

Do MCUs Dream of Electric Earth?

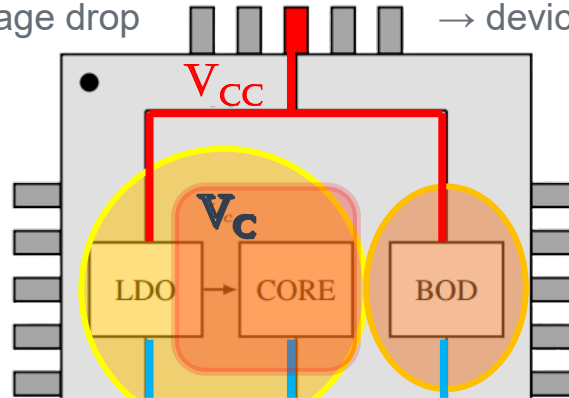
Revisiting Voltage Fault Injection Through Ground Manipulation

Khani Marvin Saß · Ran Zhang · Jean-Pierre Seifert

Security in Telecommunications (SecT) · TU Berlin

Motivation & Problem

- LDO regulators and Brown-Out Detection (BOD) are reliability features but widely assumed to also protect against voltage fault injection.
- Conventional V_{CC} -side voltage fault injection (VFI):
 - LDO attenuates the glitch → core voltage remains stable
 - BOD detects the voltage drop → device resets



Research Question: Can a single inverted fault simultaneously bypass both the internal voltage regulator and brown-out detection?

Background: LDO & BOD — Both Reference On-Die GND

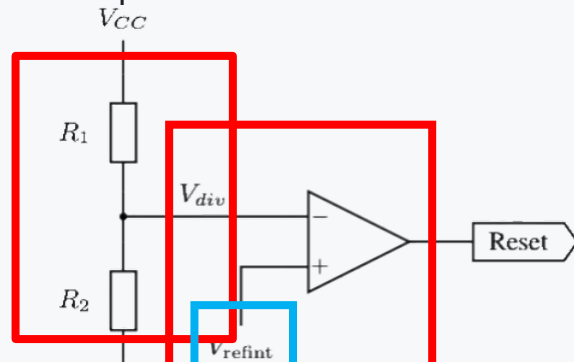
Internal LDO Regulator

- Error amplifier + pass transistor
- Regulates V_{core} from external V_{CC}
- Bandgap V_{ref} tied to on-die GND
- Loop BW ~ 1 MHz (slow vs ns edges)



Brown-Out Detection (BOD/BOR)

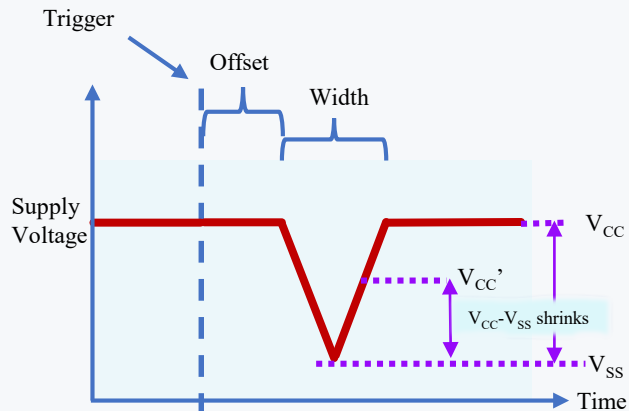
- Resistive divider taps $V_{CC} \rightarrow V_{div}$
- Comparator: reset if $V_{div} < V_{refint}$
- V_{refint} = bandgap, also tied to on-die GND
- Multiple BOR levels



Key insight: Both loops are referenced to on-die GND — this is the attack surface

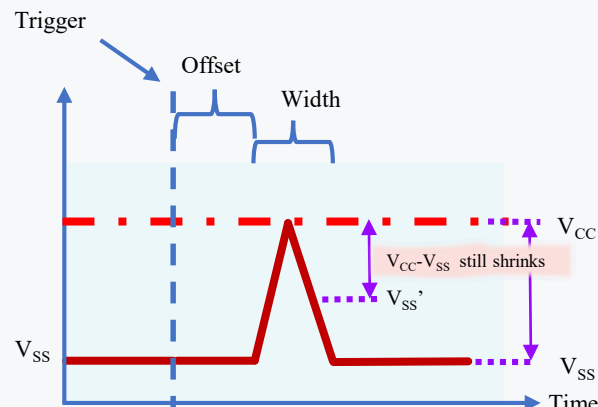
Key Idea: The Inverted Fault

Conventional (V_{CC} -side)



- LDO sees V_{CC} drop $\rightarrow$ compensates
- BOD triggers reset $\times$

Inverted (GND-side) ★



- LDO reference rides with GND $\rightarrow$ blind
- BOD sees V_{div} rise $\rightarrow$ no reset $\checkmark$

Same rail-to-rail collapse, opposite detector response

A fast GND edge outruns every slow loop referenced to on-die ground

Analytical Model: Core Collapse + BOD Evasion

① Core Collapse (LDO bypass)

$$V_{\text{core}} = V_{\text{nom}} - \alpha \cdot \varepsilon$$

- ε = ground lift amplitude
- $\alpha \approx 1$: V_c pinned near V_{CC} (slow loop)
- BW ~ 1 MHz $\ll$ ns-edge $\rightarrow$ collapse persists

② BOD Evasion

$$V_{\text{div}} = k \cdot V_{CC} + (1-k) \cdot V_{SS}$$

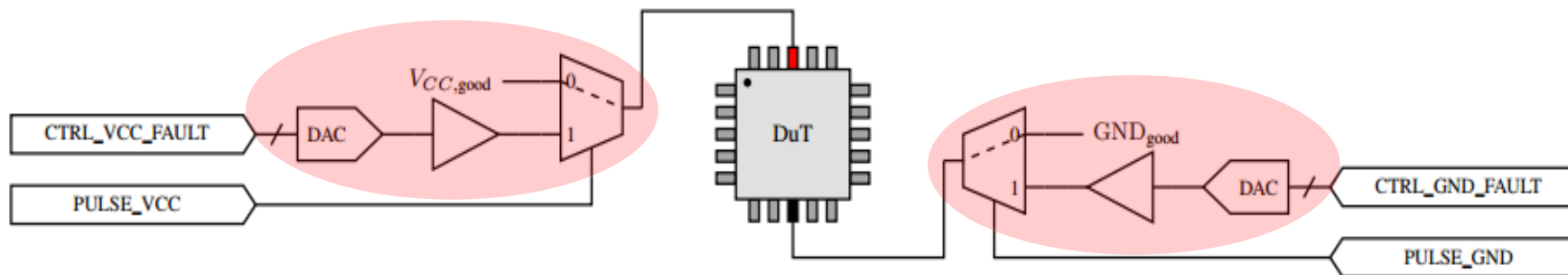
- $\partial V_{\text{div}} / \partial V_{SS} = (1-k) > 0$
- Lifting V_{SS} raises $V_{\text{div}} \rightarrow$ away from reset
- vs. V_{CC} -side: dropping V_{CC} lowers $V_{\text{div}} \rightarrow$ reset!

Unified mechanism: A fast GND edge outruns a slow loop referenced to the lifted ground

Injection Asymmetry

	Rail effect	Vdiv effect	BOD?
$V_{CC} \downarrow$	$V_{CC}-V_{SS} \downarrow$	$V_{\text{div}} \downarrow$	RESET
$V_{SS} \uparrow$	$V_{CC}-V_{SS} \downarrow$	$V_{\text{div}} \uparrow$	NO RESET

Experimental Setup



- **Dual-rail MUX injector** — mirrors VCC modulation onto GND
- **FPGA-controlled timing** — clock, trigger, MUX select pulses
- **Monte Carlo sweep** — offset $\times$ width $\times$ depth, 1M+ attempts per target

Target Platforms

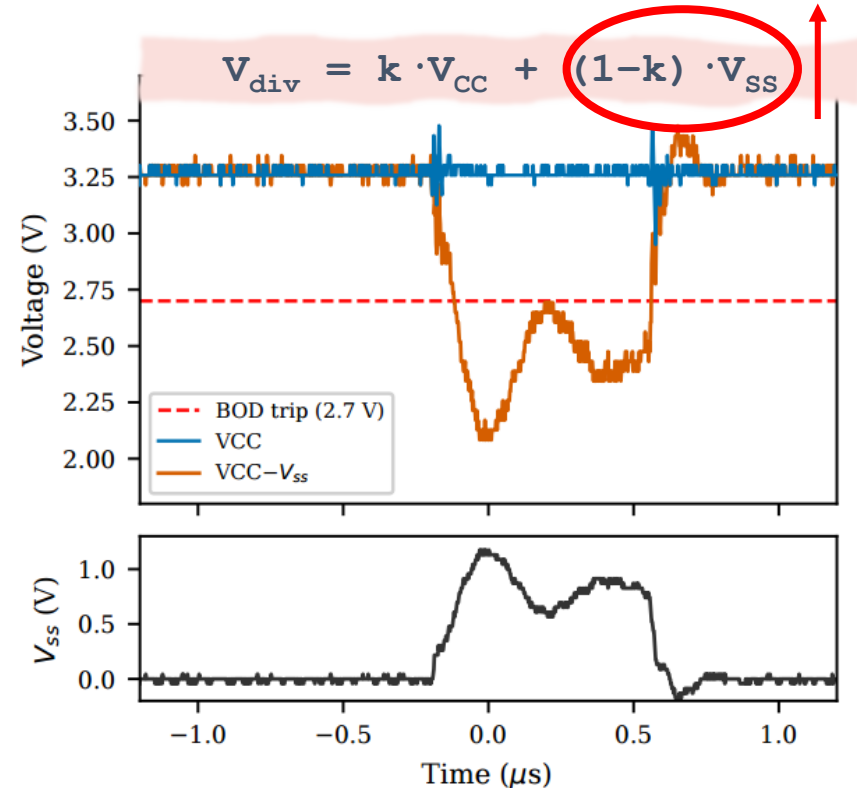
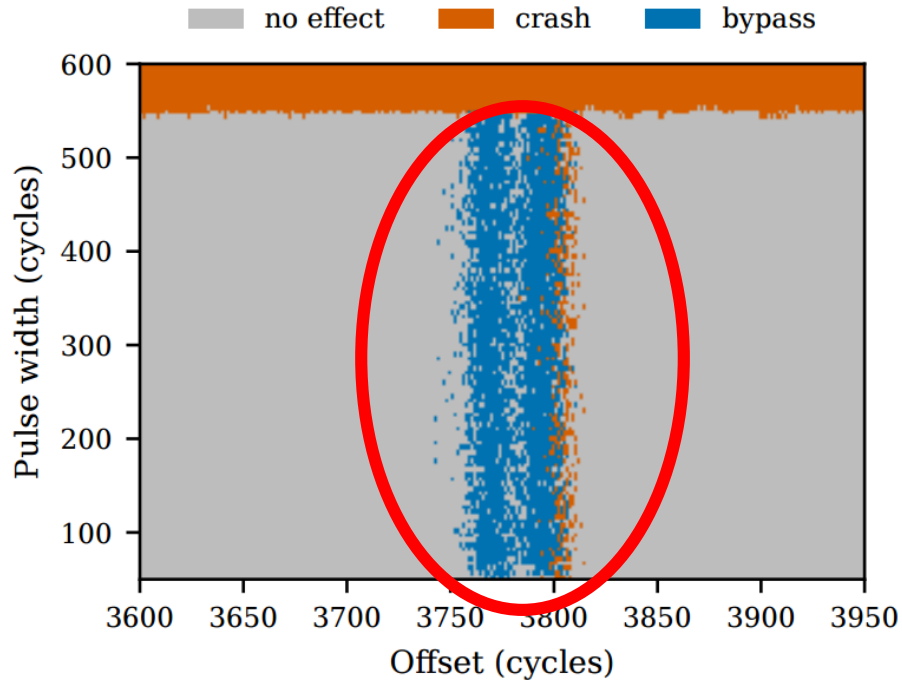
Target	Architecture	Internal LDO	BOD/BOR levels	Core exposed
ATmega328P	AVR 8-bit	No	BODLEVEL1 ----- 1.8V BODLEVEL2 ----- 2.7V BODLEVEL3 ----- 4.3V	Yes
STM32F446	Cortex-M4	Yes (1.2V)	V_{BOR1} ----- 2.13V V_{BOR2} ----- 2.44V V_{BOR3} ----- 2.75V	Yes (VCAP)
STM32F302	Cortex-M4	Yes	BOR (always-on)	No

Progression: No LDO → LDO + exposed core → LDO + hidden core + always-on BOR → dedicated detector

Results: ATmega328P (No LDO — Pure BOD Bypass)

V_{SS} Side: **6.67%** bypass rate (20,721 bypasses / 310,603 attempts)

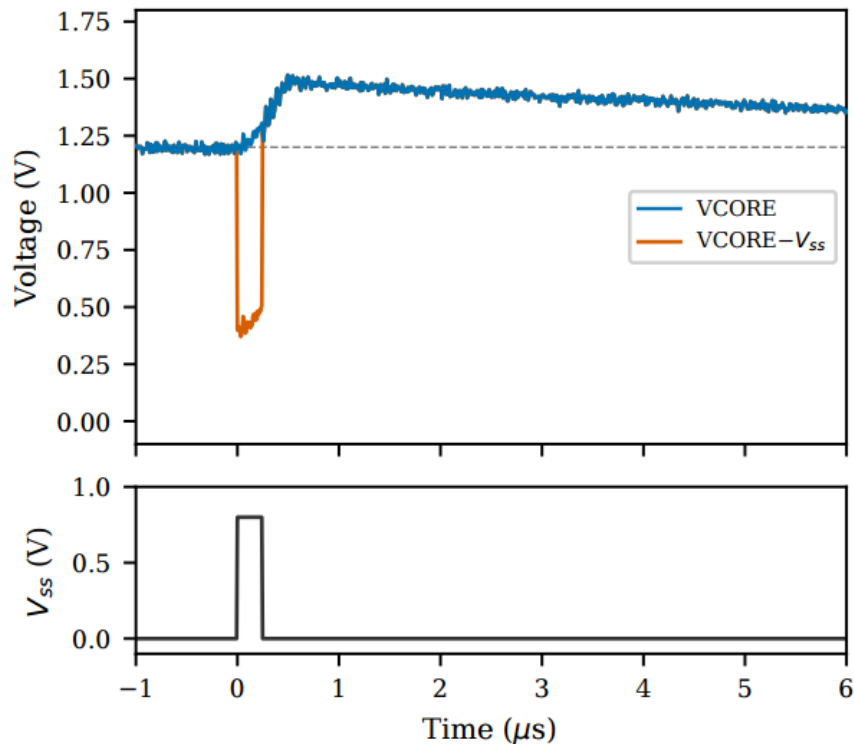
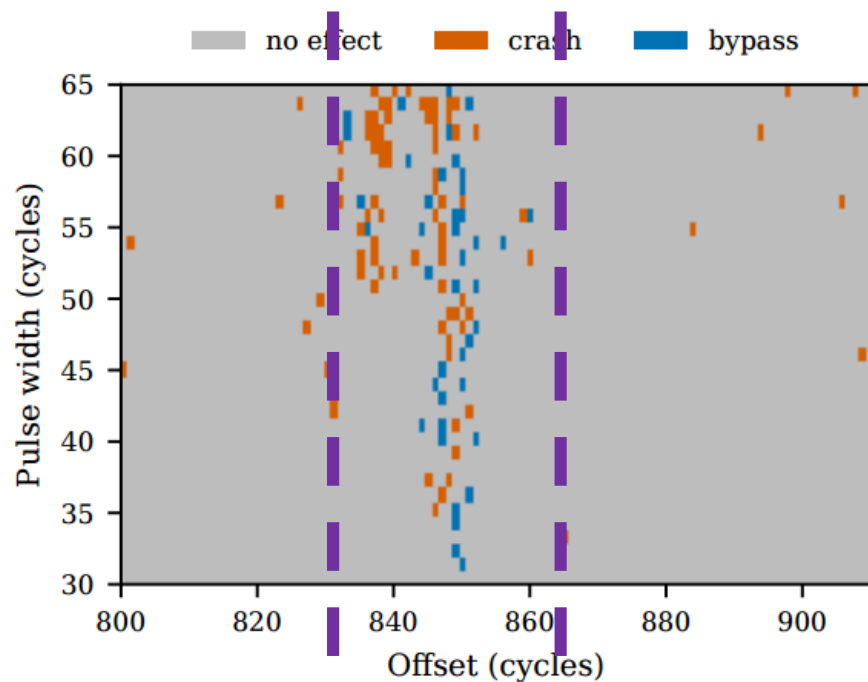
V_{CC} Side: **0%** bypass rate



Results: STM32F446 (LDO + Exposed V_{CAP})

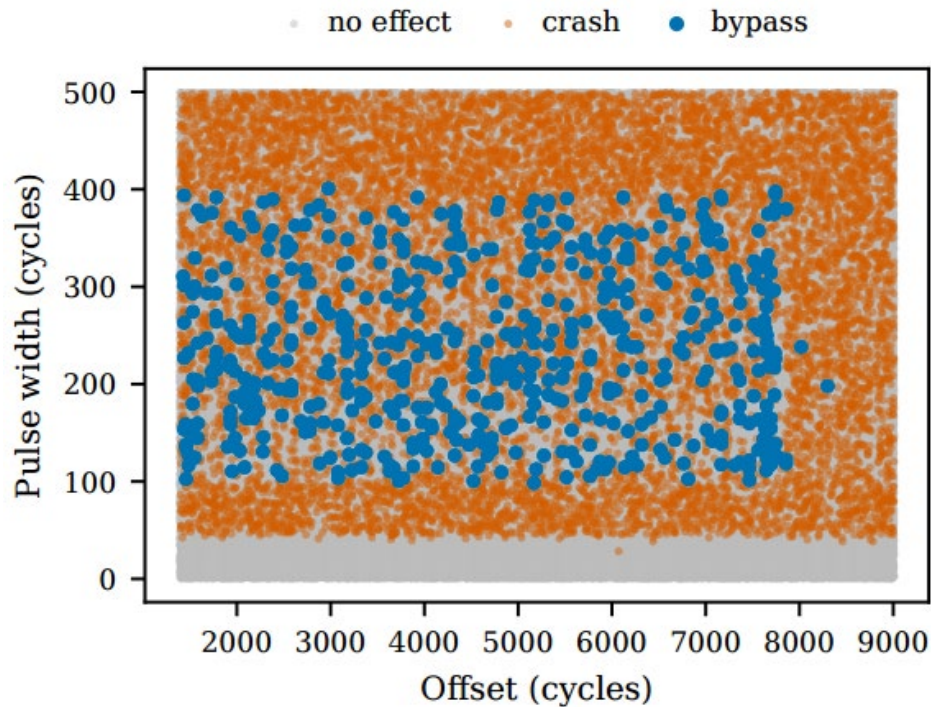
V_{SS} Side: **≈0.13%** bypass rate (93 bypasses / 74,127 attempts)

V_{CC} Side: **0%** bypass rate



Results: STM32F302

(LDO + Non-Exposed Core + Always-On BOR)



- No exposed core rail
Cannot measure, cannot disable BOR
- 567 bypasses / 292,263 attempts
Scattered among crashes
- VCC-side: 0%

Results & Takeaway

	Protection	GND-side bypasses	GND rate	VCC-side
ATmega328P	BOD only	20,721 / 310,603	6.67%	0%
STM32F446				
STM32F302				

- **One inverted**

Lifting GND

VCC-side h

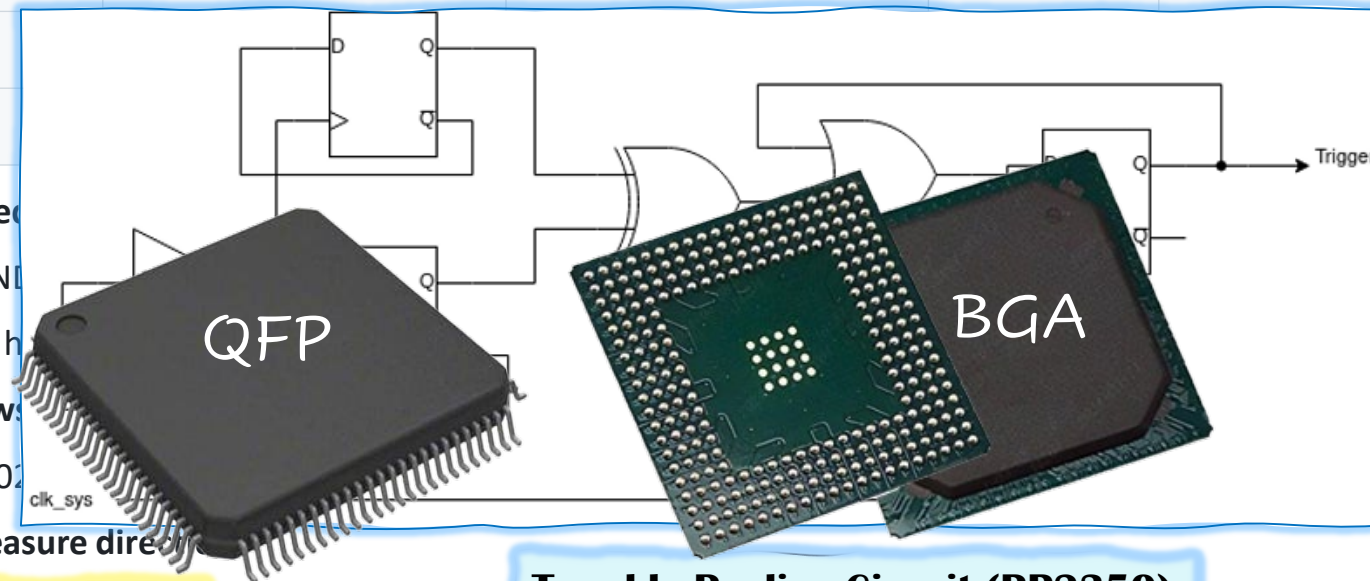
- **LDO narrow**

STM32F302

- **Countermeasure directly**

Monitor **timing margin**, not supply voltage

- **Limitation** : Package dependent (QFP vs BGA)



Tunable Replica Circuit (RP2350)

Thank You

Questions?

Ran Zhang · Xhani Marvin Saß · Jean-Pierre Seifert

