Back in the Driver's Seat

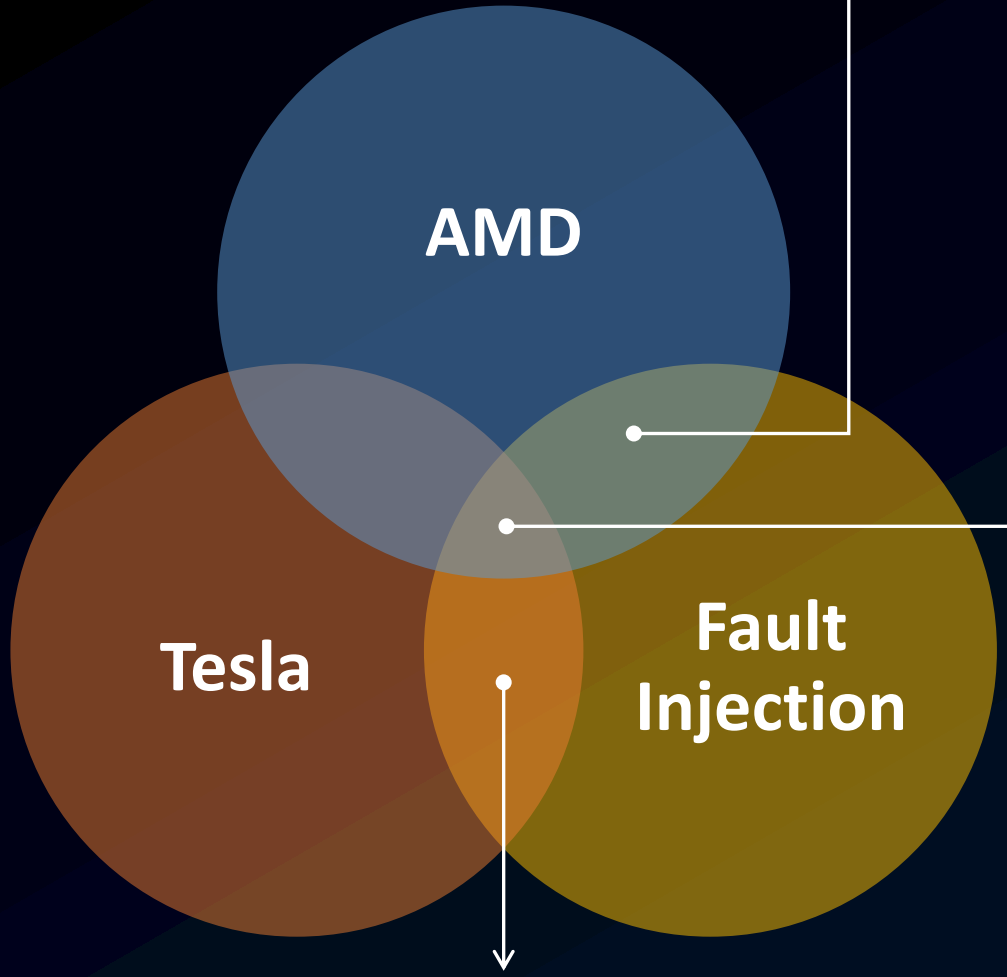
RECOVERING CRITICAL DATA FROM TESLA AUTOPILOT USING VOLTAGE GLITCHING

Christian Werling
Niclas Kühnapfel
Hans Niklas Jacob
TU Berlin

Oleg Drokin
Independent

1. Motivation & Background
2. Hardware Analysis & Attack
3. Autopilot Internals & Data Extraction

Previous work



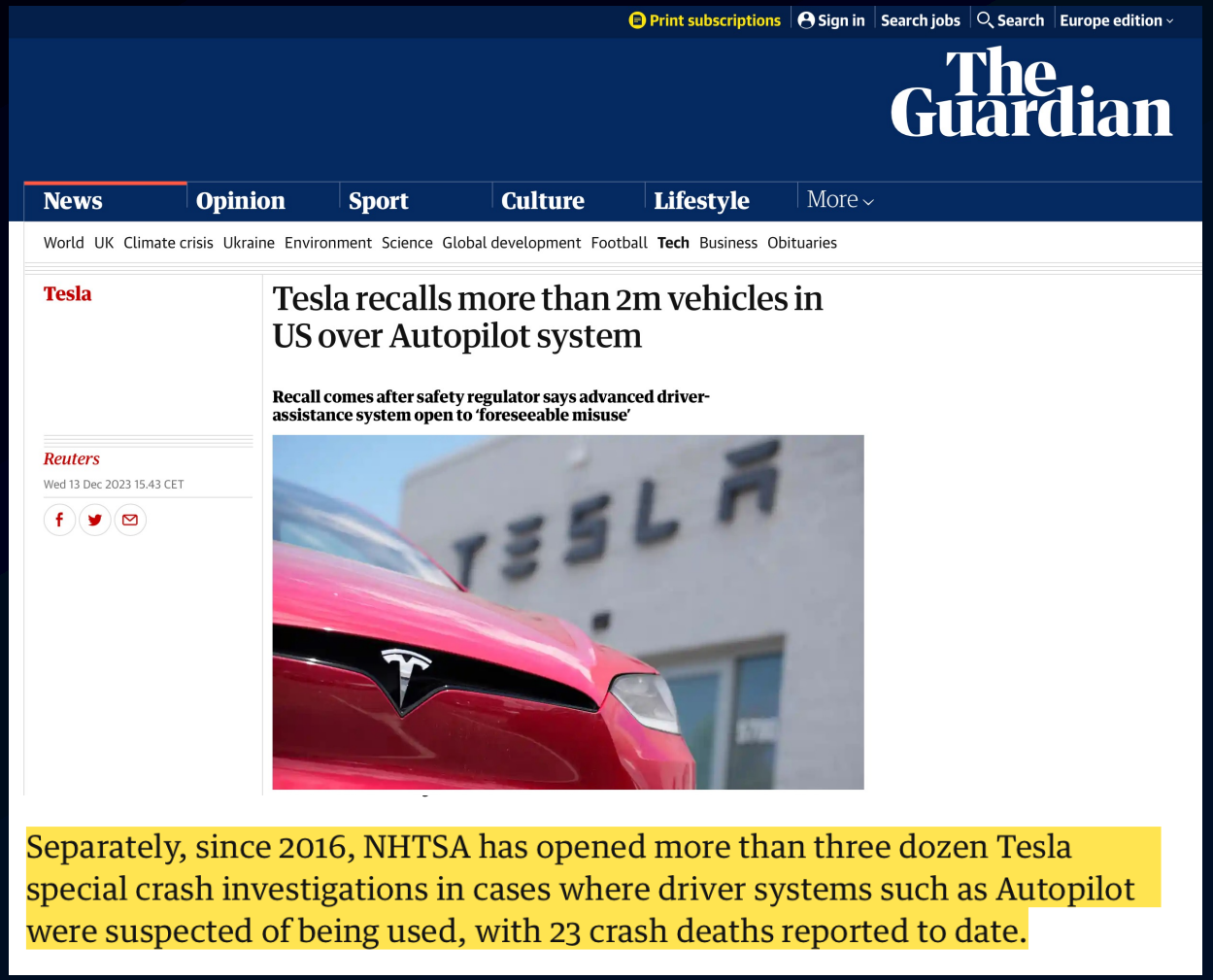
This talk

- **“One Glitch to Rule Them All”** (2021)
  Fault Injection Attacks Against AMD’s Secure Encrypted Virtualization
- **“faulTPM”** (2022)
  Exposing AMD fTPMs' Deepest Secrets
- **“EM-Fault It Yourself”** (2022)
  Building a Replicable EMFI Setup for Desktop and Server Hardware

black hat USA 2023

Motivation

- Controversial system
  - Advanced driving assistant
  - Involved in accident investigations
  - Rumors about hidden features (“Elon mode”)
- Mature *software* security practices on Infotainment
- Large amounts of data!



Print subscriptions | Sign in | Search jobs | Search | Europe edition

The Guardian

News | Opinion | Sport | Culture | Lifestyle | More

World UK Climate crisis Ukraine Environment Science Global development Football Tech Business Obituaries

Tesla

Tesla recalls more than 2m vehicles in US over Autopilot system

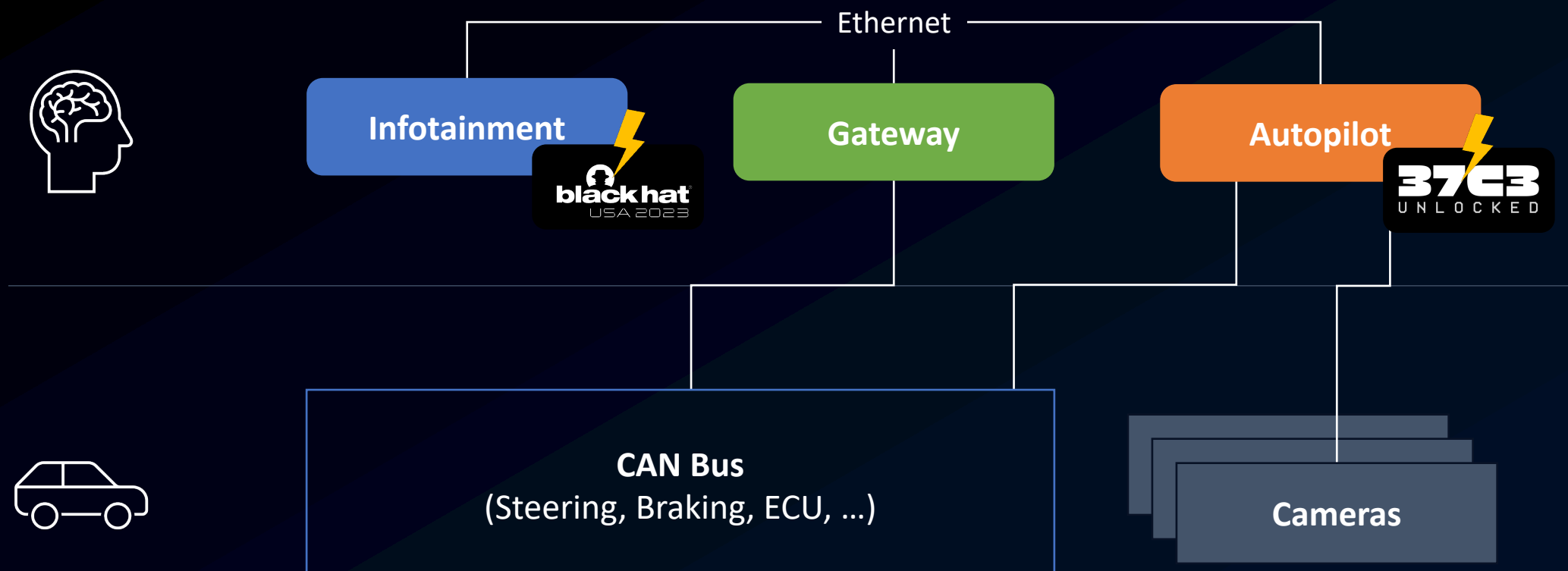
Recall comes after safety regulator says advanced driver-assistance system open to ‘foreseeable misuse’

Reuters

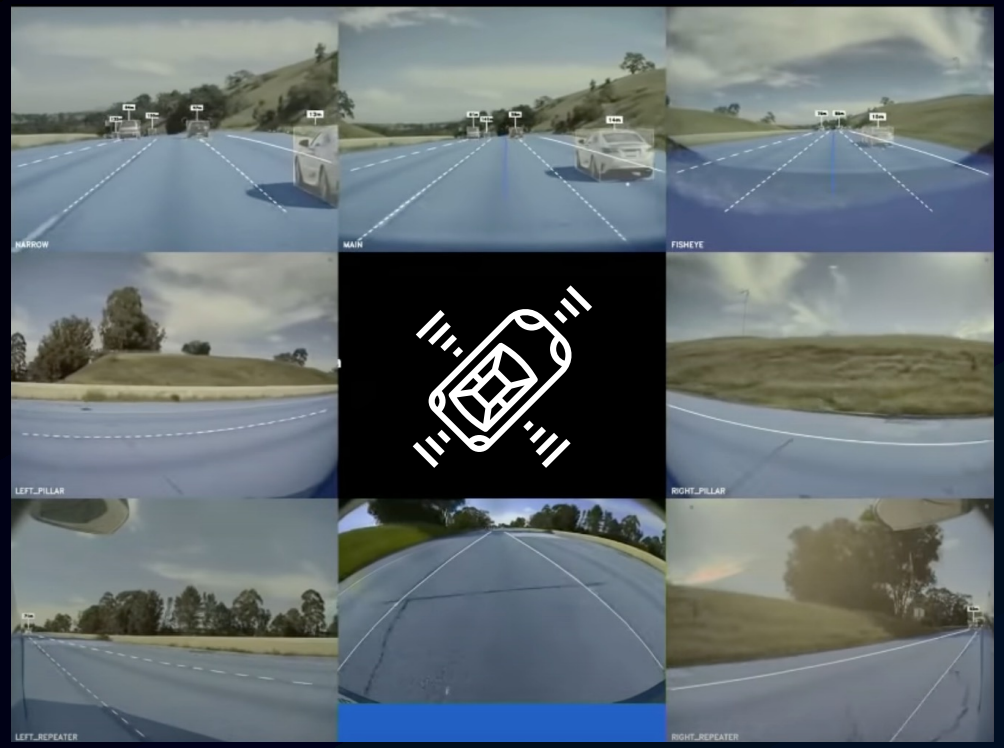
Wed 13 Dec 2023 15.43 CET

Separately, since 2016, NHTSA has opened more than three dozen Tesla special crash investigations in cases where driver systems such as Autopilot were suspected of being used, with 23 crash deaths reported to date.

System architecture



Autopilot



”Tesla Autonomy Day”, April 2019 (YouTube)
Icon by pongsakorn from the Noun Project

AI Addict/YouTube

Logging

	Information	Resolution	Duration	Trigger	Location	Access
Event Data Recorder	Misc.	Async.	< 30s	Airbag	Airbag	1,400 $ Hardware + Free Software
Logs	CAN data, no GPS	5 Hz	∞	-	Gateway SD	SD Card reader, proprietary
High Resolution Logs	CAN data, with GPS	50 Hz	< 60s	Airbag & others	Gateway SD	SD Card reader, proprietary
Snapshots	CAN data, Cameras, …	highest	any	Airbag & others	?	?

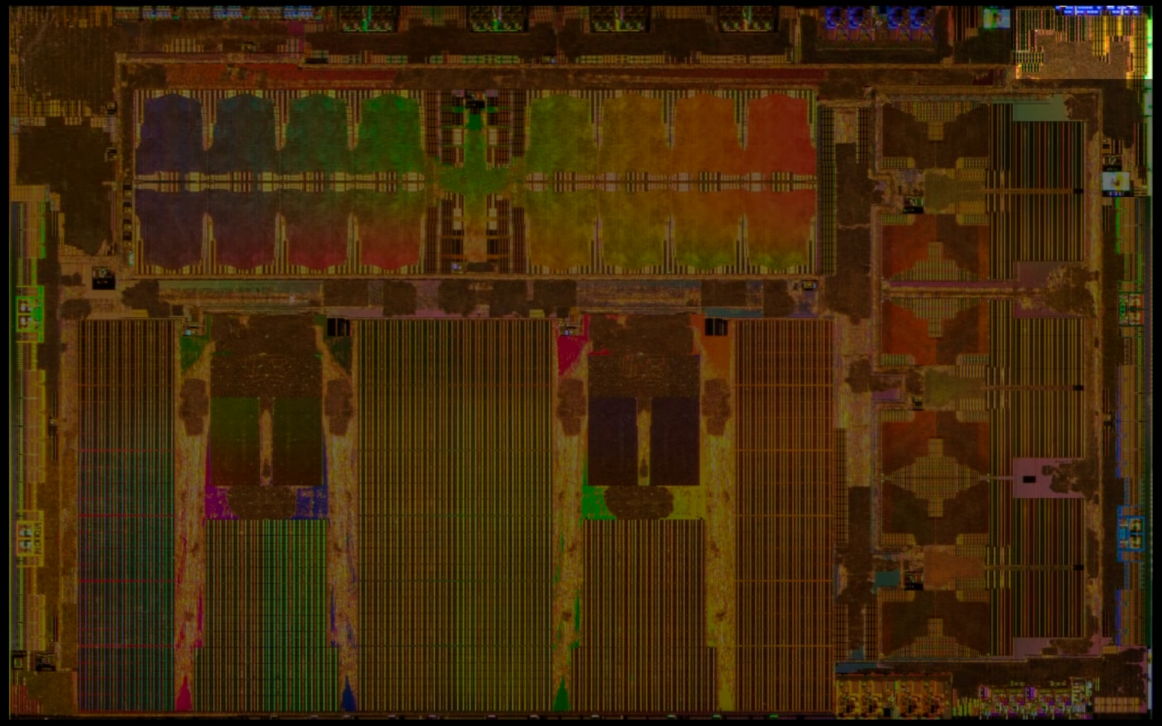
Autopilot Hardware Evolution

	HW1 (2014)	HW2 (2016)	HW2.5 (2017)	HW3 (2019)	HW4 (2023)
Cameras	1 Front-Facing (Backup n.c.)	8 Cameras (3 front-facing, 2 pillar cams, 2 side-rear facing, 1 backup)			-1 front-facing
Sensors	Bosch radar 12 Sonars		(Continental radar)		Phoenix radar
Processors	Mobileye EyeQ3	Nvidia Parker SoC Nvidia Pascal GPU Infineon TriCore CPU		2 Custom Tesla FSD chips	2 Custom Tesla FSD chips (2nd generation)
Storage		**Unencrypted eMMC**		**Encrypted UFS**	

"Learn how Elon Musk has evolved Tesla's Autopilot hardware over the years" - Blane Erwin, Current Automotive

Motivation

SECURITY SYSTEM



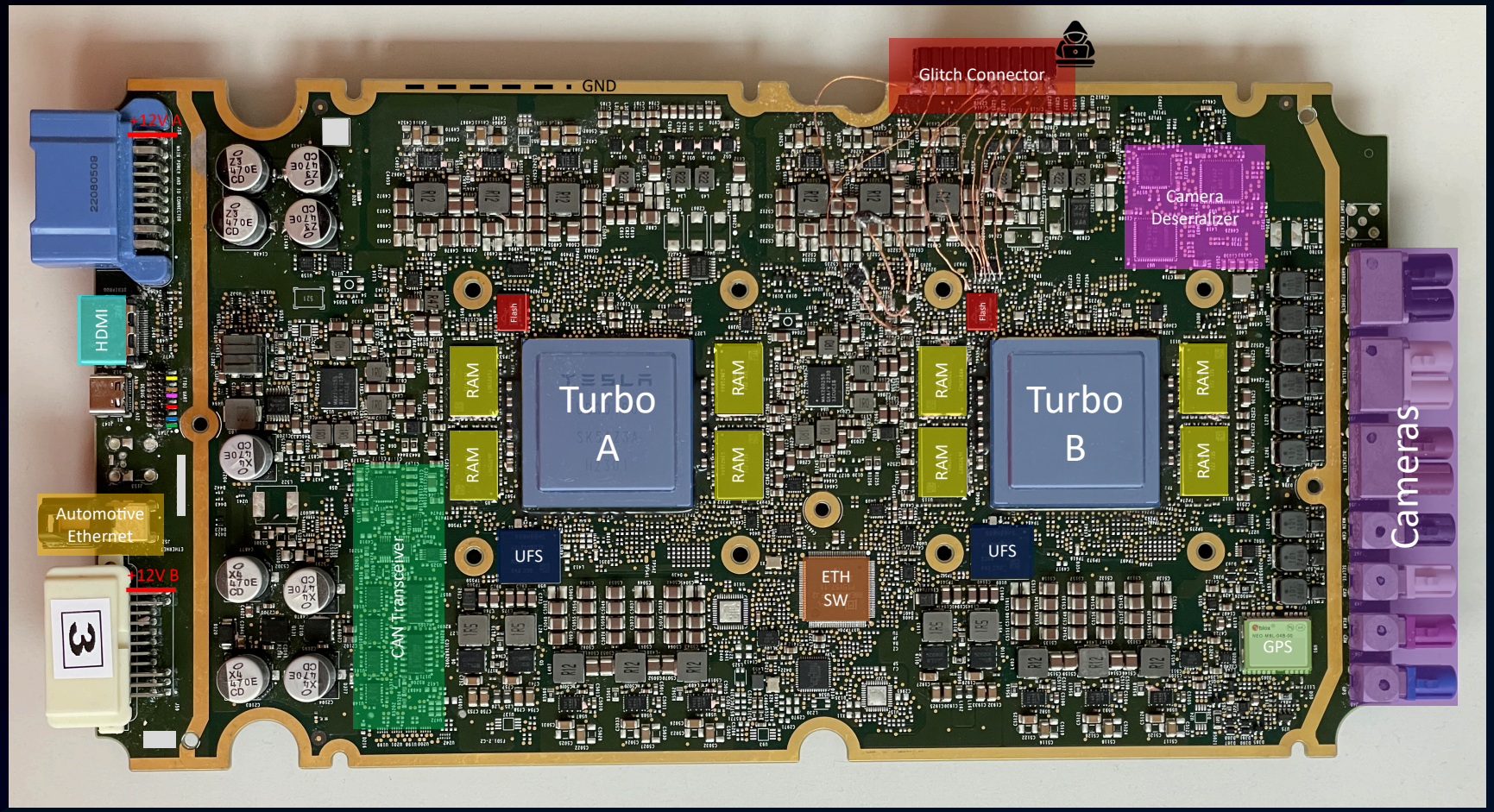
Ensure the system only runs code cryptographically signed by Tesla

TESLA LIVE

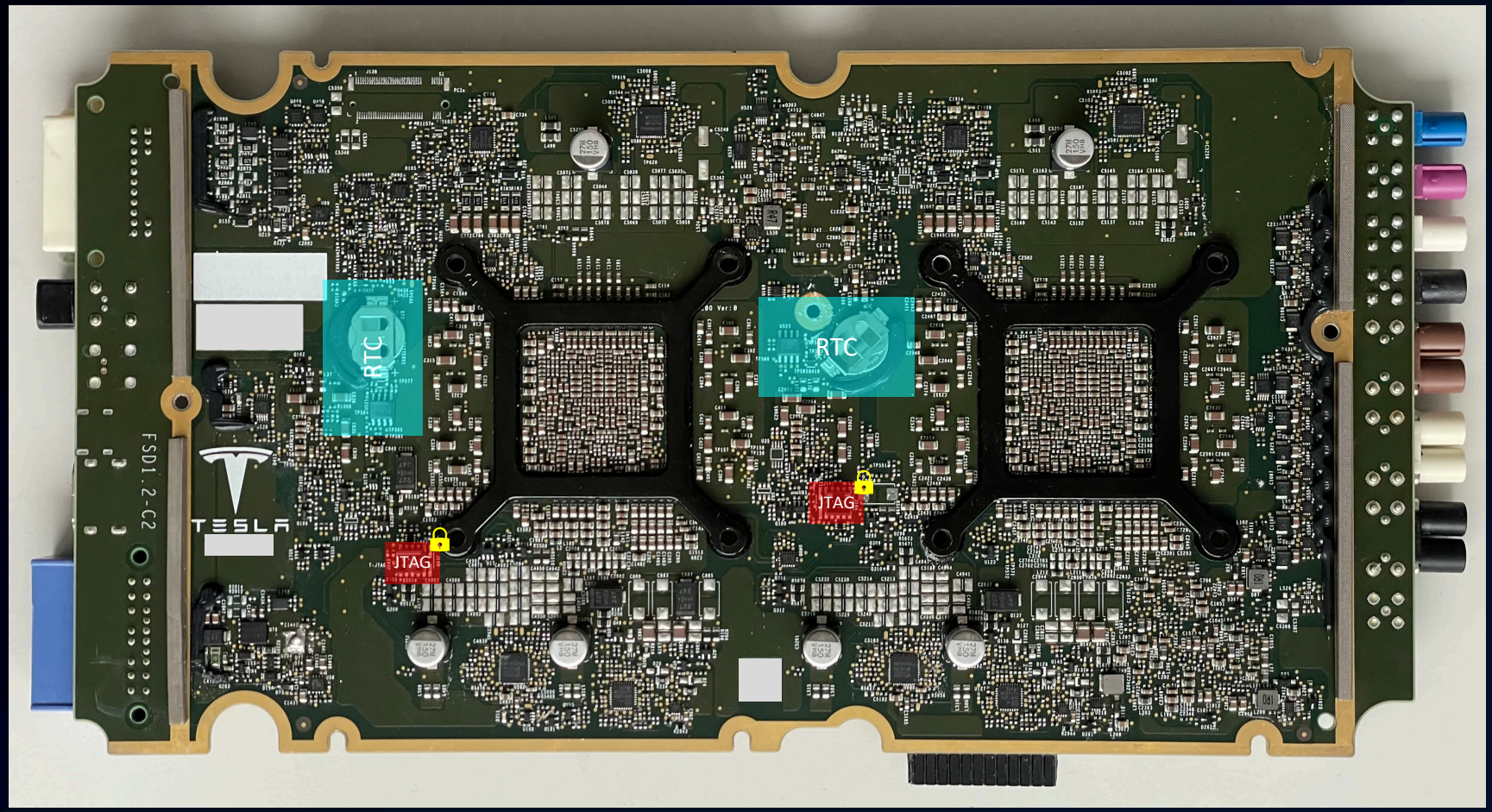
”Tesla Autonomy Day”, April 2019 (YouTube)

1. Motivation & Background
2. Hardware Analysis & Attack
3. Autopilot Internals & Data Extraction

Tesla Autopilot HW3



Tesla Autopilot Hardware 3 (Backside)



“Turbo” Architecture

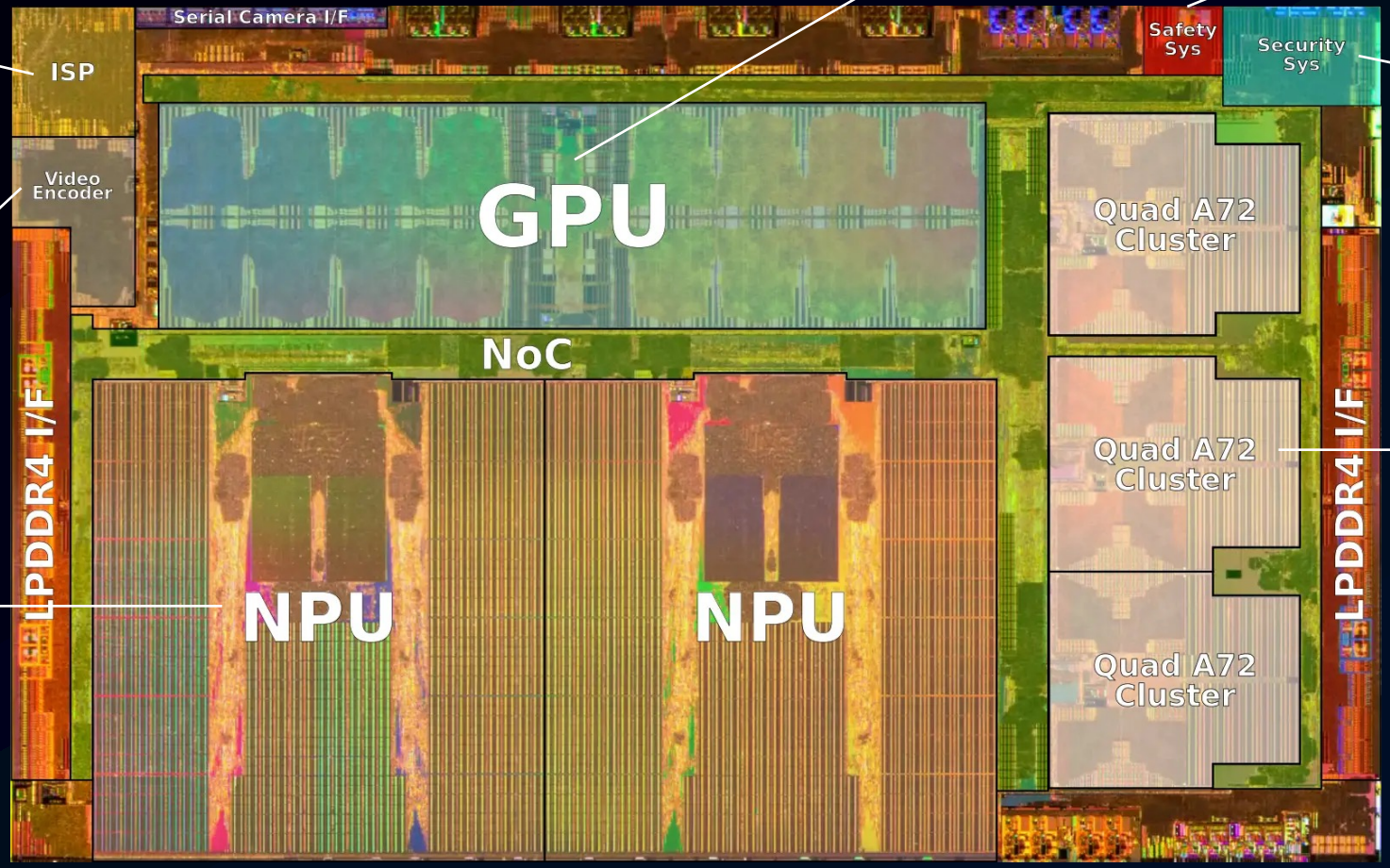


Image Signal Processor (ISP)

H.265 Video Encoder

Neural Processing Units

Mali G71 MP1

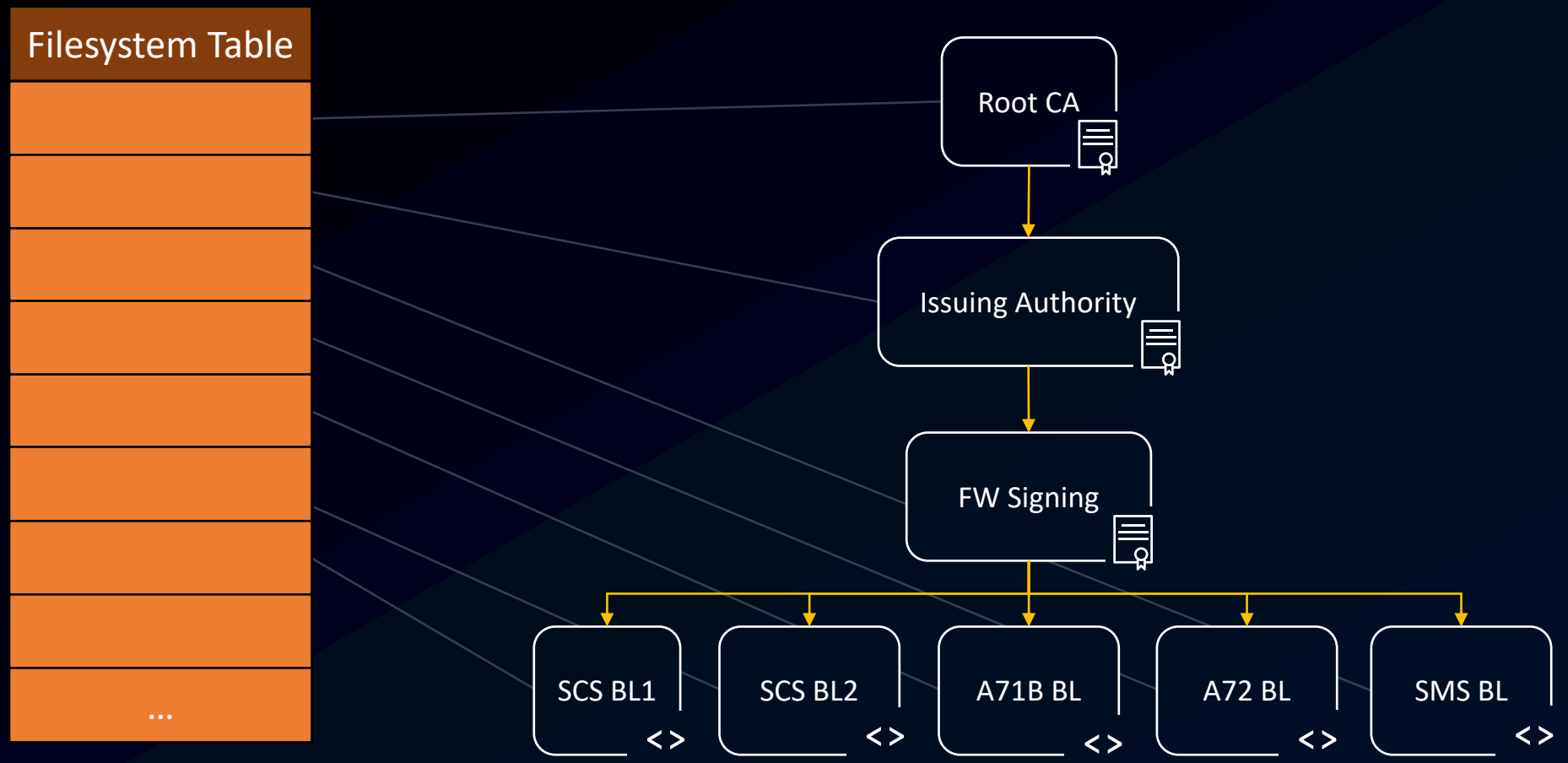
Safety System (SMS)

Security System (SCS)

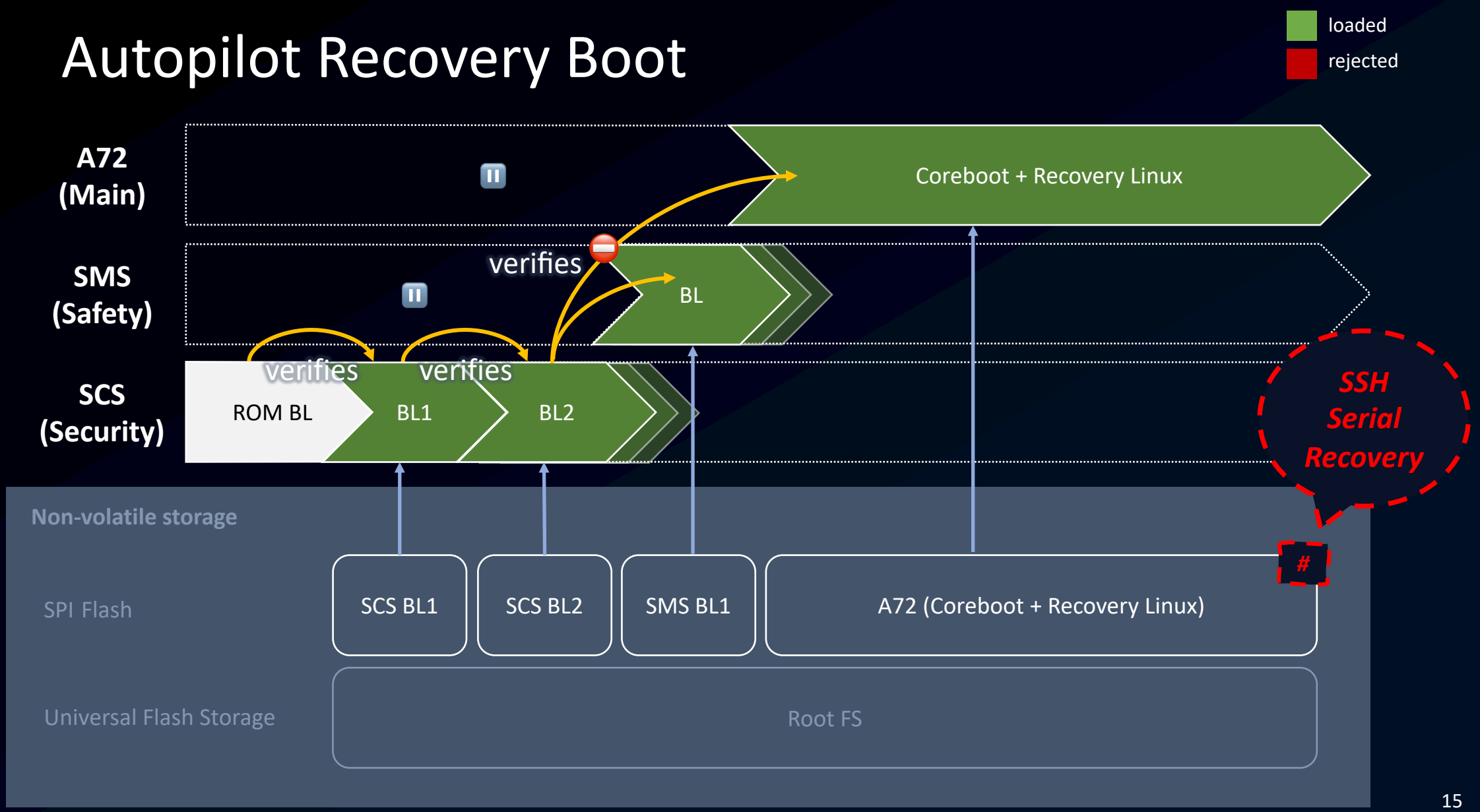
ARM Cortex-A72 Main Cores

”Tesla Autonomy Day”, April 2019 (YouTube)
Annotated by WikiChip

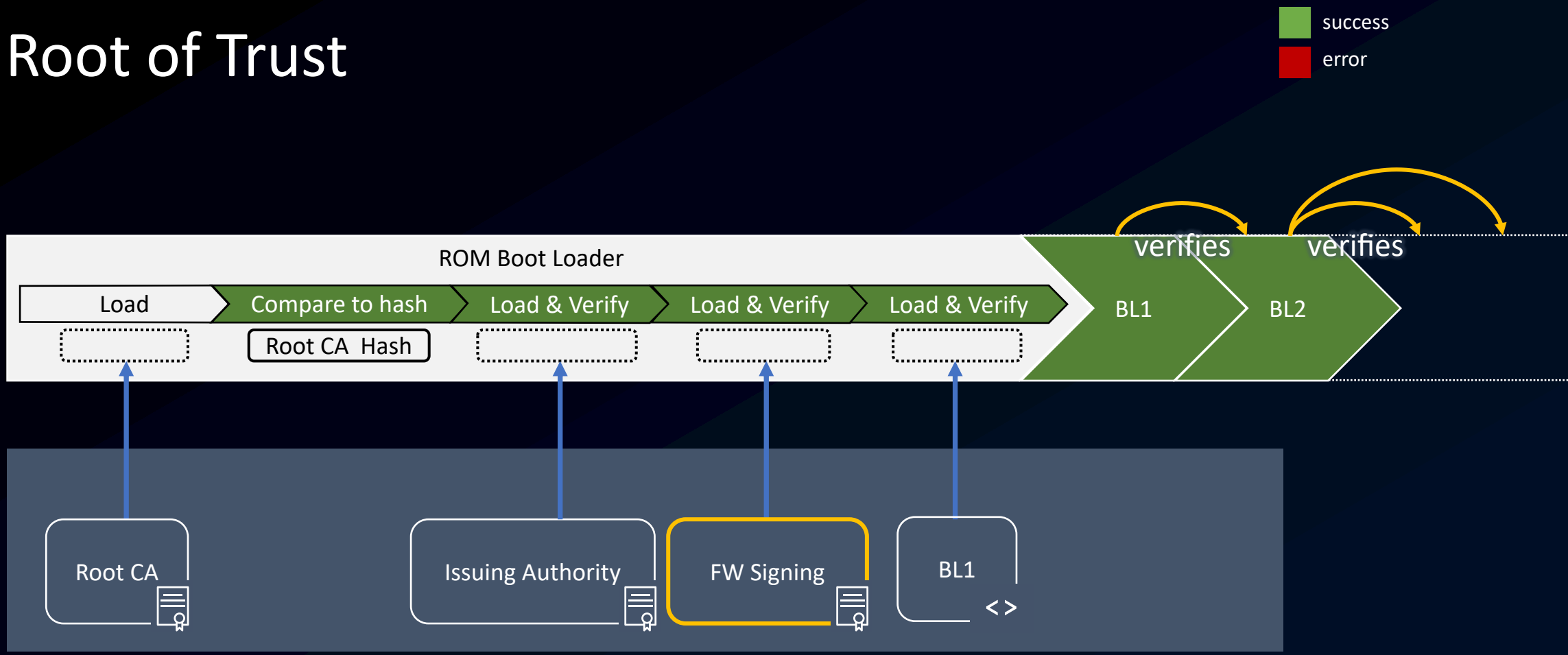
Firmware Structure on SPI Flash



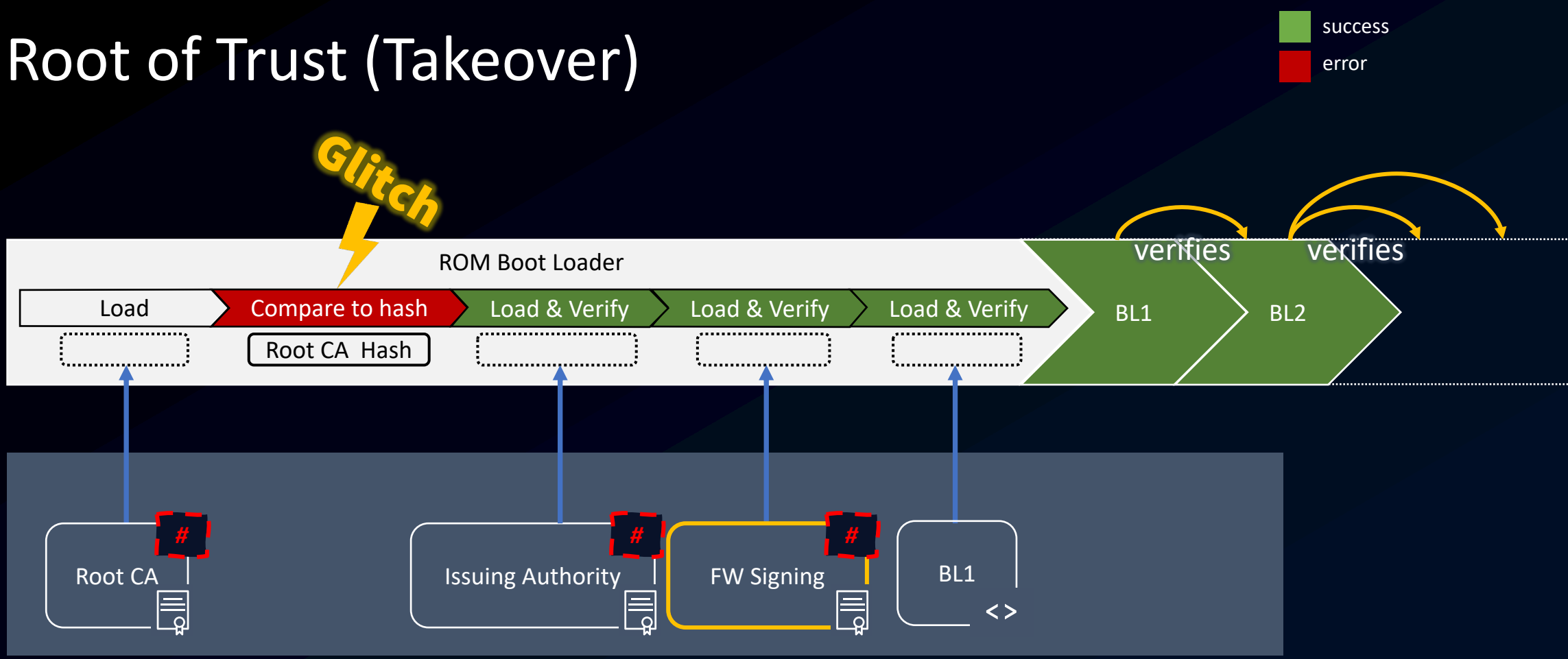
Autopilot Recovery Boot



Root of Trust



Root of Trust (Takeover)



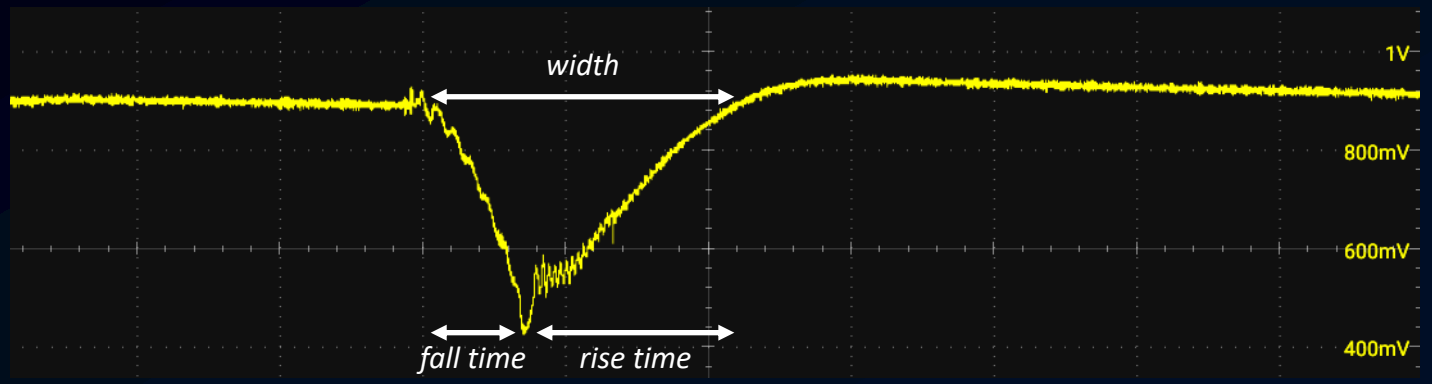
Fault Injection Attacks

Induce fault by altering the IC's environment:

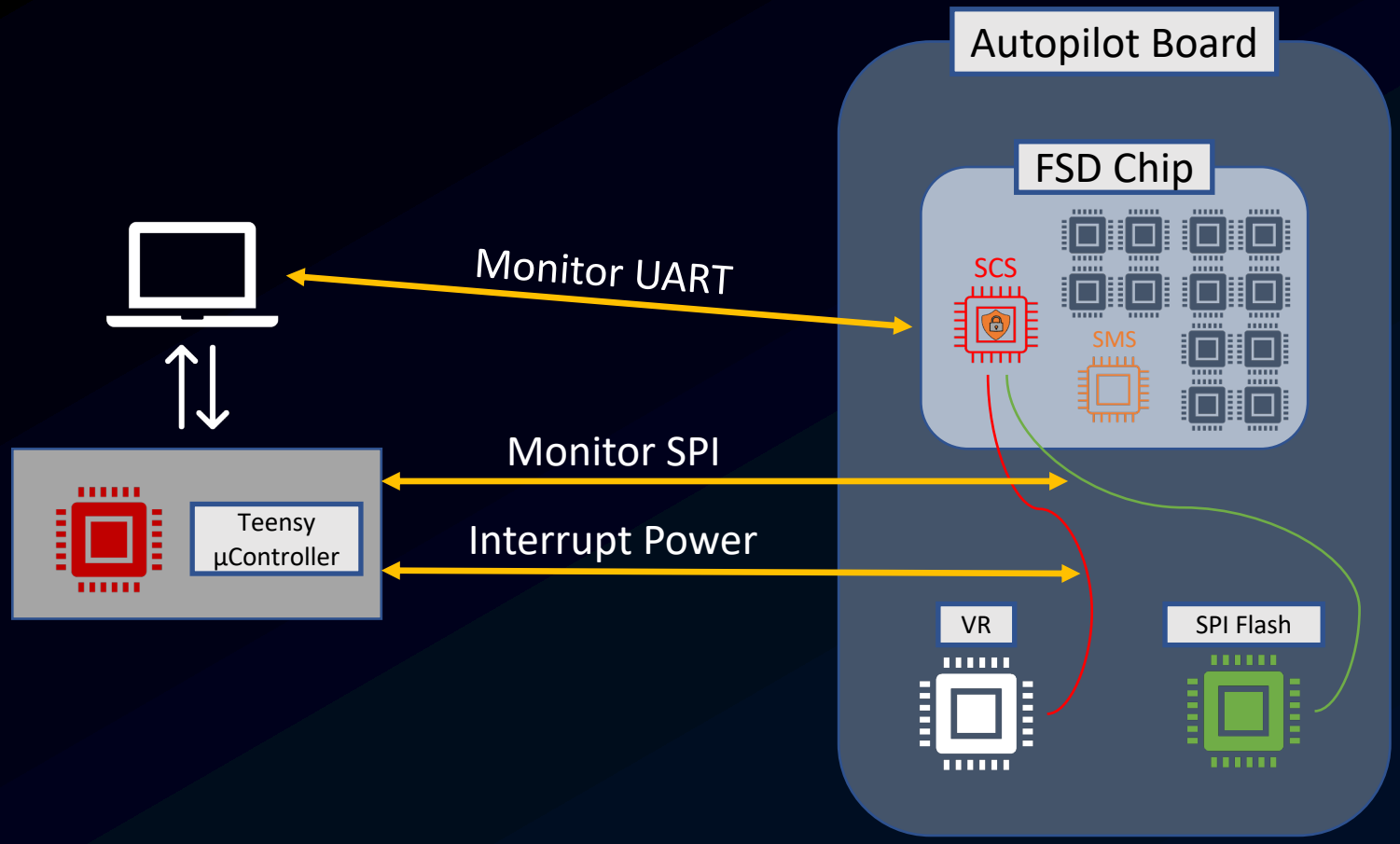
- Laser, electromagnetic-radiation, clock, supply voltage

Voltage Glitching:

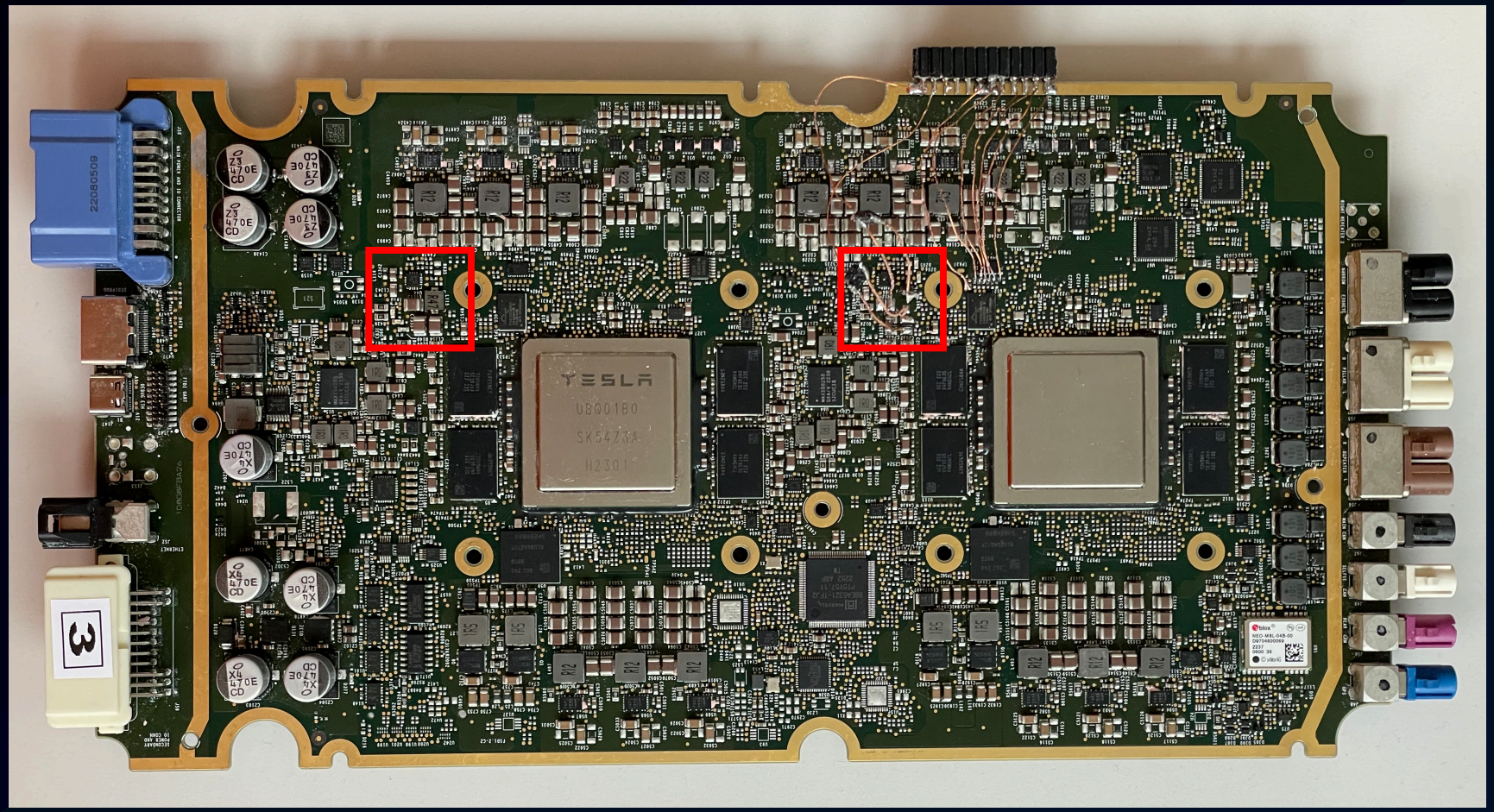
- Lowering voltage shortly



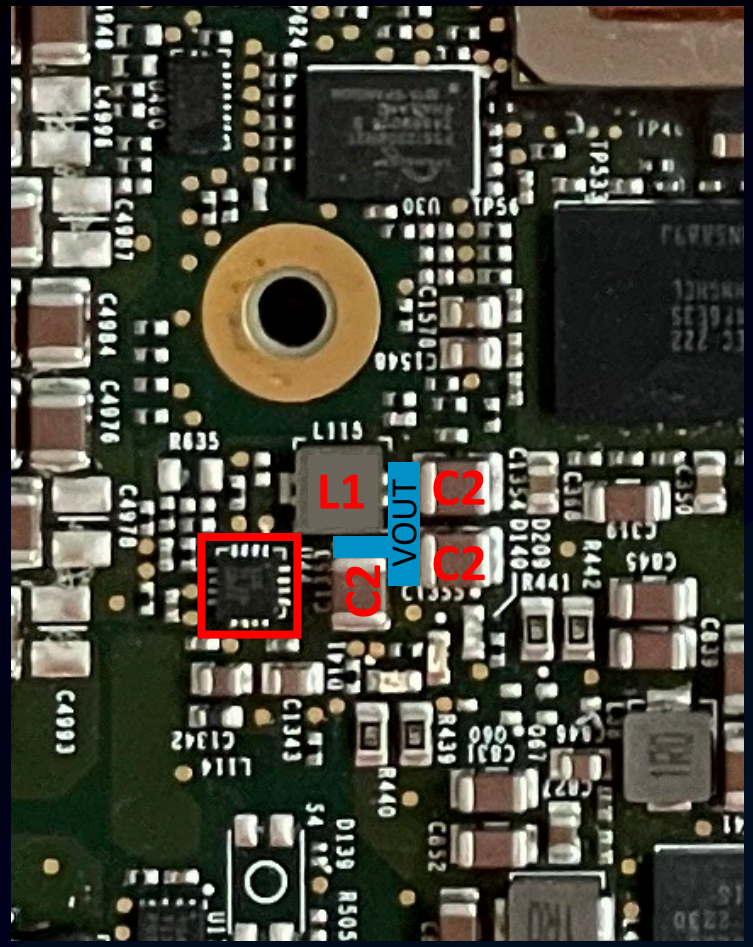
The Plan

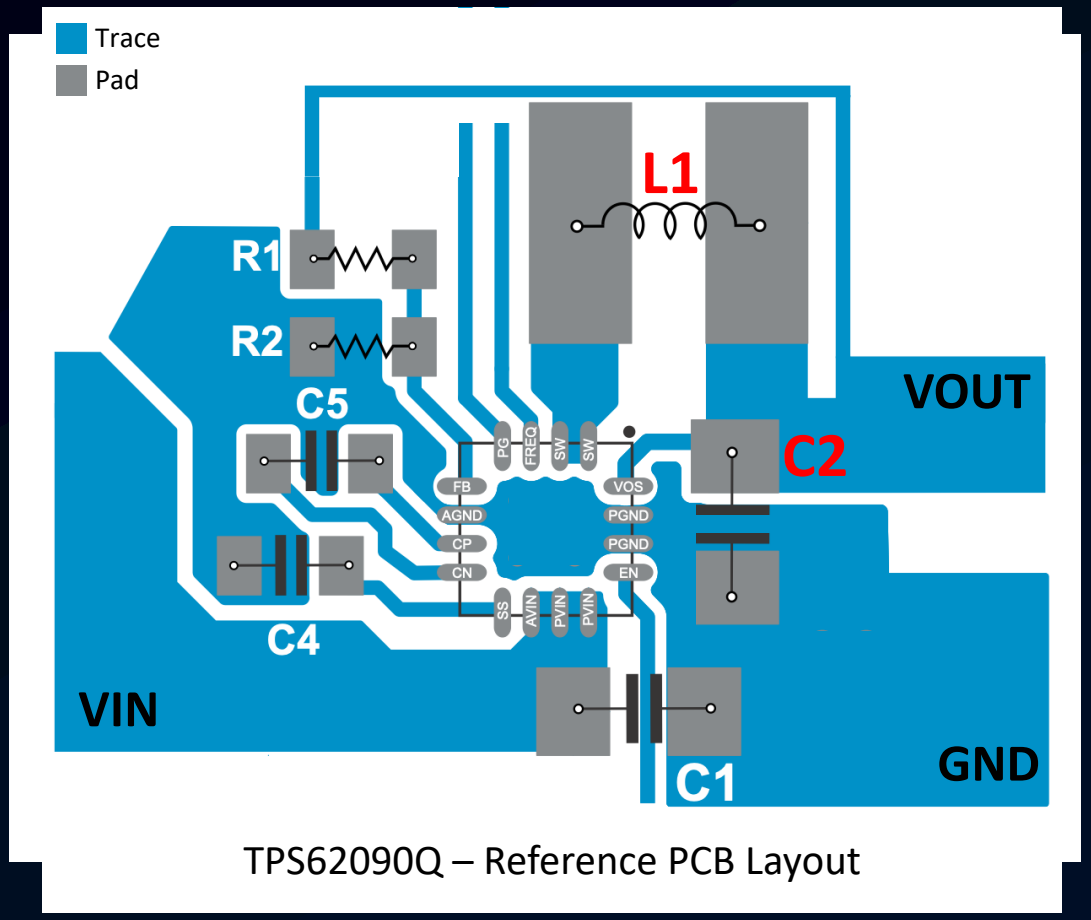

Autopilot Board
FSD Chip
SCS
SMS
Monitor UART
Monitor SPI
Interrupt Power
Teensy
µController
VR
SPI Flash

SCS Power Supply



SCS Power Supply

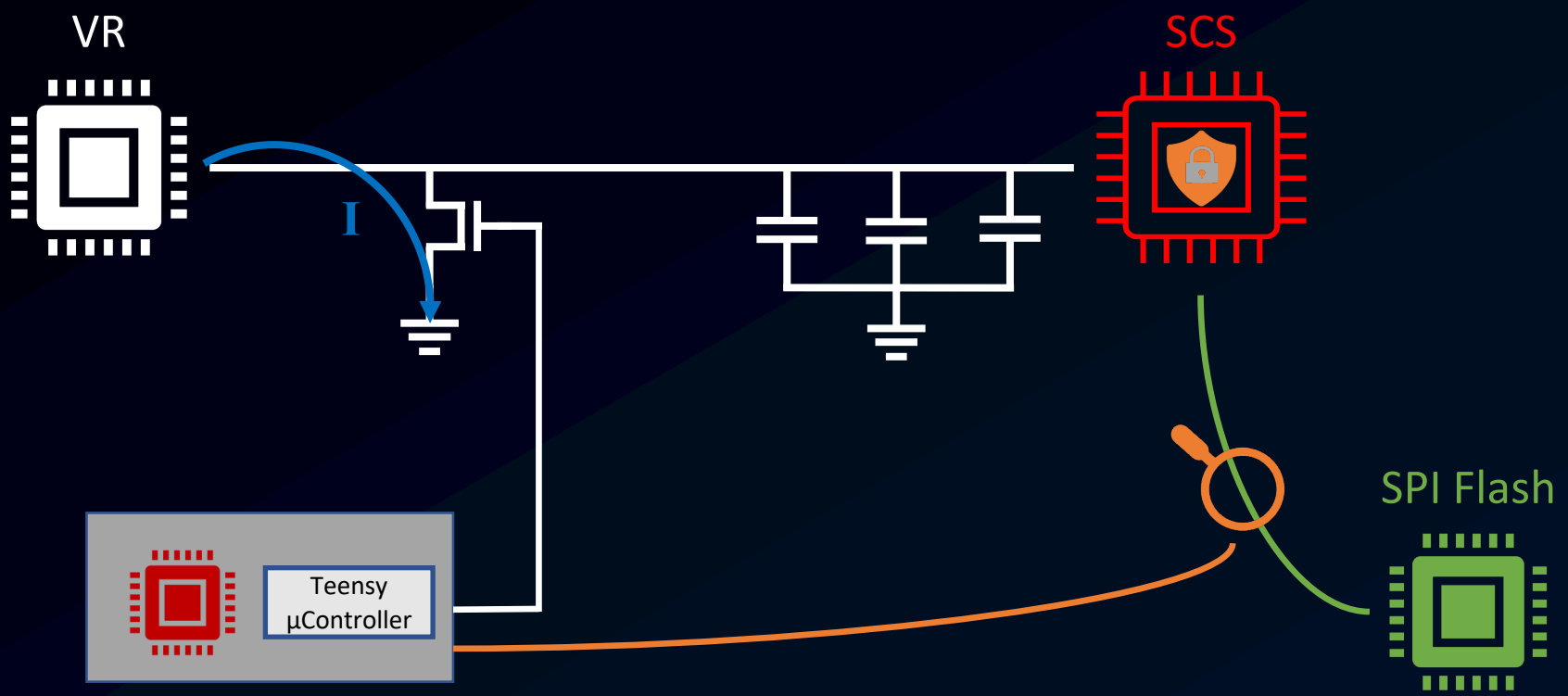




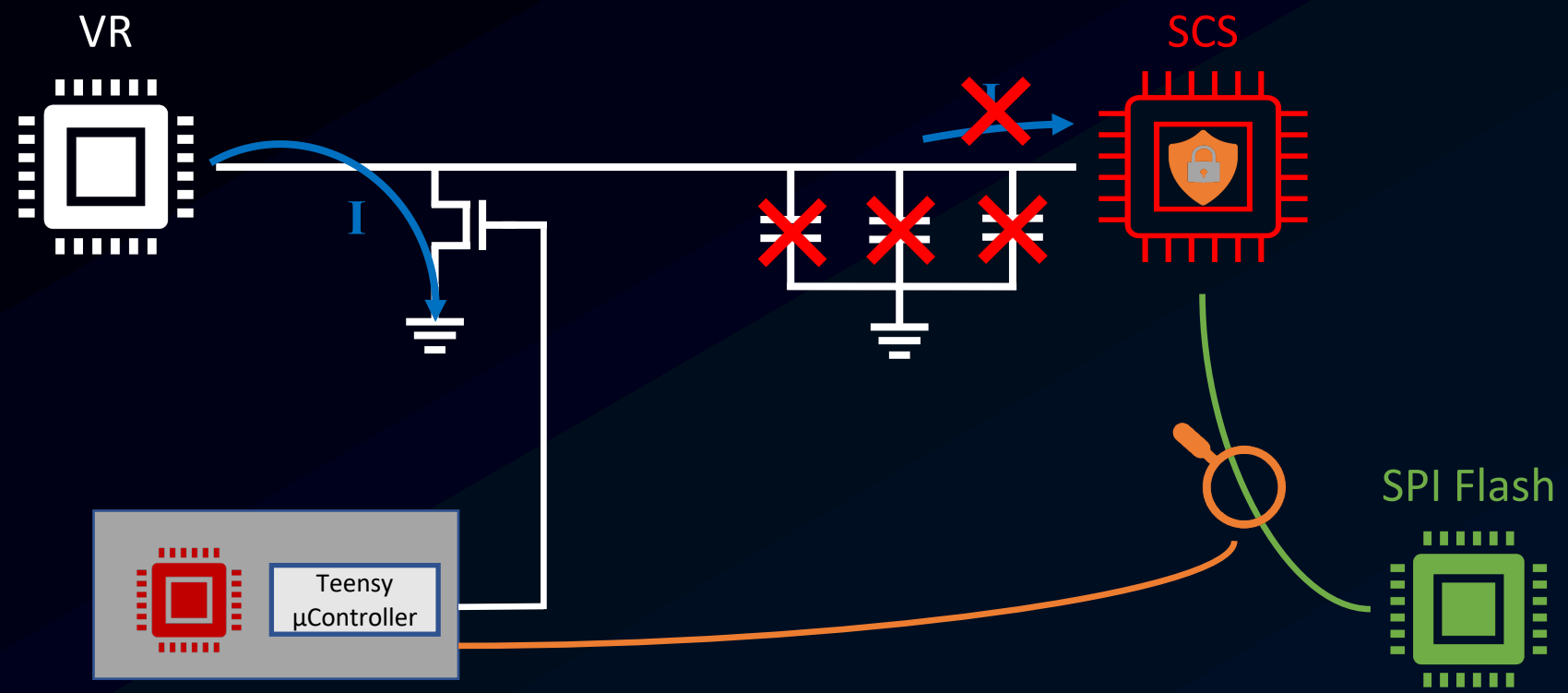
TPS62090Q – Reference PCB Layout

https://www.ti.com/lit/ds/symlink/tps62090-q1.pdf

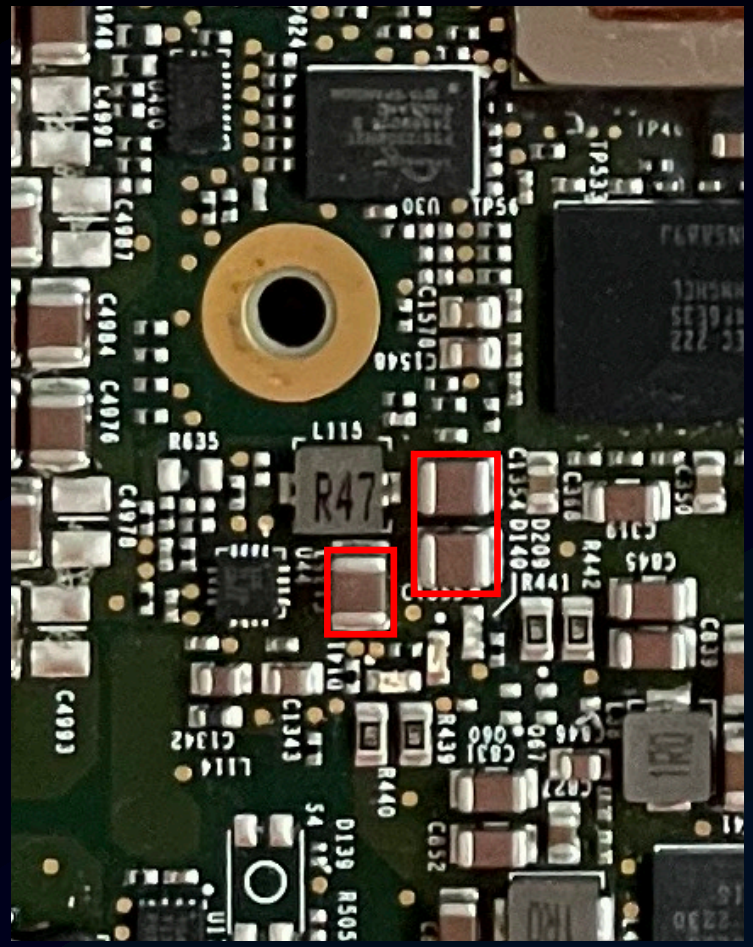
Step 1: Short SCS Voltage

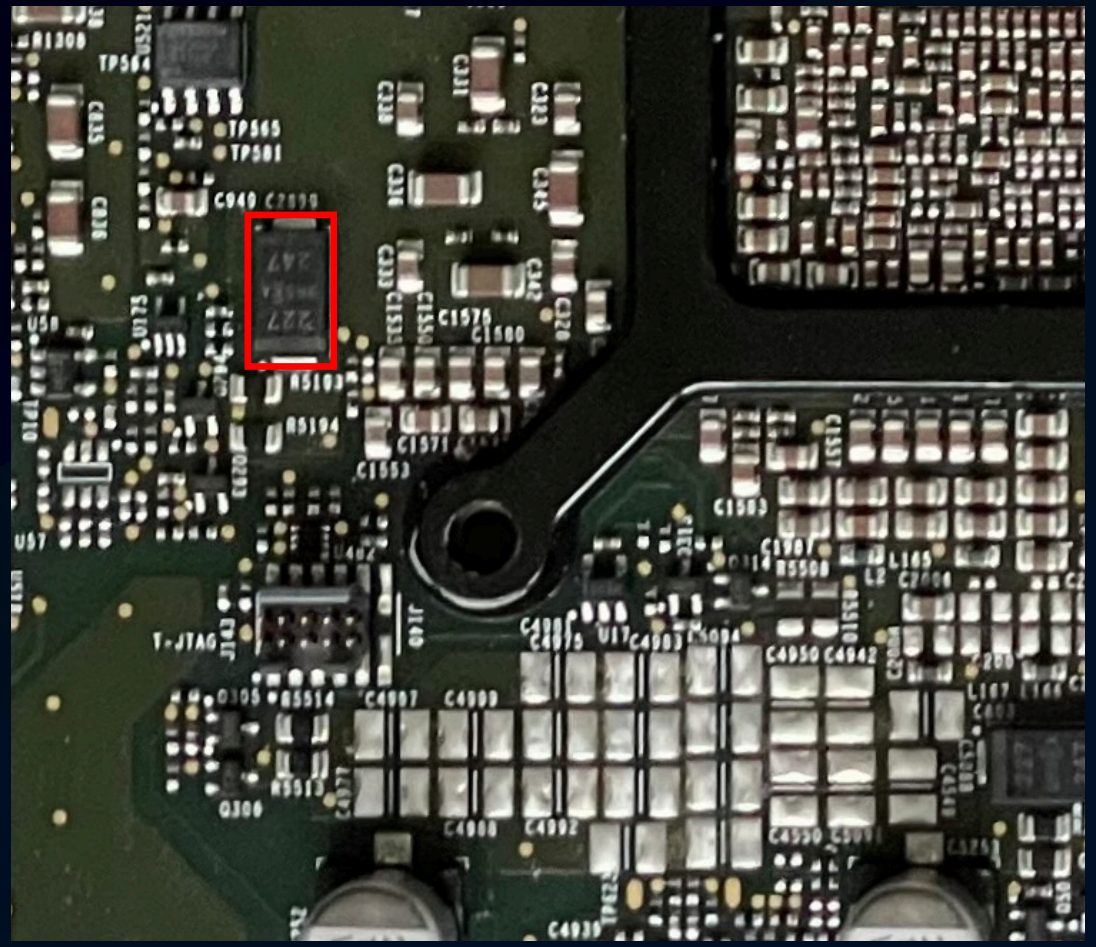


Step 2: Remove Capacitors

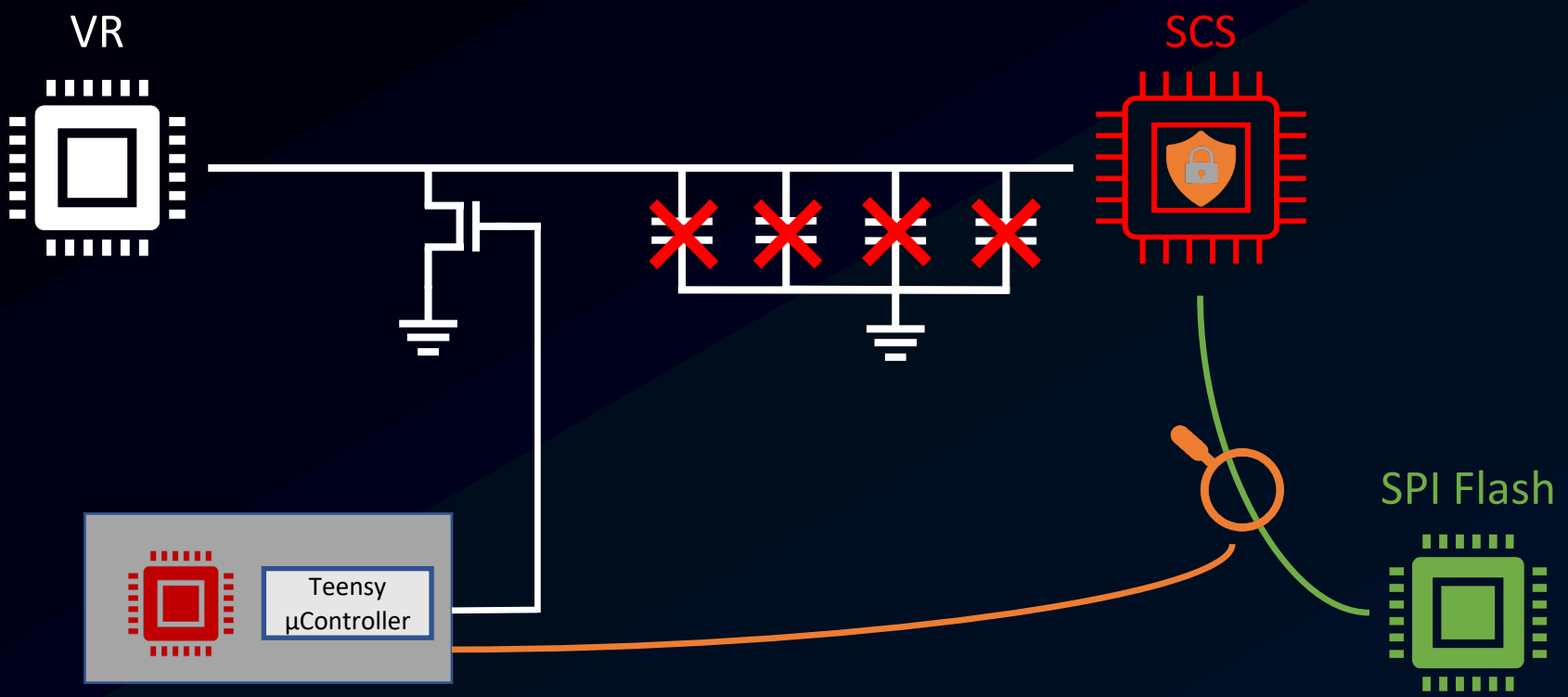


Step 2: Remove Capacitors

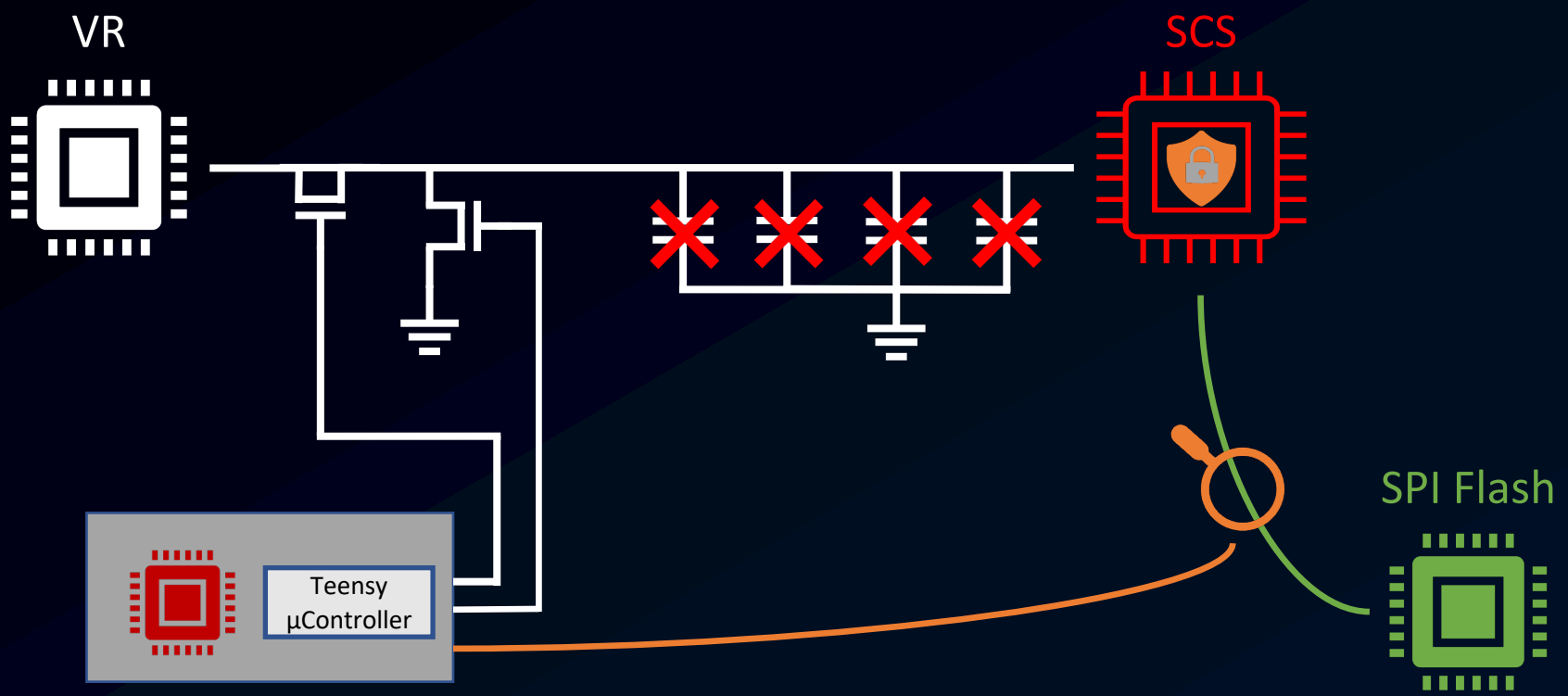




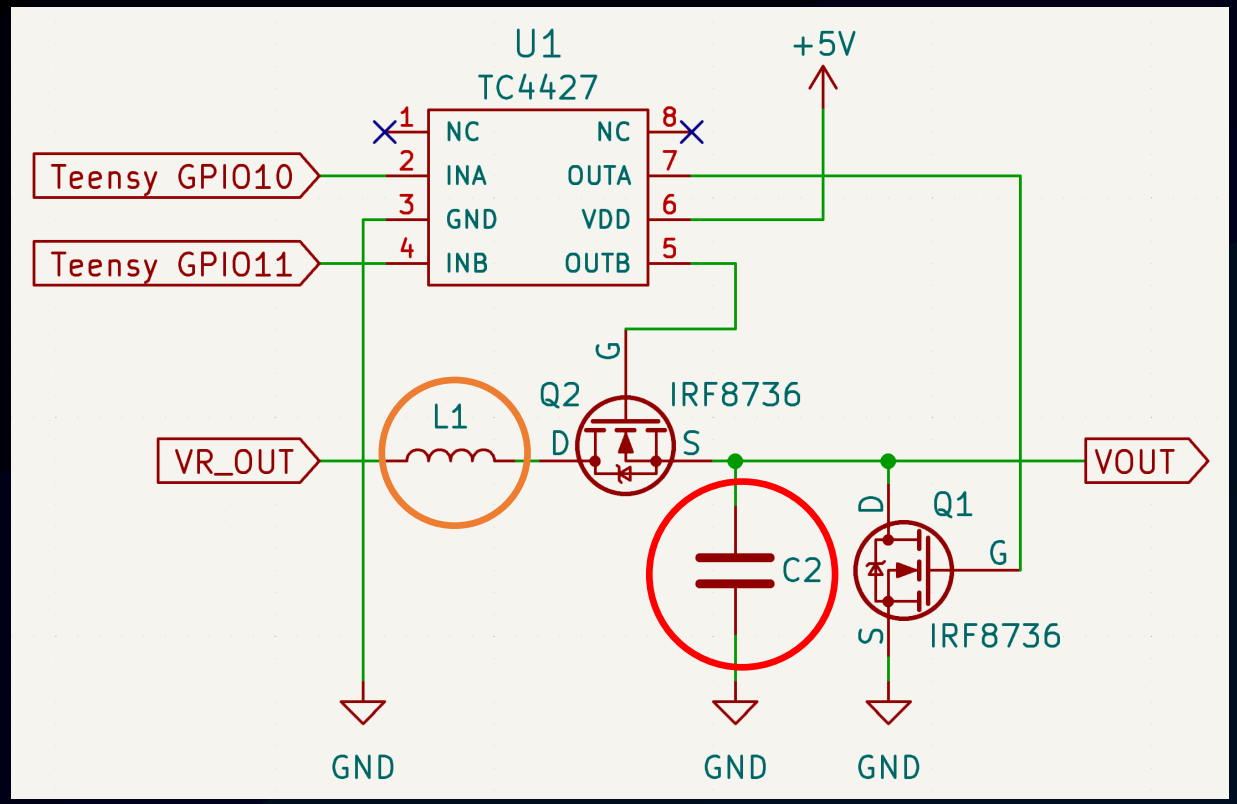
Step 2: Remove Capacitors

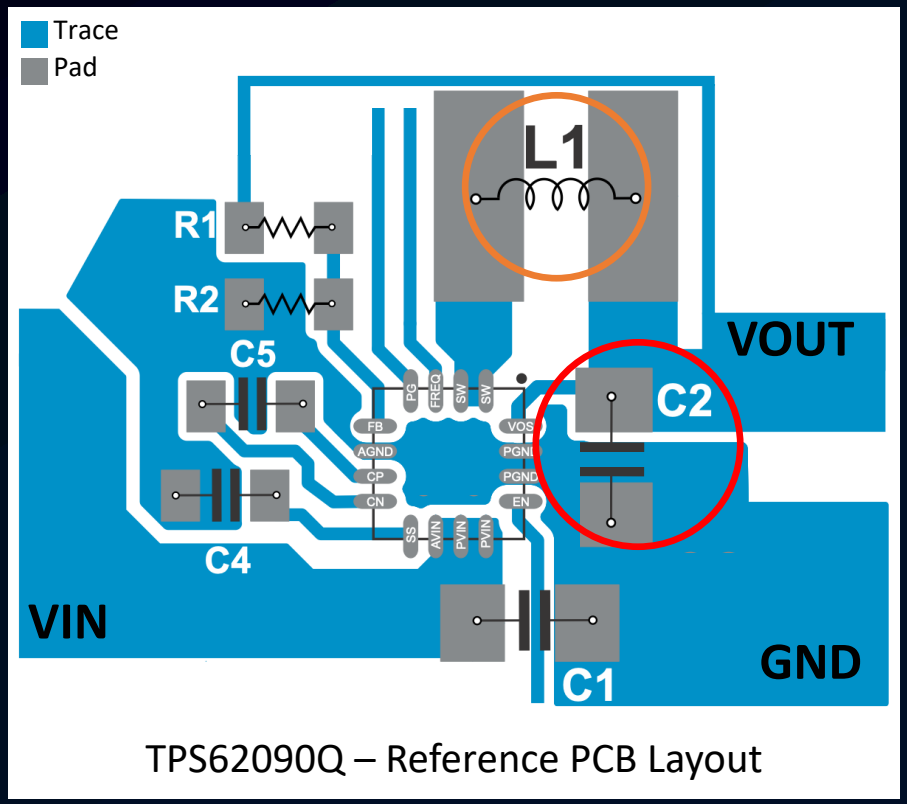


Step 3: Disconnect VR from Voltage Rail



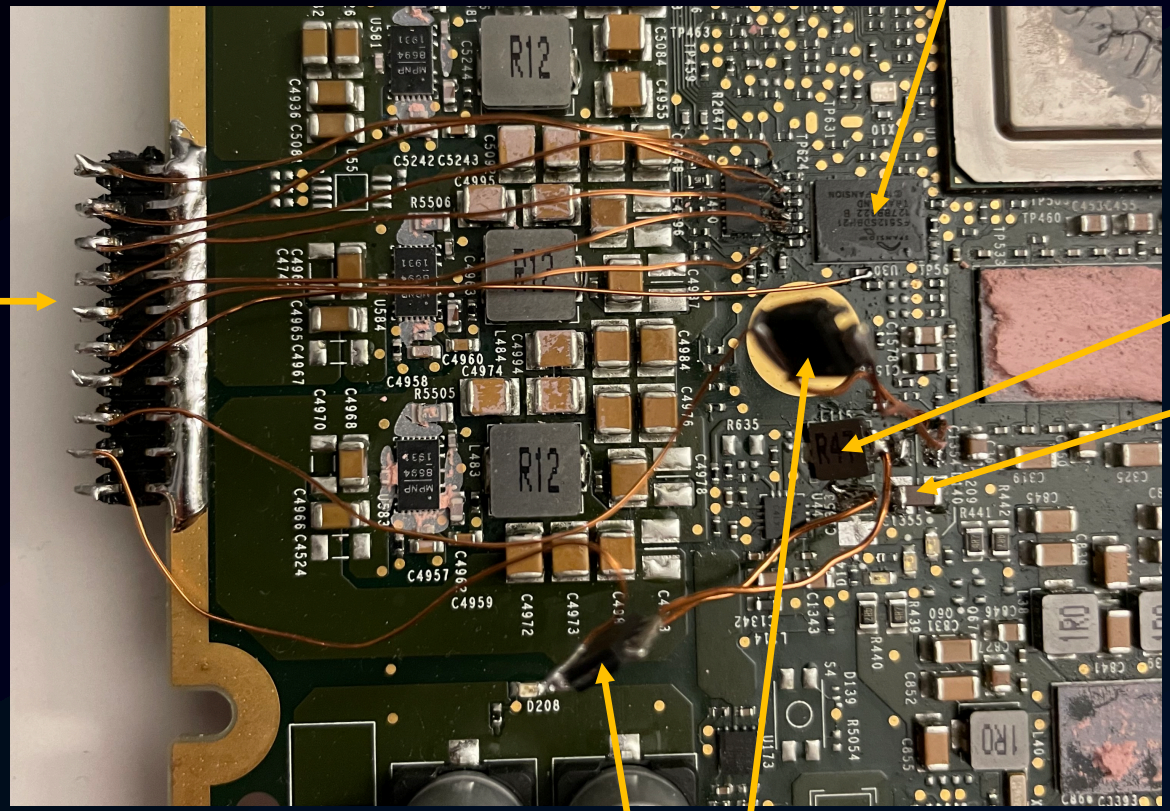
Final Glitching Circuit



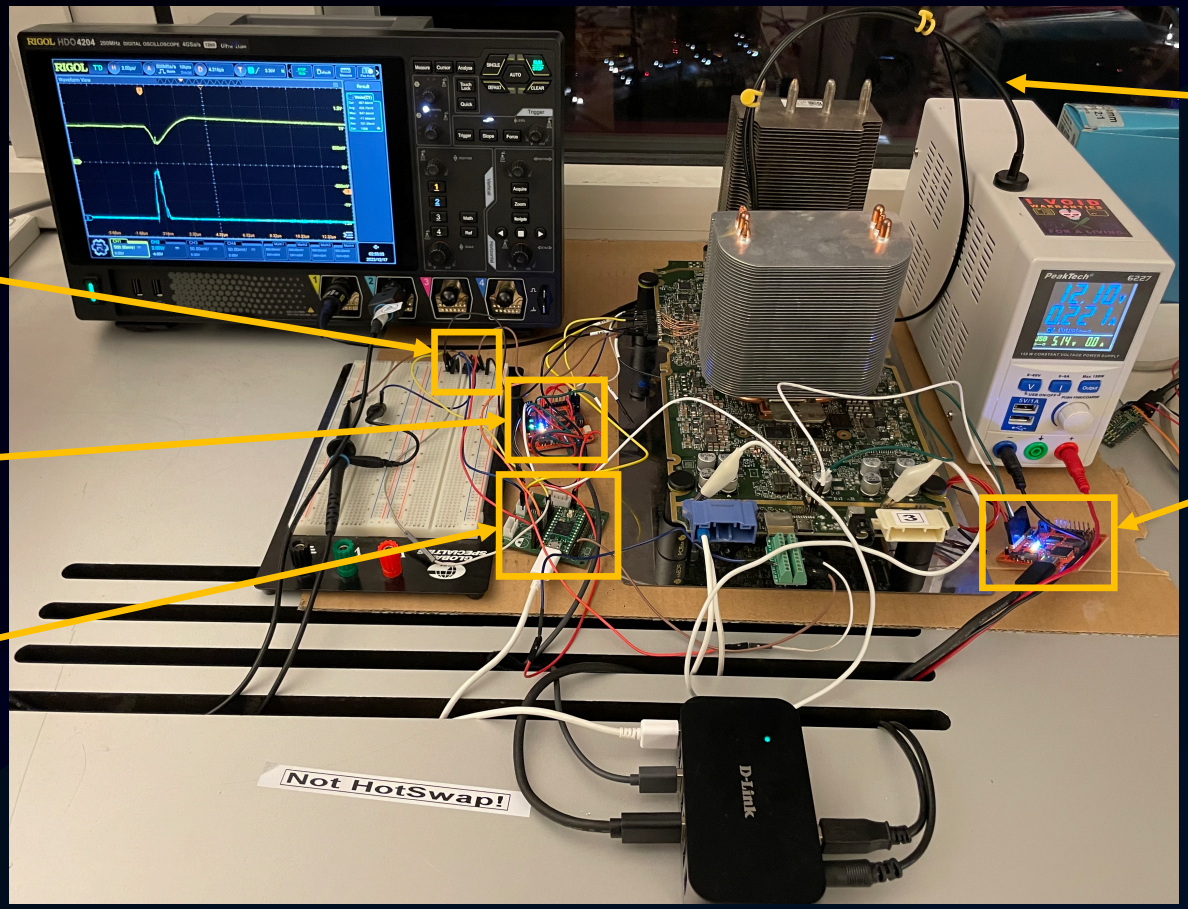


TPS62090Q – Reference PCB Layout

Setup in Reality



Setup in Reality



TC4427

Tigard Board (UART, SPI)

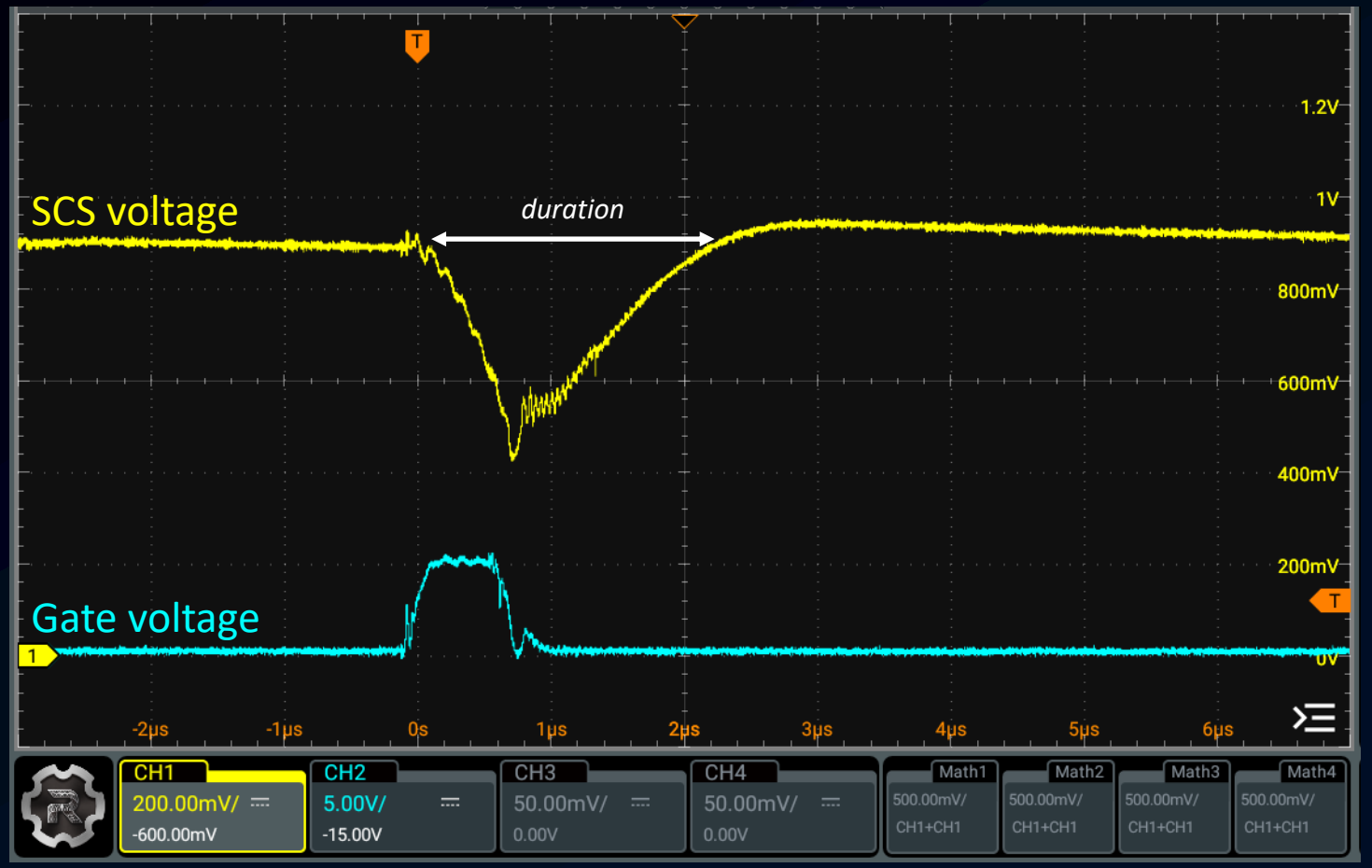
Teensy

Oscilloscope Probe

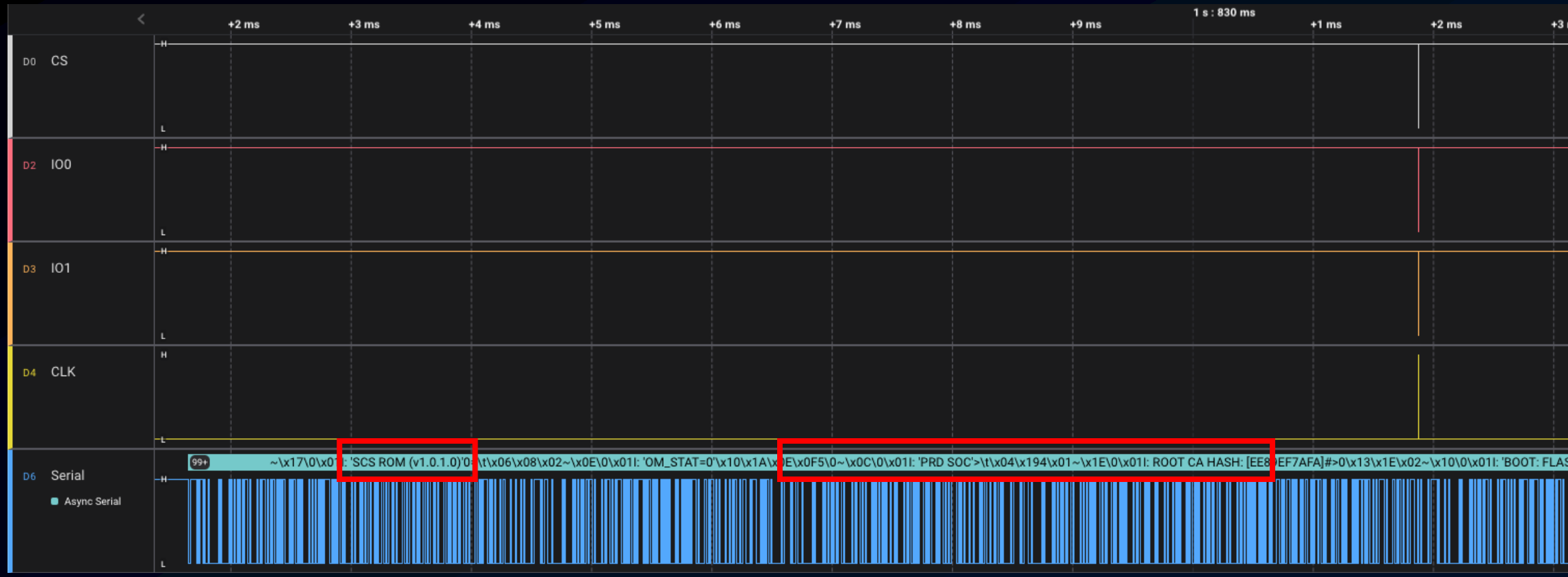
Tigard Board (UART)

Tuning the Drop

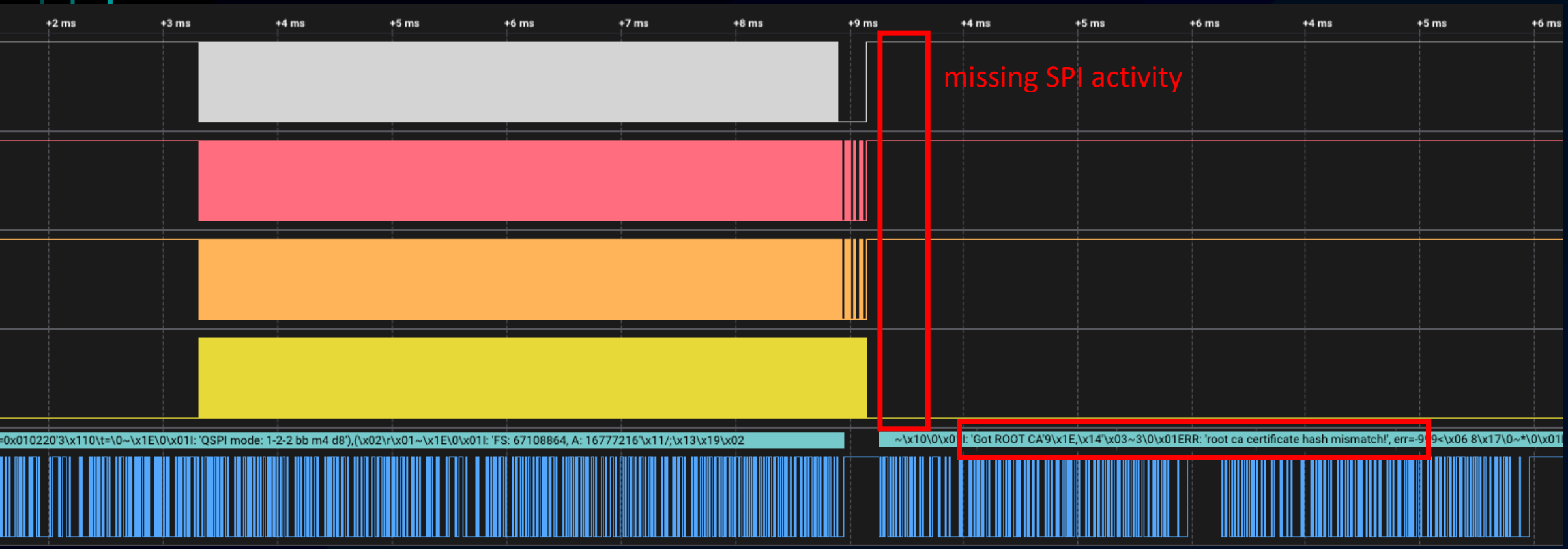
- Determine proper duration by trial and error
- Watch UART log while testing different values
- Too short = no effect
- Too long = always reset



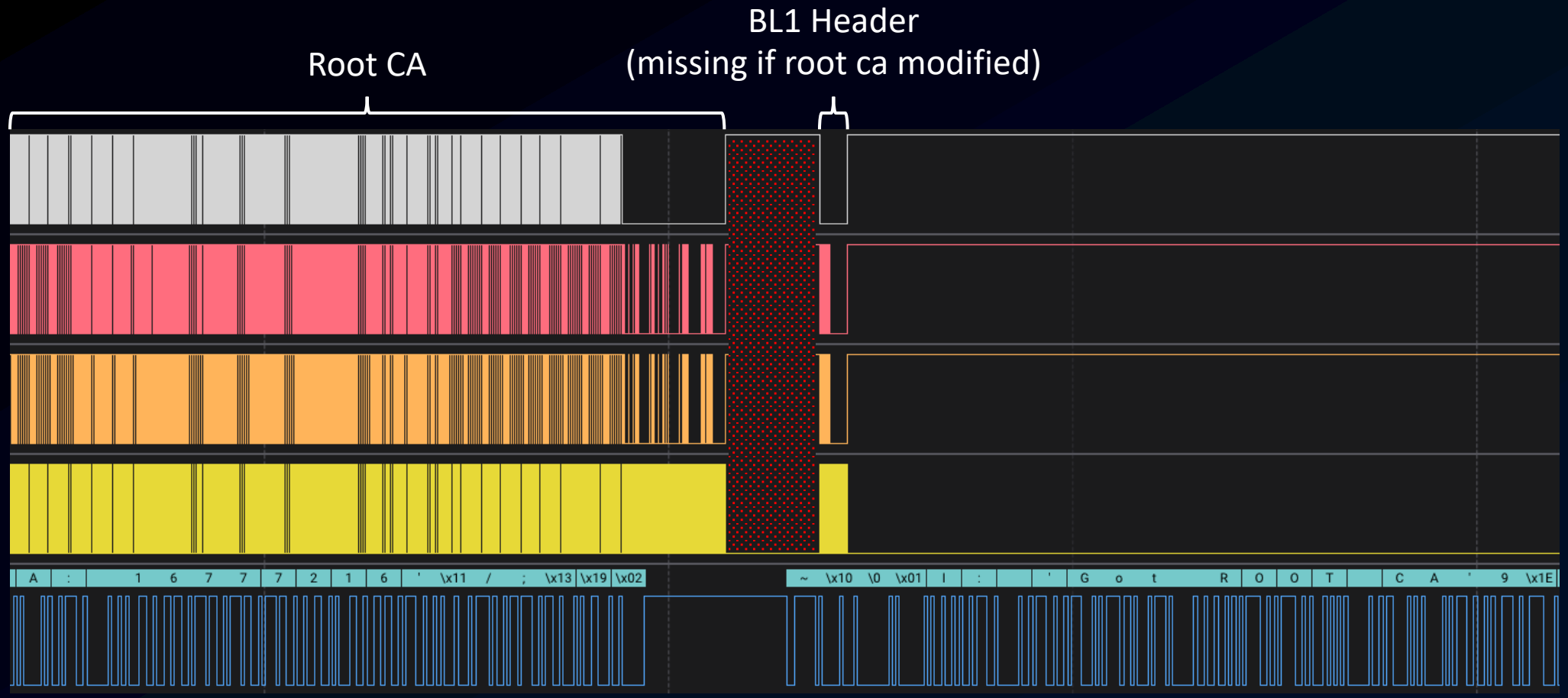
UART & SPI Boot Trace – Unmodified Root CA



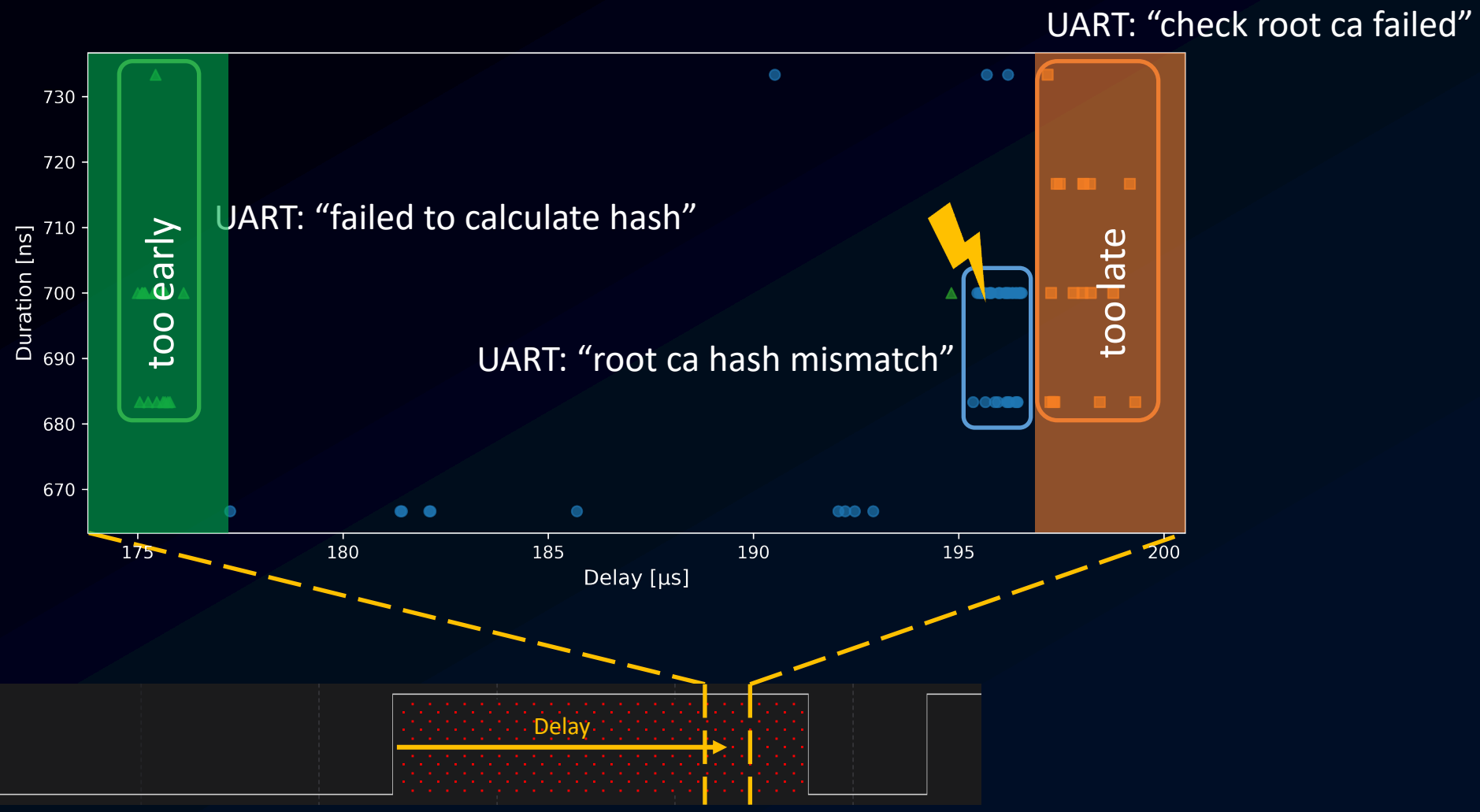
UART & SPI Boot Trace – Modified Root CA



Glitch Timing



Glitch Parameters



Integration testing is important!

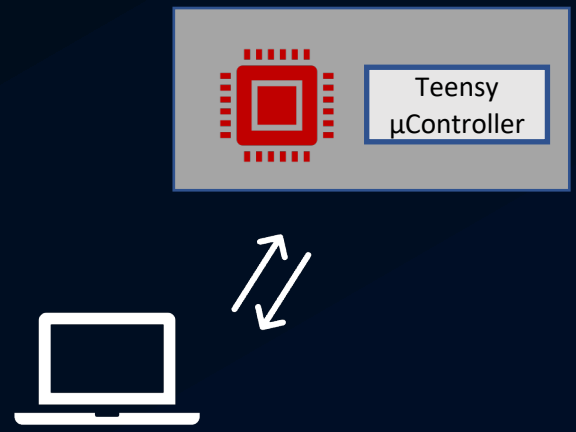
- Tried for two weeks but no success
- Testing revealed a typo in the glitch script that was already fixed in dev branch of Teensy firmware

```
def wait_for_attack(self, timeout : float = None) -> TeensyAttackResult:
    match = self.teensy.wait_match(self.__attack_re, timeout)
    cs_high = match[1] is None
    full_message = match[2]
    message = match[9]
    if match[3] == 'succeded':
        return TeensyAttackResult(True, message, cs_high)
    if match[3] == 'failed':
        return TeensyAttackResult(False, message, cs_high)
    component = match[7]
    raise TeensyAttackError(component, message, full_message)
```

Fixed spelling/minor bugs and added em_f

Open **Niclas Kühnapfel** requested to merge `dev` into `master` 10 months ago

```
117  116      prompt_use_new_line();
118  117      if (result == attack_successful) {
119  118          trigger_success_set_high();
120       -      print_str("Attack succeded");
     119  +      print_str("Attack succeeded");
121  120          trigger_success_set_low();
122  121      } else if (result == attack_failed)
123  122          trigger_fail_set_high();
```

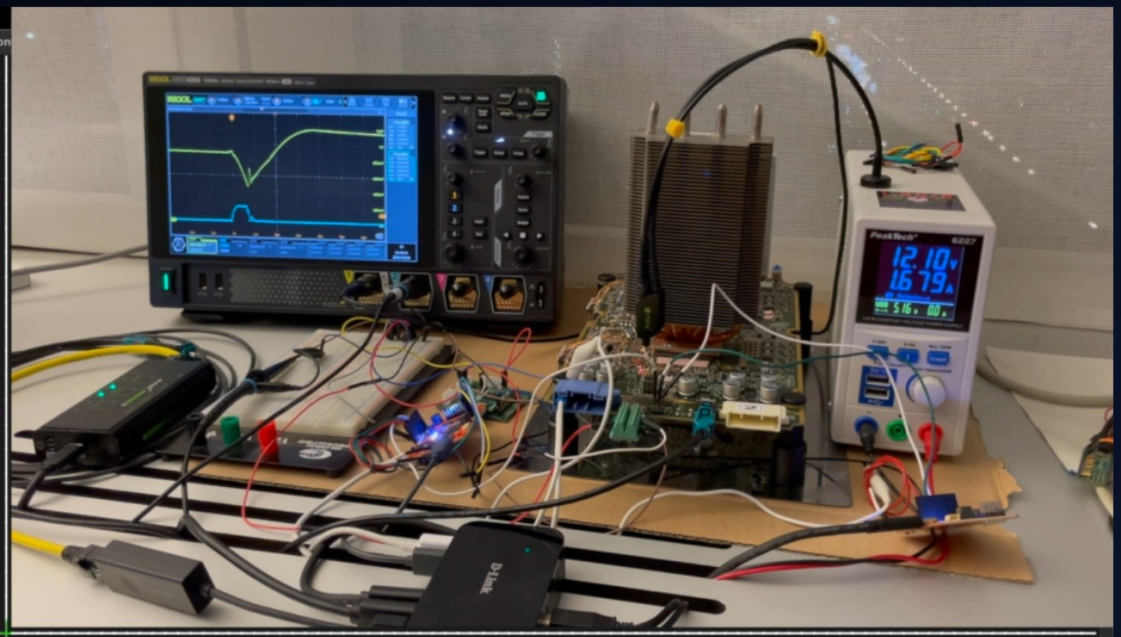


Terminal Shell Edit View Window Help

niclas — station@psp-station: ~ — ssh station

```
2023-12-19 18:32:10 [debug    ] write                          baudrate=115200 class_=TeensyCli
 data=b'atx_reset attack\r\n' timeout=20.1 tty=/dev/ttyTEENSYTESLA
2023-12-19 18:32:10 [debug    ] read_until                     baudrate=115200 class_=TeensyCli
 data=b'atx_reset attack\r\n' expected=b'atx_reset attack\r\n' timeout=20.1 tty=/dev/ttyTEENSYT
ESLA
2023-12-19 18:32:10 [debug    ] read_until                     baudrate=115200 class_=TeensyCli
 data=b'Releasing target from reset!\r\nAttack triggered!\r\nEM pulses triggered!\r\nAttack suc
ceeded!\r\n\r\x1b[K> ' expected=b'\r\x1b[K> ' timeout=20.1 tty=/dev/ttyTEENSYTESLA
2023-12-19 18:32:10 [debug    ] wait_for_prompt                baudrate=115200 class_=TeensyCli
 result=Releasing target from reset!
Attack triggered!
EM pulses triggered!
Attack succeeded! timeout=20.1 tty=/dev/ttyTEENSYTESLA
2023-12-19 18:32:10 [info     ] wait_match                     baudrate=115200 class_=TeensyCli
 expected=re.compile('Releasing target from reset!\\r\\nAttack triggered!\\r\\nEM pulses trigge
red!\\r\\n(Warning: CS was low at glitch time!\\r\\n)?(Attack ((succeeded)|(failed)|(error!\\r\
\nError during ([^:]+)))(: (.*)) message=Releasing target from reset!
Attack triggered!
EM pulses triggered!
Attack succeeded! result=<re.Match object; span=(0, 88), match='Releasing target from reset!\r\
nAttack triggered!> timeout=20.1 tty=/dev/ttyTEENSYTESLA
EXCEPTION: Attack succeeded!
```

Glitch script



```
station@psp-station:~$ ssh root@192.168.90.103
The authenticity of host '192.168.90.103 (192.168.90.103)' can't be established.
ED25519 key fingerprint is SHA256:CAng93Ae0sSjdrnoghoDKI4bxpNc5bNThlTFpelvJik.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.90.103' (ED25519) to the list of known hosts.
# uname -a
Linux ap 4.14.93-rt53-g3973ebb773 #1 SMP PREEMPT RT Fri May 19 21:16:36 2023 -0700 aarch64 GNU/
Linux
# whoami
root
# ls /
autopilot       factory         linuxrc         opt             sys
bin             home            map             proc            tmp
deploy          init            media           root            usr
dev             lib             mnt             run             var
etc             lib64           newusr          sbin            x_init_ufs.txt
#
```

SSH

```
Disk /dev/sda: 29.25 GiB, 31402754048 bytes, 7666688 sectors
Disk model: KLUBG4G1ZF-B0CQ
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 4096 bytes
I/O size (minimum/optimal): 524288 bytes / 65536 bytes
Disklabel type: gpt
Disk identifier: 66DD5AB2-538F-3E4F-8432-616DDA780852

Device       Start     End Sectors  Size Type
/dev/sda1      512    1023     512    2M Microsoft basic data
/dev/sda2     1024   17919   16896   66M Microsoft basic data
/dev/sda3    17920   34815   16896   66M Microsoft basic data
/dev/sda4    34816  296959  262144    1G Microsoft basic data
/dev/sda5   296960  559103  262144    1G Microsoft basic data
/dev/sda6   559104 6355199 5796096 22.1G Microsoft basic data
16+0 records in
16+0 records out
16+0 records in
16+0 records out
16+0 records in
16+0 records out
Sending AP_STATUS_OK ...
Starting gadget-updater ...

Please press Enter to activate this console.
```

Boot log

```
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB2
```

```
[hw3_ap_gl0:ssh* 1:bash-Z                                                    "psp-station" 18:32 19-Dez-23
```

Success Rate

- Measured only on one SoC

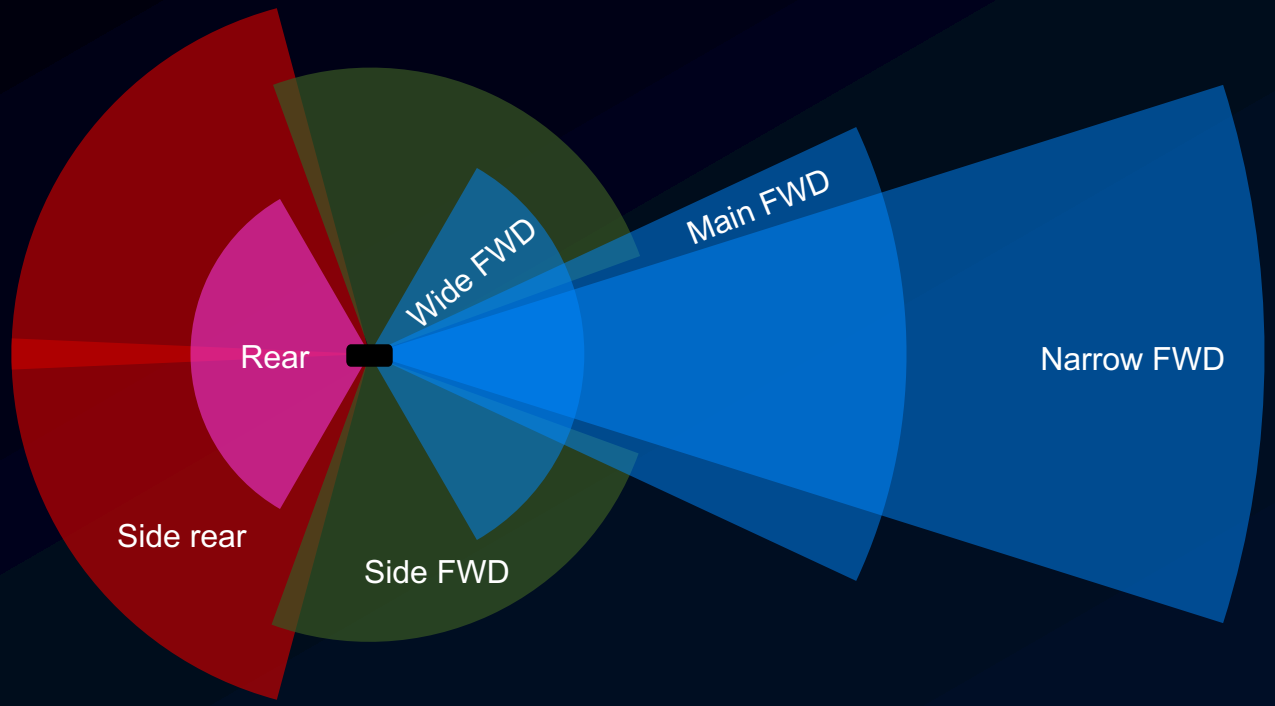
- Attempts: 11203
- Successes: 379
- False positives: 0
- Success rate: 29,56 attempts/success
- Glitch rate: 16,67 attempts/s

successful glitch every 2s!

1. Motivation & Background
2. Hardware Analysis & Attack
3. Autopilot Internals & Data Extraction

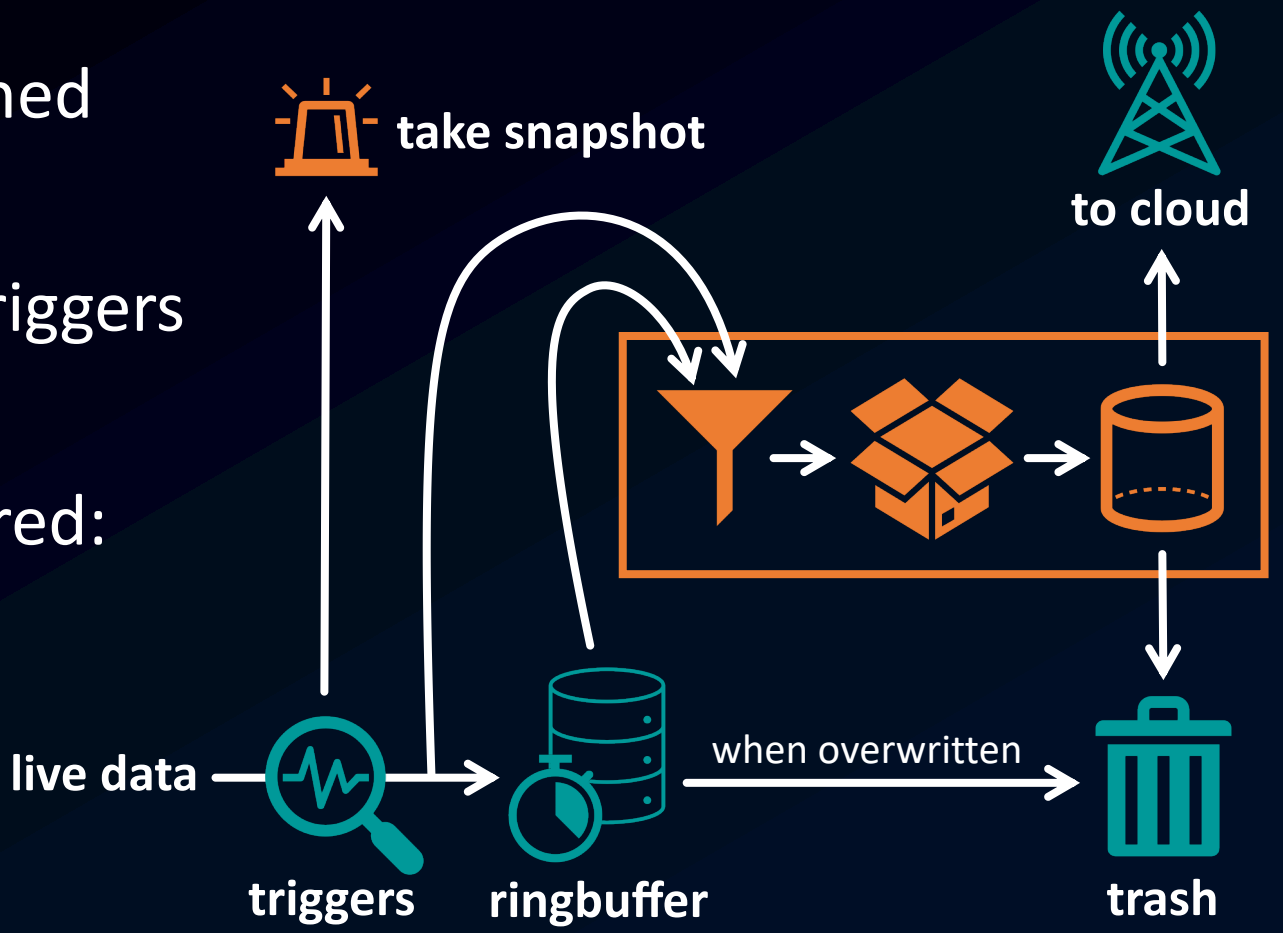
The Autopilot Dataflow

- There is lots of data
  - 8 Cameras, CAN, ML output, …
  - Good for AP training
  - Good for AP evaluation
- Small storage capacity
- Limited upload capabilties
- Solution: Upload only interesting data ‘Snapshots’

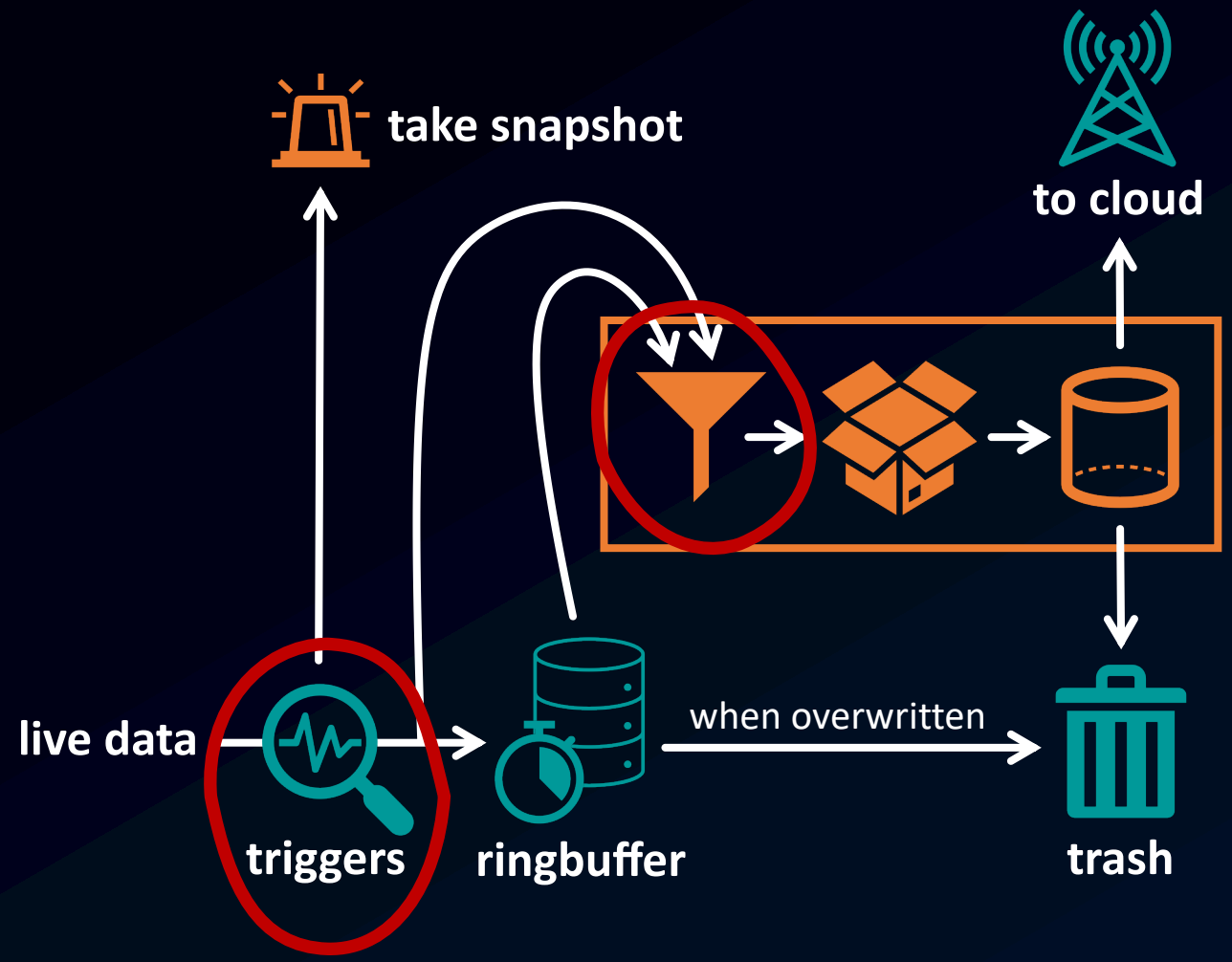


Snapshots Overview

- Live data temporarily cached
  - Fixed size ringbuffers
- Live data monitored for Triggers
  - E.g. did airbag deploy?
- Once a Snapshot is triggered:
  - Collect live & old data
  - Filter, package & store
  - Upload & delete



Snapshots


take snapshot
to cloud
live data
when overwritten
triggers
ringbuffer
trash

/home/telemetry/triggers/triggers.sqlite

active	trigger name	trigger json
Filter	Filter	Filter
1	aeb-vehicle	{"query":{"$and":[{"$eq":...
1	aeb-vru	{"query":{"$and":[{"$or":[{"$eq":...
1	generic-trip	{"query":{"$nop":false},"streams...
1	img-vid-aeb-fsd	{"query":{"$and":...
1	img-vid-ltap-aeb	{"query":{"$and":...
1	img-vid-rev-vru-aeb	{"query":{"$and":...
1	img-vid-shadow-extended-limits	{"query":{"$and":...
1	img-vid-tacc-extended-limits	{"query":{"$and":...
1	img-vid-user-request	{"query":...
1	ping-aeb	{"query":{"$eq":[{"h":...
1	ping-aeb-fsd	{"query":{"$and":...
1	ping-aeb-max-speed-reduction-override	{"query":"@ActiveSafetyOutput.lc...
1	ping-ap-pedal-int-40	{"query":{"$and":[{"$eq":...
1	ping-bcw	{"query":{"$or":...
1	ping-bsa	{"query":{"$eq":[{"h":...
1	ping-caut-light-slowdown	{"query":{"$and":...
1	ping-elk	{"query":{"$and":[{"$or":[{"$eq":...
1	ping-failsafe-ab	{"query":{"$eq":[{"h":...
1	ping-fcw	{"query":{"$eq":[{"$enum-...
1	ping-harsh-brake-inv	{"query":{"$and":[{"$eq":...

Automatic Emergency Breaking

log metadata of all trips?

collect video data for learning?

just report metadata

Elchtest?

- Holds Triggers + Metadata
  - When trigger was created
  - How often was it triggered
  - ...
- Custom JSON format:
  - Query for trigger events
  - Selectors for data streams (Video/CAN/Autopilot)
  - Metadata (e.g. GPS location/car config./FSD state)

Trigger “aeb-vru”
(Automatic Emergency Breaking – Vulnerable Road User)

hnj@piepmatz: ~

hnj

```
{
  "query": {
```

TRIGGER IF:

@ActiveSafetyOutput.[...].**threat**.input_data.**type**

IS **PEDESTRIAN** OR **BICYCLIST**

AND

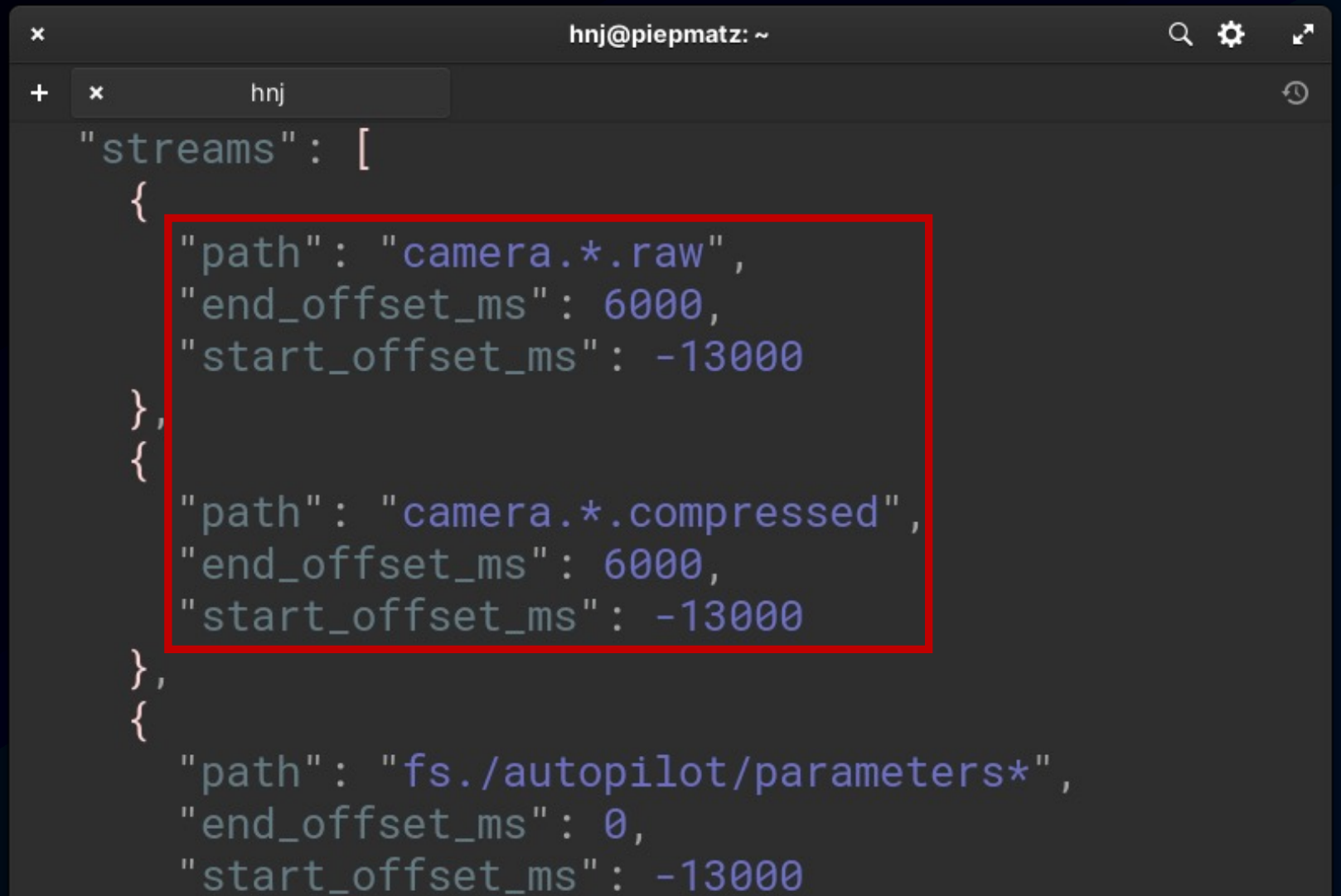
@ActiveSafetyOutput.[...].state == 8

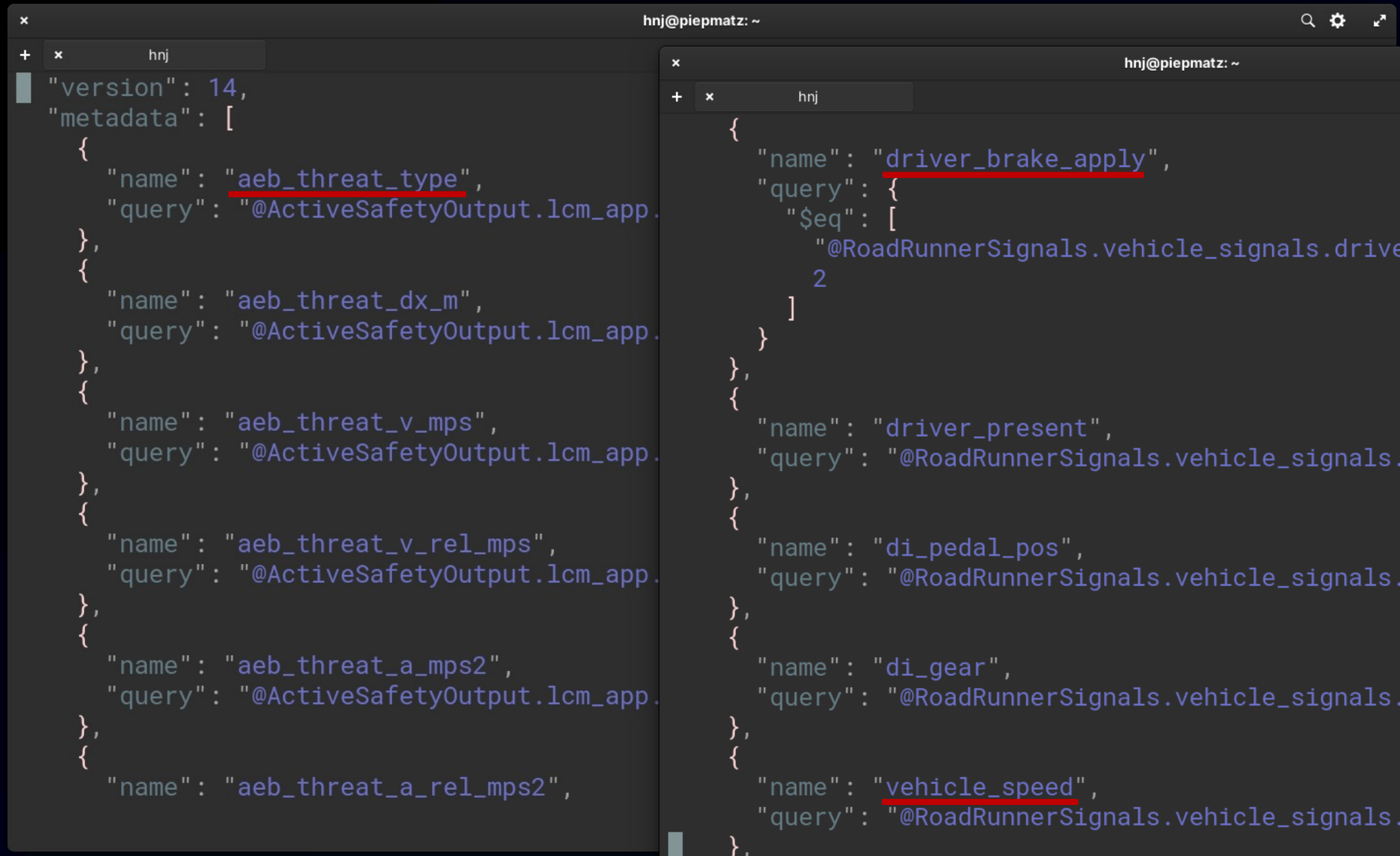
AND

@ActiveSafetyOutput.[...].aeb_event == 1

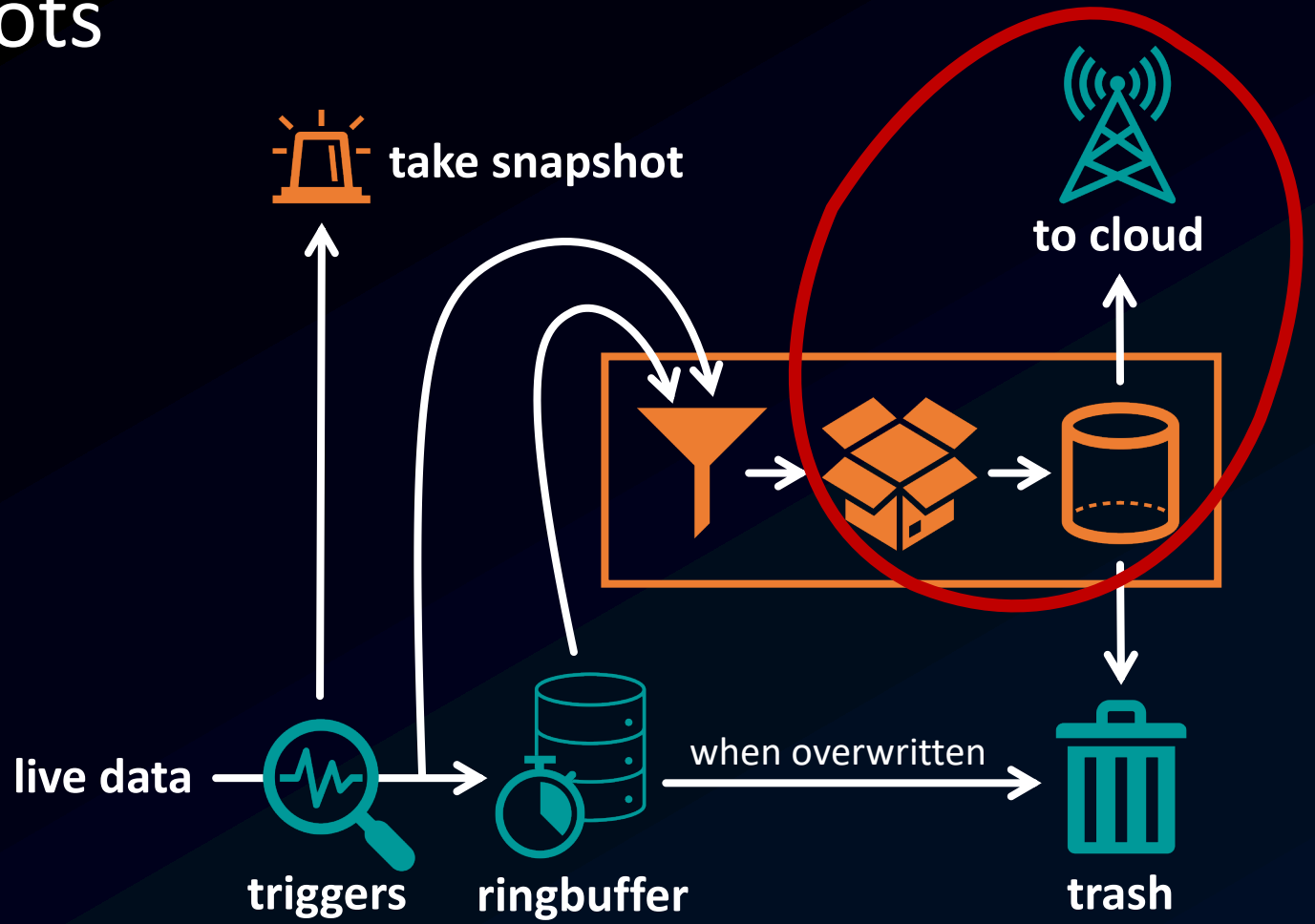
```
            },
            "BICYCLIST"
          ]
        }
```

“aeb-vru” Trigger
(Automatic Emergency Breaking – Vulnerable Road User)

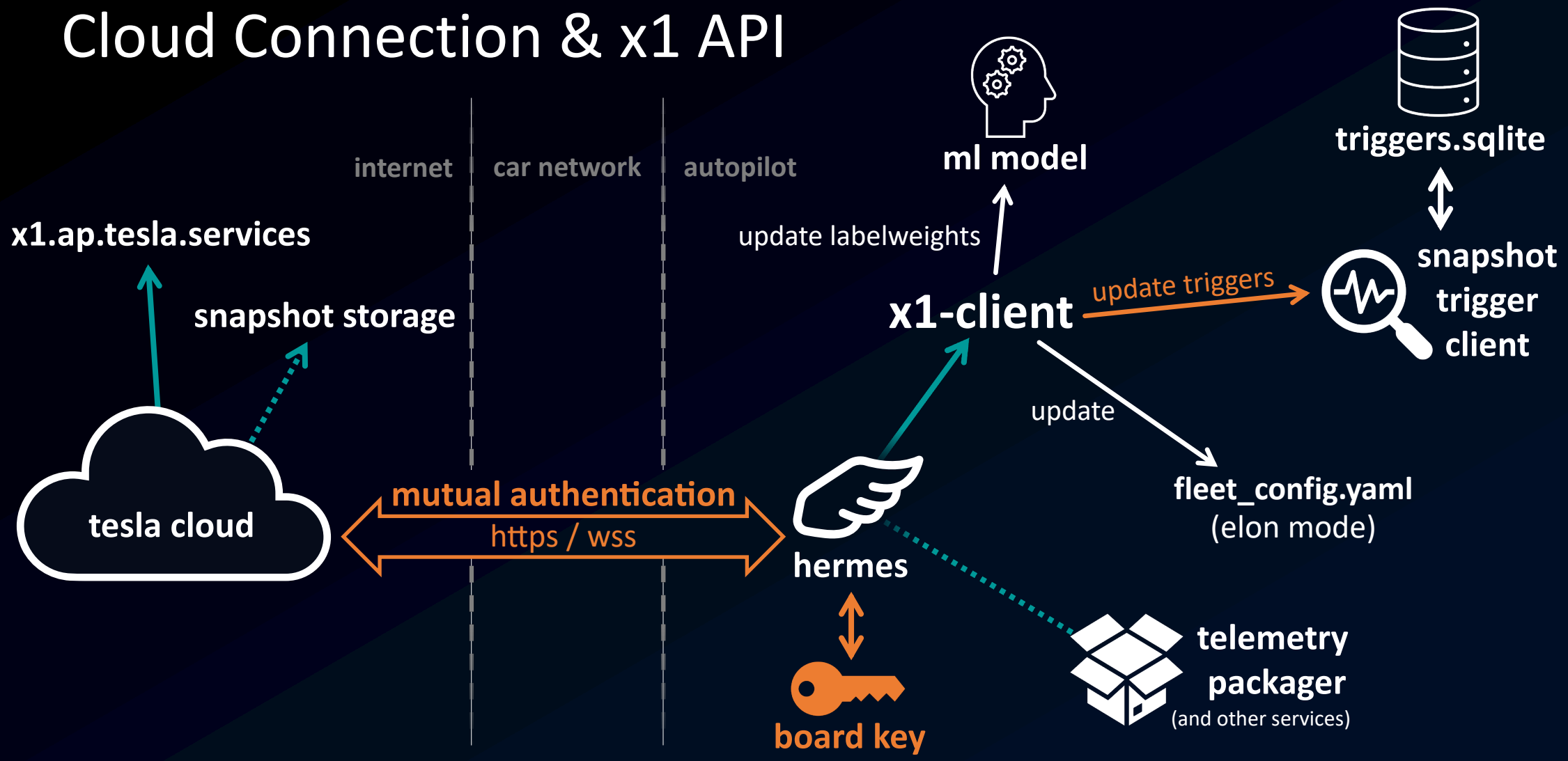



hnj@piepmatz: ~
hnj
"version": 14,
"metadata": [
{
"name": "aeb_threat_type",
"query": "@ActiveSafetyOutput.lcm_app.
},
{
"name": "aeb_threat_dx_m",
"query": "@ActiveSafetyOutput.lcm_app.
},
{
"name": "aeb_threat_v_mps",
"query": "@ActiveSafetyOutput.lcm_app.
},
{
"name": "aeb_threat_v_rel_mps",
"query": "@ActiveSafetyOutput.lcm_app.
},
{
"name": "aeb_threat_a_mps2",
"query": "@ActiveSafetyOutput.lcm_app.
},
{
"name": "aeb_threat_a_rel_mps2",
hnj@piepmatz: ~
hnj
{
"name": "driver_brake_apply",
"query": {
"$eq": [
"@RoadRunnerSignals.vehicle_signals.driver_brake_a
2
]
}
},
{
"name": "driver_present",
"query": "@RoadRunnerSignals.vehicle_signals.driver_pr
},
{
"name": "di_pedal_pos",
"query": "@RoadRunnerSignals.vehicle_signals.di_pedal_
},
{
"name": "di_gear",
"query": "@RoadRunnerSignals.vehicle_signals.di_gear"
},
{
"name": "vehicle_speed",
"query": "@RoadRunnerSignals.vehicle_signals.vehicle_s
},
45
166,1

Snapshots

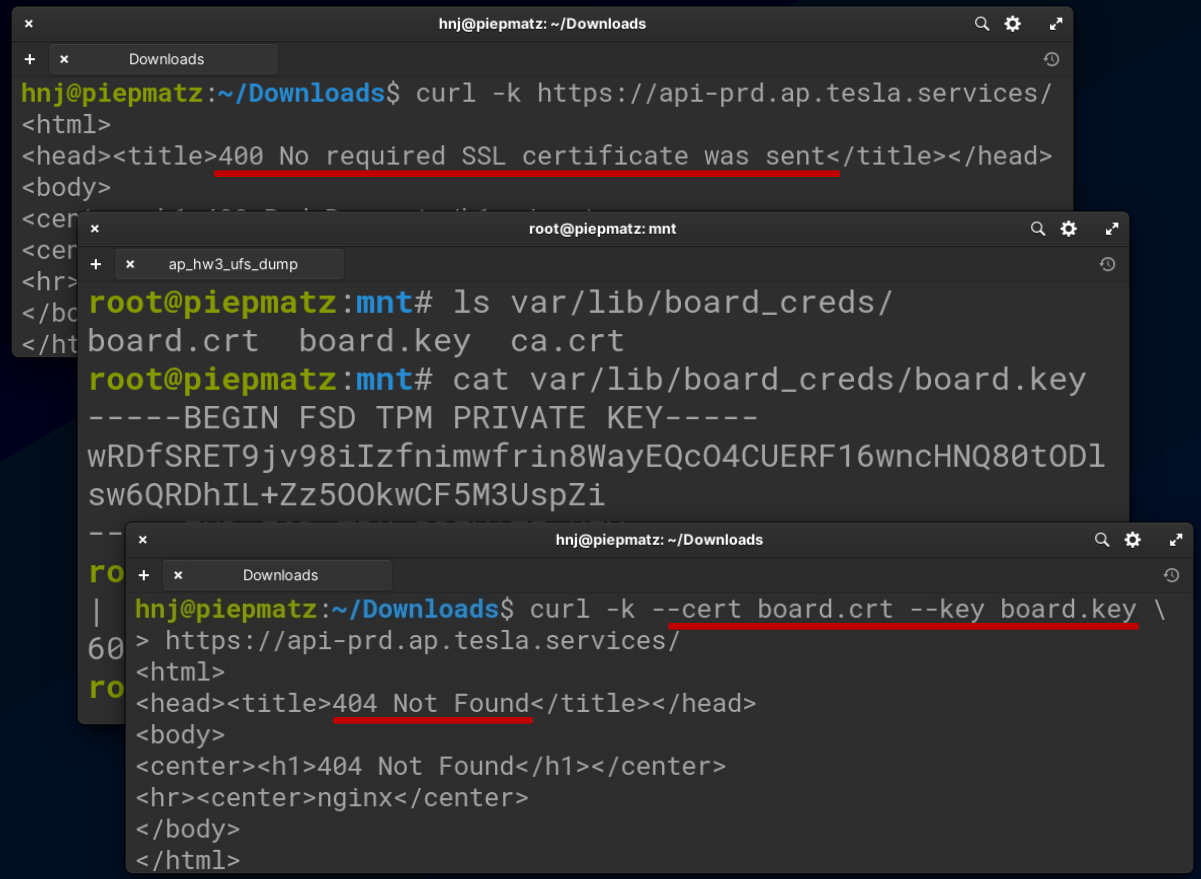

take snapshot
to cloud
live data
when overwritten
triggers
ringbuffer
trash

Cloud Connection & x1 API

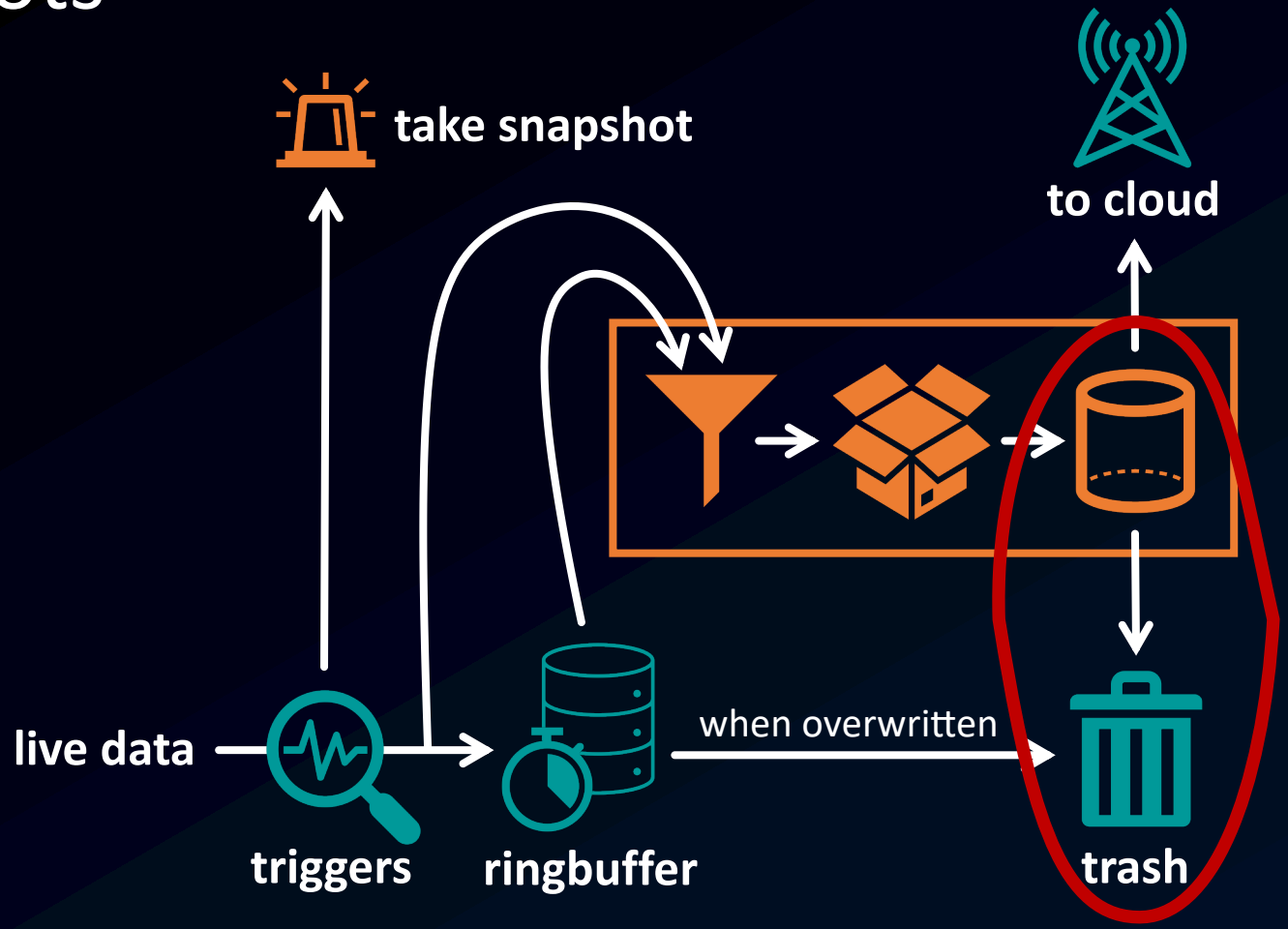


Extracting Hermes' Board Key

- Board key is encrypted
  - Tesla-signed Certificate
- Loaded into SCS for decryption
  - Similar to a TPM
- Security goals:
  - API access bound to hardware
  - Board can't be imitated or cloned
- We extracted the Key from SCS
  - API access granted!

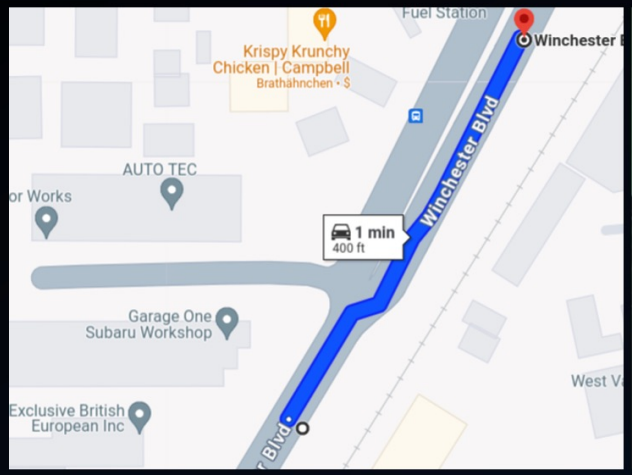


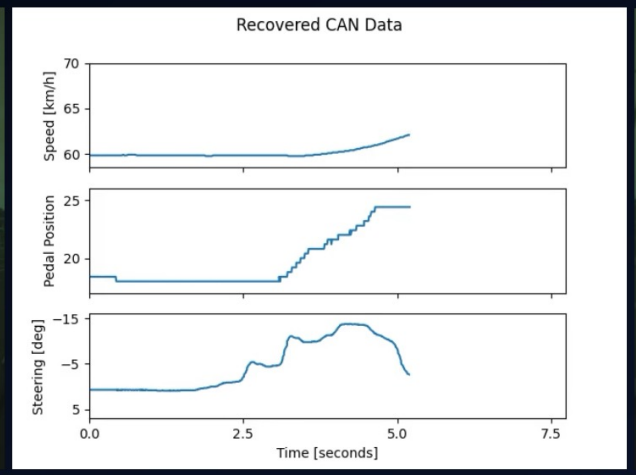
Snapshots


take snapshot
to cloud
live data
when overwritten
triggers
ringbuffer
trash

Can we find any snapshot data?

- Many snapshots on our test system ...
- ... all reporting that some camera did not initialize
- Any video snapshots where uploaded and deleted
- But: What happens when you ‘delete’ a file?
  - Its disk space is now available for other data
  - But not yet overwritten!
- We recovered a snapshot!


Fuel Station
Krispy Krunchy Chicken | Campbell
Brathähnchen · $
Winchester
Winchester Blvd
AUTO TEC
or Works
1 min
400 ft
Garage One Subaru Workshop
West V
Exclusive British European Inc
r Blvd


Recovered CAN Data
Speed [km/h]
70
65
60
Pedal Position
25
20
Steering [deg]
−15
−5
5
0.0
2.5
5.0
7.5
Time [seconds]

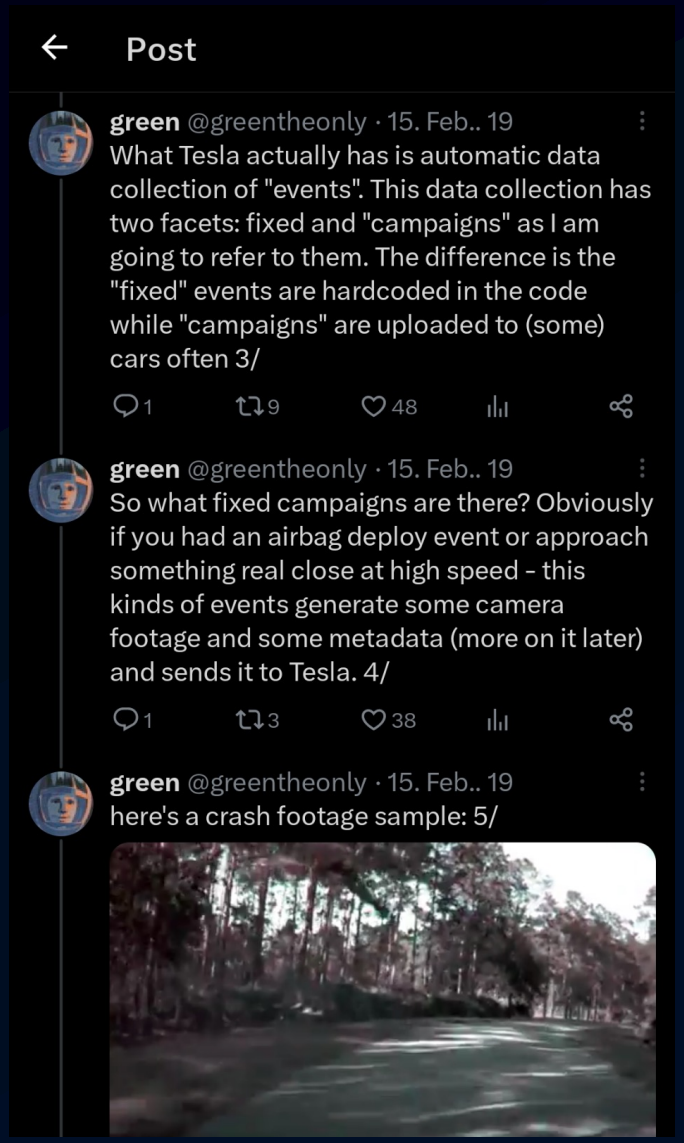
Key Takeaways

Voltage glitching is *still* a thing

1. It threatens Tesla's intellectual property (Autopilot software)
2. It enables 3rd parties to independently analyze the system
   - for data privacy violations
   - for vulnerabilities, e.g., adversarial (ML) attacks
   - for forensic investigations
3. **The window for 3rd party analysis is closing**

Thank You, Green!

- Helped us with hardware supply
- Helped whenever we had a question
- We provide an Autopilot ”Jailbreak“
- Good places for more Tesla details:
  - Twitter: @greentheonly
  - YouTube: @greentheonly
  - Tesla Motors Club: verygreen



Thank you, Segor!