JOE GRAND

Press for SAFE
Hold for ARM
Use NewAE
Probes Only.
Status
Ready
Pulse
ARM
Fault
Open
Replace probe tip.
Hold ARM to reset.
PULSE
CW520

SHOT THROUGH THE HEART

- Introduction to fault injection aka "glitching"
- Intentionally cause a fault in the target device
  - Typically used against cryptographic operations or microcontroller security (debug port access / code protection)

FAULT INJECTION

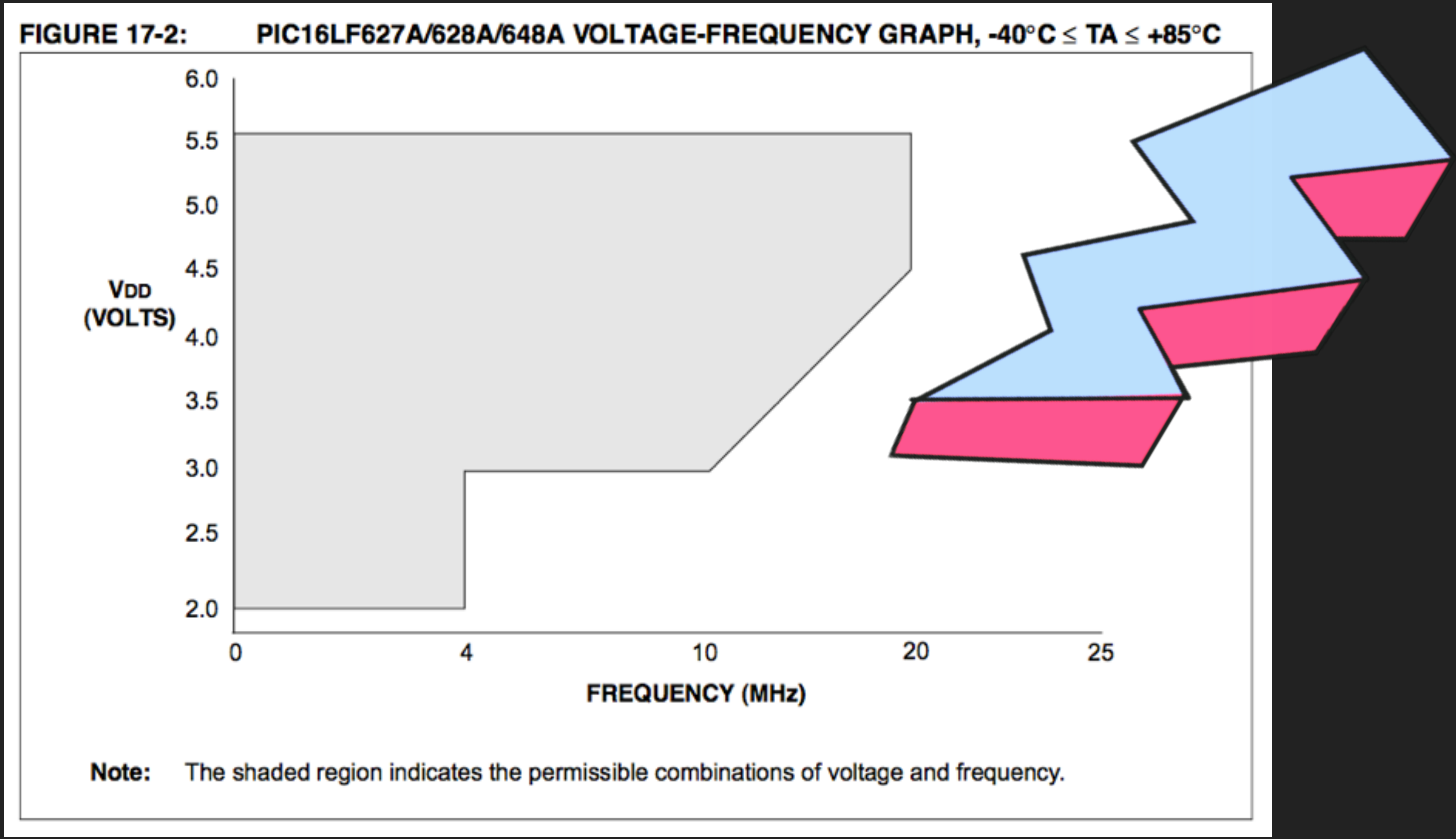


FIGURE 17-2: PIC16LF627A/628A/648A VOLTAGE-FREQUENCY GRAPH, -40°C ≤ TA ≤ +85°C

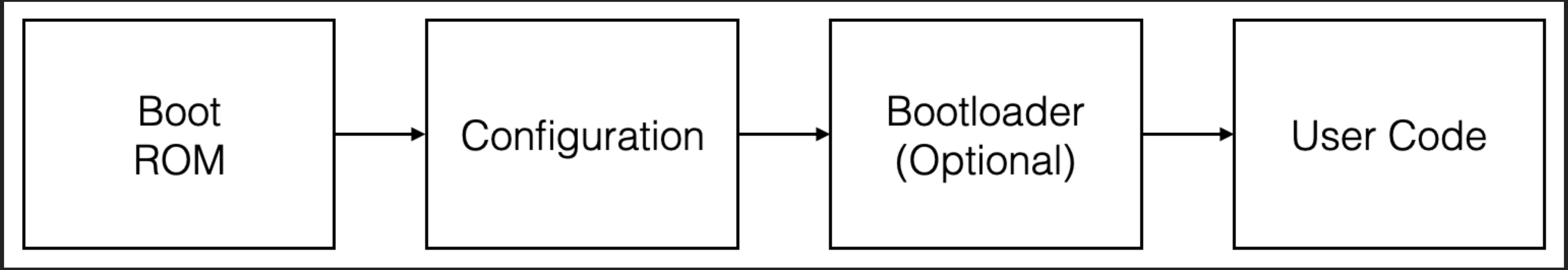
Note: The shaded region indicates the permissible combinations of voltage and frequency.

RESULTING BEHAVIORS

- System reset / halt
- Change in software decision
    - Skip an instruction
    - Affect branching
- Computational fault
    - Instruction decoding errors
    - Malformed data read / write

MICROCONTROLLER SECURITY

- Protects MCU internal memory, debug interfaces
  - May require fuse/register setting, password, challenge/response
  - Reduce access (allow subset of functionality)
  - "Permanently" disable access
- Configured/checked during chip boot process

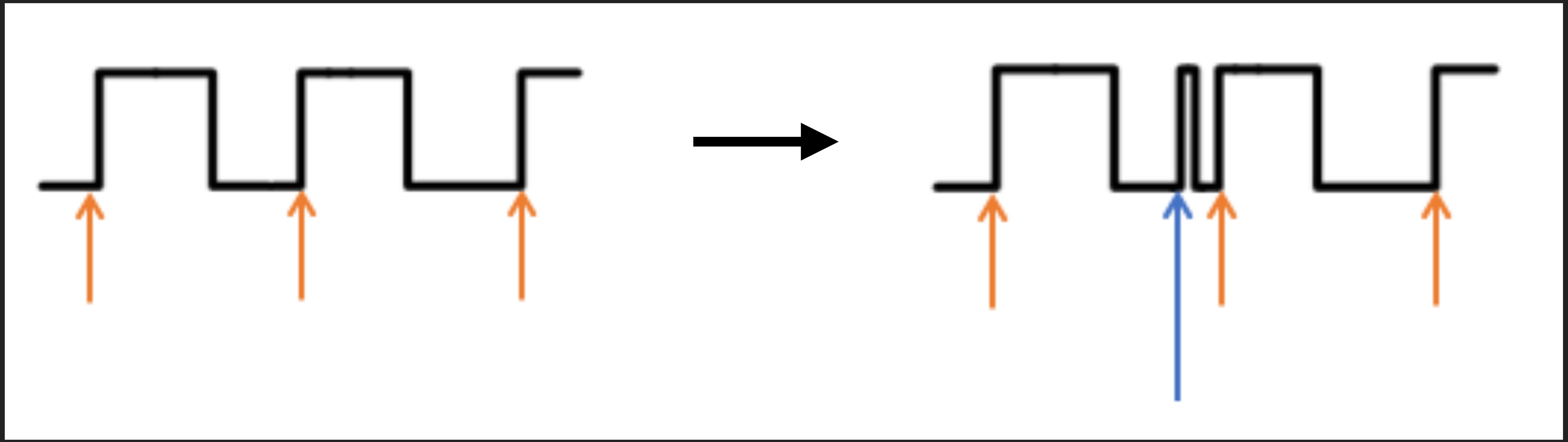


ATTACK VECTORS

- Timing
- Voltage
- Electromagnetic (EM)
- Optical / Light
- Body Biasing
- Other (Temperature, ???)

TIMING

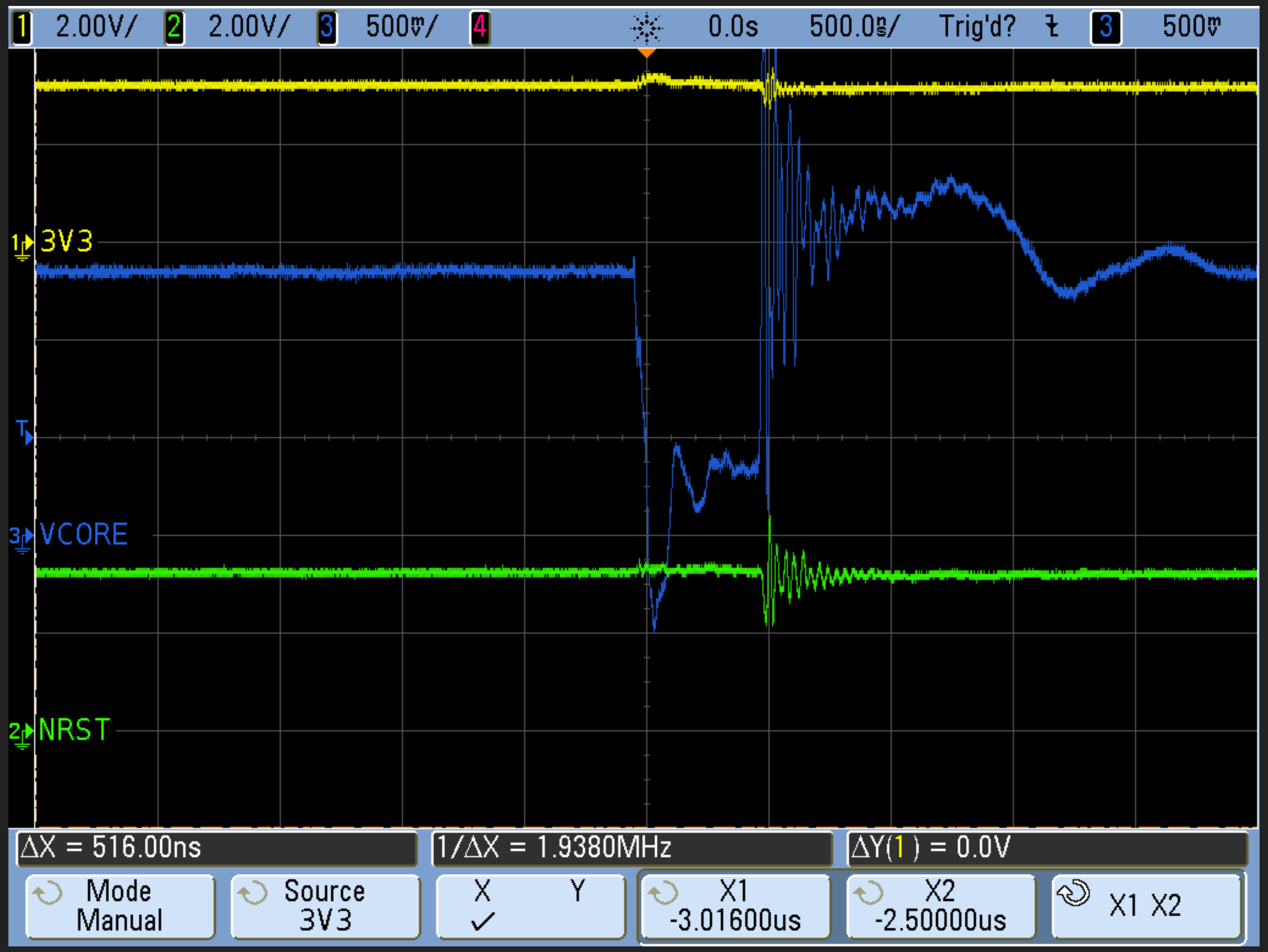
- Introduce unexpected / extra / fast clock edge(s)
- Replace or mix clock / oscillator with custom circuitry

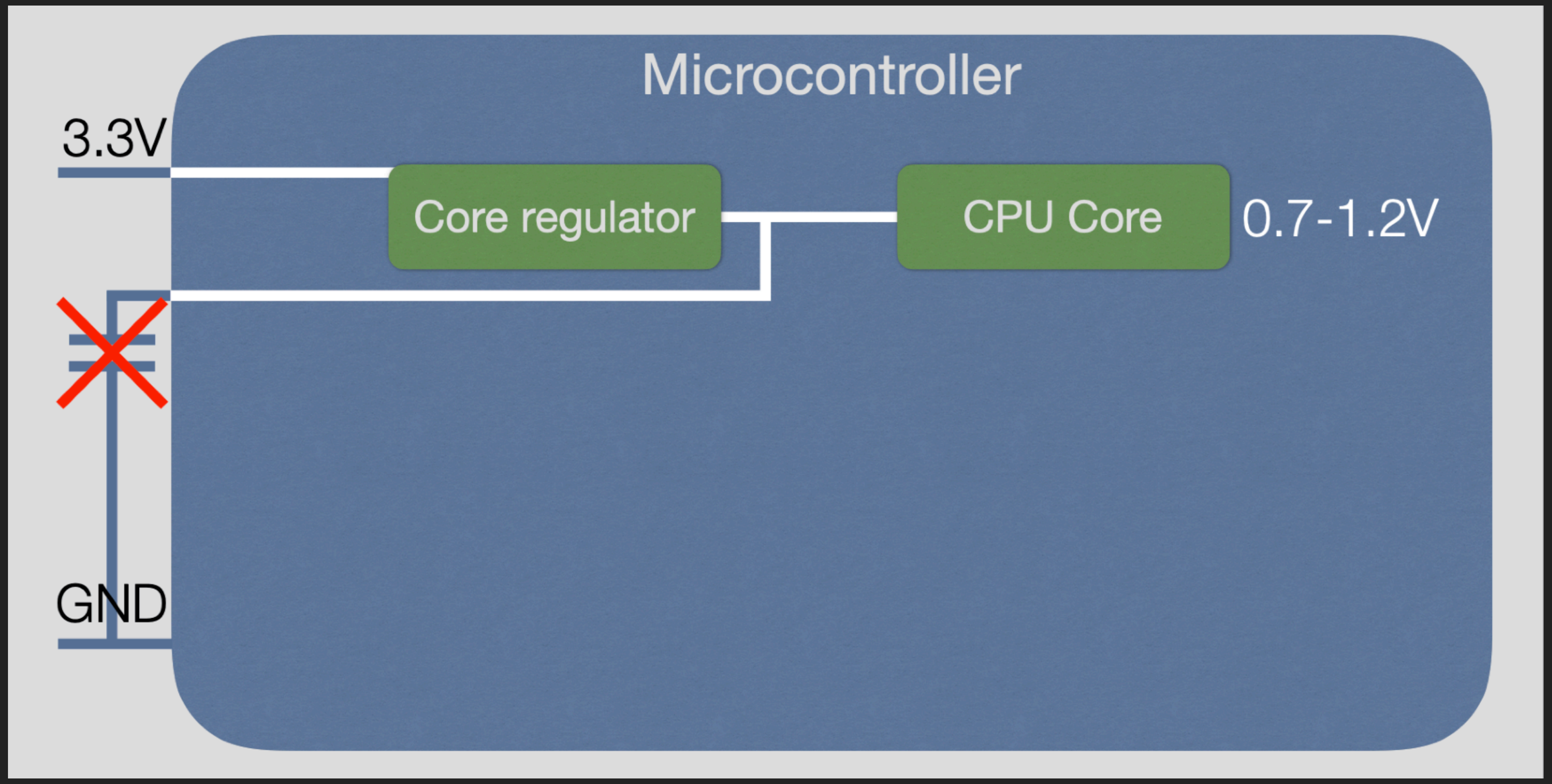


Colin O'Flynn (NewAE)

VOLTAGE

- Drop power supply below minimum (brown out)
- Target CPU core voltage for best results
- Requires target preparation to remove capacitors, access voltage rail

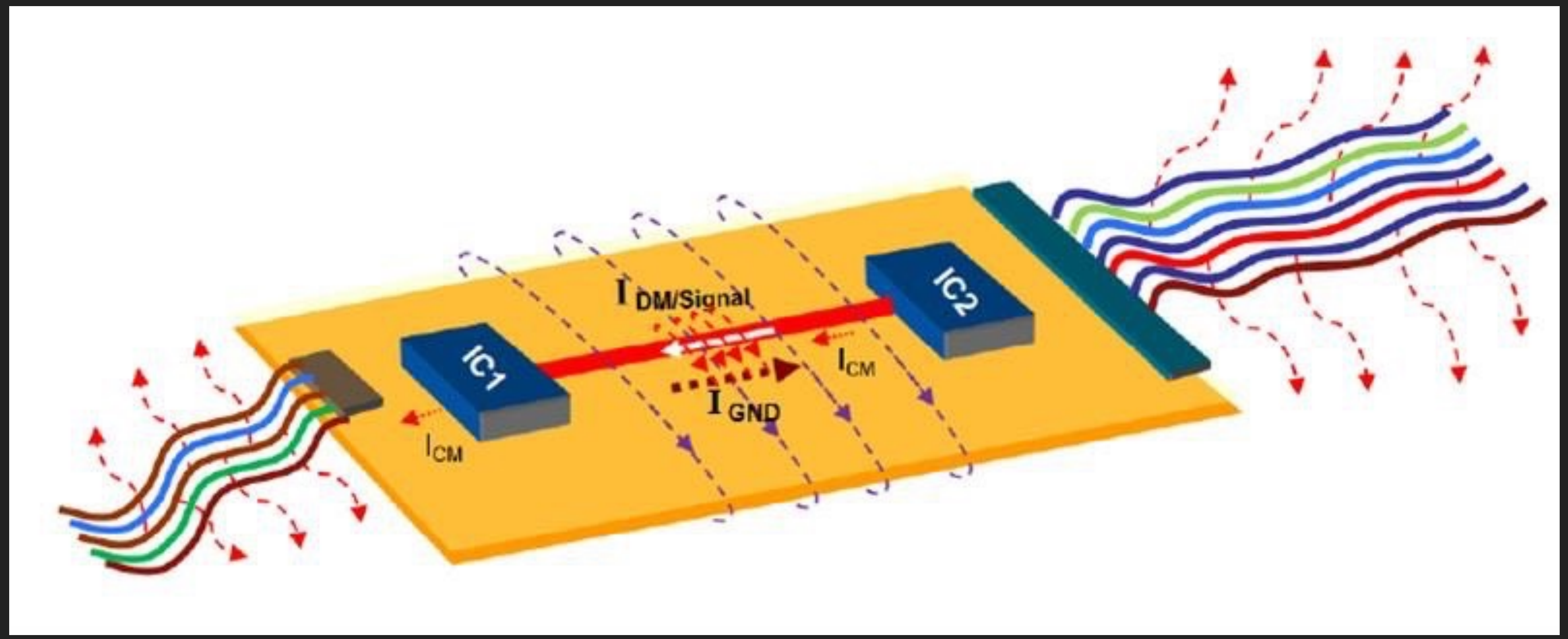


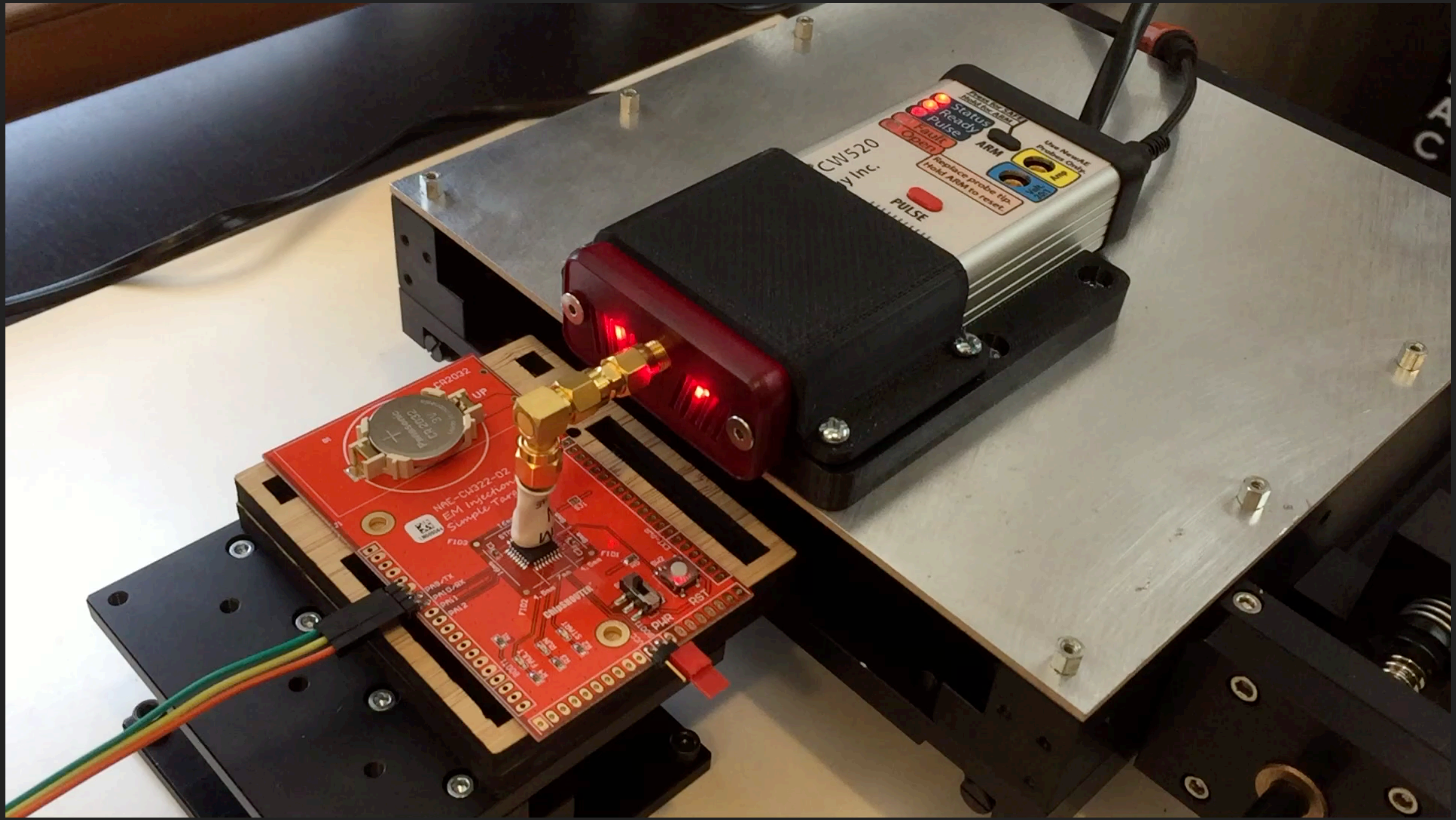


wallet.fail

ELECTROMAGNETIC (EM)

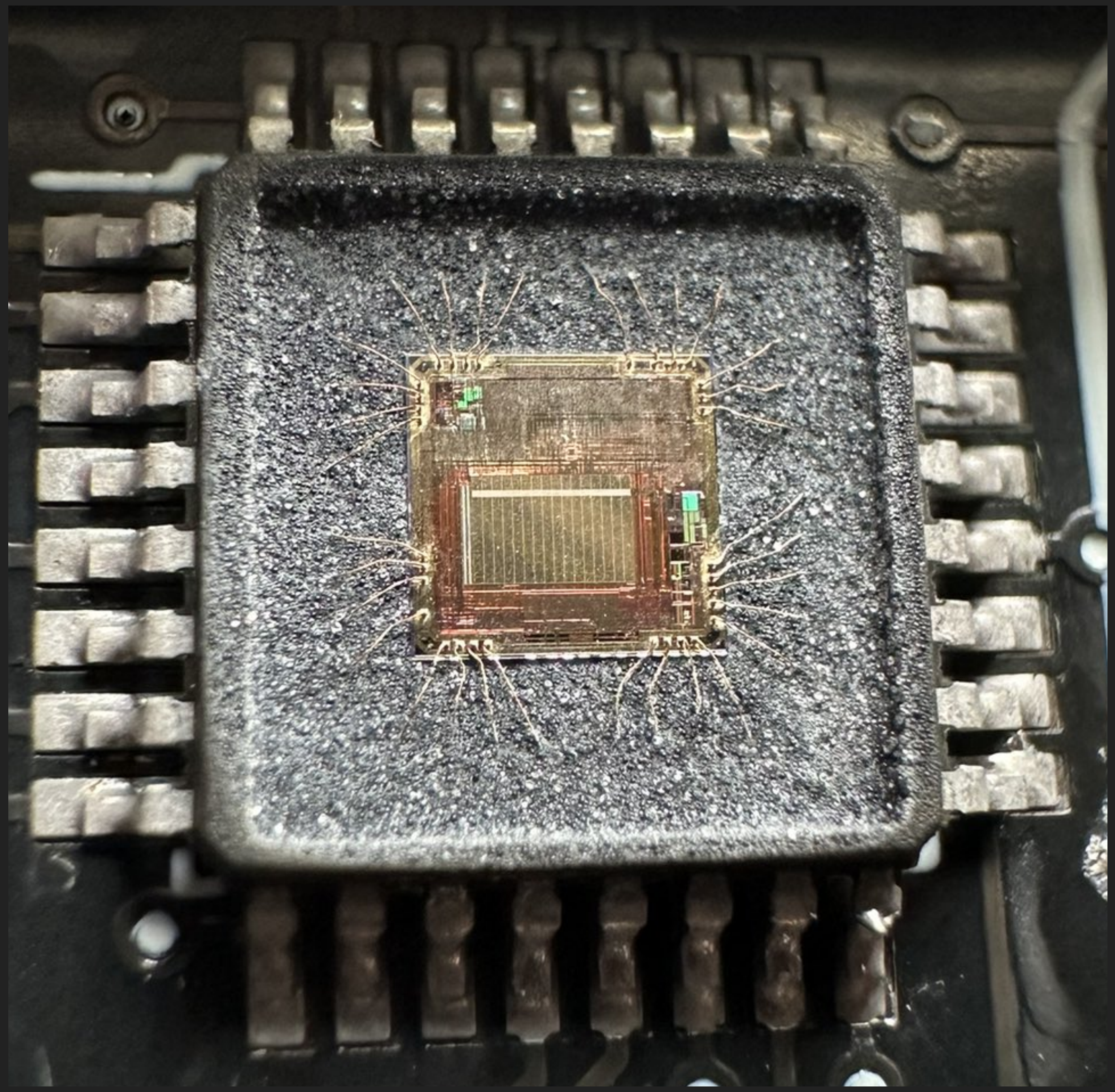
- Induce current onto internal chip structures
- No physical contact / manipulation required



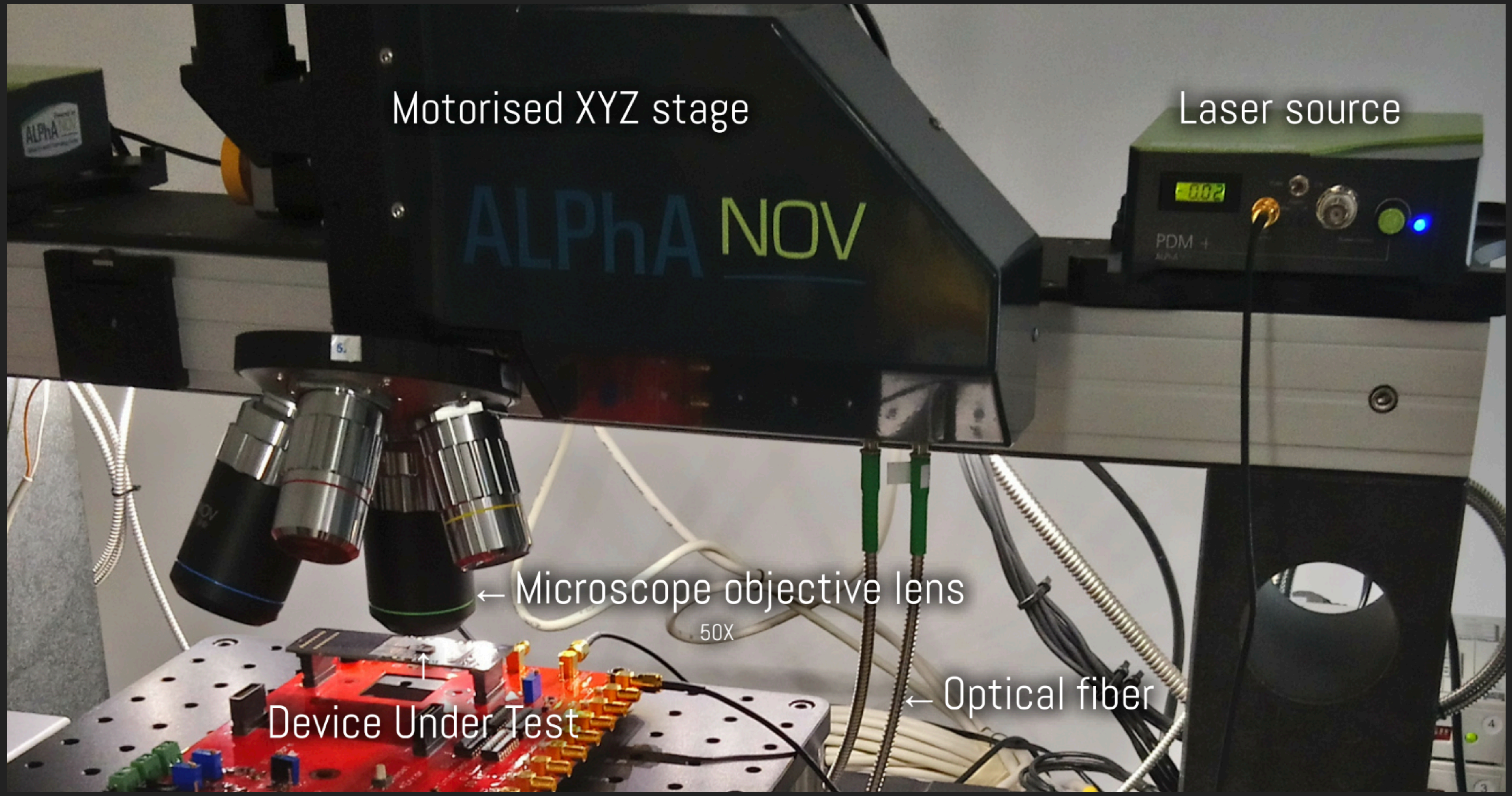


OPTICAL / LIGHT

- Induce photocurrents onto the silicon die
- Requires invasive access (decapsulation)



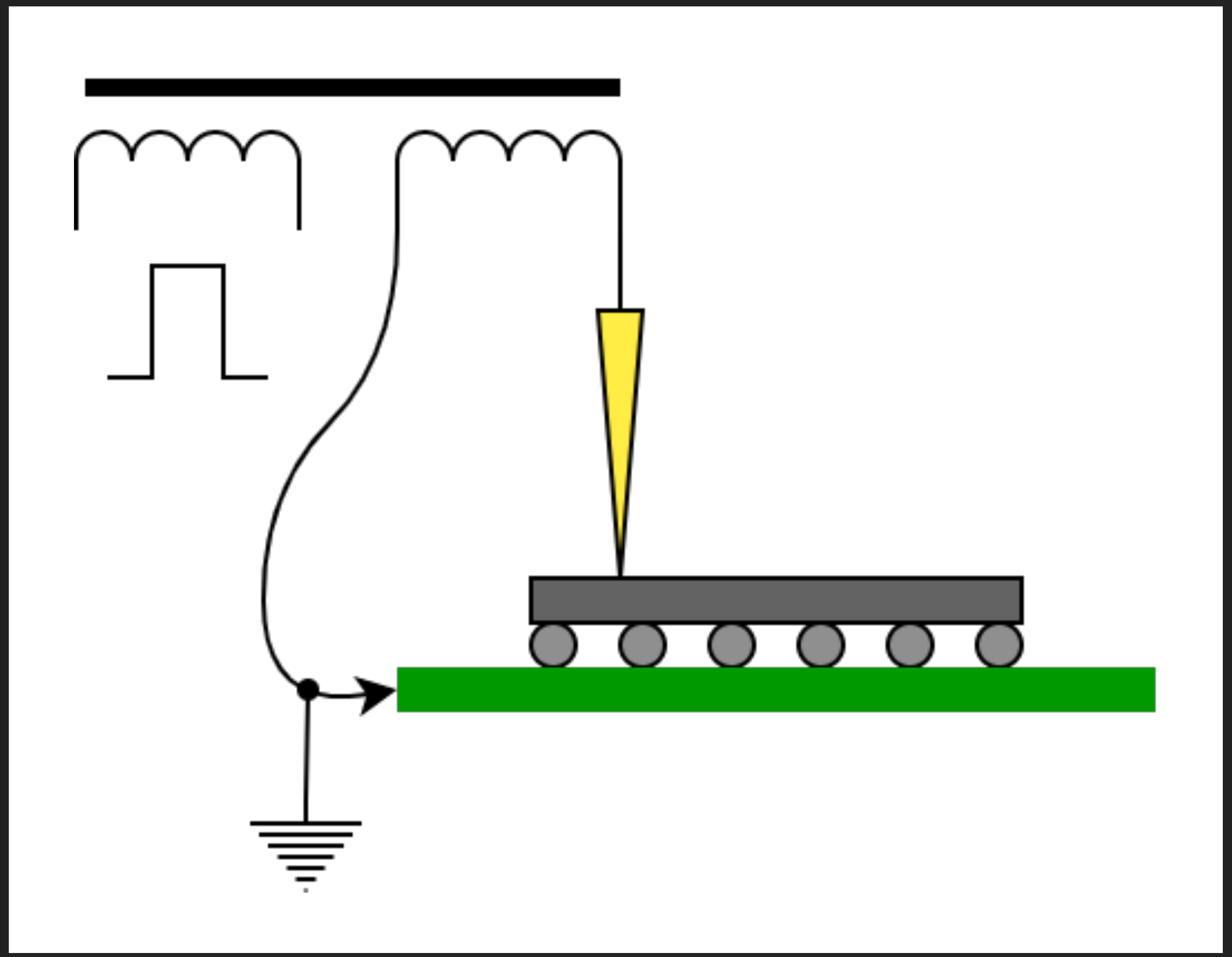
chippie.io via @BitBangingBytes

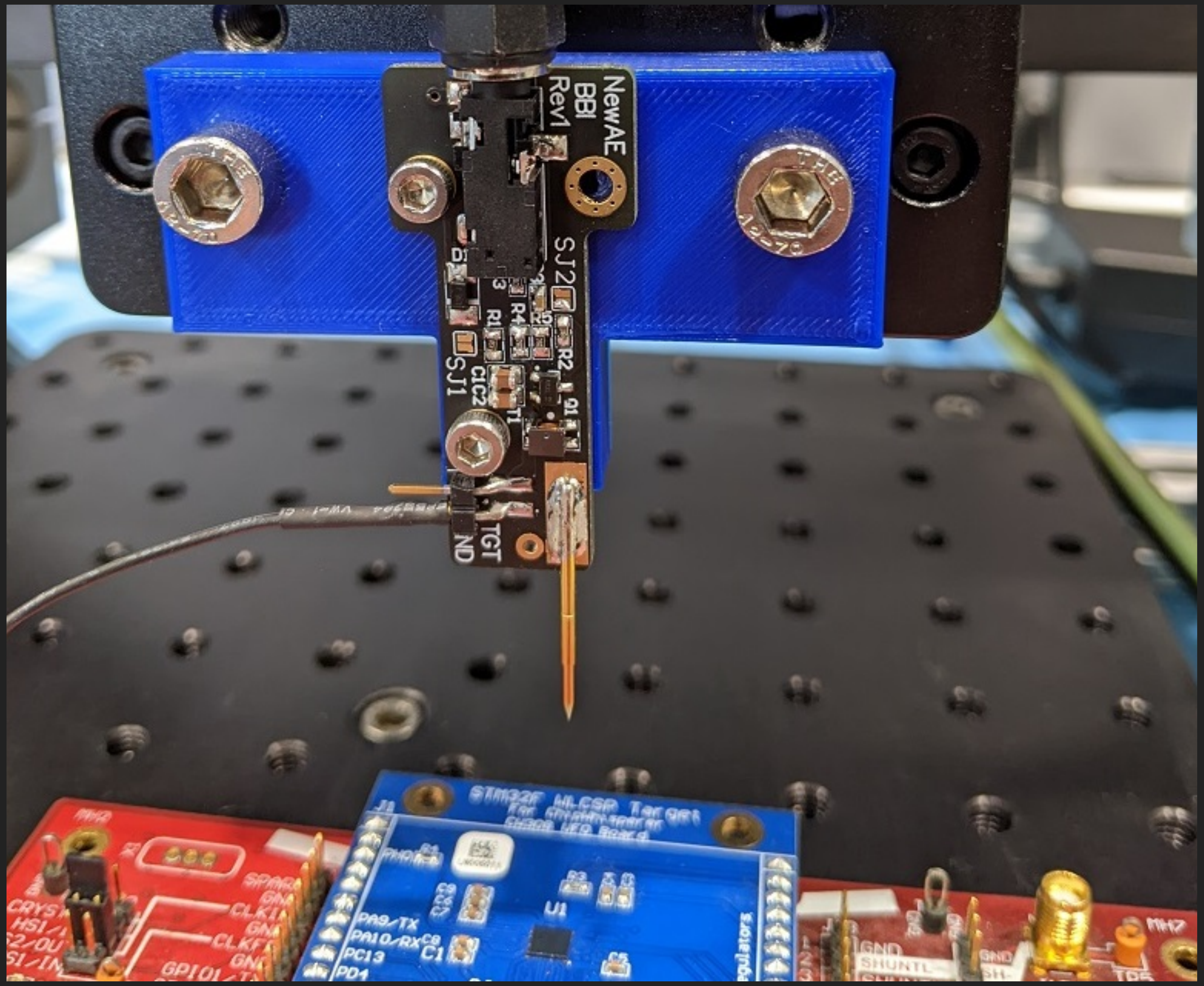


Black-Box Laser Fault Injection on a Secure Memory

BODY BIASING

- Apply voltage to exposed backside of IC die
- Requires target preparation and usually invasive (dependent on package type)

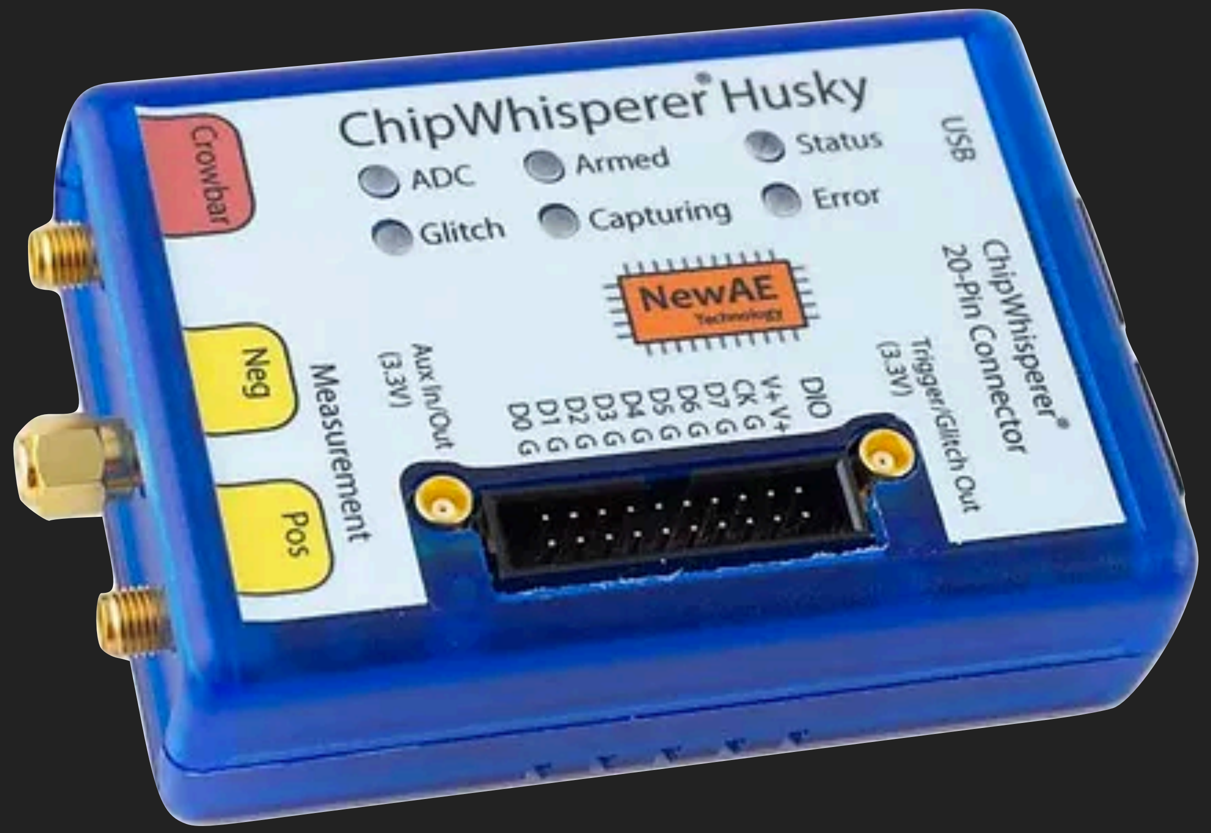


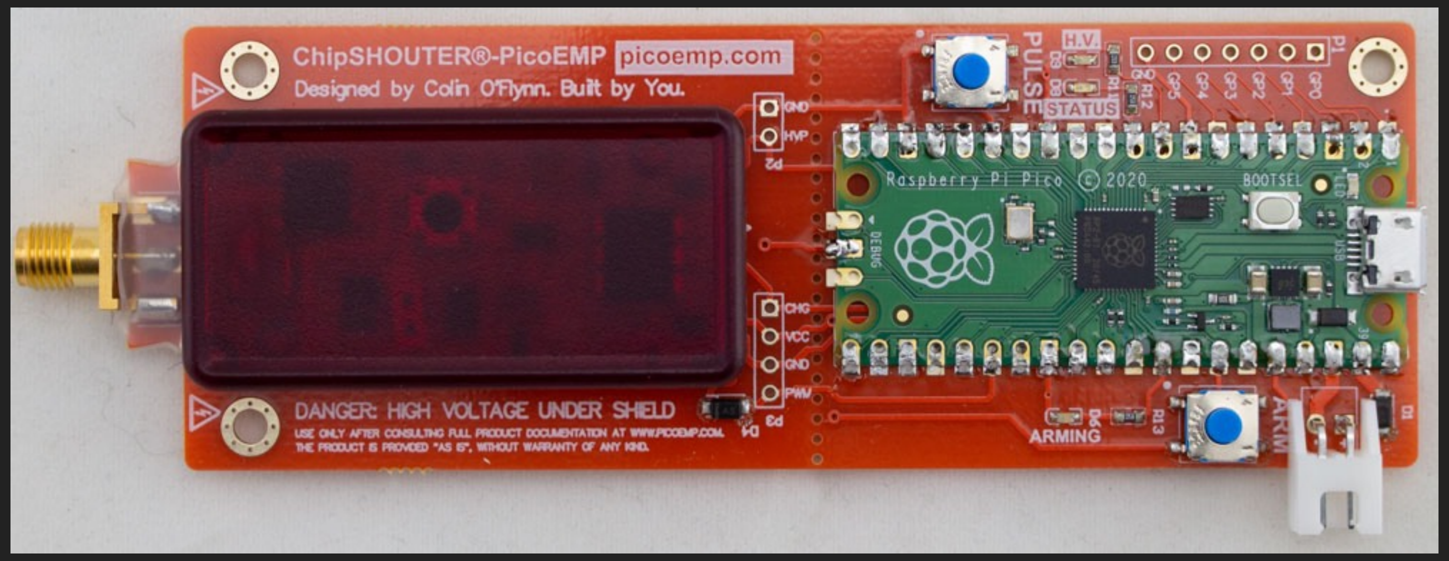


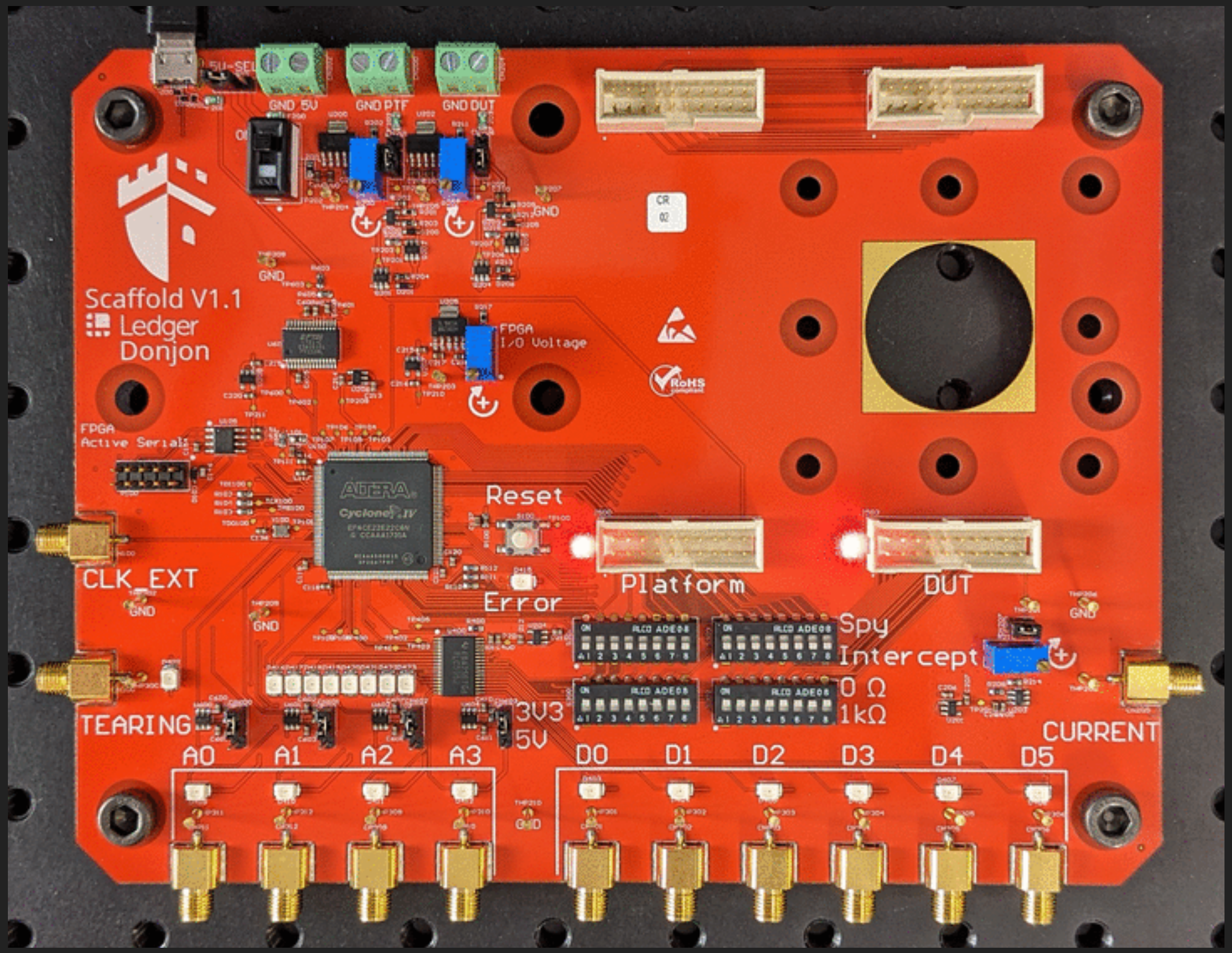
github.com/newaetech/chipjabber-basicbbi

TOOLS

- ChipWhisperer
- PicoEMP / ChipSHOUTER
- Riscure
- Ledger Donjon Scaffold
- Faultier (hextree.io)
- Raiden (h0rac)
- MCU / FPGA + MAX4619 Analog Switch

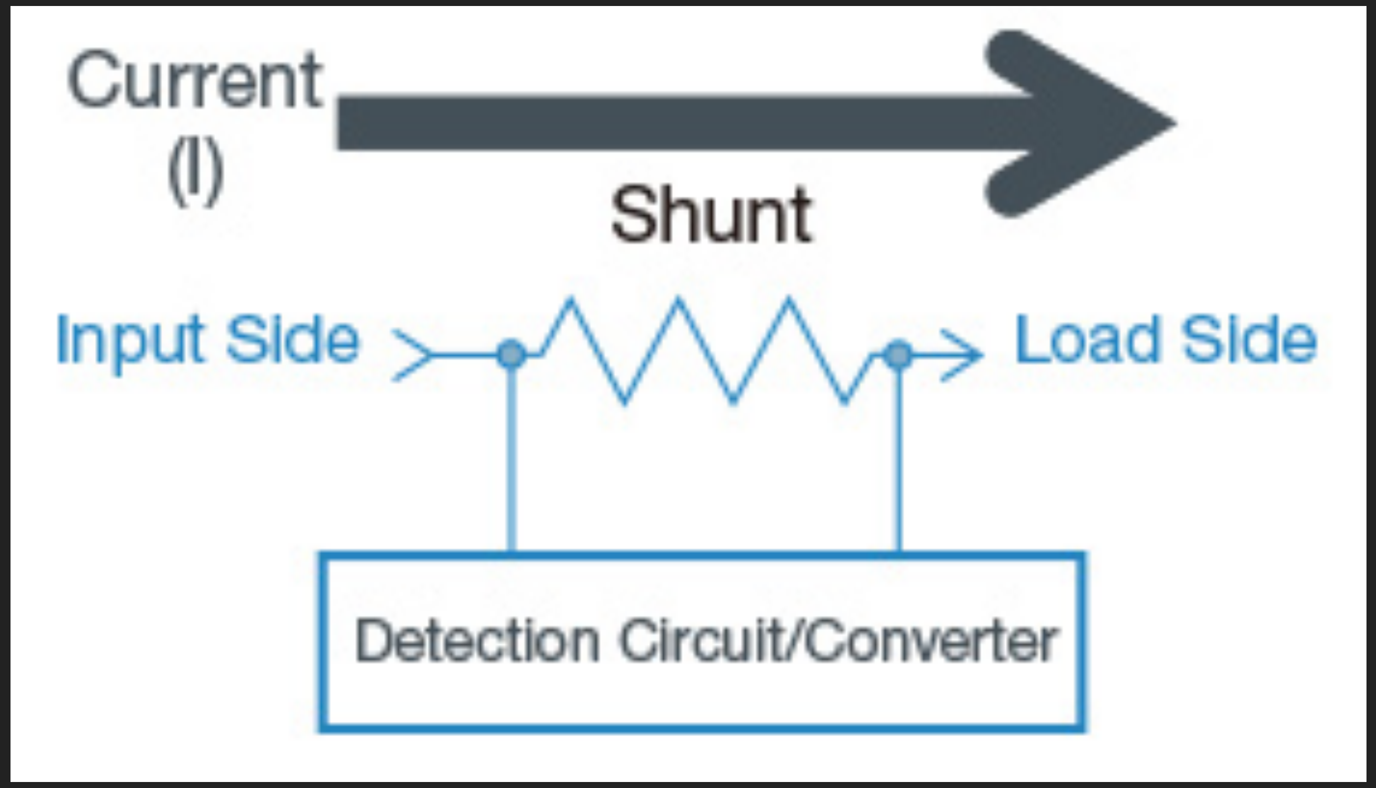



ChipSHOUTER®-PicoEMP picoemp.com
Designed by Colin O'Flynn. Built by You.
Raspberry Pi Pico © 2020
DANGER: HIGH VOLTAGE UNDER SHIELD
ARMING
PULSE
STATUS

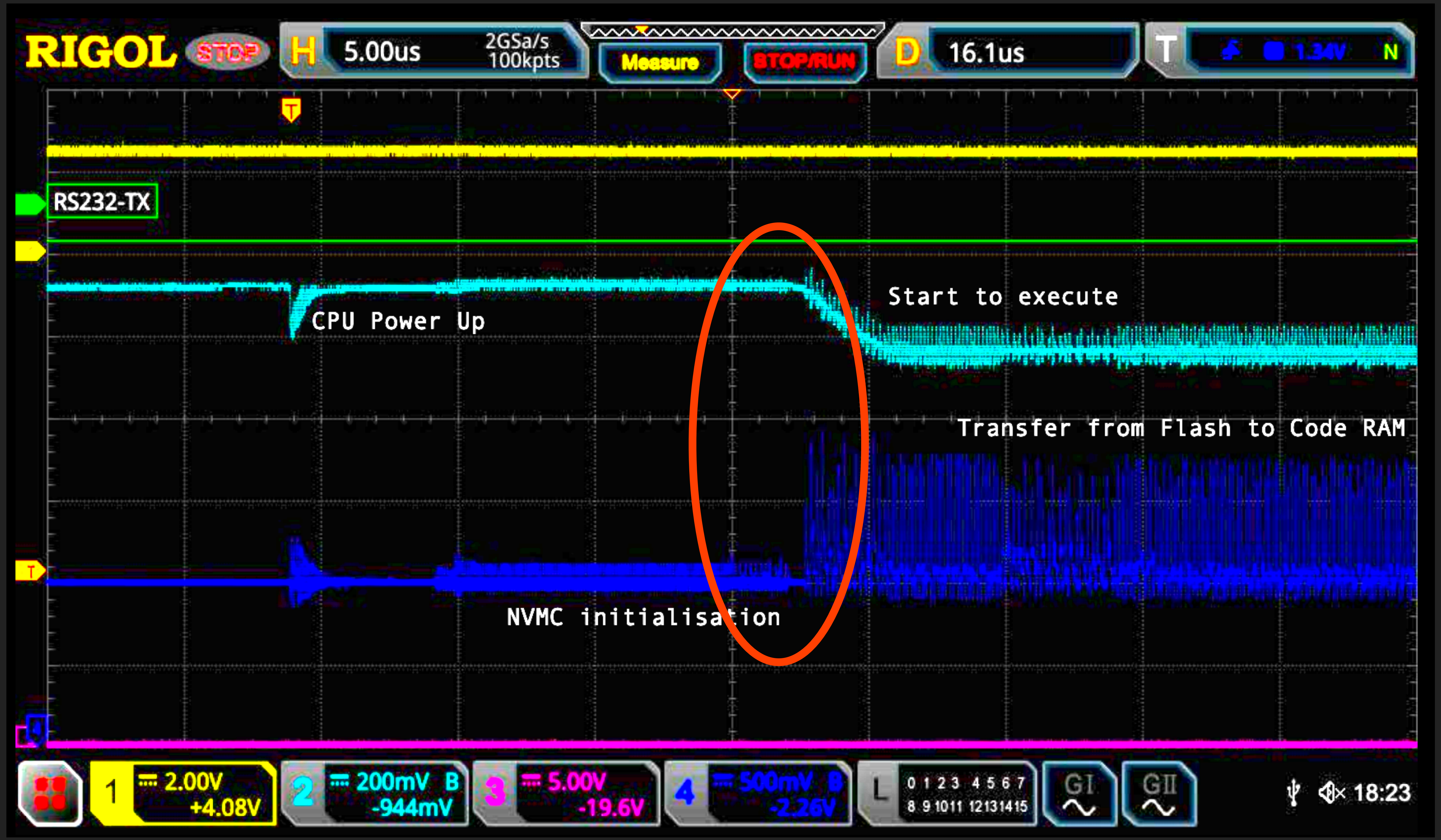


CHARACTERIZATION

- Usually triggered by external indicator or cycle counting
  - Based on a known bus / signal output
  - May require firmware / code or power / EM analysis

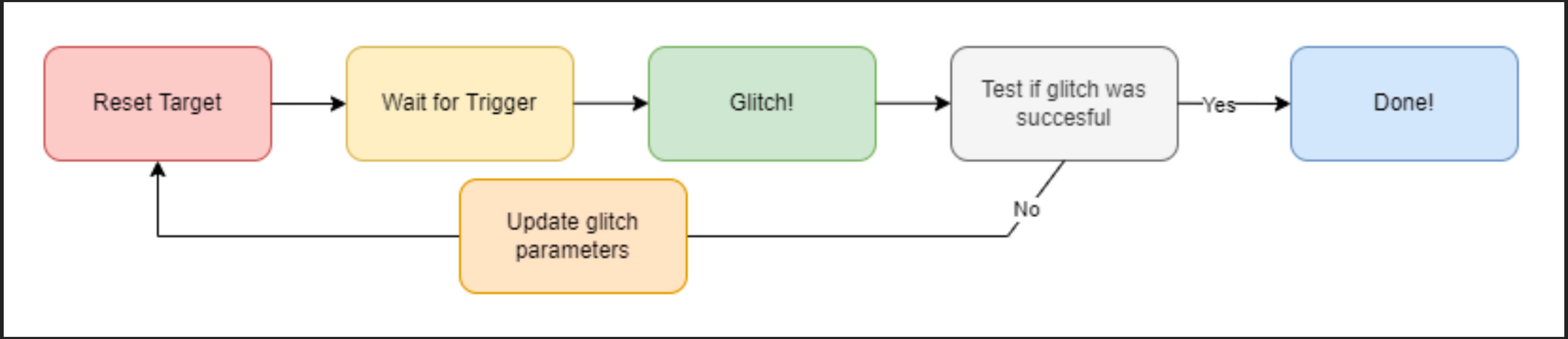


LimitedResults nRF52
Debug Resurrection



CHARACTERIZATION

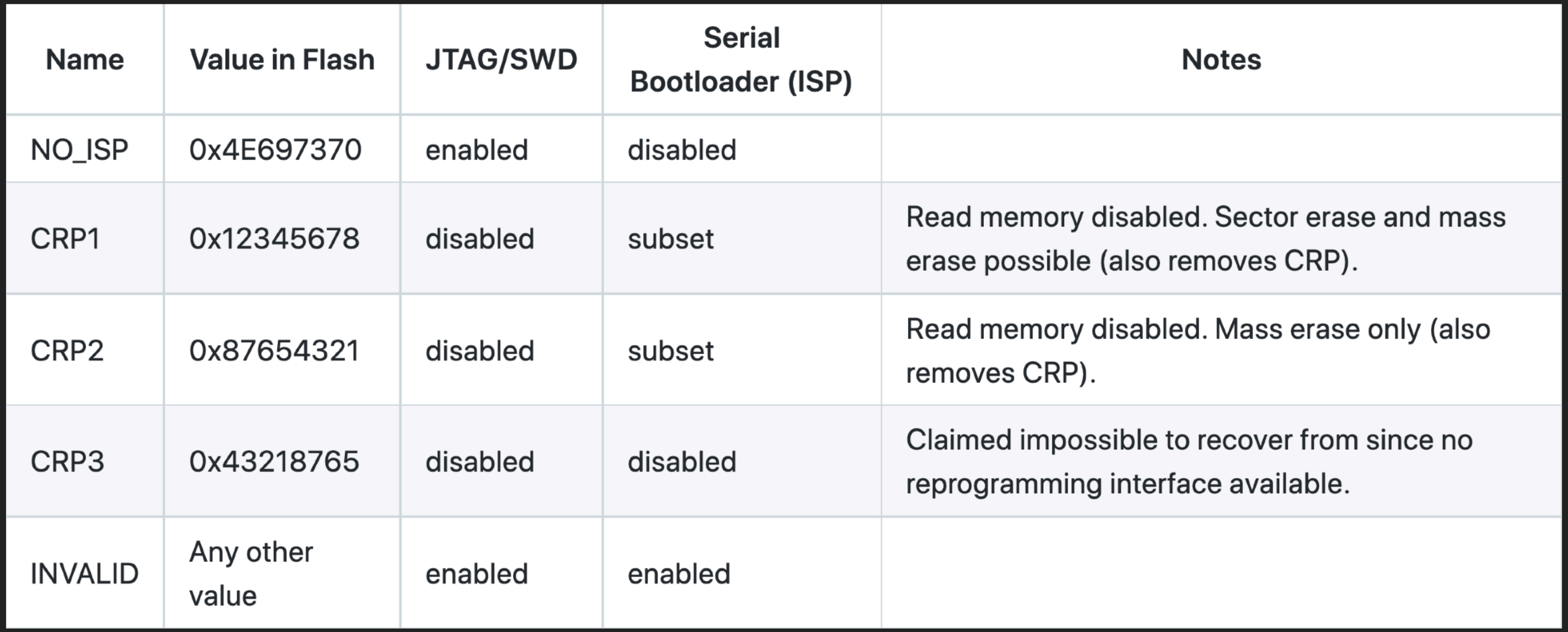
- Requires precise tuning to determine ideal glitch parameters
  - When to glitch?
  - Width of pulse?



DEMONSTRATION

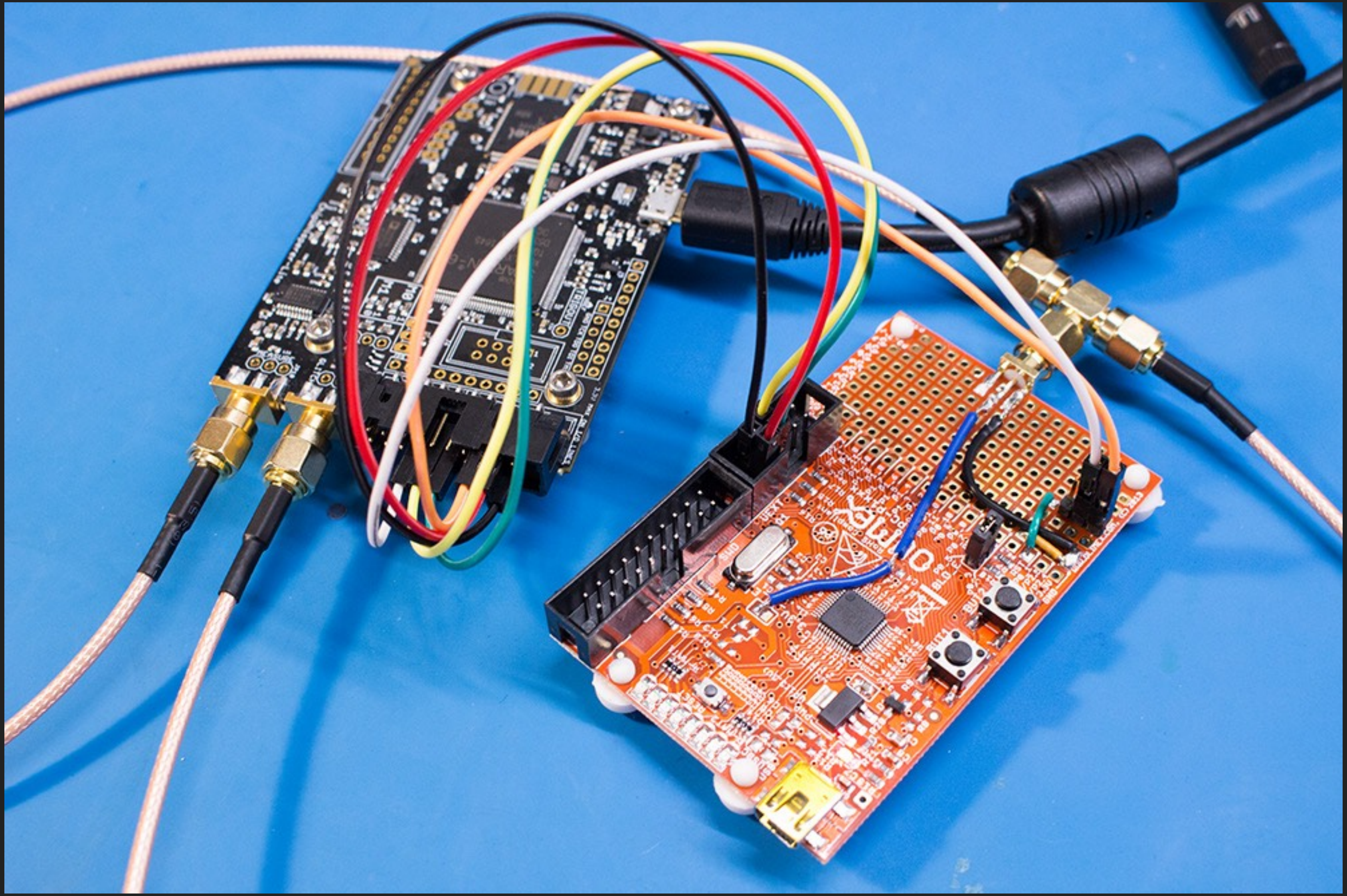
NXP LPC VOLTAGE GLITCH

- Breaking Code Read Protection on the NXP LPC-family MCUs, Gerlinsky, REcon Brussels 2017
- Code Readout Protection setting in 32-bit register
  - Only 4 defined values, any other value (2^{32} - 4) will result in unprotected device

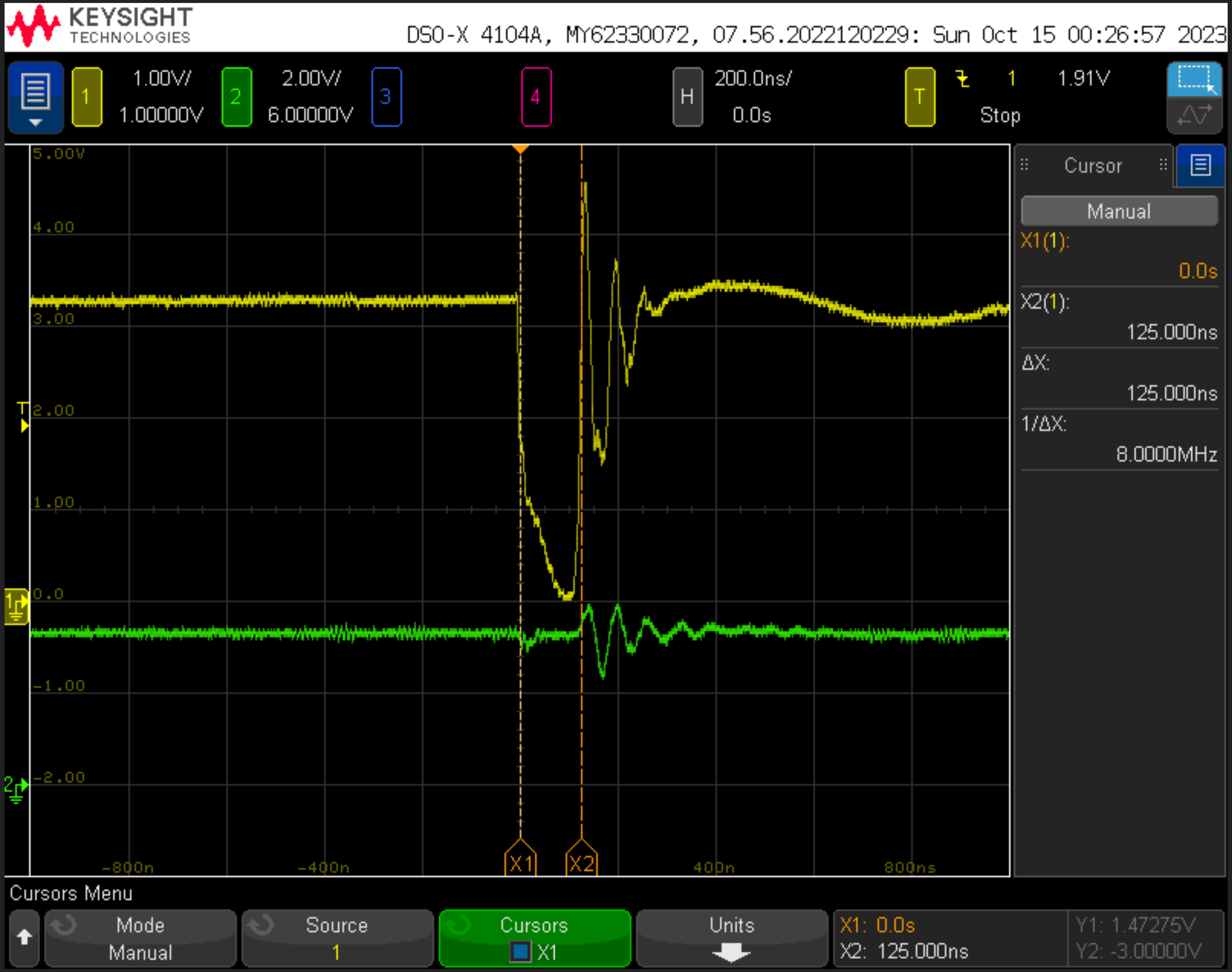


Name	Value in Flash	JTAG/SWD	Serial Bootloader (ISP)	Notes
NO_ISP	0x4E697370	enabled	disabled	
CRP1	0x12345678	disabled	subset	Read memory disabled. Sector erase and mass erase possible (also removes CRP).
CRP2	0x87654321	disabled	subset	Read memory disabled. Mass erase only (also removes CRP).
CRP3	0x43218765	disabled	disabled	Claimed impossible to recover from since no reprogramming interface available.
INVALID	Any other value	enabled	enabled	

NXP LPC VOLTAGE GLITCH



NXP LPC VOLTAGE GLITCH



DSO-X 4104A, MY62330072, 07.56.2022120229: Sun Oct 15 00:26:57 2023

1 1.00V/ 1.00000V

2 2.00V/ 6.00000V

H 200.0ns/ 0.0s

T 1 1.91V Stop

Cursor

Manual

X1(1): 0.0s

X2(1): 125.000ns

ΔX: 125.000ns

1/ΔX: 8.0000MHz

Cursors Menu

Mode Manual

Source 1

Cursors X1

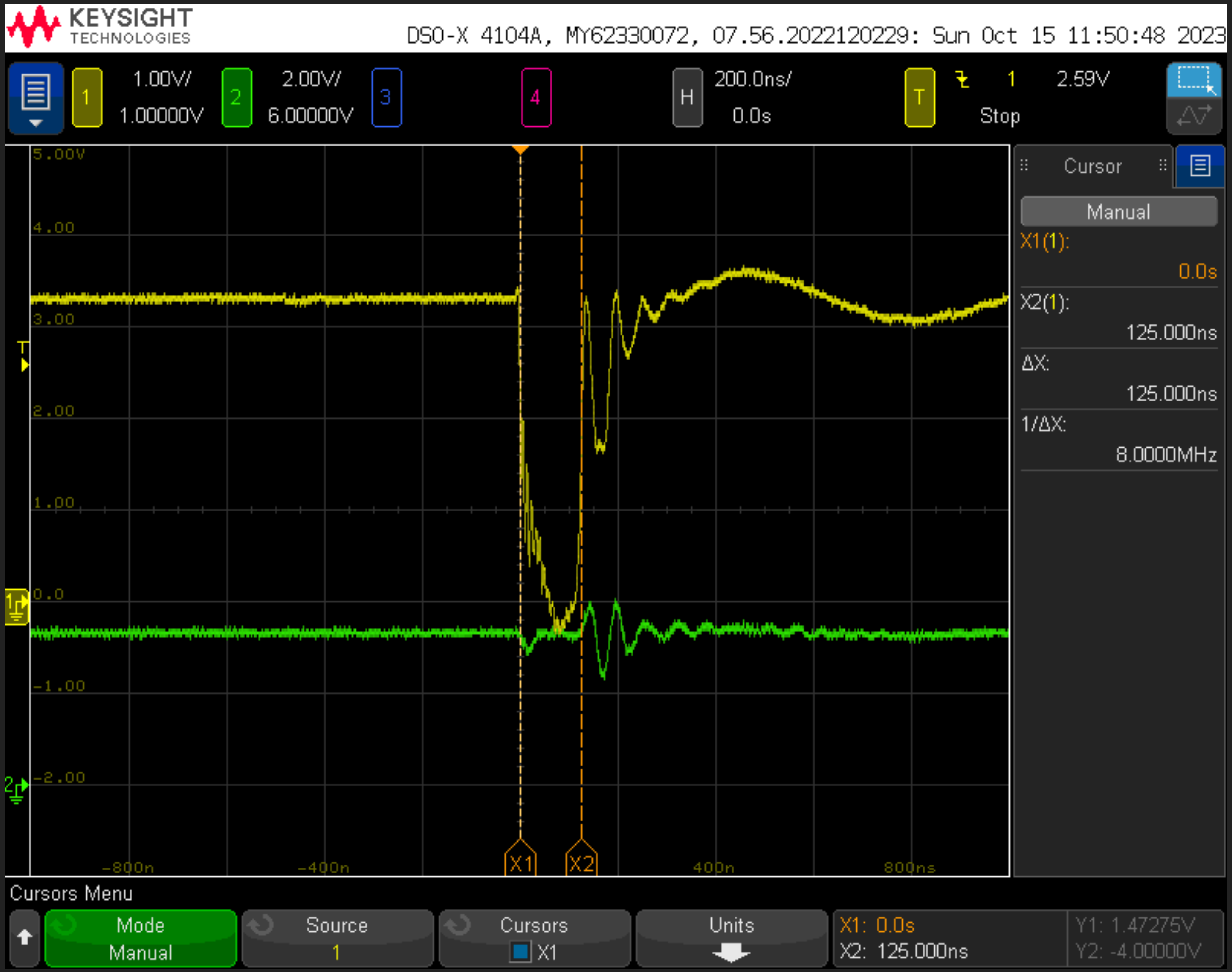
X1: 0.0s

X2: 125.000ns

Y1: 1.47275V

Y2: -3.00000V

NXP LPC VOLTAGE GLITCH



RESOURCES

- The Hardware Hacking Handbook
- Taking The Guess Out Of Glitching (Major Malfunction, Nullcon Goa 2020)
- chip.fail (Black Hat USA 2019)
- Lennert Wouters (COSIC, Glitched on Earth by Humans)
- Wrongbaud (Matthew Alt)
- Raelize (Cristofaro Mune)
- LimitedResults
- NewAE GitHub

SHOT THROUGH THE HEART

- General purpose MCU security == generally susceptible
- Fault injection is dependent on many external factors
    - Glitch type
    - Glitch parameters (timing, width)
    - Environment (cable lengths, temperature)
    - Manufacturing variances in silicon
- When it works, it feels like magic

THANK YOU

Press for SAFE
Hold for ARM
Use NewAE
Probes Only.
Status
Ready
Pulse
ARM
Amp
Fault
Open
Replace probe tip.
Hold ARM to reset.
R®CW520
ogy Inc.
PULSE