Glitching AP4:

A TECHNICAL DEEP DIVE INTO TESLA'S AUTOPOILOT COMPUTER

Niclas Kühnapfel
Christian Werling
Hans Niklas Jacob

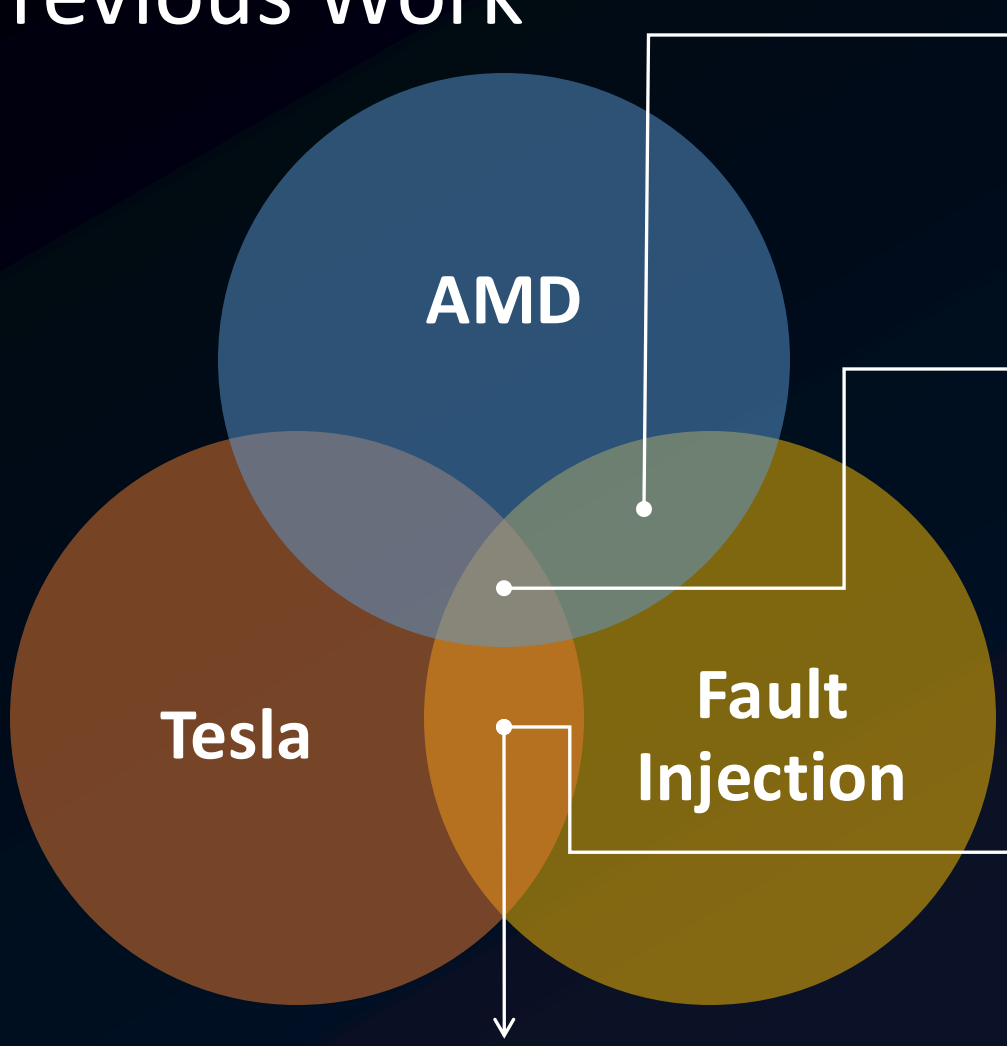
TU Berlin

Oleg Drokin

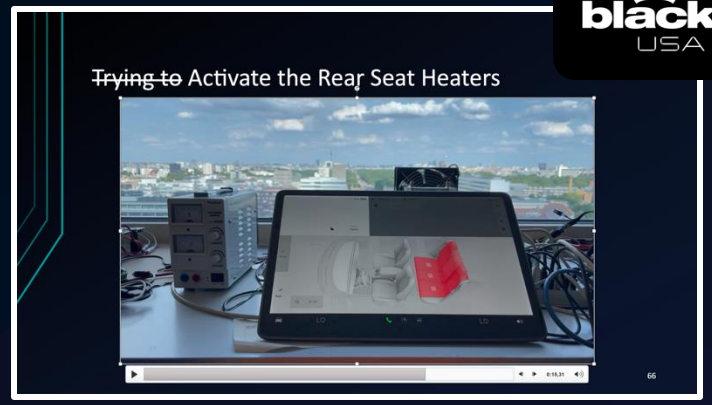
Independent

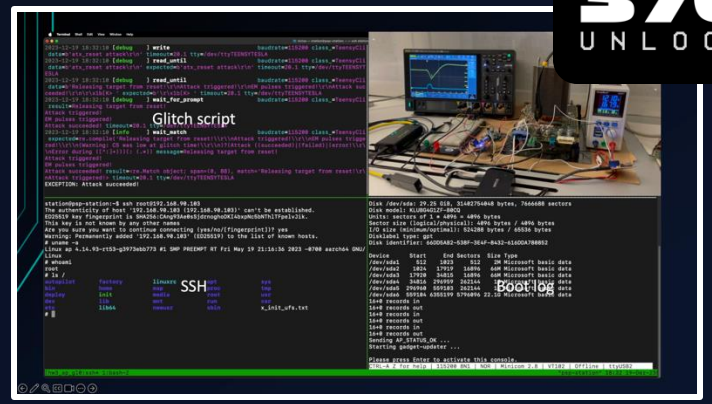
1. Motivation & Background
2. Hardware Analysis & Attack
3. Autopilot Internals

Previous Work



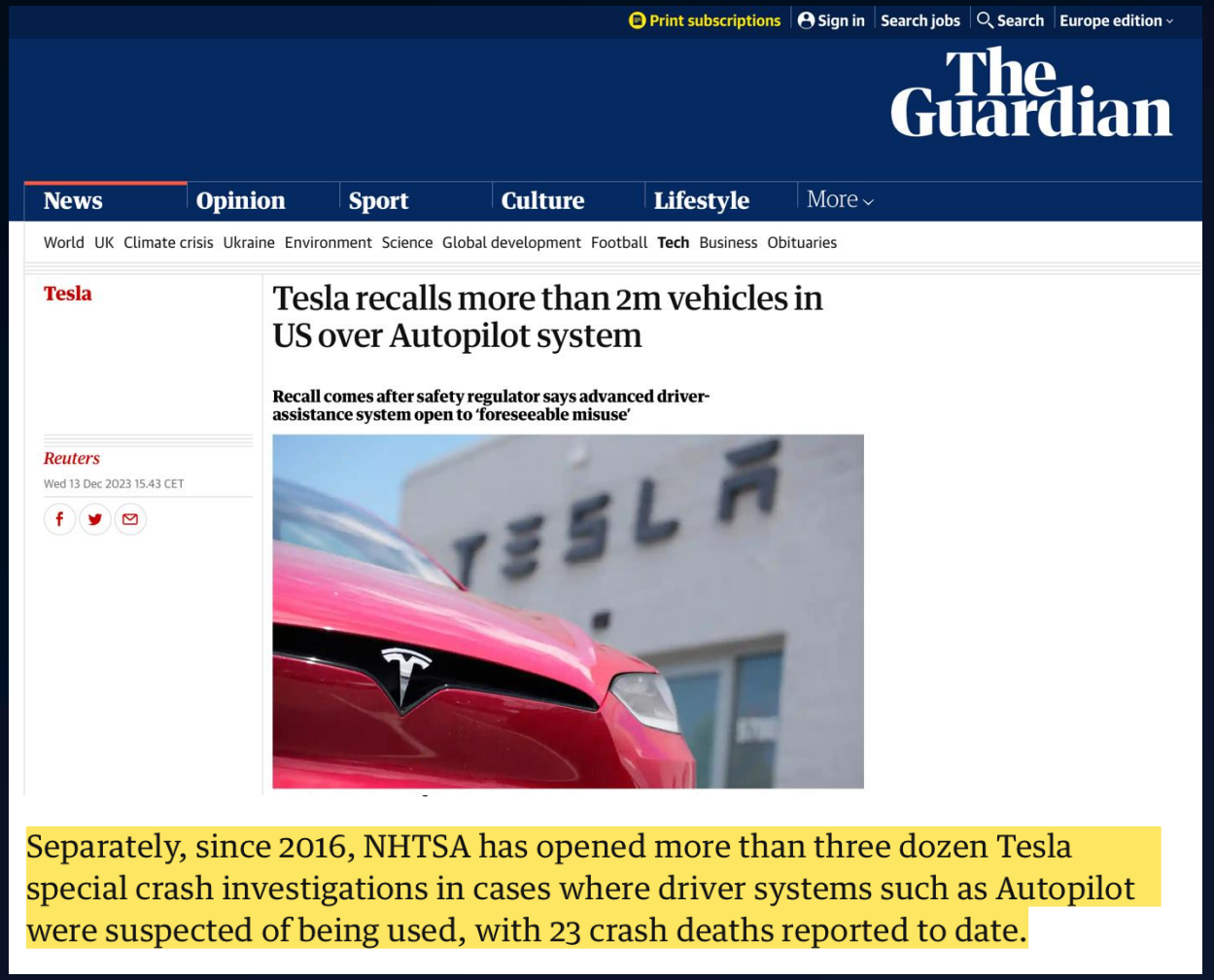
“EM-Fault It Yourself” (2022)
Building a Replicable EMFI Setup for Desktop and Server Hardware





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

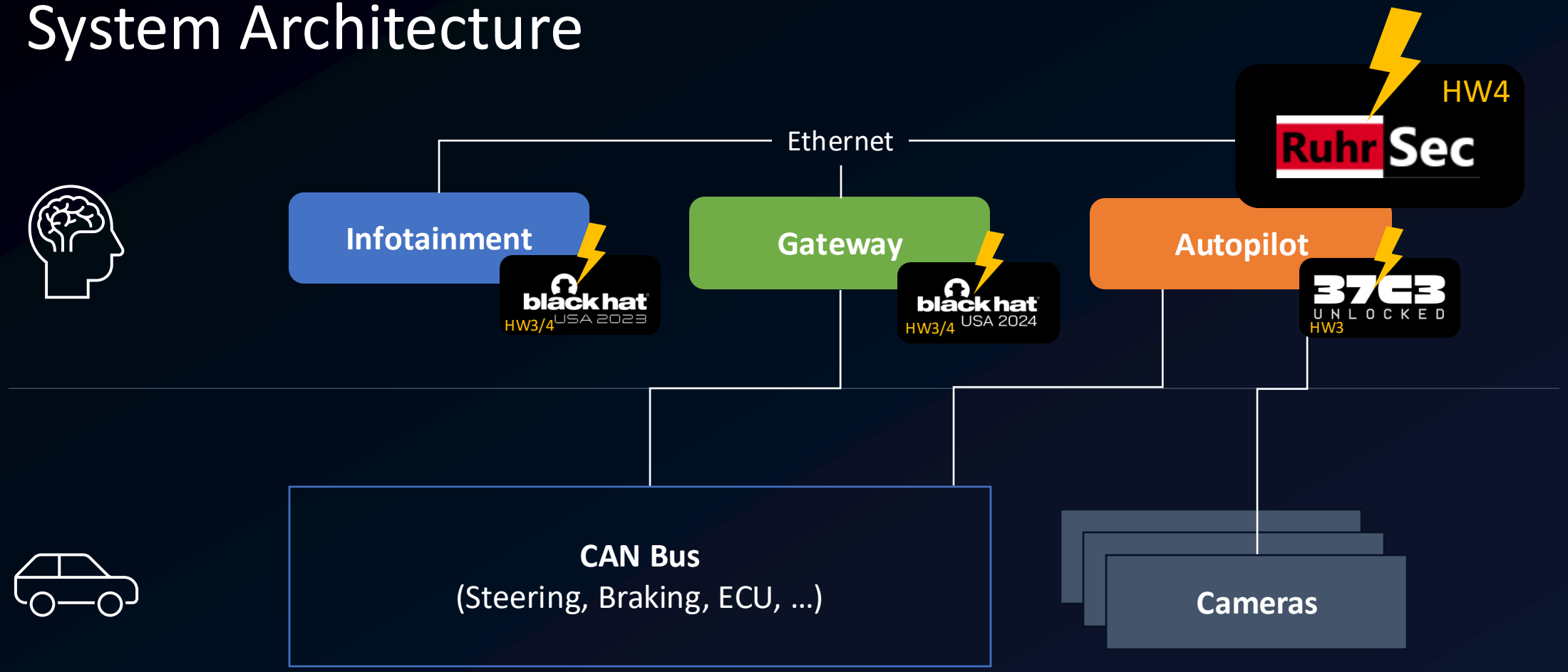
Recall comes after safety regulator says advanced driver-assistance system open to ‘foreseeable misuse’

Reuters

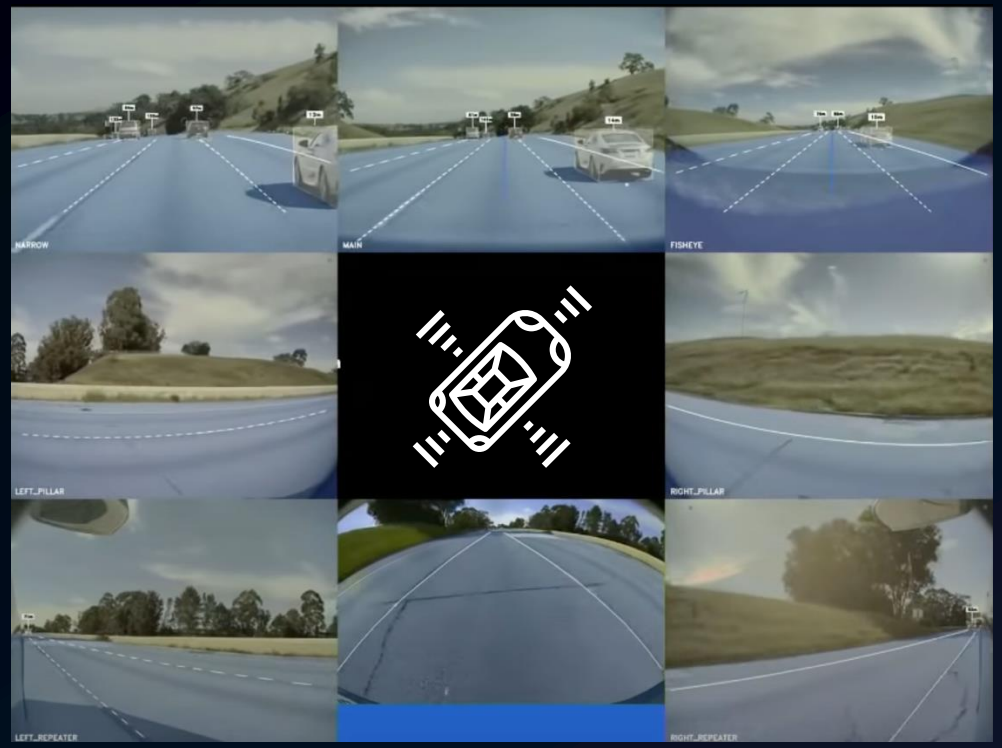
Wed 13 Dec 2023 15.43 CET

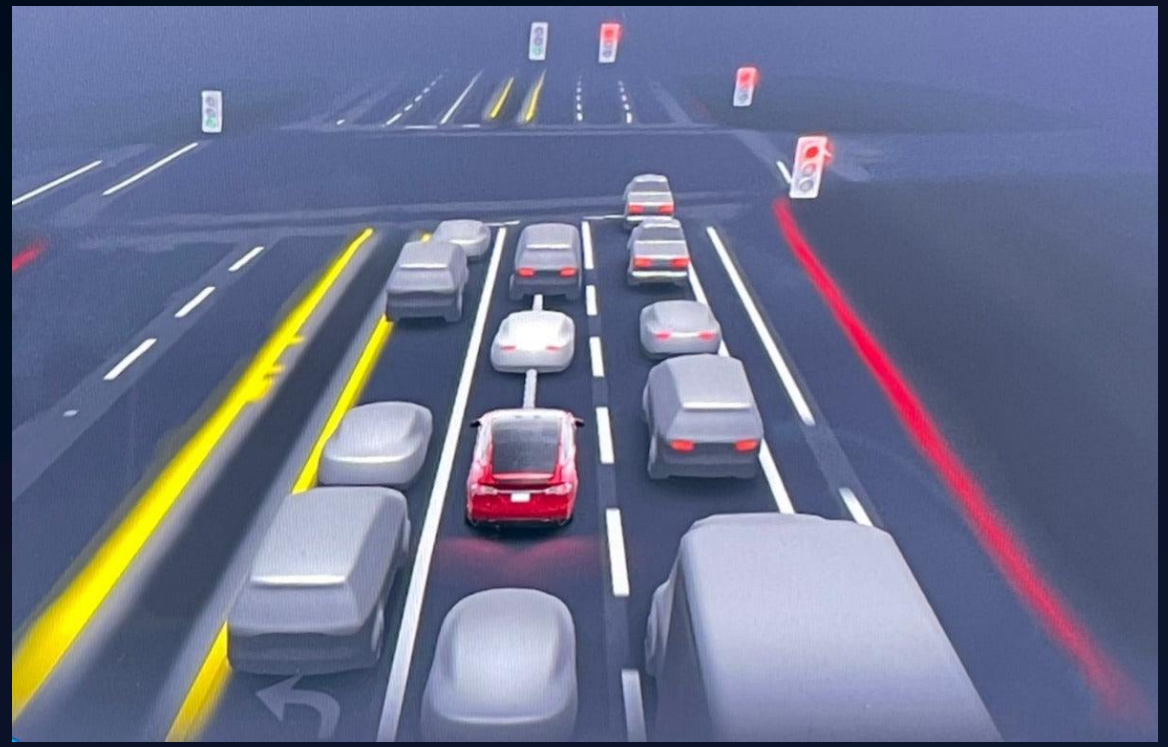
Separately, since 2016, NHTSA has opened more than three dozen Tesla special crash investigations in cases where driver systems such as Autopilot were suspected of being used, with 23 crash deaths reported to date.

System Architecture



Autopilot





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

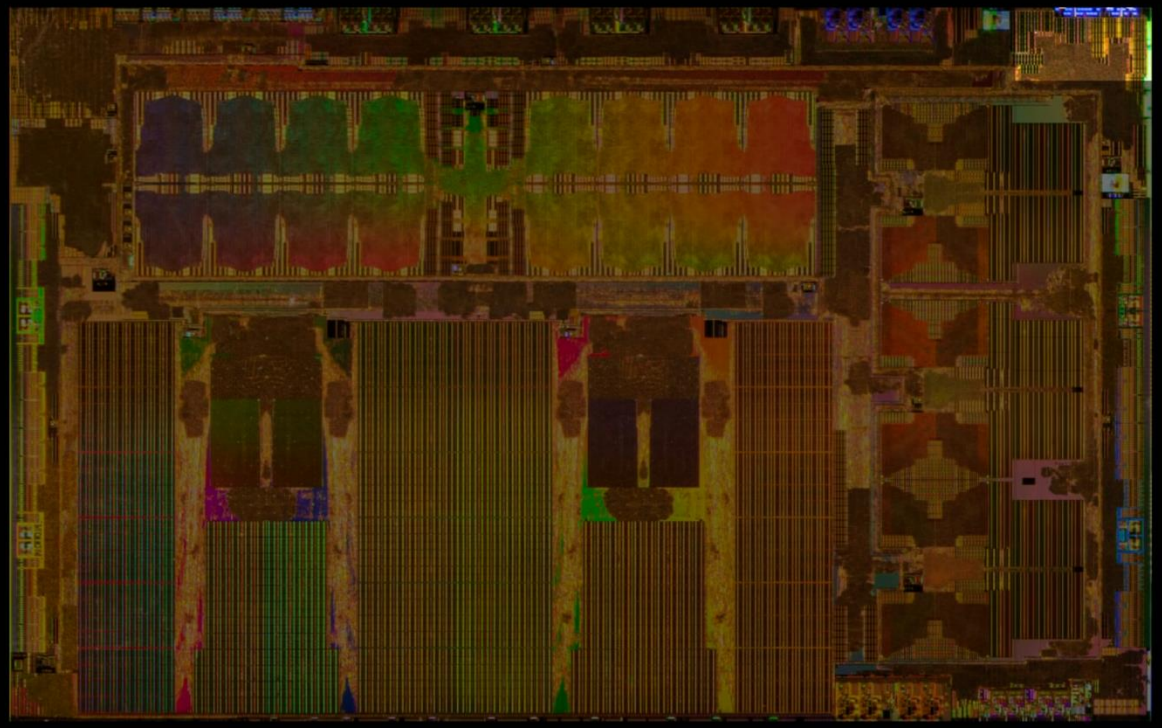
AI Addict/YouTube

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**	

Motivation

SECURITY SYSTEM



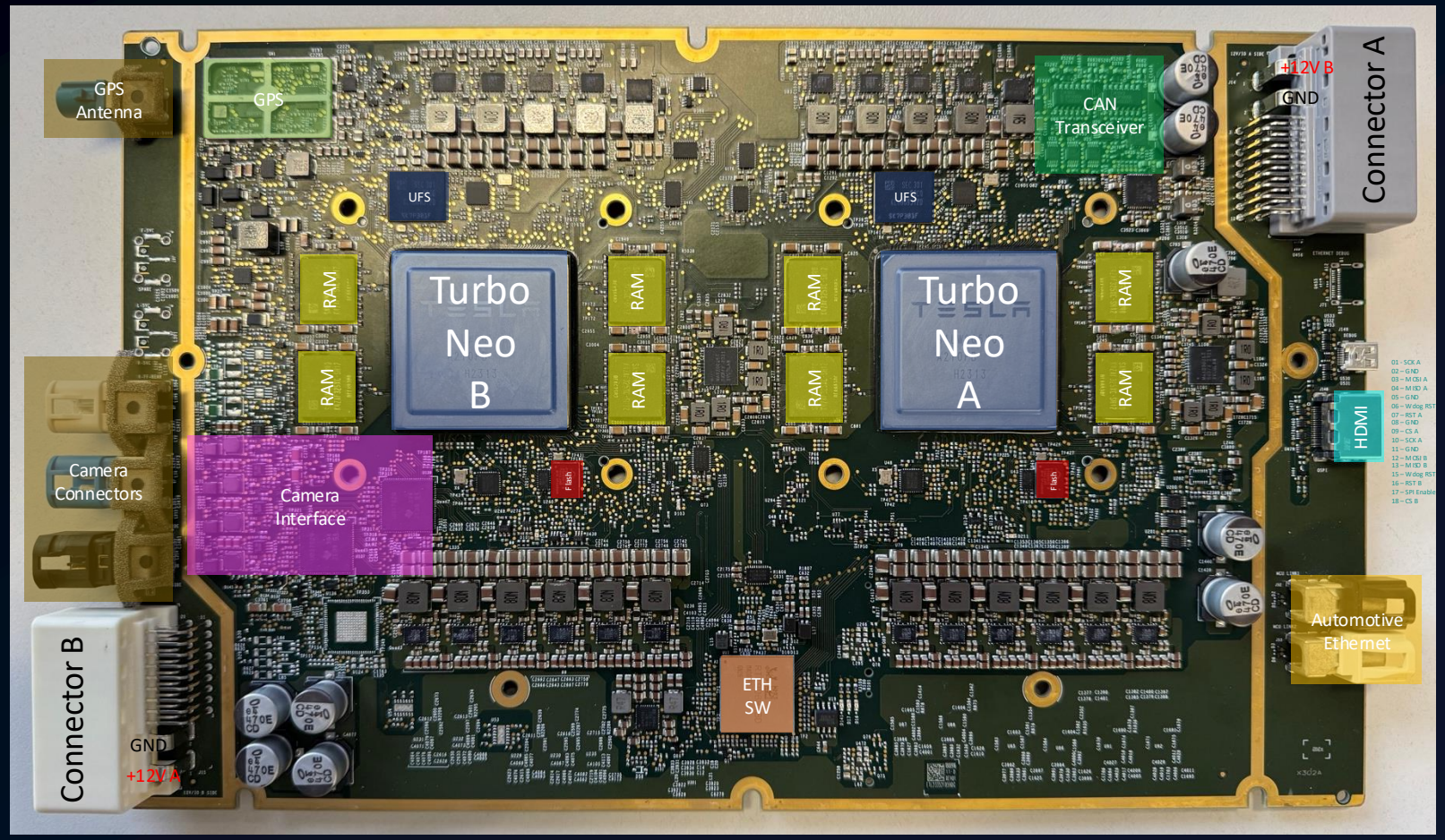
Ensure the system only runs code cryptographically signed by Tesla

TESLA LIVE

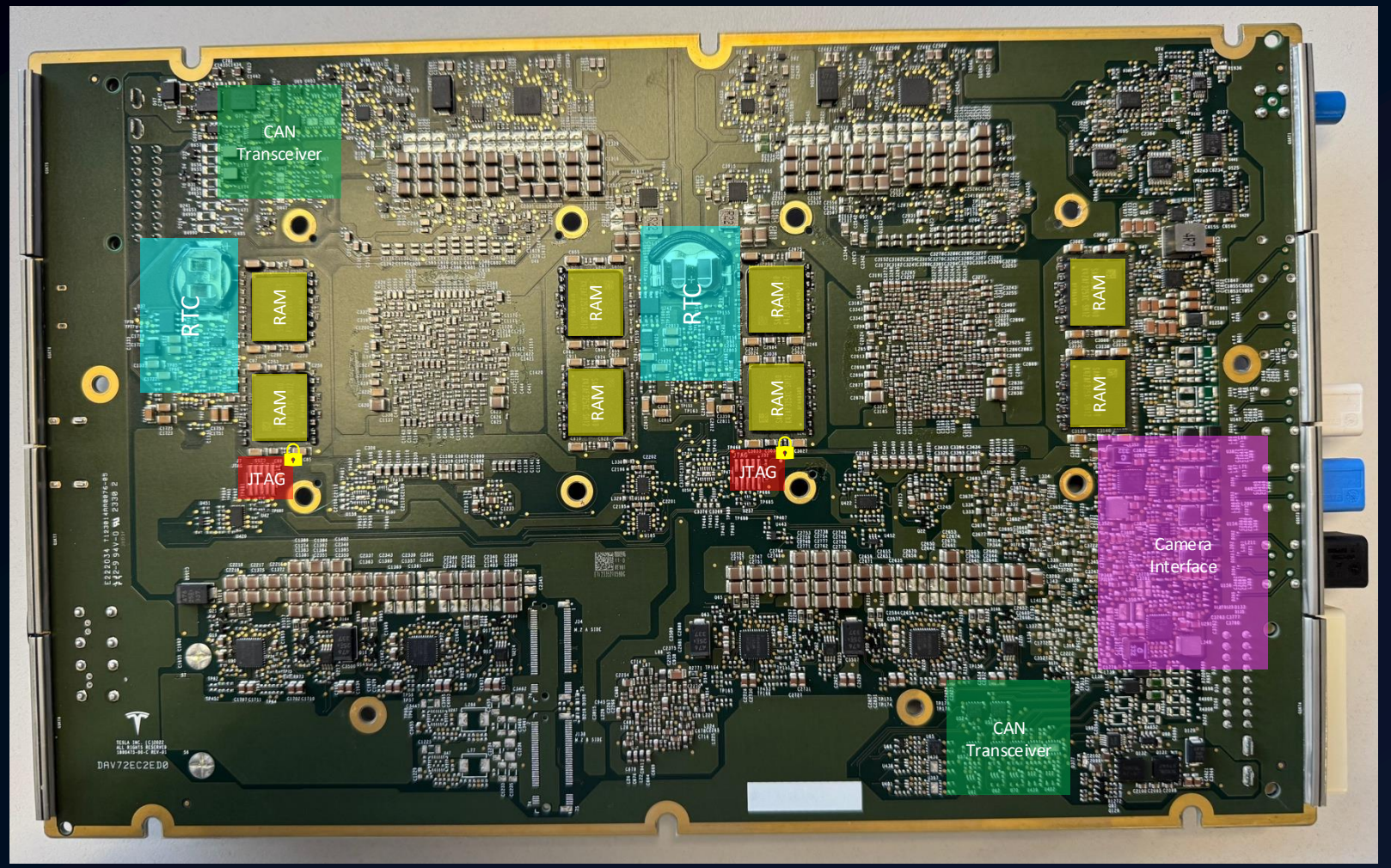
”Tesla Autonomy Day”, April 2019 (YouTube)

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

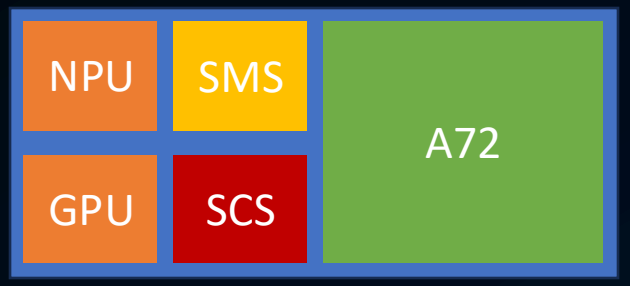
Tesla Autopilot Hardware 4 - Frontside



Tesla Autopilot Hardware 4 - Backside

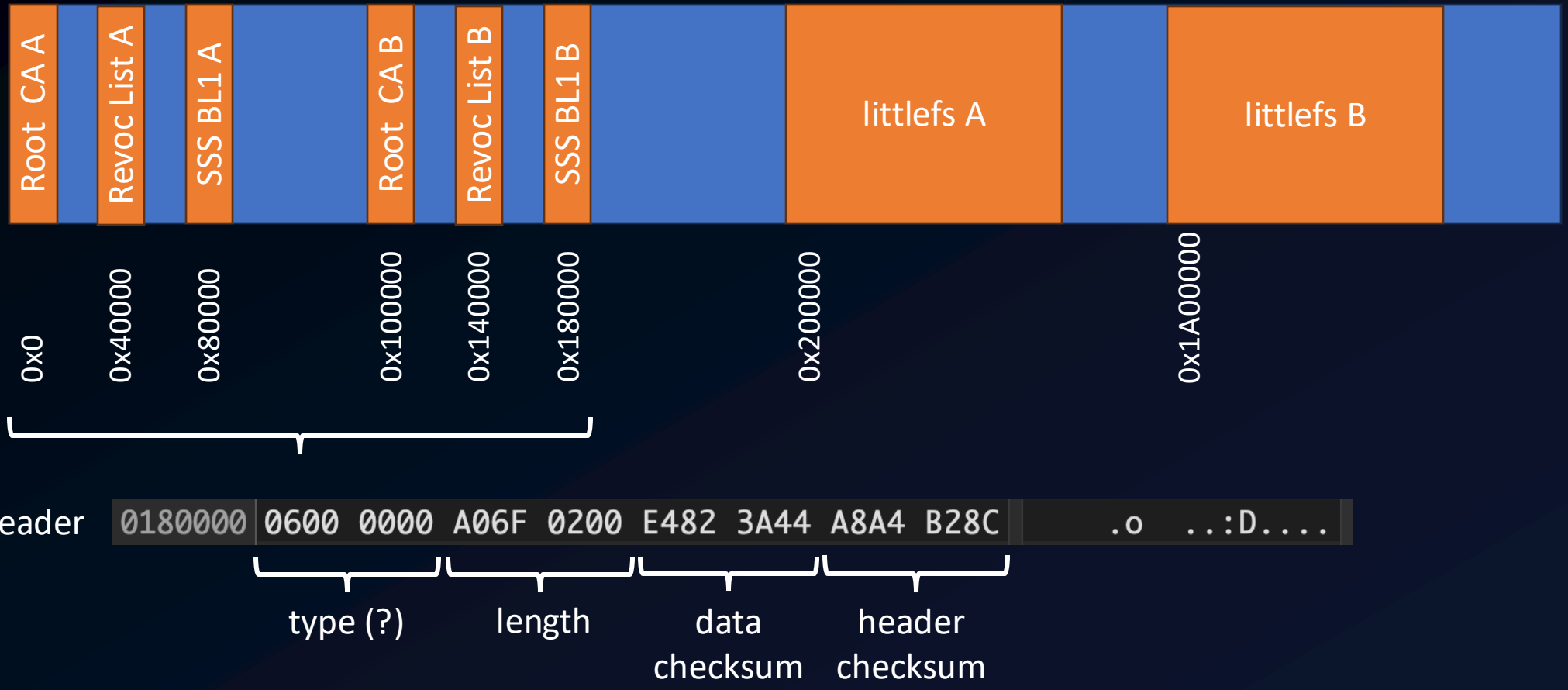


“Turbo Neo” Architecture



Turbo - HW3	Turbo Neo - HW4
Based on Samsung Exynos	Based on Samsung Exynos
3x Quad-Core ARM Cortex A72 @2.2GHz	5x Quad-Core ARM Cortex-A75 @2.35GHz
1x 16-core Mali G71	2x 8-core Mali G76
NPU (TRIP) Dual-Core @2GHz	NPU (TRIP) Triple-Core @2.2GHz
8GB LPDDR4 RAM	16GB GDDR6 RAM
Samsung UFS2.1 32GB	Samsung UFS2.1 64GB
72 TOPS	>216 TOPS

Firmware Structure on SPI Flash (Tesla Boot File System (?) – TBFS)



littlefs
A little fail-safe filesystem designed for microcontrollers.

ap-bl1.sbin
ap-coreboot.sbin
ap-dtb.sbin
ap-kernel.sbin
ap-initrd.sbin

sss-bl2.sbin
sgk-bl1.sbin
veh-bl1.sbin

toc-file.sbin
gps-bl.sbin
gps-fw.sbin
eth-switch-fw.sbin

ToC = Table of Contents

includes file hashes!

littlefs v2.4.1 (current: v2.10.1)
littlefs-python 0.4.0

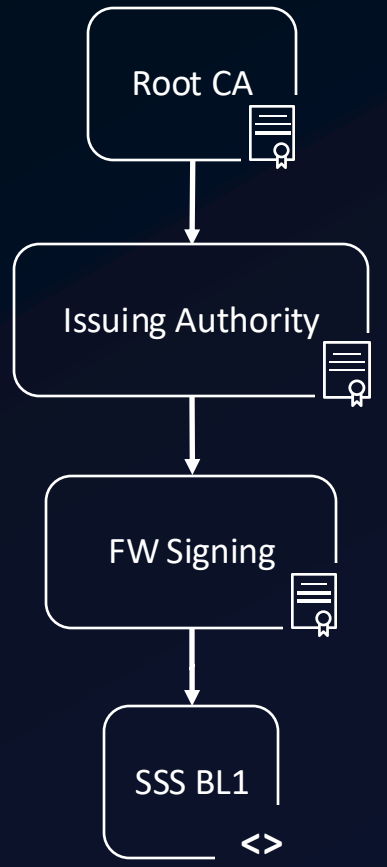
block size	= 0x40000
name max	= 0xFF
file max	= 0x7FFFFFFF
attr max	= 0x3FE

Signatures

```
01801C0 0048 5734 2052 6F6F 7420 4341 0000 0000  HW4 Root CA
```

```
01804F0 0048 5734 2050 726F 6475 6374 696F 6E20  HW4 Production
0180500 4973 7375 696E 6720 4175 7468 6F72 6974 Issuing Authorit
0180510 7900 0000 0000 0000 0000 0000 0000 0000 y
```

```
0180FF0 0048 5734 2050 726F 6475 6374 696F 6E20  HW4 Production
0181000 5353 5320 424C 3120 4669 726D 7761 7265 SSS BL1 Firmware
0181010 2053 6967 6E69 6E67 0000 0000 0000 0000  Signing
```



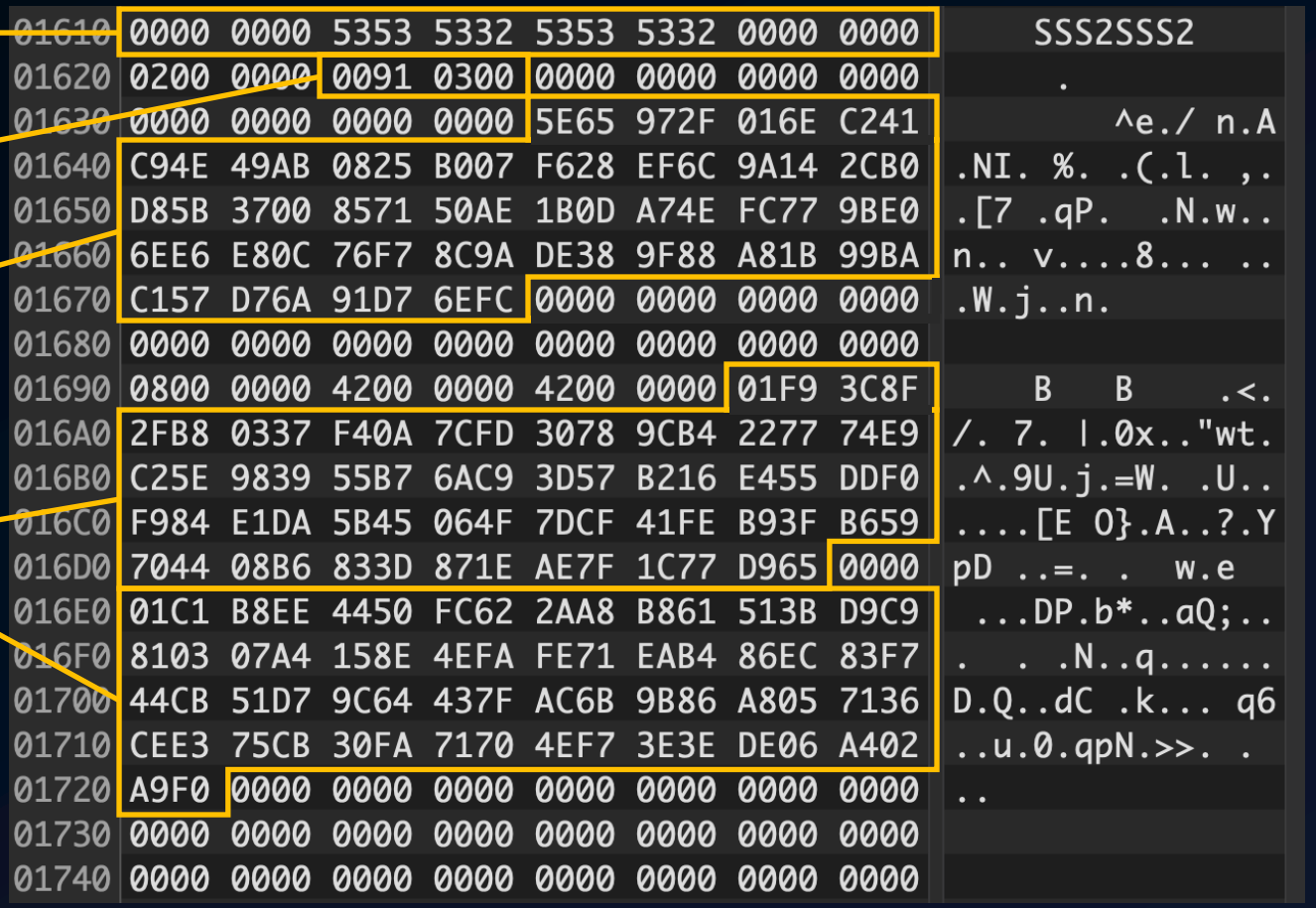
File Structure

Magic

Length

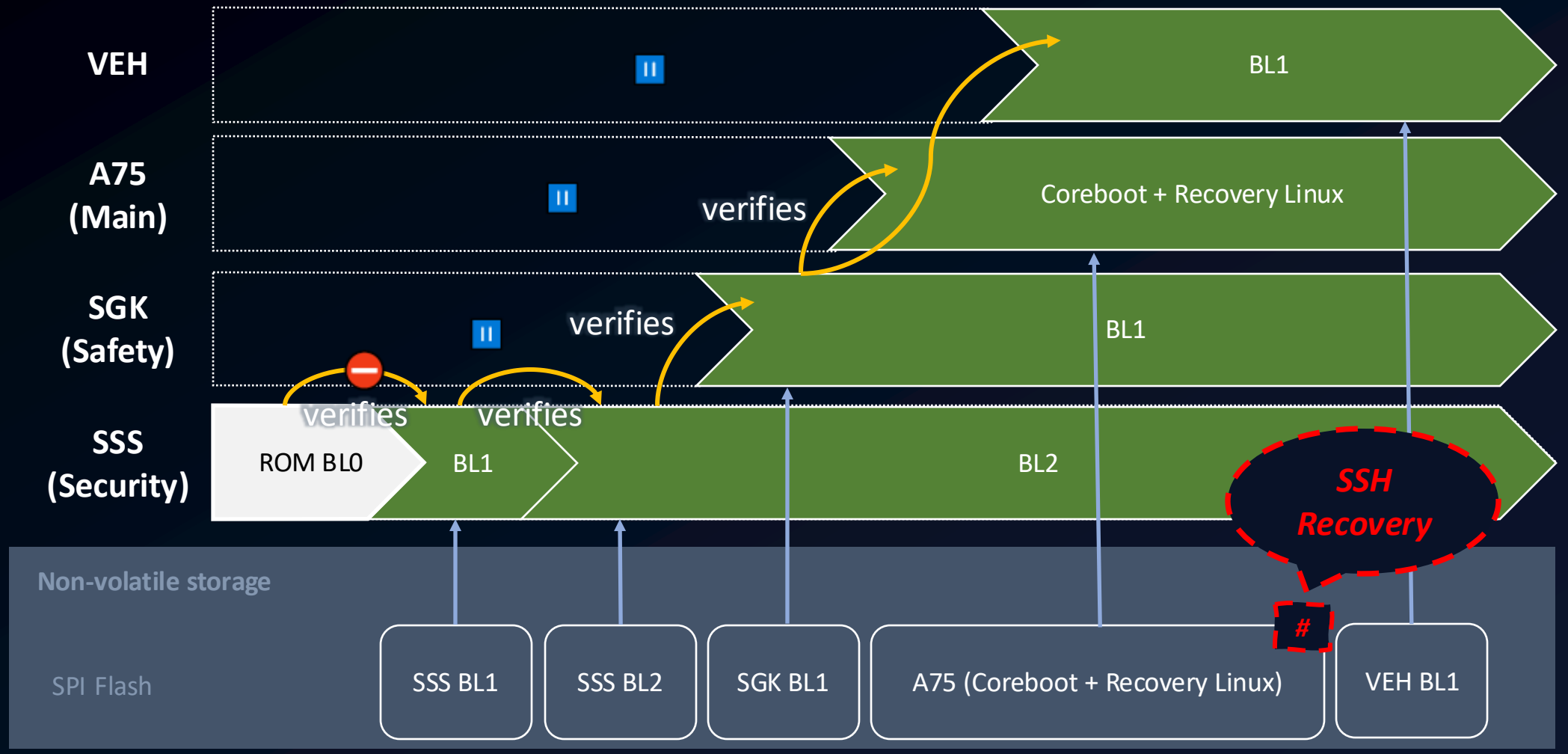
Hash

ECDSA
Signature (r, s)

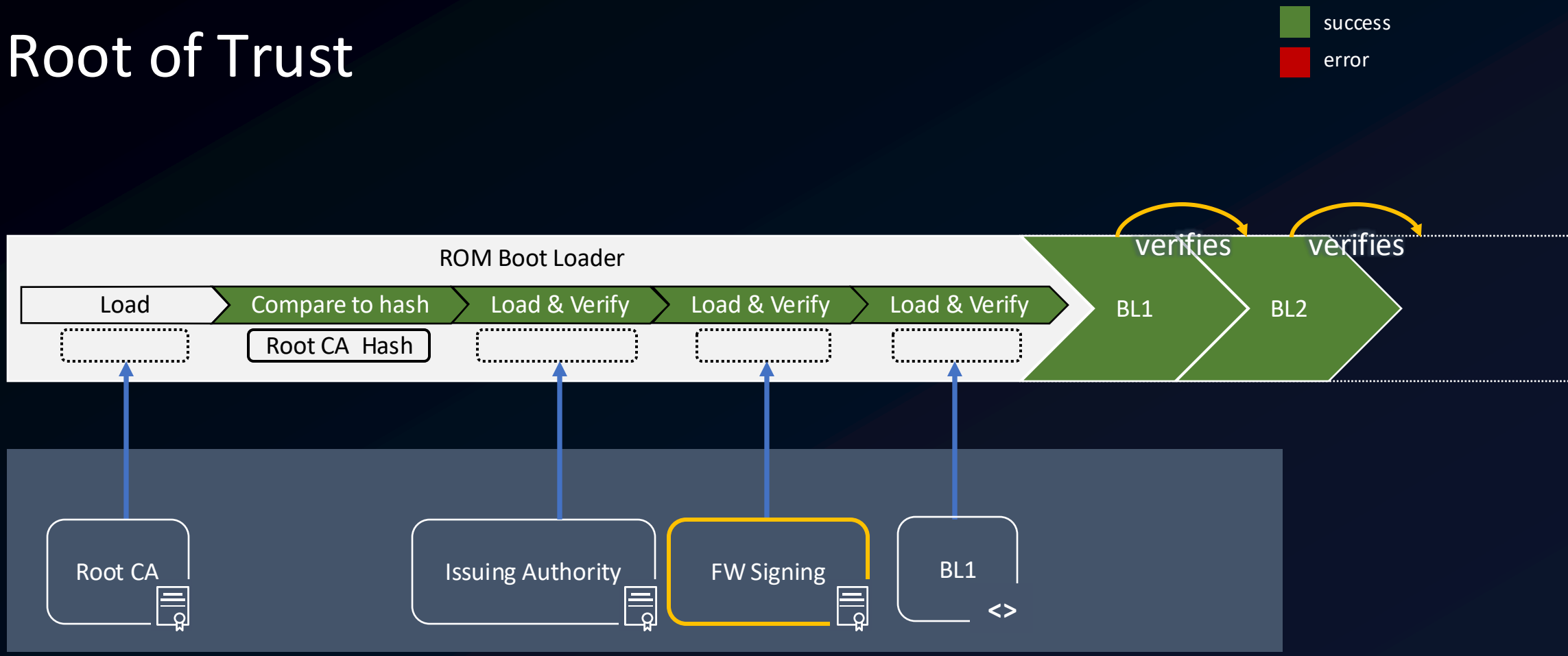


01610	0000	0000	5353	5332	5353	5332	0000	0000	SSS2SSS2
01620	0200	0000	0091	0300	0000	0000	0000	0000	.
01630	0000	0000	0000	0000	5E65	972F	016E	C241	^e./ n.A
01640	C94E	49AB	0825	B007	F628	EF6C	9A14	2CB0	.NI. %. .(.l. ,.
01650	D85B	3700	8571	50AE	1B0D	A74E	FC77	9BE0	.[7 .qP. .N.w..
01660	6EE6	E80C	76F7	8C9A	DE38	9F88	A81B	99BA	n.. v....8... ..
01670	C157	D76A	91D7	6EFC	0000	0000	0000	0000	.W.j..n.
01680	0000	0000	0000	0000	0000	0000	0000	0000	
01690	0800	0000	4200	0000	4200	0000	01F9	3C8F	B B .<.
016A0	2FB8	0337	F40A	7CFD	3078	9CB4	2277	74E9	/. 7. |.0x.."wt.
016B0	C25E	9839	55B7	6AC9	3D57	B216	E455	DDF0	.^.9U.j.=W. .U..
016C0	F984	E1DA	5B45	064F	7DCF	41FE	B93F	B659	....[E O}.A..?.Y
016D0	7044	08B6	833D	871E	AE7F	1C77	D965	0000	pD ..=. . w.e
016E0	01C1	B8EE	4450	FC62	2AA8	B861	513B	D9C9	...DP.b*..aQ;..
016F0	8103	07A4	158E	4EFA	FE71	EAB4	86EC	83F7	. . .N..q.....
01700	44CB	51D7	9C64	437F	AC6B	9B86	A805	7136	D.Q..dC .k... q6
01710	CEE3	75CB	30FA	7170	4EF7	3E3E	DE06	A402	..u.0.qpN.>>. .
01720	A9F0	0000	0000	0000	0000	0000	0000	0000	..
01730	0000	0000	0000	0000	0000	0000	0000	0000	
01740	0000	0000	0000	0000	0000	0000	0000	0000	

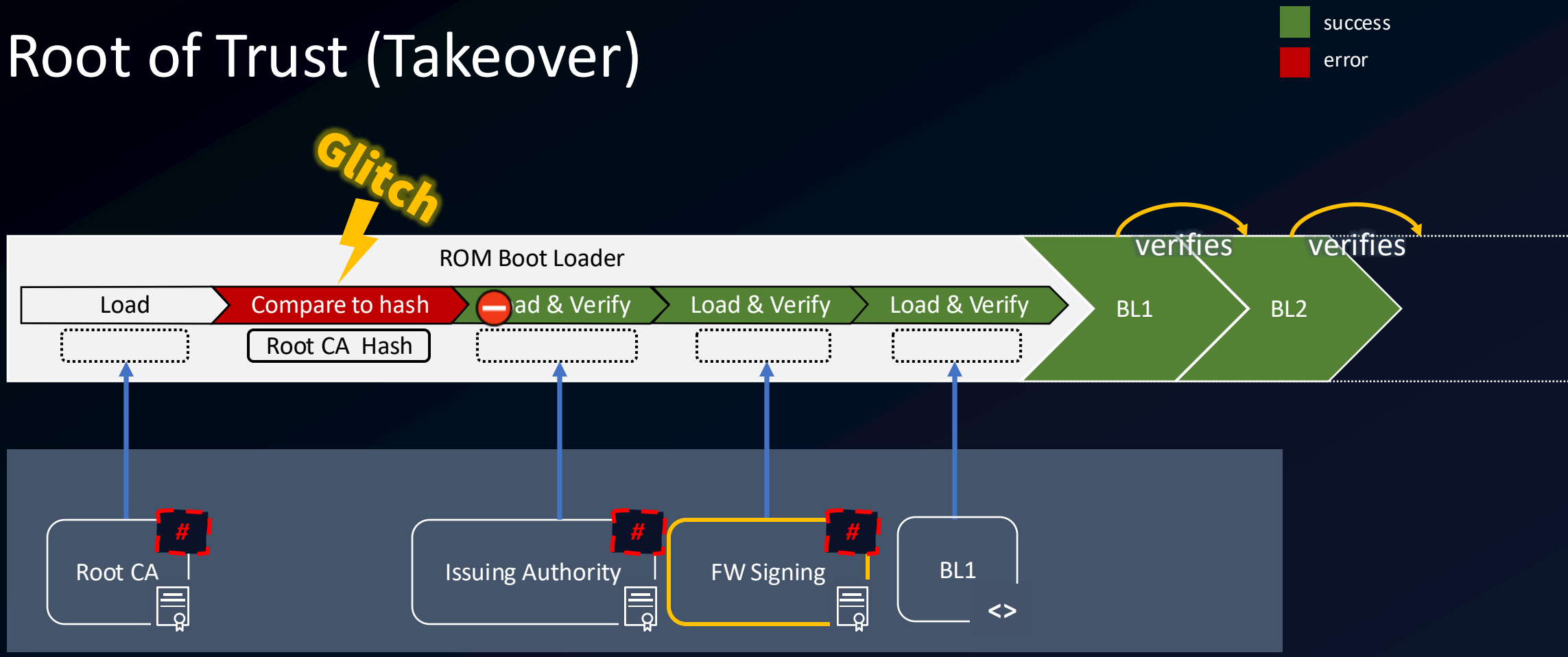
Autopilot Recovery Boot



Root of Trust



Root of Trust (Takeover)



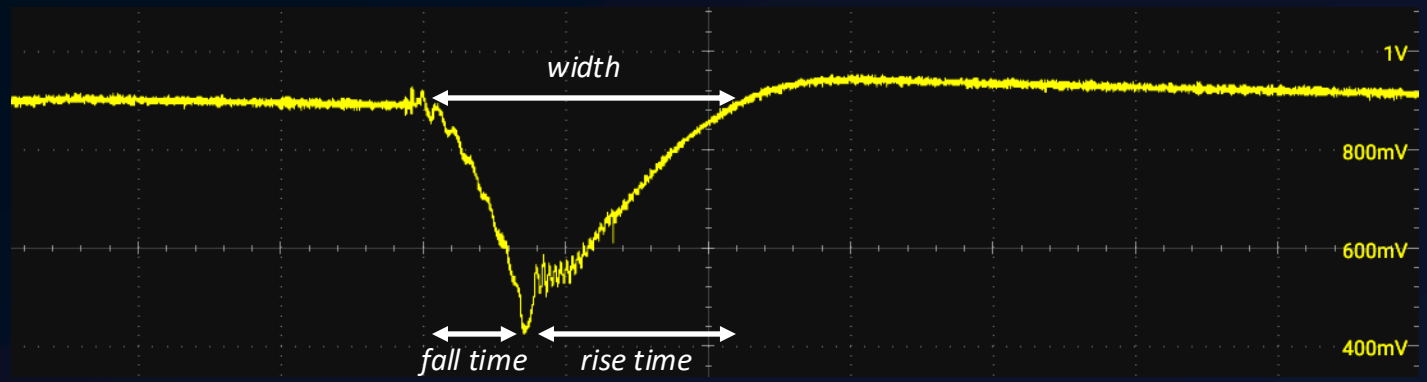
Fault Injection Attacks

Induce fault by altering the IC's environment:

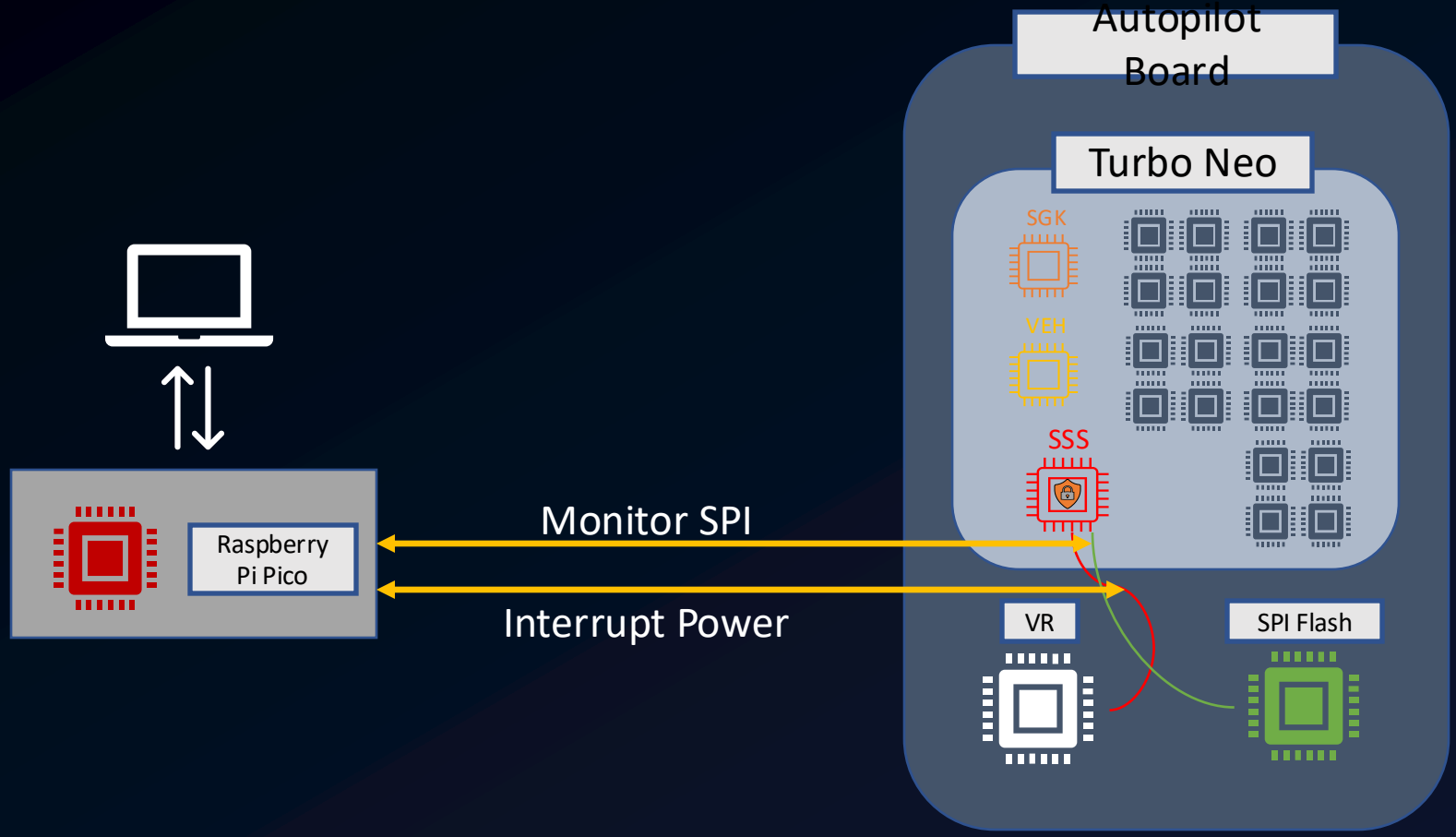
- Laser, electromagnetic-radiation, clock, supply voltage

Voltage Glitching:

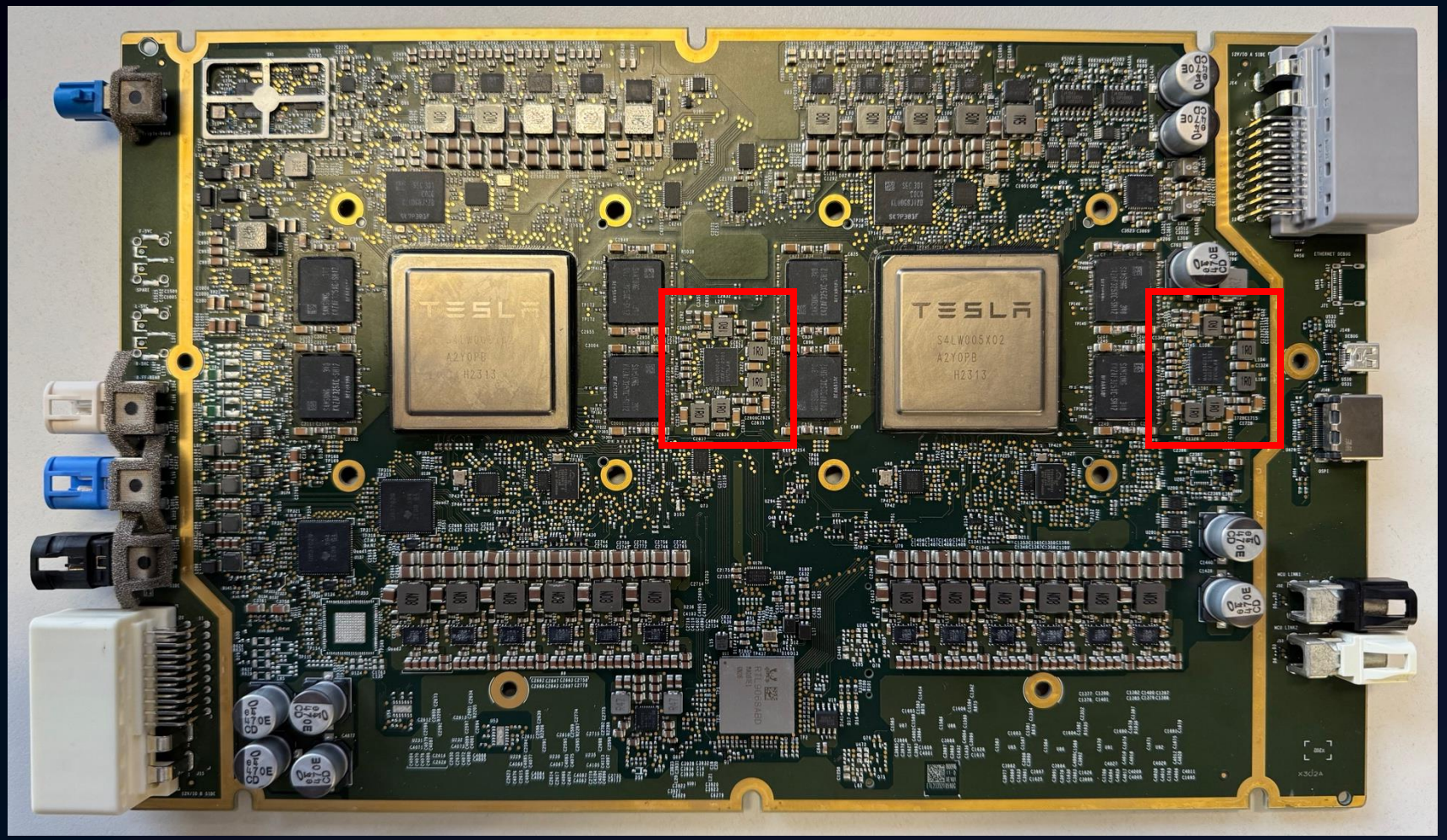
- Lowering voltage shortly



The Plan

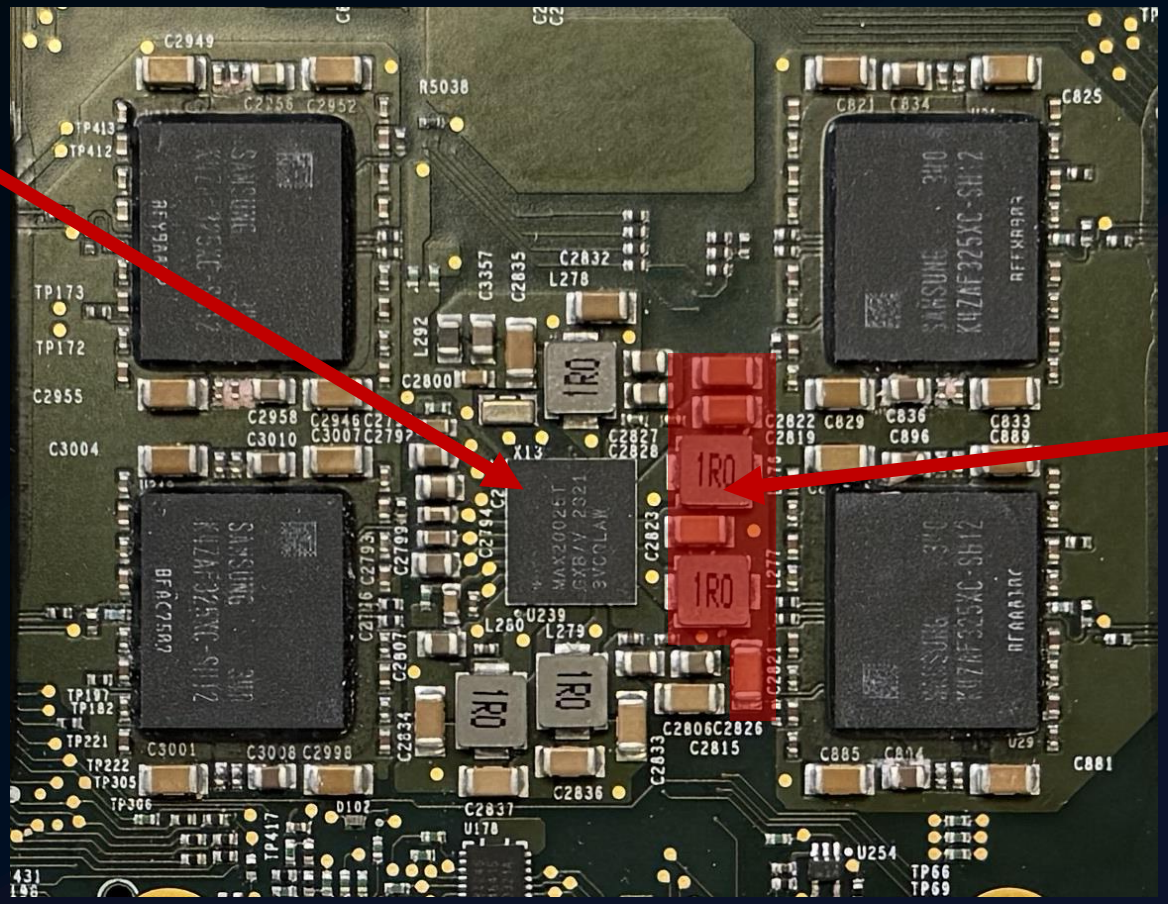

Autopilot Board
Turbo Neo
SGK
VEH
SSS
Raspberry Pi Pico
Monitor SPI
Interrupt Power
VR
SPI Flash

SSS Power Supply



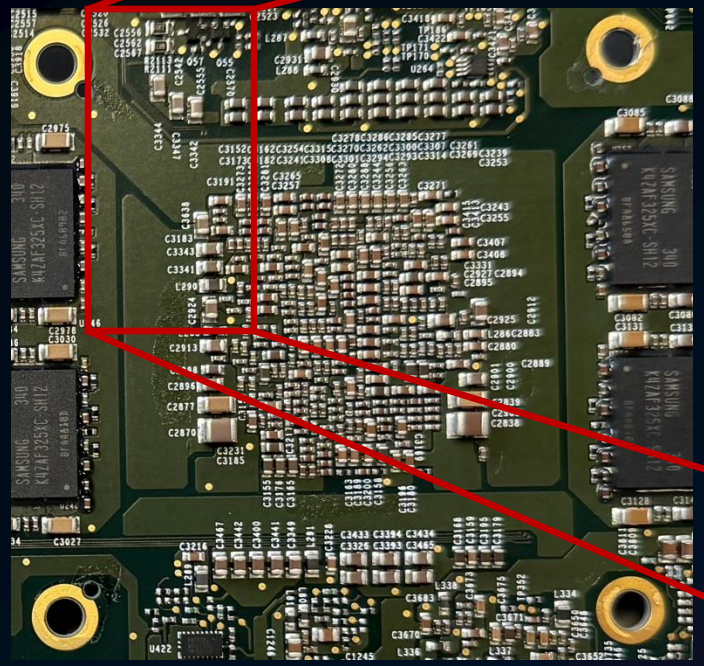
SSS Voltage Rail

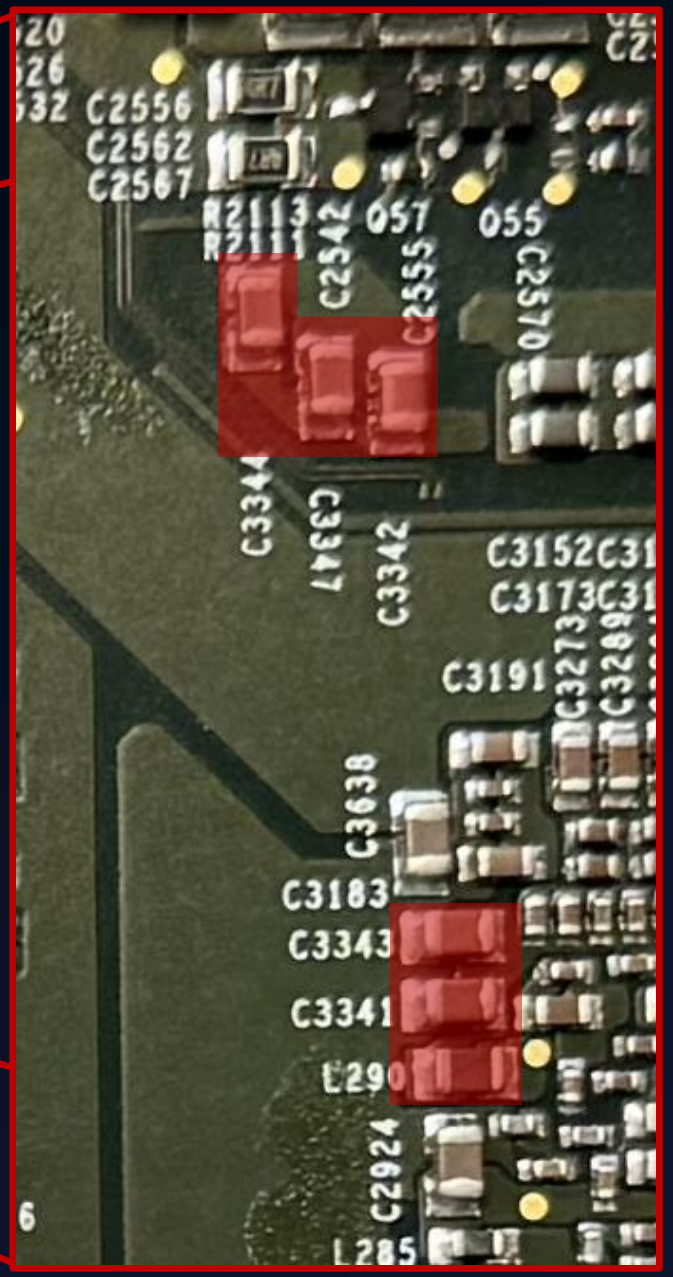
Analog Devices
MAX20025T



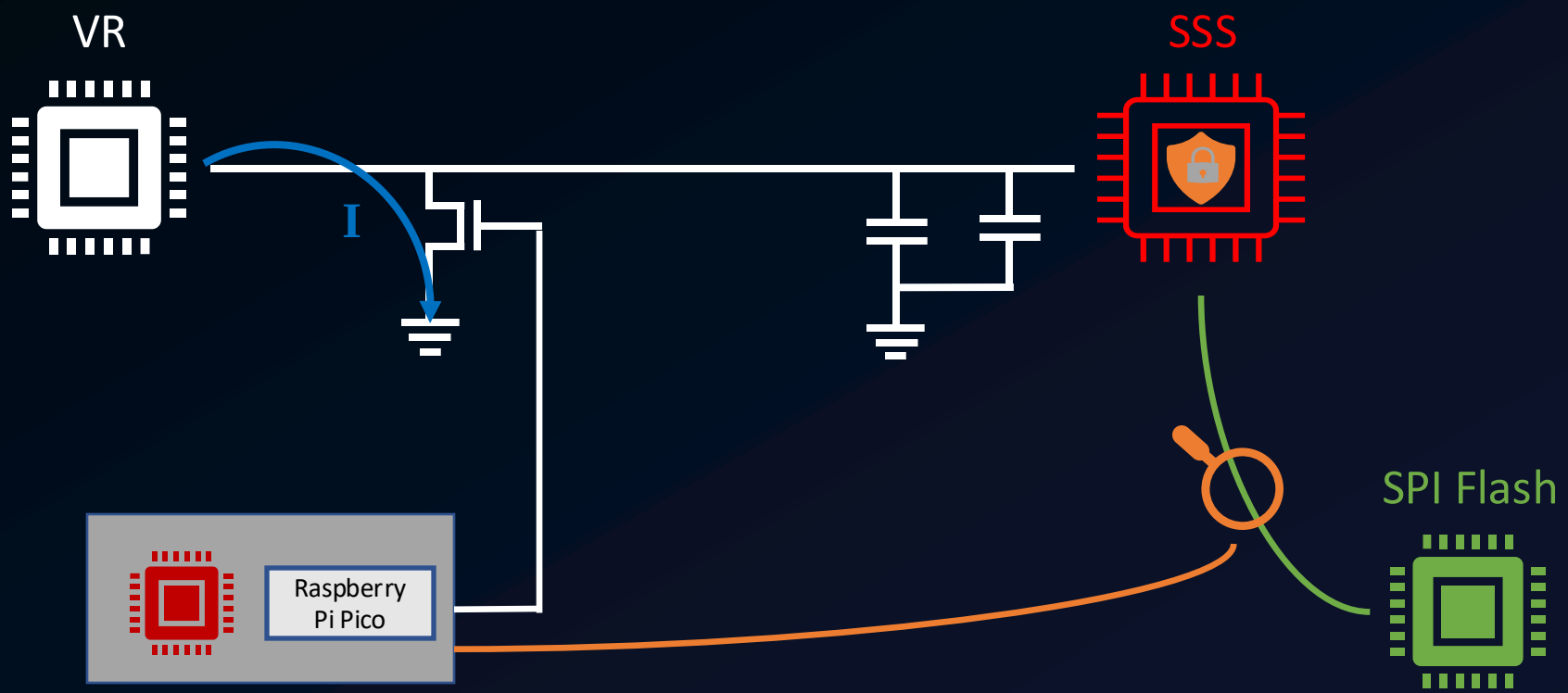
SSS Power Rail
0.75V

SSS Voltage Rail

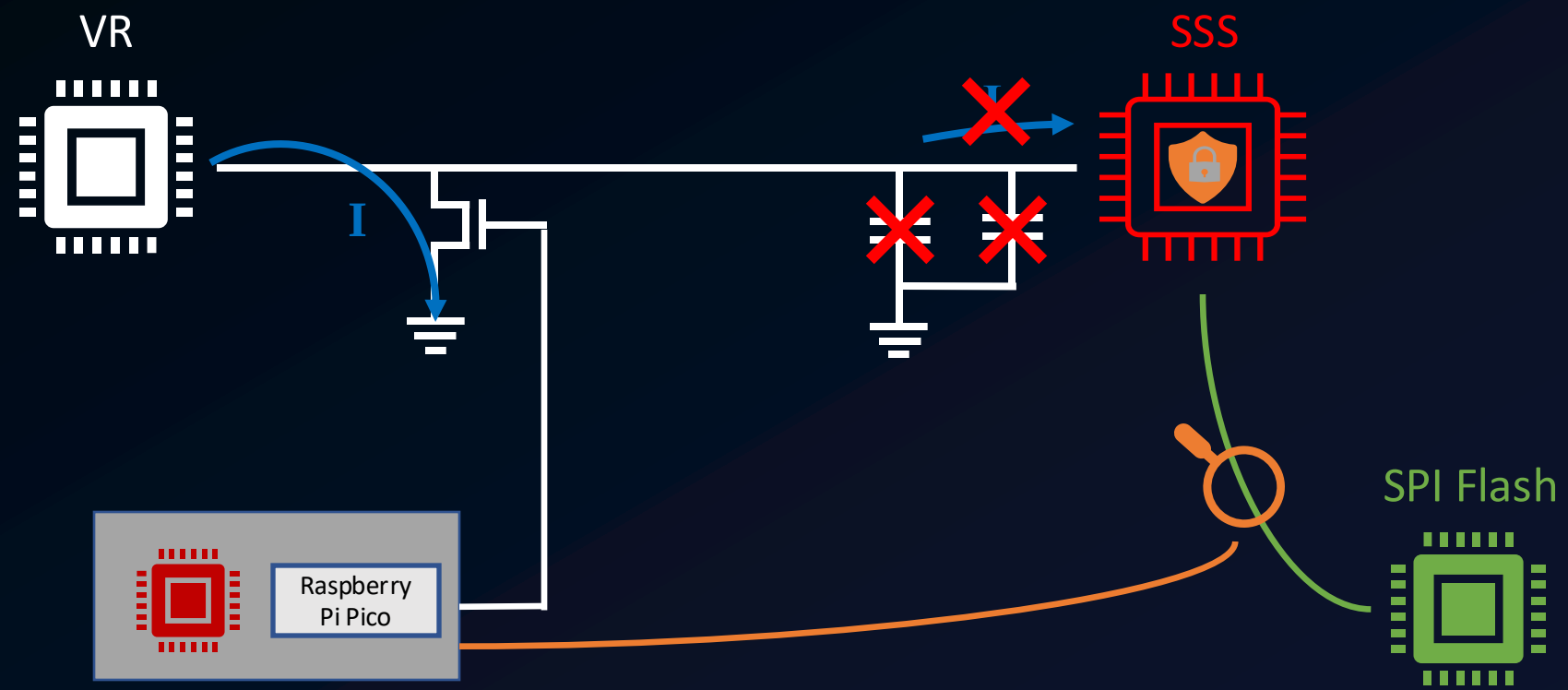




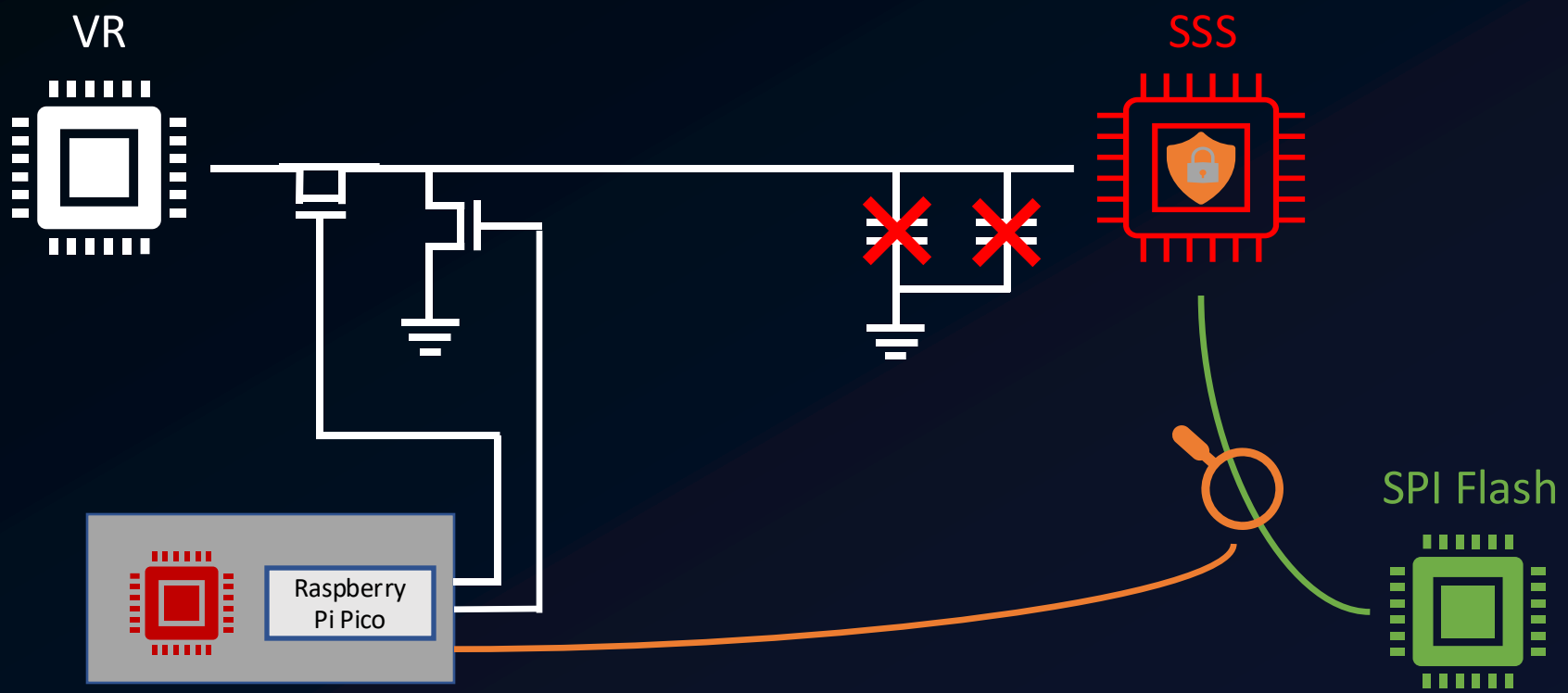
Step 1: Short SSS Voltage



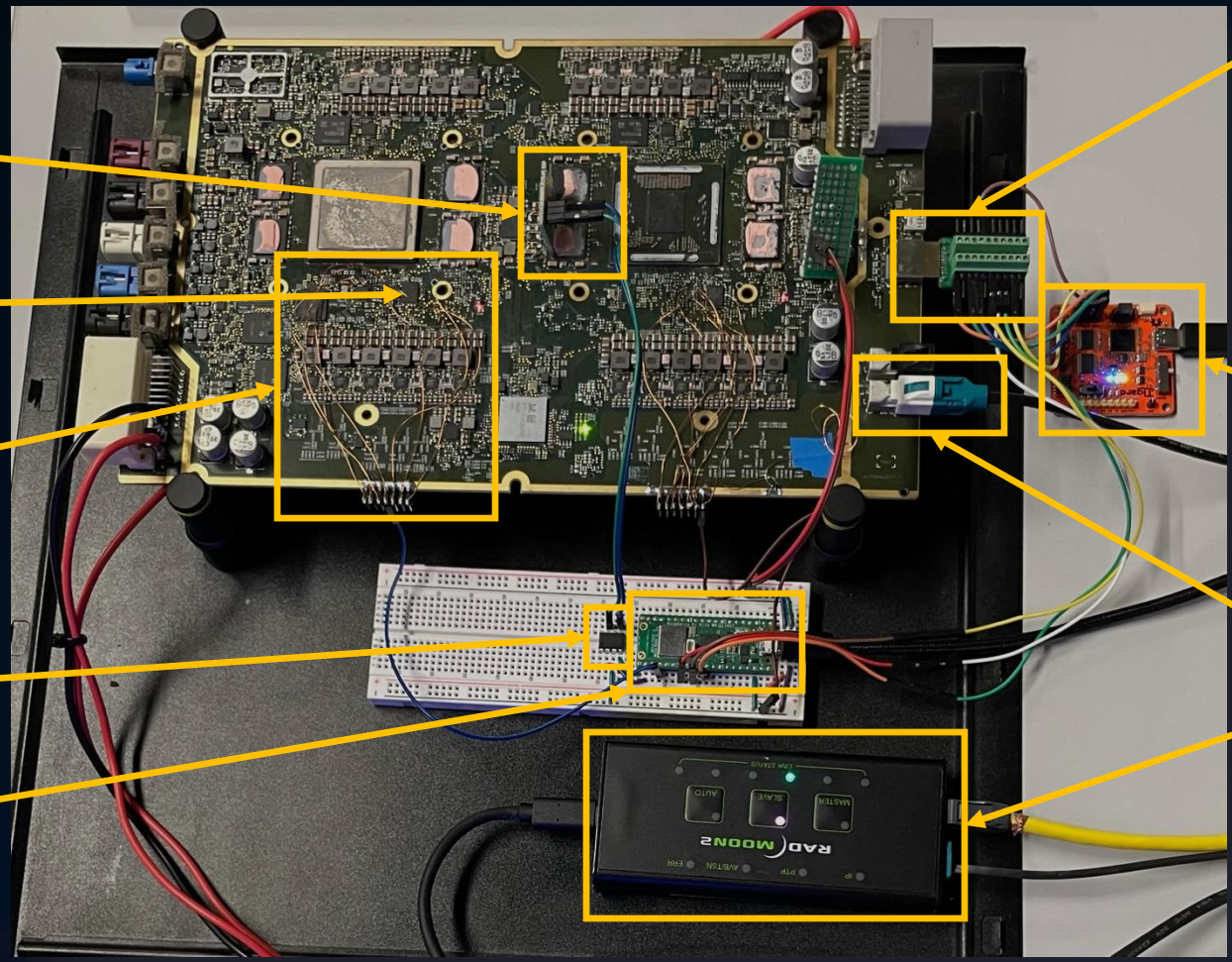
Step 2: Remove Capacitors



Step 4: Disconnect VR from Voltage Rail

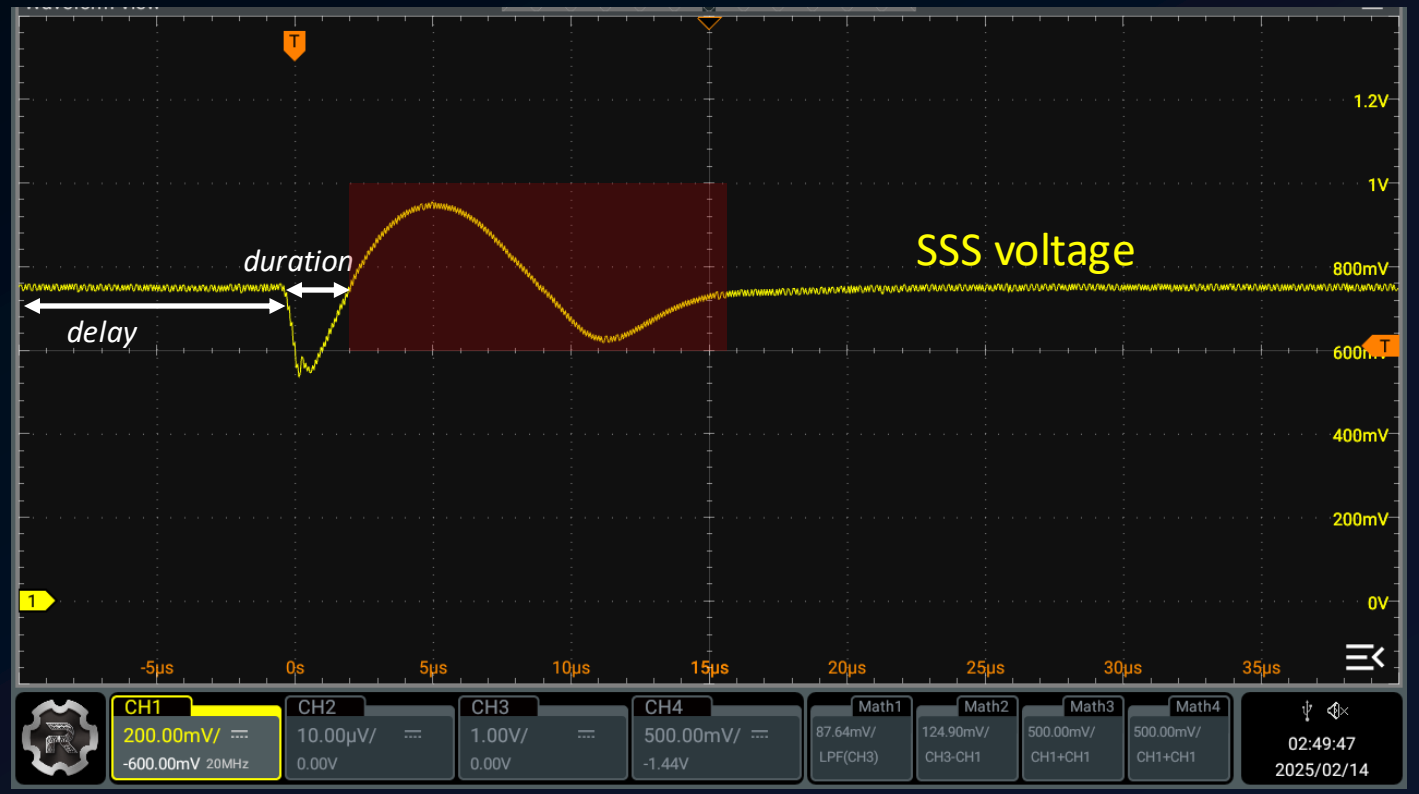


Setup in Reality

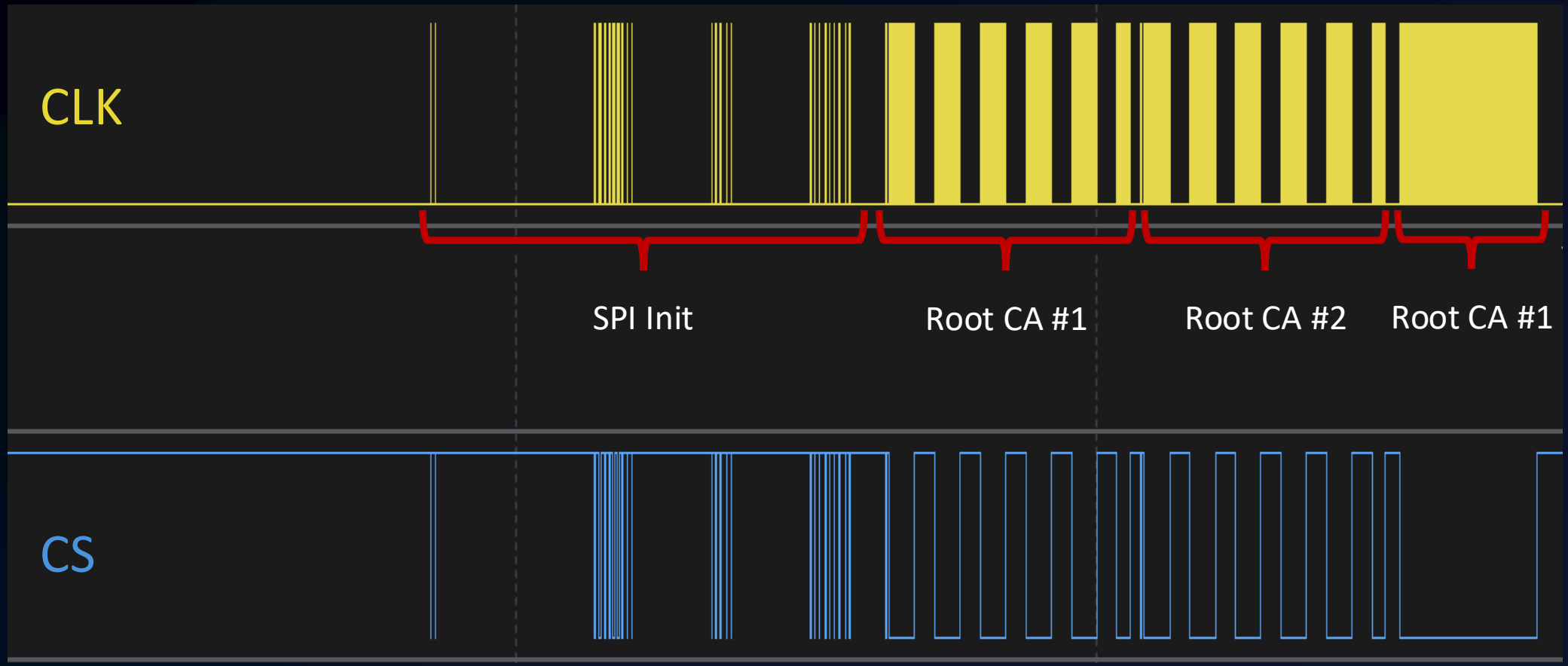


Tuning the Drop

- Determine proper duration by trial and error using original firmware
- Monitor SPI traffic while testing different values
- Too short = no effect
- Too long = system resets

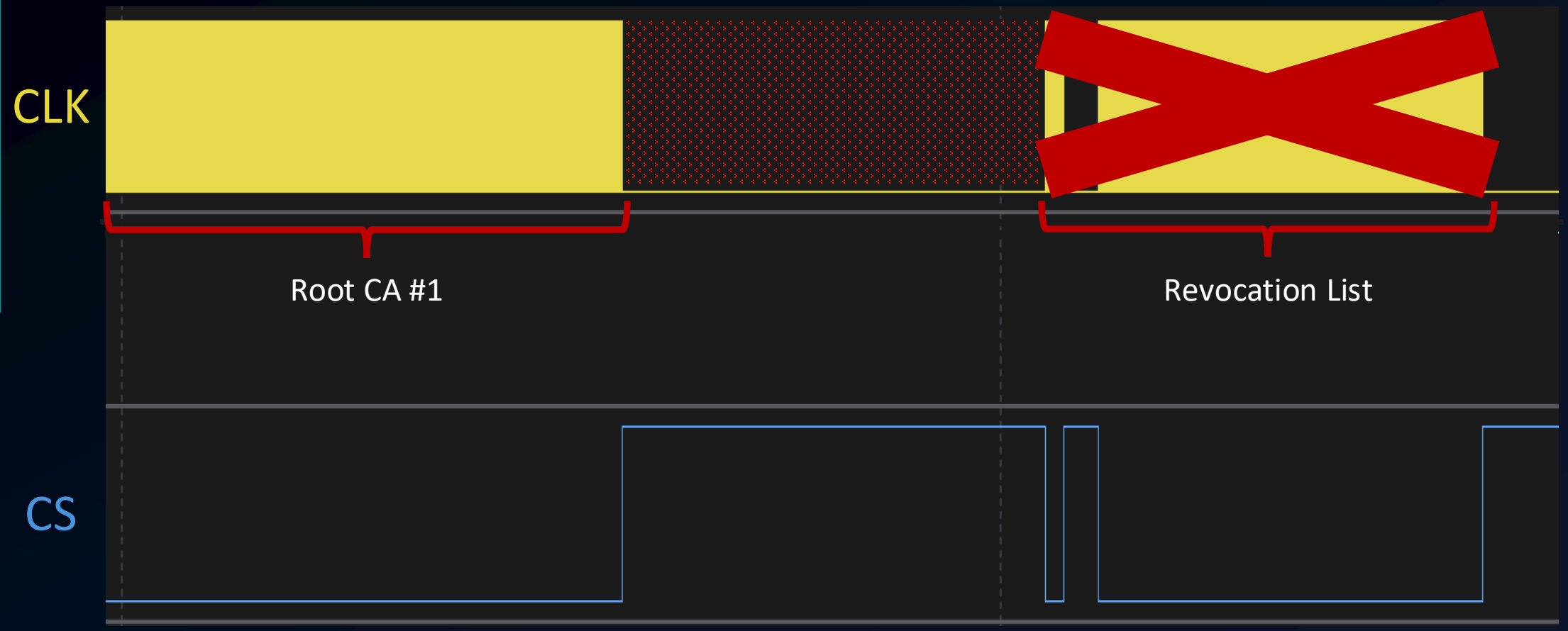


SPI Boot Trace – Unmodified



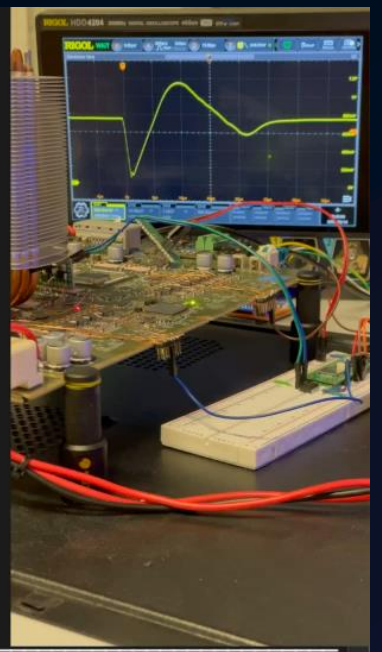
SPI Boot Trace – Root CA

SPI Boot Trace – Root CA Replaced



```
group=ineffective cs=40 counter=4294967295 delay=3074 duration=57
group=ineffective cs=40 counter=4294967295 delay=3074 duration=57
group=ineffective cs=40 counter=4294967295 delay=3073 duration=55
group=ineffective cs=40 counter=4294967295 delay=3073 duration=57
group=ineffective cs=40 counter=4294967295 delay=3073 duration=57
group=ineffective cs=40 counter=4294967295 delay=3074 duration=55
group=ineffective cs=40 counter=4294967295 delay=3073 duration=55
group=ineffective cs=40 counter=4294967295 delay=3074 duration=56
group=ineffective cs=40 counter=4294967295 delay=3075 duration=57
group=ineffective cs                                  duration=57
group=ineffective cs                                  duration=55
group=ineffective cs                                  duration=56
group=ineffective cs=40 counter=4294967295 delay=3073 duration=55
group=ineffective cs=40 counter=4294967295 delay=3074 duration=55
group=ineffective cs=40 counter=4294967295 delay=3075 duration=56
group=ineffective cs=40 counter=4294967295 delay=3073 duration=57
group=ineffective cs=40 counter=4294967295 delay=3075 duration=57
group=ineffective cs=40 counter=4294967295 delay=3075 duration=56
group=ineffective cs=40 counter=4294967295 delay=3074 duration=55
group=ineffective cs=40 counter=4294967295 delay=3073 duration=55
group=success cs=59 counter=5881 delay=3074 duration=55
Press enter to continue
```

Glitch Script



```
deploy@deploy:~/hw4_ap$ ping 192.168.90.105
```

Ping

```
deploy@deploy:~/hw4_ap$ ssh -o StrictHostKeyChecking=no root@192.168.90.105
```

SSH

```
[sshap4] 0:minicom* 1:bash-                                    "" 20:27 13-Feb-25
```

Success Rate

- Measured only on one SoC

- Attempts: 60083
- Successes: 292
- False positives: 0
- Success rate: 205.76 attempts/success
- Glitch rate: 33.38 attempts/s

successful glitch every 7s!

Comparison to HW3

- Attack mostly the same -> no new mitigations
- Had to desolder more components
- SPI flash filesystem differs but signatures are of same format
- New co-processor and new names

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

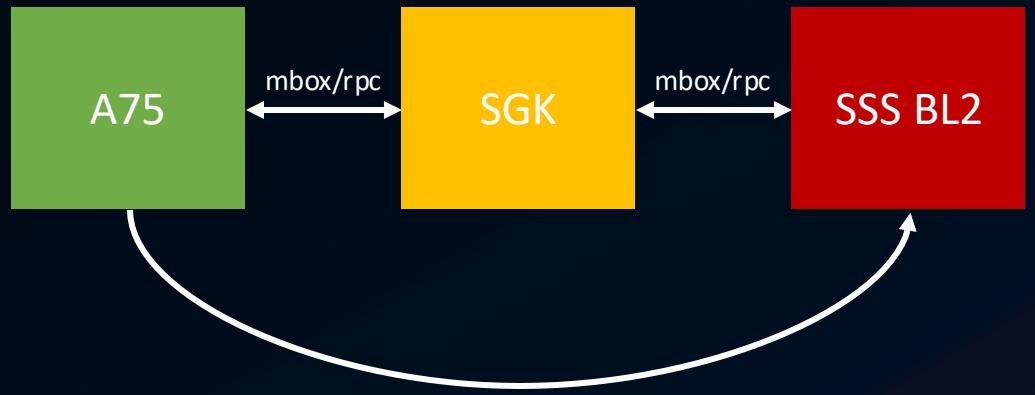
Board Credentials


```
# ls -la /media/dvg-var/lib/board_creds/
total 16
drw
drw
-rw
-r-
```

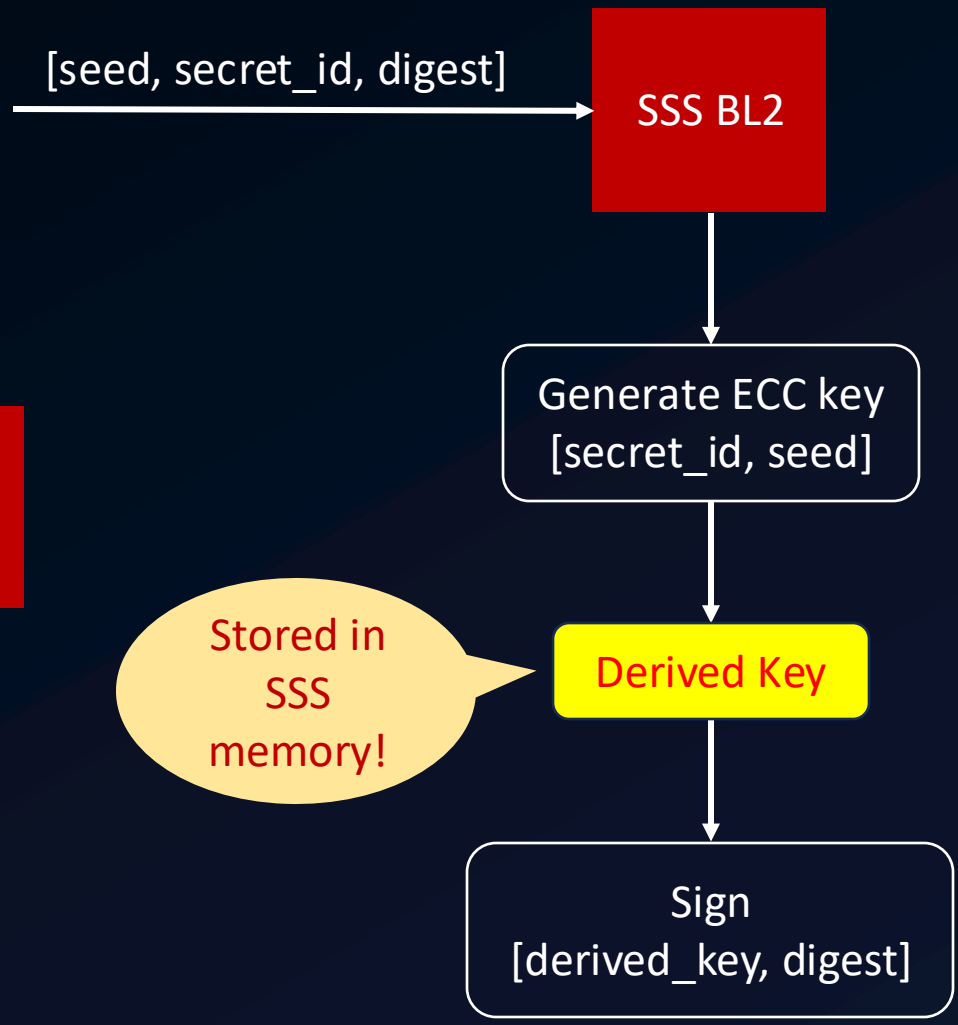
```
# cat /media/dvg-var/lib/board_creds/board.key
-----BEGIN FSD TPM PRIVATE KEY-----
CAAAAAEAAAACAAAAAwAAAGJvYXJkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END FSD TPM PRIVATE KEY-----
```

```
# /media/rootfs-a/usr/bin/fsd-tpm-ctrl print -v -i /media/dvg-var/lib/board_creds/board.key
INFO: KeyData:
INFO:   ClientId:StonefishKey_AP_User
INFO:   RootSecret:SoCRootSecret
INFO:   Type:P256
INFO:   Capabilities:
INFO:           - Signature
INFO:   Seed:  626F617264000000000000000000000000000000000000000000000000000000
```

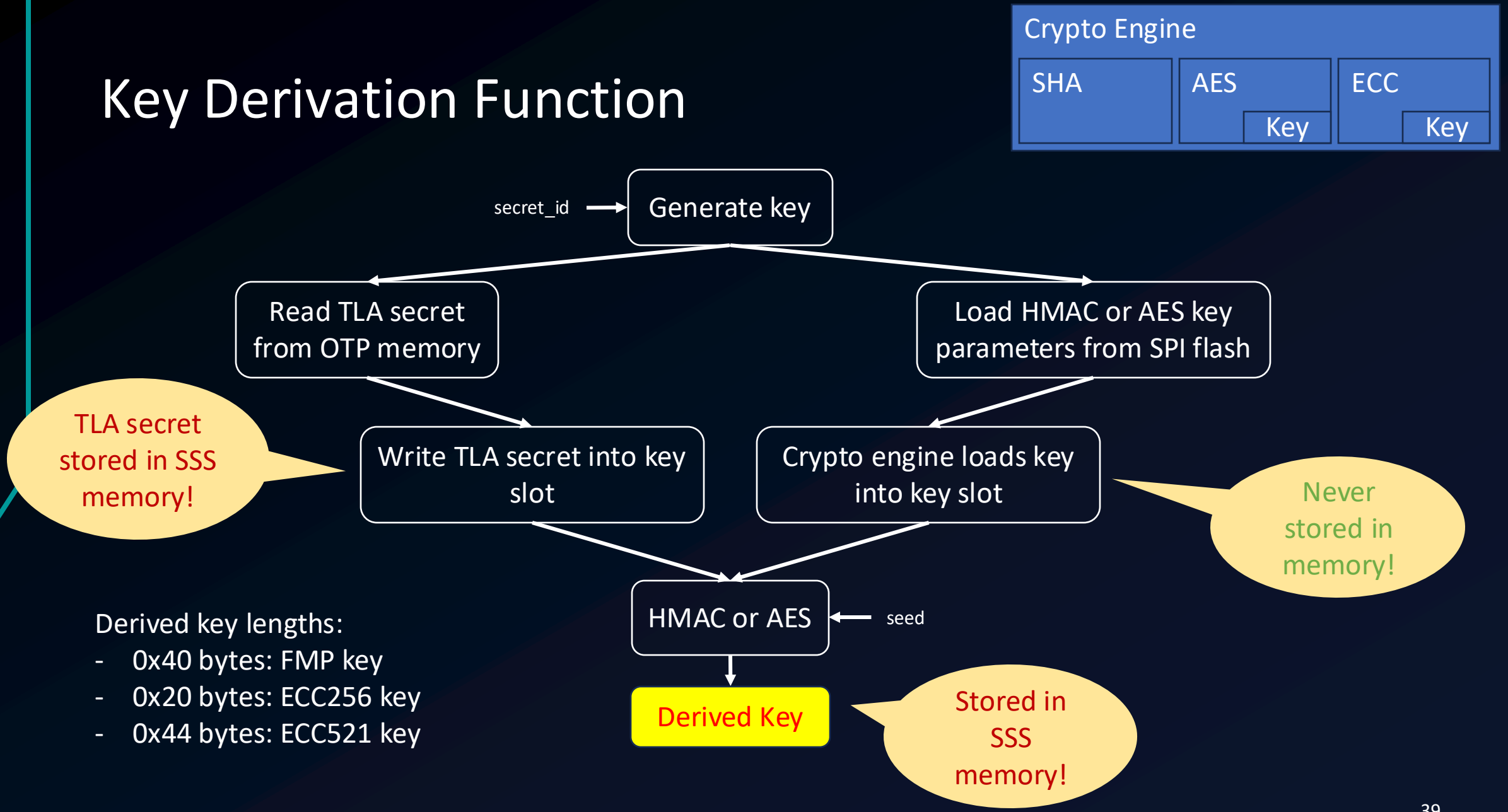
Board Credentials



Sign Request
[seed, secret_id, digest]



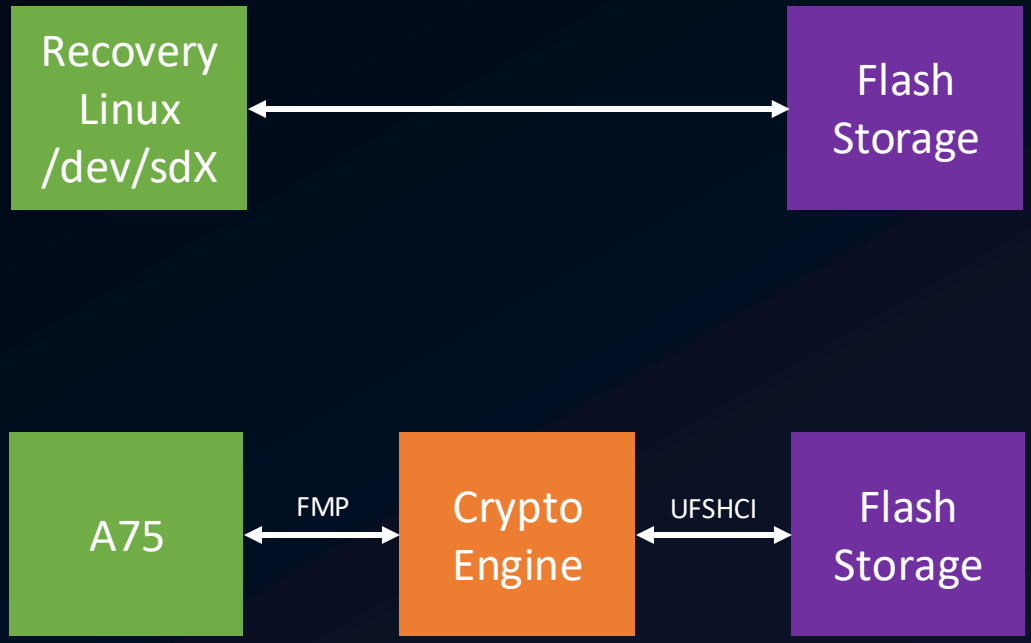
Key Derivation Function



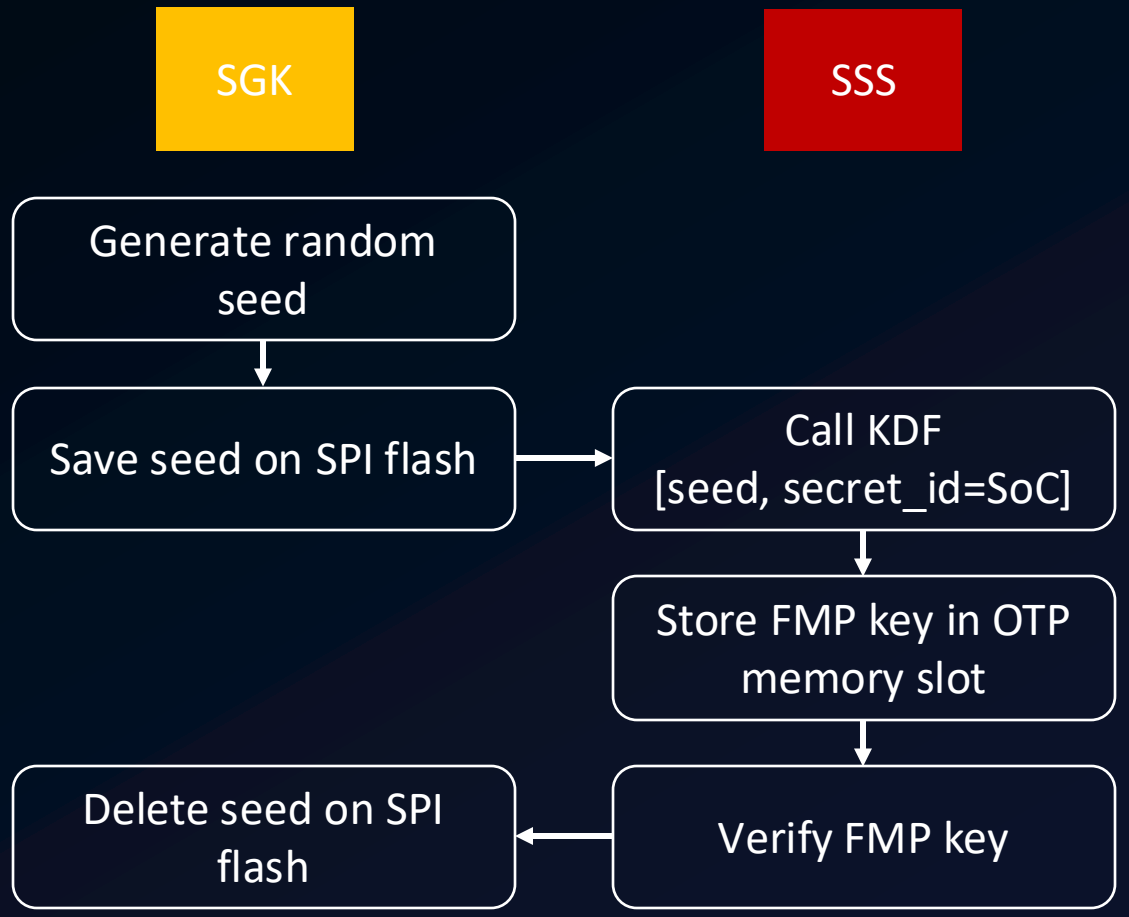
Derived key lengths:

- 0x40 bytes: FMP key
- 0x20 bytes: ECC256 key
- 0x44 bytes: ECC521 key

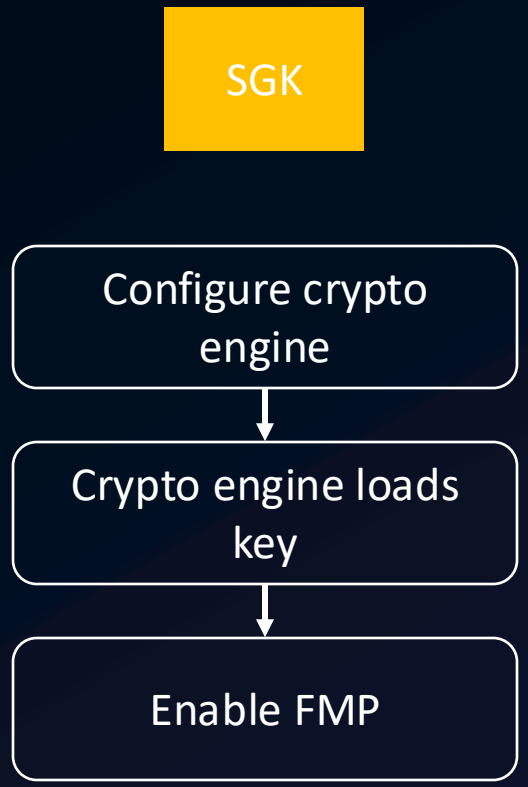
Flash Memory Protector



Flash Memory Protector - Provisioning

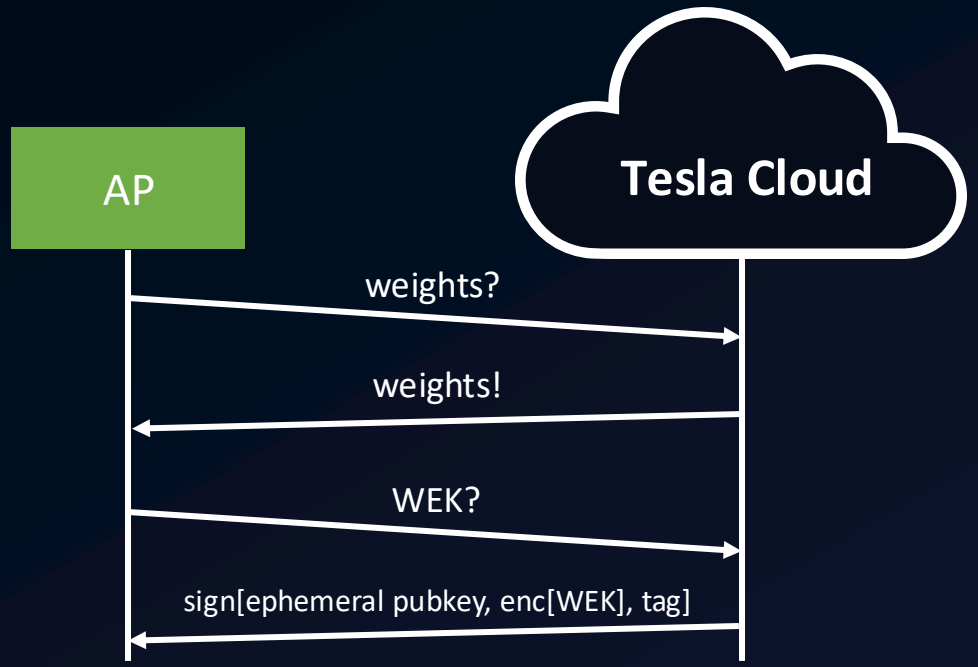


Flash Memory Protector - Activation

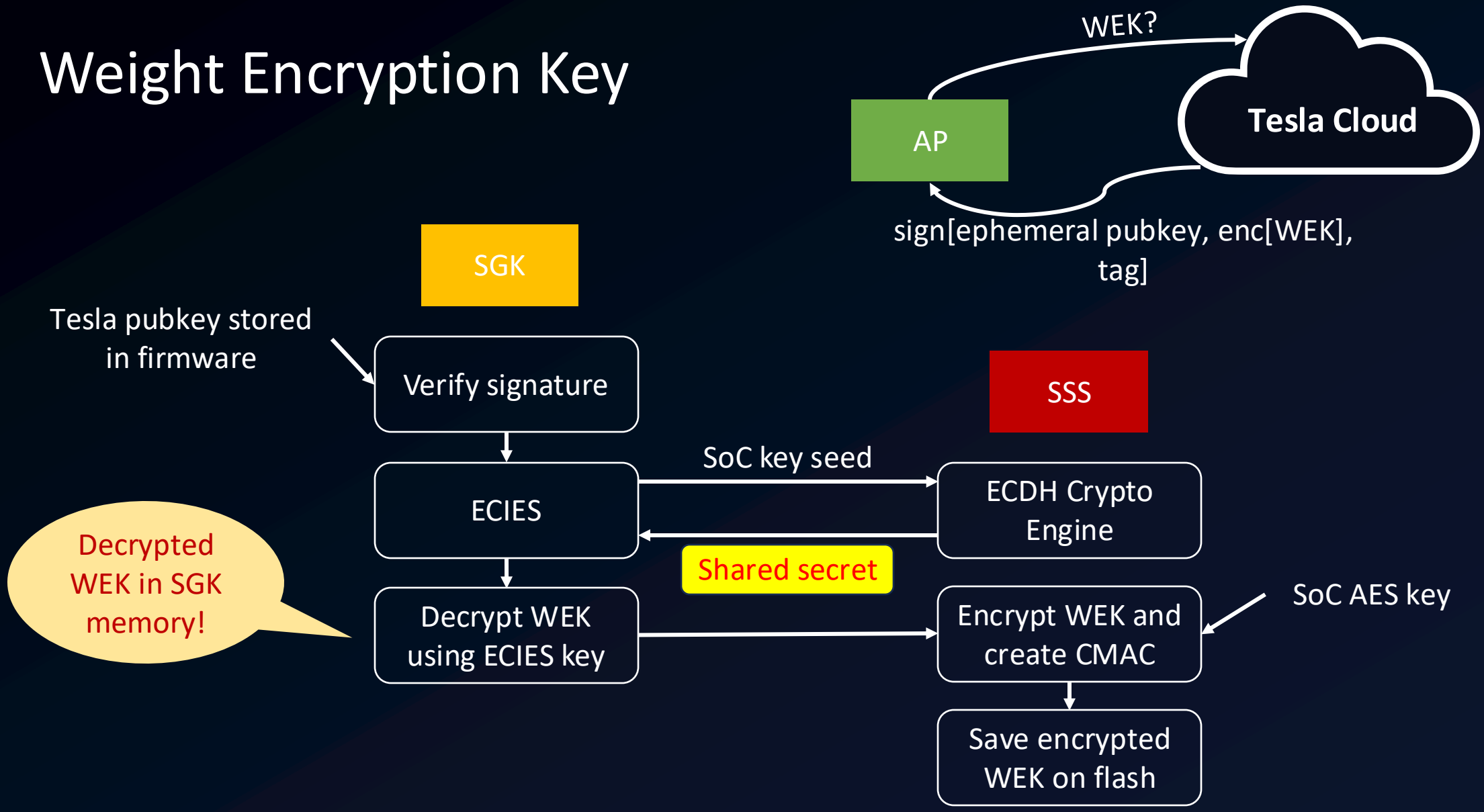


Weight Encryption

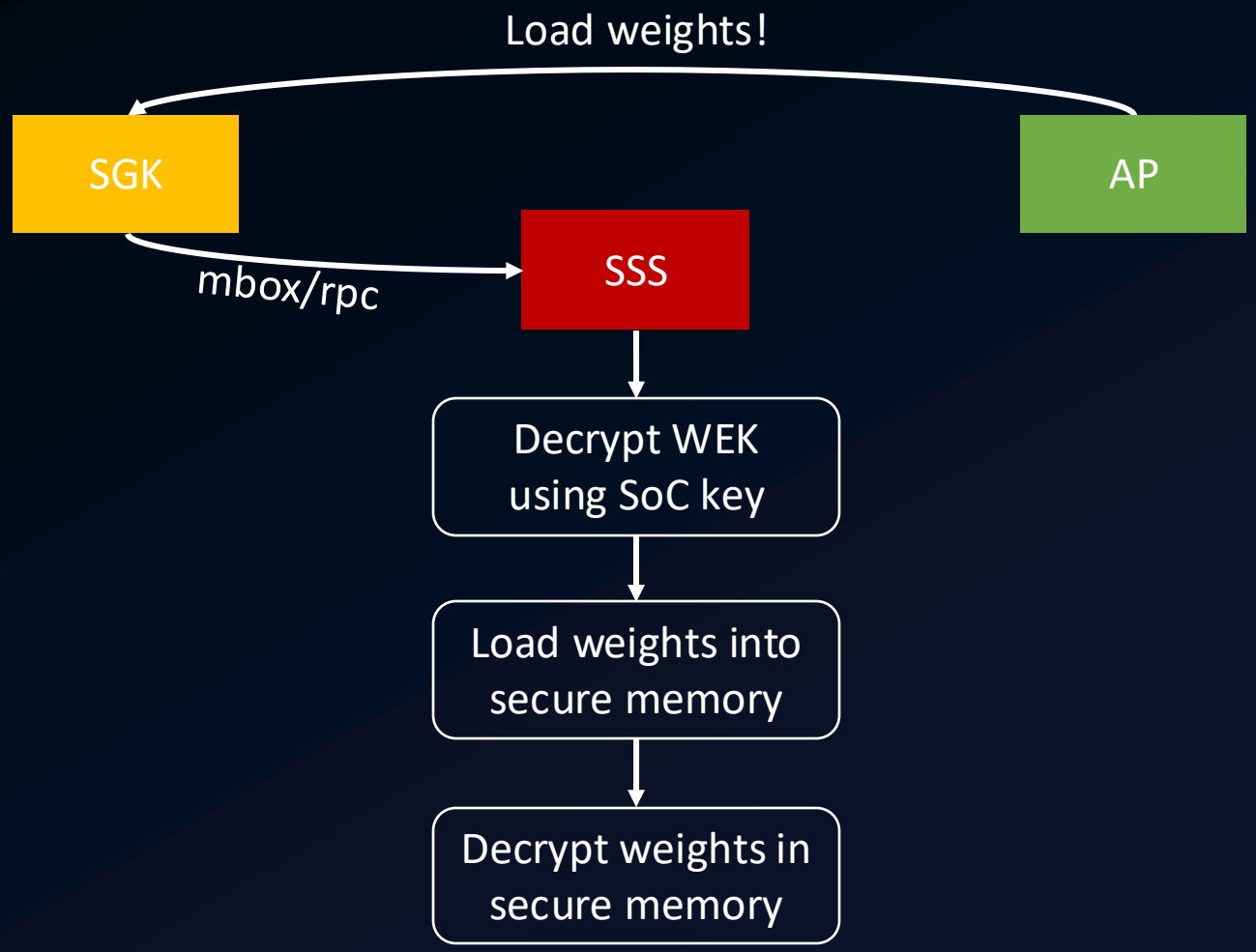
- Weights needed for ML
- AP allowed to download
- Encrypted with WEK
- WEK decrypted by SGK
- Decrypted weights never leave secure NPU memory



Weight Encryption Key



Weight Decryption



What can be extracted?

- Board key
- Flash memory protector key (?)
- Weight encryption key

- But: *SoC Root key* and *SoC AES/HMAC key* seem to be safe!

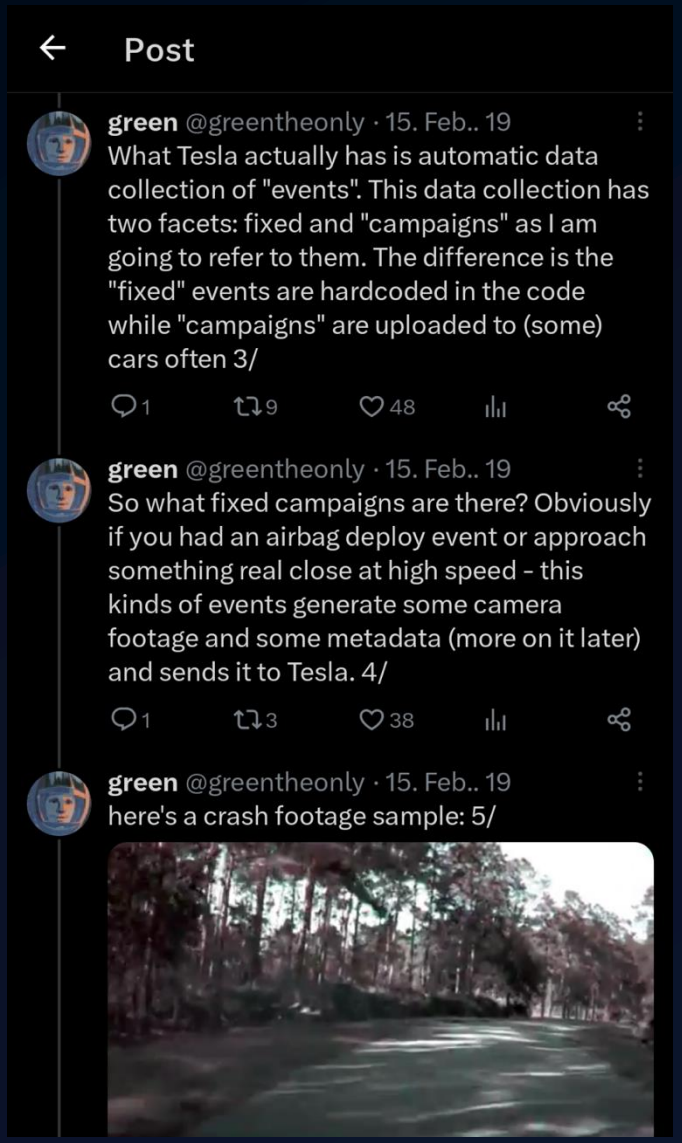
Key Takeaways

Voltage glitching is *still* a thing

1. It threatens Tesla's intellectual property (Autopilot software and especially weights)
2. It enables 3rd parties to independently analyze the system
   - for data privacy violations, forensic investigations
   - for vulnerabilities, e.g., adversarial (ML) attacks
   - for understanding elaborate crypto concepts
3. The window for 3rd party analysis is closing
4. Use key slots whenever possible to handle keys securely

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

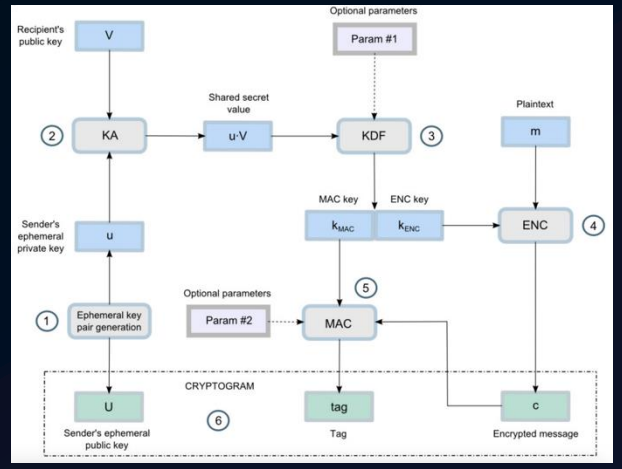


Questions?

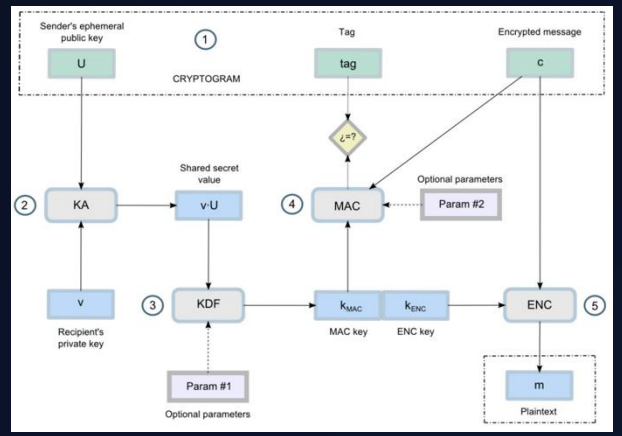
TECHNISCHE UNIVERSITÄT BERLIN

Elliptic Curve Integrated Encryption Scheme

- Encryption
  - Input: AP pubkey, server's ephemeral pubkey, "APWEK-ENC"
  - Output: ephemeral pubkey, tag, encrypted WEK
- Decryption
  - Input: private key, ephemeral pubkey, tag, encrypted WEK, "APWEK-ENC"
  - Output: verfied WEK
- KDF = SHA256
- MAC = CMAC-AES256 + "APWEK-MAC"
- ENC = AES256-CBC



https://dl.acm.org/doi/abs/10.1080/01611194.2014.988363



https://dl.acm.org/doi/abs/10.1080/01611194.2014.988363