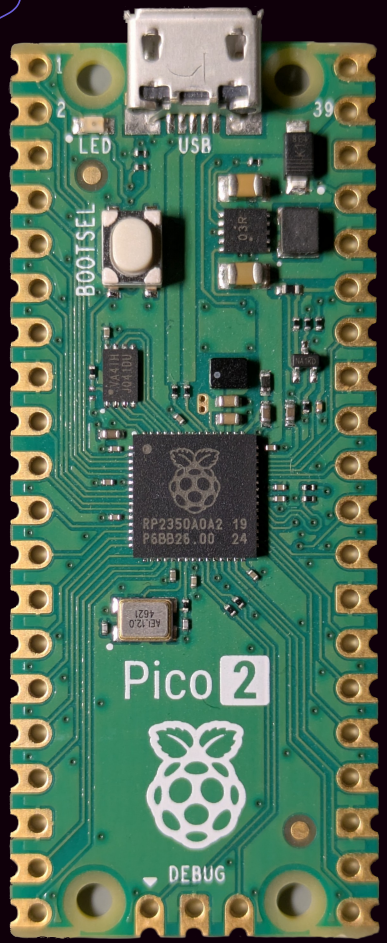


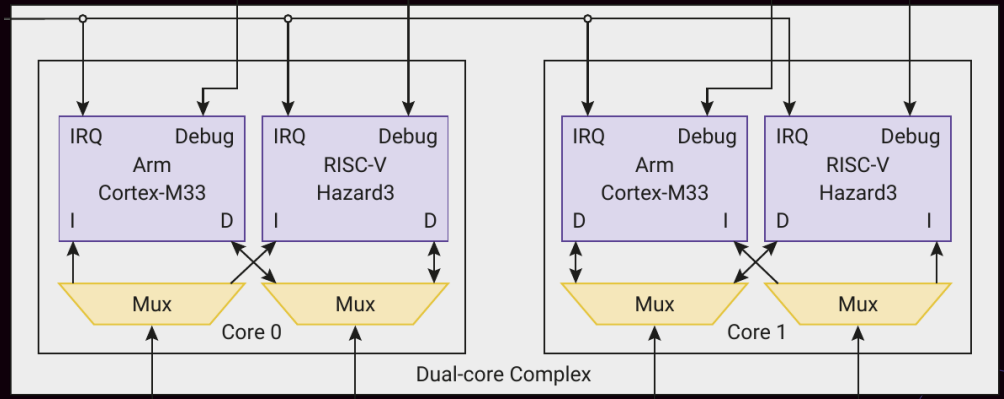
ILLEGAL
INSTRUCTIONS

HACKING THE RP2350

Aedan Cullen

A secure microcontroller with a supportive vendor?

- Raspberry Pi seems to be targeting commercial/industrial MCU customers
- Evolution of RP2040 ideas, more SRAM, etc.
- What is this weird core-swapping thing?!



"Double your embedded CPU architectures, double your fun!"

- Raspberry Pi

- Audited (to some extent?) by Hextree and NewAE
- Challenge started at DEF CON, then extended

Challenge goal: Read out a protected OTP secret

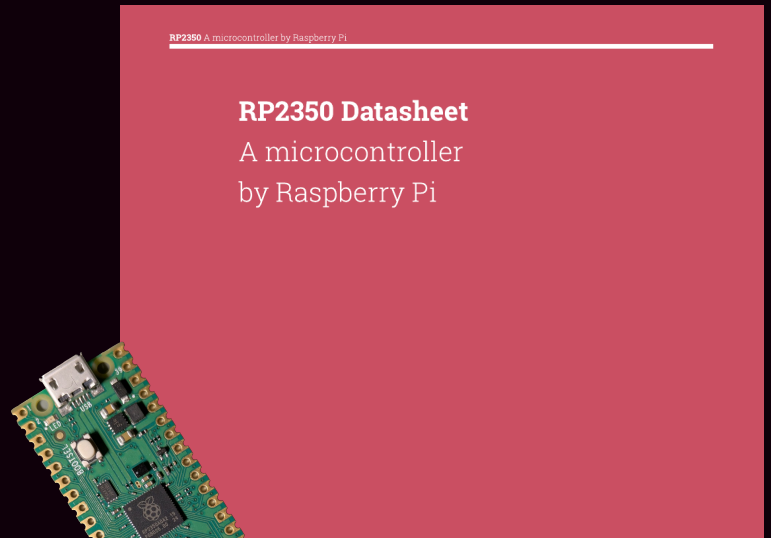
```
picotool otp set -e 0xc08 0xc0ff
picotool otp set -e 0xc09 0xffee
picotool otp set -e 0xc0a 0xc0ff
picotool otp set -e 0xc0b 0xffee
picotool otp set -e 0xc0c 0xc0ff
picotool otp set -e 0xc0d 0xffee
picotool otp set -e 0xc0e 0xc0ff
picotool otp set -e 0xc0f 0xffee
```

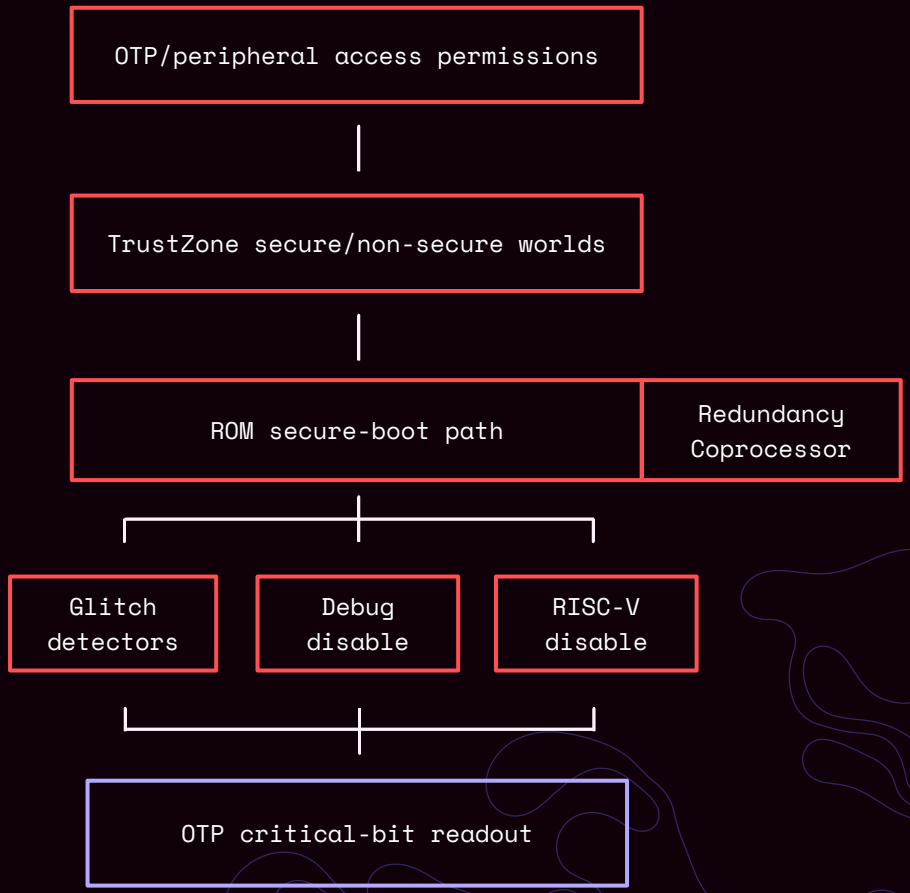
Then, lock down chip, enabling:

- OTP PAGE48 lock
- Secure boot
- Glitch detectors
- Debug-disable option

1. Critical thinking

An overview of the RP2350's security





1. Critical thinking

An overview of the RP2350's security

OTP_DATA: **CRIT1** (row 0x040; eight copies)

23:7	Reserved
6:5	**GLITCH_DETECTOR_SENS:** Increase the sensitivity of the glitch detectors from their default.
4	**GLITCH_DETECTOR_ENABLE:** Arm the glitch detectors to reset the system if an abnormal clock/power event is observed.
3	**BOOT_ARCH:** Set the default boot architecture, 0=ARM 1=RISC-V. Ignored if ARM_DISABLE, RISCV_DISABLE or SECURE_BOOT_ENABLE is set.
2	**DEBUG_DISABLE:** Disable all debug access
1	**SECURE_DEBUG_DISABLE:** Disable Secure debug access
0	**SECURE_BOOT_ENABLE:** Enable boot signature enforcement, and permanently disable the RISC-V cores

1. Critical thinking

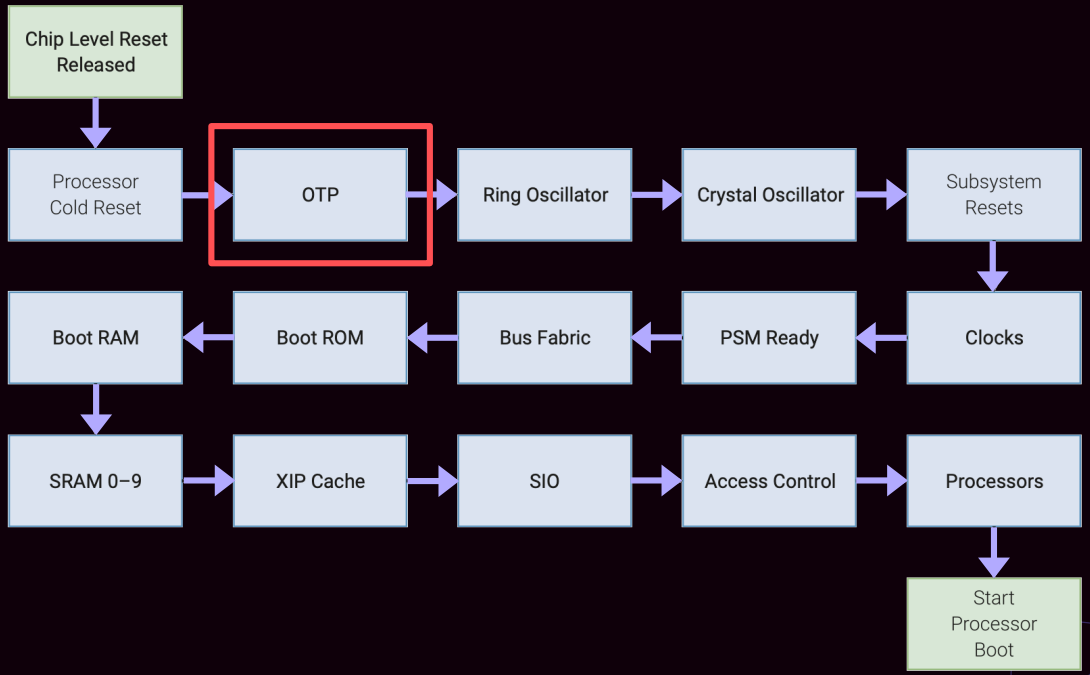
An overview of the RP2350's security

OTP_DATA: **CRIT0** (row 0x038; eight copies)

23:2	Reserved
1	**RISCV_DISABLE:** Permanently disable RISC-V processors (Hazard3)
0	**ARM_DISABLE:** Permanently disable ARM processors (Cortex-M33)

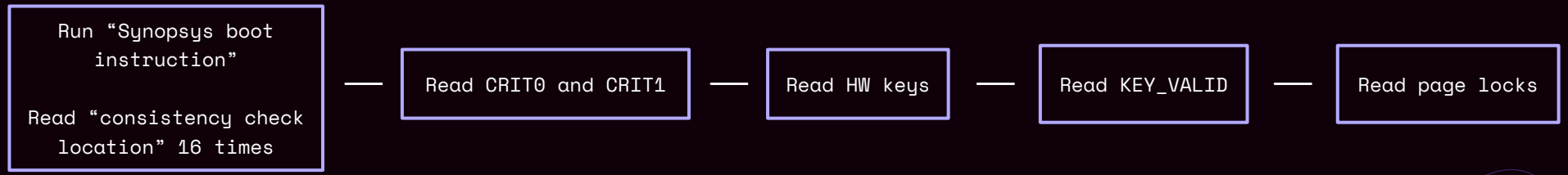
1. Critical thinking

An overview of the RP2350's security



1. Critical thinking

An overview of the RP2350's security



"Guarded reads perform an additional hardware consistency check to detect power transients. If this check fails, the read returns a bus fault. "

1. Critical thinking

An overview of the RP2350's security

OTP_DATA: **CRIT0** (three-of-eight)

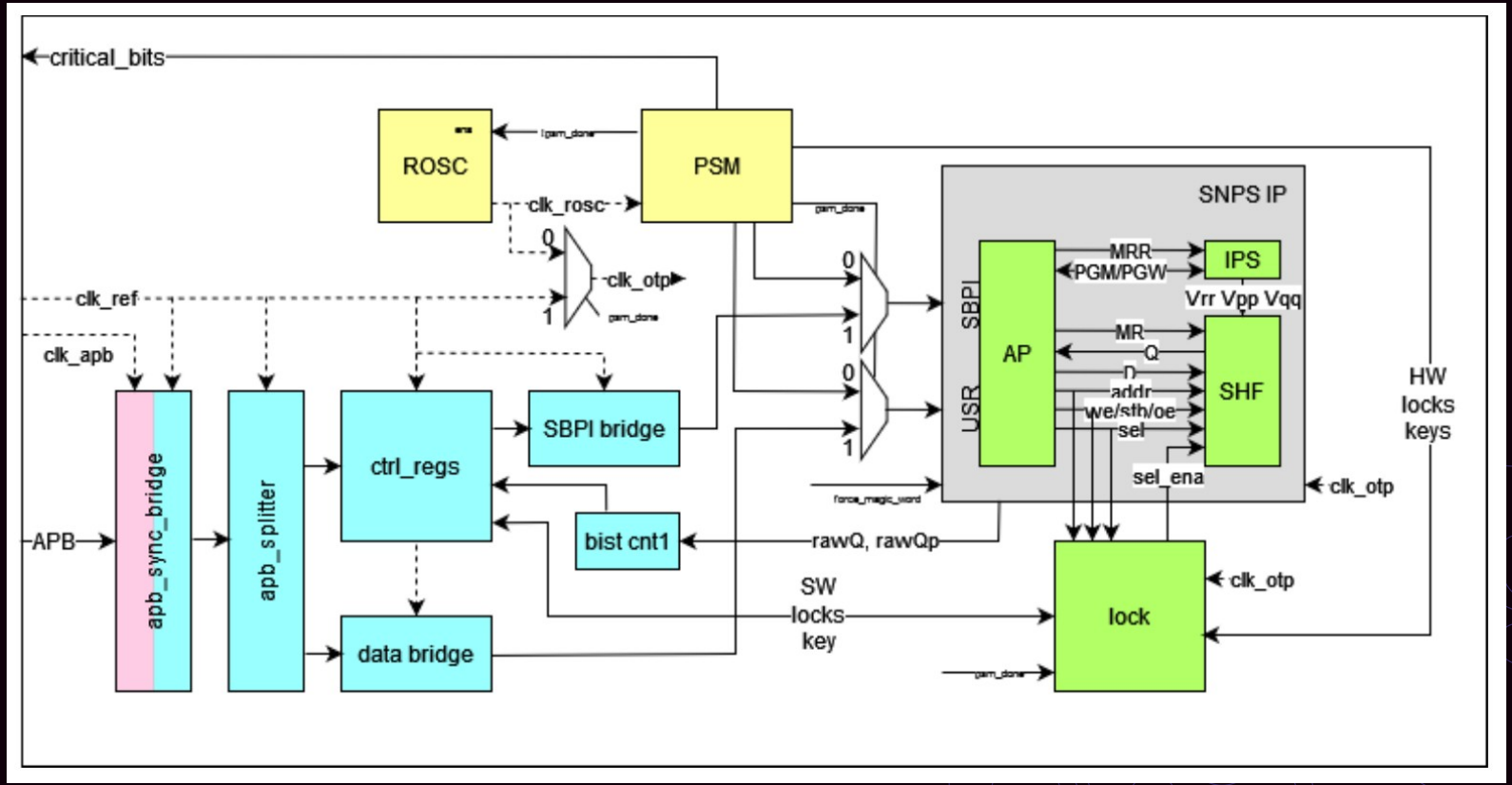
OTP_DATA: **CRIT1** (three-of-eight)

OTP: **CRITICAL** (0x40120148)

31:18	Reserved
17	RISCV_DISABLE
16	ARM_DISABLE
15:7	Reserved
6:5	GLITCH_DETECTOR_SENS
4	GLITCH_DETECTOR_ENABLE
3	DEFAULT_ARCHSEL
2	DEBUG_DISABLE
1	SECURE_DEBUG_DISABLE
0	SECURE_BOOT_ENABLE

2. Anti-fuse fuse club

Details of the chip's OTP design



2. Anti-fuse fuse club

Details of the chip's OTP design

Sidense
The Future of Logic NVM™

Sidense 1T-OTP Memory Macros Meet JEDEC Accelerated Testing Qualifications

At two TSMC 28nm process nodes

This is a Press Release edited by StorageNewsletter.com on December 31, 2013 at 2:51 pm

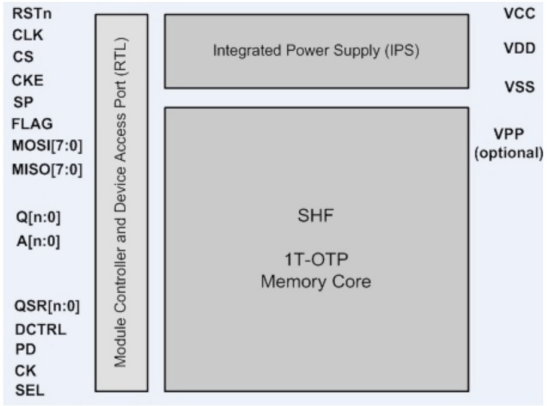
Sidense Corp., developer of non-volatile memory OTP IP cores, announced that its SHF Non-Volatile Memory (NVM) macros have met JEDEC accelerated testing requirements for TSMC's 28HPM and 28HPL process nodes.

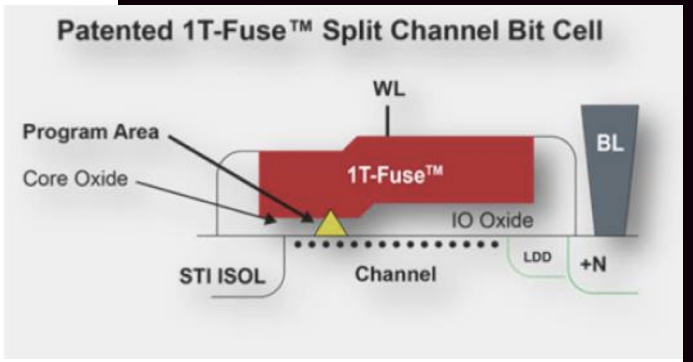
Synopsys Expands DesignWare IP Portfolio with Acquisition of Sidense Corporation

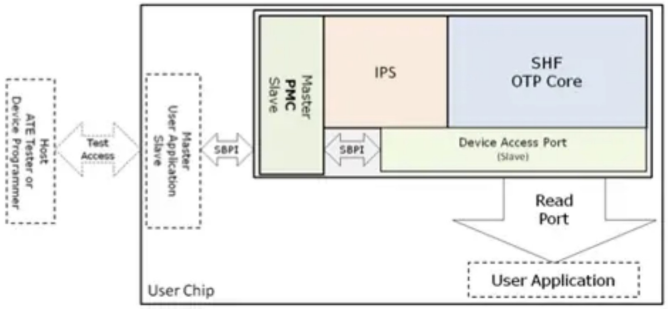
Acquisition Adds One-Time Programmable Non-Volatile Memory IP to DesignWare NVM IP Offering

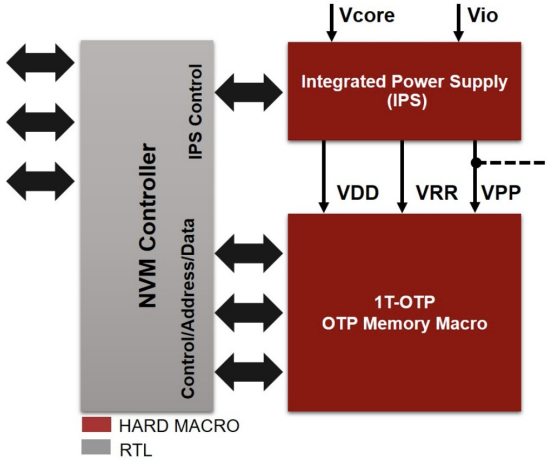
Share:

MOUNTAIN VIEW, Calif., Oct. 17, 2017 /PR



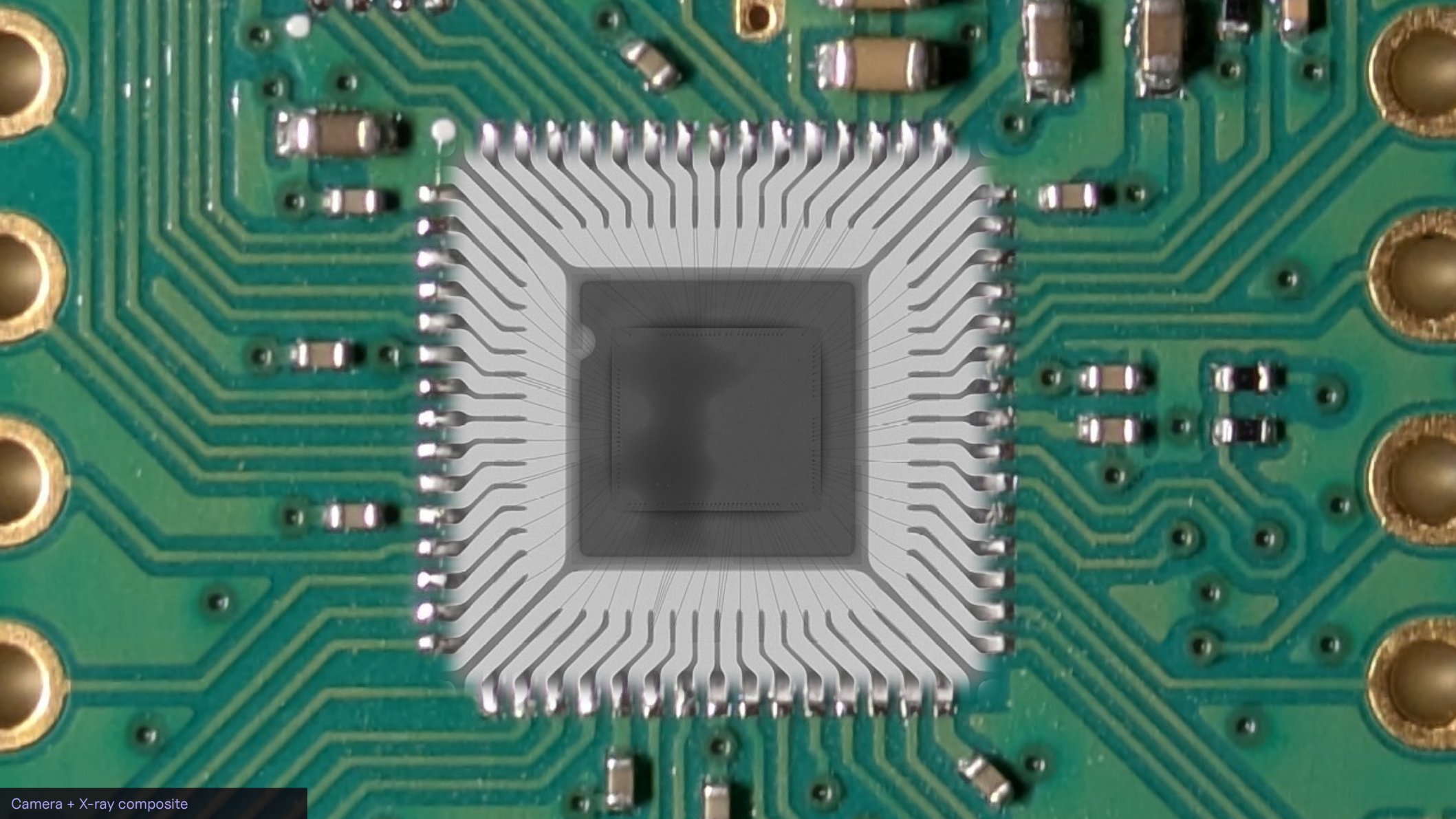


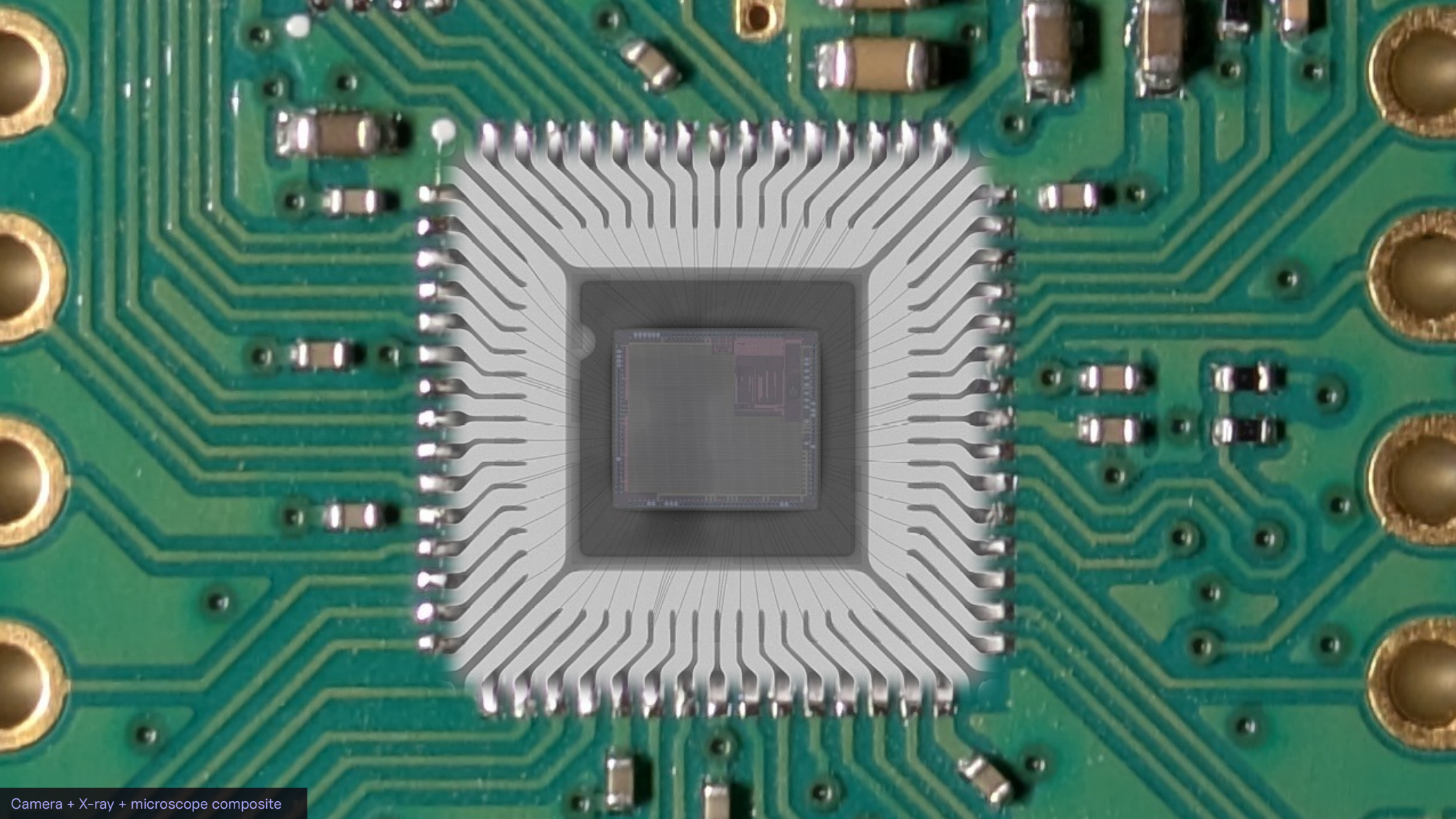




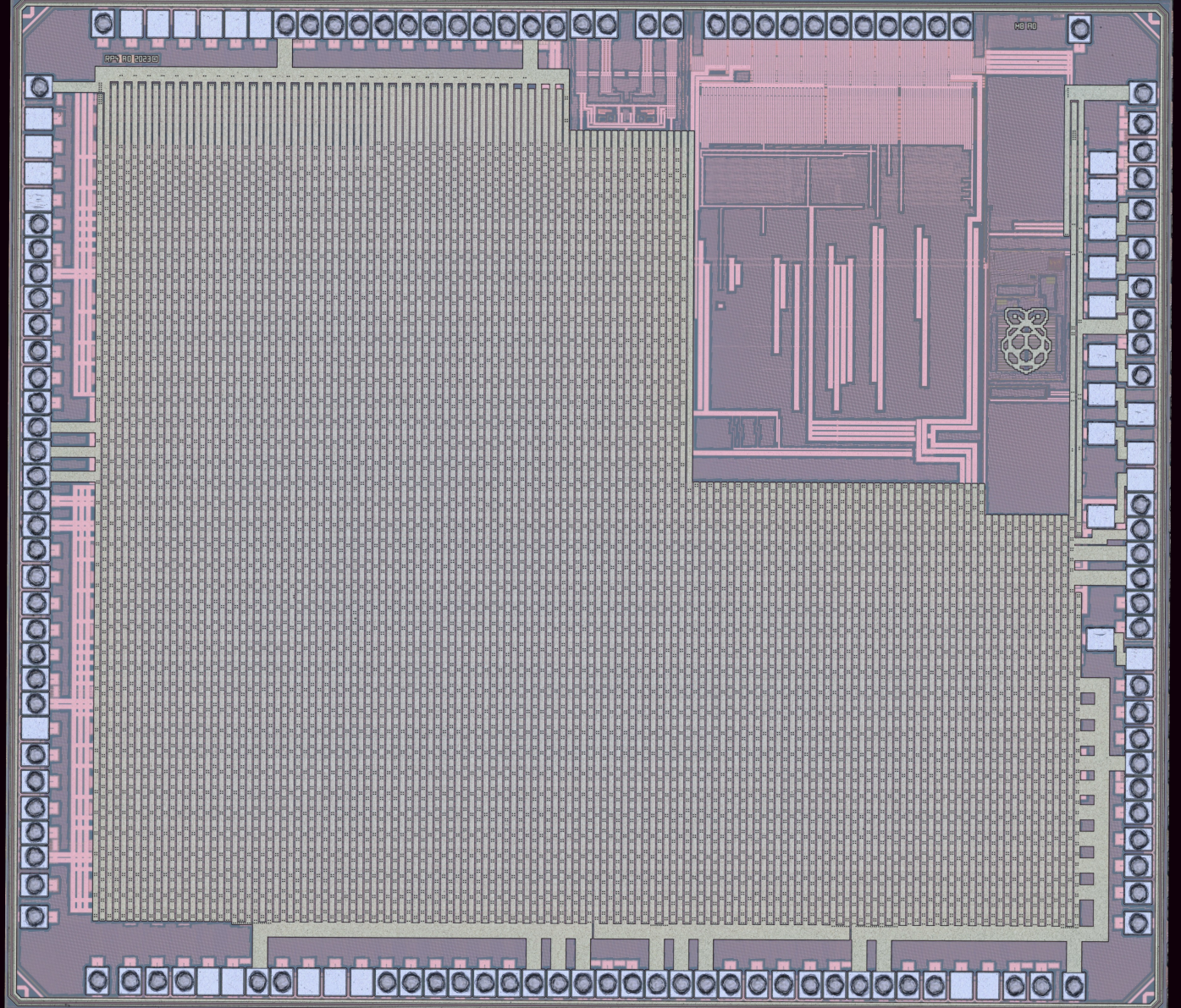
An SHF module consists of an OTP core (the bitcell array), charge pump hard macro for in-field programming (generates the non-standard voltages required), device access port (DAP) providing access through 16/32 bit parallel bus and SBPI, which provides serial and byte-wide interfaces with SPI-compatible protocols. Read speeds are as low as 20ns depending on configuration and process and (at 28/20nm) a 1us/bit write speed.


RP2350A0A2 19
P6BB26.00 24

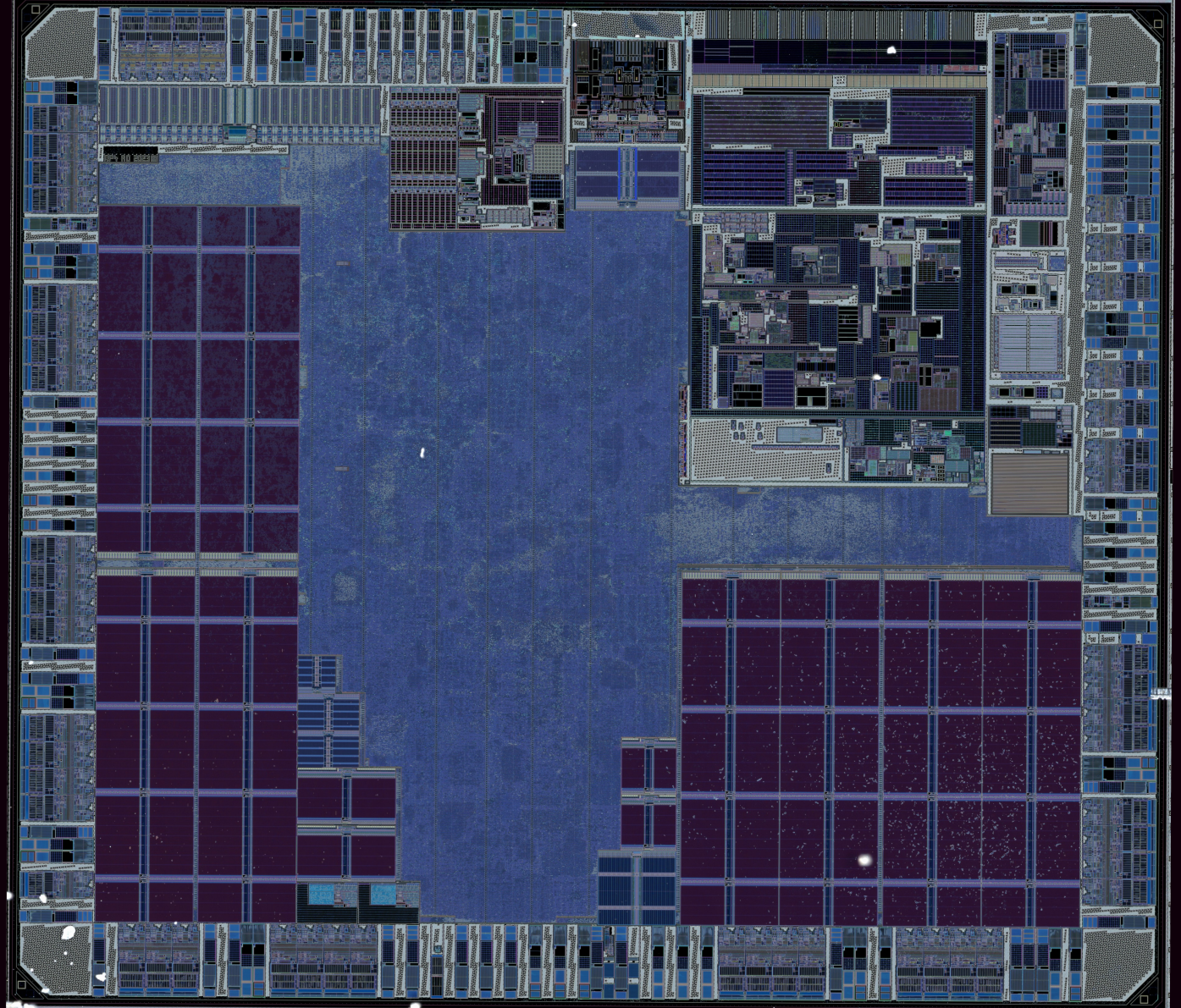

Camera + X-ray composite



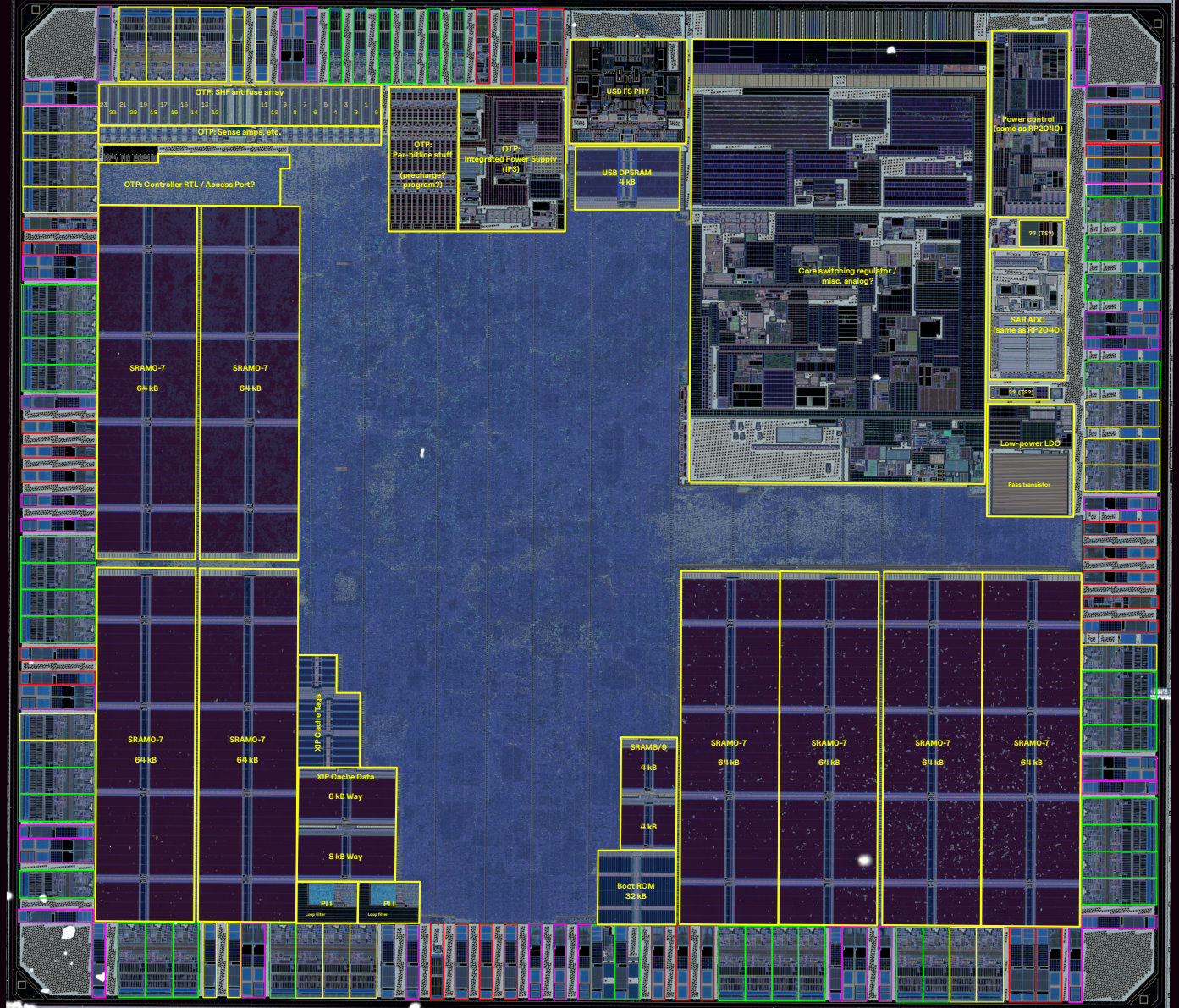
Camera + X-ray + microscope composite



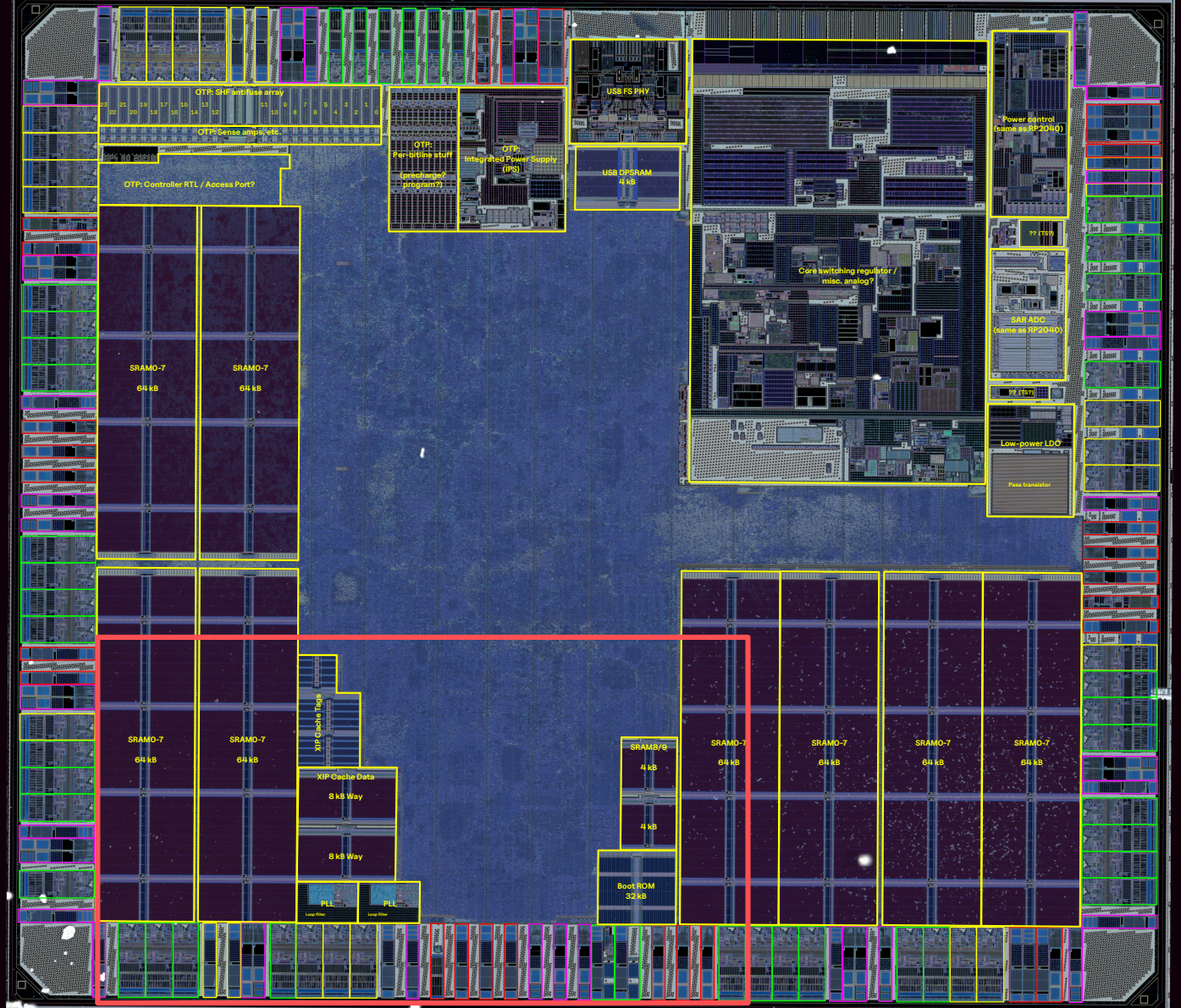
Optical microscope image



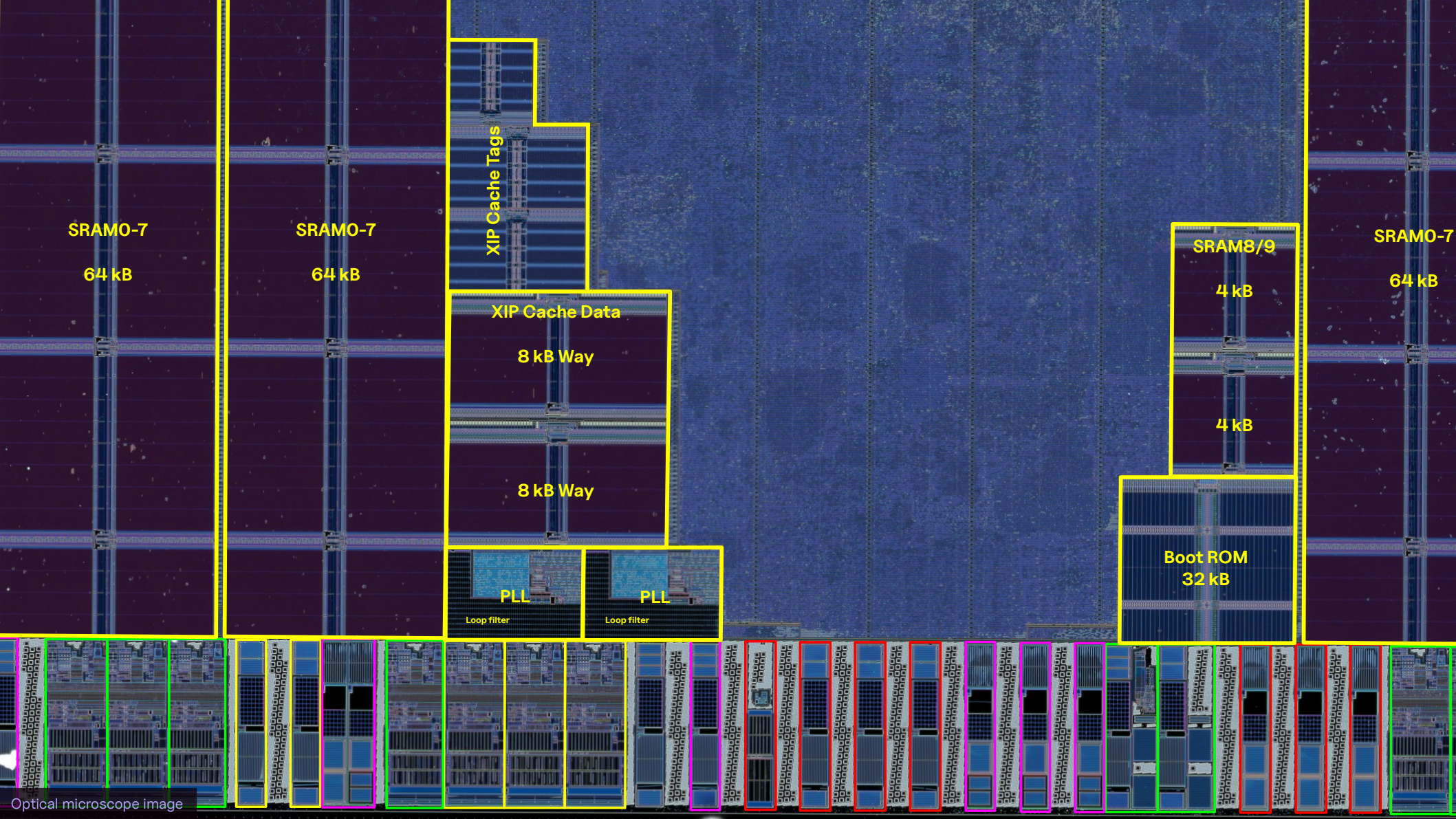
Optical microscope image

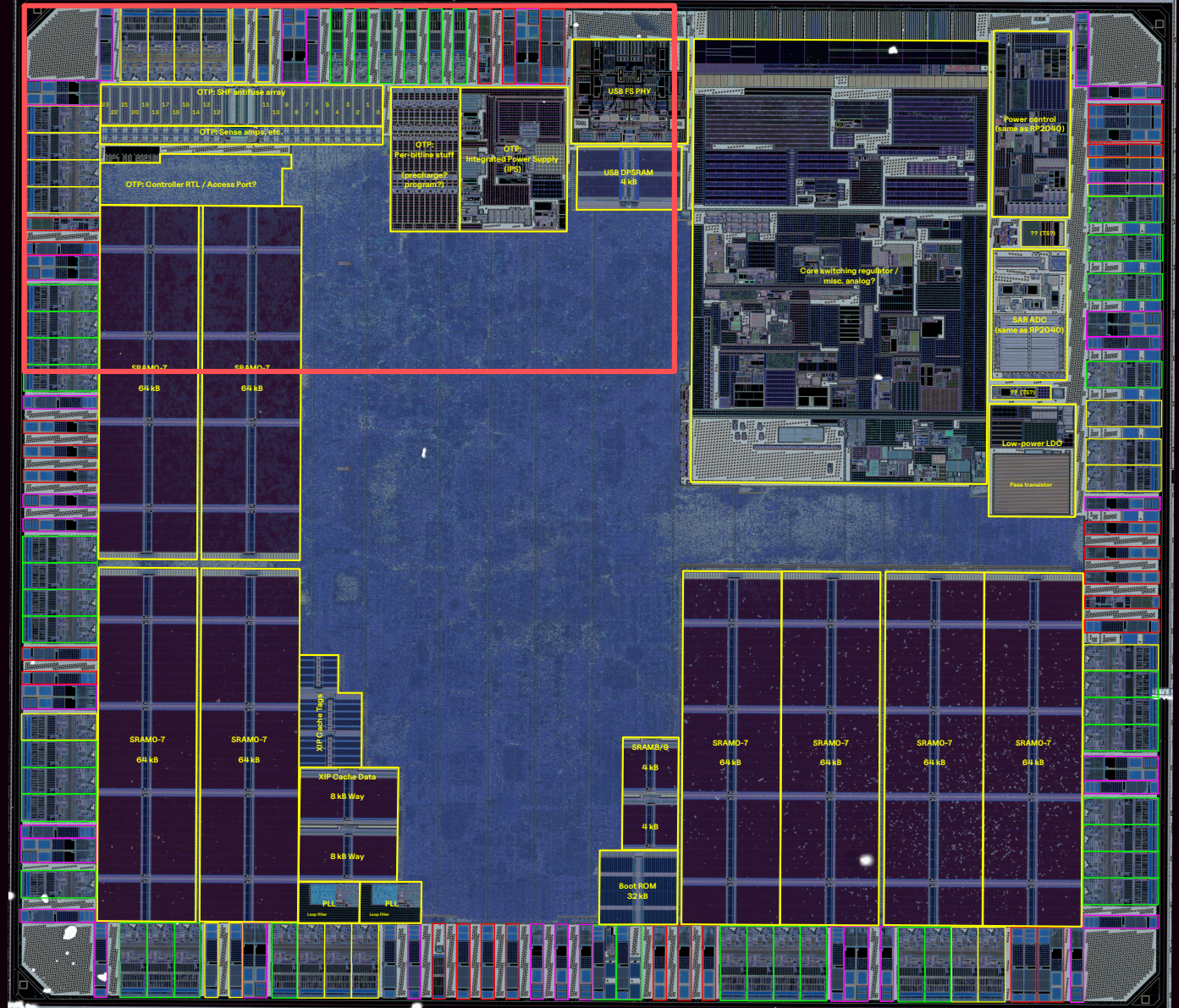


Optical microscope image

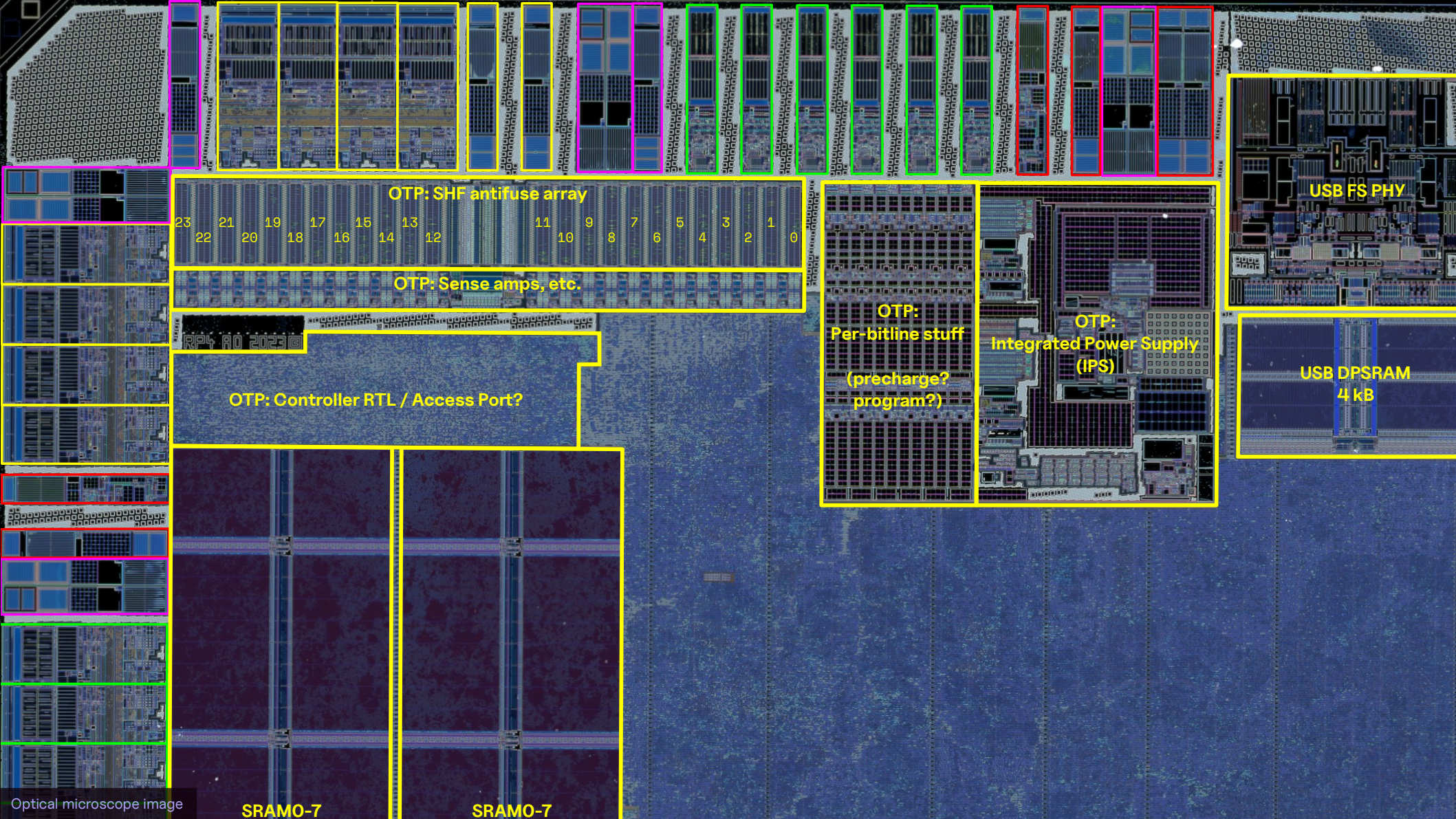


Optical microscope image

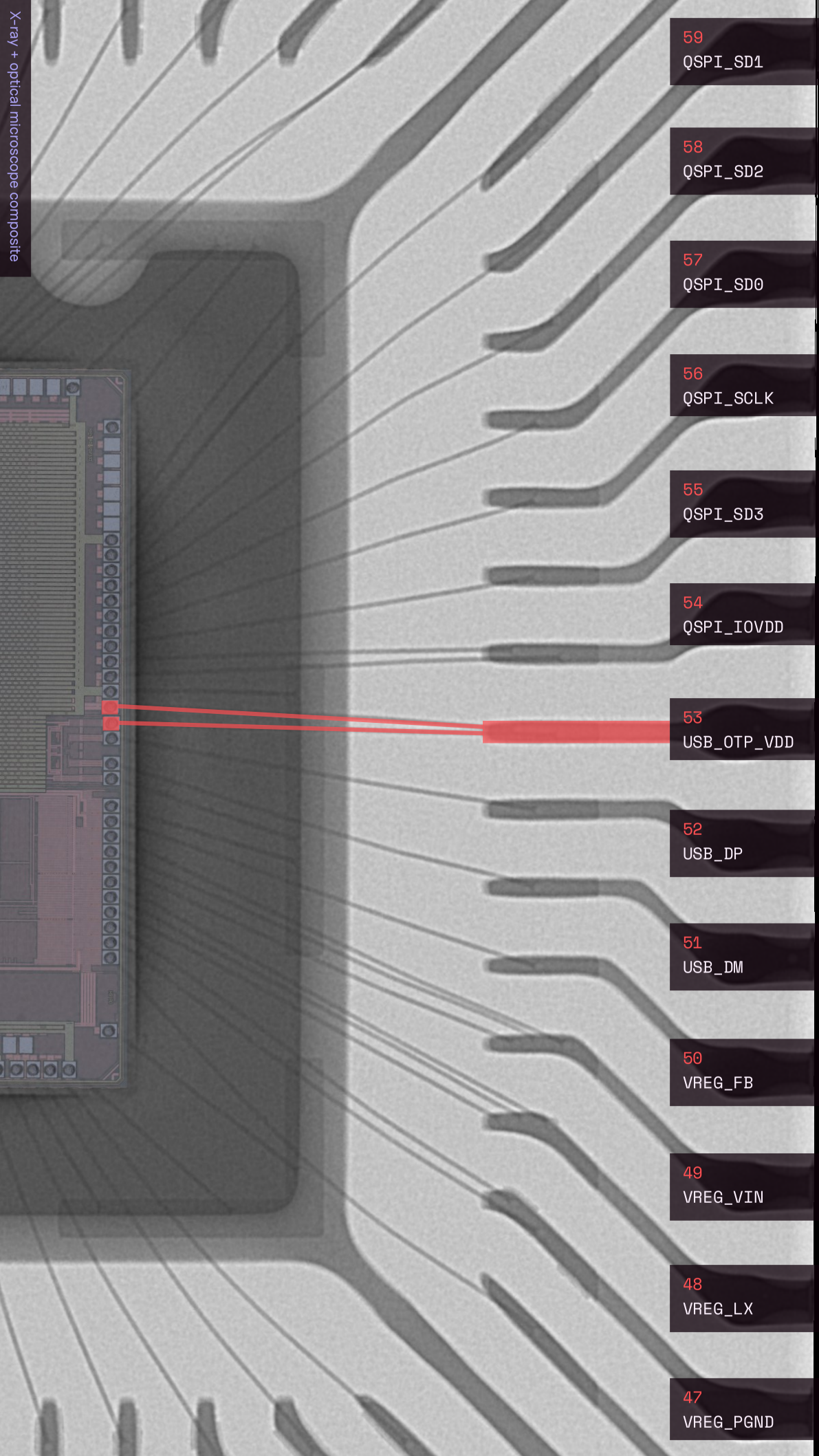

SRAM0-7
64 kB
SRAM0-7
64 kB
XIP Cache Tags
XIP Cache Data
8 kB Way
8 kB Way
PLL
Loop filter
PLL
Loop filter
SRAM8/9
4 kB
4 kB
Boot ROM
32 kB
SRAM0-7
64 kB
Optical microscope image

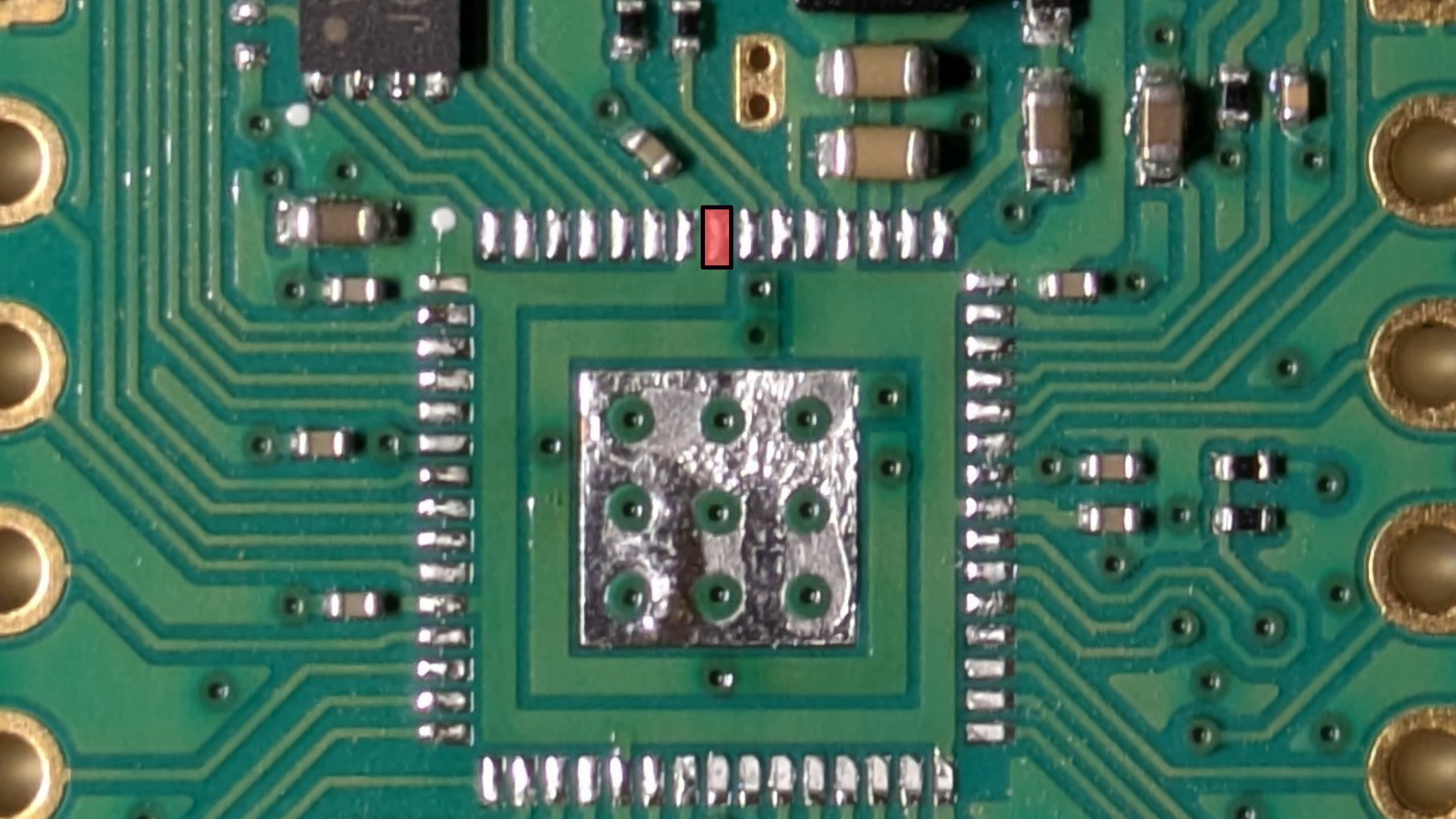


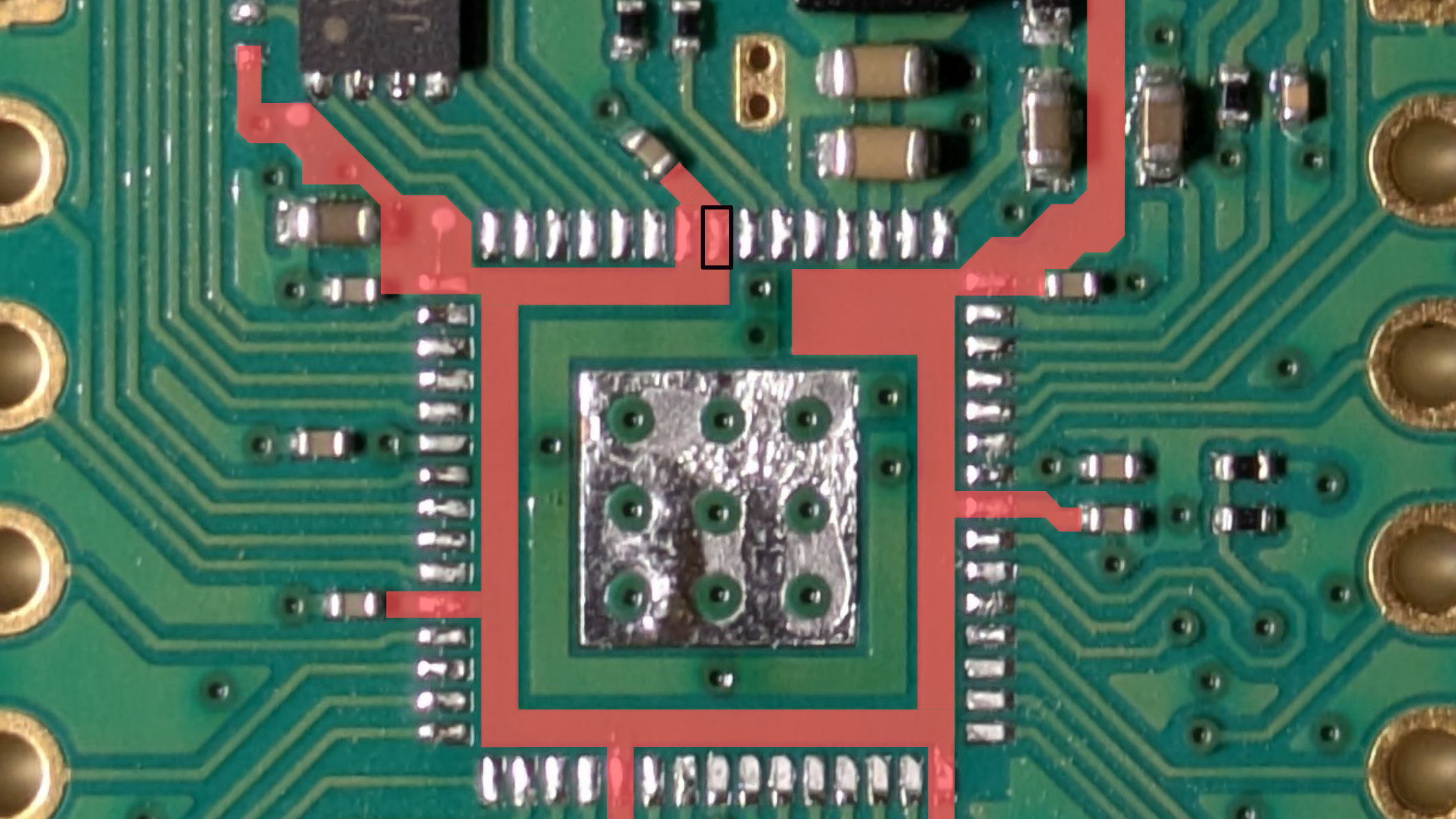
Optical microscope image

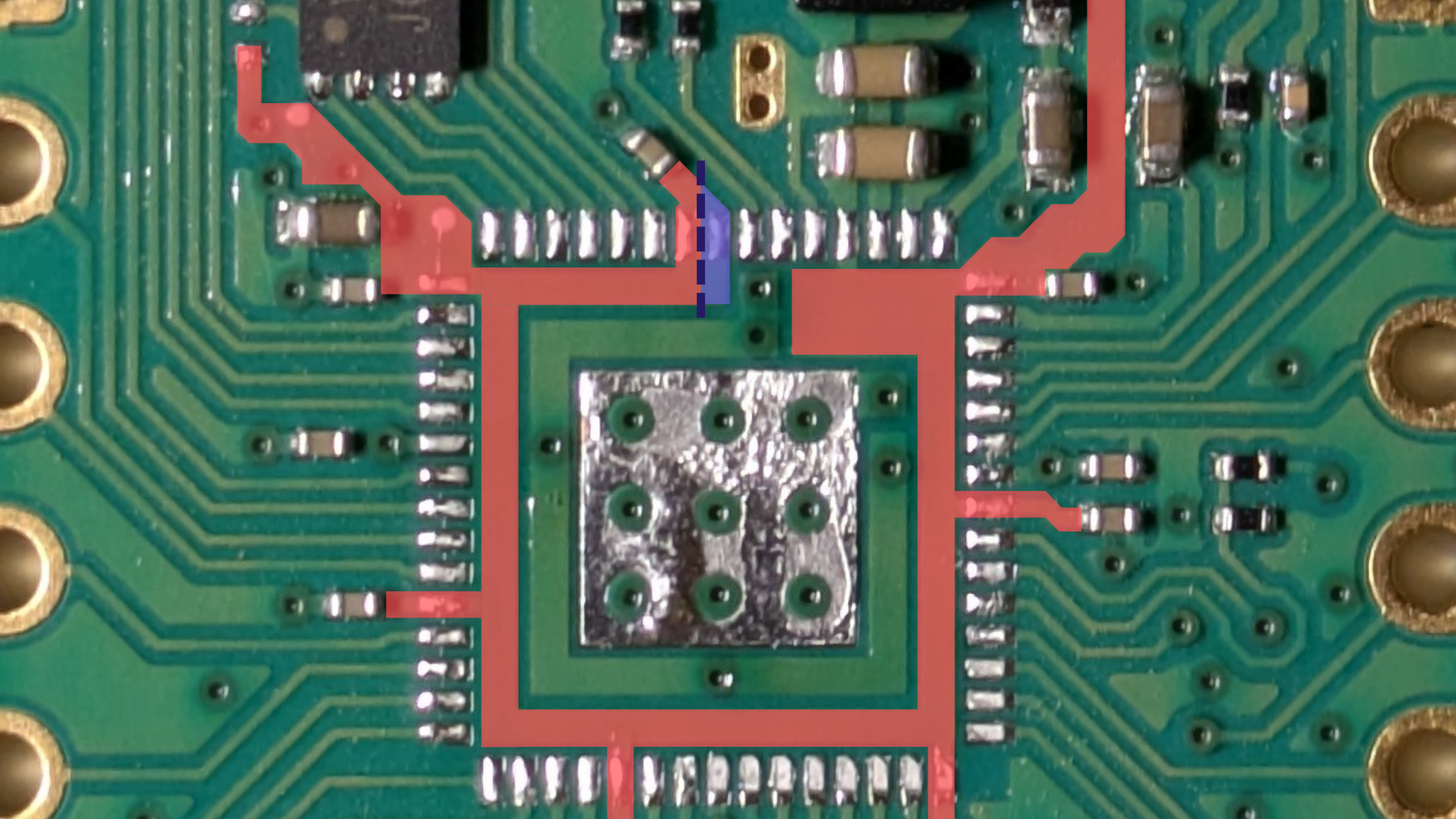

OTP: SHF antifuse array
23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
OTP: Sense amps, etc.
RP1 A0 2023
OTP: Controller RTL / Access Port?
OTP:
Per-bitline stuff
(precharge?
program?)
OTP:
Integrated Power Supply
(IPS)
USB FS PHY
USB DPSRAM
4 kB
SRAM0-7
SRAM0-7
Optical microscope image

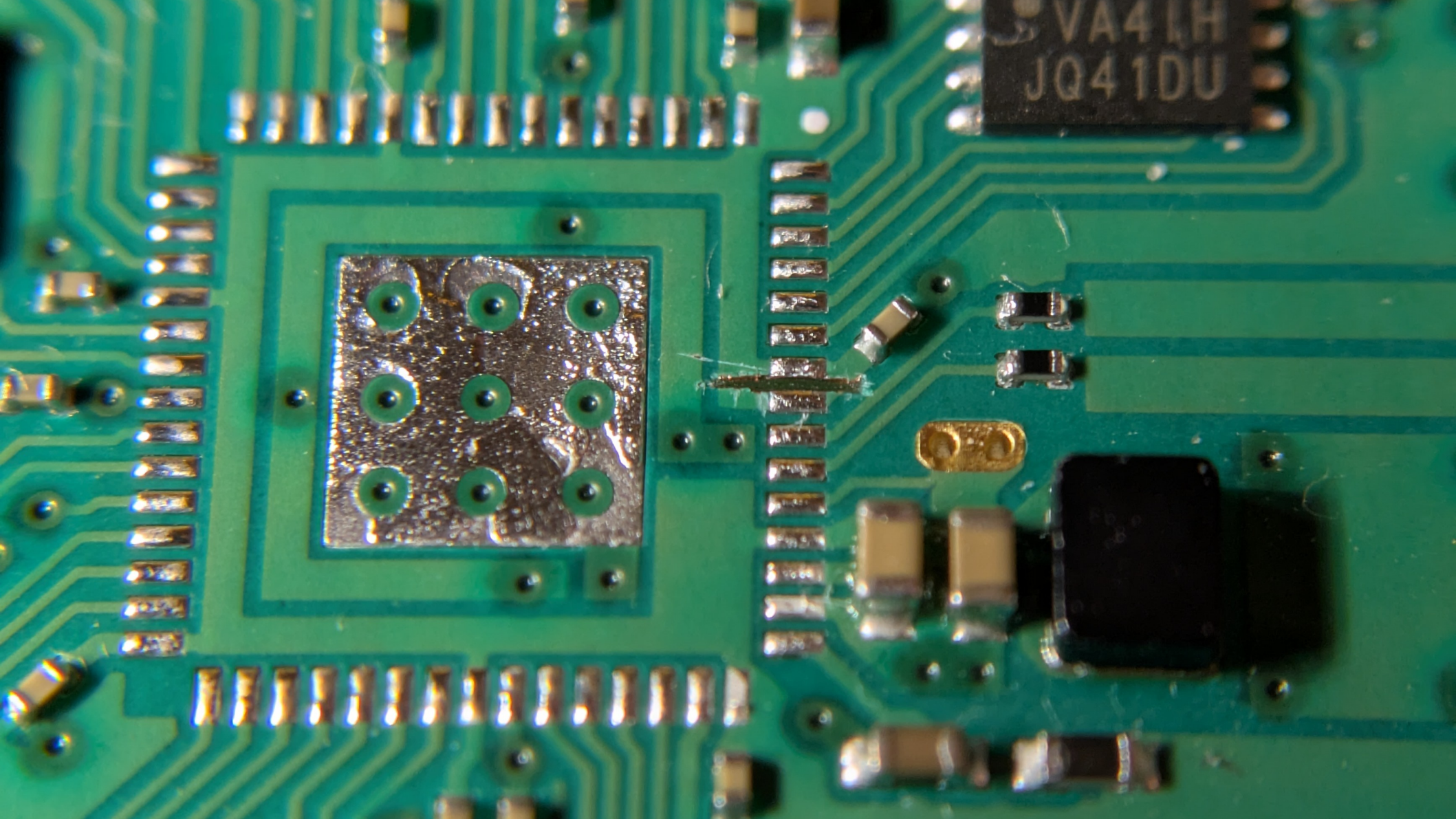
Optical microscope image

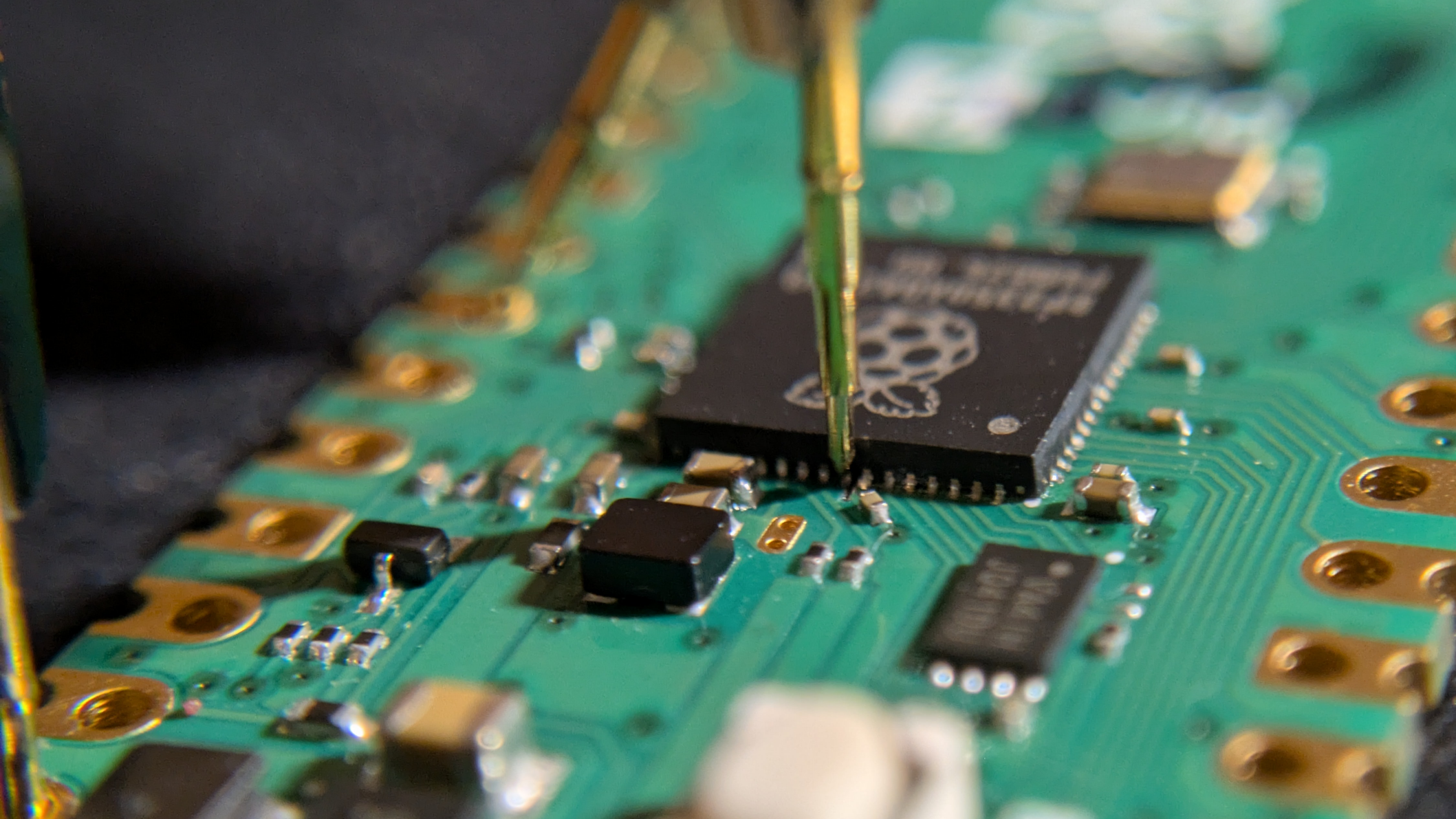

X-ray + optical microscope composite
59
QSPI_SD1
58
QSPI_SD2
57
QSPI_SD0
56
QSPI_SCLK
55
QSPI_SD3
54
QSPI_IOVDD
53
USB_OTP_VDD
52
USB_DP
51
USB_DM
50
VREG_FB
49
VREG_VIN
48
VREG_LX
47
VREG_PGND

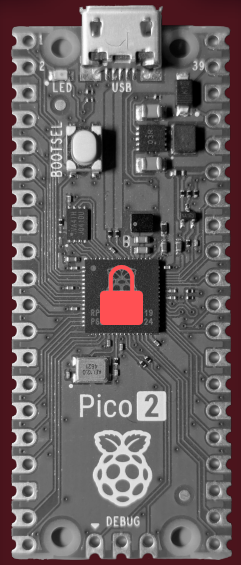




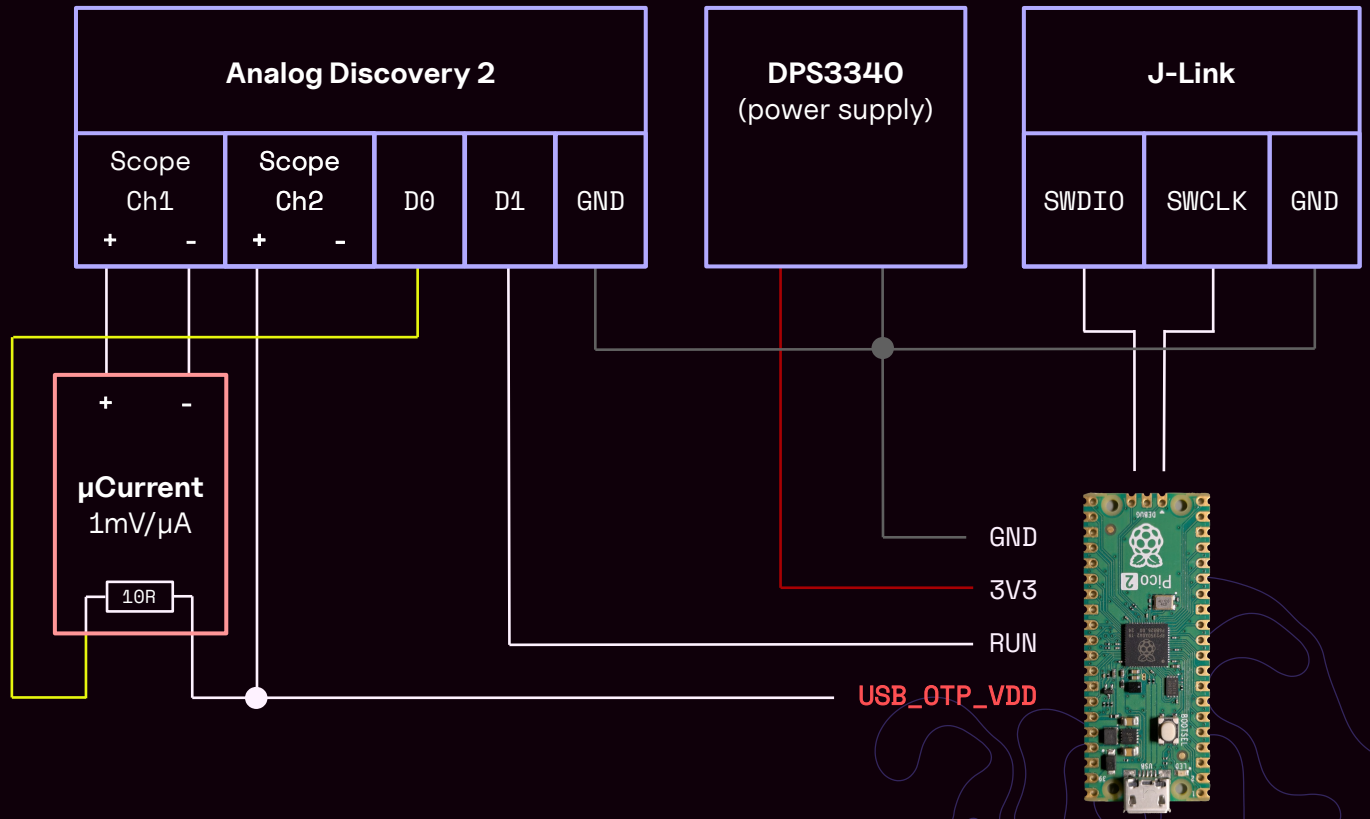


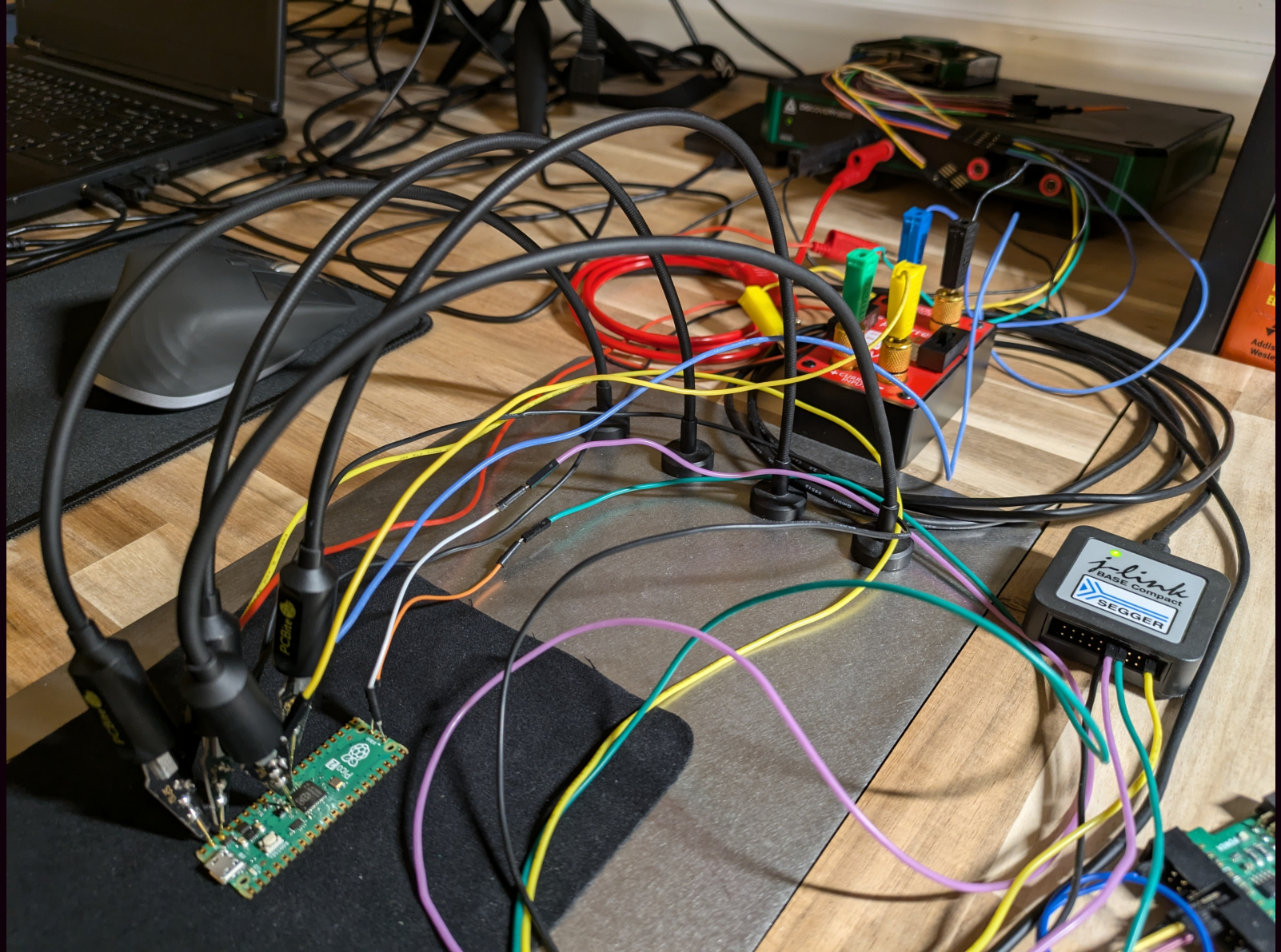

VA41H
JQ41DU

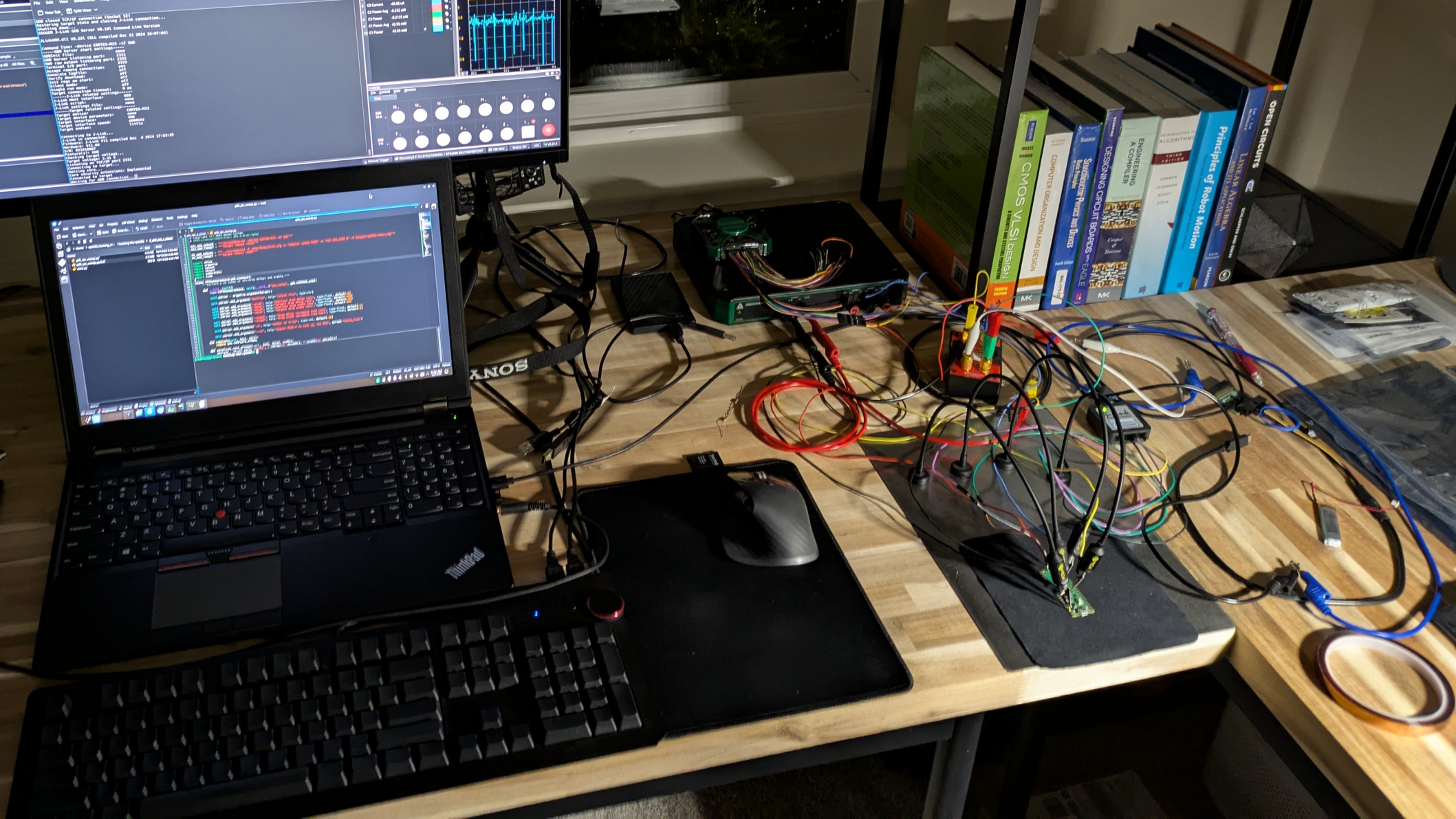


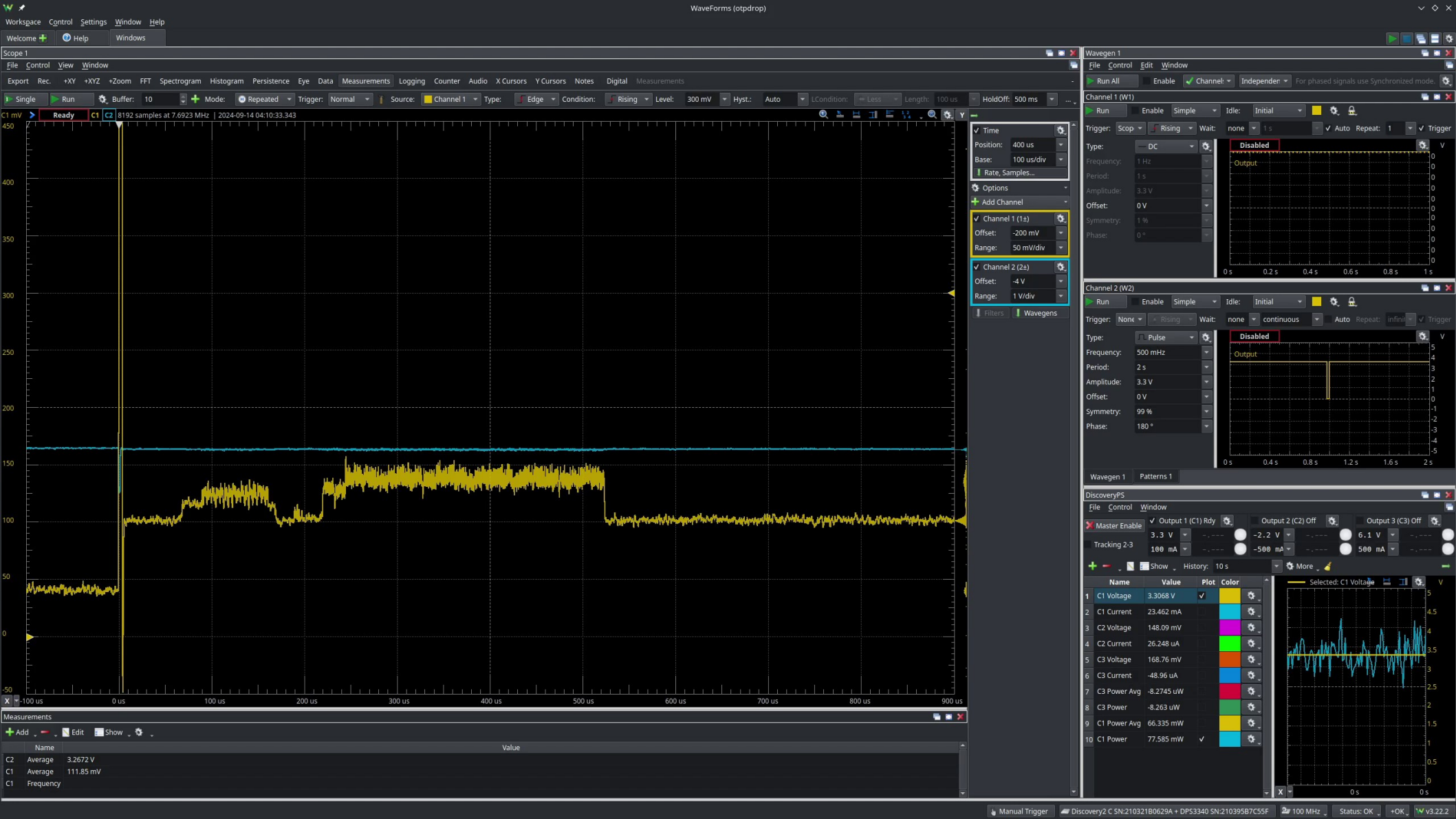


lock_chip.sh


Analog Discovery 2
Scope Ch1
+ -
Scope Ch2
+ -
D0
D1
GND
DPS3340
(power supply)
J-Link
SWDIO
SWCLK
GND
+ -
µCurrent
1mV/µA
10R
GND
3V3
RUN
USB_OTP_VDD

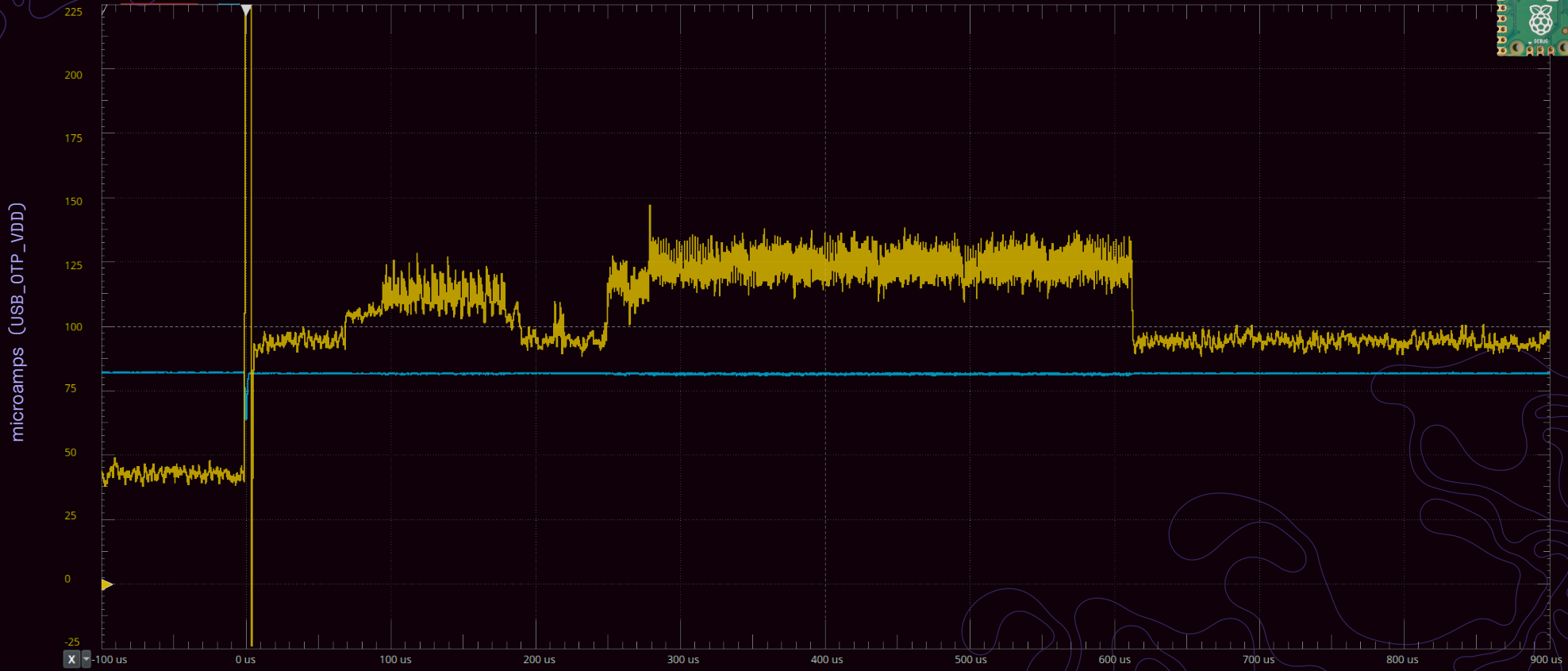

J-link
BASE Compact
SEGGER


CMOS VLSI DESIGN
COMPUTER ORGANIZATION AND DESIGN
DESIGNING CIRCUIT BOARDS WITH EAGLE
ENGINEERING A COMPILER
Principles of Robot Motion
LINEAR ALGEBRA
OPEN CIRCUITS
ThinkPad


WaveForms (otpdrop)
Workspace Control Settings Window Help
Welcome Help Windows
Scope 1
File Control View Window
Export Rec. +XY +XYZ +Zoom FFT Spectrogram Histogram Persistence Eye Data Measurements Logging Counter Audio X Cursors Y Cursors Notes Digital Measurements
Single Run Buffer: 10 Mode: Repeated Trigger: Normal Source: Channel 1 Type: Edge Condition: Rising Level: 300 mV Hyst.: Auto LCondition: Less Length: 100 us HoldOff: 500 ms
C1 mV Ready C1 C2 8192 samples at 7.6923 MHz | 2024-09-14 04:10:33.343
Time Position: 400 us Base: 100 us/div Rate, Samples...
Options
Add Channel
Channel 1 (1±) Offset: -200 mV Range: 50 mV/div
Channel 2 (2±) Offset: -4 V Range: 1 V/div
Filters Wavegens
Measurements
Add Edit Show
Name Value
C2 Average 3.2672 V
C1 Average 111.85 mV
C1 Frequency
Wavegen 1
File Control Edit Window
Run All Enable Channel Independent For phased signals use Synchronized mode.
Channel 1 (W1)
Run Enable Simple Idle: Initial
Trigger: Scop Rising Wait: none 1 s Auto Repeat: 1 Trigger
Type: DC
Frequency: 1 Hz
Period: 1 s
Amplitude: 3.3 V
Offset: 0 V
Symmetry: 1 %
Phase: 0 °
Disabled
Output
Channel 2 (W2)
Run Enable Simple Idle: Initial
Trigger: None Rising Wait: none continuous Auto Repeat: Infini Trigger
Type: Pulse
Frequency: 500 mHz
Period: 2 s
Amplitude: 3.3 V
Offset: 0 V
Symmetry: 99 %
Phase: 180 °
Disabled
Output
Wavegen 1 Patterns 1
DiscoveryPS
File Control Window
Master Enable
Output 1 (C1) Rdy
Output 2 (C2) Off
Output 3 (C3) Off
Tracking 2-3
3.3 V 100 mA
-2.2 V -500 mA
6.1 V 500 mA
Show History: 10 s More
Name Value Plot Color
1 C1 Voltage 3.3068 V
2 C1 Current 23.462 mA
3 C2 Voltage 148.09 mV
4 C2 Current 26.248 uA
5 C3 Voltage 168.76 mV
6 C3 Current -48.96 uA
7 C3 Power Avg -8.2745 uW
8 C3 Power -8.263 uW
9 C1 Power Avg 66.335 mW
10 C1 Power 77.585 mW
Selected: C1 Voltage
Manual Trigger
Discovery2 C SN:210321B0629A + DPS3340 SN:210395B7C55F
100 MHz
Status: OK
+OK
v3.22.2

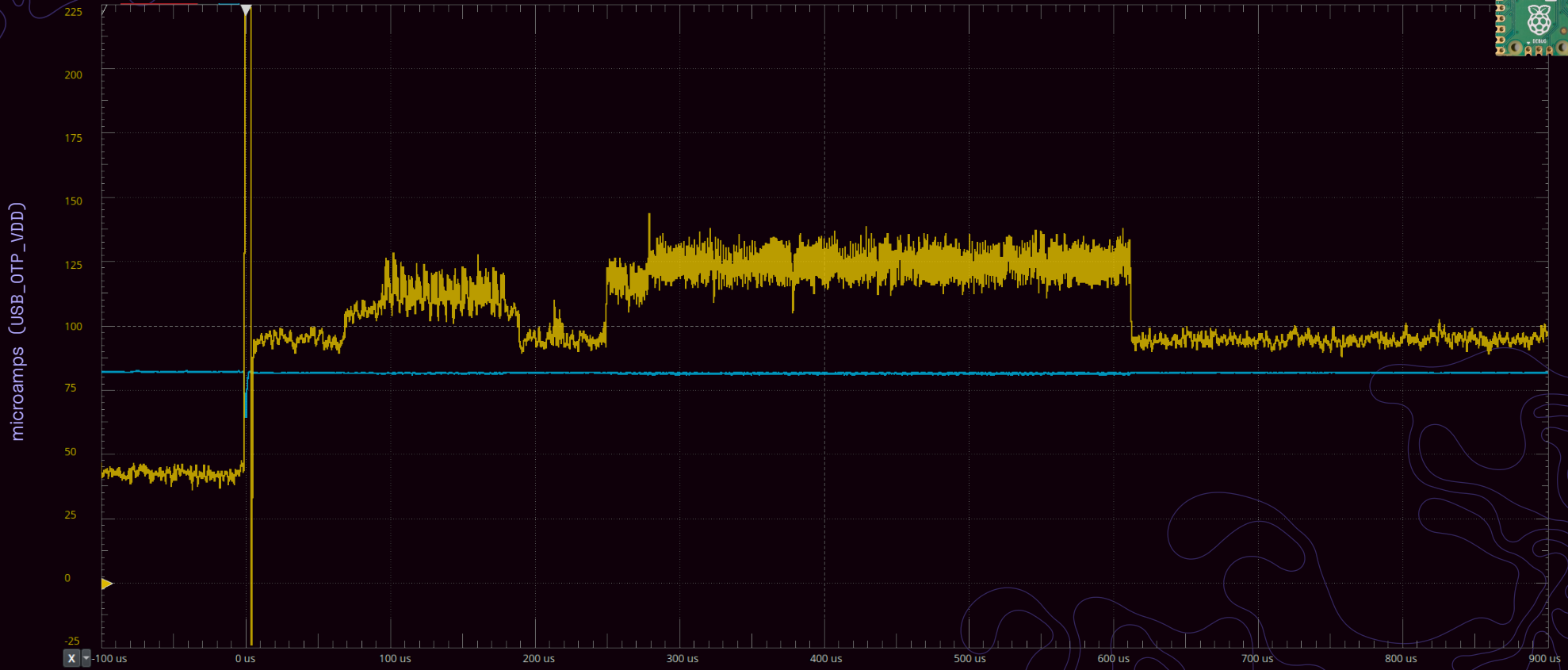
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



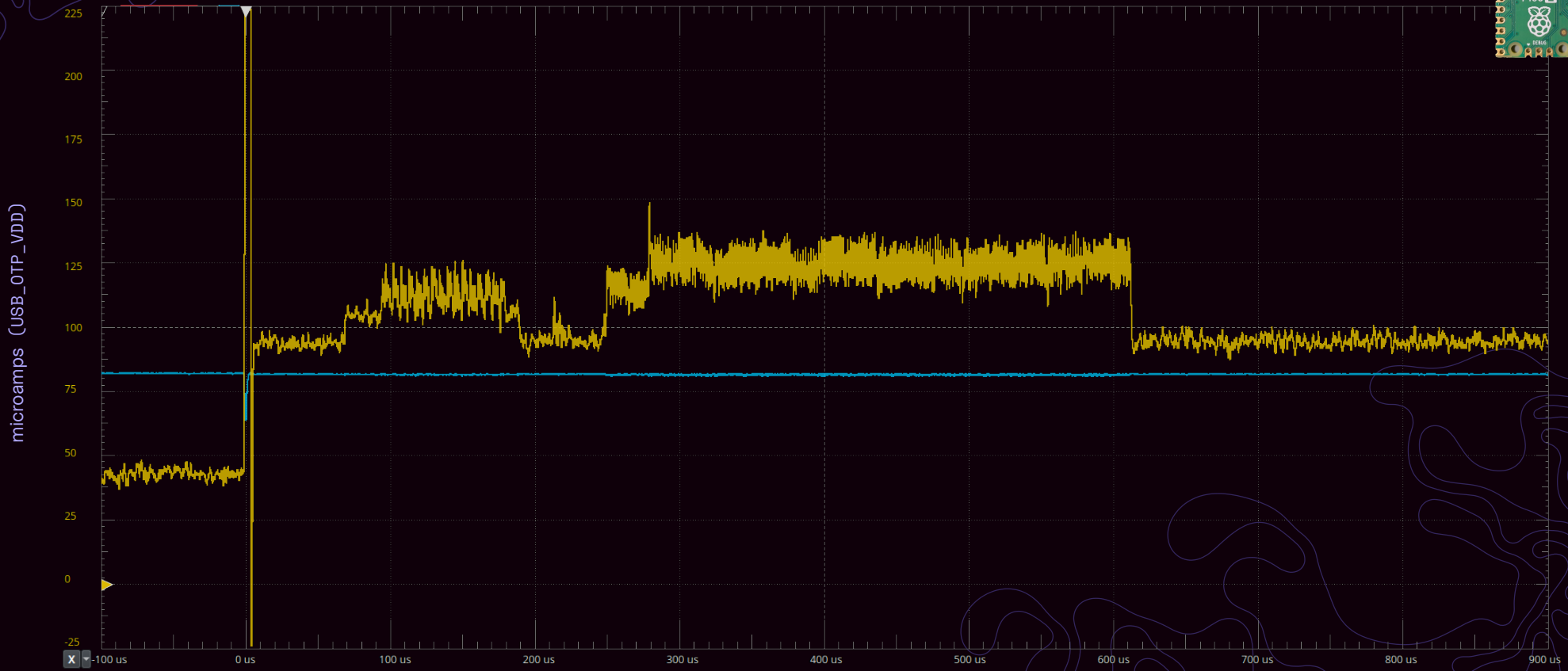
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



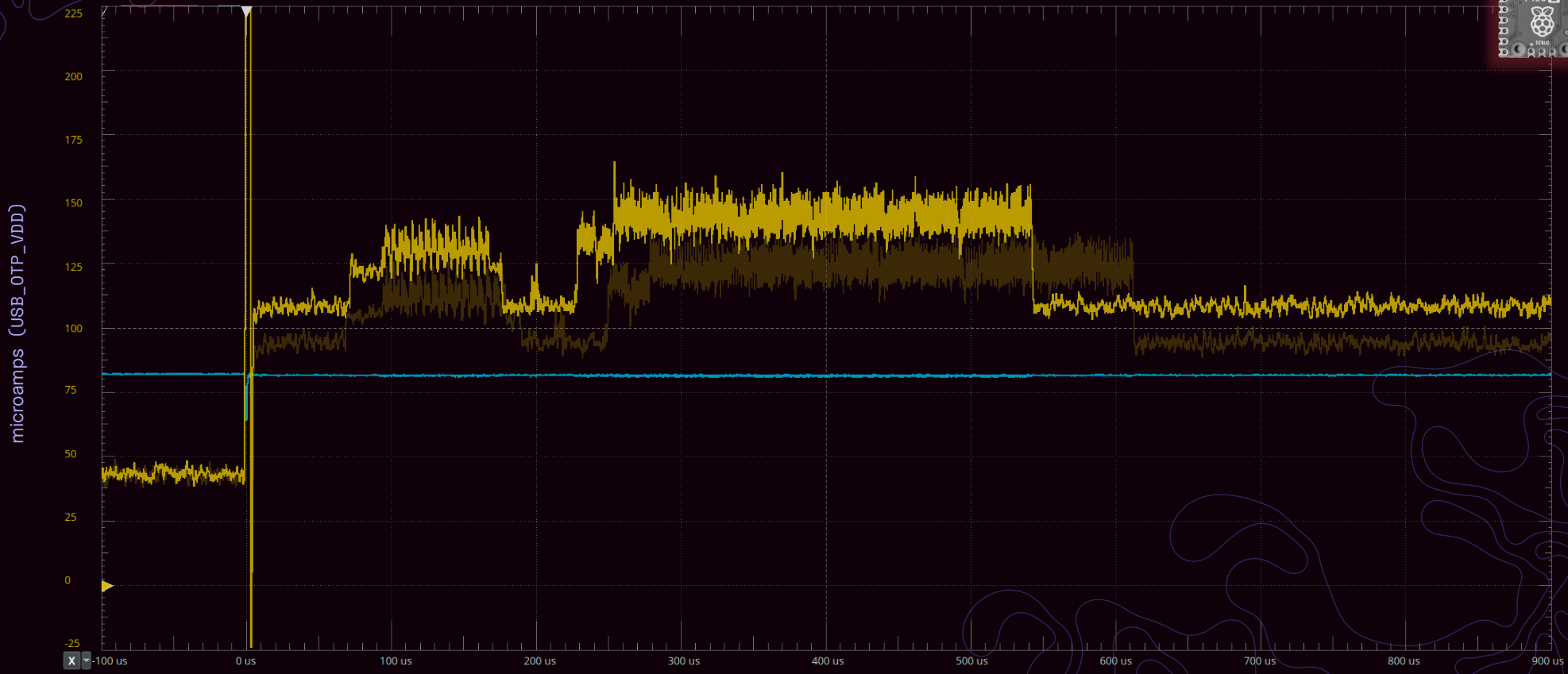
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



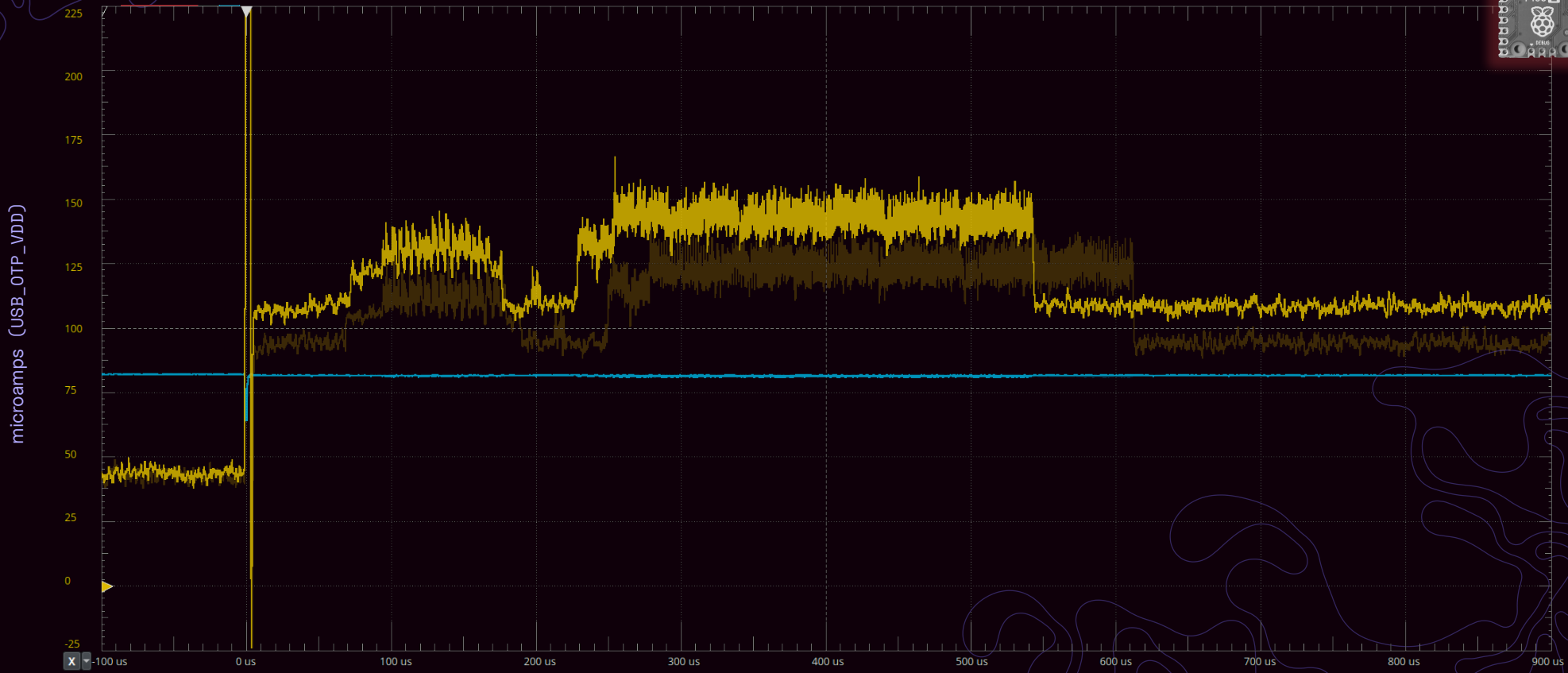
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



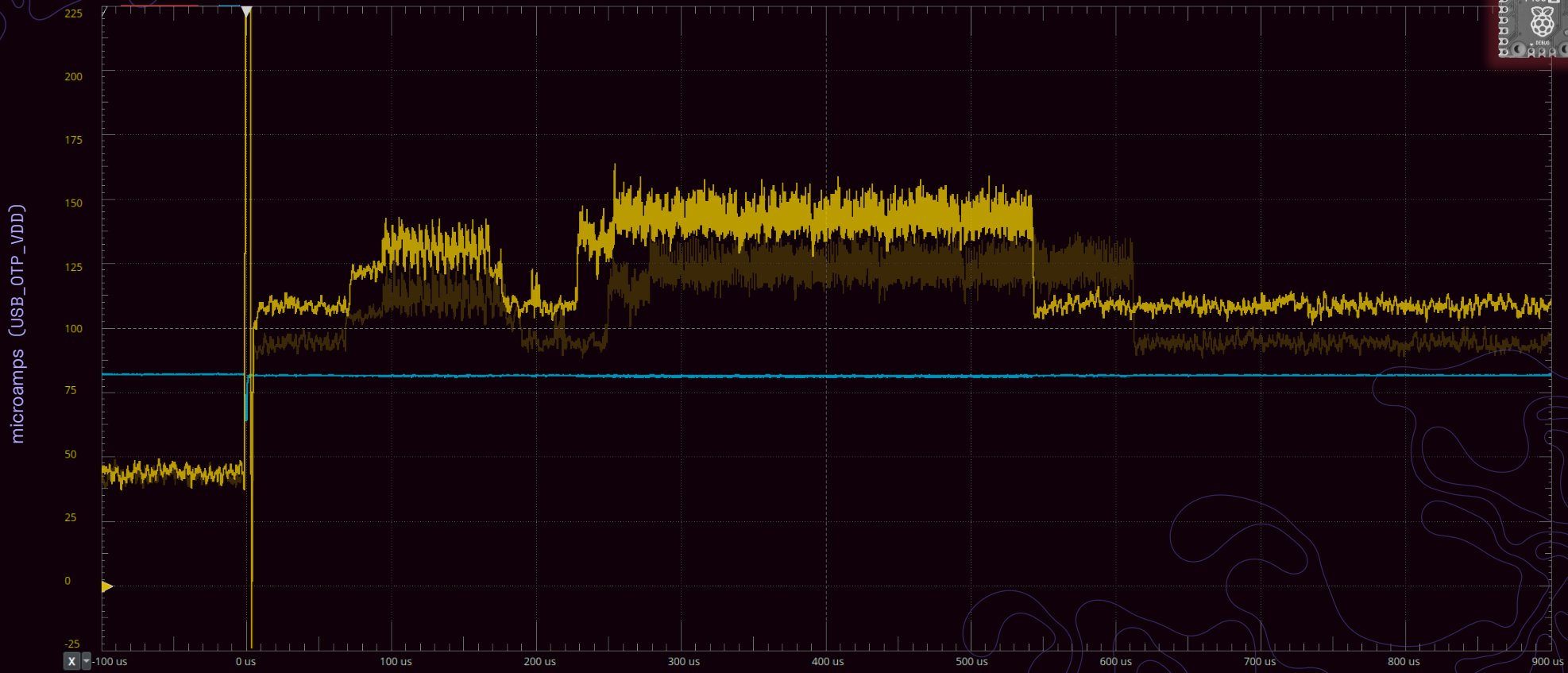
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



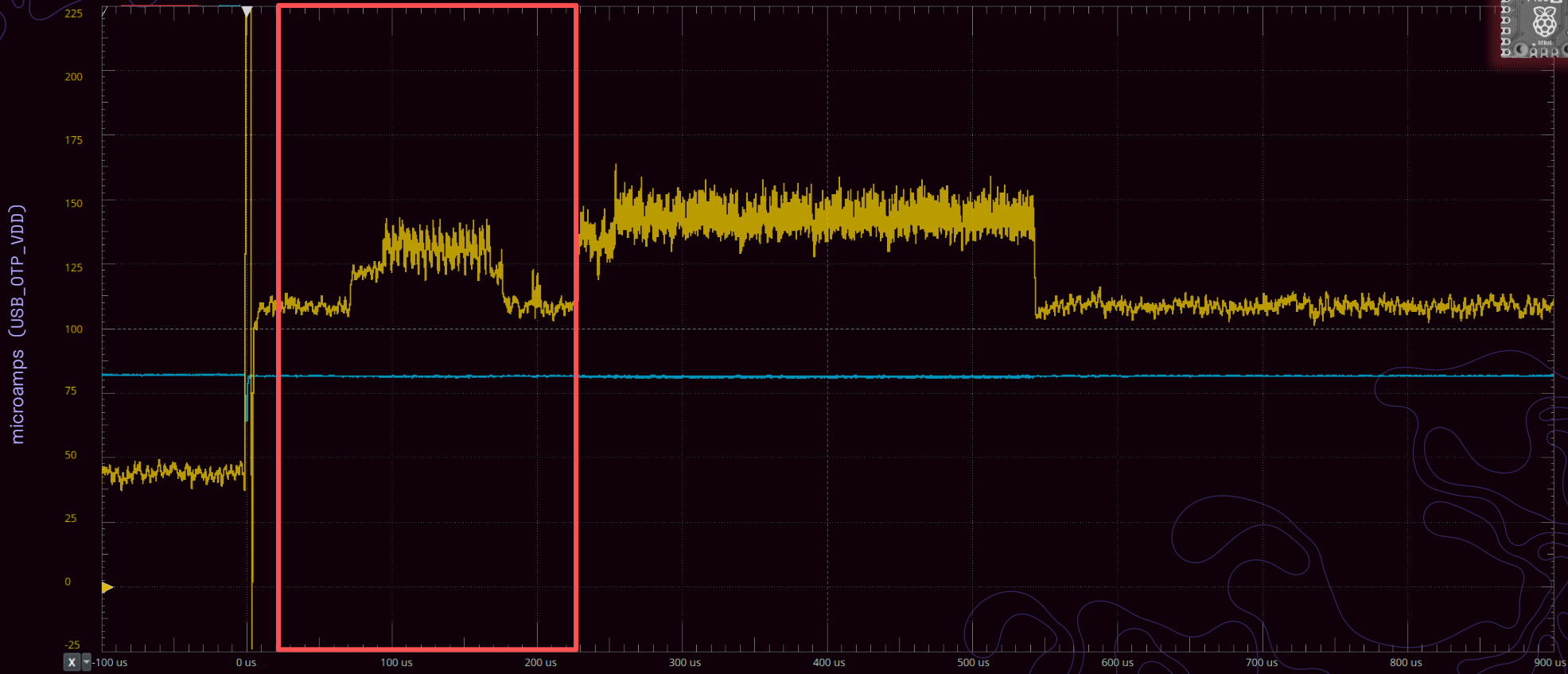
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



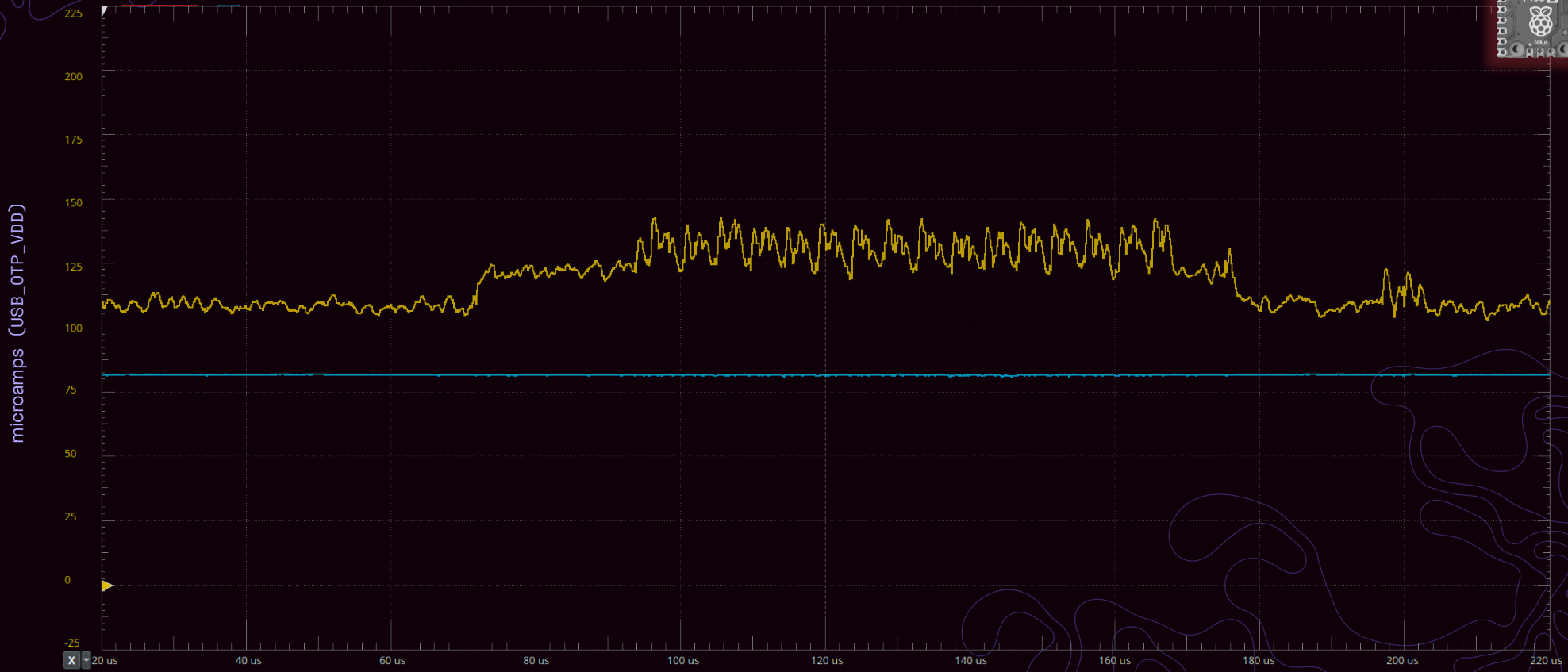
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



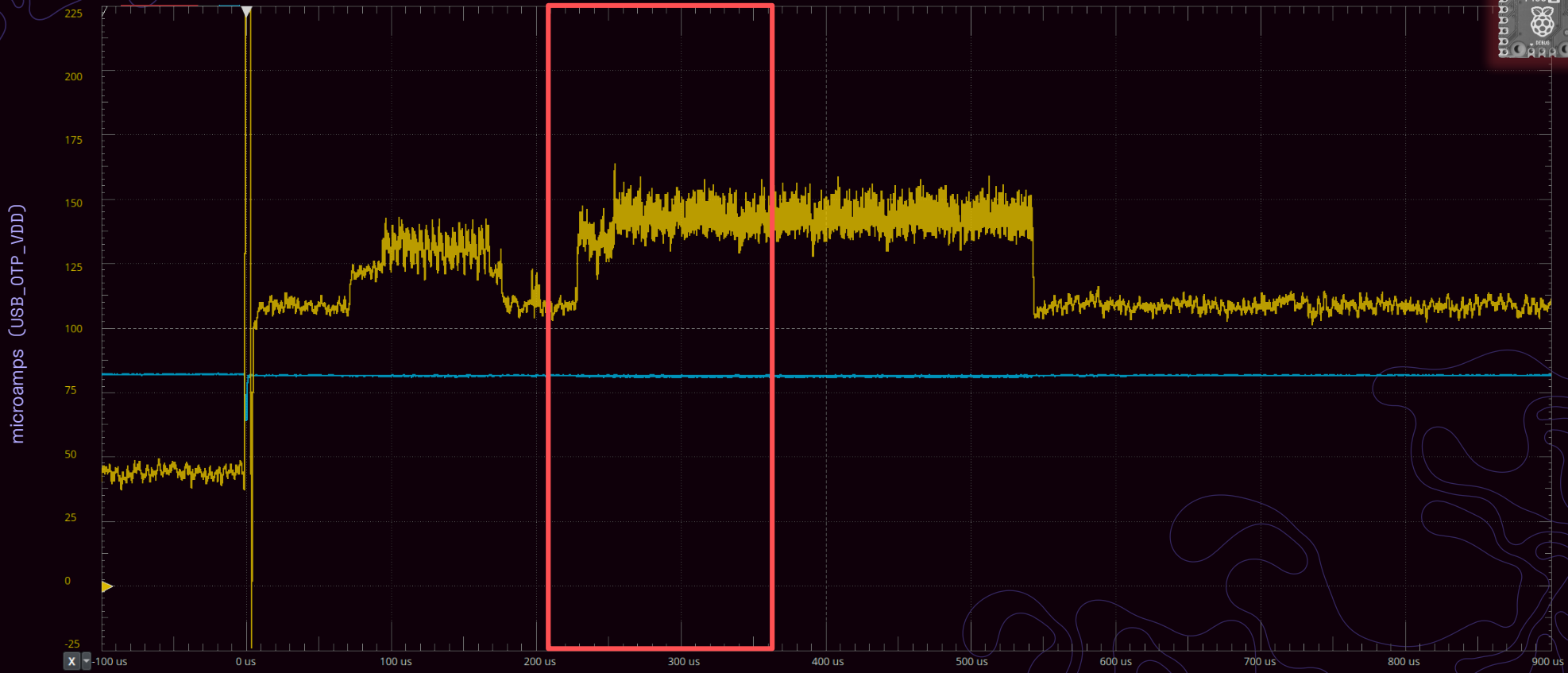
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



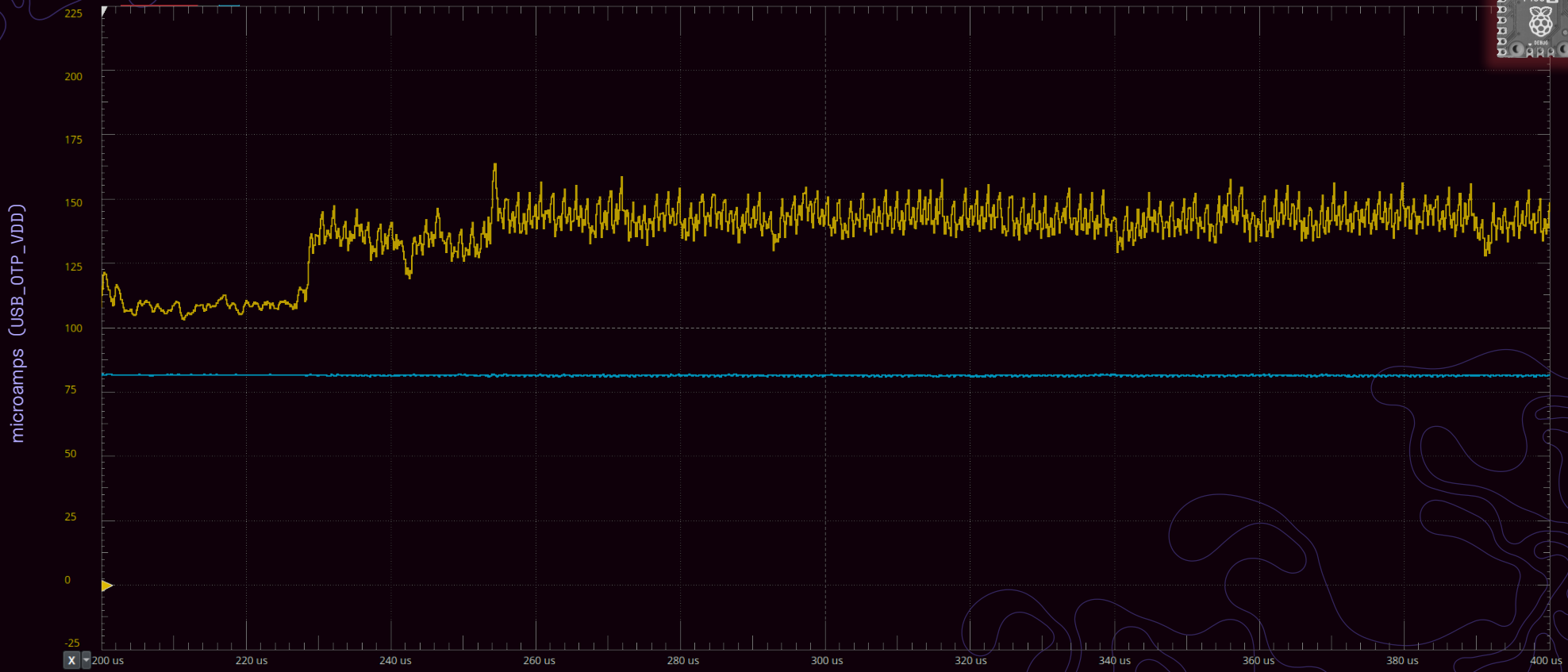
3. Interruptible power supply

Experimenting with the IPS and OTP PSM



3. Interruptible power supply

Experimenting with the IPS and OTP PSM



3. Interruptible power supply

Experimenting with the IPS and OTP PSM

3. Interruptible power supply

Experimenting with the IPS and OTP PSM

3. Interruptible power supply

Experimenting with the IPS and OTP PSM

3. Interruptible power supply

Experimenting with the IPS and OTP PSM

3. Interruptible power supply

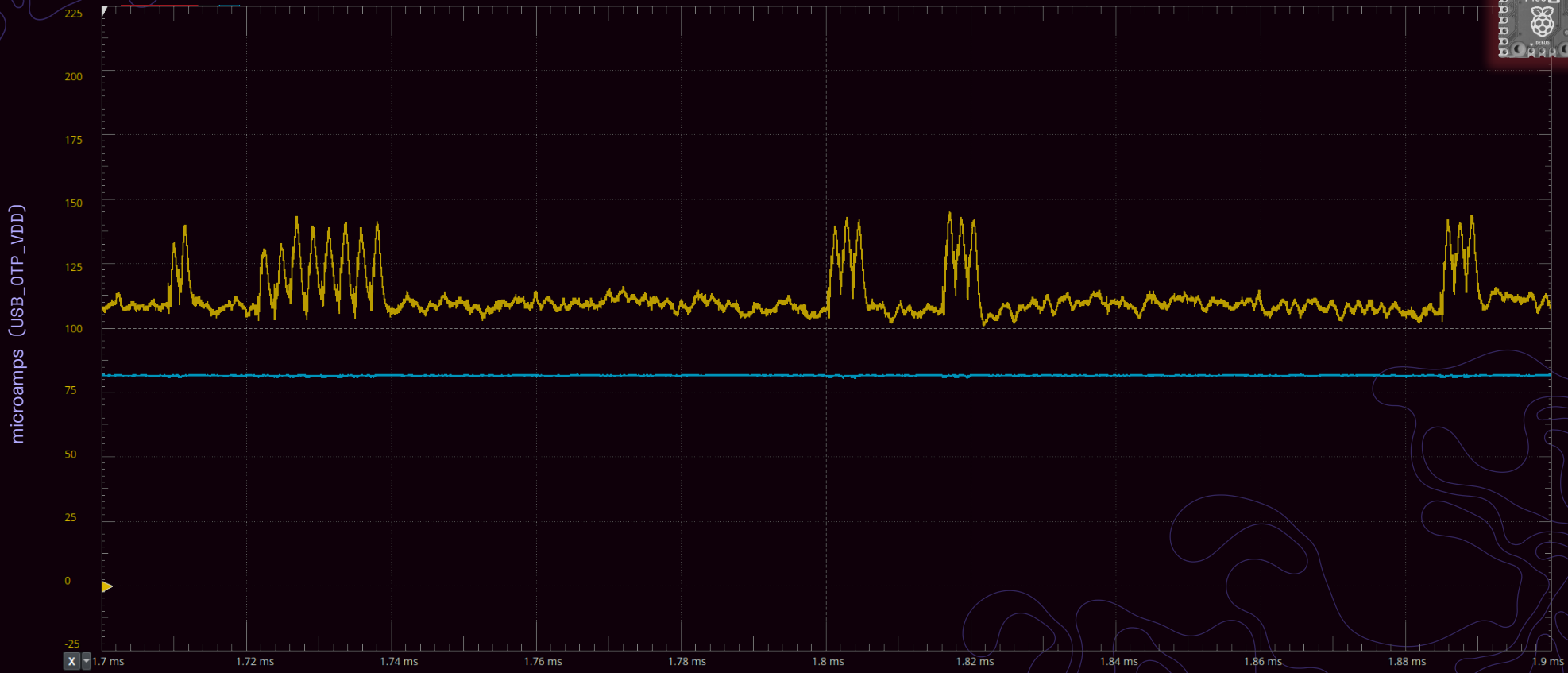
Experimenting with the IPS and OTP PSM

3. Interruptible power supply

Experimenting with the IPS and OTP PSM

3. Interruptible power supply

Experimenting with the IPS and OTP PSM

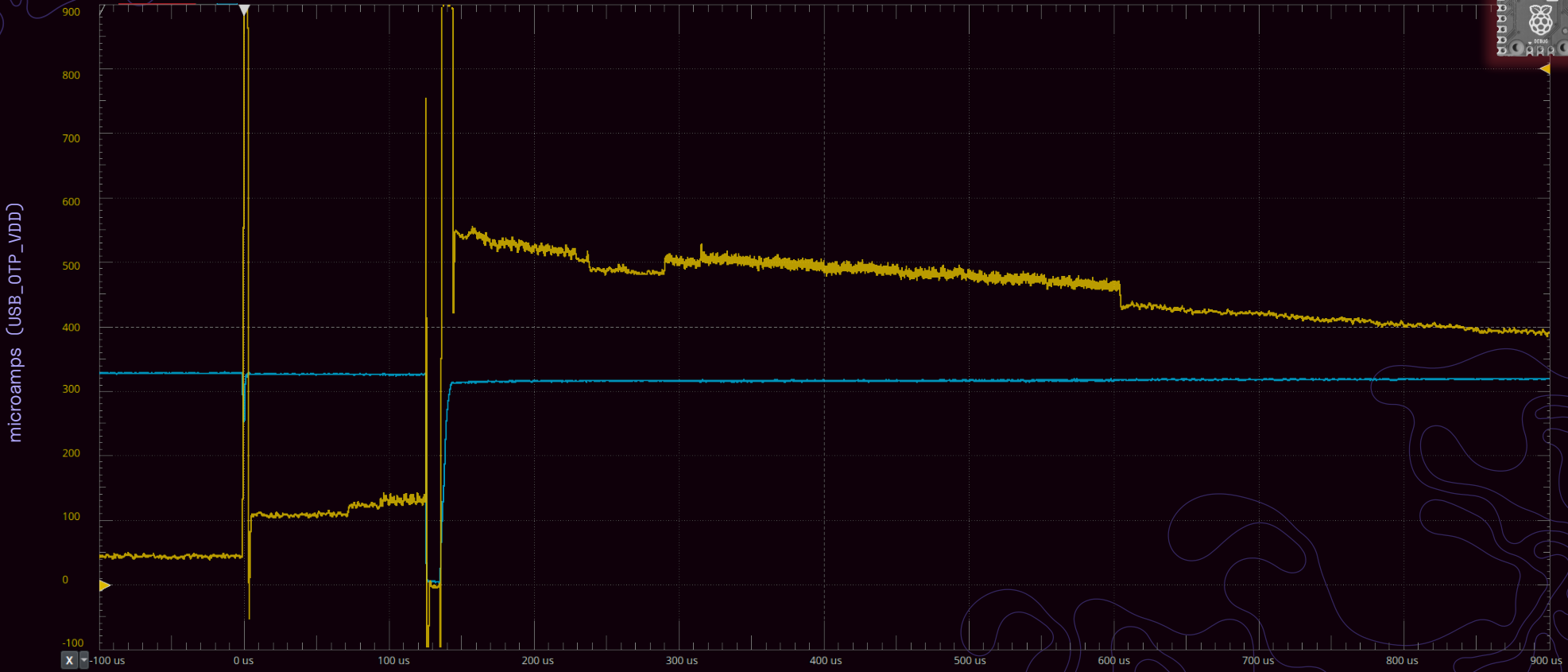


3. Interruptible power supply

Experimenting with the IPS and OTP PSM

10 µs pulse after 125 µs

OTP controller boot restarts immediately

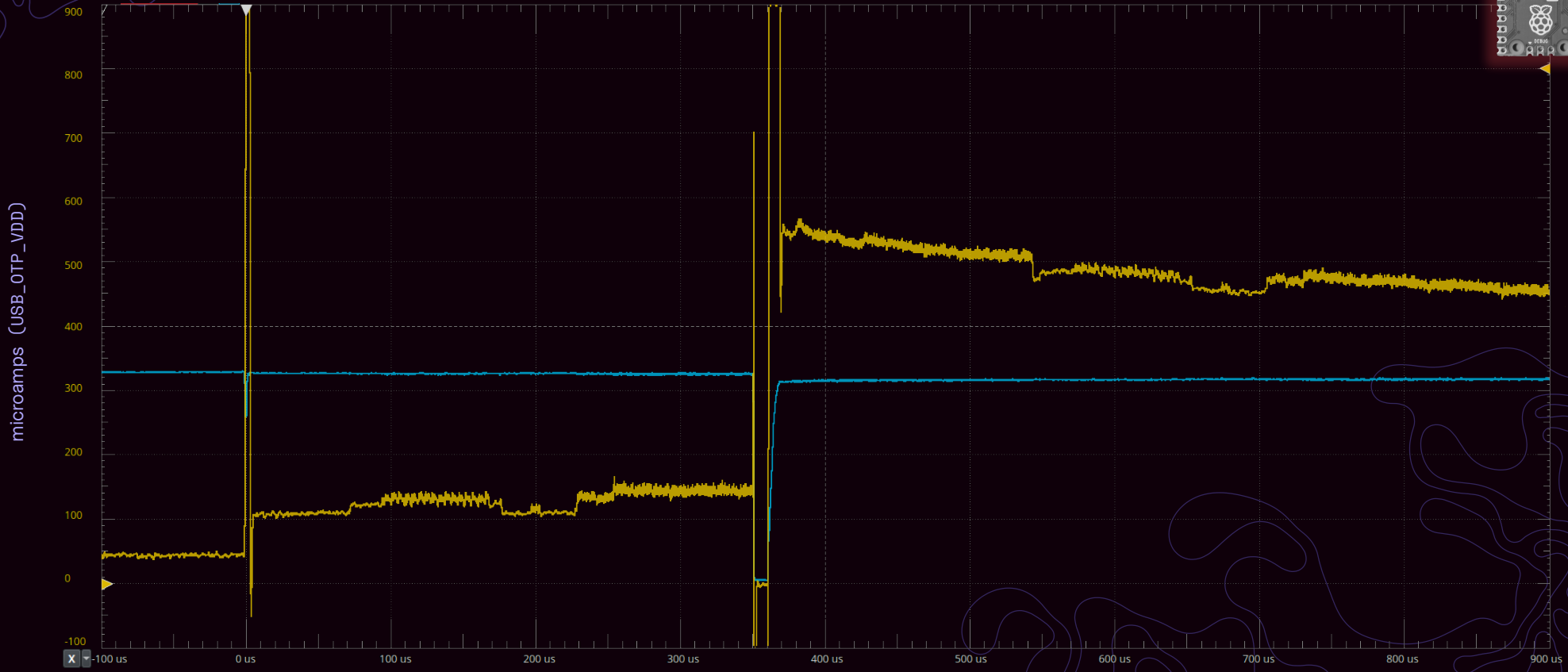


3. Interruptible power supply

Experimenting with the IPS and OTP PSM

10 µs pulse after 350 µs

OTP PSM finishes, then restarts itself from beginning

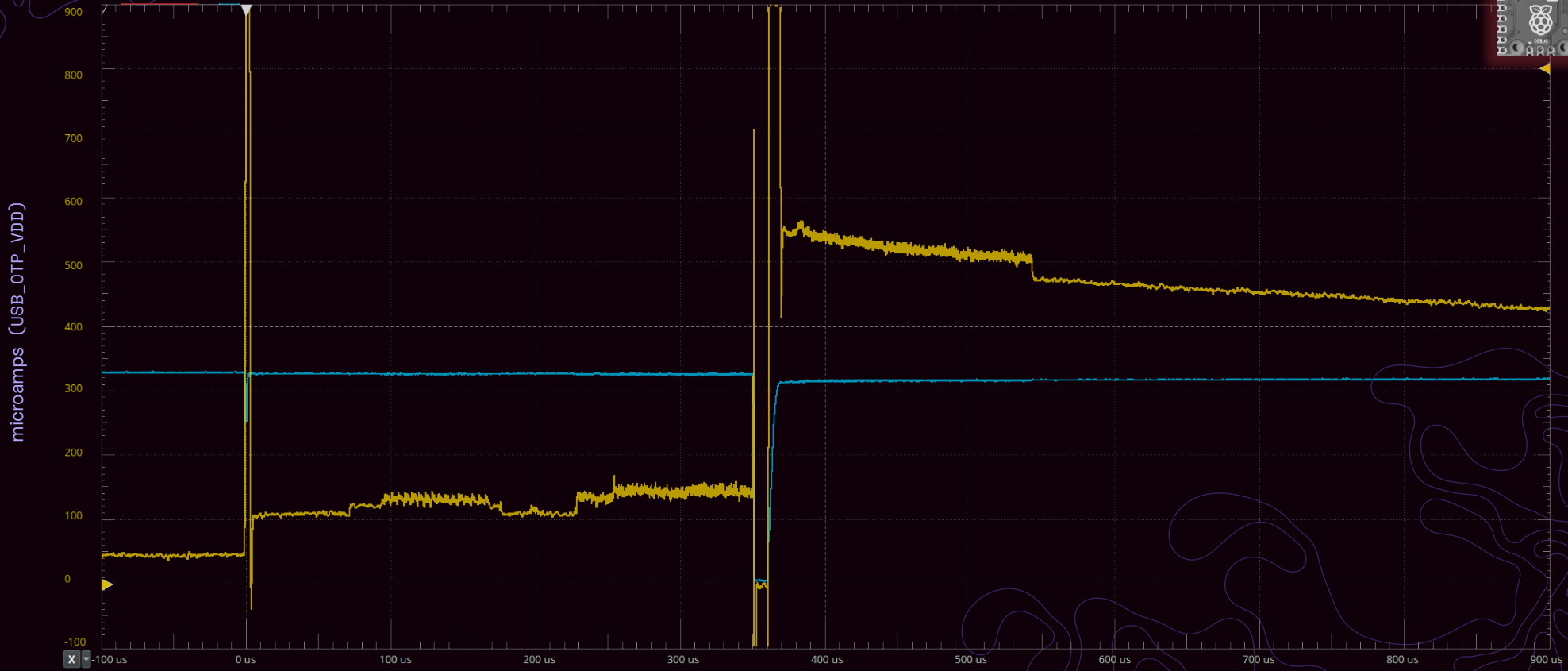


3. Interruptible power supply

Experimenting with the IPS and OTP PSM

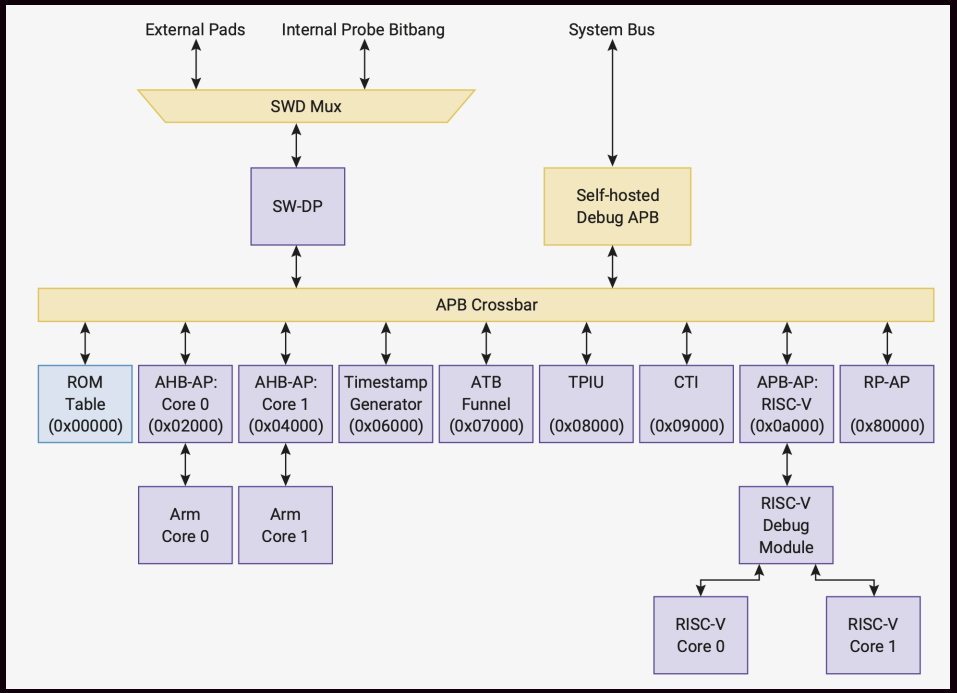
10 µs pulse after 350 µs

Sometimes, OTP PSM finishes and is happy (?)



3. Interruptible power supply

Experimenting with the IPS and OTP PSM



Debug is still locked down :(

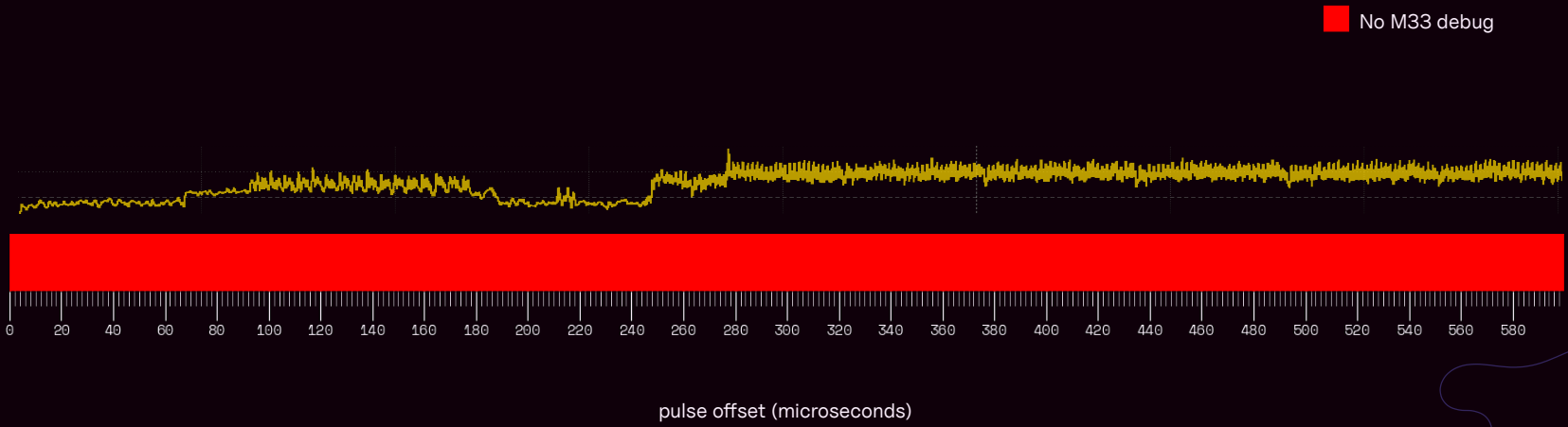
```
$ JLinkExe -device CORTEX-M33 -if SWD -speed 4000
...
...
Connecting to target via SWD
Found SW-DP with ID 0x4C013477
DPIDR: 0x4C013477
CoreSight SoC-600 or later (DPv3 detected)
Detecting available APs
APSpace base (BASEPTR0): 0x00000000
APSpace size (DPIDR1.ASIZE): 20-bit (1024 KB)
Top-level ROM table, that describes AP map, found
Scanning top-level ROM table and nested ones to find APs
AP[0] (APAddr 0x00002000): AHB-AP (IDR: 0x34770008)
AP[1] (APAddr 0x00004000): AHB-AP (IDR: 0x34770008)
Iterating through AP map to find AHB-AP to use
AP[0]: Skipped. Could not read CPUID register
AP[1]: Skipped. Could not read CPUID register
Attach to CPU failed. Executing connect under reset.
```

4. Siri, set a timer for 5 µs

Visualizing 60,000 IPS power faults

No obvious progress on debug-disabled M33

5 µs pulse, 10 tries every 100ns offset

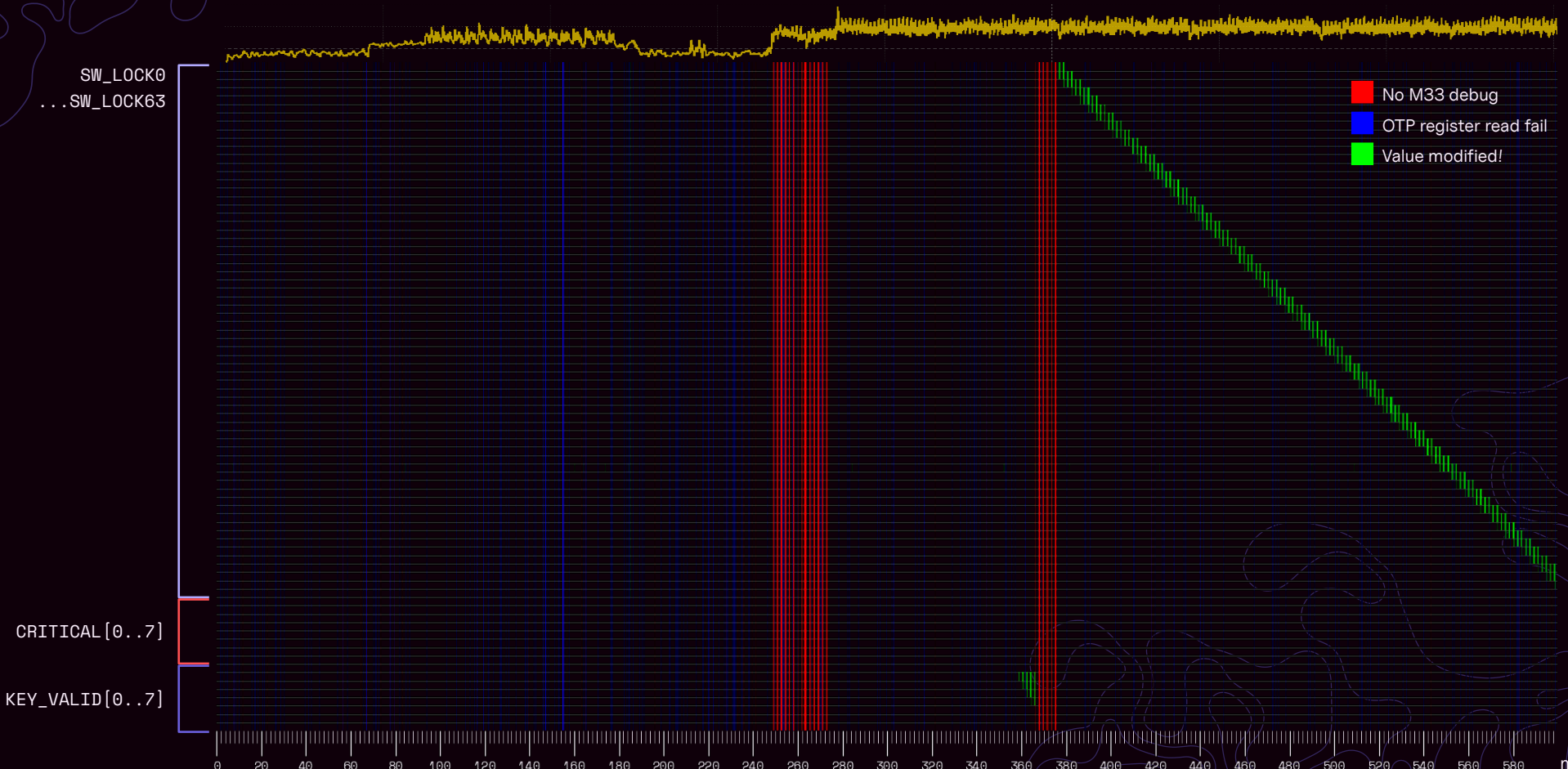


4. Siri, set a timer for 5 µs

Visualizing 60,000 IPS power faults

Learning more on a debuggable chip

5 µs pulse, 10 tries every 100ns offset



4. Siri, set a timer for 5 µs

Visualizing 60,000 IPS power faults

Learning more on a debuggable chip

5 µs pulse, 10 tries every 100ns offset

SW_LOCK0
...SW_LOCK63

CRITICAL[0..7]

KEY_VALID[0..7]

No M33 debug
OTP register read fail
Value modified!

0 20 40 60 80 100 120 140 160 180 200 220 240 260 280 300 320 340 360 380 400 420 440 460 480 500 520 540 560 580

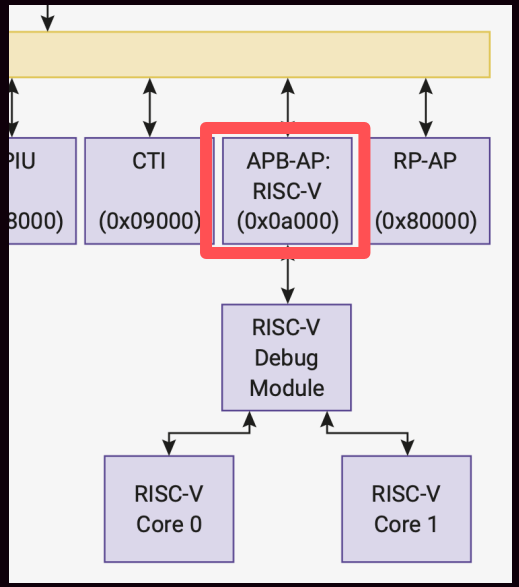
microseconds

Why is it failing there?

50 µs pulse at ~250 µs

```
$ JLinkExe -device CORTEX-M33 -if SWD -speed 4000
...
...
Connecting to target via SWD
Found SW-DP with ID 0x4C013477
DPIDR: 0x4C013477
CoreSight SoC-600 or later (DPv3 detected)
Detecting available APs
APSpace base (BASEPTR0): 0x00000000
APSpace size (DPIDR1.ASIZE): 20-bit (1024 KB)
Top-level ROM table, that describes AP map, found
Scanning top-level ROM table and nested ones to find APs
AP[0] (APAddr 0x0000A000): APB-AP (IDR: 0x24770006)
Iterating through AP map to find AHB-AP to use
AP[0]: Skipped. Not an AHB-AP
Attach to CPU failed. Executing connect under reset.
```

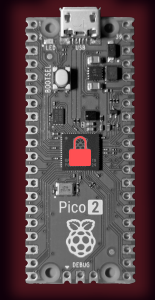

```
AP[0] (APAddr 0x0000A000): APB-AP (IDR: 0x24770006)
```

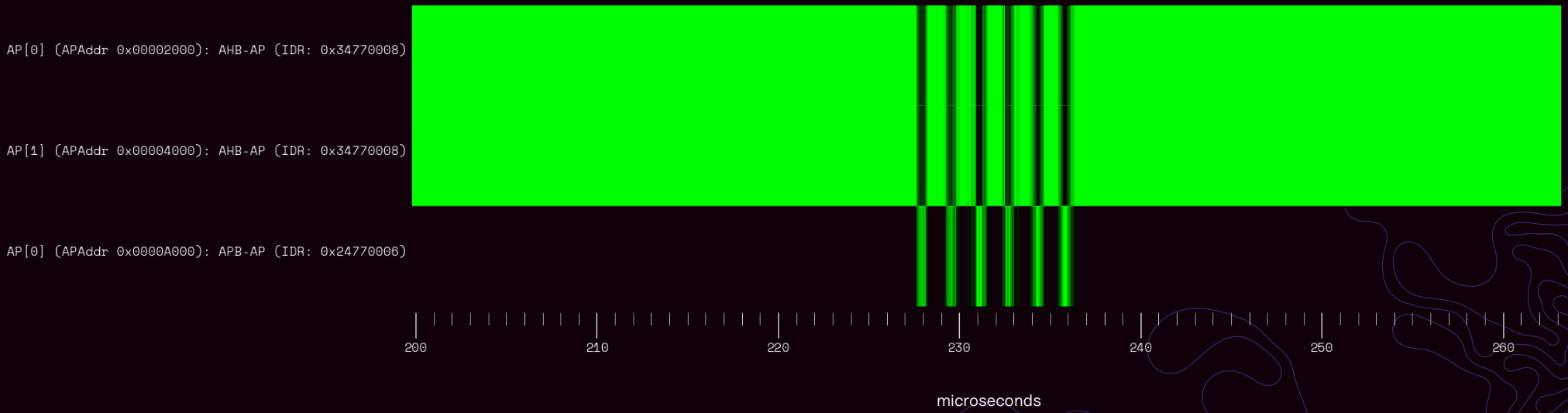


That’s the RISC-V debug access port...

The RISC-V APB-AP also appears when secured!

5 µs pulse, 10 tries every 100ns offset





5. I don’t drink coffee

Reading secrets and more with the RISC-V cores


```
$ openocd -f jlink.cfg -c "adapter speed 5000" -c "set USE_CORE 0" -f rp2350-riscv.cfg
Open On-Chip Debugger 0.12.0+dev-gebec9504d (2024-09-14-03:22)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.org/doc/doxygen/bugs.html
adapter speed: 5000 kHz
0
Info : Listening on port 6666 for tcl connections
Info : Listening on port 4444 for telnet connections
Info : J-Link V11 compiled Dec  4 2024 17:53:35
Info : Hardware version: 11.00
Info : VTarget = 3.315 V
Info : clock speed 5000 kHz
Info : SWD DPIDR 0x4c013477
Info : [rp2350.dap.core0] datacount=1 progbufsize=2
Info : [rp2350.dap.core0] Disabling abstract command reads from CSRs.
Info : [rp2350.dap.core0] Disabling abstract command writes to CSRs.
Info : [rp2350.dap.core0] Examined RISC-V core
Info : [rp2350.dap.core0]  XLEN=32, misa=0x40901105
Info : [rp2350.dap.core0] Examination succeed
Info : starting gdb server for rp2350.dap.core0 on 3333
Info : Listening on port 3333 for gdb connections
```

5. I don’t drink coffee

Reading secrets and more with the RISC-V cores


```
(gdb) target remote :3333
Remote debugging using :3333
warning: No executable has been specified and target does not support
determining executable automatically.  Try using the "file" command.
0x00007640 in ?? ()
(gdb) x/32wx 0x40137020
0x40137020:     0x0022c0ff      0x0014ffee      0x0022c0ff      0x0014ffee
0x40137030:     0x0022c0ff      0x0014ffee      0x0022c0ff      0x0014ffee
0x40137040:     0x00000000      0x00000000      0x00000000      0x00000000
0x40137050:     0x00000000      0x00000000      0x00000000      0x00000000
0x40137060:     0x00000000      0x00000000      0x00000000      0x00000000
0x40137070:     0x00000000      0x00000000      0x00000000      0x00000000
0x40137080:     0x00000000      0x00000000      0x00000000      0x00000000
0x40137090:     0x00000000      0x00000000      0x00000000      0x00000000
(gdb) x/1wx 0x40120148
0x40120148:     0x00030033
(gdb)
```

5. I don’t drink coffee

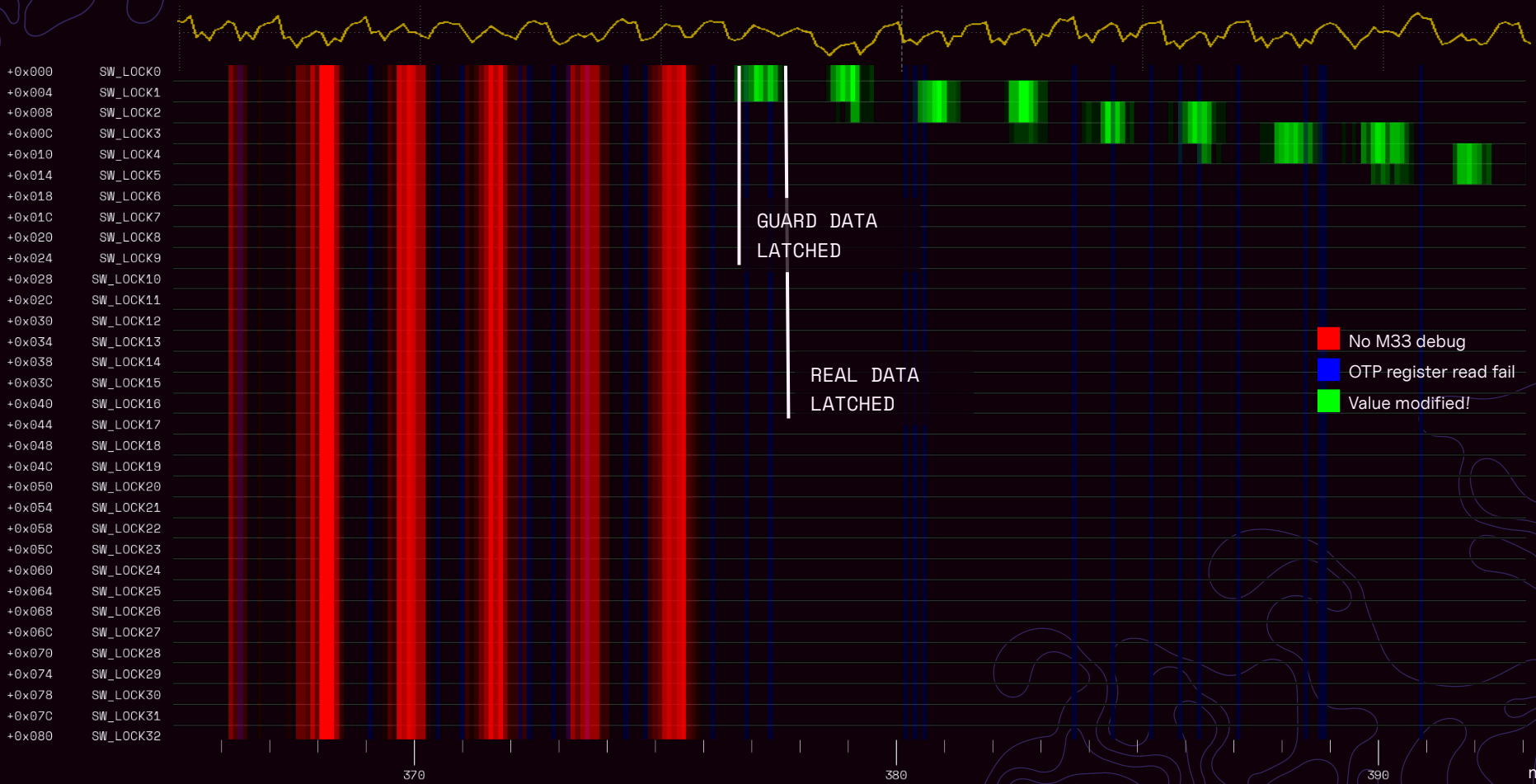
Reading secrets and more with the RISC-V cores

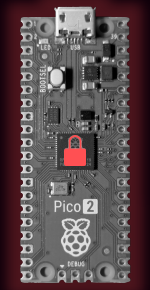
0x00030033

OTP: **CRITICAL** (0x40120148)

31:18	Reserved	
17	**RISCV_DISABLE**	■ Selects RISC-V
16	**ARM_DISABLE**	■ Selects RISC-V
15:7	Reserved	
6:5	**GLITCH_DETECTOR_SENS**	□■
4	**GLITCH_DETECTOR_ENABLE**	■
3	**DEFAULT_ARCHSEL**	□
2	**DEBUG_DISABLE**	□ — Allows RISC-V full-privilege debug
1	**SECURE_DEBUG_DISABLE**	■ — Don’t care
0	**SECURE_BOOT_ENABLE**	■ — Don’t care

The guard word is 0x333333, and RPi is unaware the SHF has persistence





Can we escalate from RISC-V to M33 secure-mode debug?

Easy!

```
(gdb) set *0x40120150 = 0x0000010f      (Set all DEBUGEN bits)
(gdb) set *0x40018008 = 0x00000002      (Set system PSM WDSEL to OTP)
(gdb) set *0x400d8000 = 0x80000000      (Trigger watchdog reset)
```


```
$ JLinkExe -device CORTEX-M33 -if SWD -speed 4000
...
...
Connecting to target via SWD
Found SW-DP with ID 0x4C013477
DPIDR: 0x4C013477
CoreSight SoC-600 or later (DPv3 detected)
Detecting available APs
APSpace base (BASEPTR0): 0x00000000
APSpace size (DPIDR1.ASIZE): 20-bit (1024 KB)
Top-level ROM table, that describes AP map, found
Scanning top-level ROM table and nested ones to find APs
AP[0] (APAddr 0x00002000): AHB-AP (IDR: 0x34770008)
AP[1] (APAddr 0x00004000): AHB-AP (IDR: 0x34770008)
Iterating through AP map to find AHB-AP to use
AP[0]: Core found
AP[0]: AHB-AP ROM base: 0xE00FF000
CPUID register: 0x411FD210. Implementer code: 0x41 (ARM)
Feature set: Mainline
Cache: No cache
Found Cortex-M33 r1p0, Little endian.
FPUnit: 8 code (BP) slots and 0 literal slots
Security extension: implemented
Secure debug: enabled
```

6. Summary

Attempted mitigations:

Guard reads: Fundamental HW misunderstanding

OTP PSM ring osc. randomization: Nonexistent? Insignificant?

Irrelevant security features:

Glitch detectors: Not on USB_OTP_VDD!

RCP: Game over *before* ROM code!

6. Summary

Lessons:

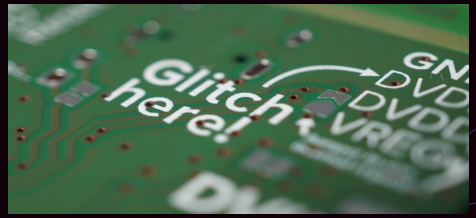
Human communication factors are huge

Sidense knew how to do guards properly, and RPi missed out

“Permanent” is not a thing unless it involves chip destruction

There is some copper somewhere with each signal...

Remember to glitch in the places they *don’t* tell you to



@aedancullen@treehouse.systems