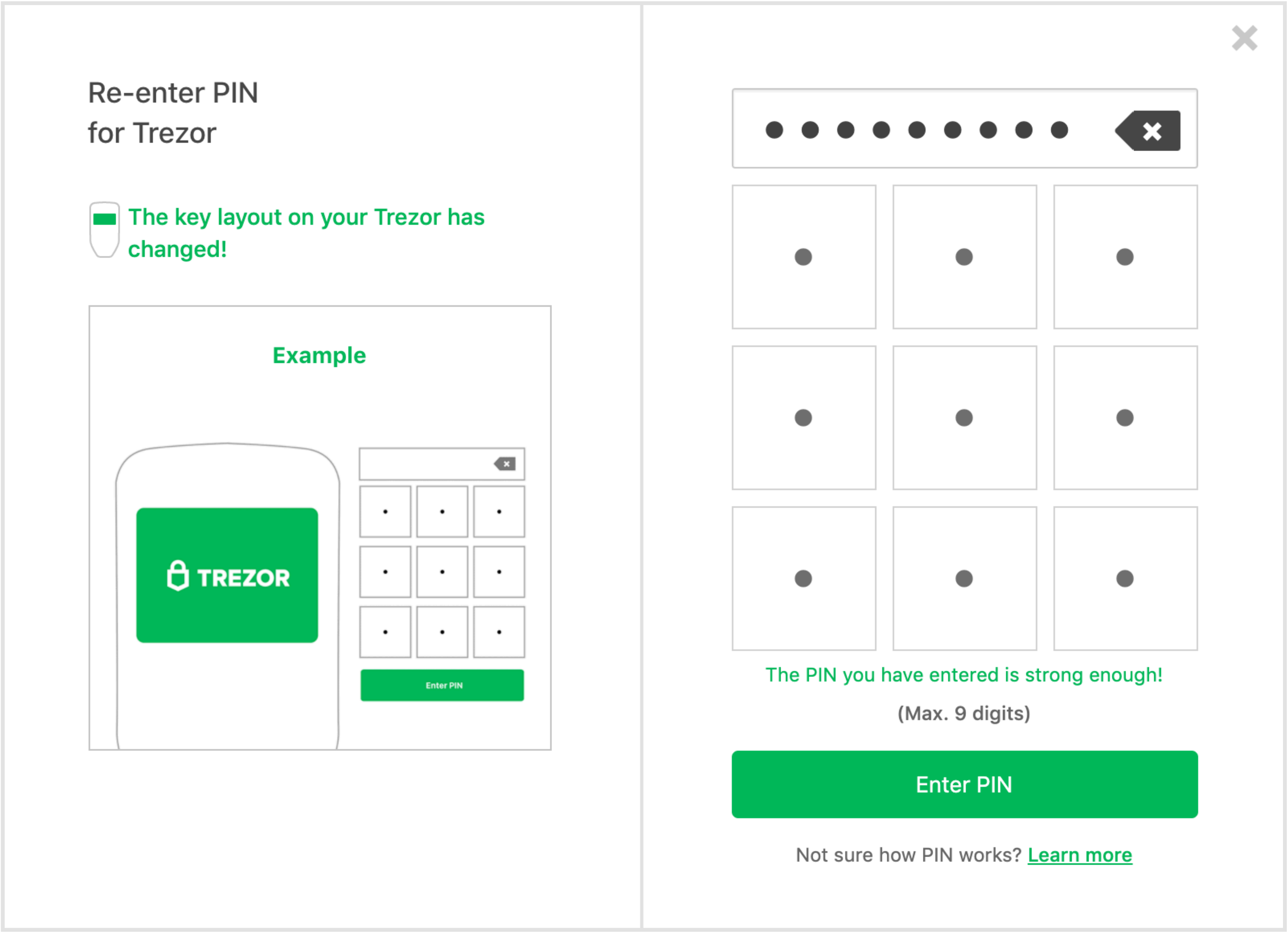
JOE GRAND AKA KINGPIN

THAT TIME I HACKED A HARDWARE WALLET AND RECOVERED $2 MILLION....

THIS IS A TRUE STORY

"I'M REACHING OUT BECAUSE OF AN ISSUE I HAVE WITH MY TREZOR WALLET. IN 2017, I BOUGHT SOME CRYPTO AND HAVEN'T TOUCHED THE WALLET SINCE. WHEN I WAS MOVING EARLIER THIS YEAR, I THINK THAT I ACCIDENTALLY THREW OUT THE RECOVERY SEED."



Re-enter PIN
for Trezor

The key layout on your Trezor has changed!

The PIN you have entered is strong enough!

(Max. 9 digits)

Not sure how PIN works? Learn more

MERCURY
SONY
Digi-Key
amazon.com
LANTRONIX
prime
T-2000
brother
BENRO
SONY

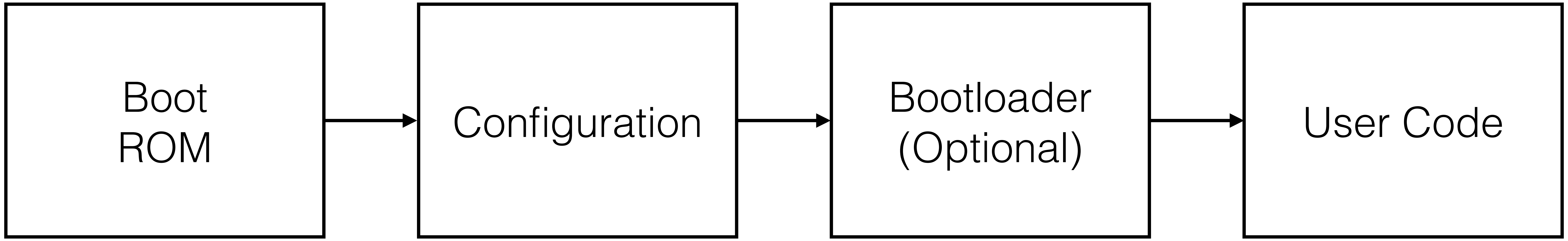
HARDWARE HACKING

PROCESS

- Information Gathering
  - Obtain information about the target
- Teardown
  - Product disassembly, component/subsystem ID
- Buses & Interfaces
  - Signal monitoring/analysis/emulation/fault injection
- Memory & Firmware
  - Extract/modify/analyze/reprogram code or data
- Chip-Level
  - Silicon die modification/data extraction

MICROCONTROLLER SECURITY

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



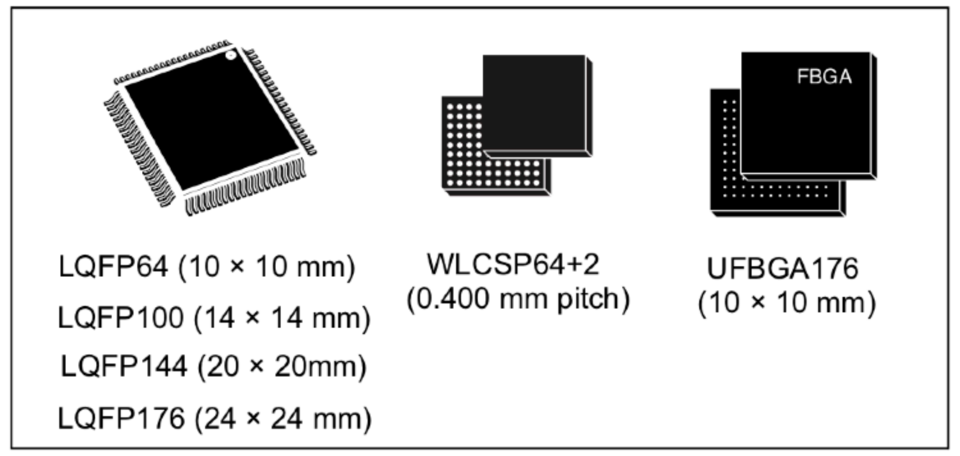
STM32F205xx
STM32F207xx

Arm®-based 32-bit MCU, 150 DMIPs, up to 1 MB Flash/128+4KB RAM, USB OTG HS/FS, Ethernet, 17 TIMs, 3 ADCs, 15 comm. interfaces and camera

Datasheet - production data

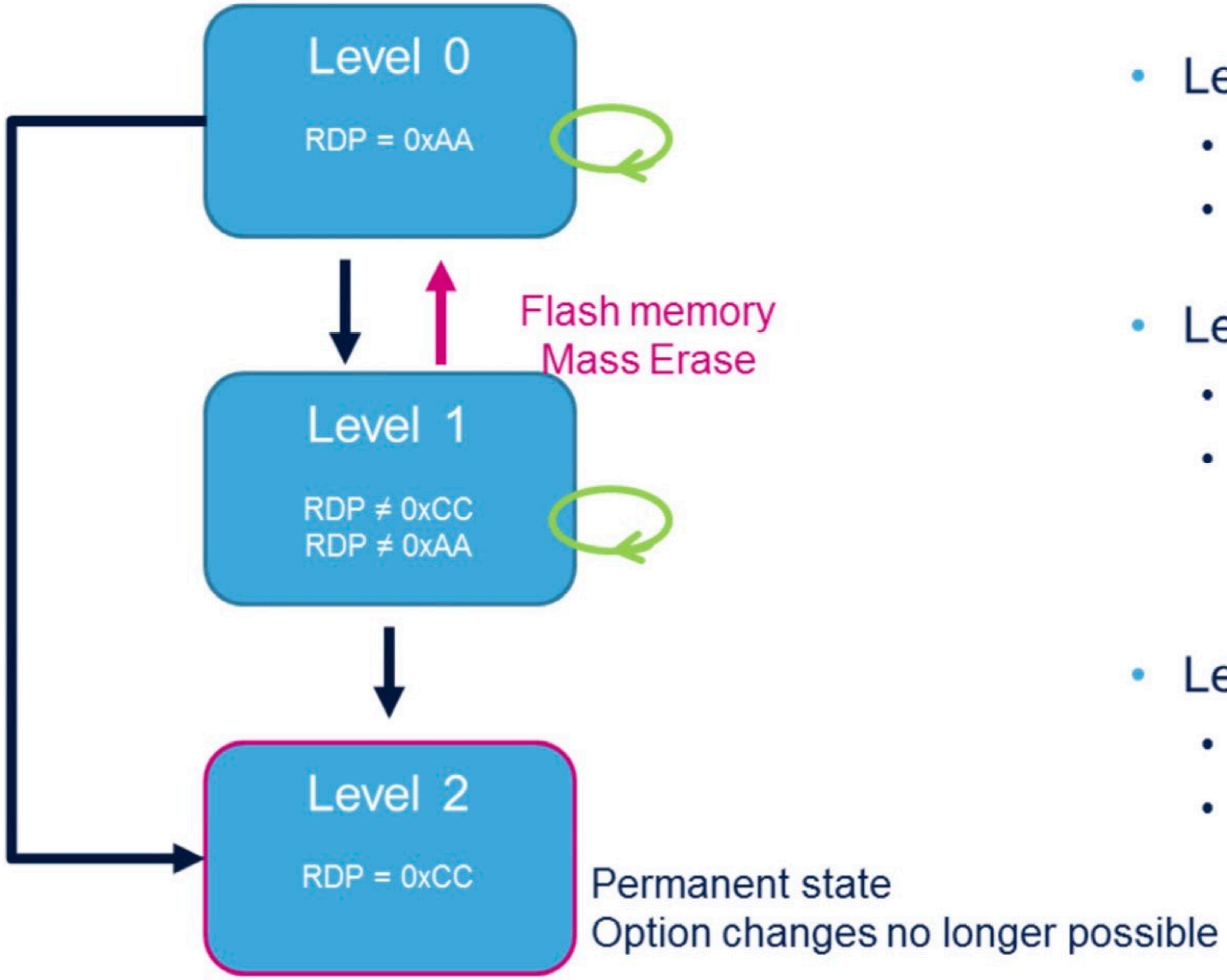
Features

- Core: Arm® 32-bit Cortex®-M3 CPU (120 MHz max) with Adaptive real-time accelerator (ART Accelerator™) allowing 0-wait state execution performance from Flash memory, MPU, 150 DMIPS/1.25 DMIPS/MHz (Dhrystone 2.1)
- Memories
  - Up to 1 Mbyte of Flash memory
  - 512 bytes of OTP memory
  - Up to 128 + 4 Kbytes of SRAM
  - Flexible static memory controller that supports Compact Flash, SRAM, PSRAM, NOR and NAND memories
  - LCD parallel interface, 8080/6800 modes
- Clock, reset and supply management
  - From 1.8 to 3.6 V application supply + I/Os
  - POR, PDR, PVD and BOR
  - 4 to 26 MHz crystal oscillator
  - Internal 16 MHz factory-trimmed RC
  - 32 kHz oscillator for RTC with calibration
  - Internal 32 kHz RC with calibration
- Low-power modes
  - Sleep, Stop and Standby modes
  - V_{BAT} supply for RTC, 20 × 32 bit backup registers, and optional 4 Kbytes backup SRAM
- 3 × 12-bit, 0.5 µs ADCs with up to 24 channels and up to 6 MSPS in triple interleaved mode
- 2 × 12-bit D/A converters
- General-purpose DMA: 16-stream controller with centralized FIFOs and burst support
- Up to 17 timers
  - Up to twelve 16-bit and two 32-bit timers, up to 120 MHz, each with up to four IC/OC/PWM or pulse counter and quadrature (incremental) encoder input
- Debug mode: Serial wire debug (SWD), JTAG, and Cortex®-M3 Embedded Trace Macrocell™



- Up to 140 I/O ports with interrupt capability:
  - Up to 136 fast I/Os up to 60 MHz
  - Up to 138 5 V-tolerant I/Os
- Up to 15 communication interfaces
  - Up to three I²C interfaces (SMBus/PMBus)
  - Up to four USARTs and two UARTs (7.5 Mbit/s, ISO 7816 interface, LIN, IrDA, modem control)
  - Up to three SPIs (30 Mbit/s), two with muxed I²S to achieve audio class accuracy via audio PLL or external PLL
  - 2 × CAN interfaces (2.0B Active)
  - SDIO interface
- Advanced connectivity
  - USB 2.0 full-speed device/host/OTG controller with on-chip PHY
  - USB 2.0 high-speed/full-speed device/host/OTG controller with dedicated DMA, on-chip full-speed PHY and ULPI
  - 10/100 Ethernet MAC with dedicated DMA: supports IEEE 1588v2 hardware, MII/RMII
- 8- to 14-bit parallel camera interface (48 Mbyte/s max.)
- CRC calculation unit
- 96-bit unique ID

RDP transition scheme



- Level 0
  - Option byte mods are allowed
  - Can transition to Level 1 or Level 2
- Level 1
  - Option byte mods are allowed.
  - Can transition to Level 0 or Level 2
    - Level 0 → Mass erase of user Flash memory, backup regs and SRAM2
- Level 2
  - Option bytes are frozen
  - No transition possible

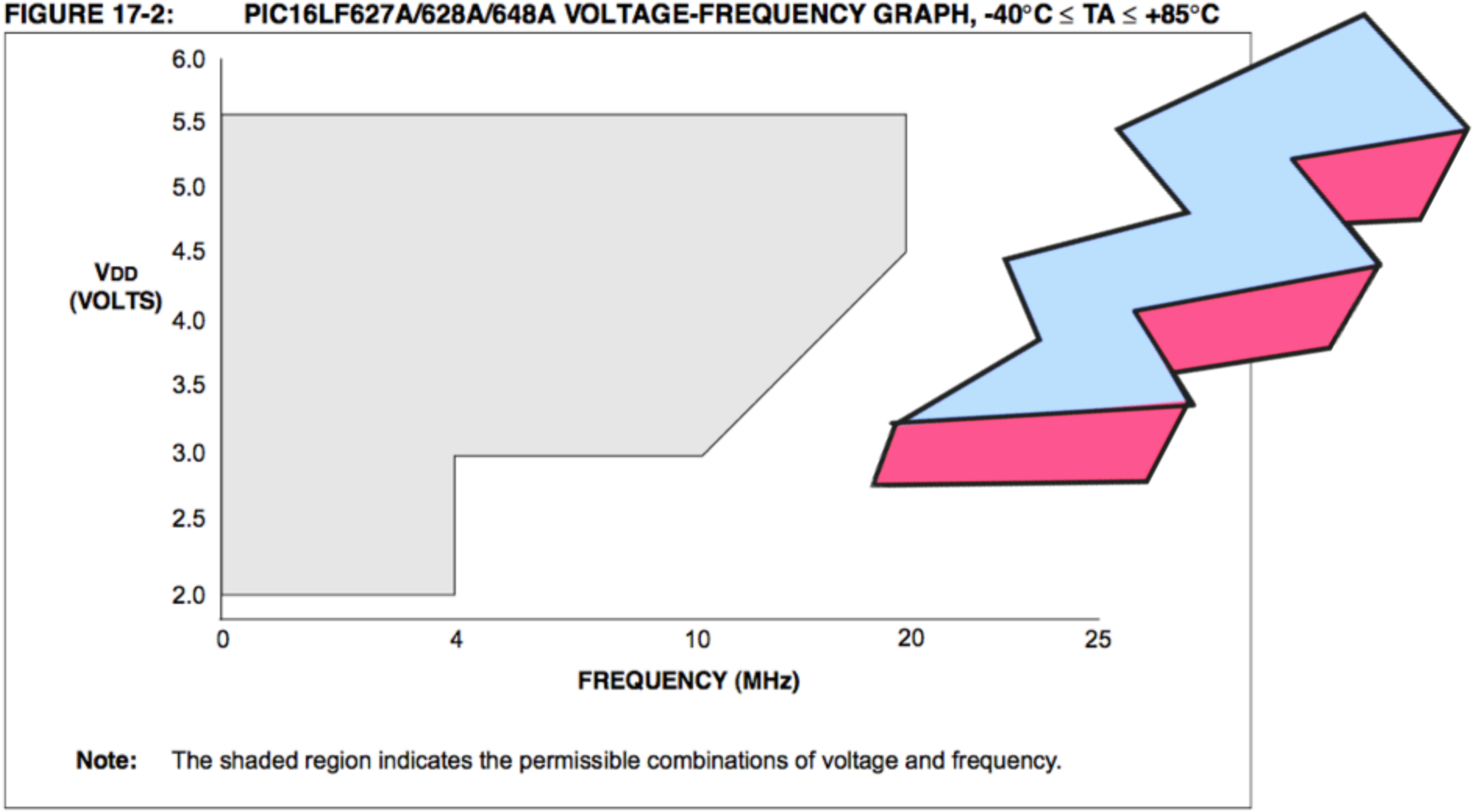
life.augmented

FAULT INJECTION

- Intentionally cause a fault in the target device
  - System reset/halt
  - Change in software decision
    - Skip an instruction
    - Affect branching
  - Computational fault
    - Instruction decoding errors
    - Malformed data read/write

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.

FAULT INJECTION

- Requires precise tuning to determine ideal glitch parameters
    - When to glitch?
    - Width of pulse?
    - Target preparation often needed
- Usually triggered by external indicator or cycle counting
    - Based on a known bus/signal output
    - May require firmware/code analysis
- Not a persistent attack (need to perform each time)

INSPIRATION

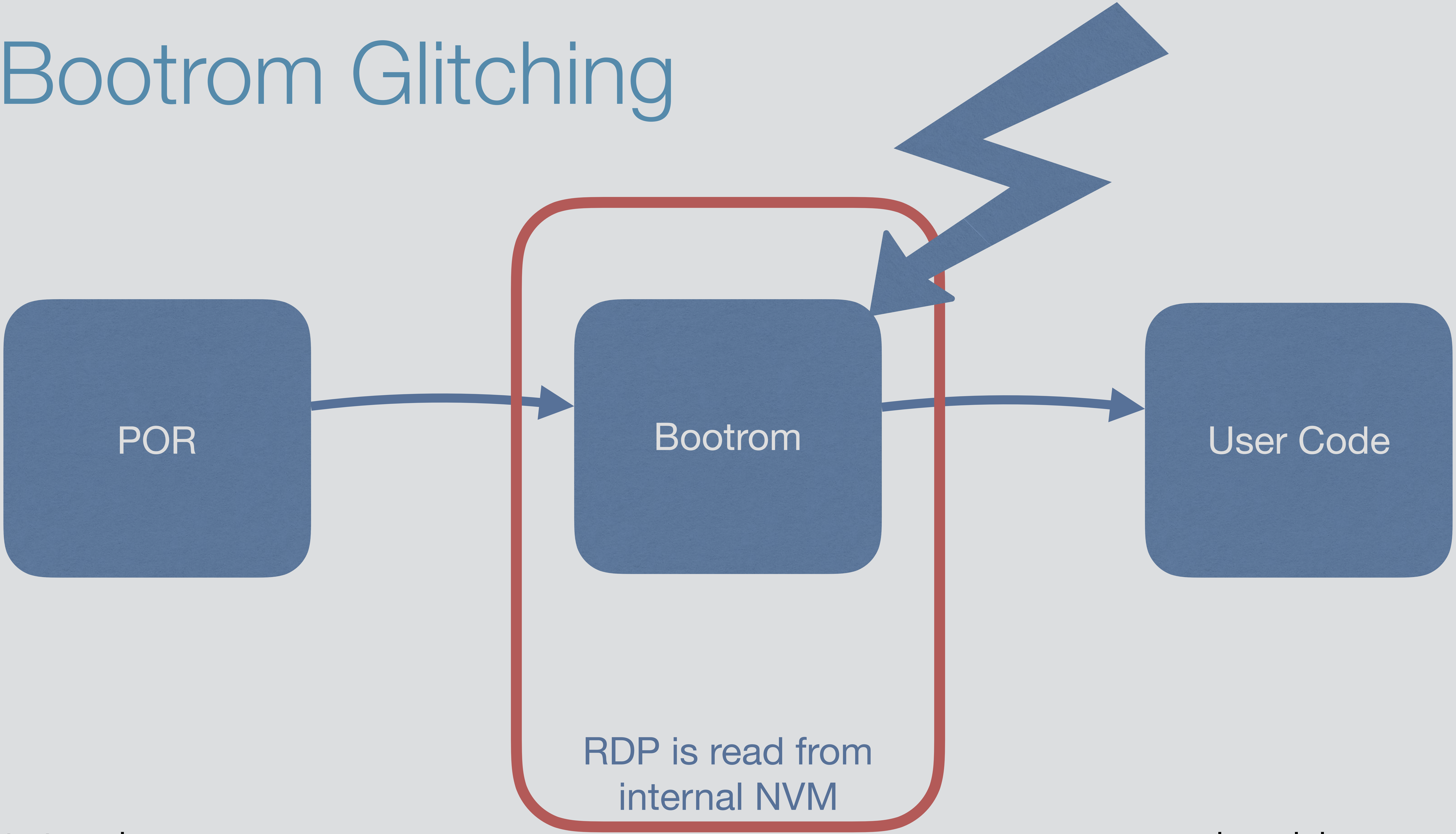
wallet.fail

Thomas Roth, Dmitry Nedospasov, Josh Datko

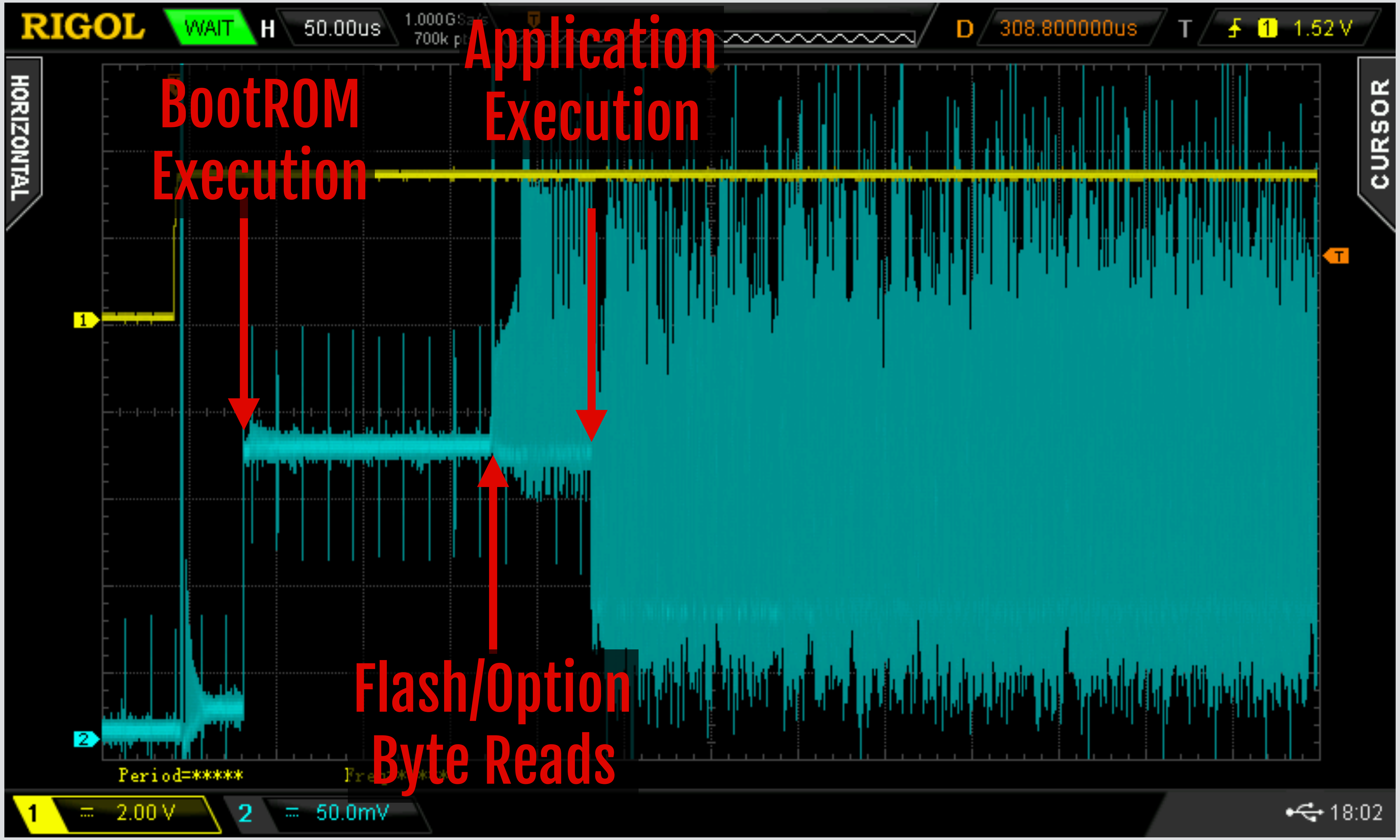
9563

chip.fail

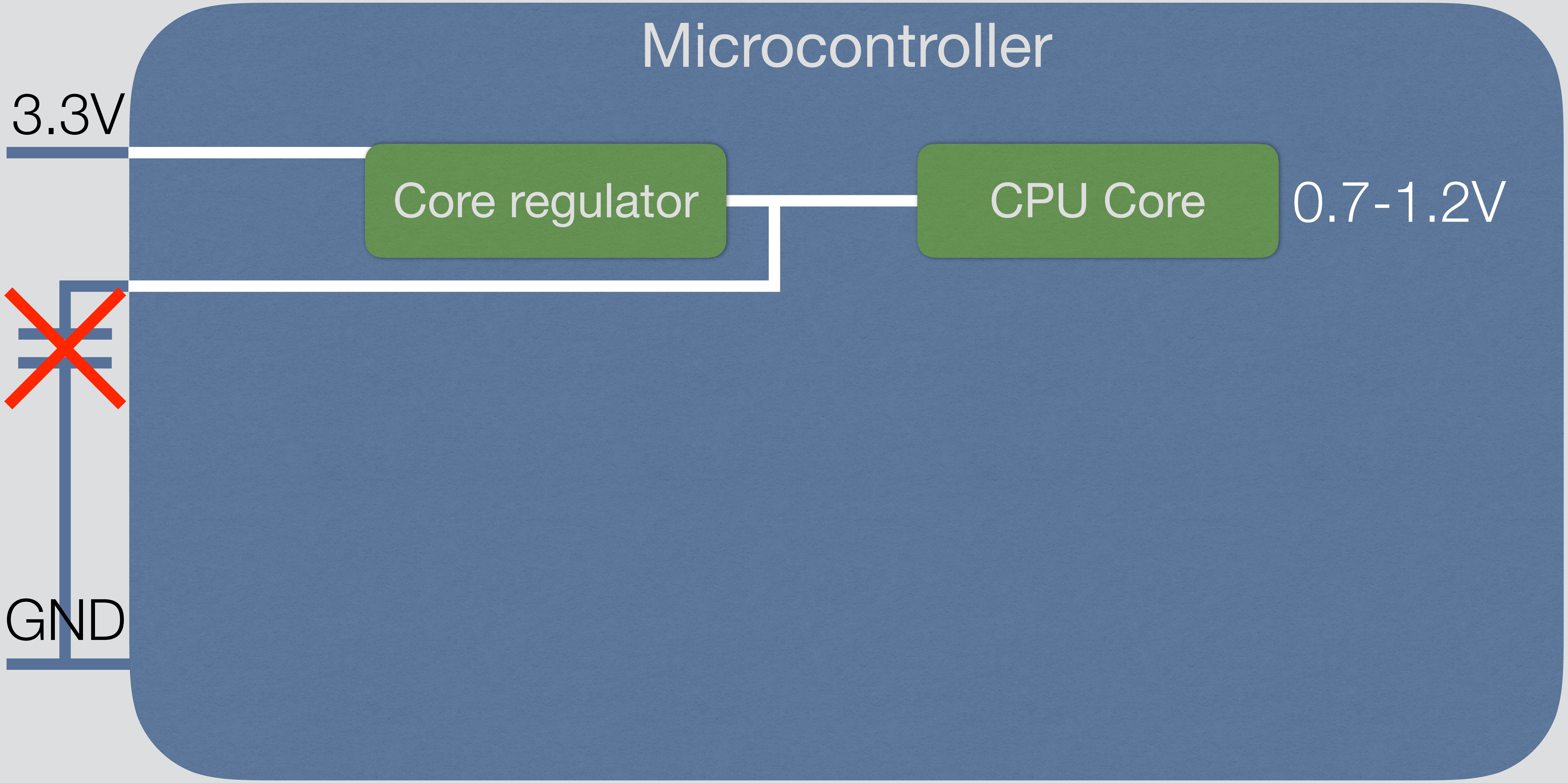
Bootrom Glitching



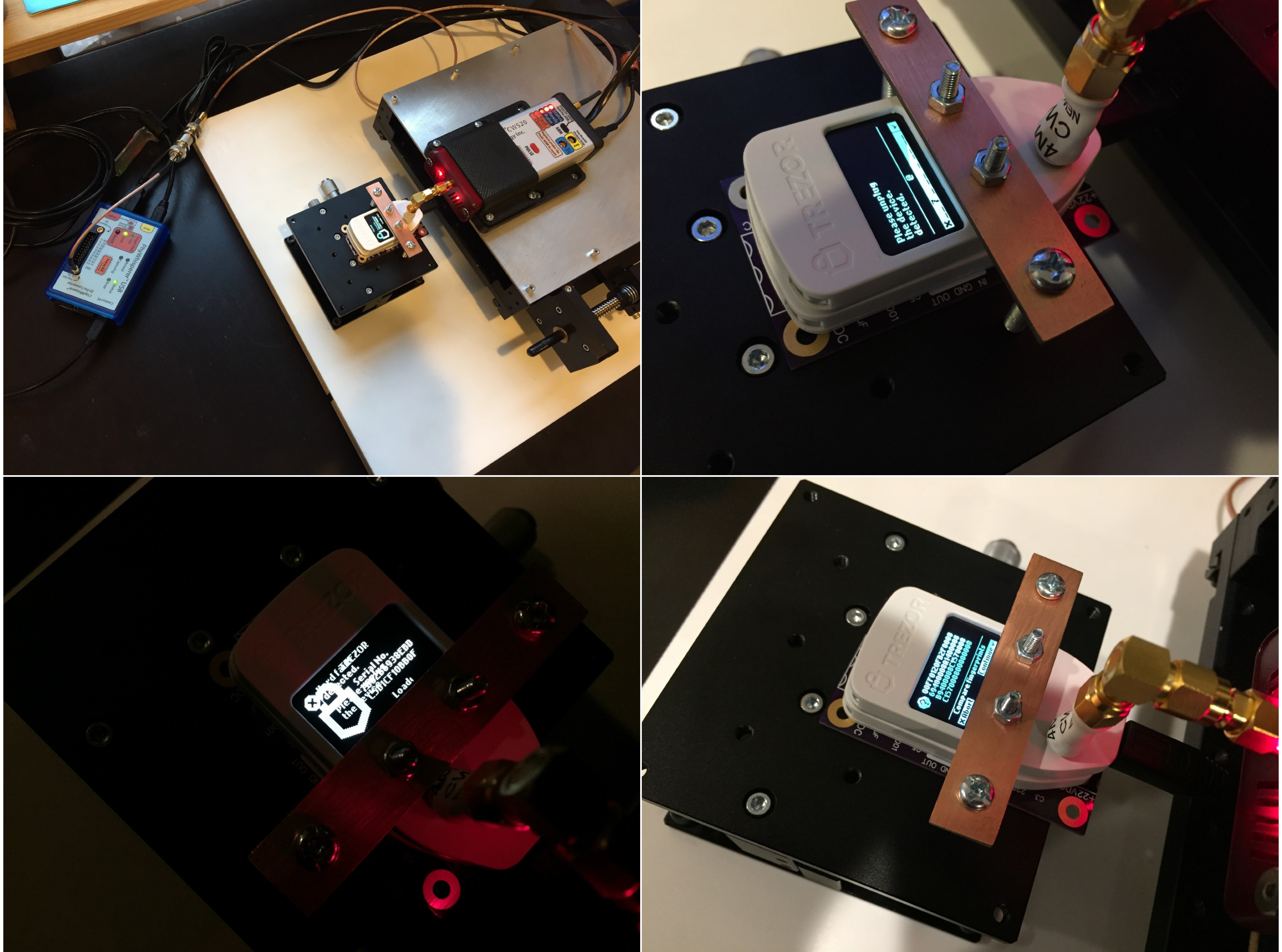
Power consumption after reset (200µs)

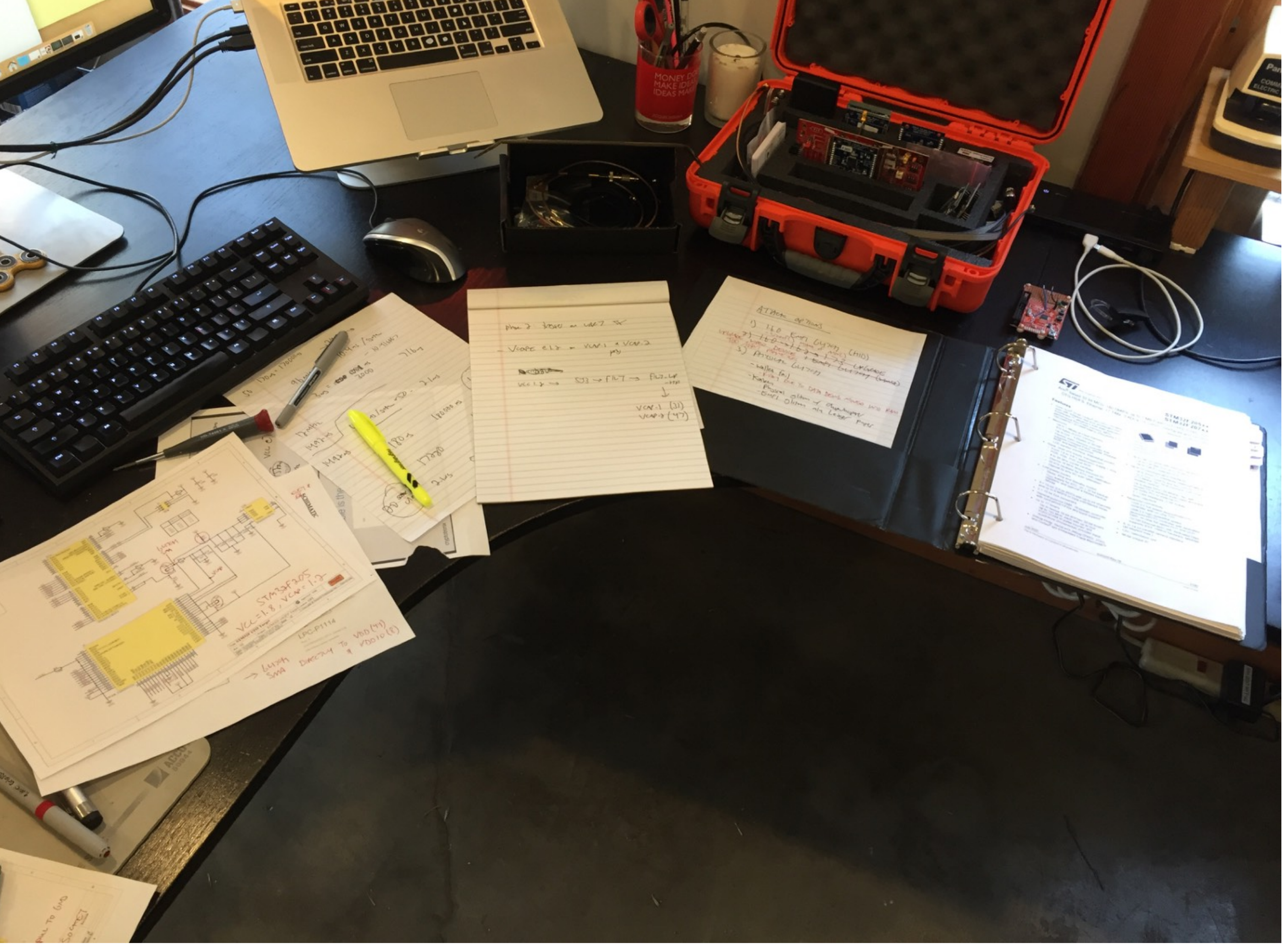


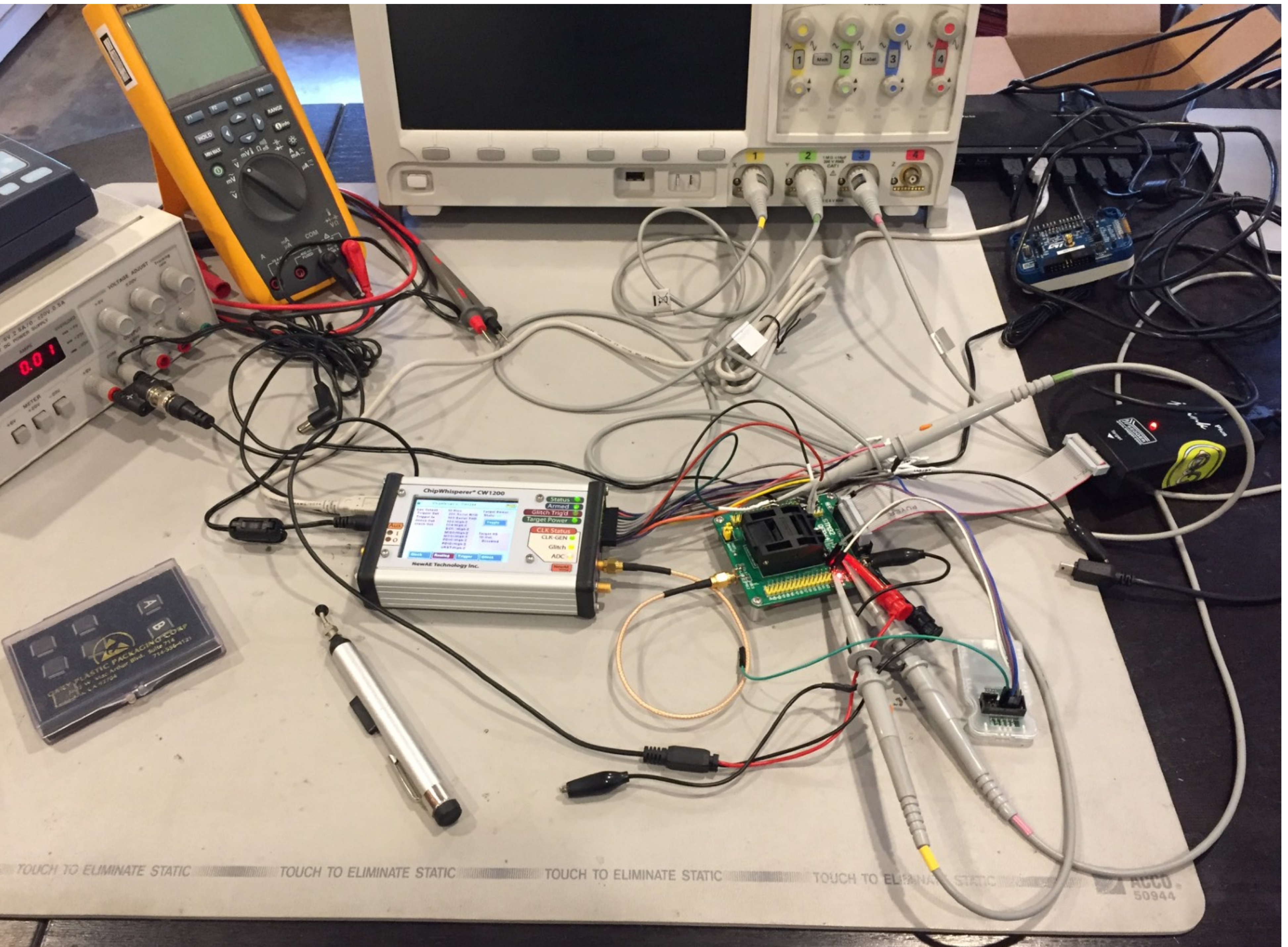
Power domains

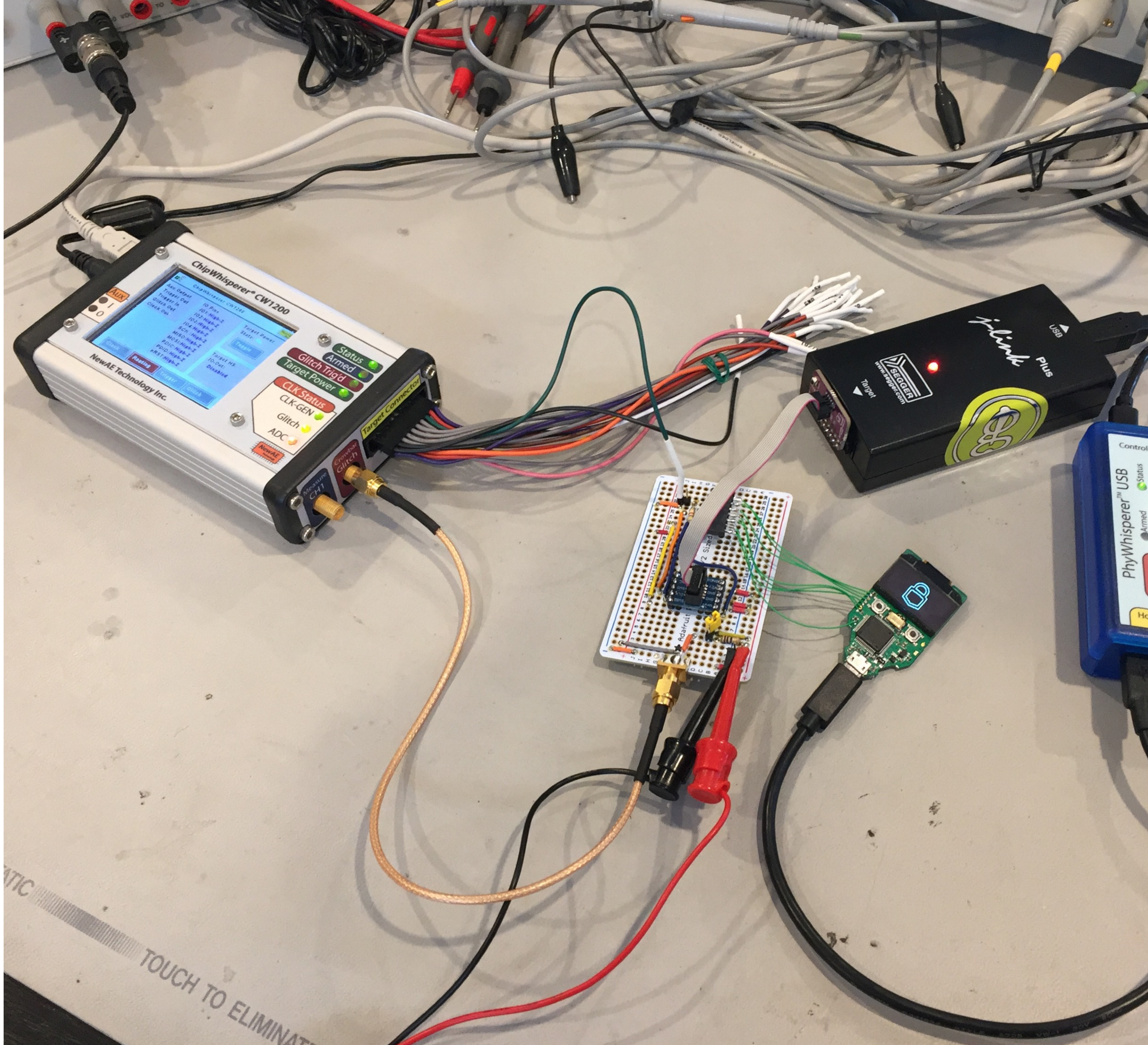


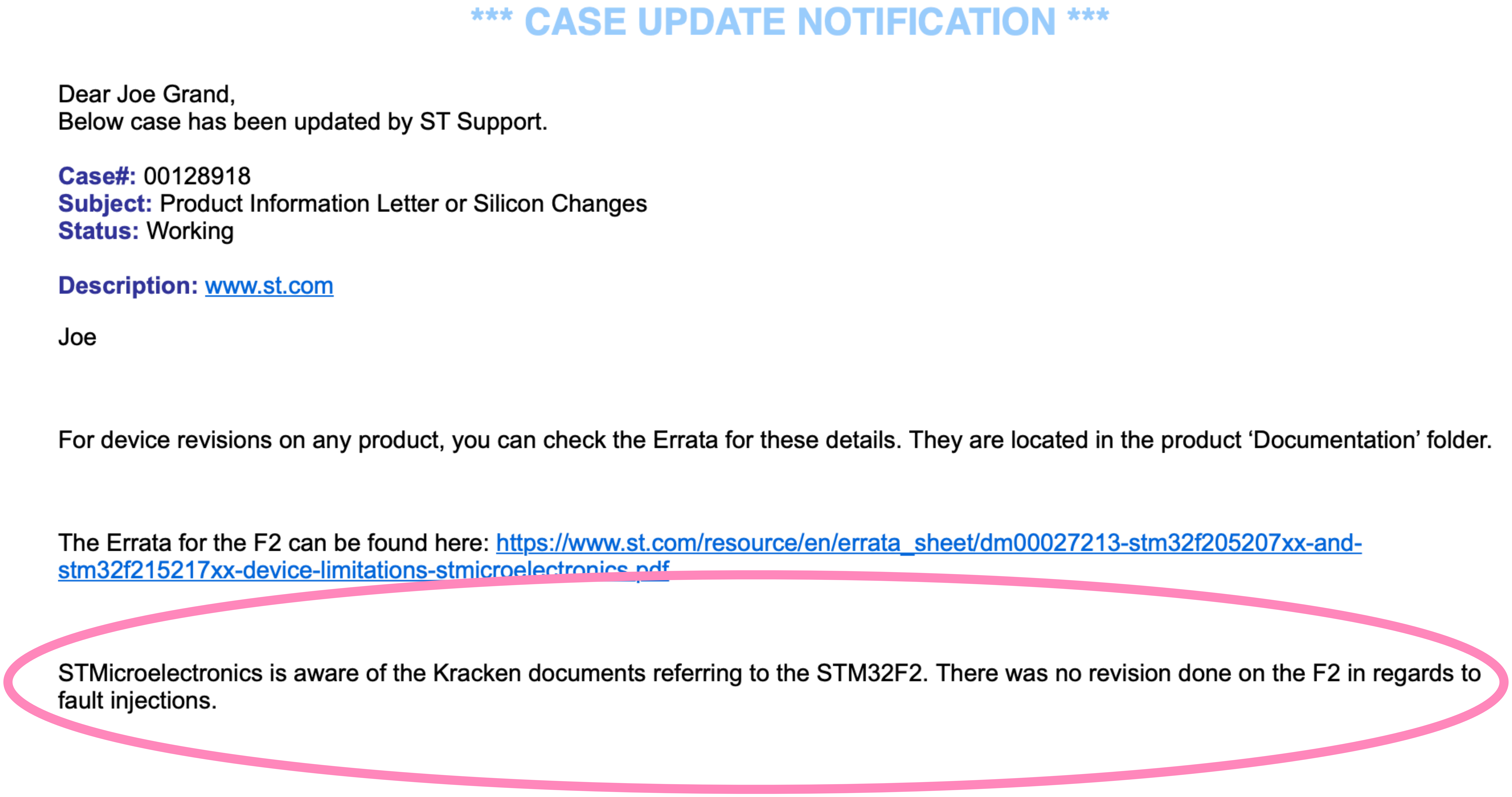
TRIAL AND ERROR


PhyWhisperer-USB
CW520
TREZOR
Please unplug the device.
TREZOR
Serial No.
Load
TREZOR
Compare fingerprints
Abort
Continue




ChipWhisperer CW1200
NewAE Technology Inc.
TOUCH TO ELIMINATE STATIC
TOUCH TO ELIMINATE STATIC
TOUCH TO ELIMINATE STATIC
TOUCH TO ELIMINATE STATIC


ChipWhisperer CW1200
NewAE Technology Inc.
AUX
Status
Armed
Glitch Trig'd
Target Power
CLK Status
CLK-GEN
Glitch
ADC
Target Connector
Measure CH1
Crowbar Glitch
j-link Plus
SEGGER
www.segger.com
USB
Target
PhyWhisperer USB
Status
Armed
Control
TOUCH TO ELIMINATE STATIC



*** CASE UPDATE NOTIFICATION ***

Dear Joe Grand,
Below case has been updated by ST Support.

Case#: 00128918
Subject: Product Information Letter or Silicon Changes
Status: Working

Description: www.st.com

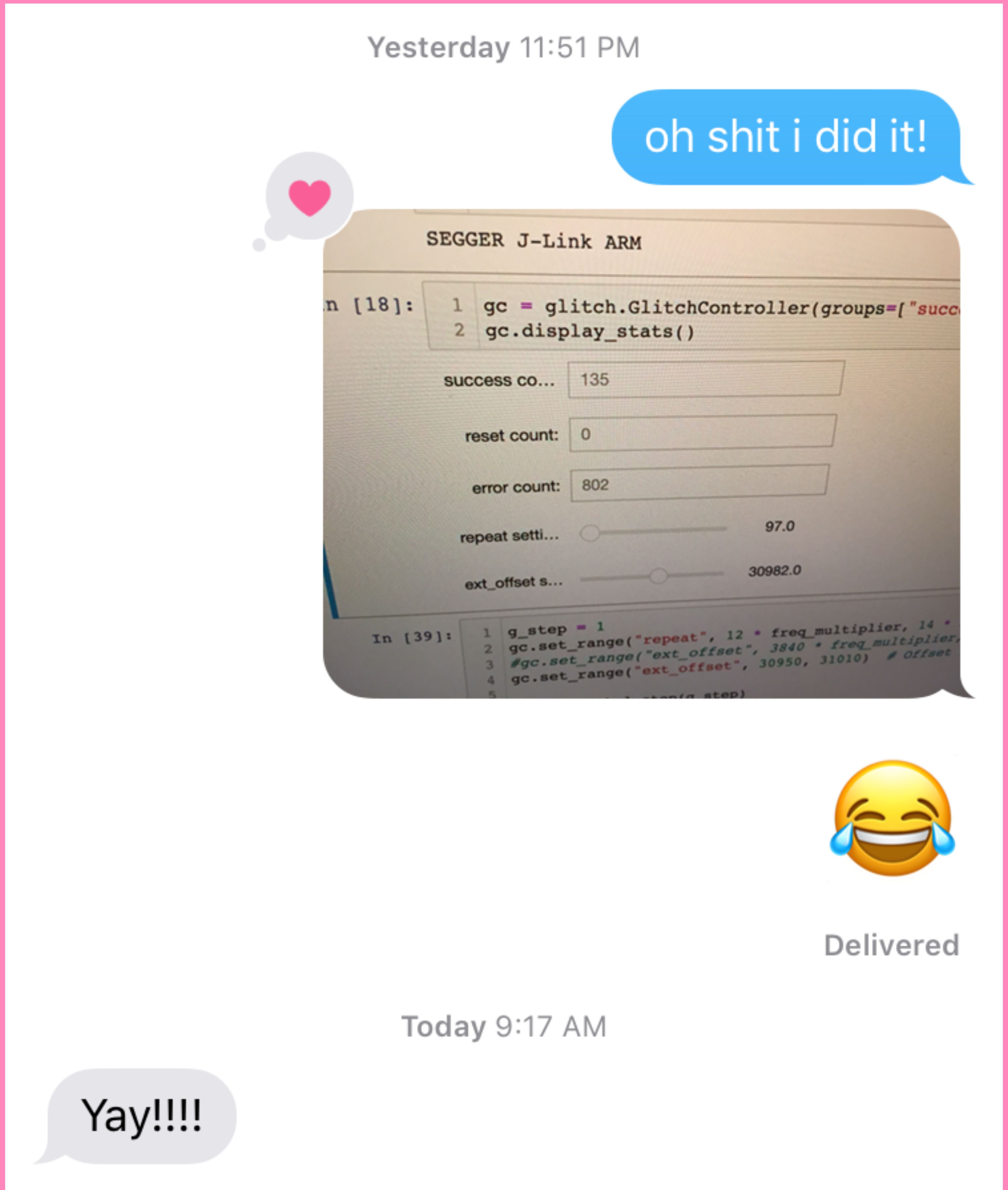
Joe

For device revisions on any product, you can check the Errata for these details. They are located in the product ‘Documentation’ folder.

The Errata for the F2 can be found here: https://www.st.com/resource/en/errata_sheet/dm00027213-stm32f205207xx-and-stm32f215217xx-device-limitations-stmicroelectronics.pdf

STMicroelectronics is aware of the Kracken documents referring to the STM32F2. There was no revision done on the F2 in regards to fault injections.

STM32F2
HAS NOT BEEN FIXED



Yesterday 11:51 PM

oh shit i did it!

SEGGER J-Link ARM

```
n [18]:  gc = glitch.GlitchController(groups=["succ
         gc.display_stats()
```

success co... 135

reset count: 0

error count: 802

repeat setti... 97.0

ext_offset s... 30982.0

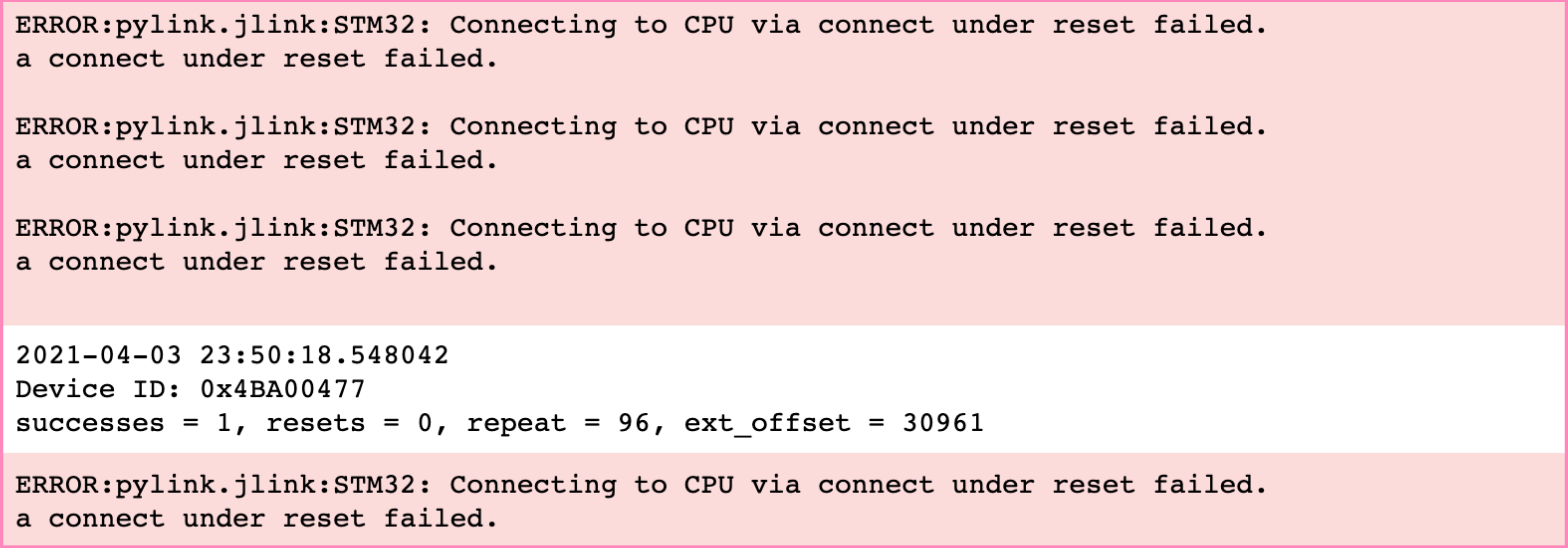
```
In [39]:  g_step = 1
          gc.set_range("repeat", 12 * freq_multiplier, 14 *
          gc.set_range("ext_offset", 3840 * freq_multiplier,
          #gc.set_range("ext_offset", 30950, 31010)  # Offset
          gc.set_range("ext_offset",
```

😂

Delivered

Today 9:17 AM

Yay!!!!

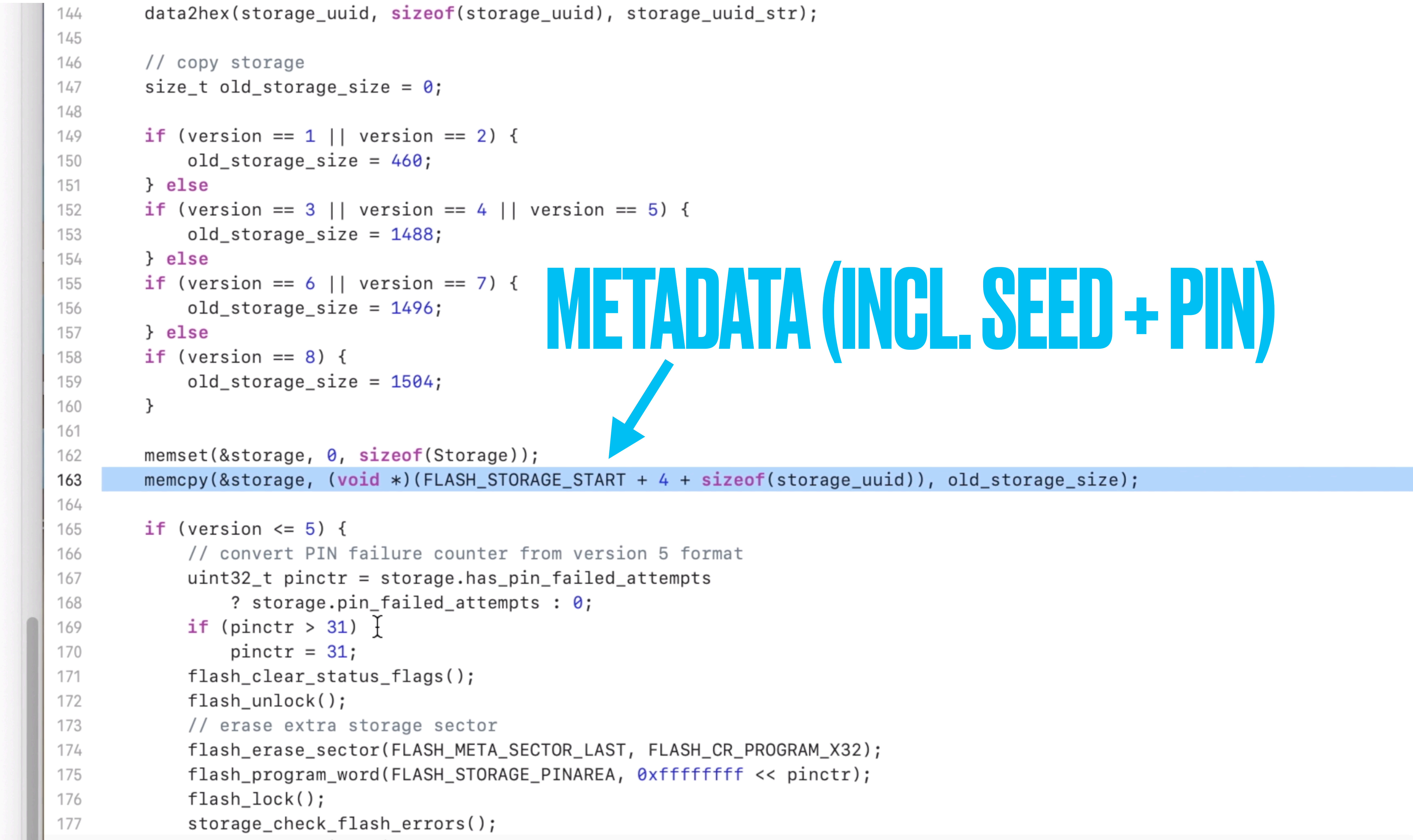


```
ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.
a connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.
a connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.
a connect under reset failed.

2021-04-03 23:50:18.548042
Device ID: 0x4BA00477
successes = 1, resets = 0, repeat = 96, ext_offset = 30961
ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.
a connect under reset failed.
```



```c
    data2hex(storage_uuid, sizeof(storage_uuid), storage_uuid_str);

    // copy storage
    size_t old_storage_size = 0;

    if (version == 1 || version == 2) {
        old_storage_size = 460;
    } else
    if (version == 3 || version == 4 || version == 5) {
        old_storage_size = 1488;
    } else
    if (version == 6 || version == 7) {
        old_storage_size = 1496;
    } else
    if (version == 8) {
        old_storage_size = 1504;
    }

    memset(&storage, 0, sizeof(Storage));
    memcpy(&storage, (void *)(FLASH_STORAGE_START + 4 + sizeof(storage_uuid)), old_storage_size);

    if (version <= 5) {
        // convert PIN failure counter from version 5 format
        uint32_t pinctr = storage.has_pin_failed_attempts
            ? storage.pin_failed_attempts : 0;
        if (pinctr > 31)
            pinctr = 31;
        flash_clear_status_flags();
        flash_unlock();
        // erase extra storage sector
        flash_erase_sector(FLASH_META_SECTOR_LAST, FLASH_CR_PROGRAM_X32);
        flash_program_word(FLASH_STORAGE_PINAREA, 0xffffffff << pinctr);
        flash_lock();
        storage_check_flash_errors();
```

METADATA (INCL. SEED + PIN)

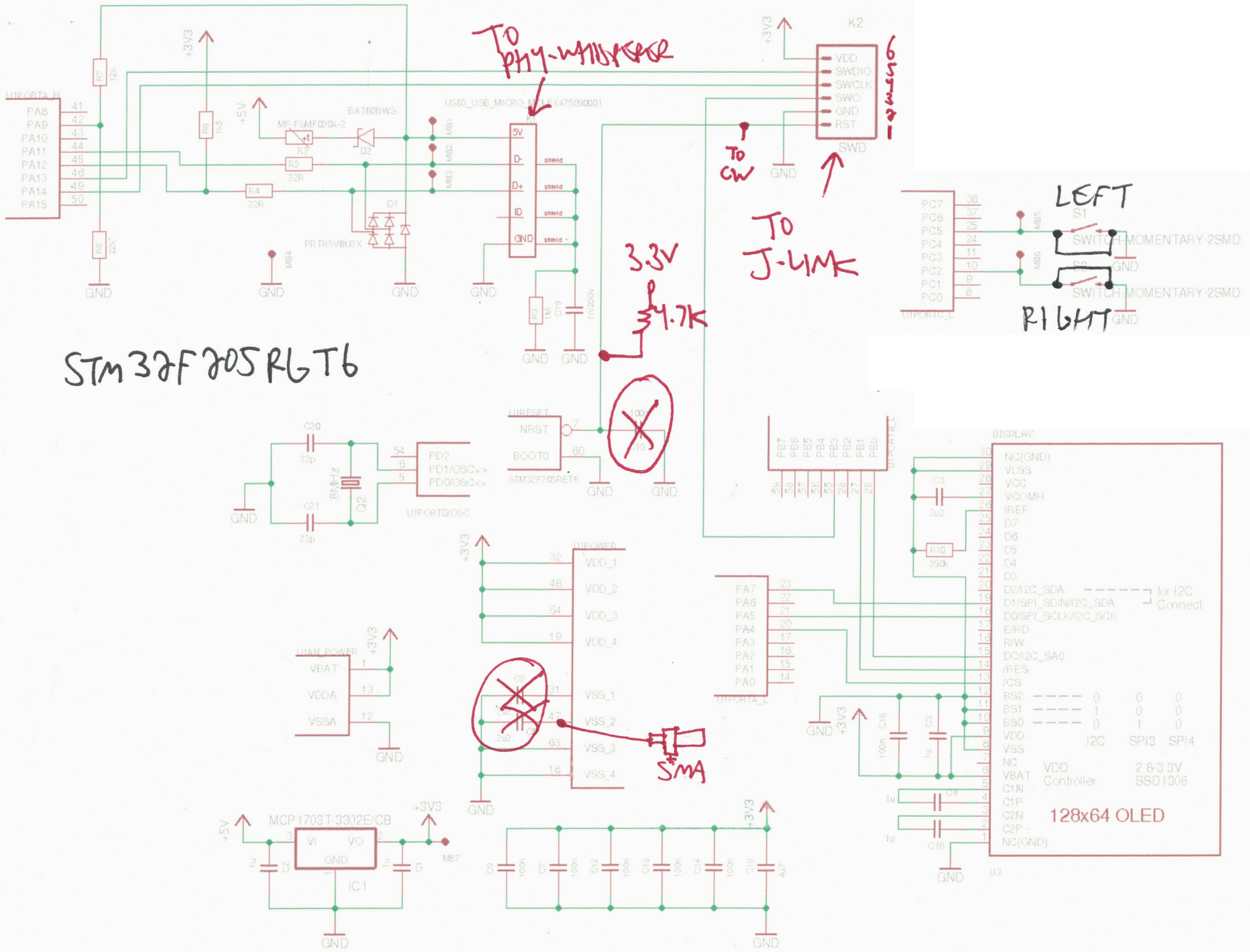
CHIPWHISPERER

PHYWHISPERER

SEGGER J-LINK

105
1720
017

Trezor HW 1.1



To PHY-WALLYSCOPE
To CW
To J-LINK
3.3V
4.7K
SMA
LEFT
RIGHT
STM32F205RGT6
6 5 4 3 2 1
U1PORTA_H
PA8
PA9
PA10
PA11
PA12
PA13
PA14
PA15
+3V3
+5V
R7 12k
R6 1k5
R8 22K
MF-FSMF020X-2
R2
BAT60BWS
D2
R3 22R
R4 22R
D1
PRTR5V0U2X
MB1
MB2
MB3
MB4
USB5_USB_MICRO_MOLEX475890001
K1
5V
D-
D+
ID
GND
shield
R9 1M
C19 10/200V
K2
VDD
SWDIO
SWCLK
SWO
GND
RST
SWD
PC7
PC6
PC5
PC4
PC3
PC2
PC1
PC0
U1PORTC_L
MB5
MB6
S1
S2
SWITCH-MOMENTARY-2SMD
U1RESET
NRST
BOOT0
STM32F205RET6
C15 100n
C20 22p
C21 22p
8MHz
Q2
PD2
PD1/OSC>>
PD0/OSC<<
U1PORTD/OSC
PB7
PB6
PB5
PB4
PB3
PB2
PB1
PB0
U1PORTB_L
U1POWER
VDD_1
VDD_2
VDD_3
VDD_4
VSS_1
VSS_2
VSS_3
VSS_4
U1AN_POWER
VBAT
VDDA
VSSA
C8 2u2
PA7
PA6
PA5
PA4
PA3
PA2
PA1
PA0
U1PORTA_L
DISPLAY
NC(GND)
VLSS
VCC
VCOMH
IREF
D7
D6
D5
D4
D3
D2/I2C_SDA
D1/SPI_SDIN/I2C_SDA
D0/SPI_SCLK/I2C_SCK
E/RD
R/W
DC/I2C_SA0
/RES
/CS
BS2
BS1
BS0
VDD
VSS
NC
VBAT
C1N
C1P
C2N
C2P
NC(GND)
for I2C Connect
I2C
SPI3
SPI4
VDD Controller
2.8-3.3V SSD1306
128x64 OLED
U3
C5 2u2
R10 390k
C16 100n
C3 1u
C4 1u
C18 1u
MCP1703T-3302E/CB
VI
VO
GND
IC1
MB7
C9
C10
C11
C12
C13
C14
100n
4u7
GND

THE REAL DEAL

DC 27
HODL
JE10
QUICK BRAID

DC 27
WIRE JUMPER KIT
JE10
QUICK BRAID
EASY BRAID
NO-CLEAN
Property of
BRAND 00153
SlickVise

ChipWhisperer® CW1200
Aux
Status
Armed
Glitch Trig'd
Target Power
CLK Status
CLK-GEN
Glitch
ADC
NewAE Technology Inc.
NewAE
j-link
Plus
SEGGER
www.segger.com
USB
Target
Adafruit
Control PC
ChipWhisperer®
20-Pin Connector
Trig Out (3.3V)
Status
Error
Armed
Capturing
PhyWhisperer™ USB
NewAE
DIO
V+ V+
CK G
D7 G
D6 G
D5 G
D4 G
D3 G
D2 G
D1 G
D0 G
Target PWR
+5V
Host
On/Off
Shunt Active
Normal
Shunt Out 5V
Host
Target

ΔX = 150.96000us
1/ΔX = 6.6243kHz
ΔY(1) = 0.0V

Mode
Normal

Coupling
DC

Noise Rej

HF Reject

Holdoff
60ns

DC 27
THAT PLANT LIFE

Home Page - Select or create a
Tribble - Jupyter Notebook
http://localhost:8888/notebooks/Tribble.ipynb
jupyter
Tribble Last Checkpoint: 5 hours ago (unsaved changes)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Trusted
Python 3
Run
Code

```
ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.
```

Step 2: Extract RAM Contents

On Trezor One firmware versions <= 1.6.0, the critical metadata (recovery seed + PIN) are stored in RAM on power-up. We can now use OpenOCD to extract the contents.

In [9]:

```
# Close PyLink to give control of Segger back to OS
jlink.close()
```

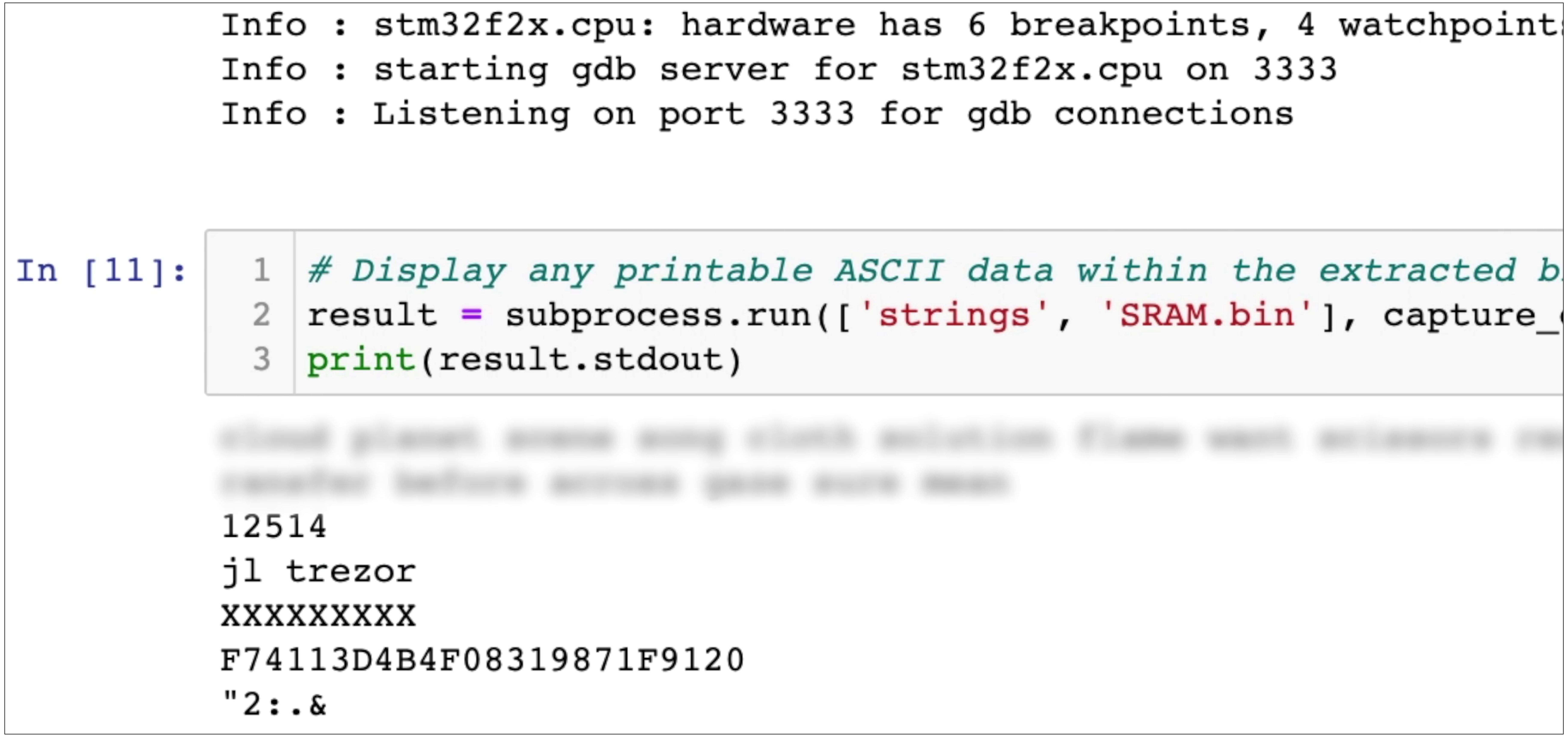
In [10]:

```
# Launch OpenOCD to extract RAM
# openocd -f interface/jlink.cfg -c "transport select swd" -f target/stm32f2x.cfg -c "init" -c "dump_image SRAM.bi
result = subprocess.run(['openocd', '-f', 'openocd_swd_trezor.cfg'], capture_output=True, text=True)
print(result.stderr)
```

```
Open On-Chip Debugger 0.11.0-rc2+dev-00006-gf68ade529-dirty (2021-02-03-18:32)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.org/doc/doxygen/bugs.html
Info : J-Link V9 compiled Dec 13 2019 11:14:50
Info : Hardware version: 9.30
Info : VTarget = 3.319 V
Info : clock speed 1000 kHz
Info : SWD DPIDR 0x2ba01477
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoints
Error: stm32f2x.cpu -- clearing lockup after double fault
Polling target stm32f2x.cpu failed, trying to reexamine
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoints
Info : starting gdb server for stm32f2x.cpu on 3333
Info : Listening on port 3333 for gdb connections
```

In [ ]:

```
# Display any printable ASCII data within the extracted binary
result = subprocess.run(['strings', 'SRAM.bin'], capture_output=True, text=True)
print(result.stdout)
```



```
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoint
Info : starting gdb server for stm32f2x.cpu on 3333
Info : Listening on port 3333 for gdb connections
```

In [11]:

```
# Display any printable ASCII data within the extracted b
result = subprocess.run(['strings', 'SRAM.bin'], capture_
print(result.stdout)
```

[redacted]

```
12514
jl trezor
XXXXXXXXX
F74113D4B4F08319871F9120
"2:.&
```

WHITE PAPER
Grand Ideas
#FreeTheta
Theta

LESSONS LEARNED

LESSONS LEARNED

- General purpose MCU security is not always suitable

LESSONS LEARNED

- General purpose MCU security is not always suitable
- Fault injection is dependent on many external factors
  - Glitch "quality"
  - Glitch parameters (timing, width)
  - Temperature
  - Manufacturing variances in silicon

LESSONS LEARNED

- General purpose MCU security is not always suitable
- Fault injection is dependent on many external factors
  - Glitch "quality"
  - Glitch parameters (timing, width)
  - Temperature
  - Manufacturing variances in silicon
- When it works, it feels like magic

RESOURCES

- Trezor
- wallet.fail and chip.fail
- Kraken Identifies Critical Flaw in Trezor Hardware Wallets
- Verifying Code Readout Protection Claims
- Shedding too much Light on a Microcontroller’s Firmware Protection
- Trezor - security glitches reveal your private keys!
- Cracking a $2 million crypto wallet (The Verge)
- How I hacked a hardware crypto wallet and recovered $2 million (YouTube)
- offspec.io

HACKED BY
Joe GRAND
$KINGPIN$