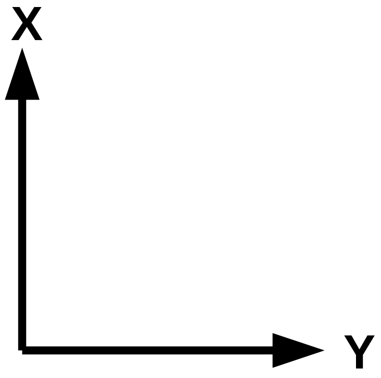
Electromagnetic Fault Injection on System-on-Chip in black-box context

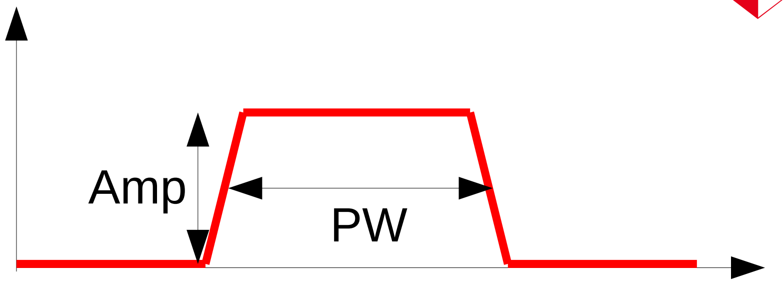
Clément Fanjas, Driss Aboulkassimi, Simon Pontié, Jessy Clédière

Table of contents

I. Context
II. Related works
III. Methodology
IV. Conclusion

Context





EMFI parameters :

- Probe position (XY)
- Pulse parameters
  - Pulse width
  - Pulse amplitude

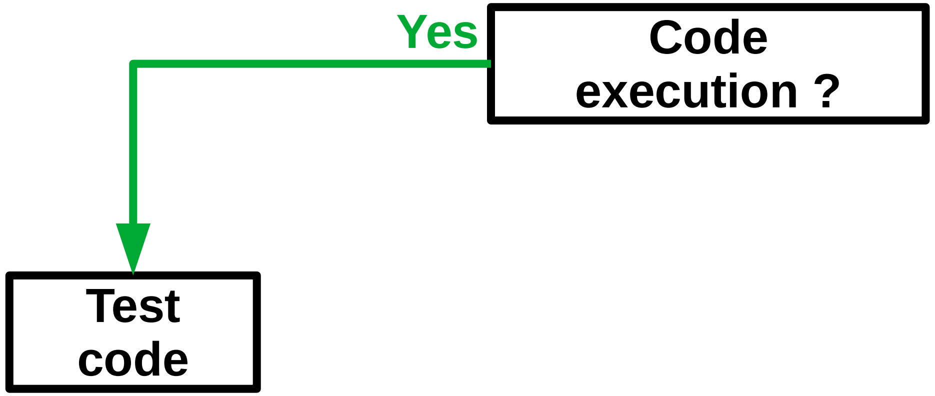
Target :

- Smartphone ⇒ System-on-Chip

Problematic:

How to identify suitable parameters to inject a fault on complex target such as smartphone SoC?

Related works



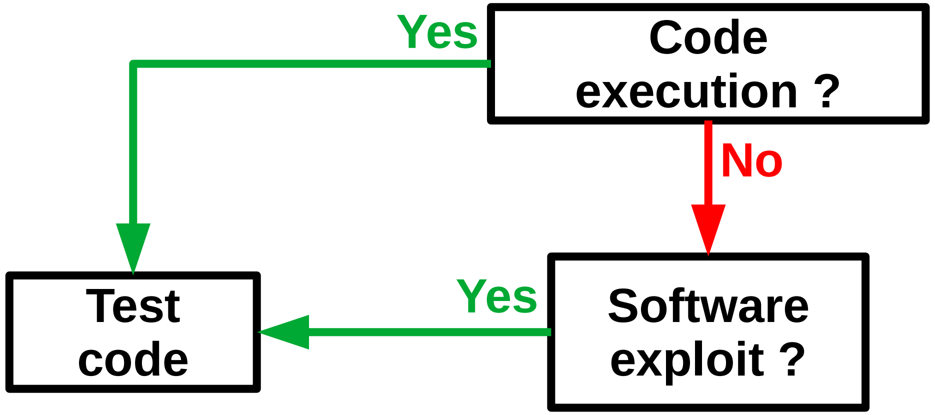
Code execution ?

Yes

Test code

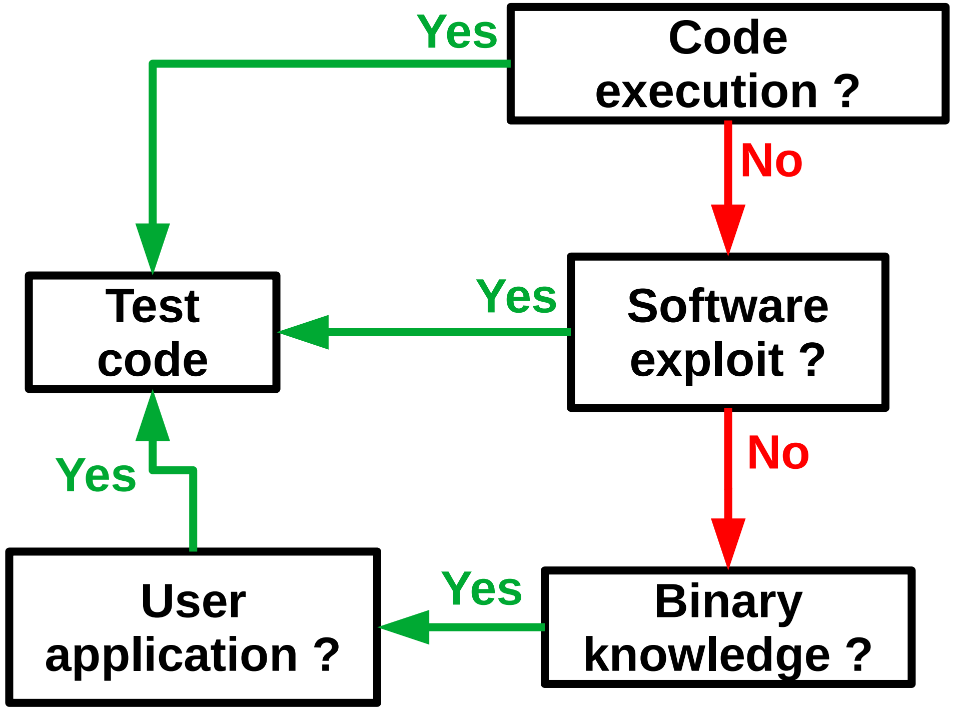
Paper	Context	Issue
Werner et al. (2021) Werner et al. (2022) Wu et al. (2020) Maldini et al. (2019) Carpi et al. (2014) Bozzato et al. (2019) Gaine et al. (2020) ...	**White Box**	**Not a realistic scenario for an attacker**

Related works



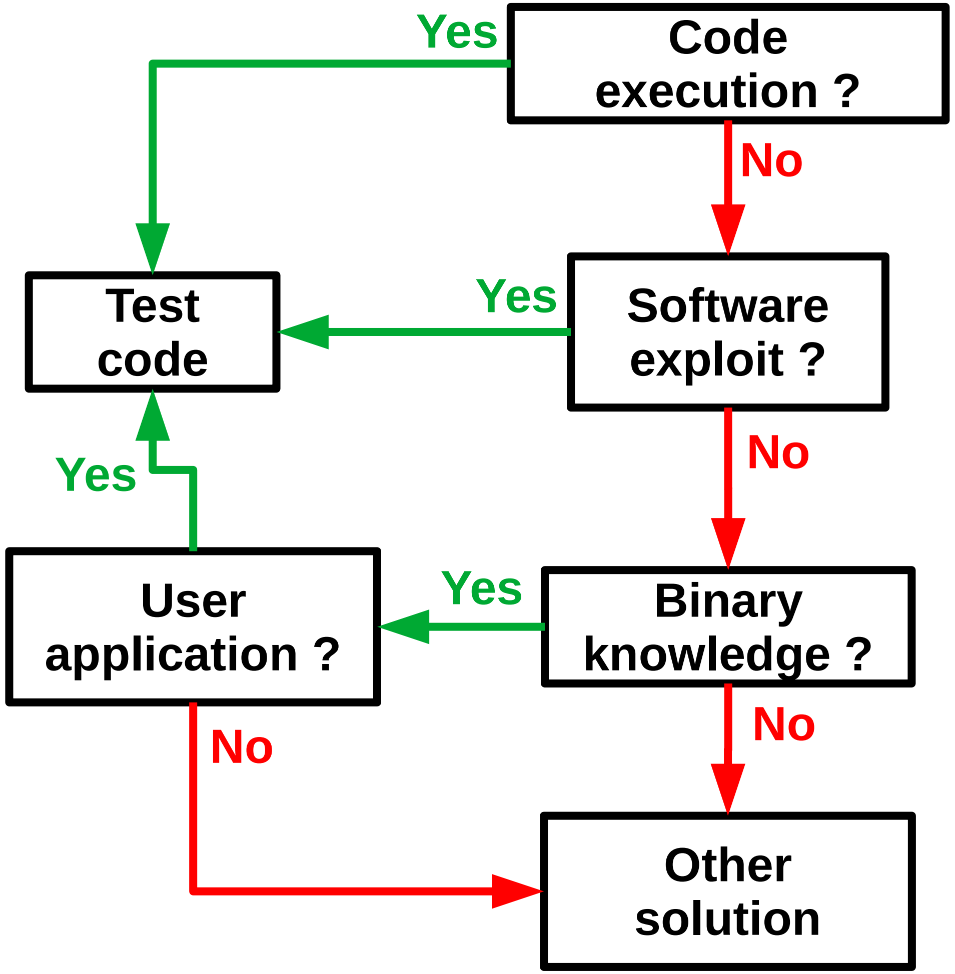
Paper	Context	Issue
Werner et al. (2021) Werner et al. (2022) Wu et al. (2020) Maldini et al. (2019) Carpi et al. (2014) Bozzato et al. (2019) Gaine et al. (2020) ...	**White Box**	**Not a realistic scenario for an attacker**
Kuhnapfel et al. (2022) Vasselle et al. (2017)	**Software exploit to gain code execution**	**Not always feasible**

Related works



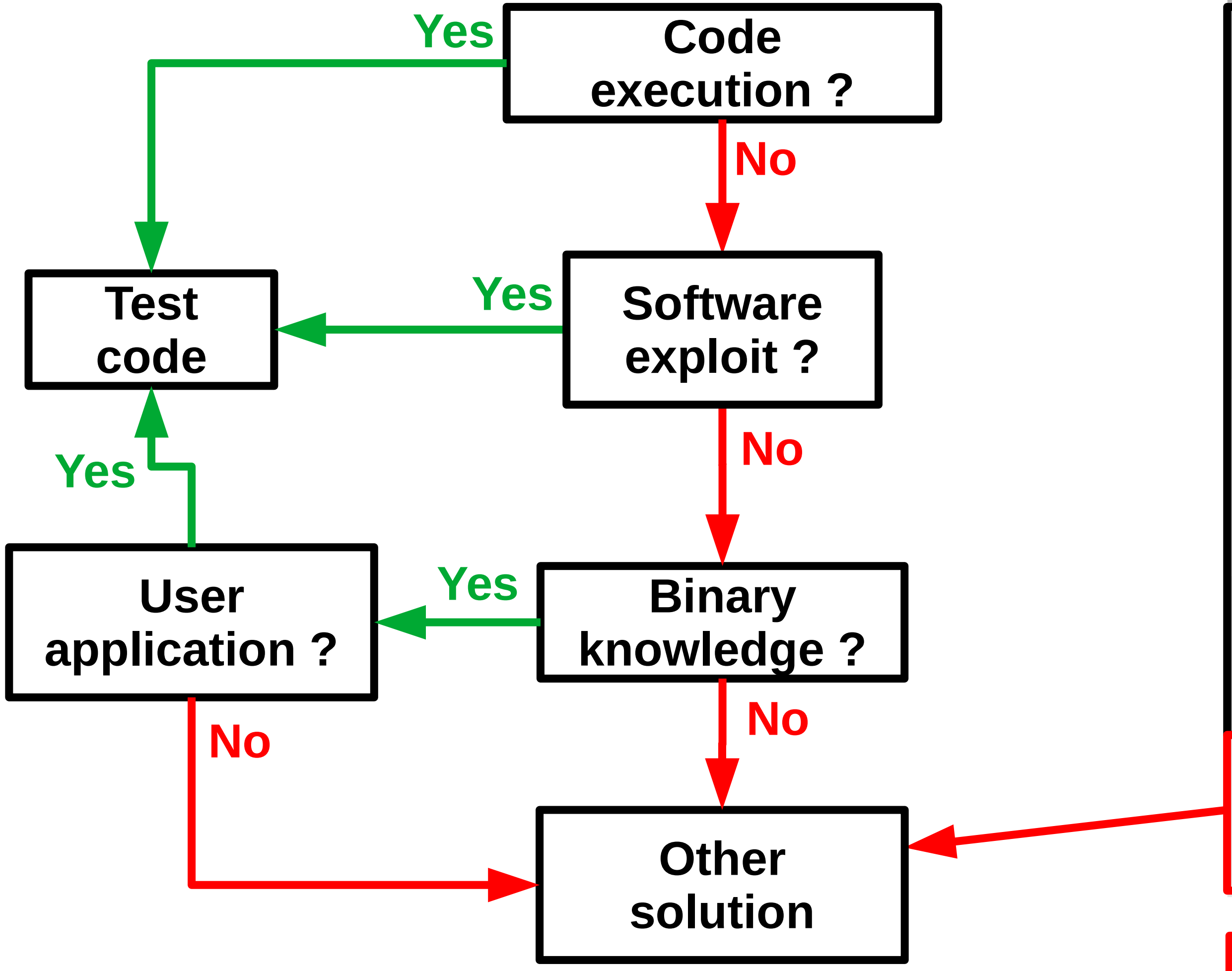
Paper	Context	Issue
Werner et al. (2021) Werner et al. (2022) Wu et al. (2020) Maldini et al. (2019) Carpi et al. (2014) Bozzato et al. (2019) Gaine et al. (2020) ...	**White Box**	**Not a realistic scenario for an attacker**
Kuhnapfel et al. (2022) Vasselle et al. (2017)	**Software exploit to gain code execution**	**Not always feasible**
Van den Herrewegen et al. (2021)	**Binary dumped and executed at application level**	**Execution context different**

Related works



Paper	Context	Issue
Werner et al. (2021) Werner et al. (2022) Wu et al. (2020) Maldini et al. (2019) Carpi et al. (2014) Bozzato et al. (2019) Gaine et al. (2020) ...	**White Box**	**Not a realistic scenario for an attacker**
Kuhnapfel et al. (2022) Vasselle et al. (2017)	**Software exploit to gain code execution**	**Not always feasible**
Van den Herrewegen et al. (2021)	**Binary dumped and executed at application level**	**Execution context different**
Madau (2019) Madau et al. (2018) Probst et al. (2024)	**EM Side-Channel to localise EMFI sensitive areas**	**Only works with EMFI**

Related works



Paper	Context	Issue
Werner et al. (2021) Werner et al. (2022) Wu et al. (2020) Maldini et al. (2019) Carpi et al. (2014) Bozzato et al. (2019) Gaine et al. (2020) ...	White Box	Not a realistic scenario for an attacker
Kuhnapfel et al. (2022) Vasselle et al. (2017)	Software exploit to gain code execution	Not always feasible
Van den Herrewegen et al. (2021)	Binary dumped and executed at application level	Execution context different
Madau (2019) Madau et al. (2018) Probst et al. (2024)	EM Side-Channel to localise EMFI sensitive areas	Only works with EMFI

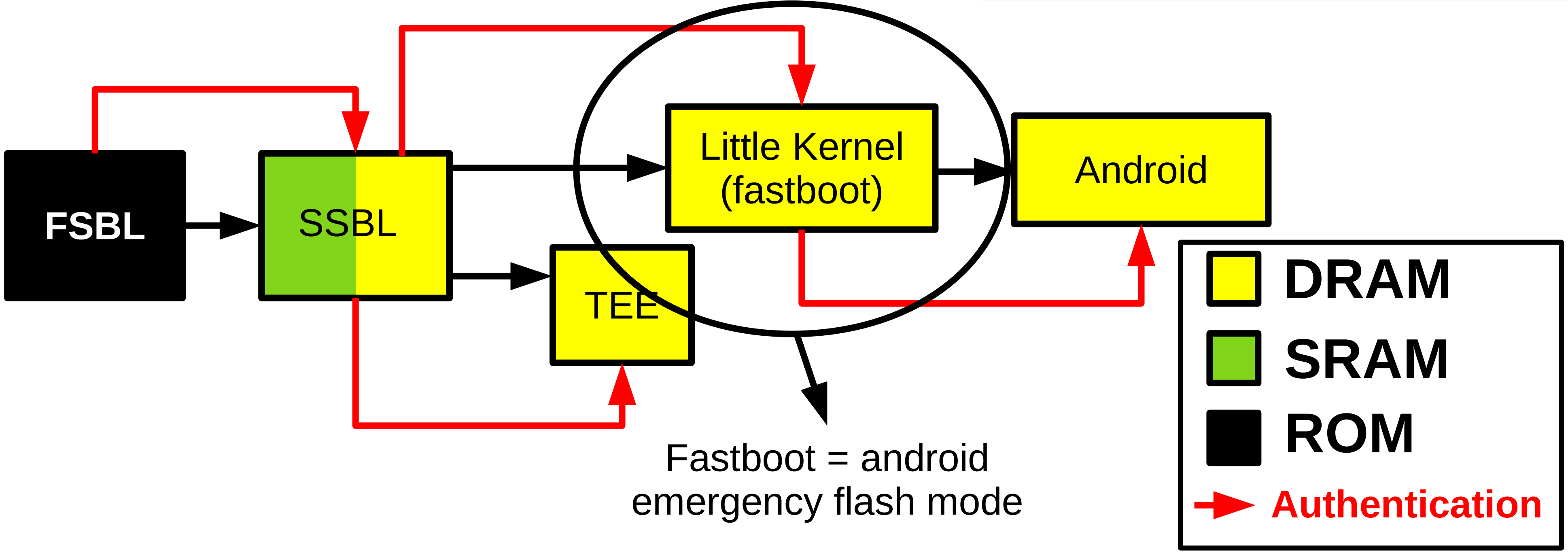
How to find Fault Injection parameters without having code execution privileges ?

Target

<u>Target:</u> Smartphone System-on-Chip

- 8 cores Cortex A53 (28nm)
- Frequency up to 1.4GHz (800MHz)
- **Secure-Boot enabled**

<u>Objective:</u>
Find EMFI parameters value despite not having code execution privileges



Fastboot = android emergency flash mode

Methodology

Step 0 (optional):

Side-Channel map

Step 1 (optional):

Crash map

Step 2:

Loop identification (Side-Channel Analysis)

Step 3:

Fault Injection parameters scan using the identified loop as test code.

Proof of concept:

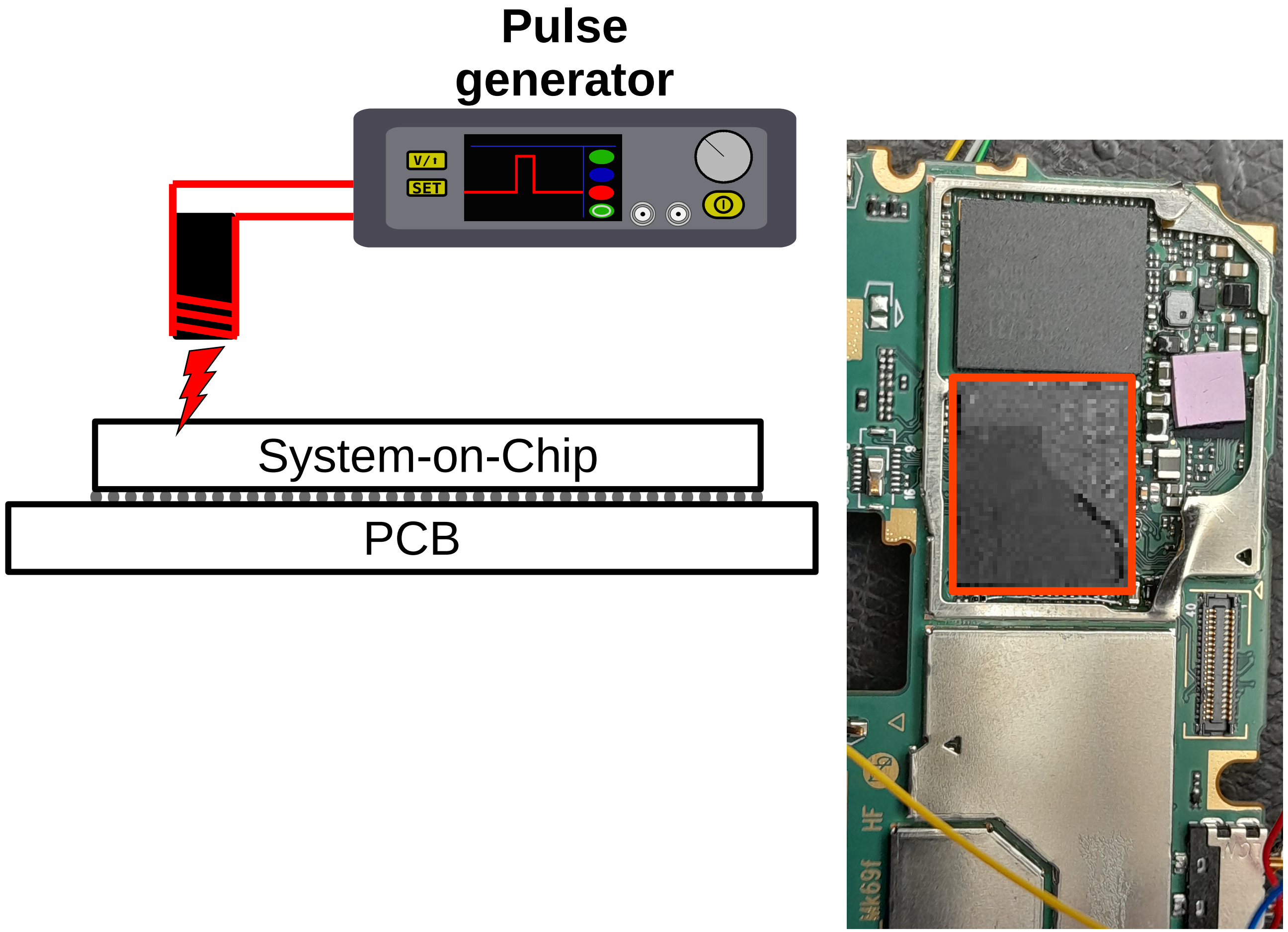
Authentication function bypassed

Parameters researched:

1. Probe position (XY)
2. Pulse parameters
    2.1 Amplitude
    2.2 Width

Methodology

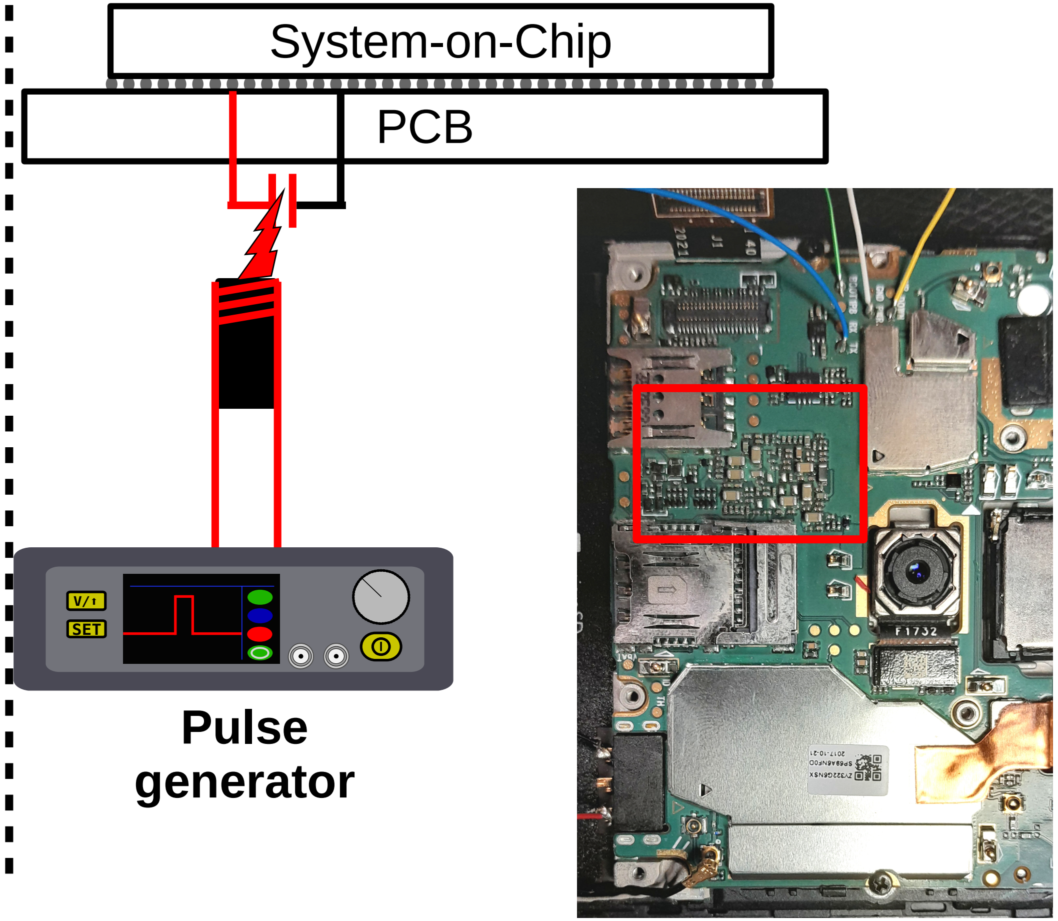
EMFI applied above the SoC and above the decoupling capacitors :



Pulse generator

System-on-Chip

PCB



System-on-Chip

PCB

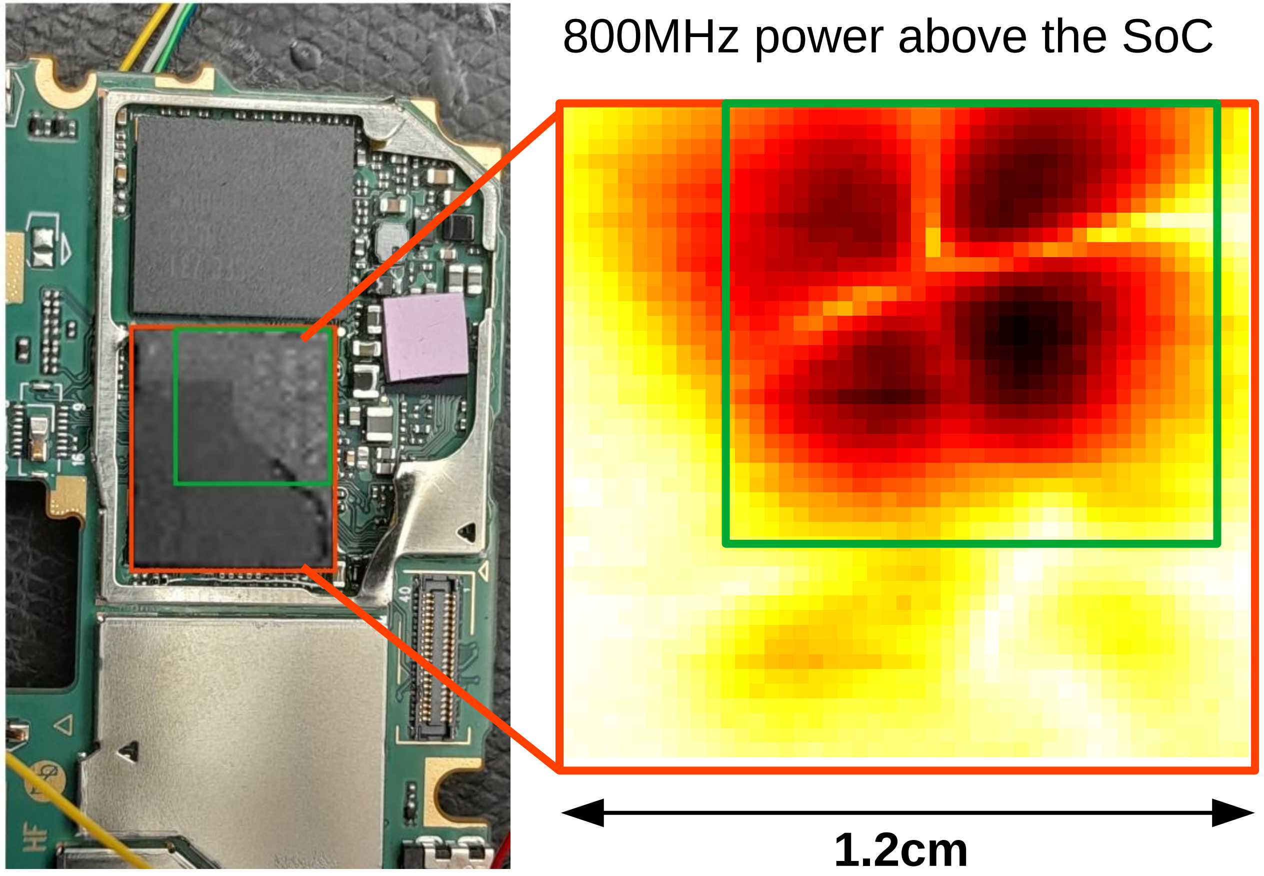
Pulse generator

Methodology

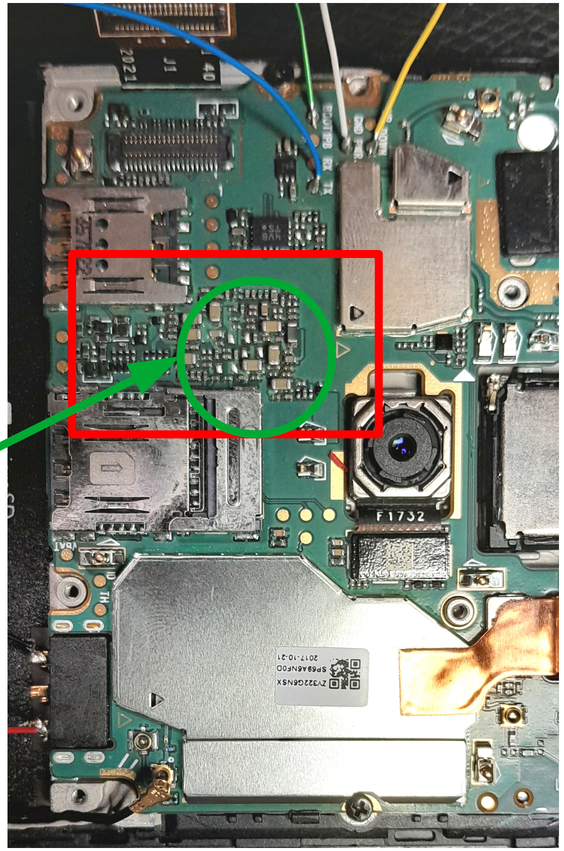
Step 0: Side-Channel Analysis

Side-Channel scan above the SoC

800MHz power above the SoC



Side-Channel scan above the decoupling capacitors



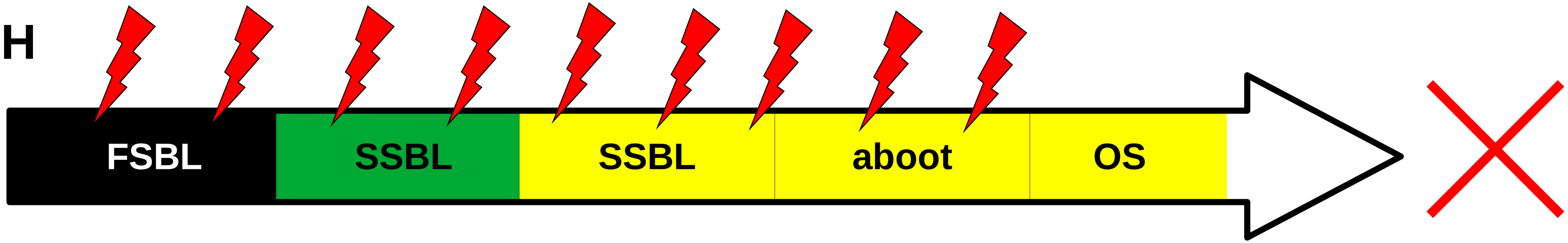
Rough Side-Channel position

Methodology

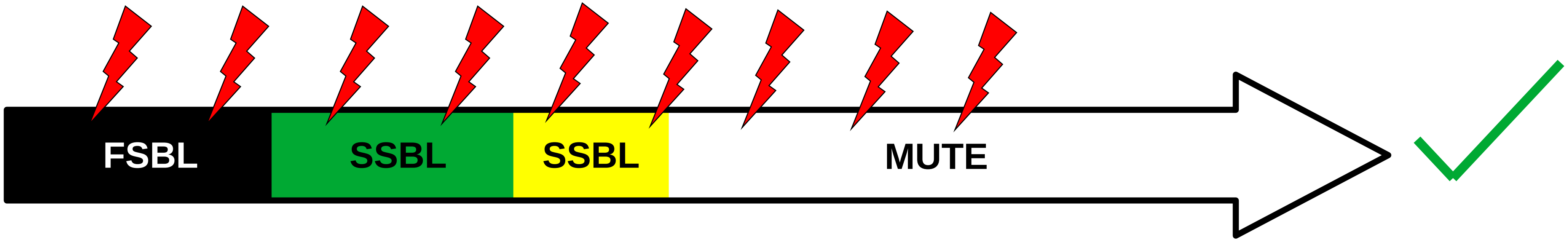
Step 1: Crash map

⇒ Put the target under high stress, then eliminate position where no effect are induced

- **NO CRASH**



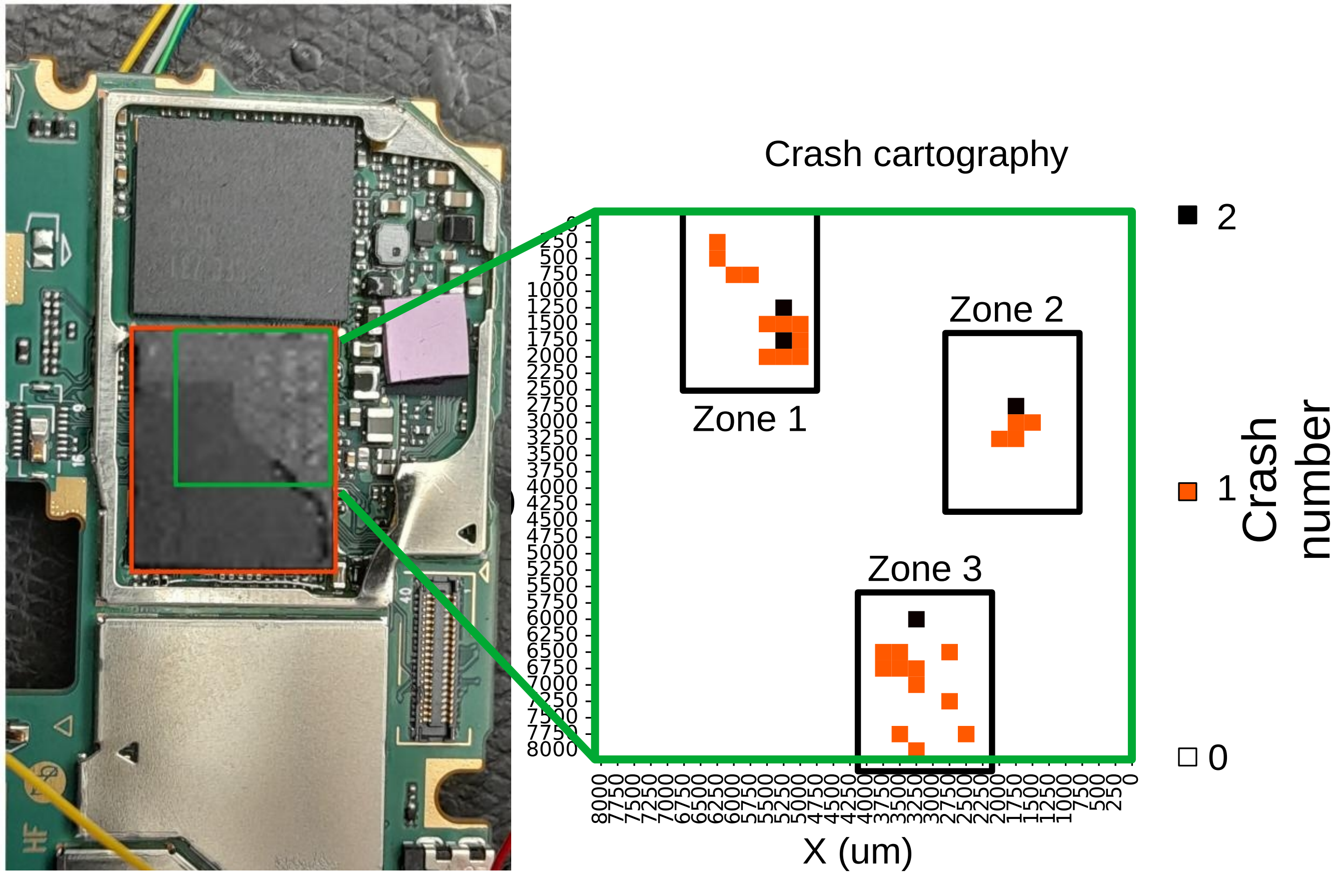
- **CRASH**



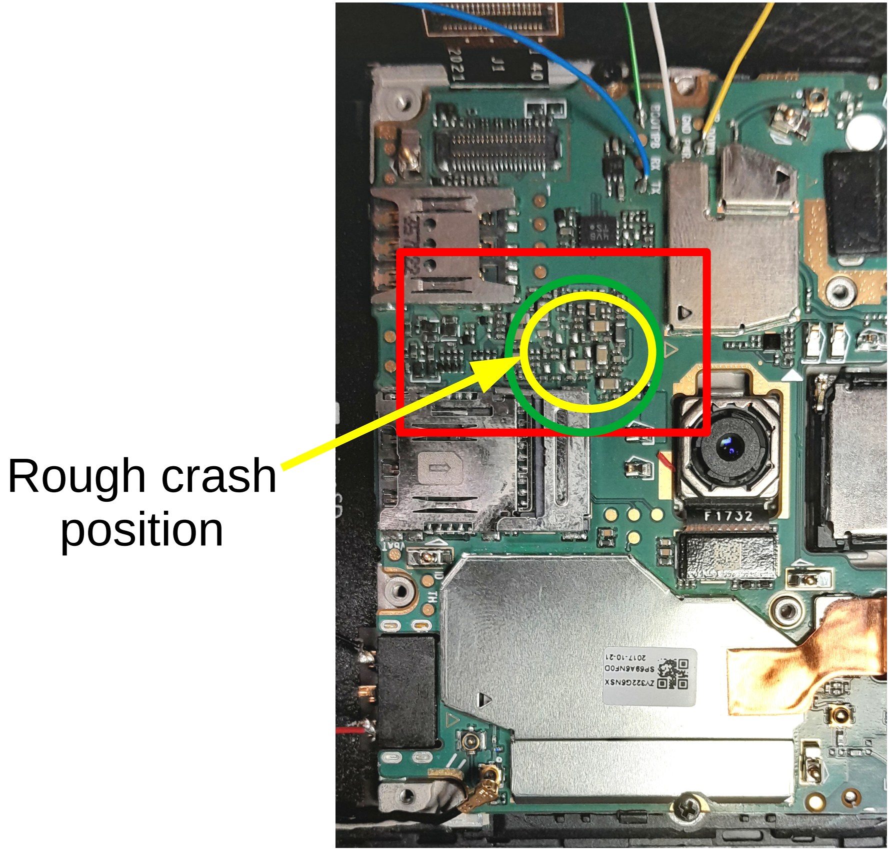
Methodology

Step 1: Crash map

Crash scan above the SoC



Crash scan above the decoupling capacitors



Methodology

Step 0 and 1 ⇒ Allow to roughly identify interesting EMFI spots

Issue:

⇒ Still need to identify:

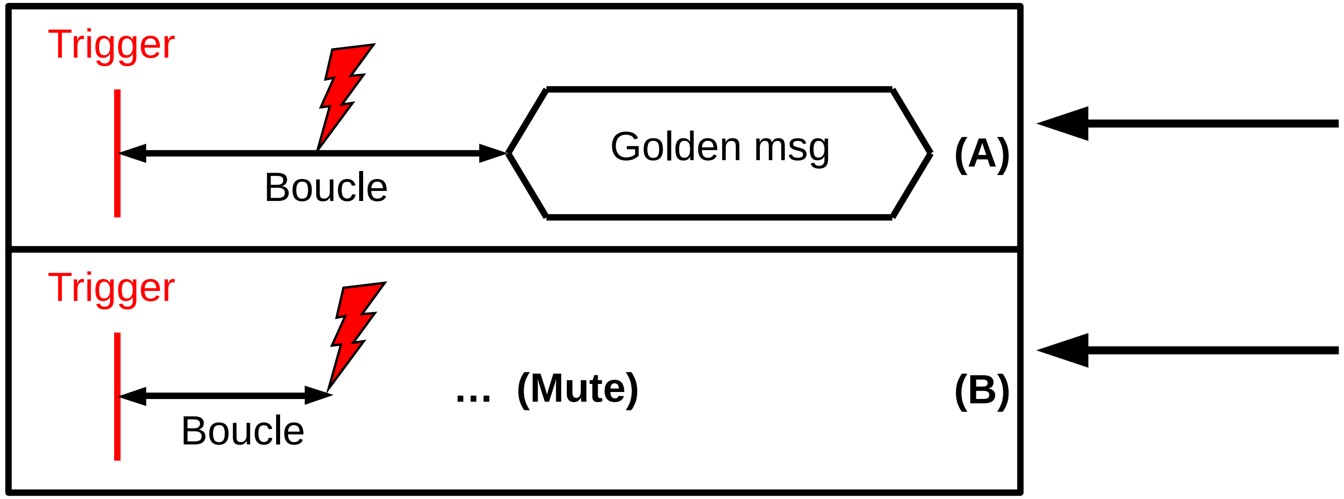
- Accurate probe position
- Pulse parameters

Solution: EMFI during a loop

Methodology

Fault Injection during a loop

Golden msg = expected message when no fault are injected



Injection effects :

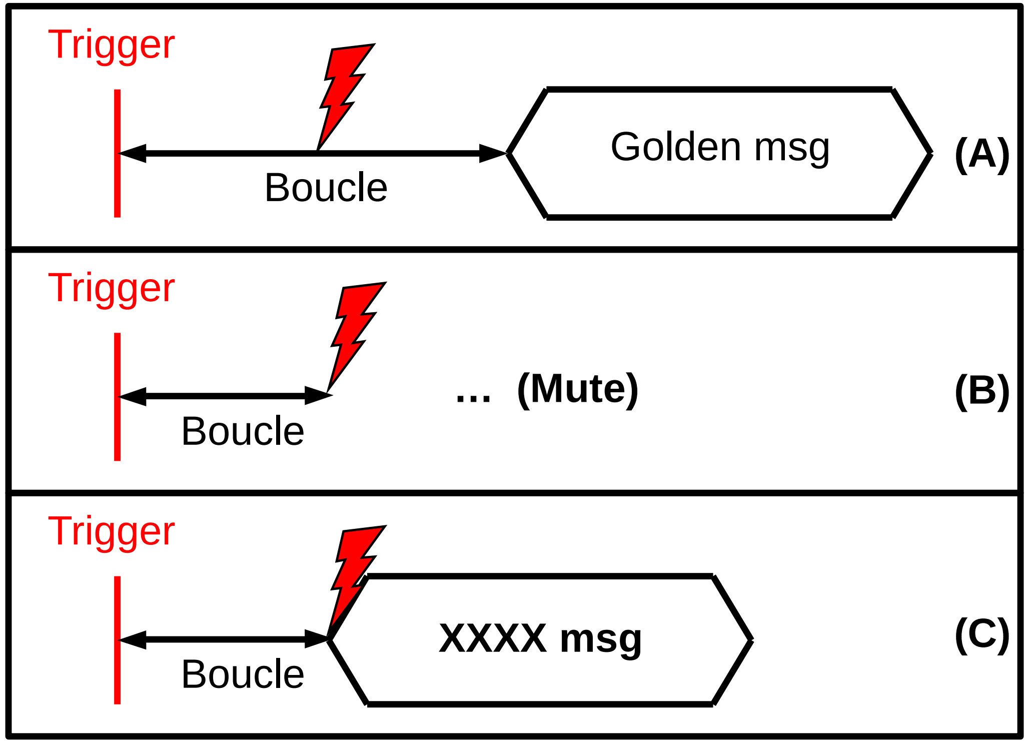
1. No effect detected

2 . Crash detected

Methodology

Fault Injection during a loop

Golden msg = expected message when no fault are injected



Injection effects :

1. No effect detected

2 . Crash detected

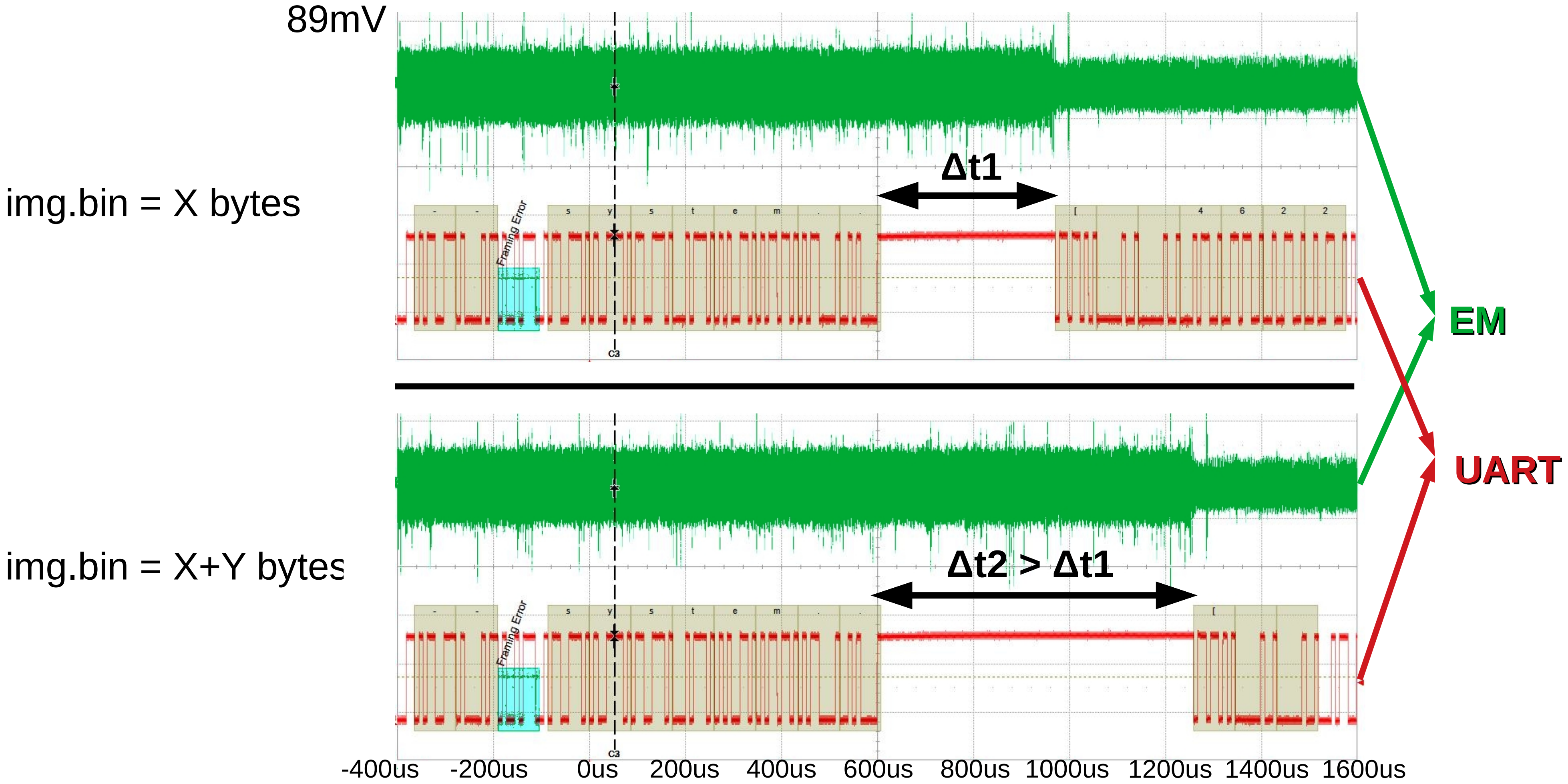
3. Fault Injected
   Control-Flow deviation

Side-Channel traces can be used instead of communication bus

Methodology

Step 2: Loop identification in the existing code

$fastboot flash system img.bin ⇒ Flash system partition with img.bin

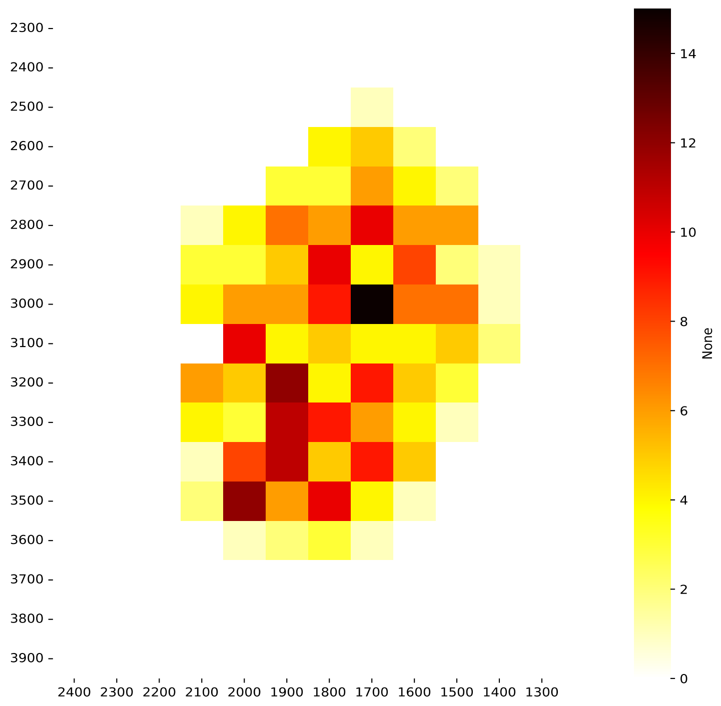


Methodology

Step 3: Fault Injection during the loop

Golden msg = expected message when no fault are injected

Zone 2



Injection effects :

1. No effect detected

2 . Crash detected

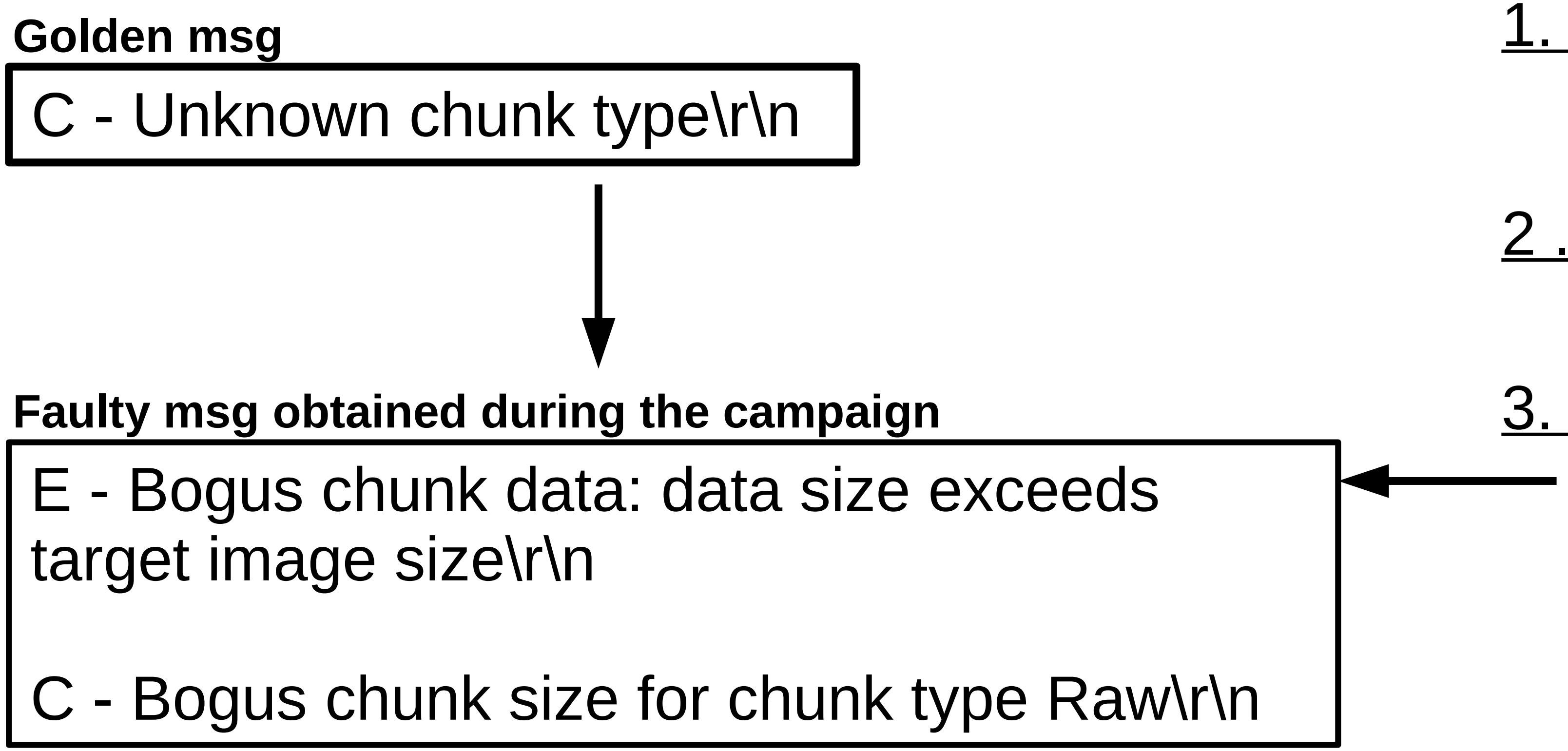
3. Fault Injected

Control-Flow deviation

Methodology

Step 3: Fault Injection during the loop

Golden msg = expected message when no fault are injected



Golden msg

C - Unknown chunk type\r\n

Faulty msg obtained during the campaign

E - Bogus chunk data: data size exceeds target image size\r\n

C - Bogus chunk size for chunk type Raw\r\n

Injection effects :

1. No effect detected

2 . Crash detected

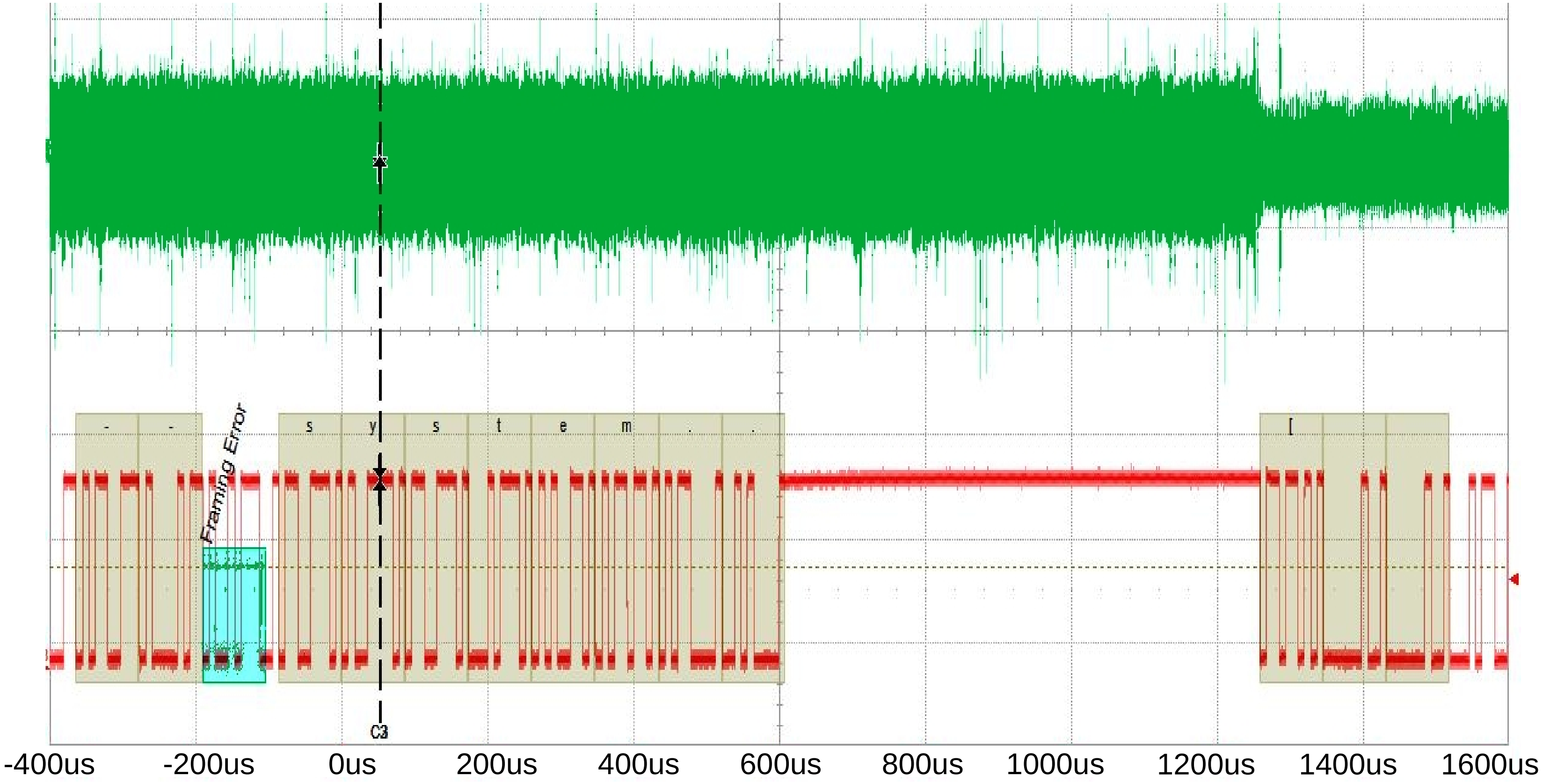
3. Fault Injected

Control-Flow deviation

Methodology

Step 3: Fault Injection during the loop

Loop without EMFI

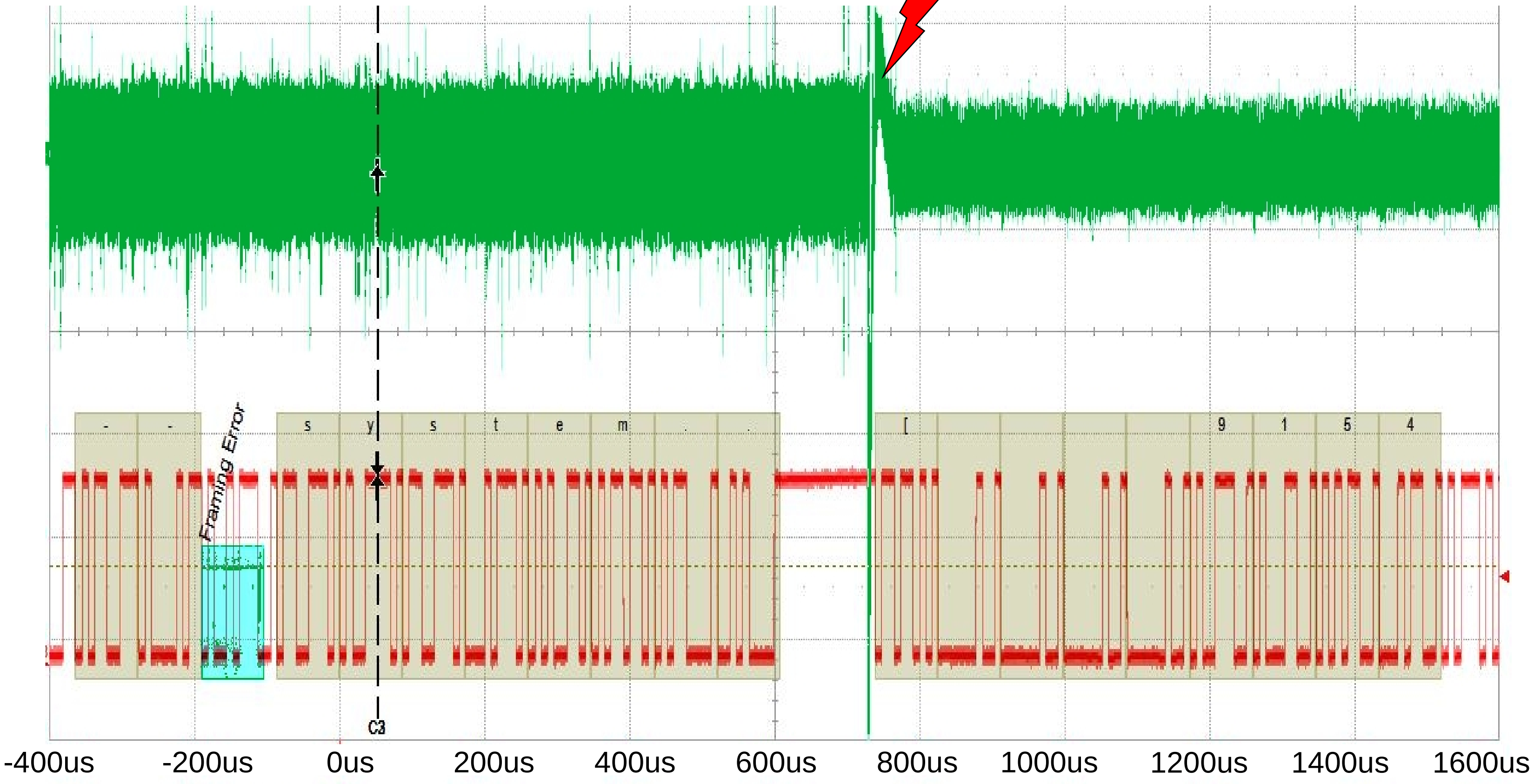


Methodology

Step 3: Fault Injection during the loop

Loop with EMFI

EMFI



Methodology

Step 3 above the decoupling capacitors :

EMFI parameters :

- Probe position (XYZ) ✓ → Crash cartography highlighted **only one area** above the decoupling capacitors.
- Pulse parameters
  - Pulse width
  - Pulse amplitude

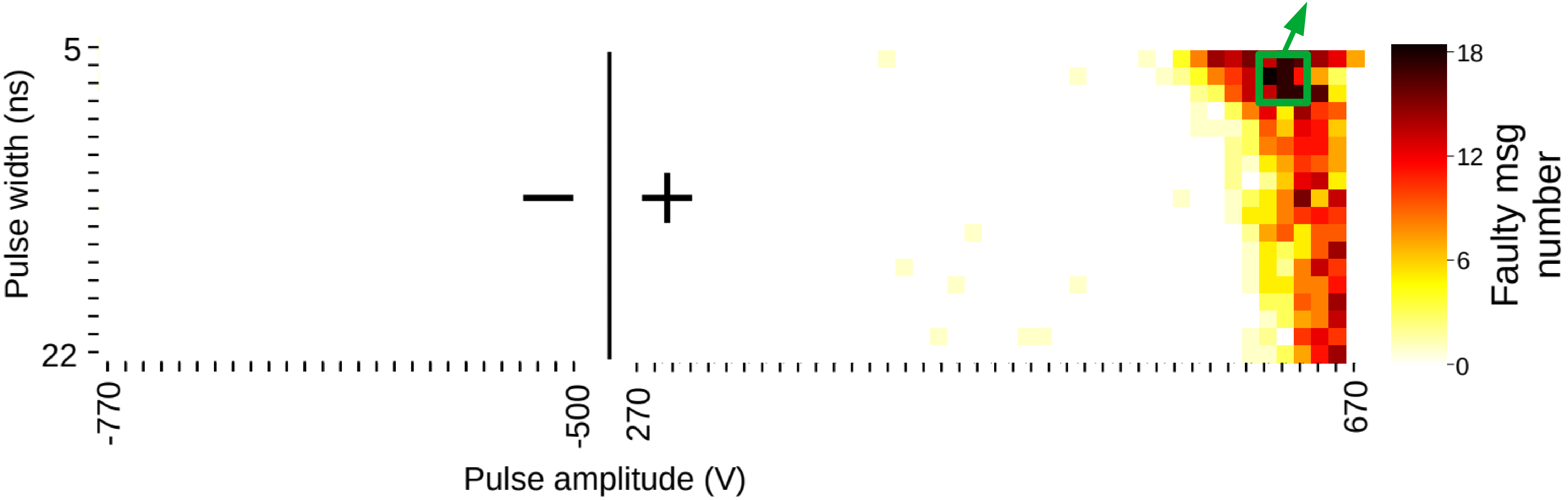
?

Methodology

Step 3 above the decoupling capacitors :

Pulse parameters scan (Faulty msg map)

Best pulse parameters to induce faulty messages



Methodology

Same procedure applied above the decoupling capacitors of the target :

EMFI parameters :

- Probe position (XYZ) ✓
- Pulse parameters ✓
  - Pulse width
  - Pulse amplitude

Methodology validation:

Firmware Update : Authentication function bypassed using the EMFI parameters identified

Conclusion

Contributions:

Methodology proposed to find suitable Fault Injection parameters based on:

- **EM Side-Channel analysis to reduce spatial exploration (Madau2018, Probst2024).**
- **Crash map to further reduce spatial exploration and highlight sensitive area.**
- **Fault Injection during loop in the target original code to induce control-flow deviation.**

Conclusion

<u>Contributions:</u>

Methodology proposed to find suitable Fault Injection parameters based on:

- **EM Side-Channel analysis to reduce spatial exploration (Madau2018, Probst2024).**
- **Crash map to further reduce spatial exploration and highlight sensitive area.**
- **Fault Injection during loop in the target original code to induce control-flow deviation.**

Proof of concept :

- **Smartphone without code execution privileges**
- **Image authentication bypass using the EMFI parameters identified.**

Conclusion

Contributions:

Methodology proposed to find suitable Fault Injection parameters based on:

- **EM Side-Channel analysis to reduce spatial exploration (Madau2018, Probst2024).**
- **Crash map to further reduce spatial exploration and highlight sensitive area.**
- **Fault Injection during loop in the target original code to induce control-flow deviation.**

Proof of concept :

- **Smartphone without code execution privileges**
- **Image authentication bypass using the EMFI parameters identified.**

Futur works:

- **Apply this methodology in other context**
  - **⇒ No UART/communication bus from the target : only Side-Channel allowed**
  - **⇒ Use this methodology with other Fault Injection method than EMFI**
- **Apply this methodology on modern smartphones**
- **Use other parameters search strategy to quickly converge towards a solution**

Thank you for your attention.

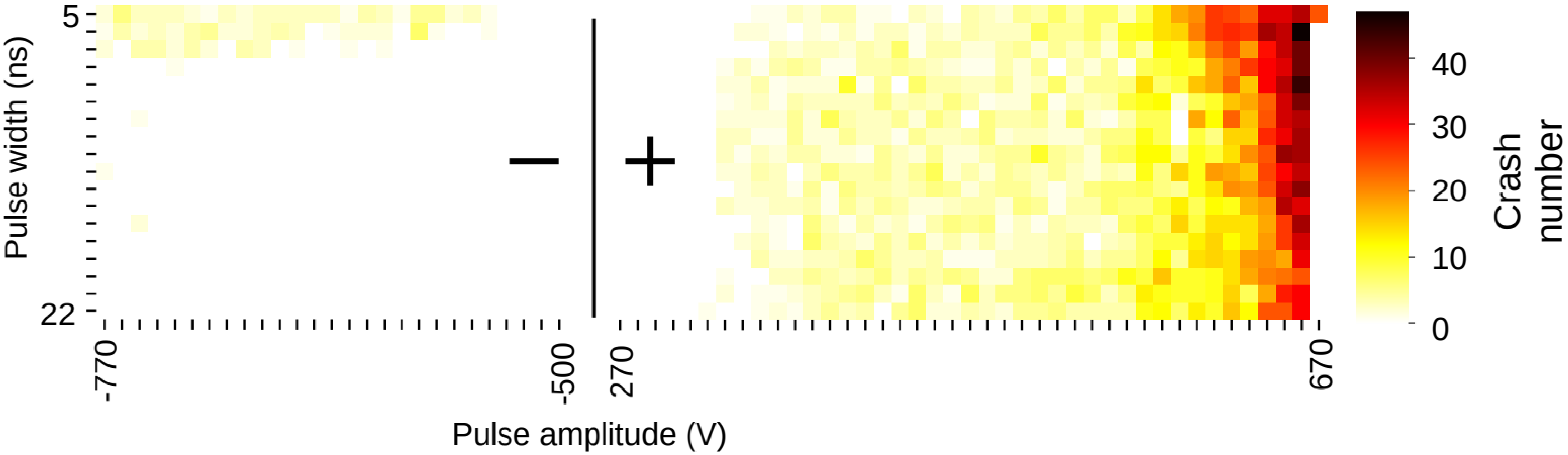
Clément Fanjas

clement.fanjas@cea.fr

Methodology

Step 3 above the decoupling capacitors :

Pulse parameters scan
(CRASH map)



Proof of concept

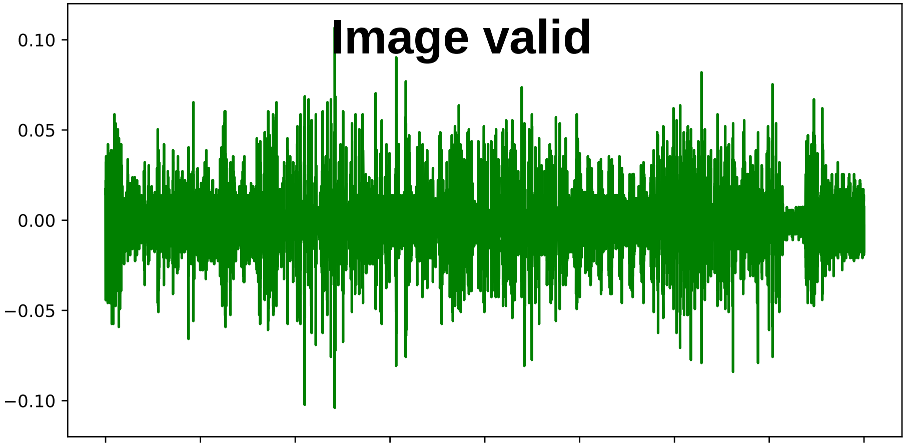
Authentication of recovery image during flash

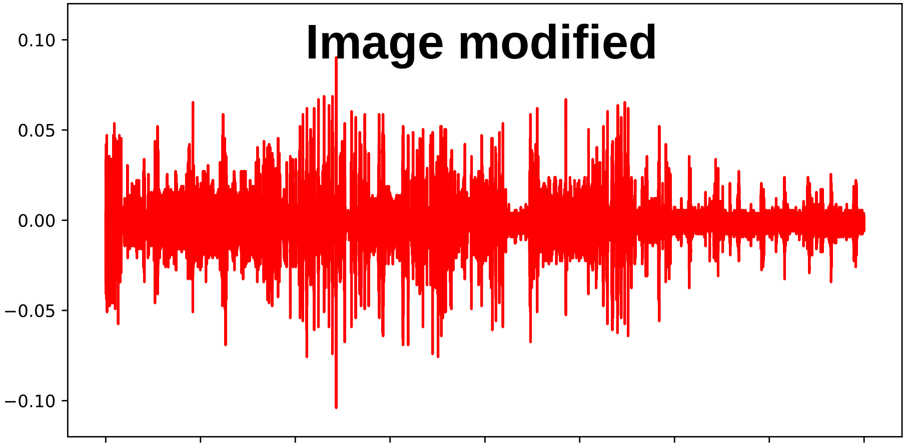
$fastboot flash recovery img.bin

	Image valid	Image modified
UART	I - cmd: flash:recovery I - SSM validating recovery ssm_en_hab = 1 **I - start flashing image recovery** I - erasing recovery I - Erasing card: 0x74000:0x6000	I - cmd: flash:recovery I - SSM validating recovery ssm_en_hab = 1 E - HAB check fail 0x56 **E - Failed to verify hab image recovery**
USB	sending 'recovery' (16484 KB)… OKAY [0.555s] writing 'recovery'… OKAY [0.689s] **finished. total time: 1.244s**	sending 'recovery' (16484 KB)… OKAY [0.541s] writing 'recovery'… **(bootloader) Image recovery failed validation** (bootloader) Preflash validation failed FAILED (remote failure) finished. total time: 0.718s

Proof of concept

Authentication of recovery image during flash





Proof of concept

Authentication of recovery image during flash

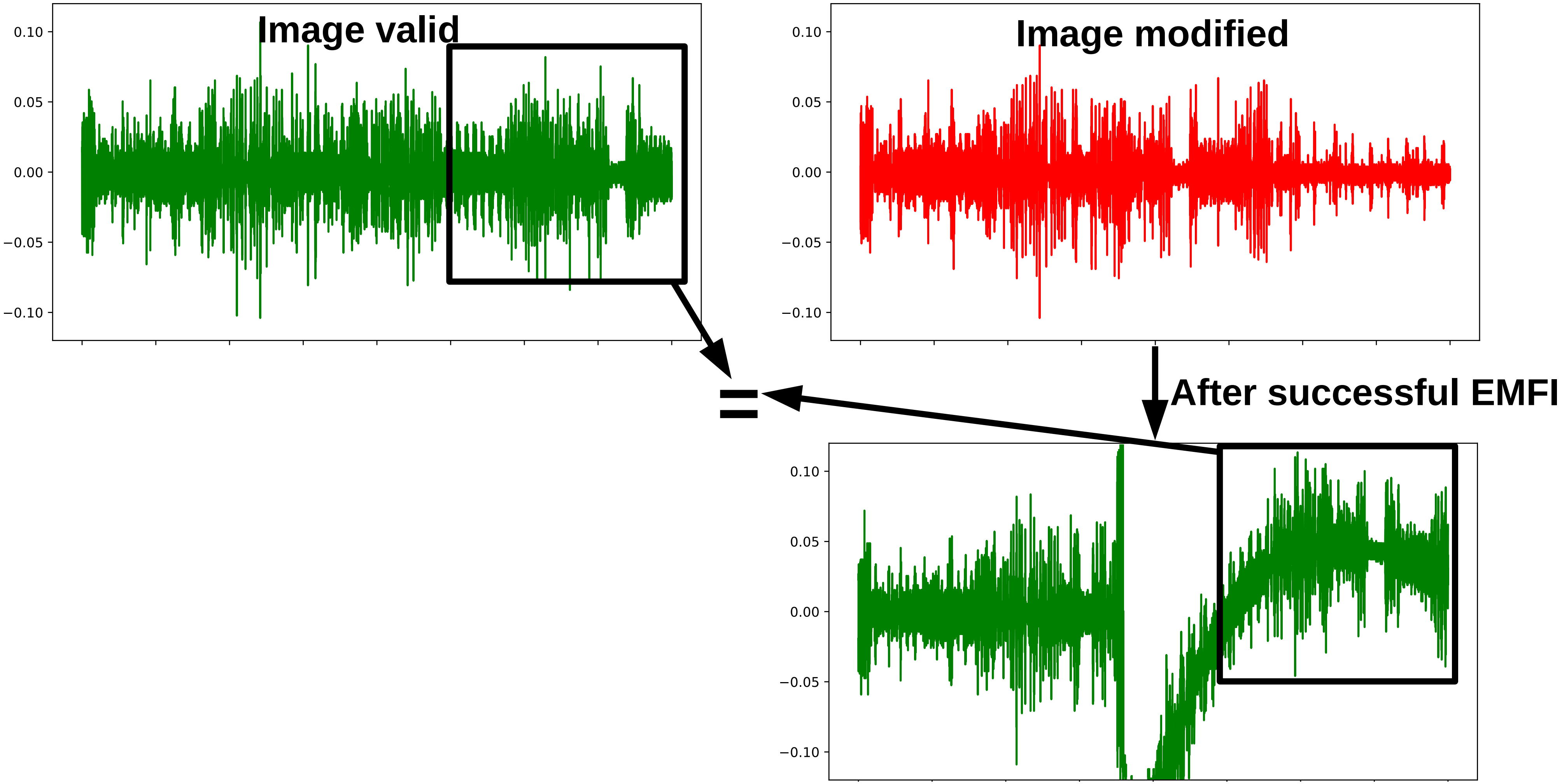


Image valid

Image modified

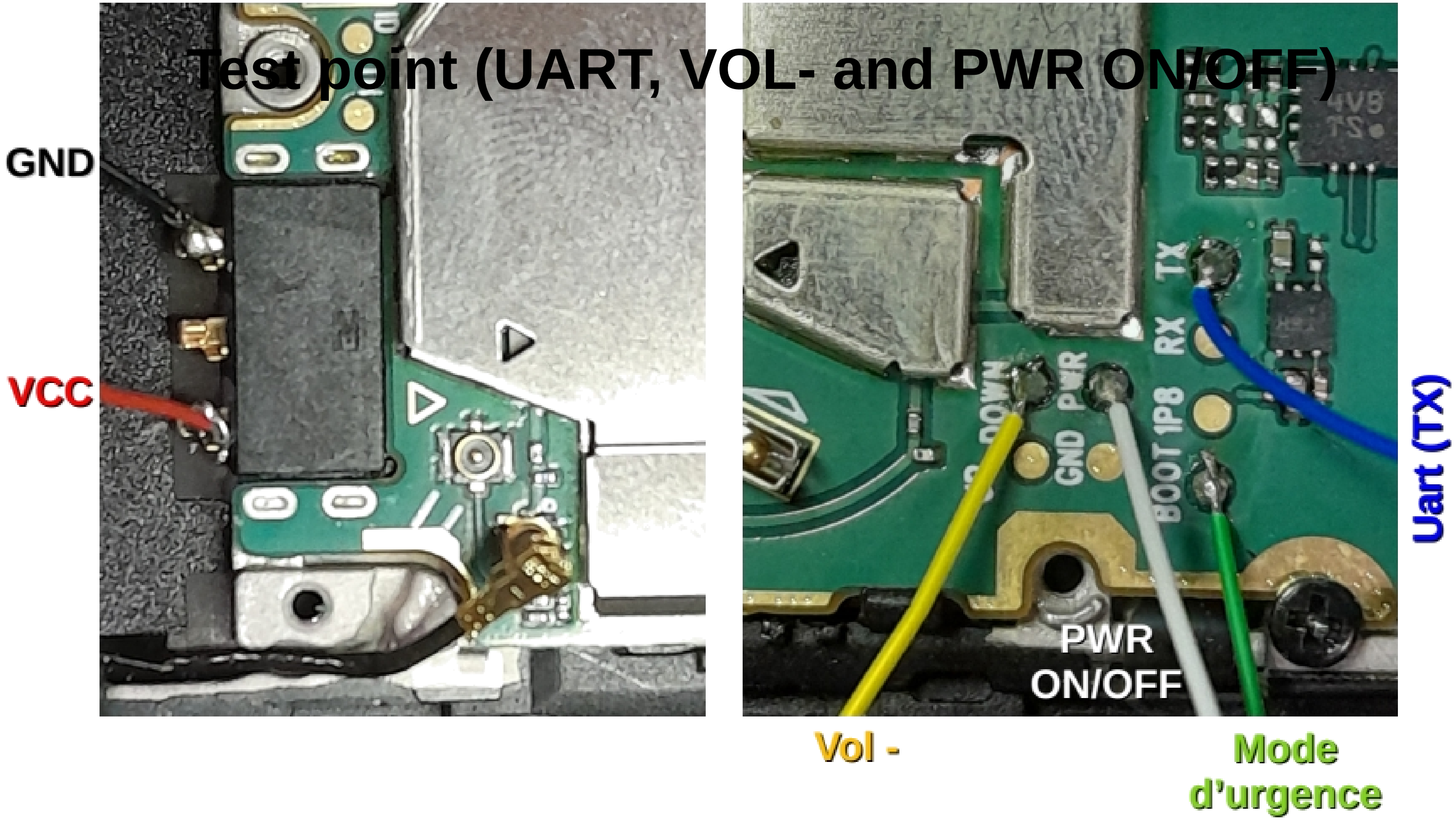
After successful EMFI

=

Methodology

Target: Smartphone System-on-Chip

Test point (UART, VOL- and PWR ON/OFF)



Methodology

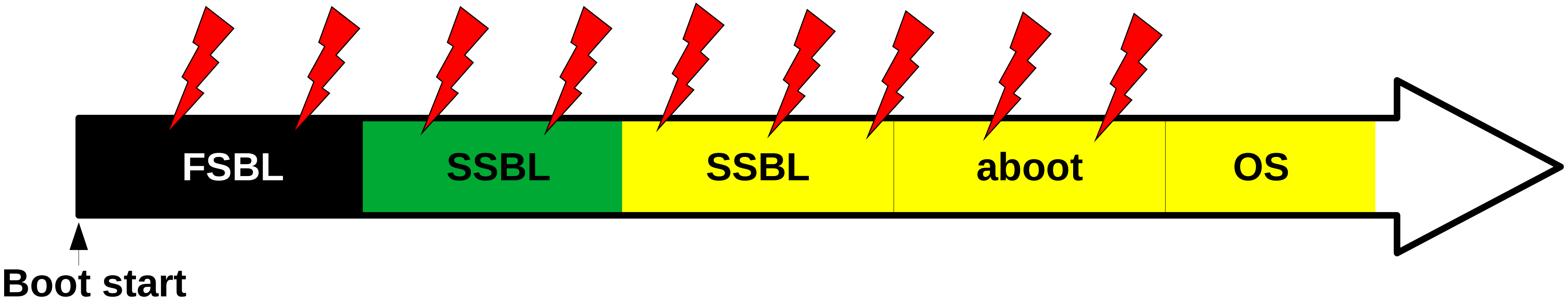
Step 1:

- Procedure

  ⇒ Moving the probe above the target while injecting several high amplitude pulses during the boot.

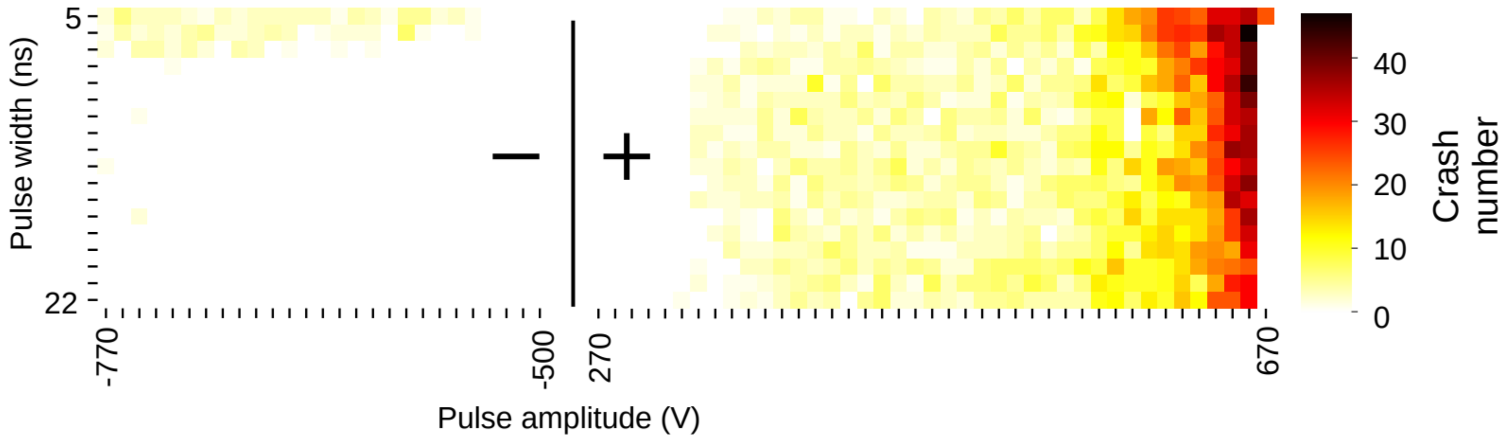
- Motivation

  ⇒ If a high stress (high amplitude pulse) is applied several time at the same position without any **CRASH** then its unlikely that fault effect are injected at this position.

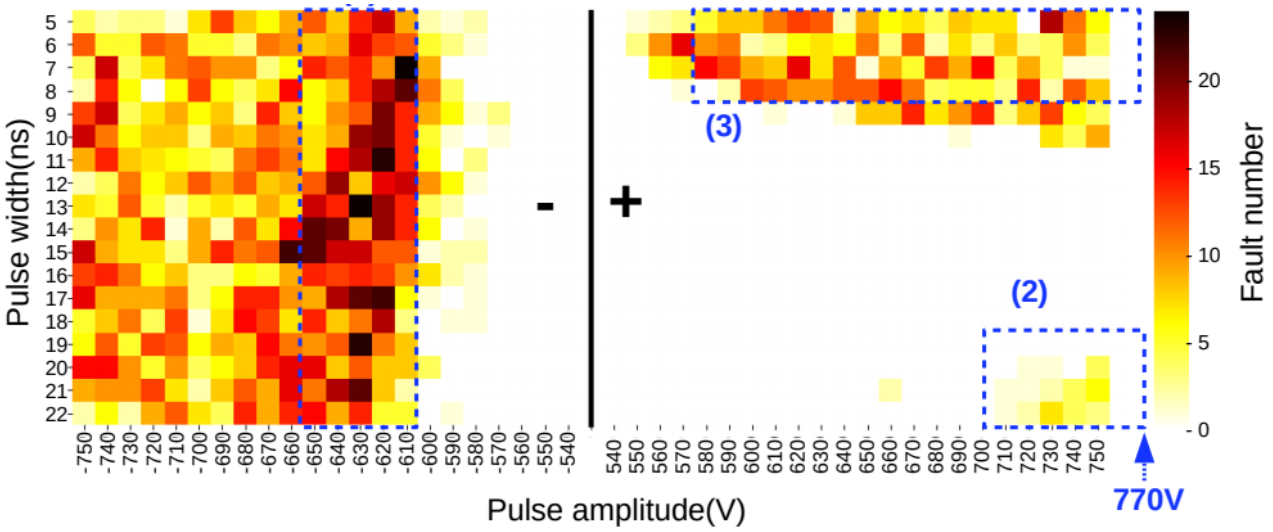


Methodology

Pulse parameters scan (CRASH map)



JAIF2024



FDTC2024 (EMFI above decoupling capacitors: other target)