	0x12	0x34	0x43	0x21

Retrieved K10 bytes and original AES-128 secret key

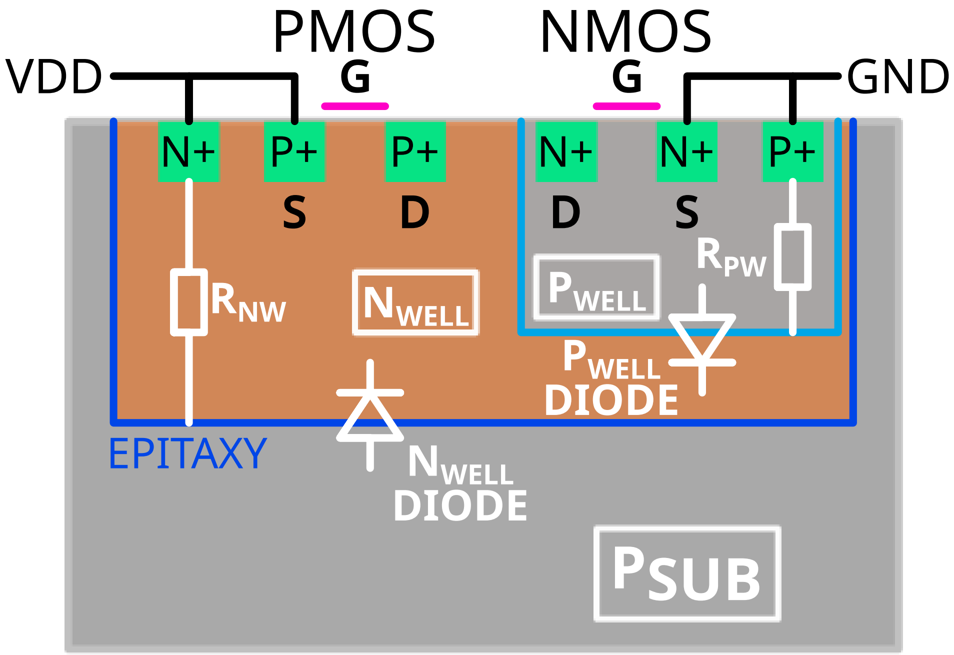


From more complex simulation models to fault model

Complex IC models: Triple-Well

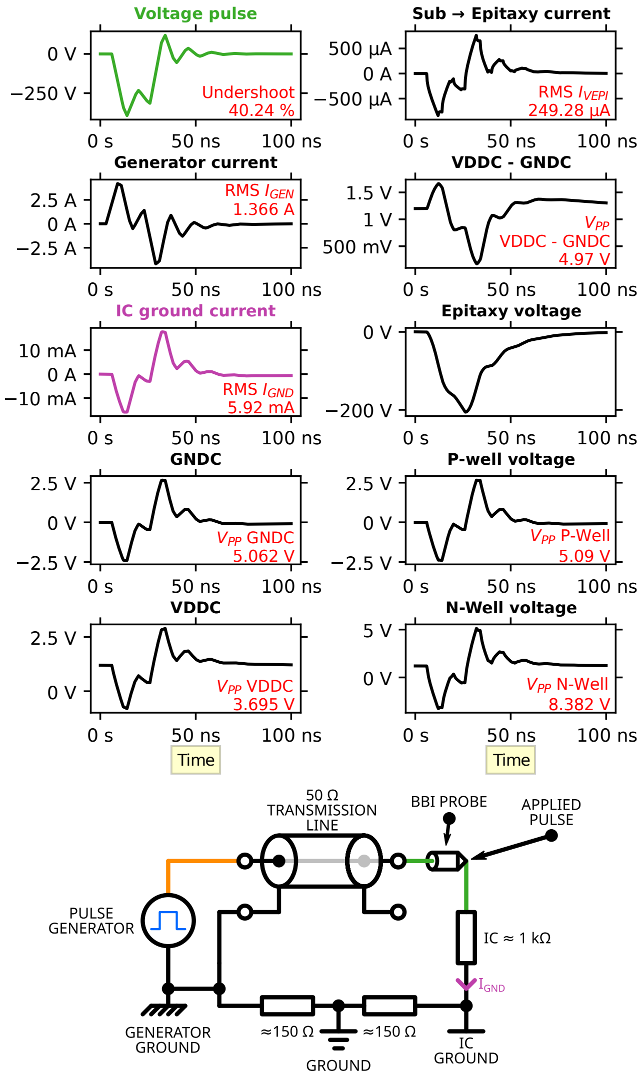


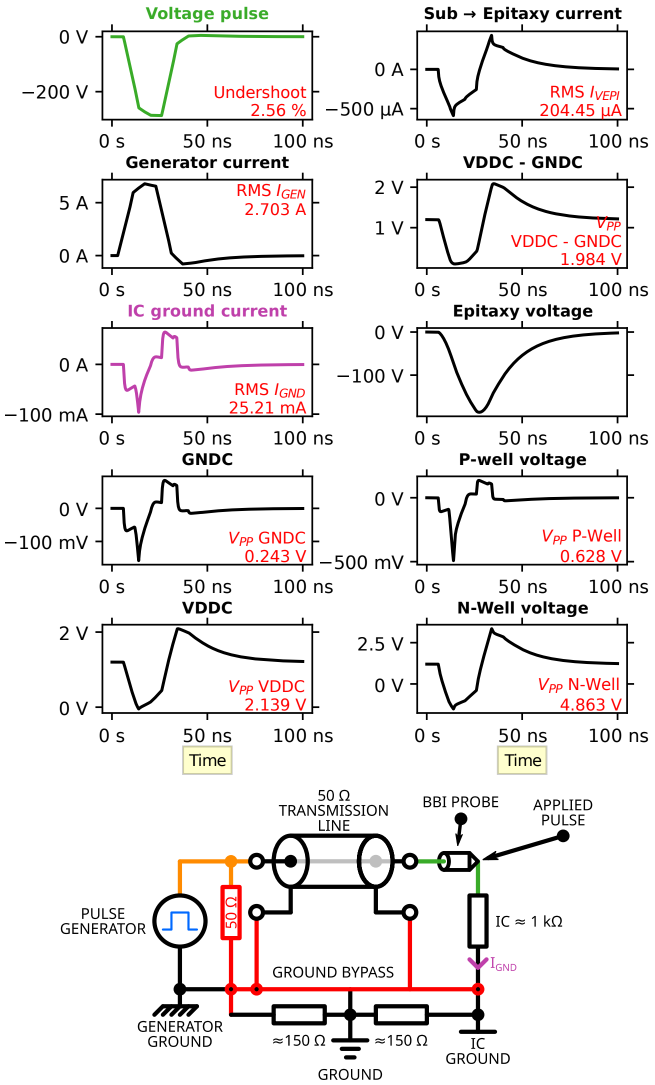
Standard-cell segment



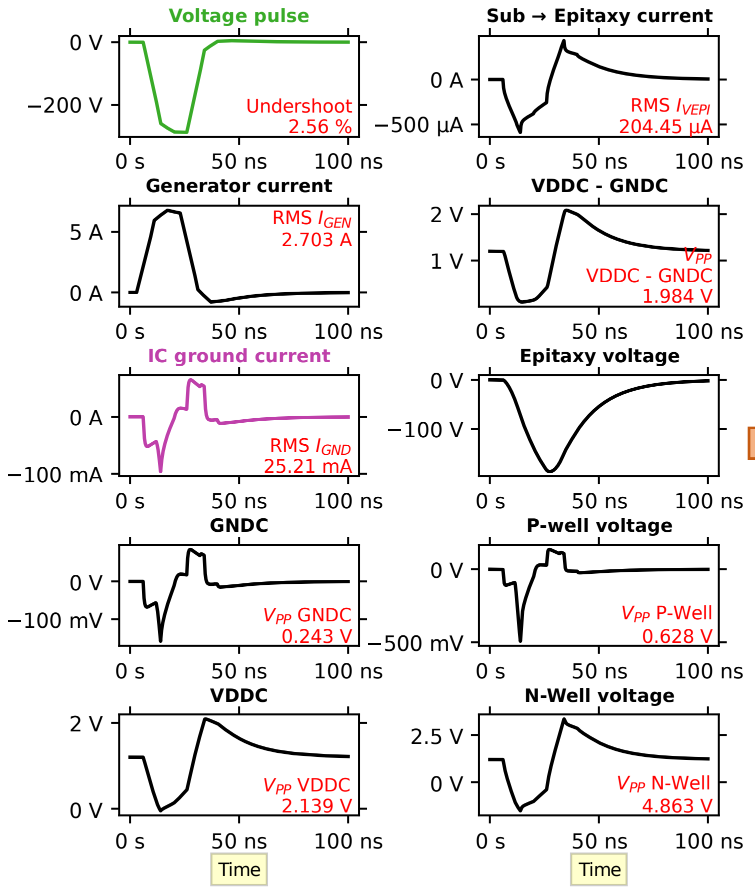
Logic inverter

Effect of enhancements on a Triple-Well IC

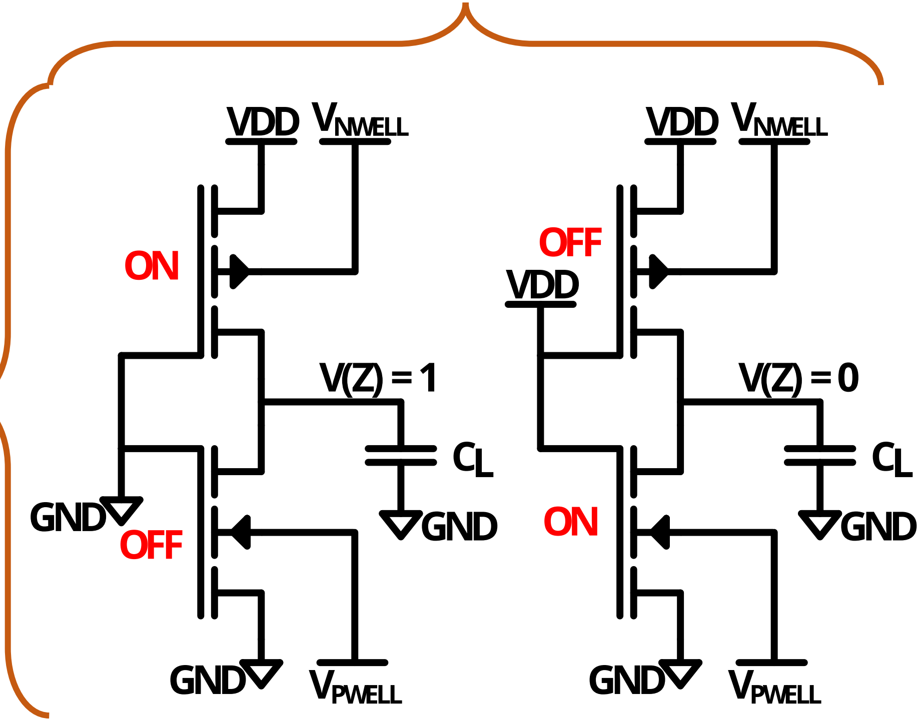




CMOS logic gates evaluation



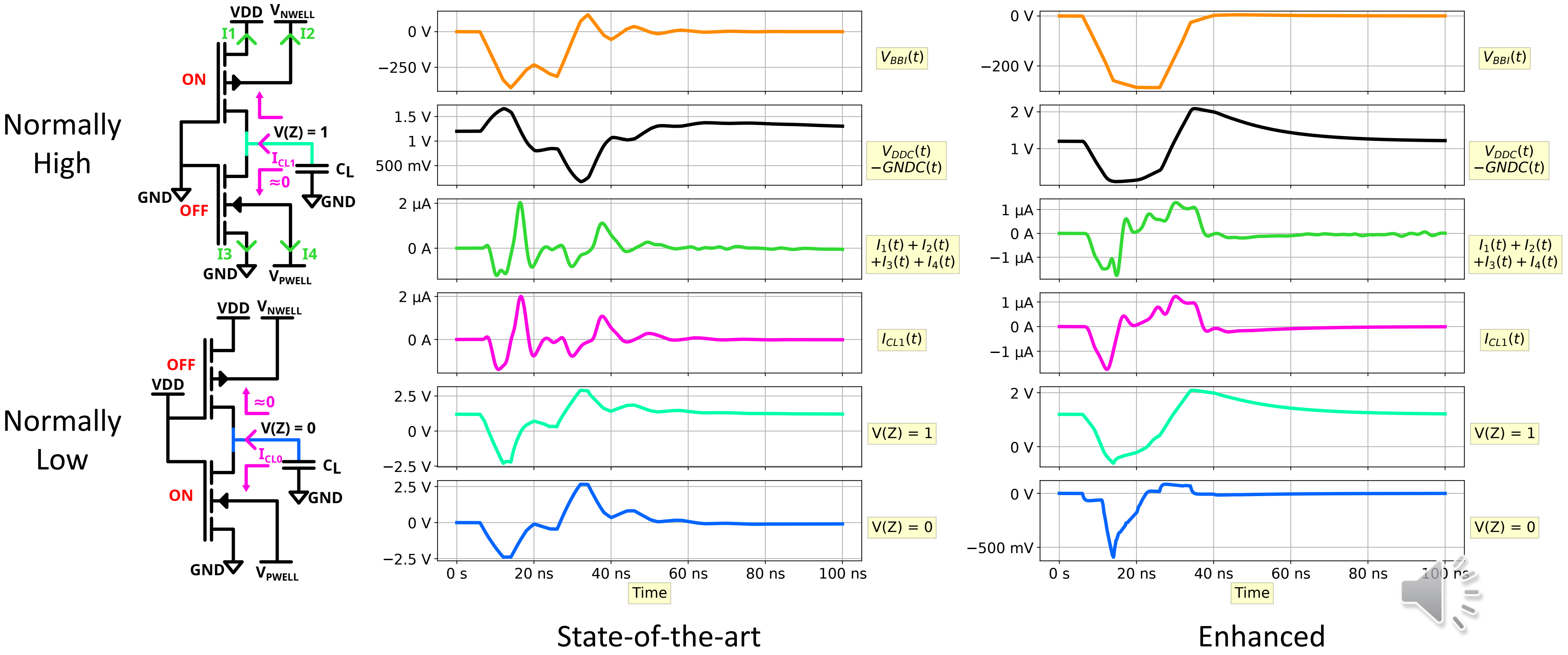
CMOS inverters



Normally high

Normally low

BBI impact on CMOS logic gates



Conclusion

- Enhanced BBI platforms:
  - Generator impedance matching
  - Platform parameters requirements met (PW, voltage…)
  - Better repeatability
  - Giraud’s single-bit DFA feasible
  - New step in simulation flow → logic gates disturbances simulations