

---

# Mitigating and Understanding Electromagnetic Fault Injection Using Digital Sensors

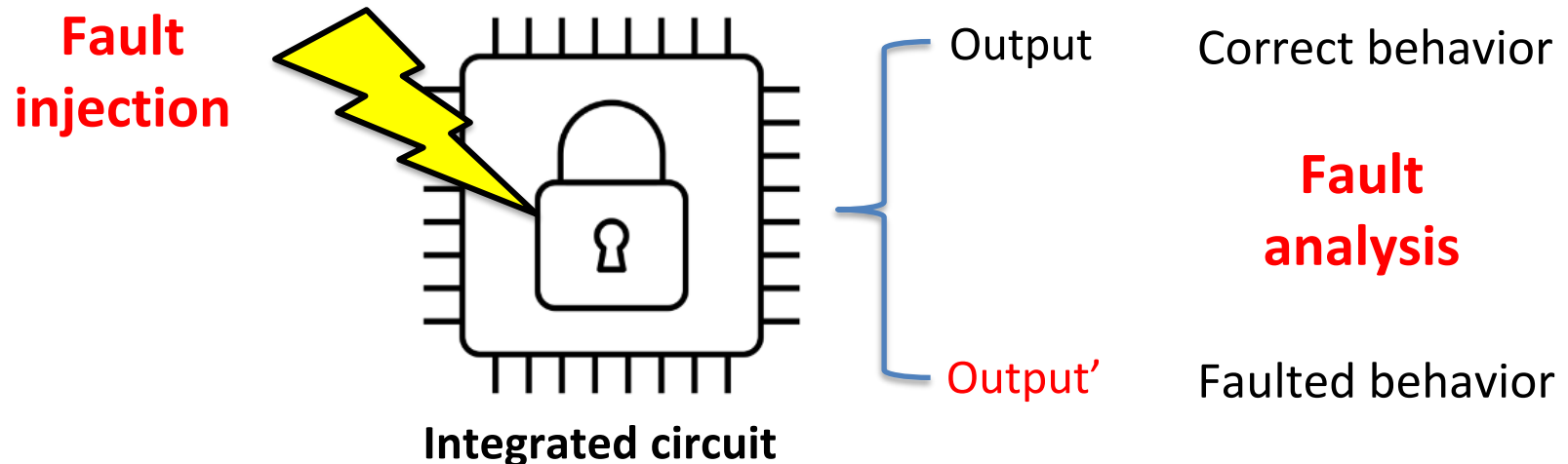
---

Roukoz Nabhan, Jean-Max Dutertre

PHISIC 2025

# Hardware Security

- The Internet Of Things (*IoT*) is about networking physical objects through the Internet
- Sensitive data (passwords and cryptographic keys) exchanged between IoT devices are potentially at risk of being broken by attackers
- Fault Injection Attacks (FIA)

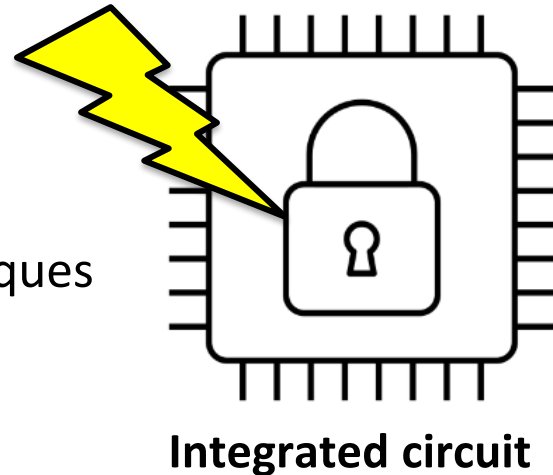


- Securing Integrated Circuit (IC) against fault injection attacks is an ongoing challenge
- Several countermeasures exist, one of which is a **sensor to detect FIA**

# Fault injection techniques

## ➤ Fault injection techniques with **global** impact:

- Underfeeding
- Overclocking
- Overheating
- Aging
- Clock glitching
- Voltage glitching
- Body biasing injection



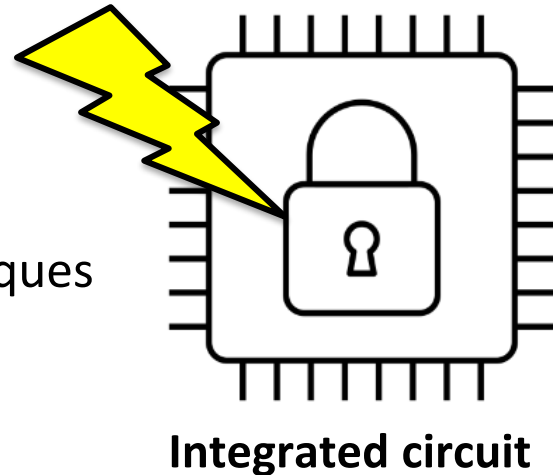
## ➤ Fault injection techniques with **local** impact:

- ElectroMagnetic Fault Injection (EMFI)
- X-Ray fault injection
- Laser Fault Injection (LFI)

# Fault injection techniques

➤ Fault injection techniques with **global** impact:

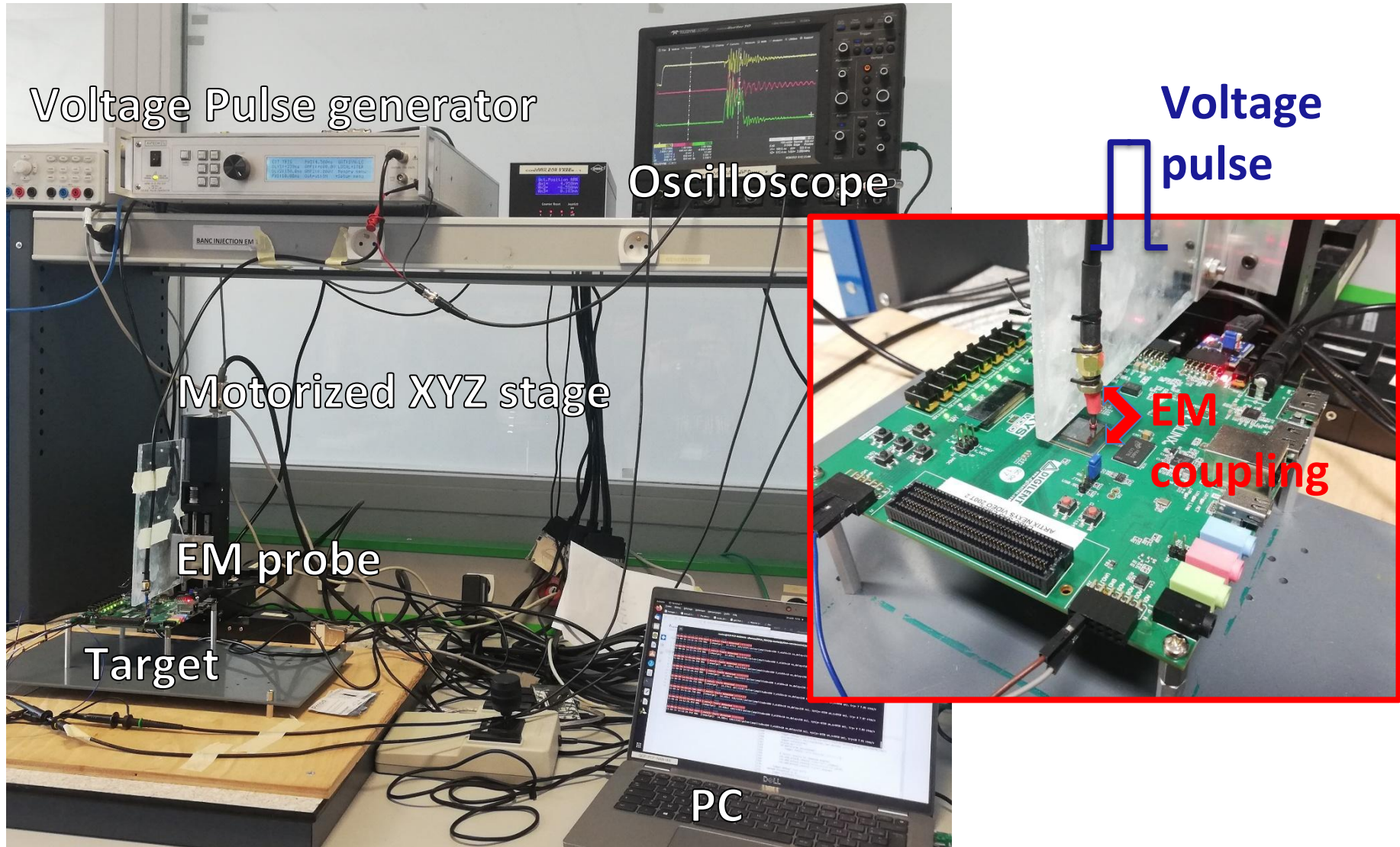
- Underfeeding
- Overclocking
- Overheating
- Aging
- Clock glitching
- Voltage glitching
- Body biasing injection



➤ Fault injection techniques with **local** impact:

- **ElectroMagnetic Fault Injection (EMFI)**
- X-Ray fault injection
- Laser Fault Injection (LFI)

# ElectroMagnetic Fault Injection (EMFI)

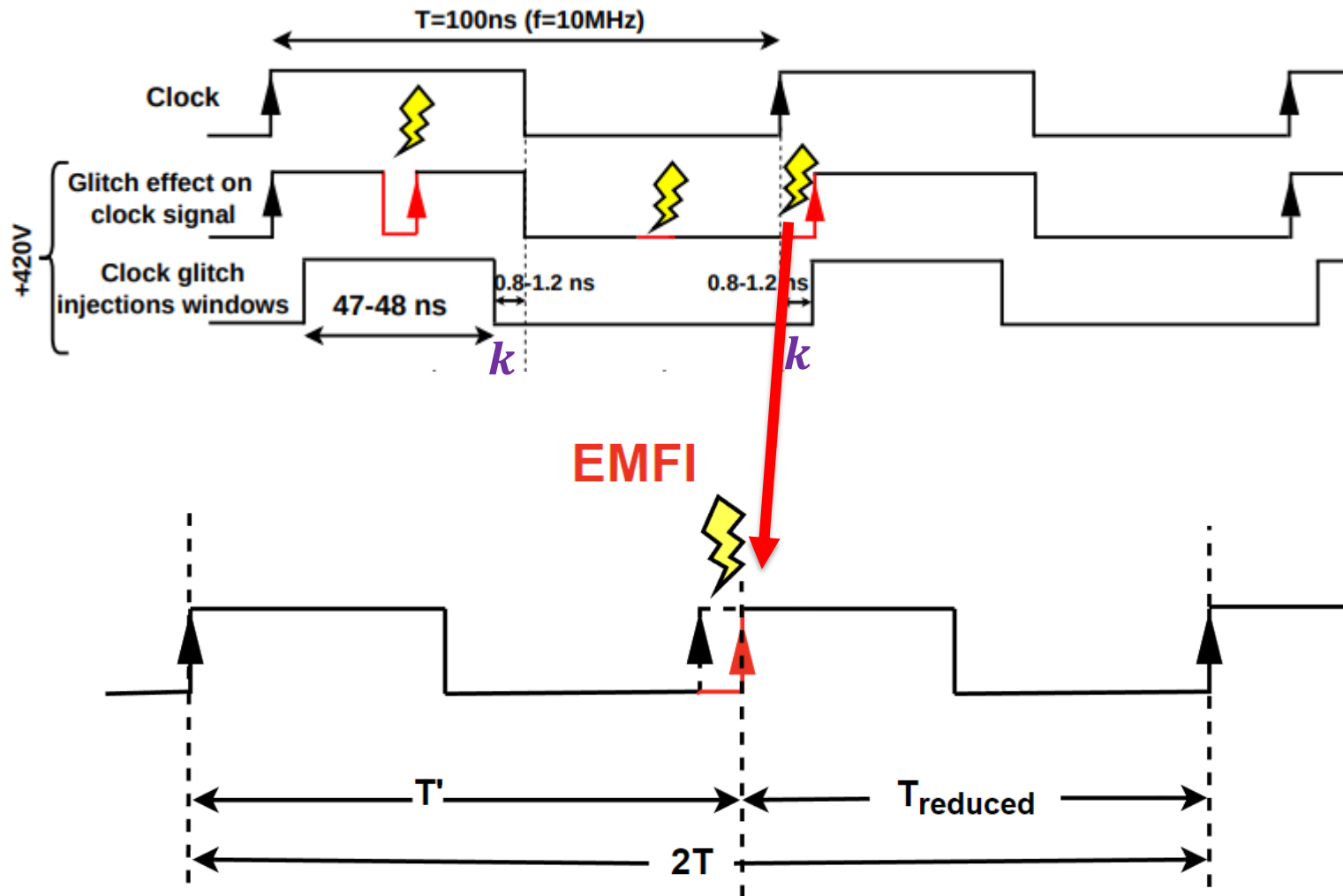


# Outline

- **Previous work: EMFI-induced clock glitches mechanism**
- Novel sensor: Frozen dual-clock detector
- Experimental setup and sensors implementations
- Spatial and temporal exploration of the sensor performance
- Conclusion and perspectives

# EMFI-induced clock glitch principle (+420V)

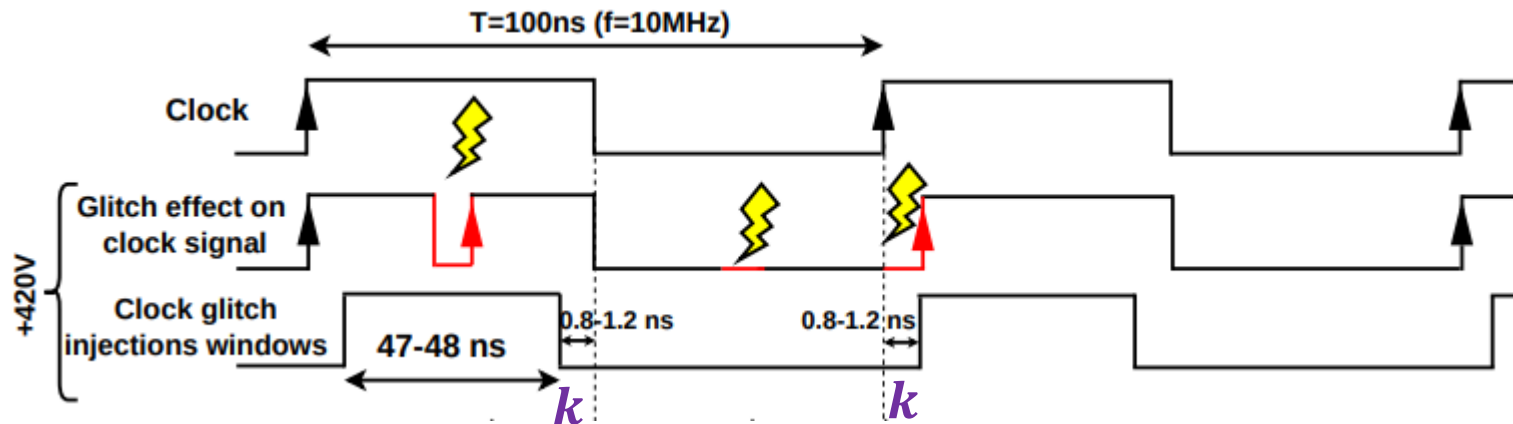
Nabhan et al.<sup>1</sup> demonstrated that EMFI-induced clock glitches on the clock signals



<sup>1</sup>R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "A Tale of Two Models : Discussing the Timing and Sampling EM Fault Injection Models" In 2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). 2023, p. 1-12

# EMFI-induced clock glitch principle (+420V)

Nabhan et al.<sup>1</sup> demonstrated that EMFI-induced clock glitches on the clock signals



The width of the susceptibility window caused by EMFI-induced clock glitches:

$$w_{EMFI} = \frac{T}{2} - 2k$$

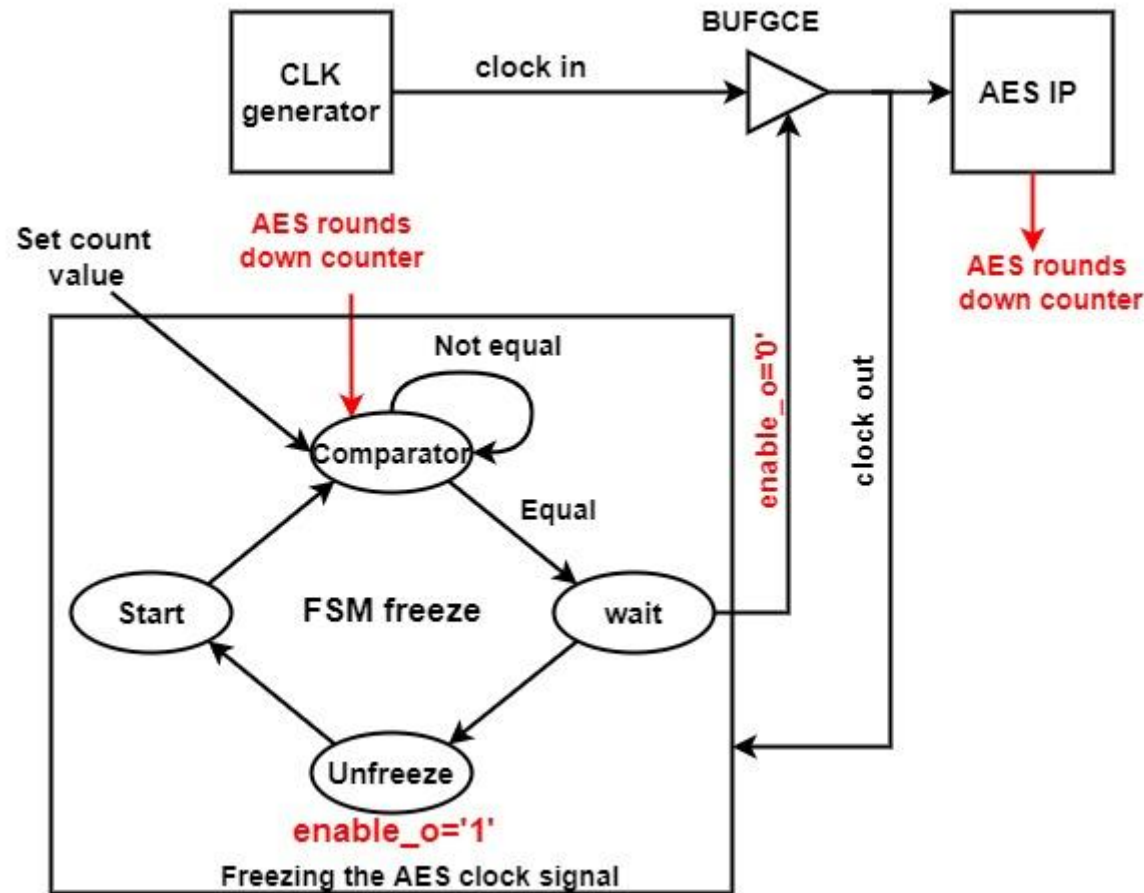
Where  $k$  is a constant margin during which clock edges get a small shift

**Symmetric behavior with a negative voltage pulse**

<sup>1</sup>R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "A Tale of Two Models : Discussing the Timing and Sampling EM Fault Injection Models" In 2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). 2023, p. 1-12



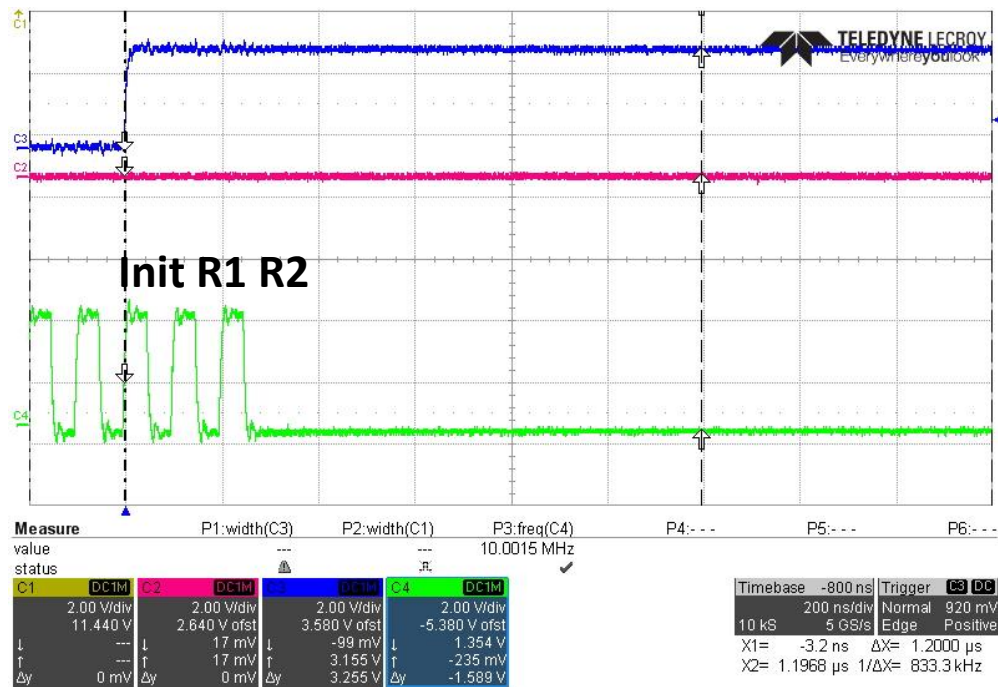
# Test: Freezing the input clock of the AES calculation



An FSM controls the clock enable (CE) of the buffer

# Test: freeze case

Freezing the AES clock signal

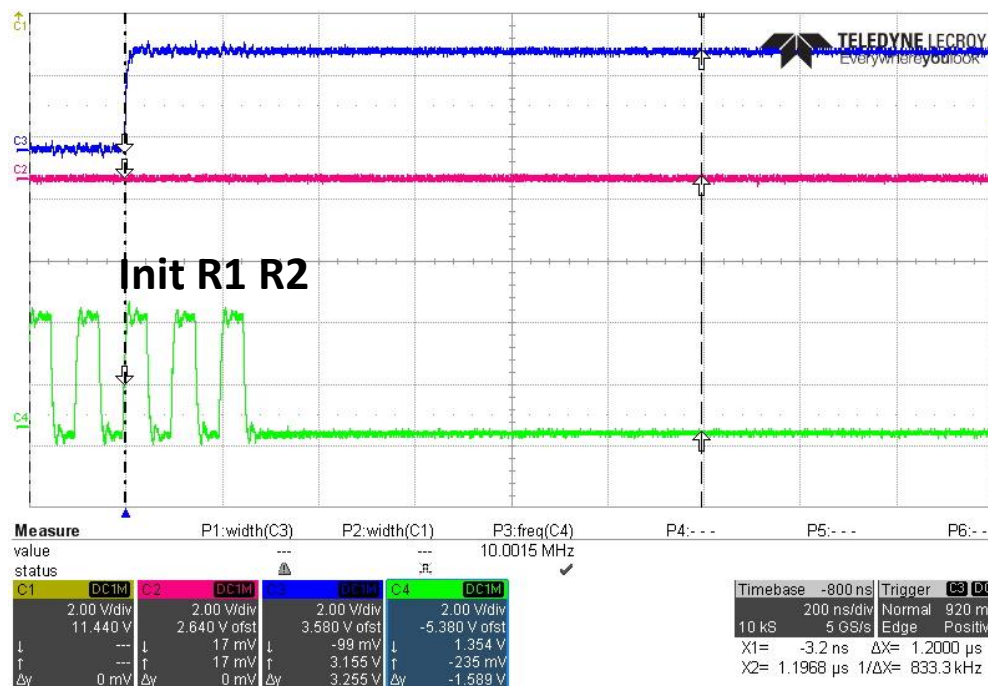


Clock stopped

Pulser: voltage amplitude=-420V, width=4,5 ns

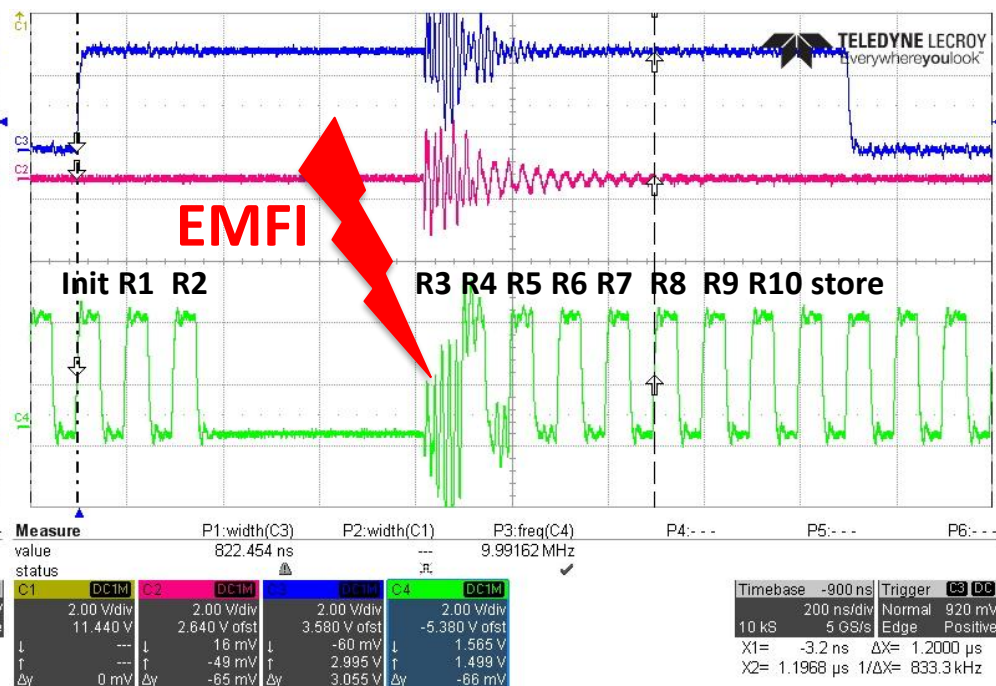
# Test: freeze case

Freezing the AES clock signal



Clock stopped

Unfreezing the clock by EMFI attack



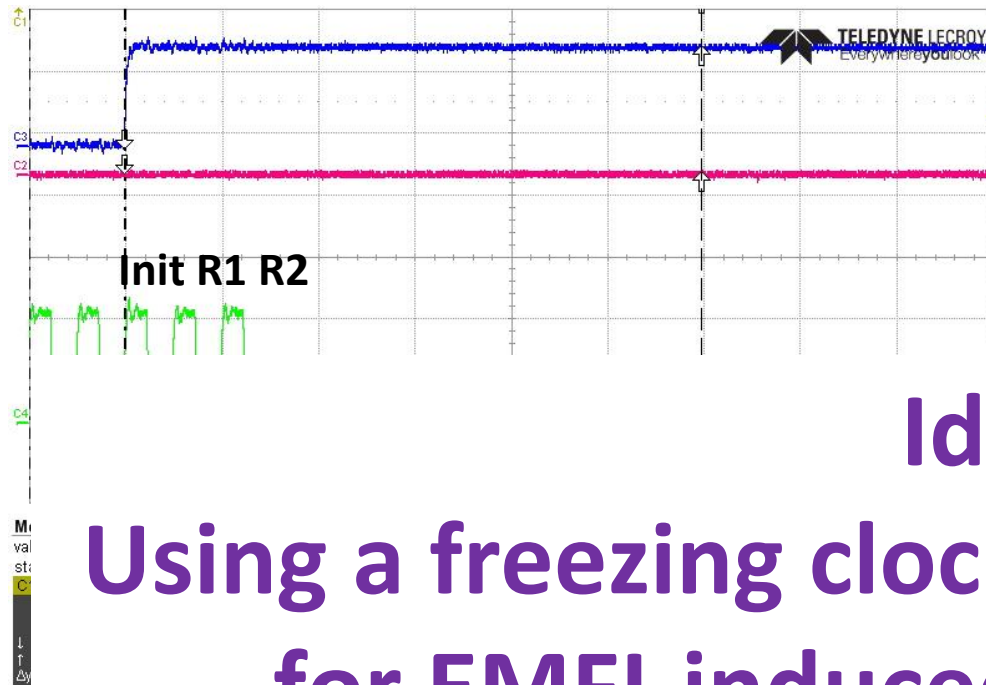
Received ciphertext is not faulted

The induced clock glitches can replace genuine clock rising edges

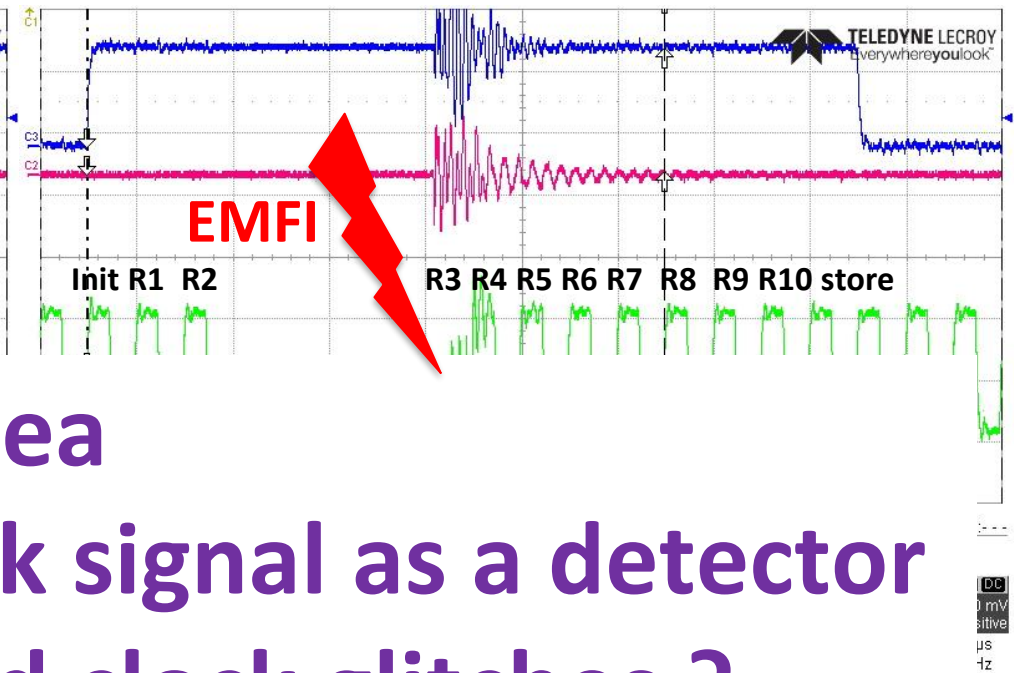
Pulser: voltage amplitude=-420V; width=4.5ns

# Test: freeze case

Freezing the AES clock signal



Unfreezing the clock by EMFI attack



Idea

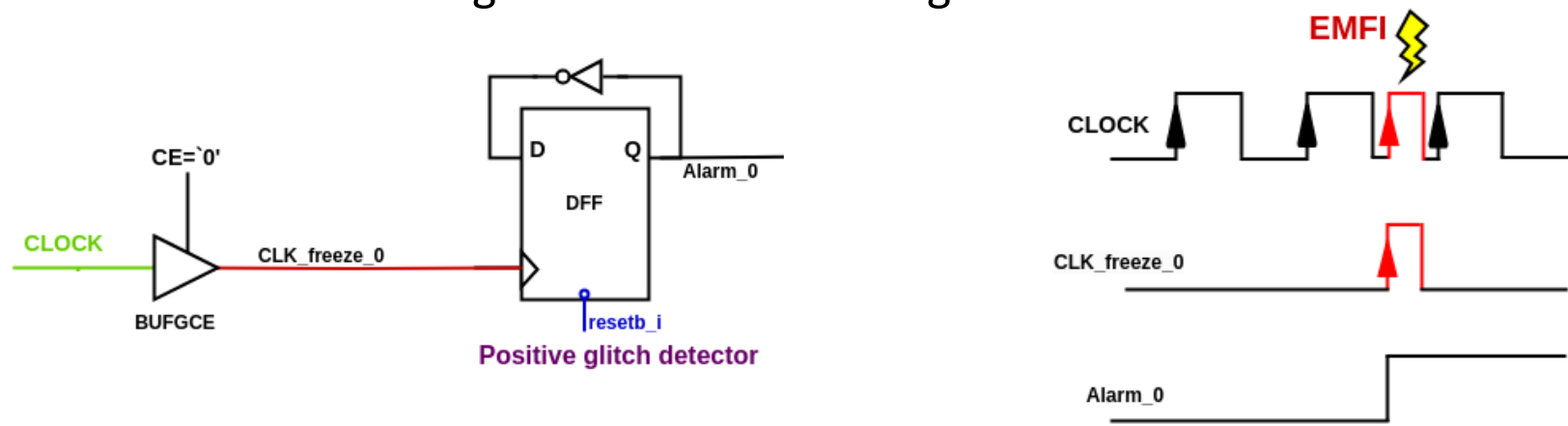
Using a freezing clock signal as a detector  
for EMFI-induced clock glitches ?

# Outline

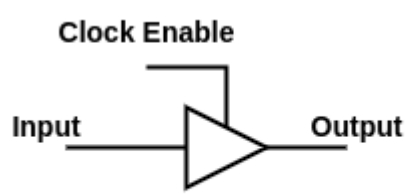
- Previous work: EMFI-induced clock glitches mechanism
- **Novel sensor: Frozen dual-clock detector**
- Experimental setup and sensors implementations
- Spatial and temporal exploration of the sensor performance
- Conclusion and perspectives

# From Mechanism Analysis to Novel Sensor Design

Digital sensor for detecting EMFI-induced clock glitches



Dummy clock signal (clk\_freeze\_0) to detect positive glitches

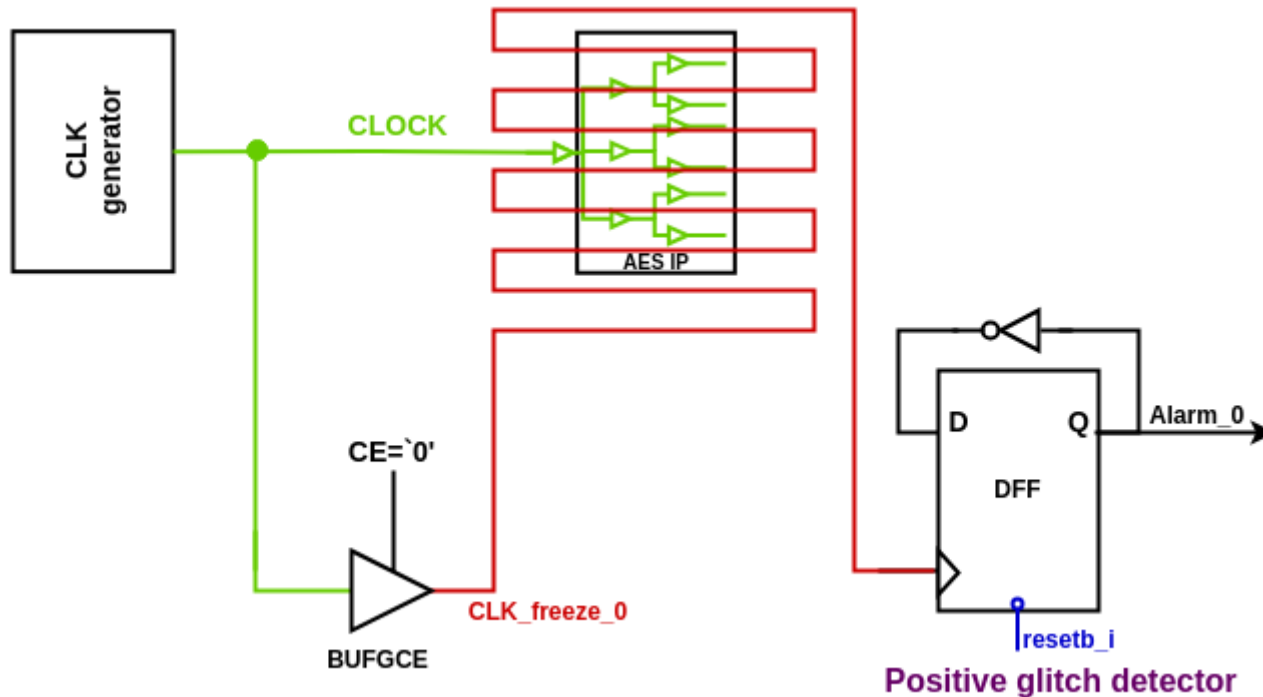


Input I	Clock Enable CE	Output
X	0	0
1	1	1

General Clock Buffer with Clock Enable

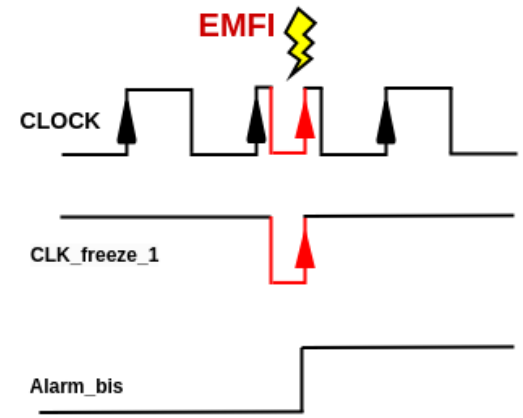
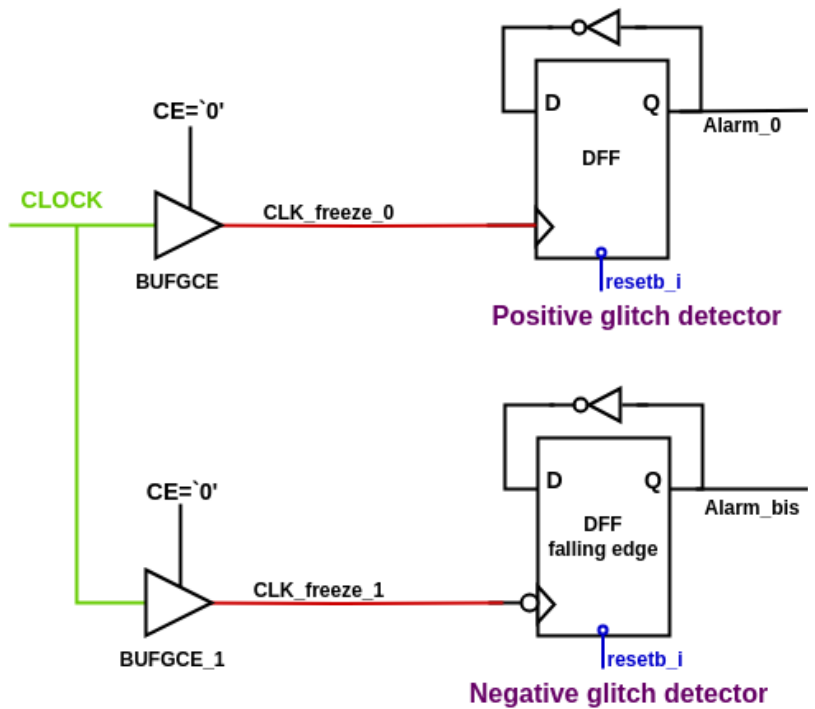
# From Mechanism Analysis to Novel Sensor Design

## ➤ Concept and implementation strategy

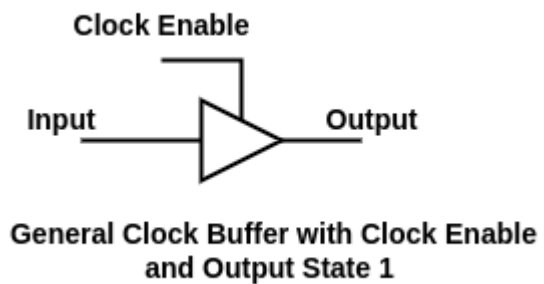


- Dummy clock paths in a frozen state: `clk_freeze_0` and `clk_freeze_1`
- Serpentine form
- Covering the circuit's clock tree (EMFI is local)

# Architecture of the frozen dual-clock signals



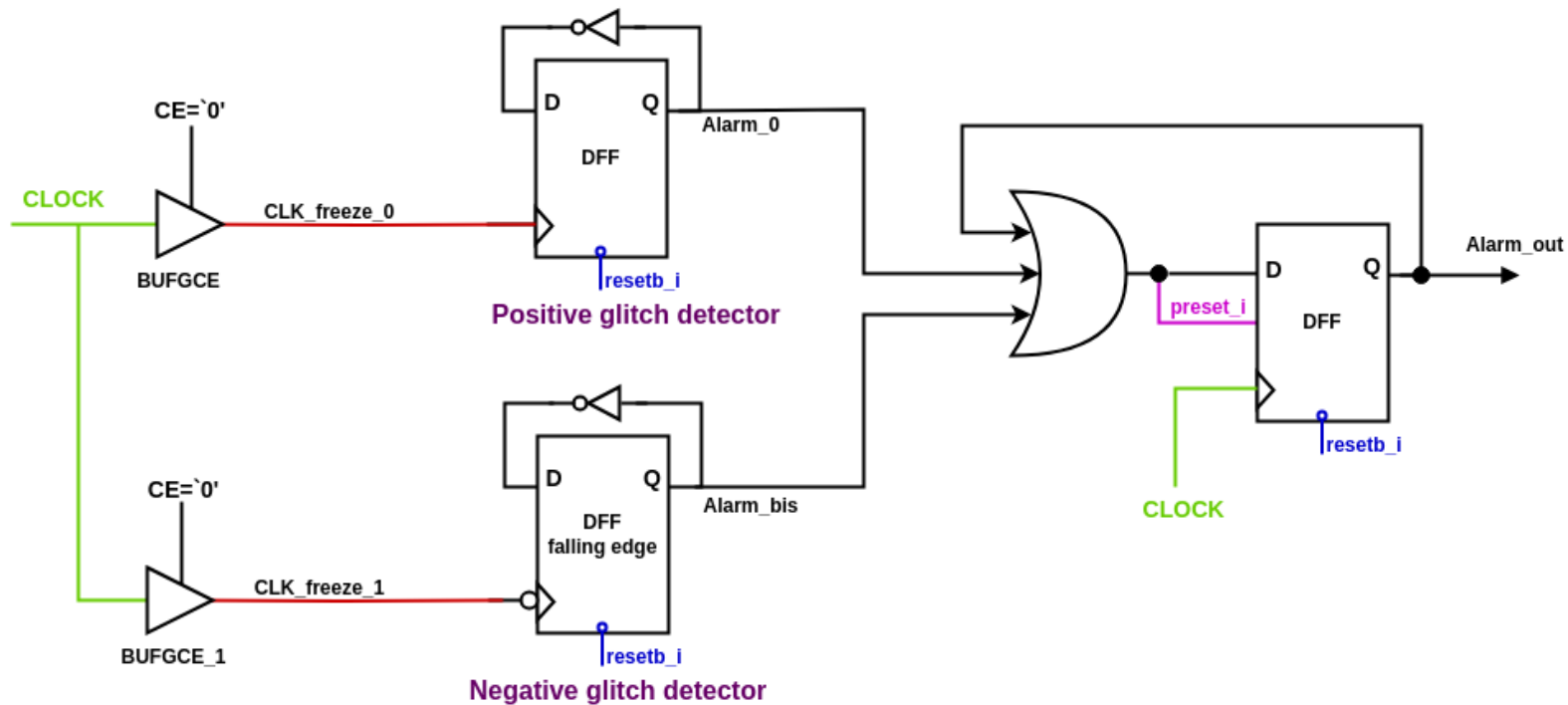
Dummy clock signal (clk\_freeze\_1) to detect negative glitches



Input I	Clock Enable CE	Output
X	0	1
1	1	1



# Architecture of the frozen dual-clock signals

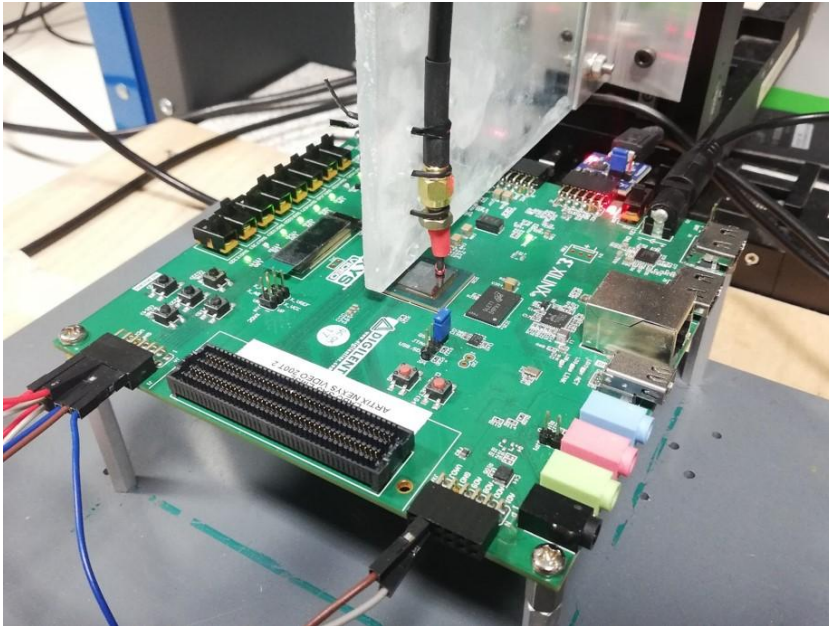


Digital sensor for detecting both negative and positive clock glitches induced by EMFI

# Outline

- Previous work: EMFI-induced clock glitches mechanism
- Novel sensor: Frozen dual-clock detector
- **Experimental setup and sensors implementations**
- Spatial and temporal exploration of the sensor performance
- Conclusion and perspectives

# Experimental setup: EMFI platform



## ➤ FPGA target

- Xilinx Artix7: XCZA200T-SBV484
- Process: CMOS 28nm
- Easy rear side access
  - Heat sink to be removed
- Nexys Video 7 board



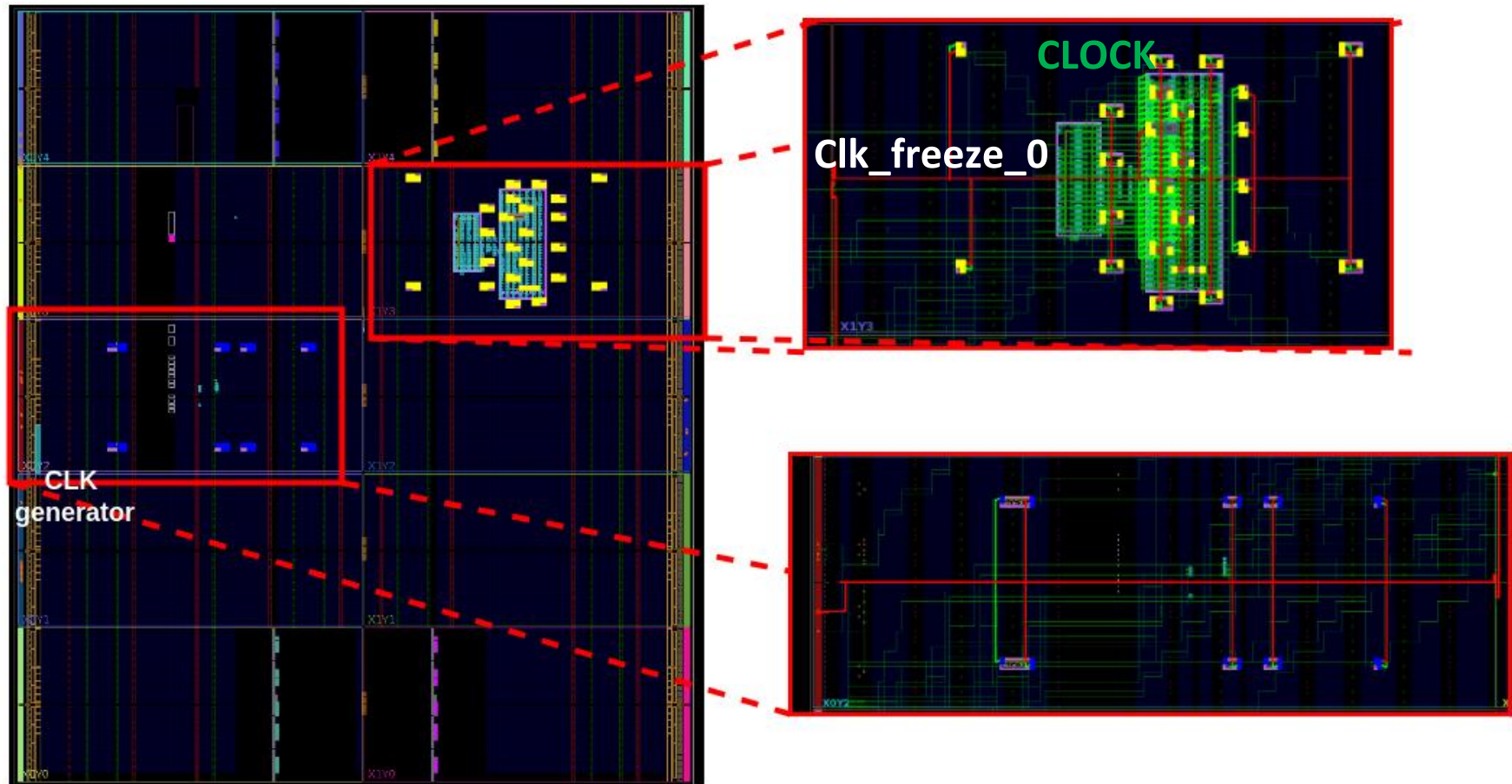
## ➤ AV-Tech voltage pulse generator

- Pulse amplitude: up to +/- 750V
- Pulse-width: 4.5-20ns
- Pulse rise and fall time: 2ns
- Remotely controlled using the telnet protocol

## ➤ EM injection probe

- Homemade EM probe
- Thickness of the copper wire: 0.2mm
- 4 turns
- Cylindrical ferrite core: 2mm

# Sensors implementation

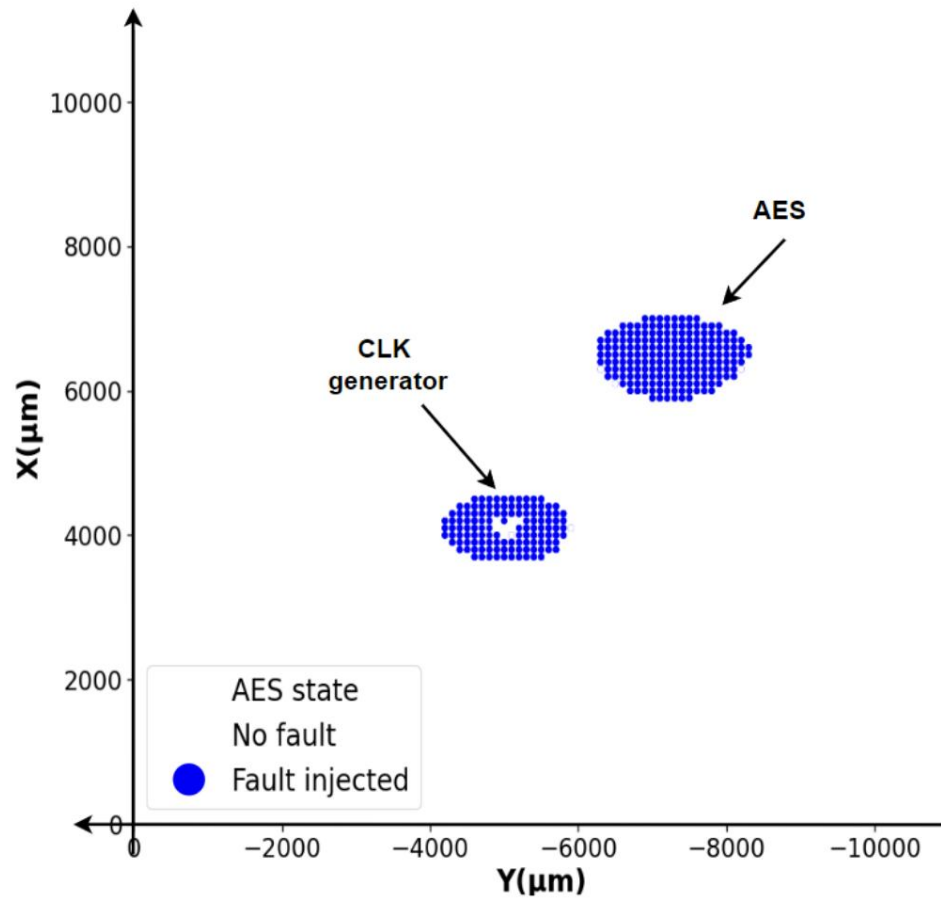


32 sensors → 2 dummy clock paths + 32 detection logic blocks

# Outline

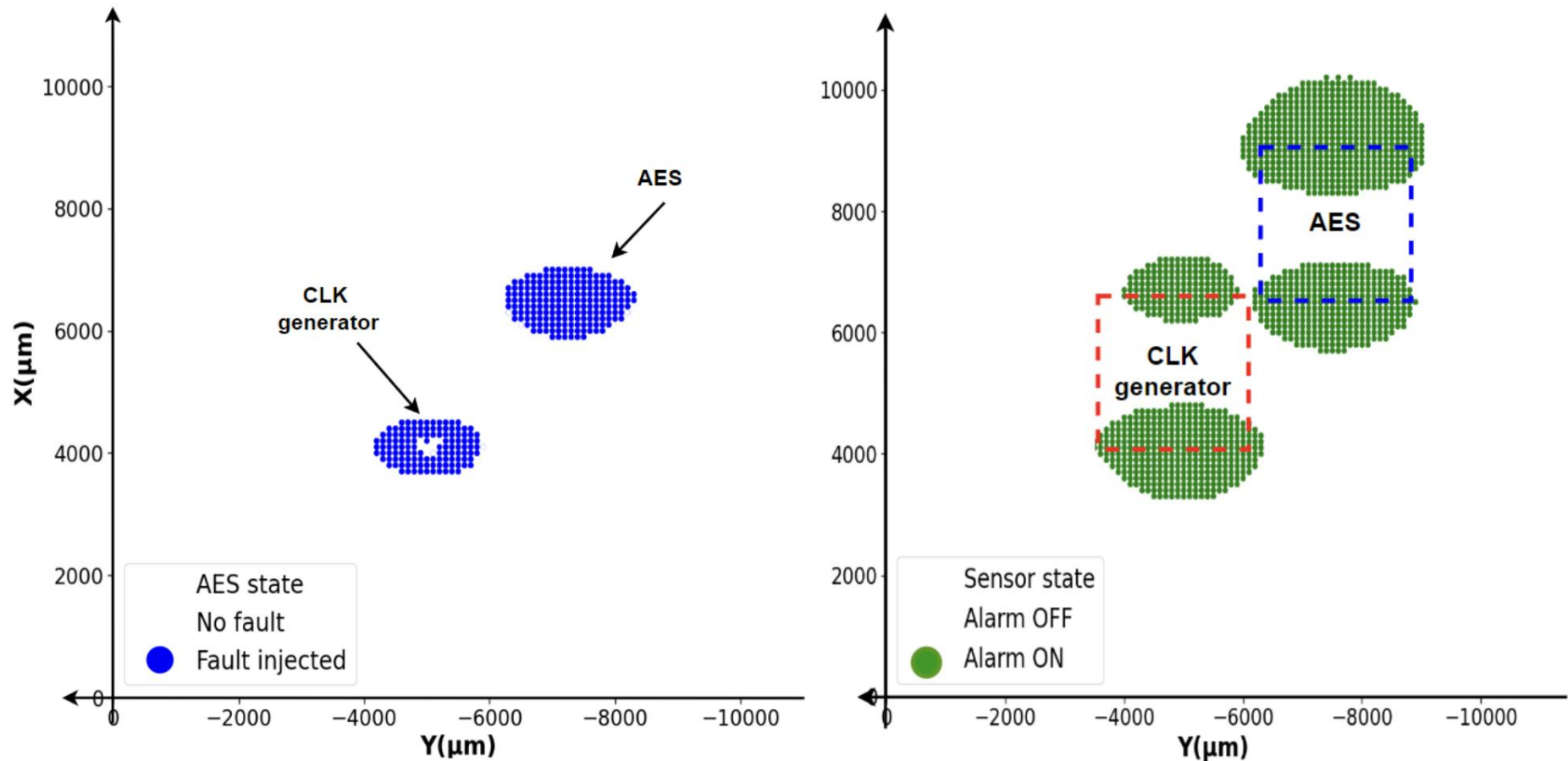
- Previous work: EMFI-induced clock glitches mechanism
- Novel sensor: Frozen dual-clock detector
- Experimental setup and sensors implementations
- **Spatial and temporal exploration of the sensor performance**
- Conclusion and perspectives

# Spatial exploration of sensor performance



EMFI sensitivity maps for faults injected into the AES (left) and triggering sensor alarm (right) launched at 100 MHz (pulse width=4.5 ns, pulse amplitude= +420 V)

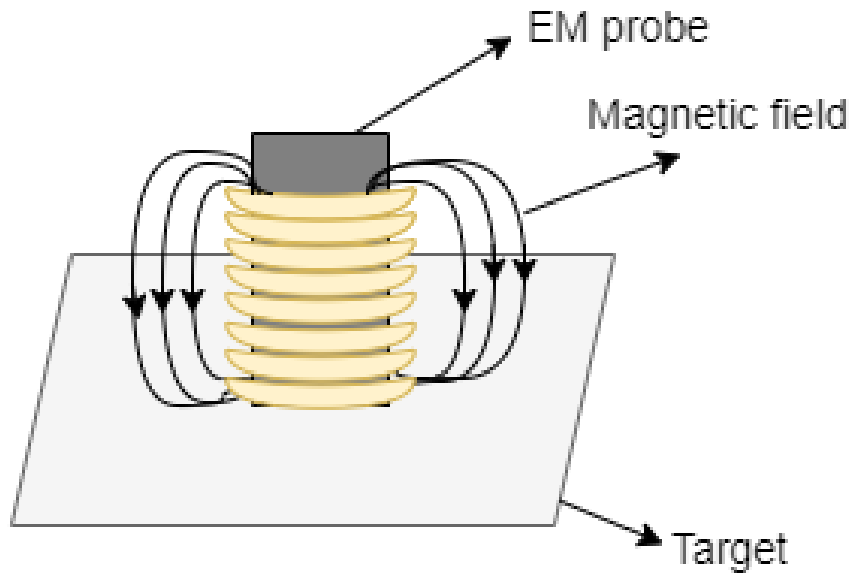
# Spatial exploration of sensor performance



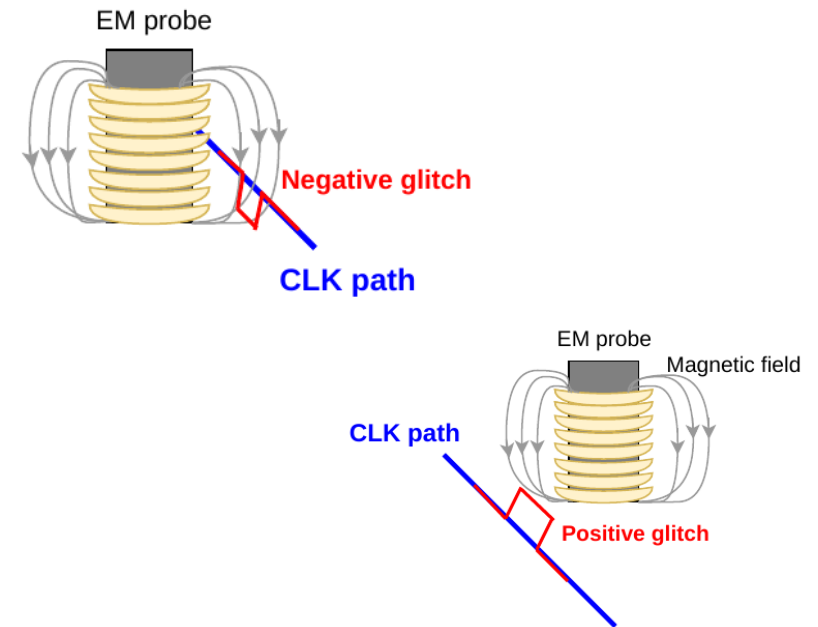
**All injected faults are detected**

EMFI sensitivity maps for faults injected into the AES (left) and triggering sensor alarm (right) launched at 100 MHz (pulse width=4.5 ns, pulse amplitude= +420 V)

# Coupling between EM probe and the target's chip



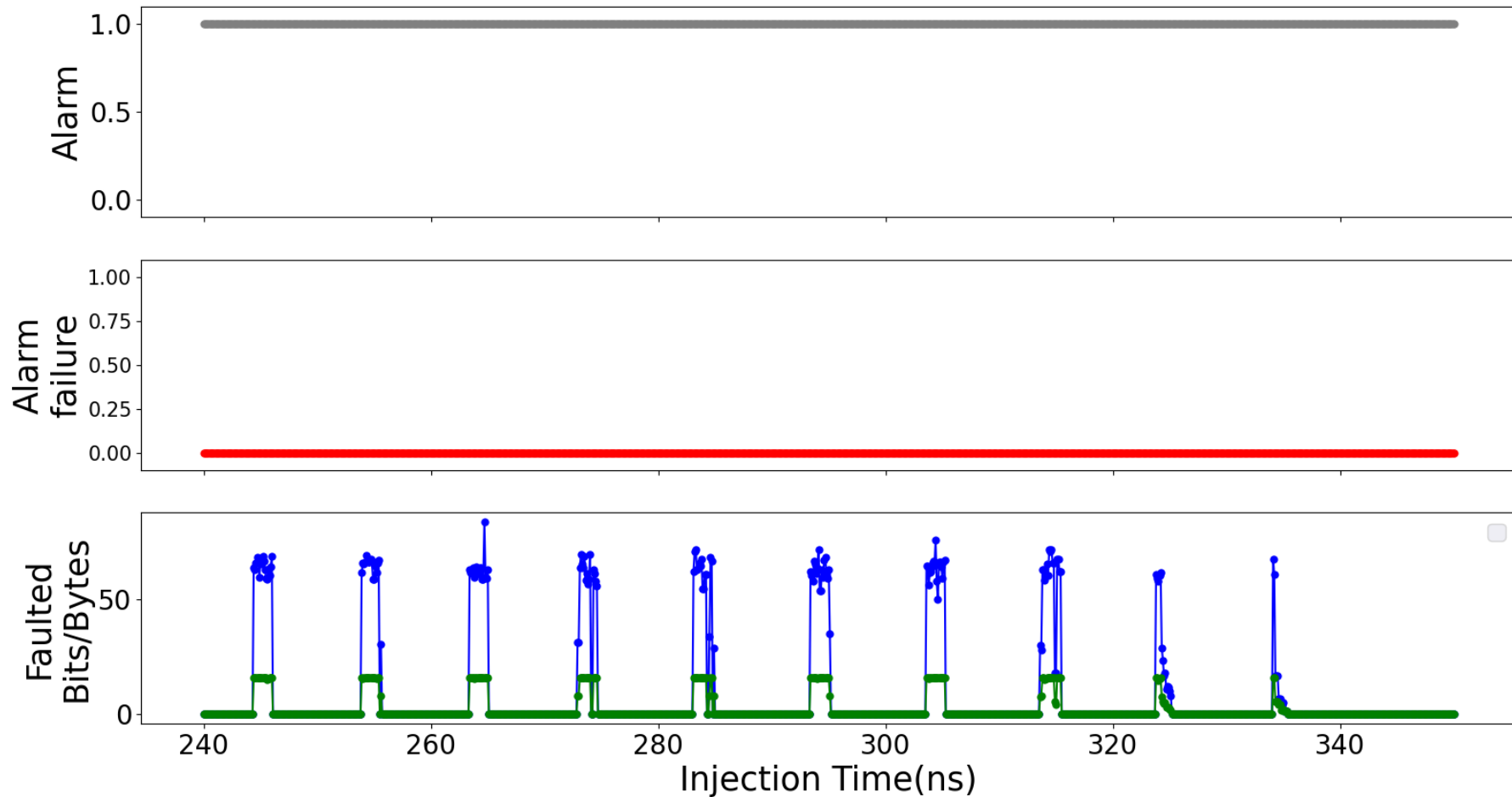
Example: Positive pulse



**Spatial positioning of the EM probe can impact the sign of the induced glitch**

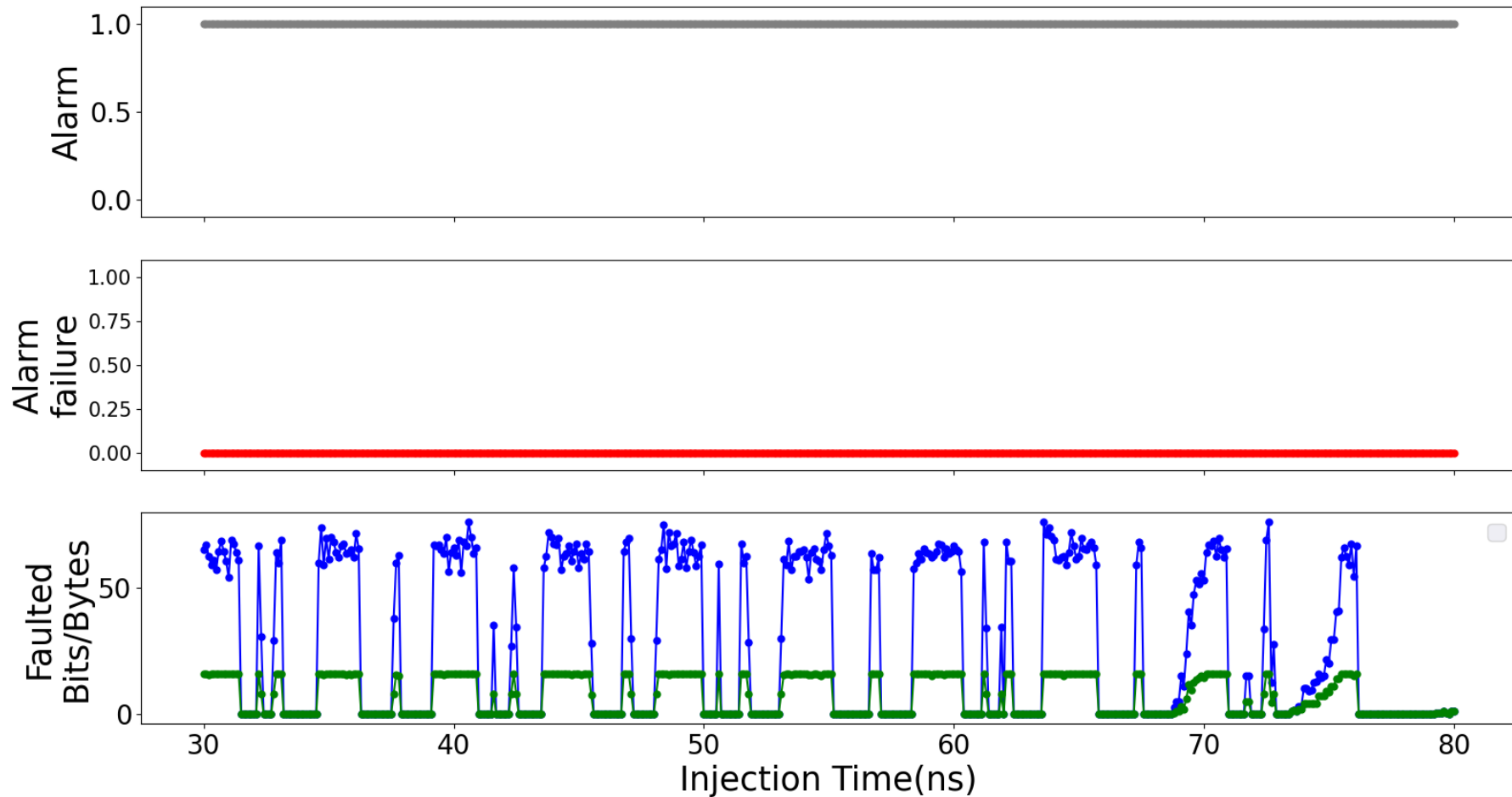


# EMFI results: @100MHZ (+420V)



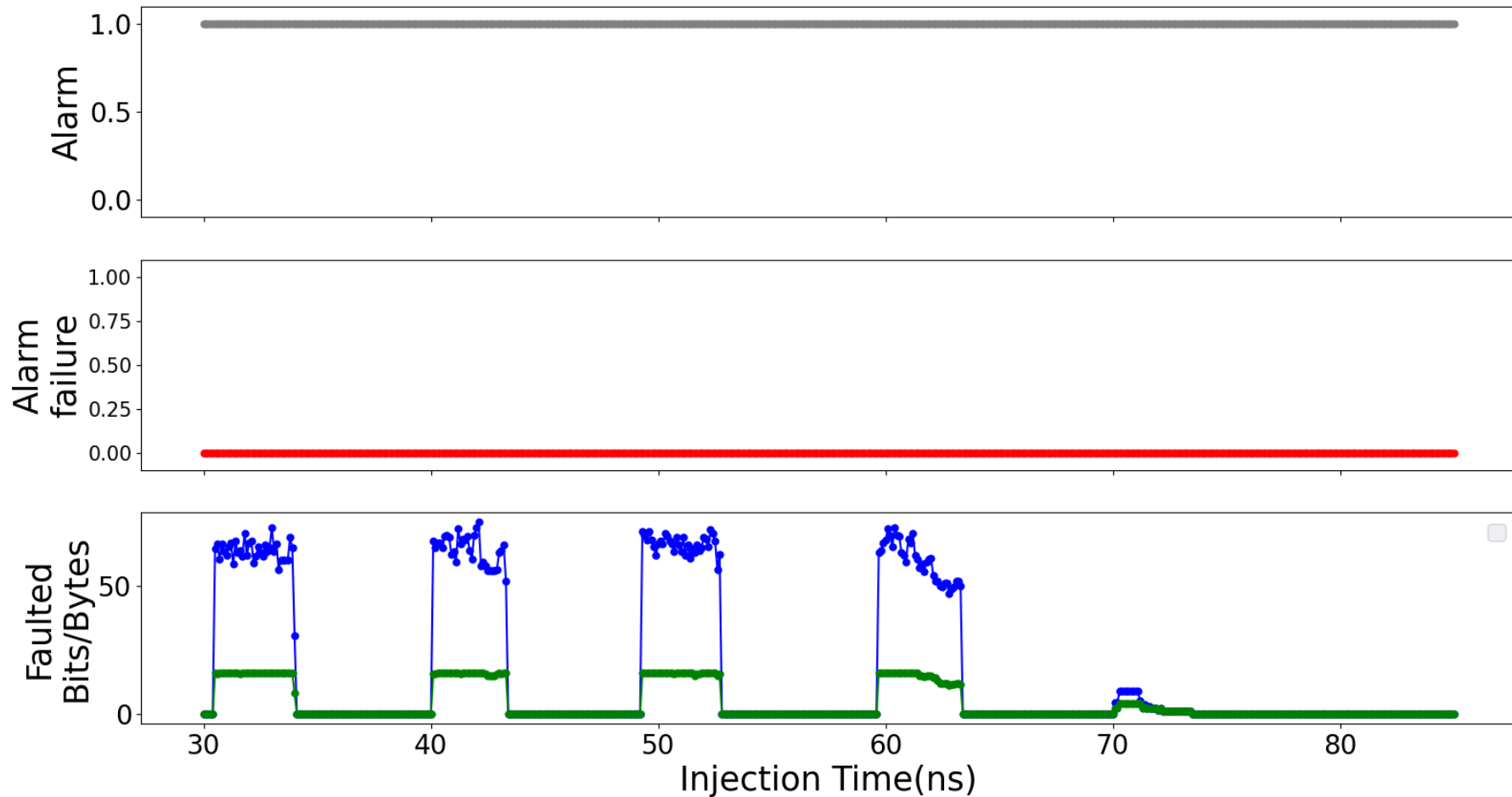
**100 % fault detection rate throughout the experiments,  
regardless of the EM injection time**

# EMFI results: @200MHZ (+420V)



All injected faults into the AES computations are detected

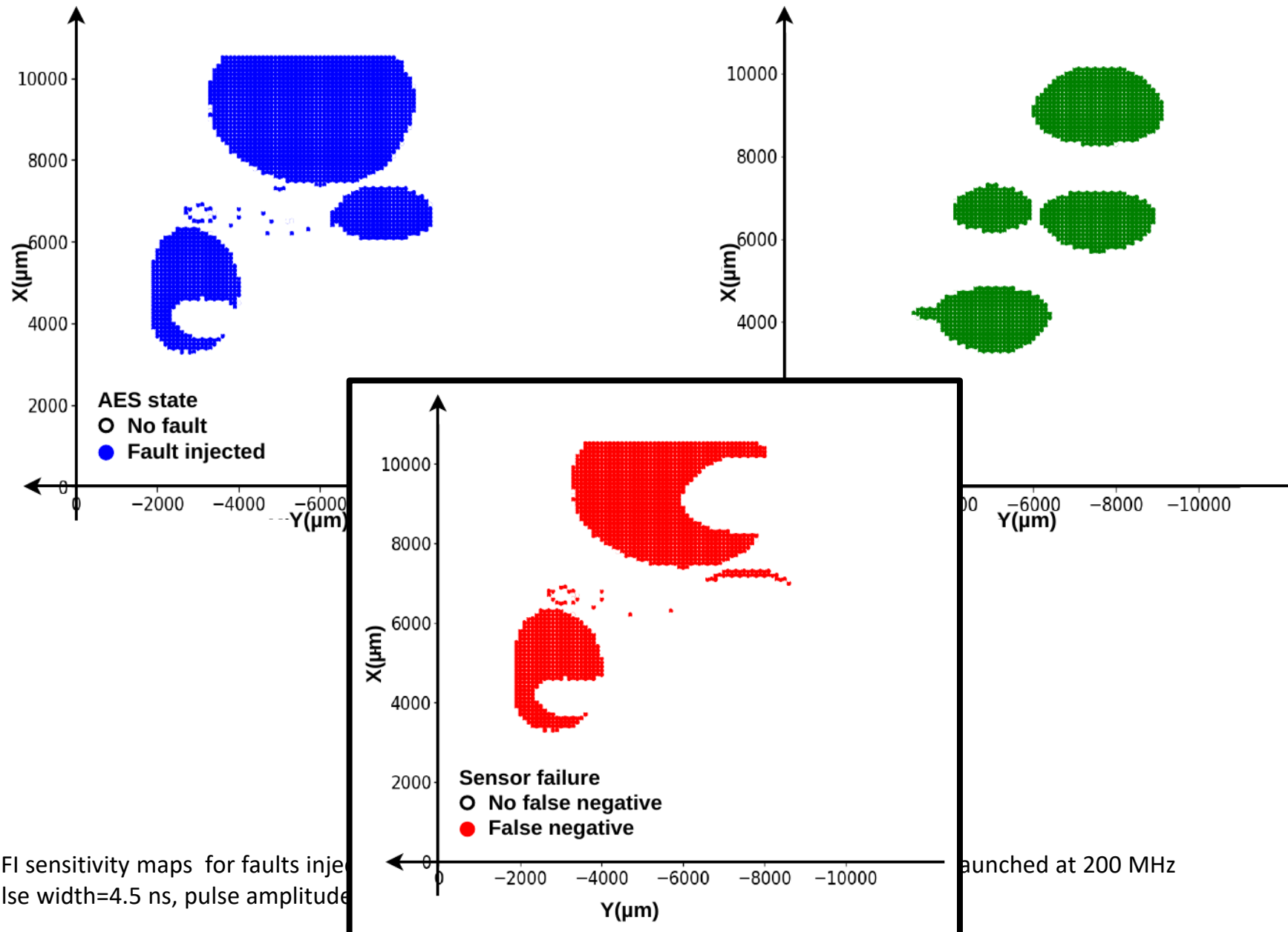
# EMFI results: @200MHZ (+300V)



This sensor can also detect faults injected due to the timing fault mechanism provided that

$$\text{Sensor threshold}_{\text{clock glitches}} < \text{Threshold}_{\text{timing violations}}$$

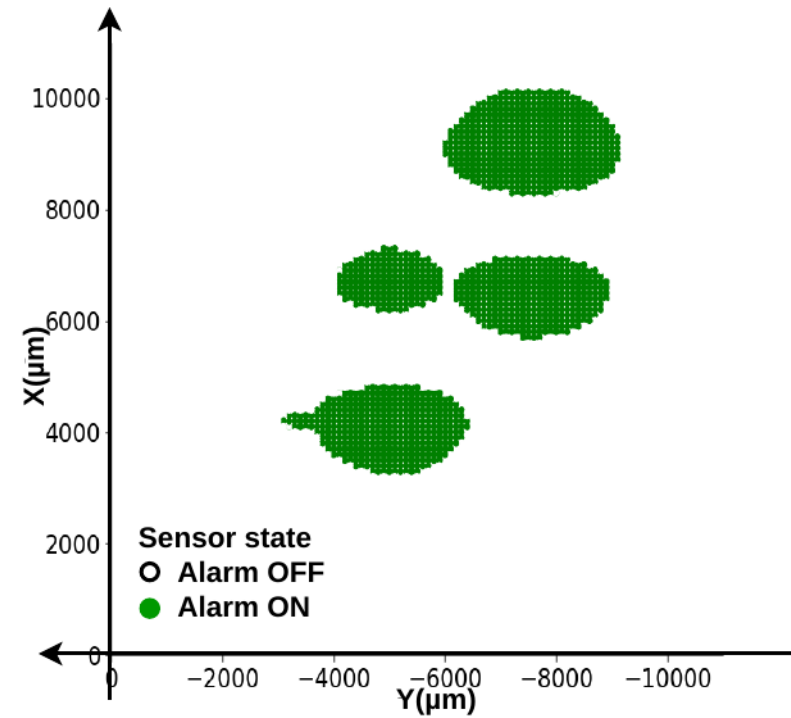
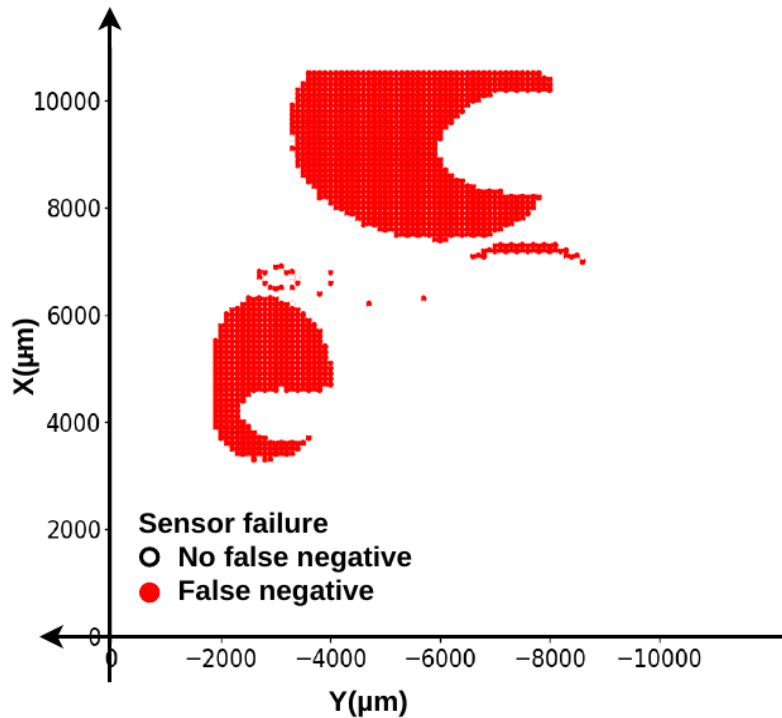
# Spatial exploration @200MHz



EMFI sensitivity maps for faults injected at 200 MHz (pulse width=4.5 ns, pulse amplitude=100 mV)

launched at 200 MHz

# Spatial exploration @200MHz



- EMFI sensitivity maps for undetected faults:
- Sensor EMFI detection is local
  - For low time margin, timing faults have large sensitivity areas
  - No detection of timing faults for probe positions outside the sensor coverage area

# Outline

- Previous work: EMFI-induced clock glitches mechanism
- Novel sensor: Frozen dual-clock detector
- Experimental setup and sensors implementations
- Spatial and temporal exploration of the sensor performance
- **Conclusion and perspectives**

# Conclusion : Novel sensor performance study

## ➤ Strengths:

- Detection of EMFI-induced clock glitches (positives and negatives) across the circuit's full-frequency range
- Detection of timing faults (except for critical paths whose fault threshold is lower than the threshold for inducing glitches on the sensor's dummy clock paths)
- 100% detection rate at the time domain, regardless of the EM injection time
- Low impact on the dynamic energy consumption (dummy clock paths remain in a static state)

# Conclusion : Novel sensor performance study

## ➤ Weaknesses:

- High density of sensors is required to achieve a good spatial coverage
- No detection of clock glitches induced on the main clock if they are not created on one of the sensors clock paths
- No detection for the timing faults obtained at high frequency outside the sensor coverage area



# Conclusion : Novel sensor performance study

- **Perspective** : Further work and experiments are still needed to consolidate these findings:
  - Investigation of the optimal sensor spacing to maintain a high fault detection rate
  - Associate Zussa<sup>1</sup>'s sensor for detecting timing faults

<sup>1</sup>Zussa, L., Dehbaoui, A., Tobich, K., Dutertre, J. M., Maurine, P., Guillaume-Sage, L. & Tria, A. (2014, March). Efficiency of a glitch detector against electromagnetic fault injection. In 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 1-6). IEEE.



---

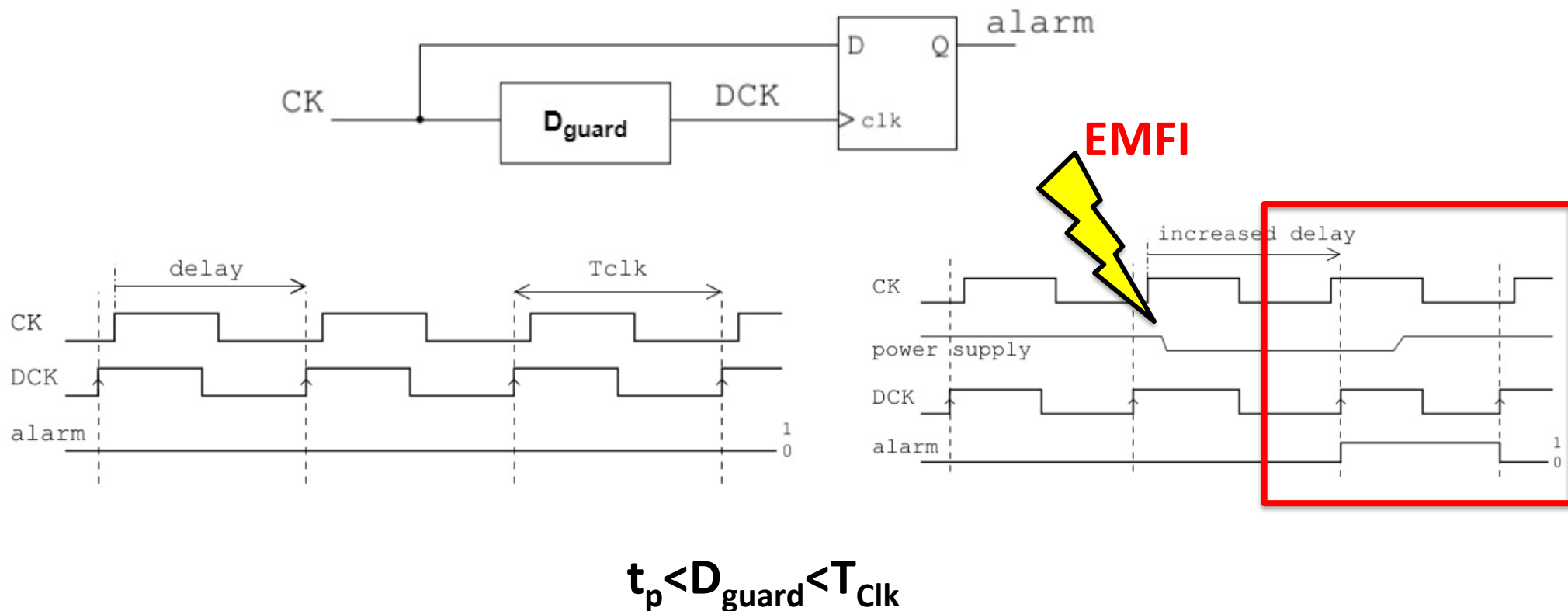
## Questions

Contact: [roukoz.nabhan@emse.fr](mailto:roukoz.nabhan@emse.fr)

---

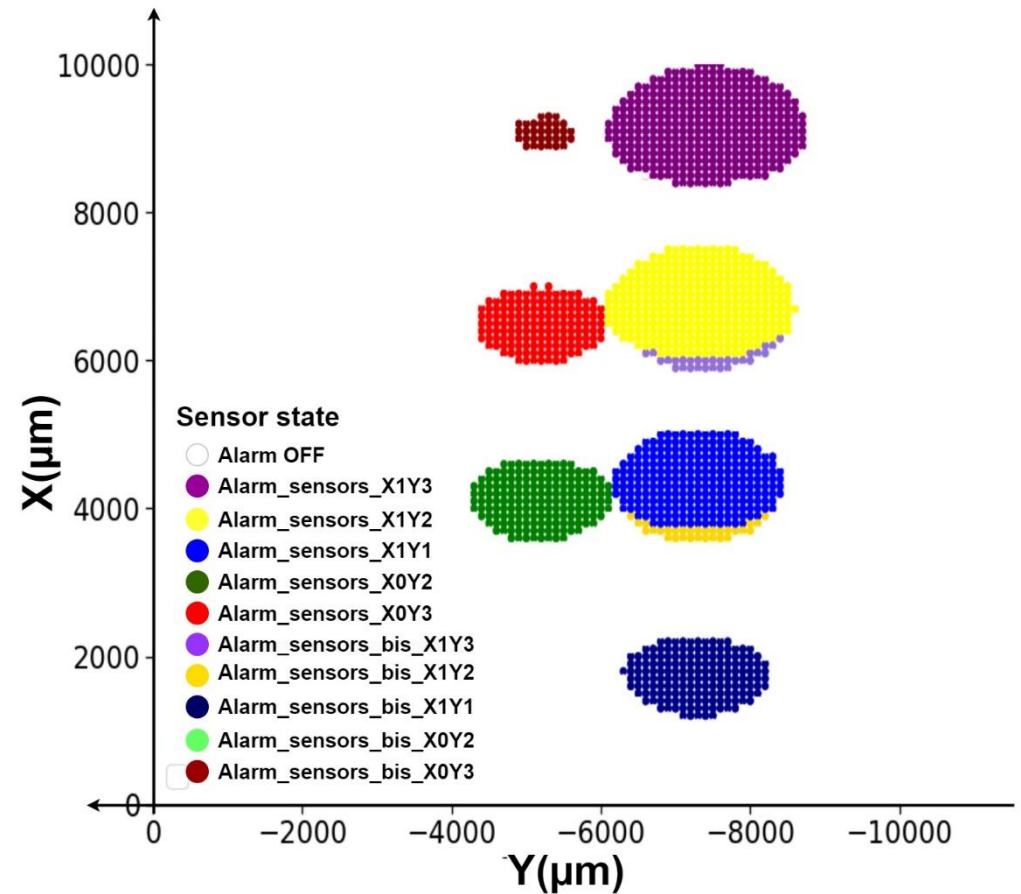
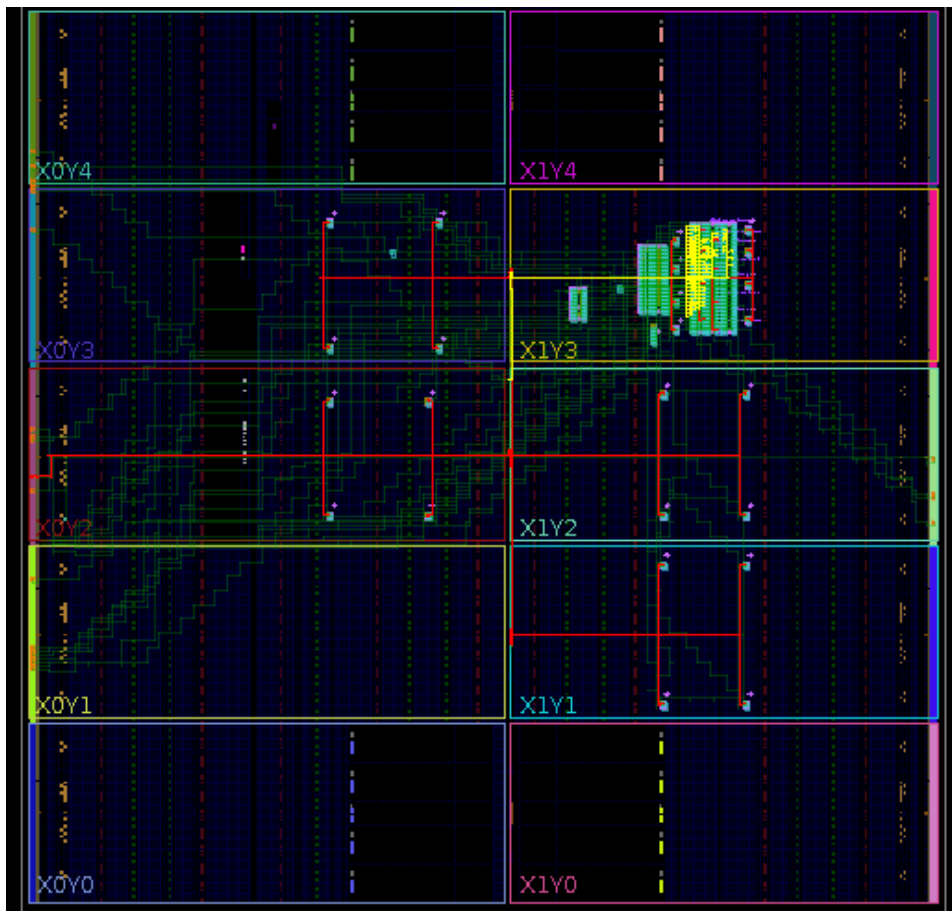
# State of the art: EMFI sensors

From timing faults to guarding delay sensor designed by *Zussa et al*\*



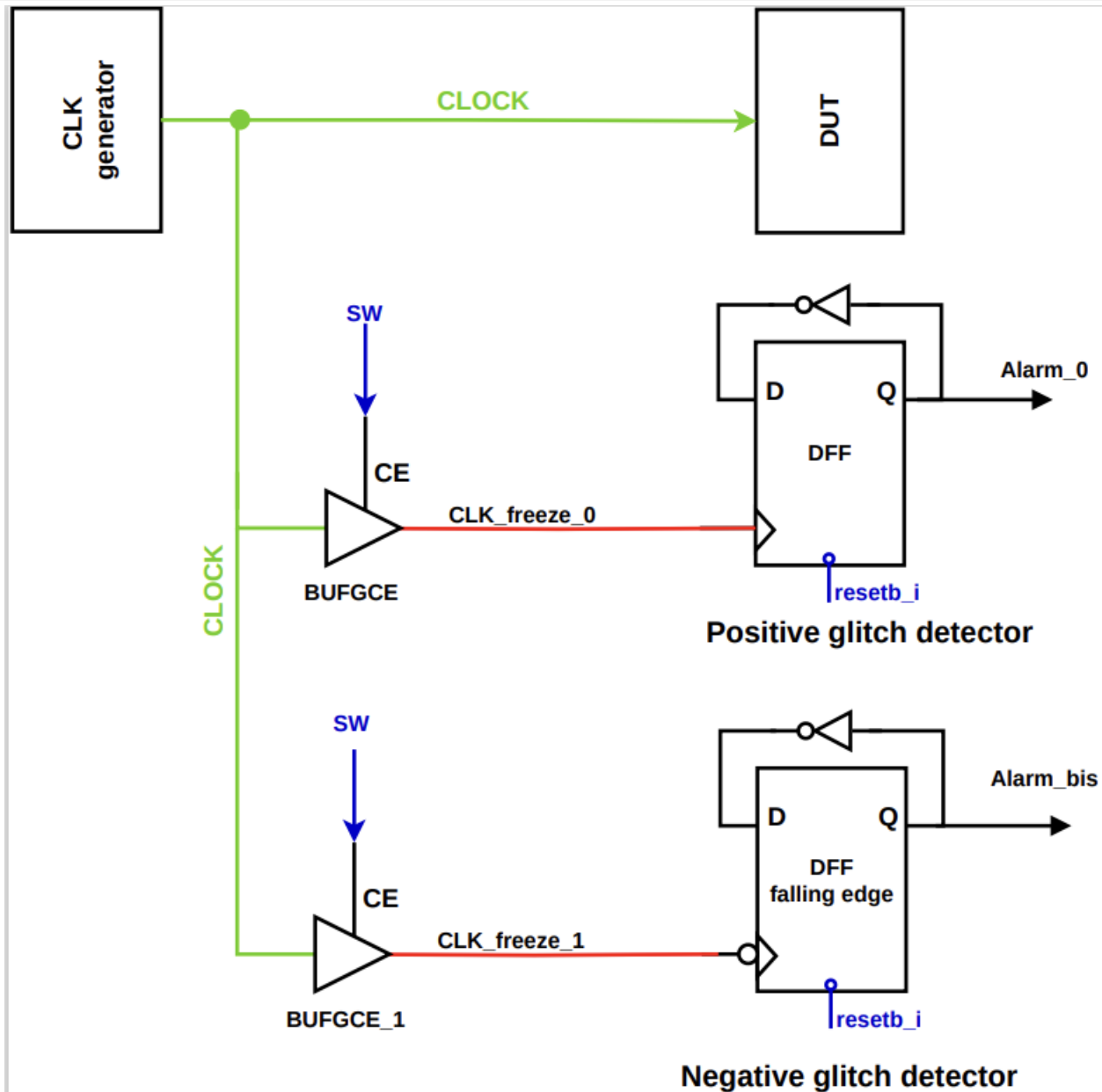
\*Zussa, L., Dehbaoui, A., Tobich, K., Dutertre, J. M., Maurine, P., Guillaume-Sage, L. & Tria, A. (2014, March). Efficiency of a glitch detector against electromagnetic fault injection. In 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 1-6). IEEE.

# Spatial exploration of the sensor distributions



An in-depth investigation into the relationship between the positioning of sensors on the floor plan and the resulting sensitivity map.

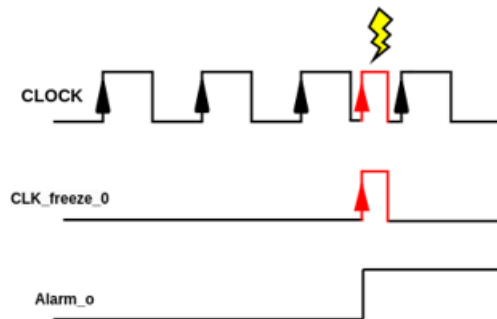
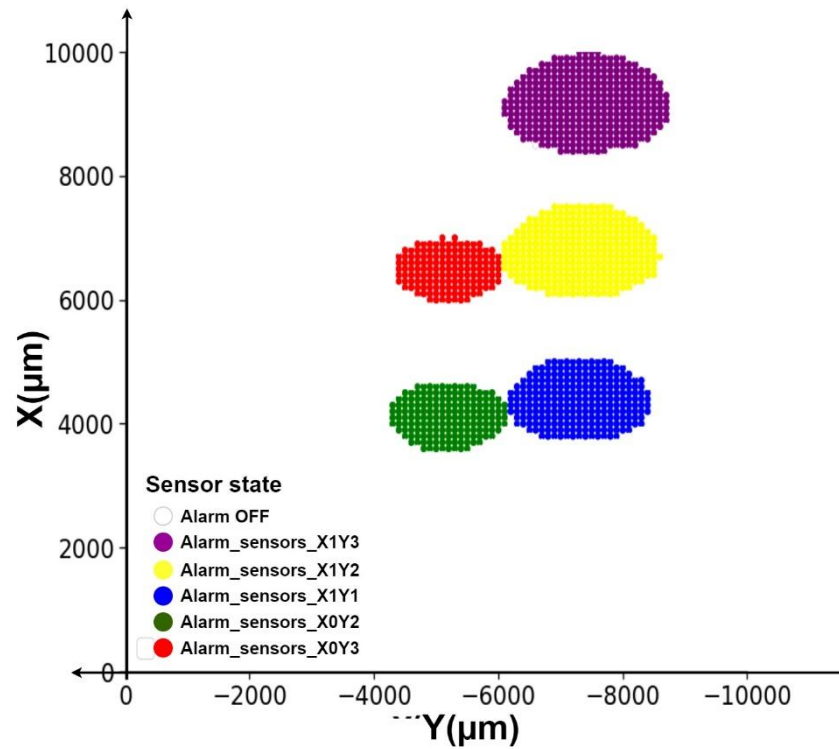
# Spatial exploration of the sensor distributions



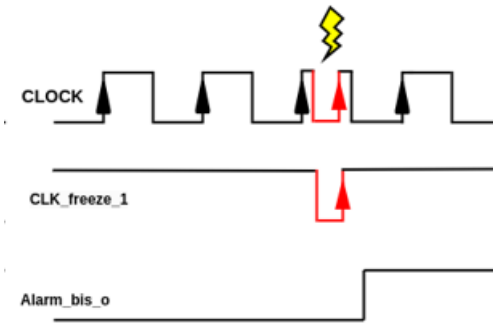
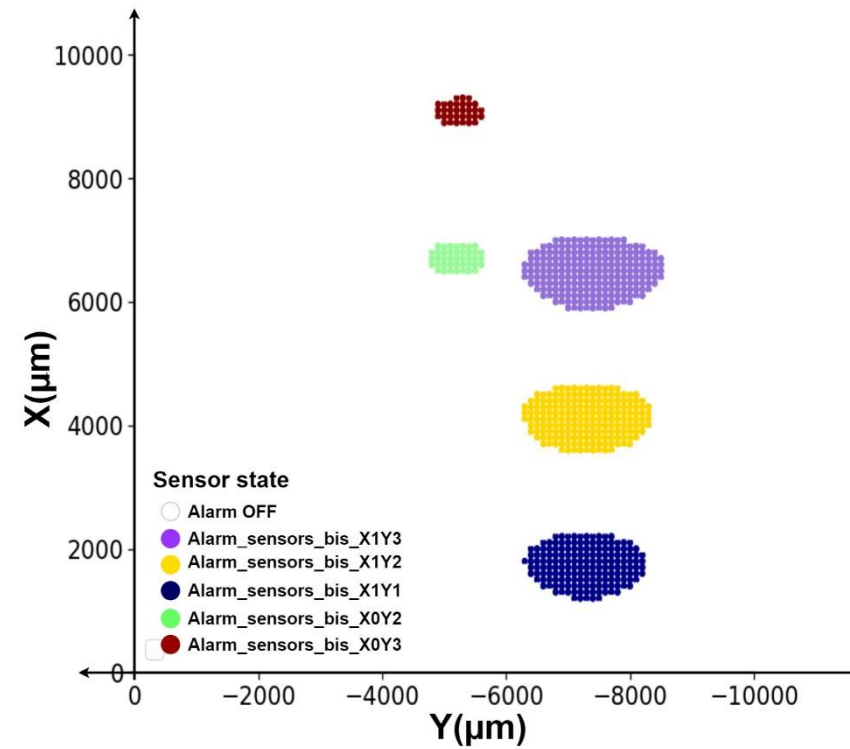
Separation of alarms output

# Spatial exploration of the sensor distributions

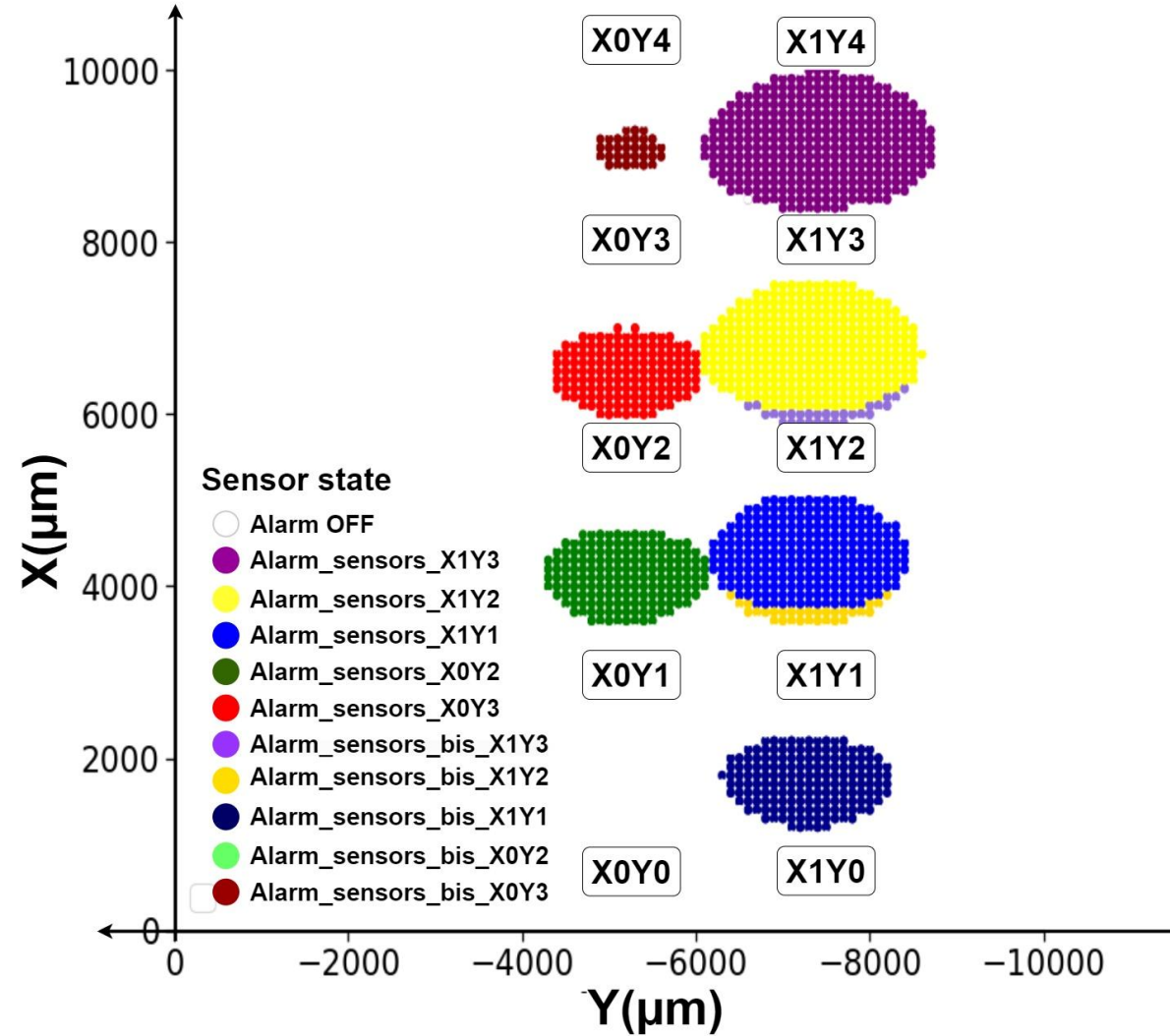
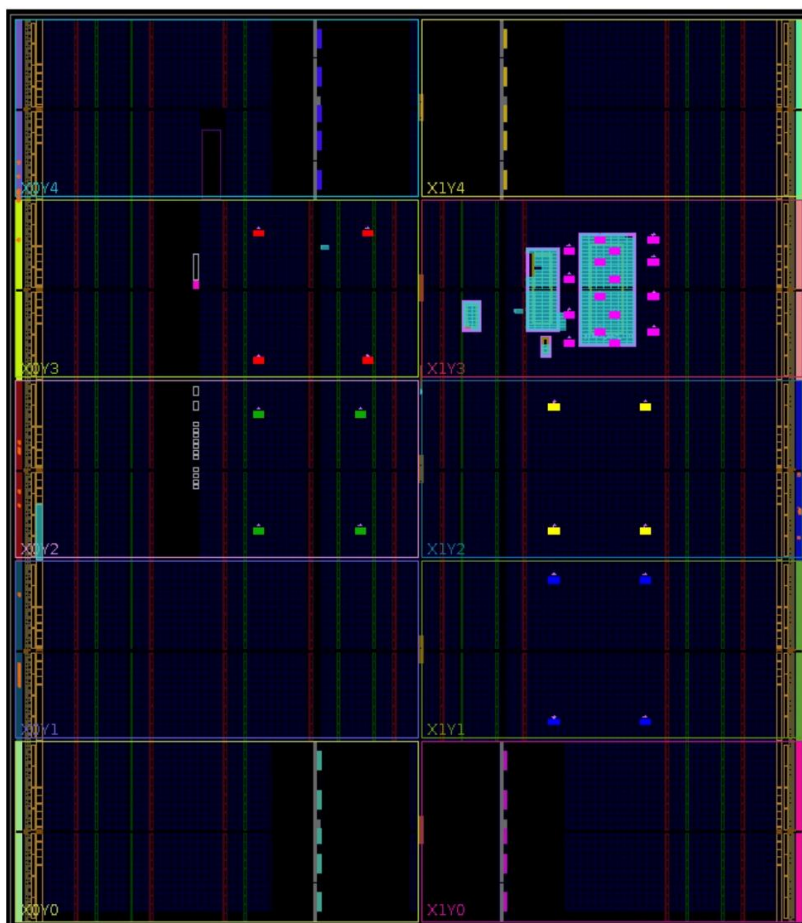
Alarm\_0



Alarm\_bis

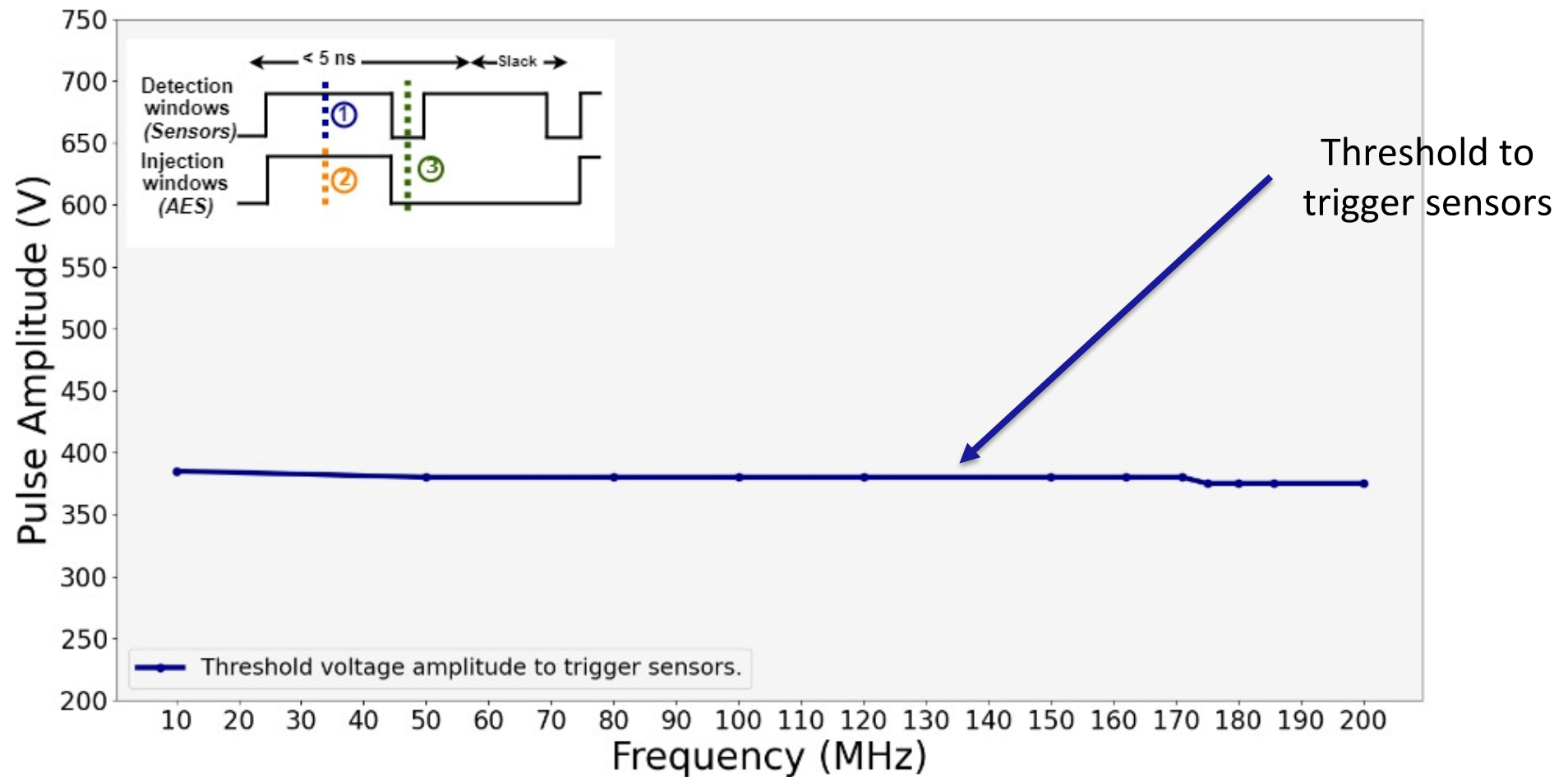


# Correlation between the hardware and software floorplans



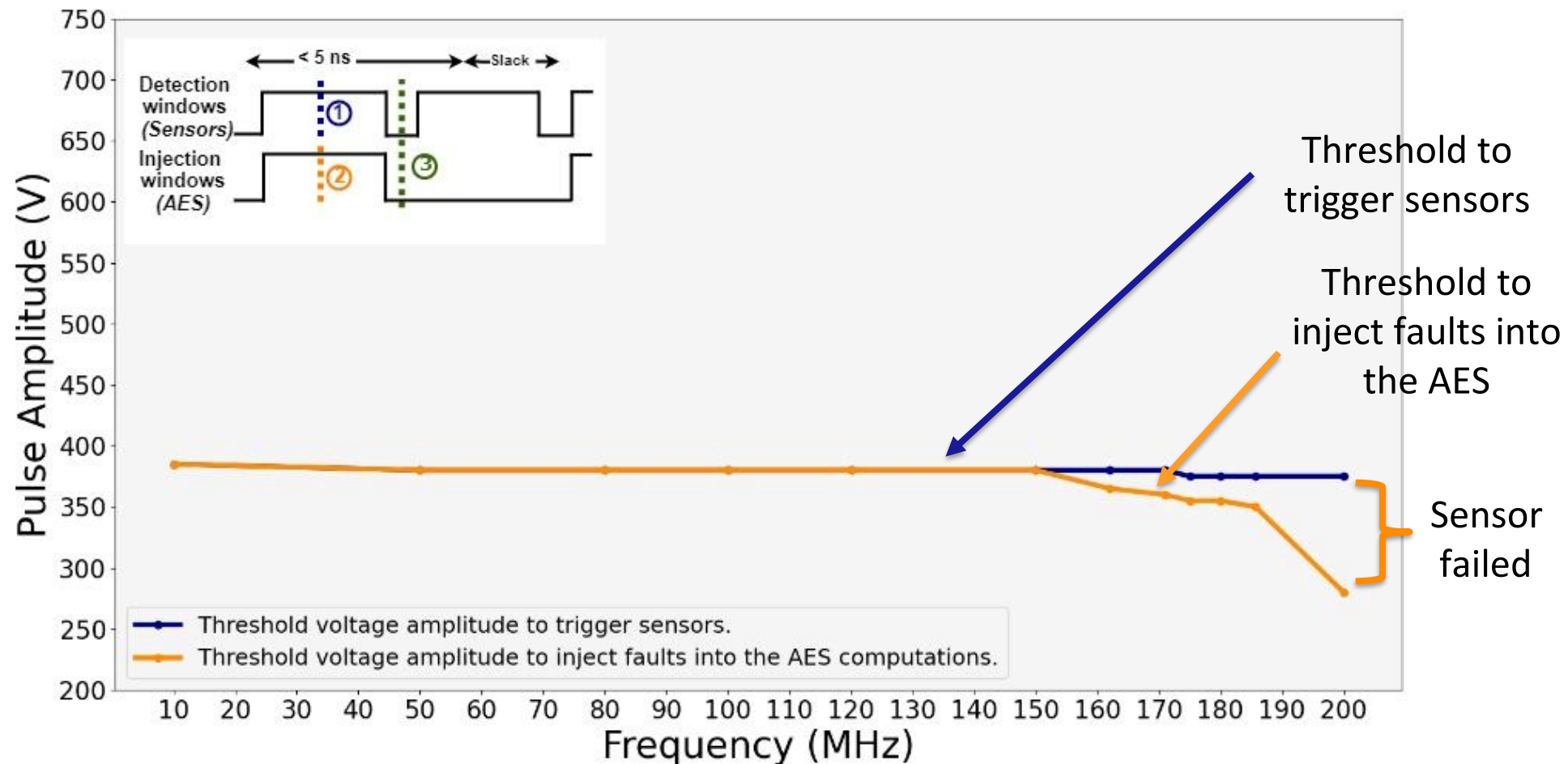


# Exploration of EMFI mechanisms

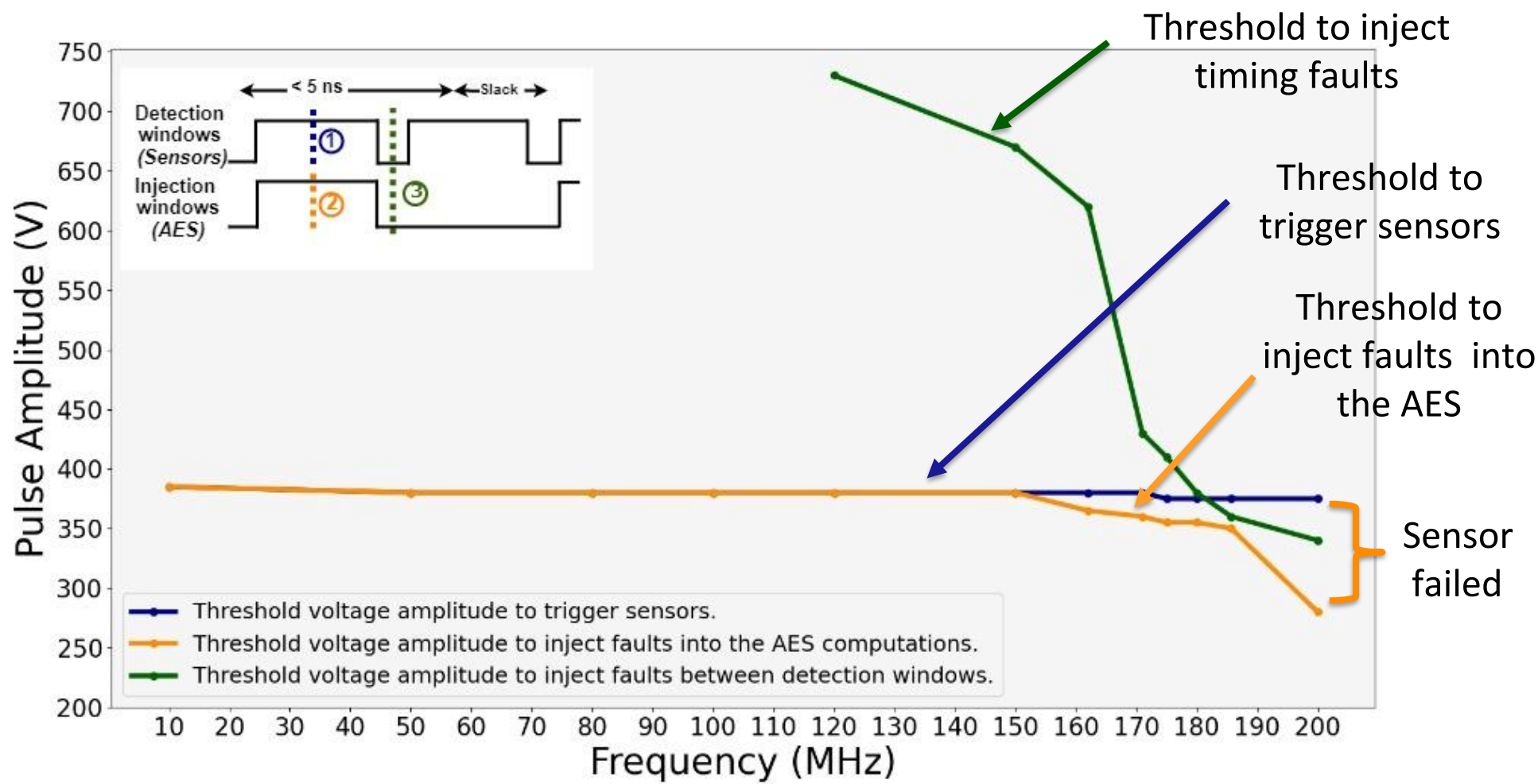




# Exploration of EMFI mechanisms



# Exploration of EMFI mechanisms

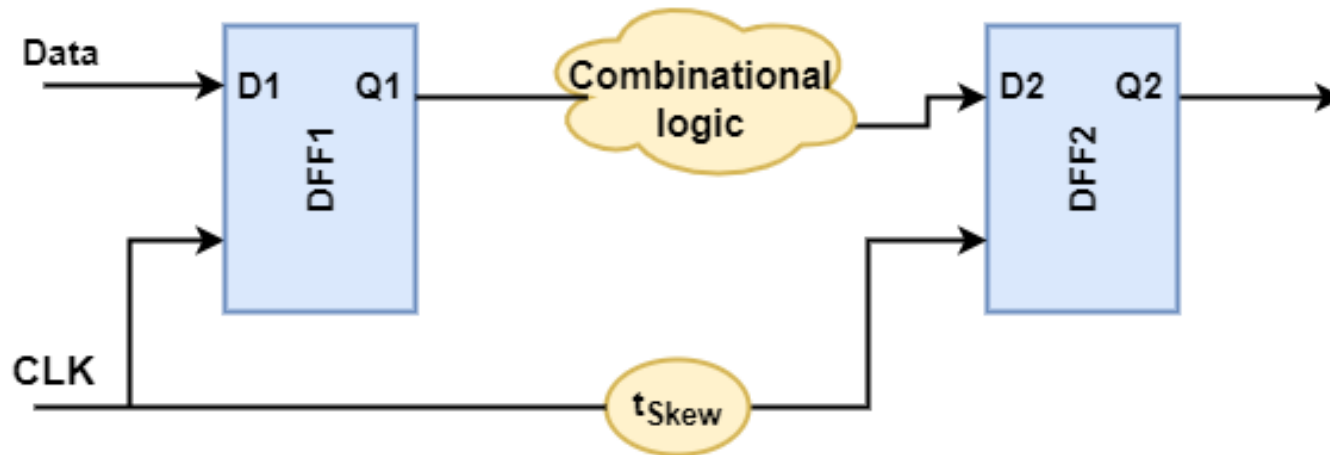


## Coexistence of two distinct fault injection mechanisms to explain EMFI<sup>1</sup>

<sup>1</sup>Nabhan, R., Dutertre, J. M., Rigaud, J. B., Danger, J. L., & Sauvage, L. (2023, April). Highlighting Two EM Fault Models While Analyzing a Digital Sensor Limitations. In *2023 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1-2). IEEE

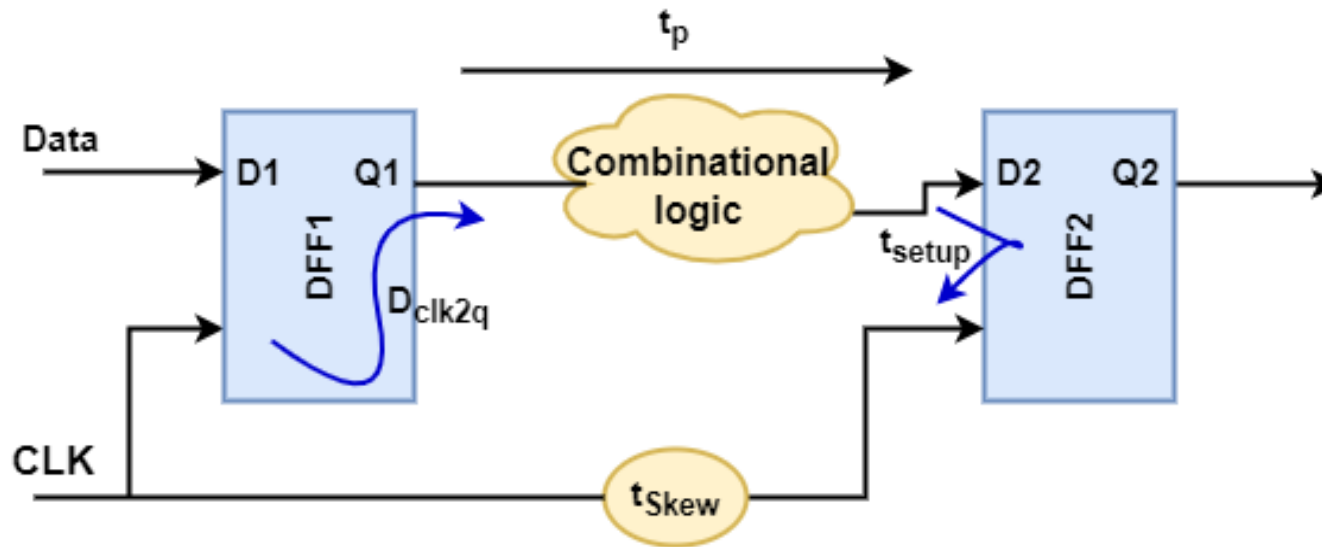
# Digital synchronous circuits

- Understanding EMFI mechanisms → Requires an interest in the internal architecture of synchronous circuits



# Digital synchronous circuits

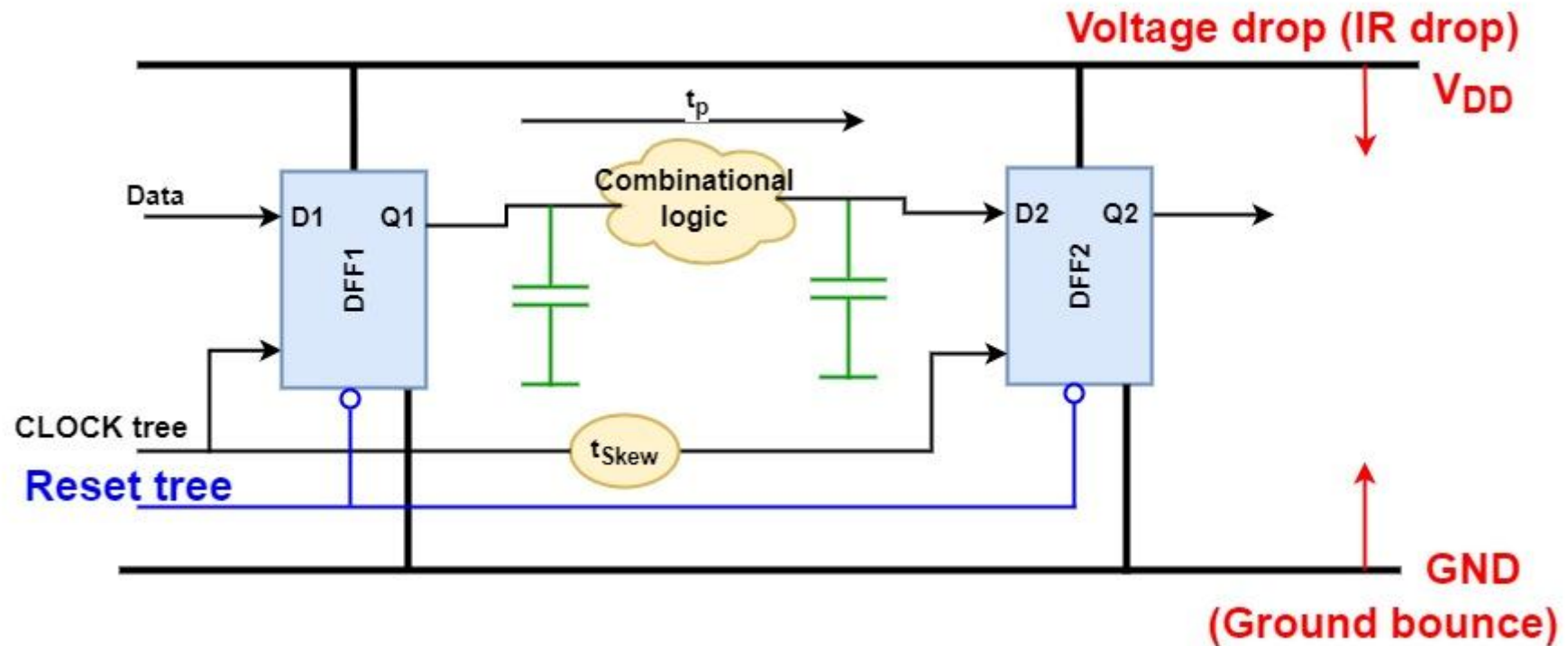
## Timing constraints of digital circuits



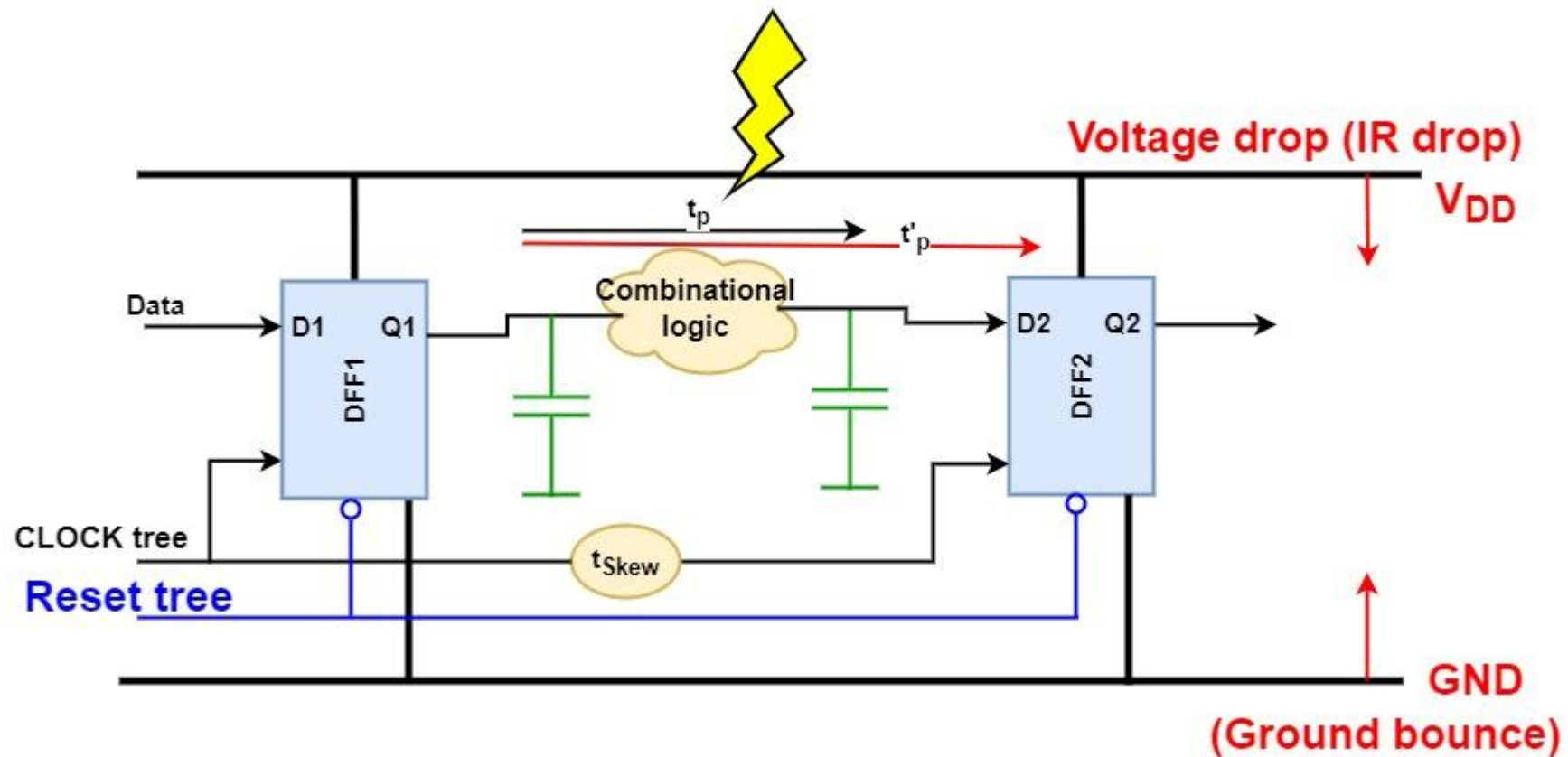
Digital synchronous circuits have to fulfill the setup timing constraints:

$$T_{clk} > D_{clk2q} + t_{pmax} + t_{setup} - t_{skew}$$

# State of the art: EMFI models



# State of the art: EMFI models

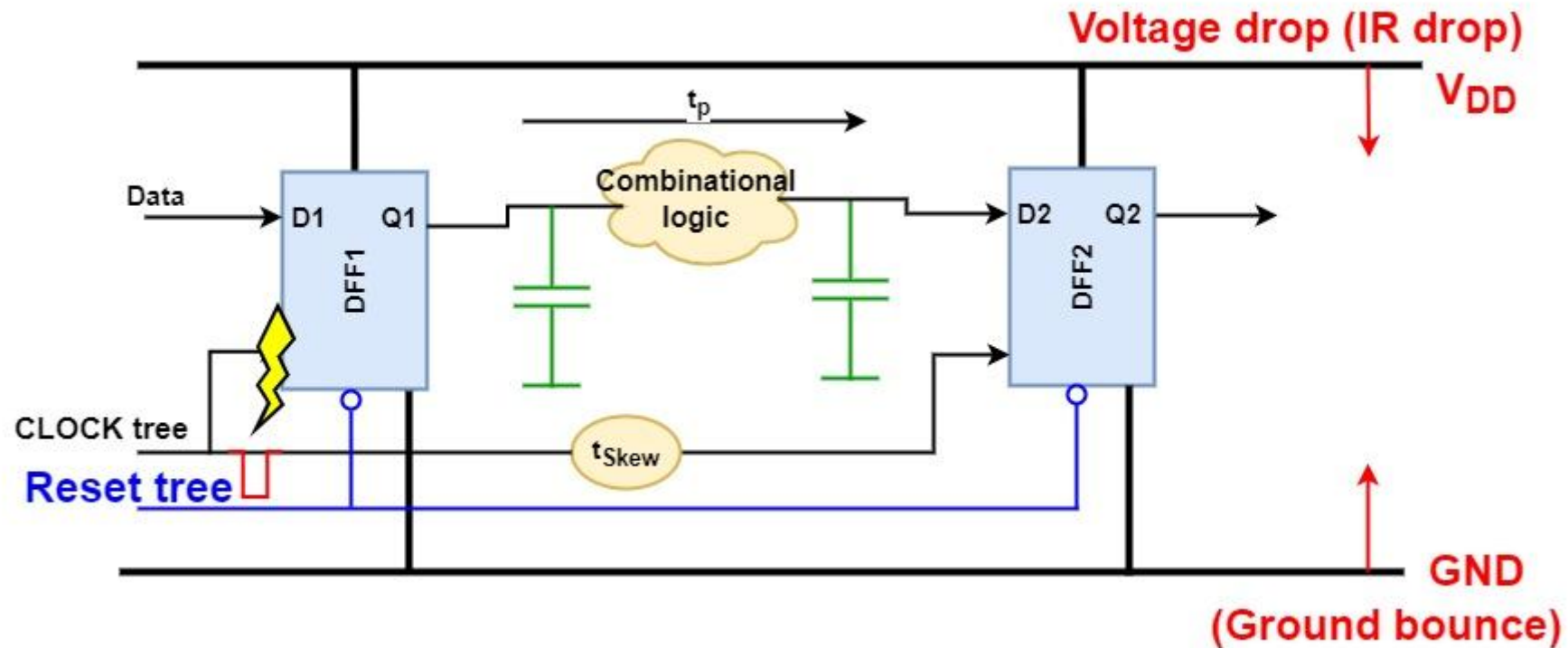


## ➤ Timing faults<sup>1</sup>: Timing violations fault model

- EM disturbances coupling with the target's Power Distribution Network (PDN)
- Increased critical path surpassing the clock period ( $V_{dd} \searrow \rightarrow t_p \nearrow$ )
- Bit-flip

<sup>1</sup>Amine Dehbaoui et al. « Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES ». In : 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012.

# State of the art: EMFI models



## ➤ Clock glitch fault mechanism<sup>5</sup>: Timing violations fault model

- EM disturbances induced glitches on the target's Clock Distribution Network (CDN)
- Shortened clock period
- Bit-flip

<sup>5</sup>Marjan Ghodrati et al. « Inducing local timing fault through EM injection ». In : 2018 55<sup>th</sup> ACM/ESDA/IEEE Design Automation Conference (DAC). IEEE. 2018