Securing the IOT against Fault Injection Attacks using Digital Sensors

18th CryptArchi Workshop - Porquerolles 2022

Roukoz Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, L. Sauvage

ANR-20-CYAL-0007

Thesis overview

- Part of the ANR Franco-German project **APRIORI**[1].

- Design a mesh architecture of several sensors dedicated to protect the *IoT* devices against Fault Injection attacks (FIA).

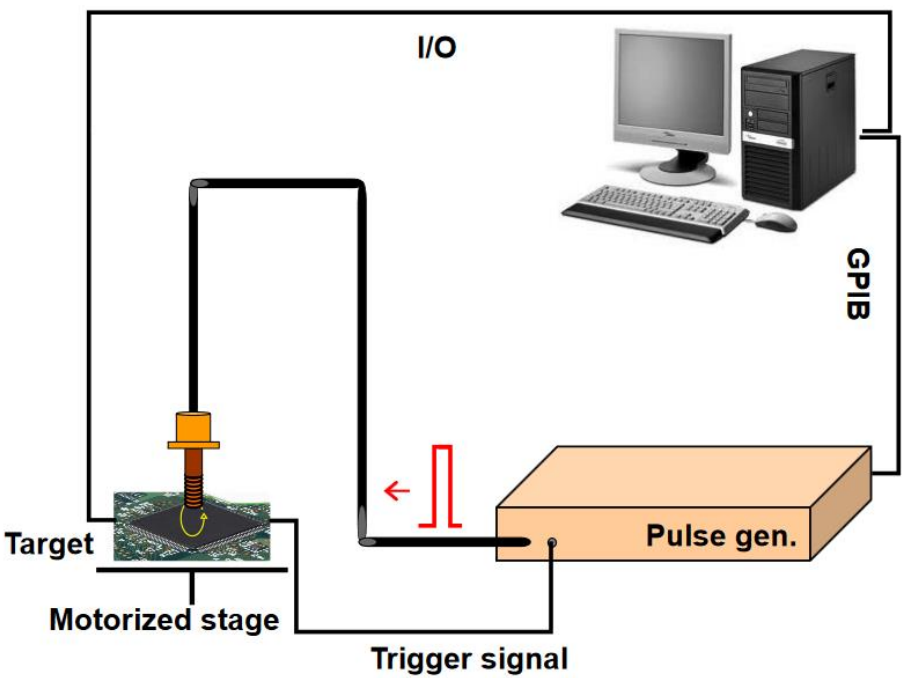
- The best detector of FIA should comply with several specifications:
  - ✓ Fully digital.
  - ✓ High detection rate against EMFI.
  - ✓ Easy to implement and low-cost at silicon area.
  - ✓ Embedded in ASICs and FPGAs implementation.
  - ✓ **Alert handler:** Alert the operator about deviations from normal operating conditions.

[1]**APRIORI**: Advanced PRivacy of IOt devices through Robust hardware Implementation. https://anr.fr/Project-ANR-20-CYAL-0007

Outline

- Previous works.
- The fully digital detector.
- EMFI platform.
- DUT block diagram.
- Experimental results.
- Synthesis.
- Conclusion.

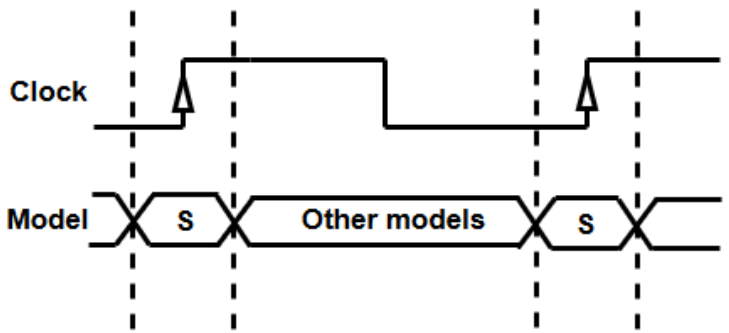
ElectroMagnetic Fault injection (EMFI)



- Sending a voltage pulse into a homemade EM probe located over a chip.
- An EM coupling created between the probe and the power tree of the target.
- Inducing a transient voltage inside the chip.
- Corrupting the normal operation.
- Injecting fault.

EM injection probe:
Several turns of copper wire coiled around a cylindrical ferrite core.

Previous works



S: Sampling fault model.

Recent publications[1] presumed that EMFI models are:

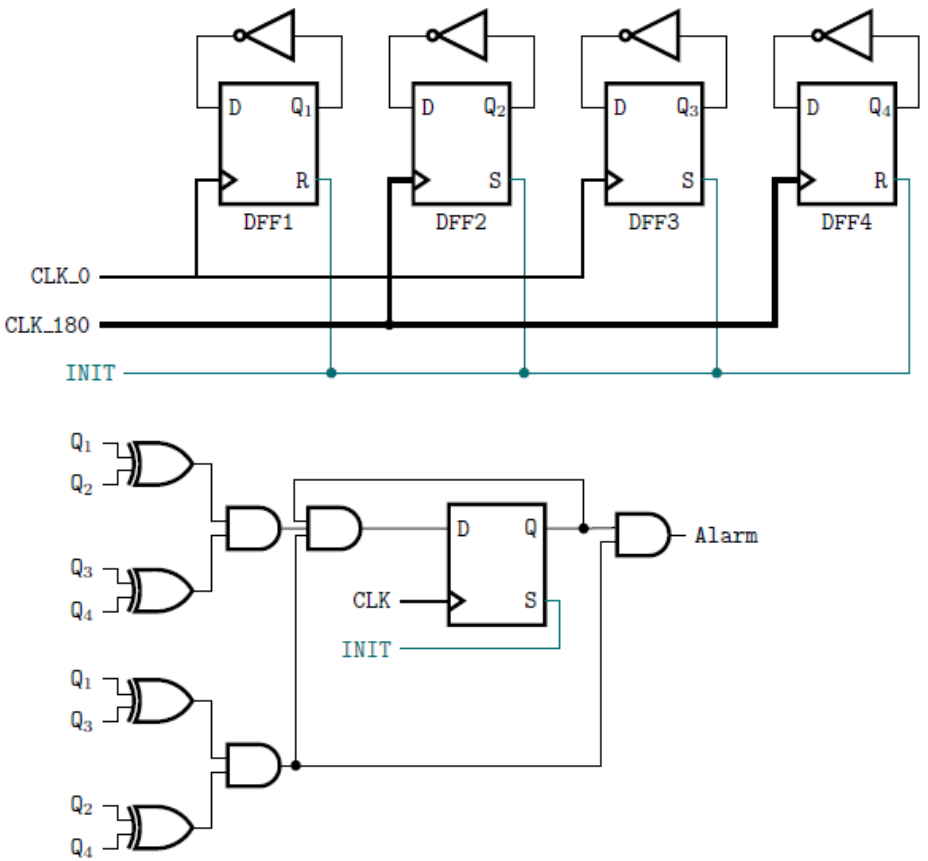
- Sampling fault models around the clock rising edge.
- Elsewhere not specified.

- Reused the **fully digital detector** designed by *D. EL-Baze et al*[2].
- Detector based on sampling fault mechanisms.

[1] M. Dumont, P. Maurine, and M. Lisart, "Modeling of electromagnetic fault injection," in 2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 2019, pp. 246–248

[2] D. El-Baze, et al., An embedded digital sensor against EM and BB fault injection. FDTC 2016

Fully digital detector*

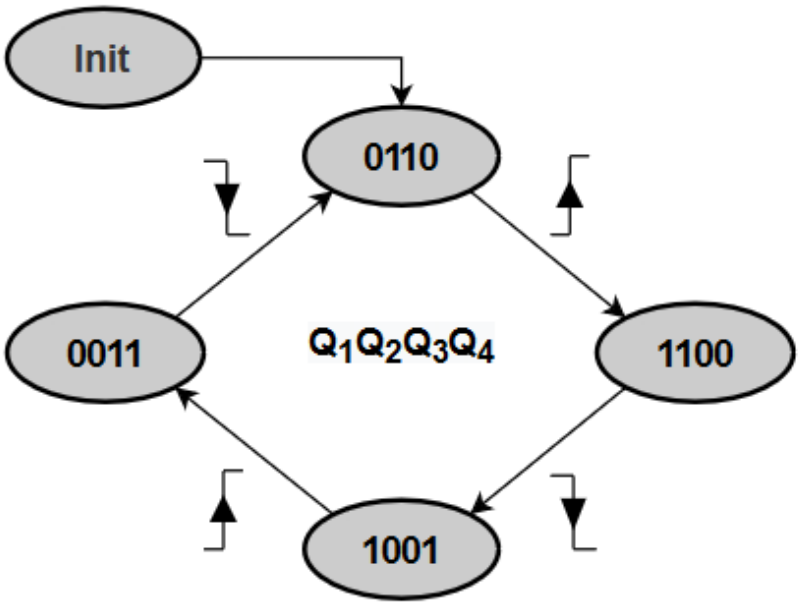


- Architecture description:
  - Two DFFs (DFF1&DFF3) toggling on clock rising edge of the principal clock signal.
  - Two DFFs (DFF2&DFF4) toggling on clock rising edge of the clock signal phase-shifted by 180°.
  - DFF1 and DFF4 are initialized at 0.
  - DFF2 and DFF3 are initialized at 1.
  - Initial combination is 0110.

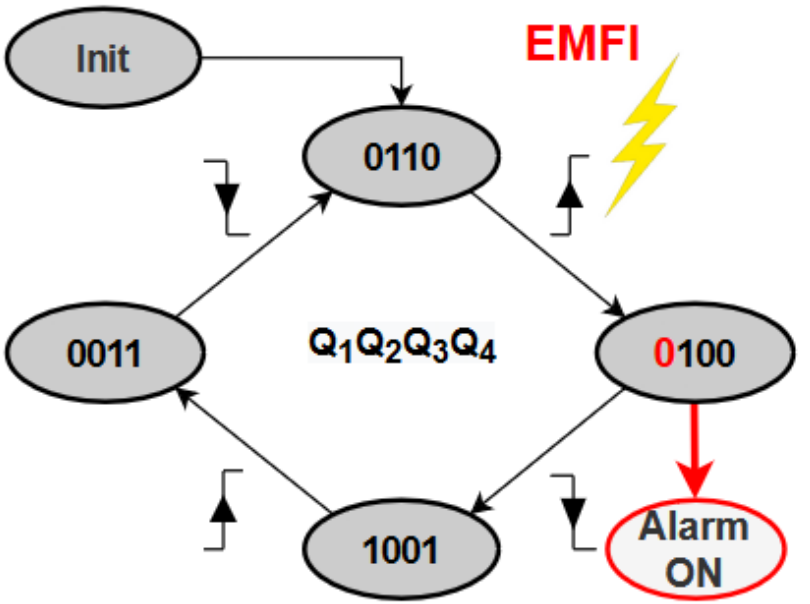
Alarm is raised for any deviation in $Q_1Q_2Q_3Q_4$ states from the normal behavior.

*D. El-Baze, et al., An embedded digital sensor against EM and BB fault injection. FDTC 2016

How does this detector work?



Normal behavior



Under attack behavior

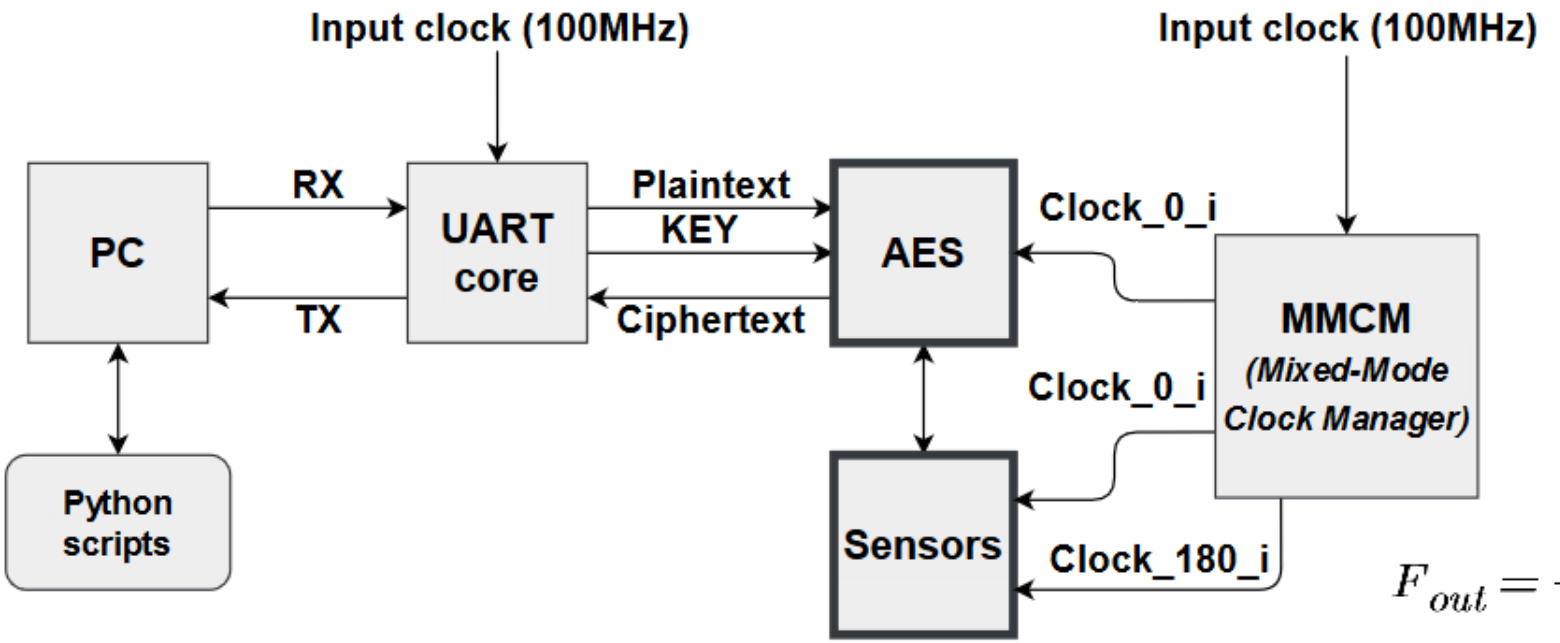
Alarm is raised for any deviation in $Q_1Q_2Q_3Q_4$ states from the normal behavior.

FPGA target for FIA exp.

➢ FPGA target

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

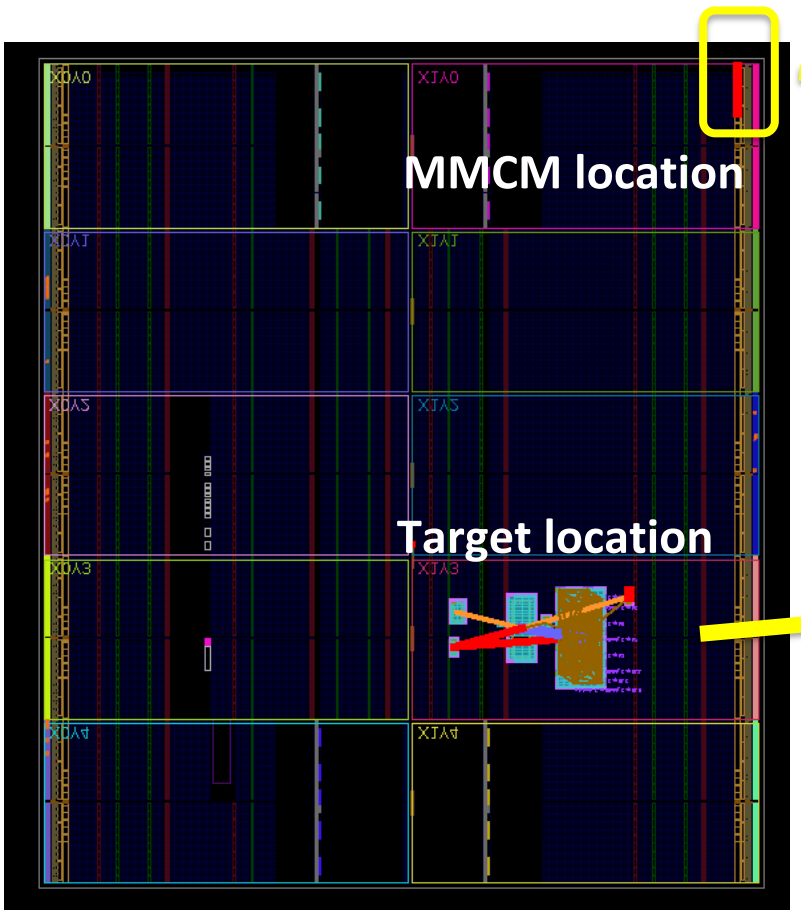
DUT block diagram: AES + sensors.



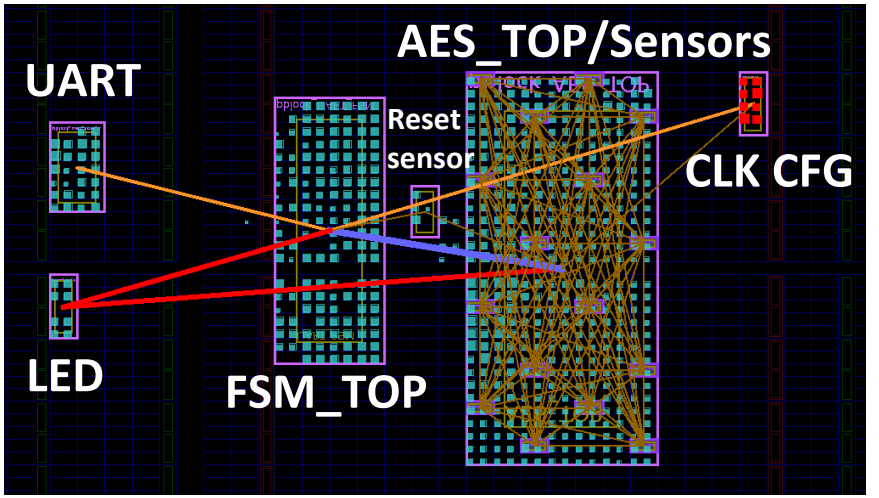
$$F_{out} = \frac{M}{D*O} F_{in}$$

- *Mixed-mode clock management (MMCM)* module authorizes a:
  - Dynamic reconfiguration for the divide counters (M, D, O).
  - Dynamic change of the output clock frequency.
  - **Keep the same hardware implementation for all experiments** →no modification of the bit stream file.

FPGA implementation : Floorplan

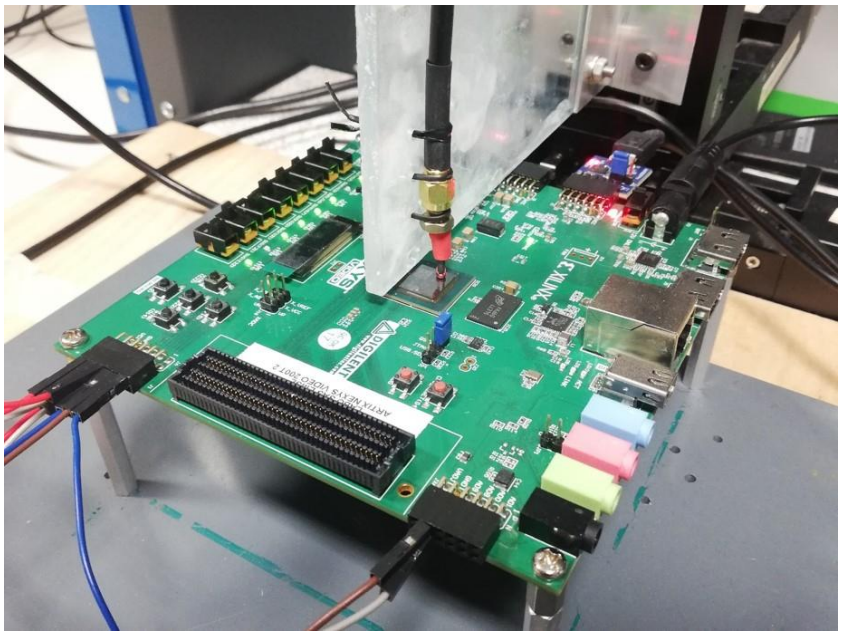


- Default MMCM advanced IP block:
  - MMCME2 ADV



16 sensors embedded in the AES.

EMFI platform

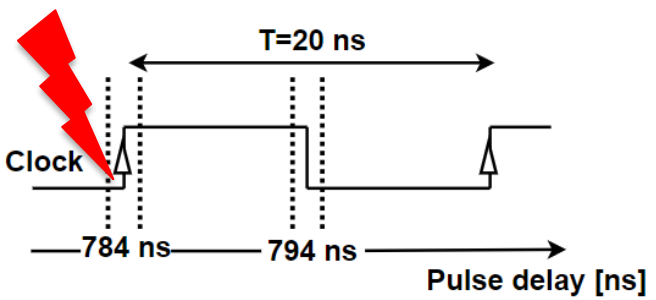


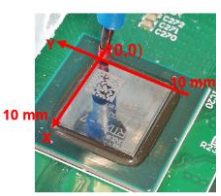
- AV-Tech voltage pulse generator
  - Pulse amplitude: up to +/- 750V.
  - Pulse-width: 4.5-20ns.
  - Pulse rise and fall time: 4 ns.
  - Remotely controlled using the telnet protocol.

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

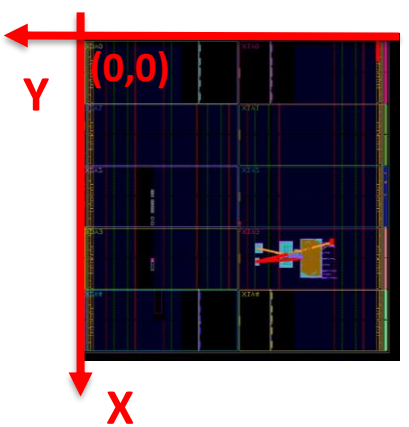
Spatial exploration (50 MHZ) (1)

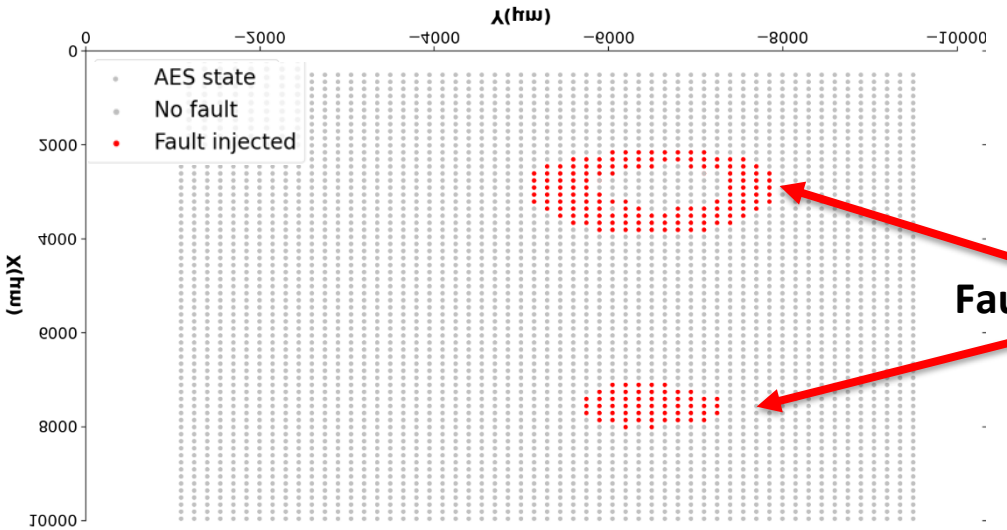
- **Sensitivity map around the CLK rising edge.**
- Clock frequency=50MHz.
- Pulse amplitude=420V.
- Pulse delay=784 ns (R6).

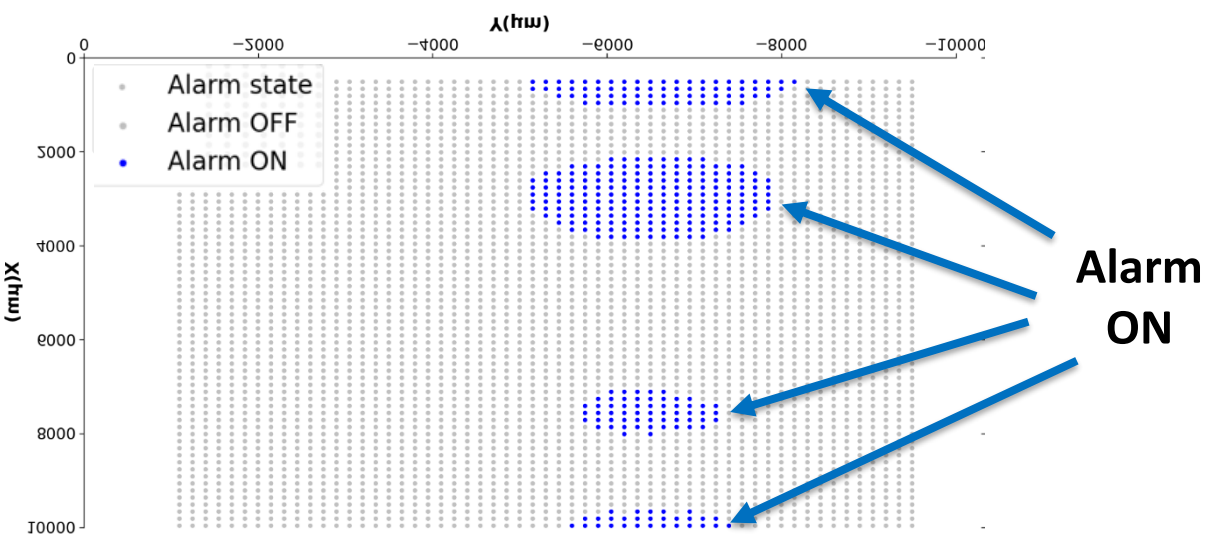




Artix-7 chip

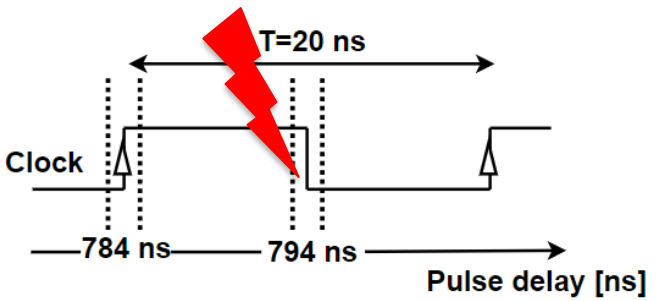


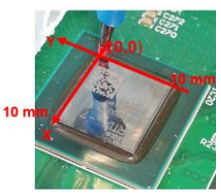




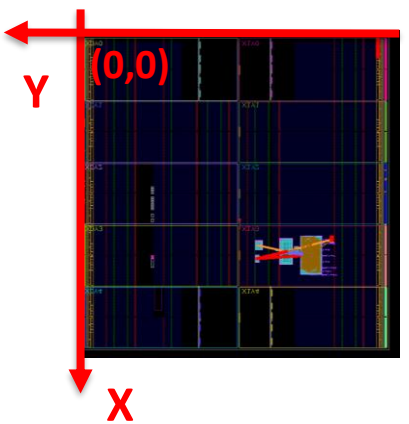
Spatial exploration (50 MHZ) (2)

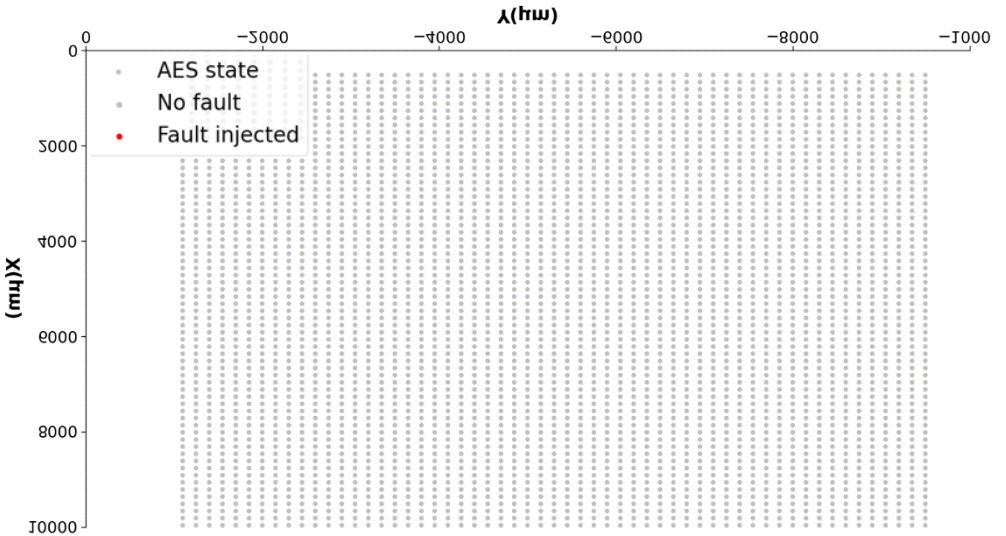
- **Sensitivity map around the CLK falling edge.**
- Clock frequency=50MHz.
- Pulse amplitude=420V.
- Pulse delay=794 ns (R6).



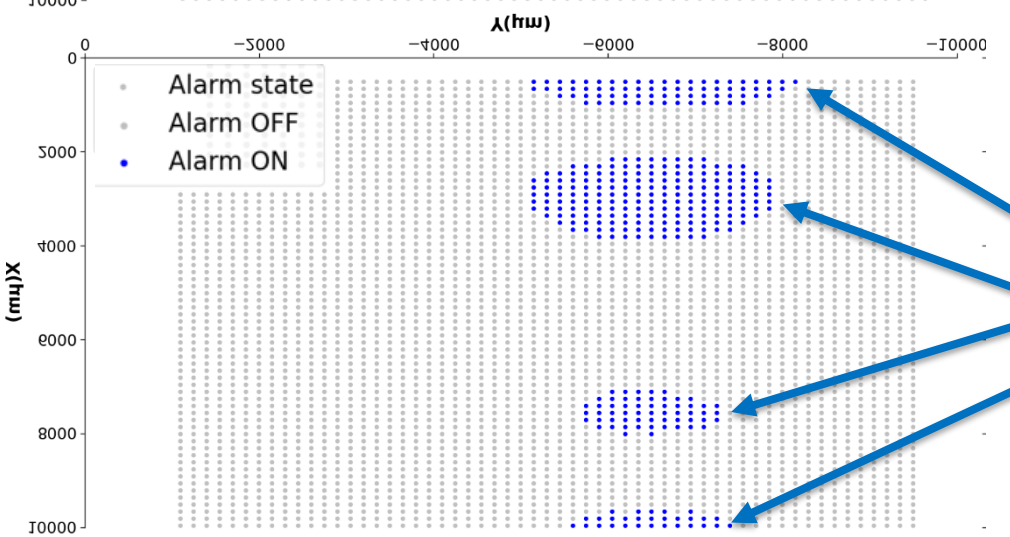


Artix-7 chip





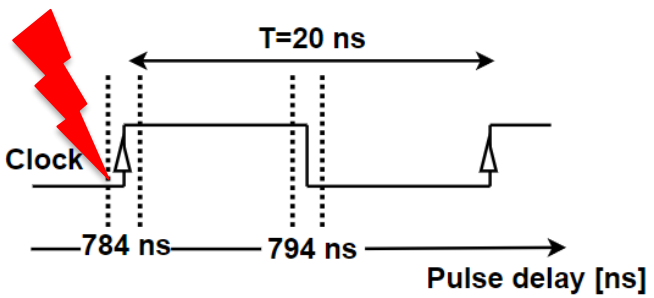
No Fault injected

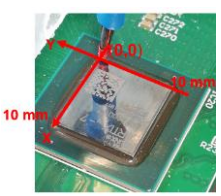


Alarm ON

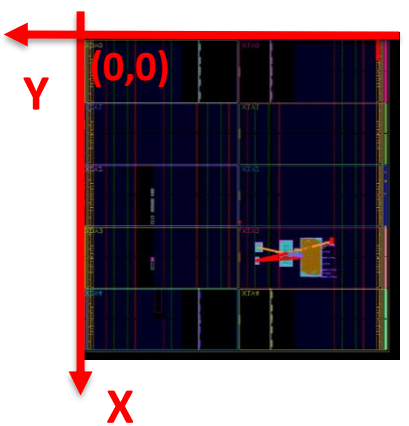
Spatial exploration (50 MHZ) (3)

- **Sensitivity map around the CLK rising edge.**
- Clock frequency=50MHz.
- Pulse amplitude=420V.
- Pulse delay=784 ns (R6).

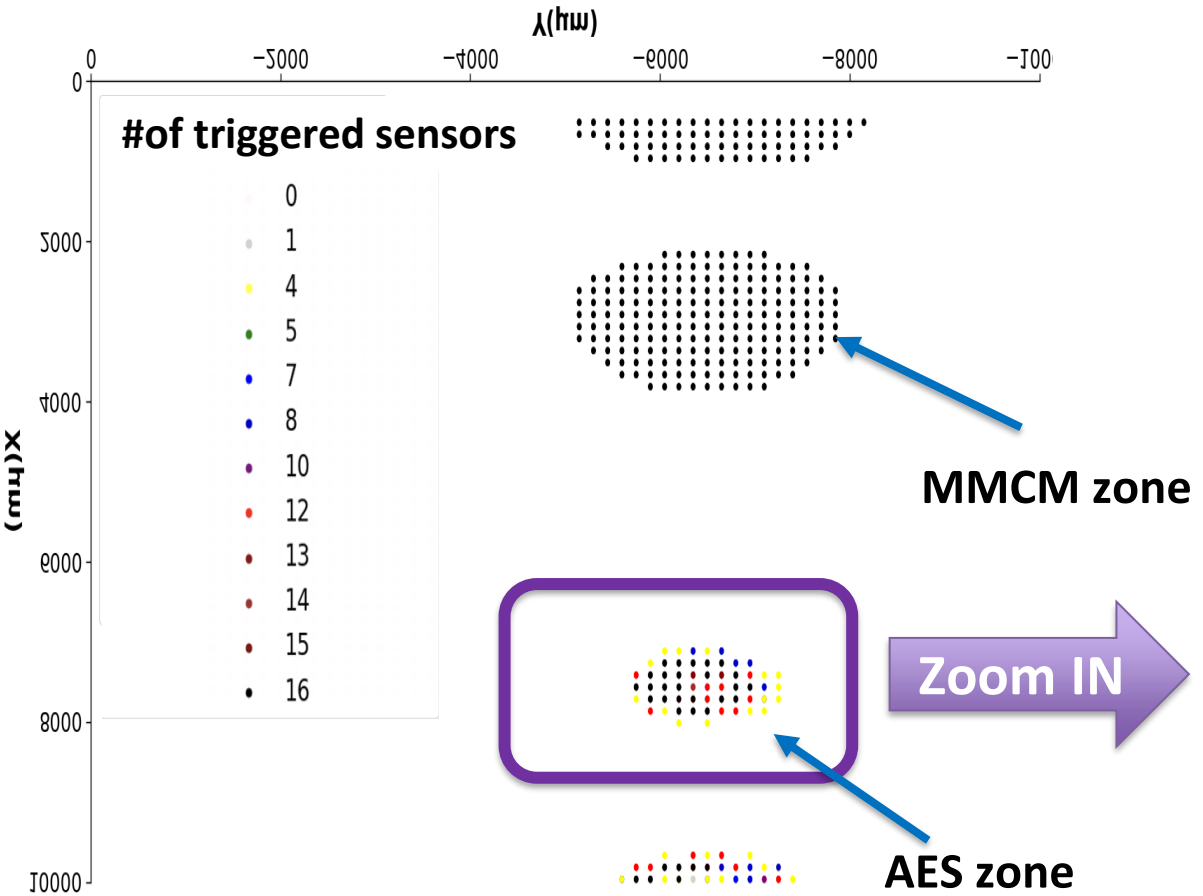




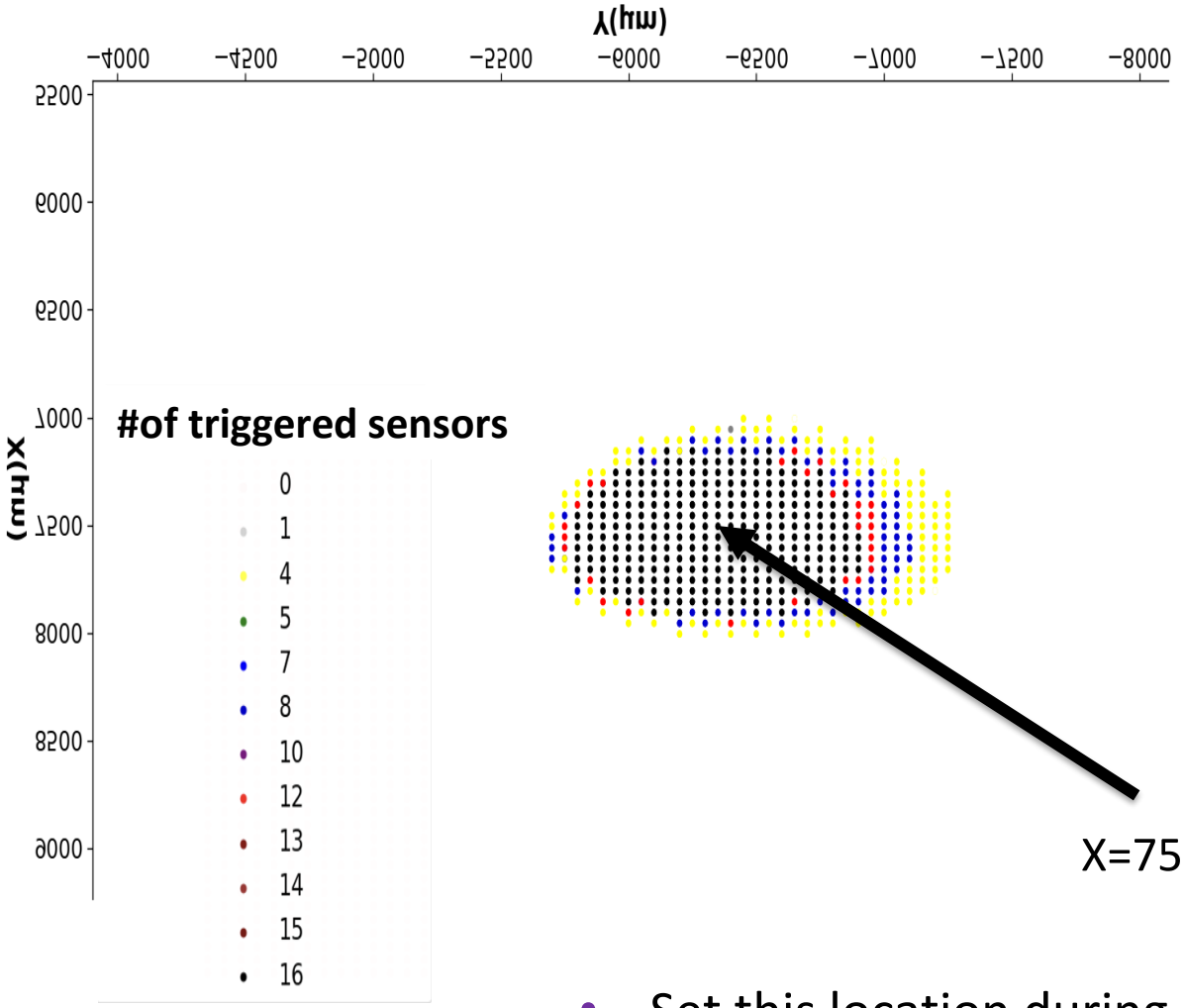
Artix-7 chip



Examine the number of triggered sensors



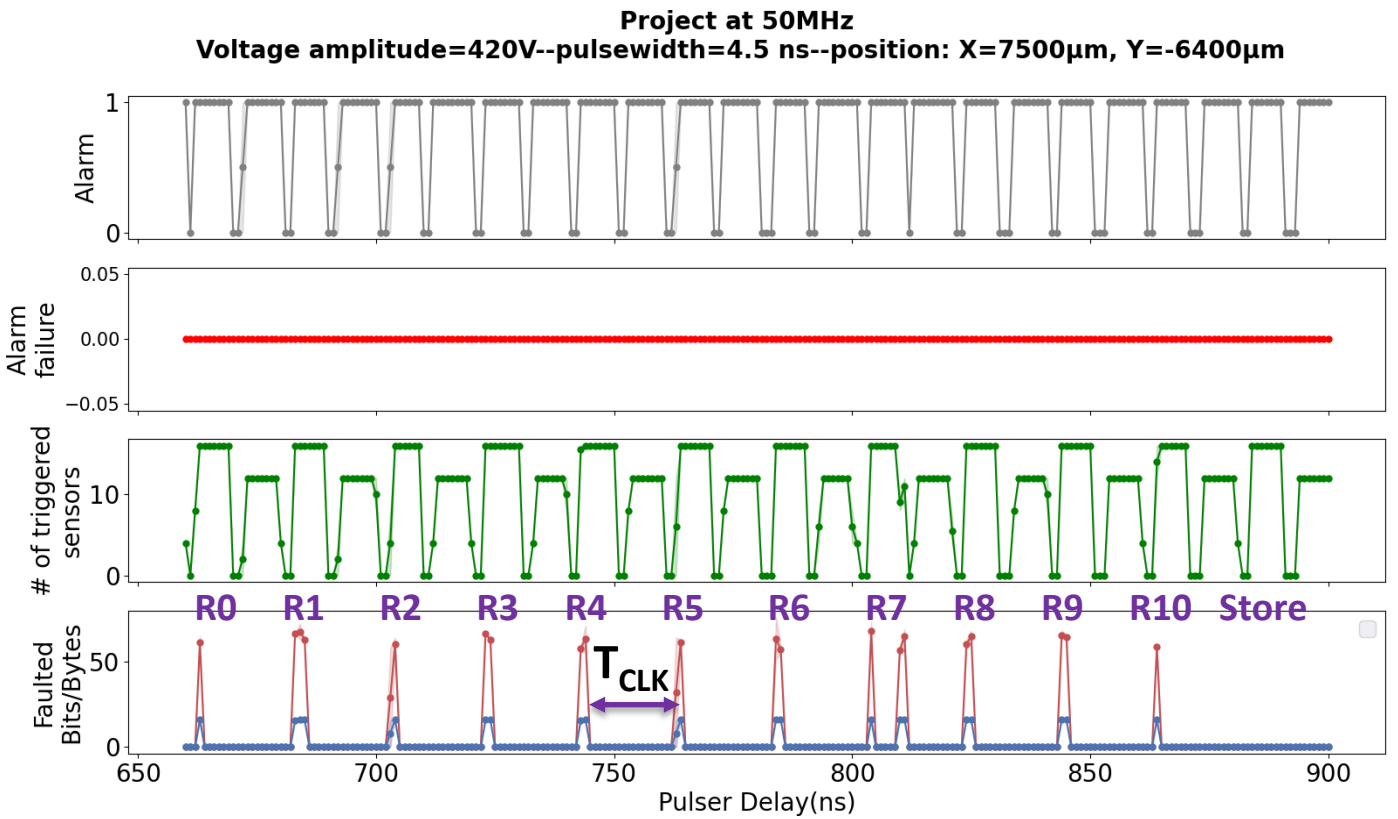
Sensitive zone



X=7500µm;Y=-6400µm

- Spatial distribution of the number of triggered sensors.
- Set this location during all FIA experiments.

EMFI results: project behavior at 50MHZ

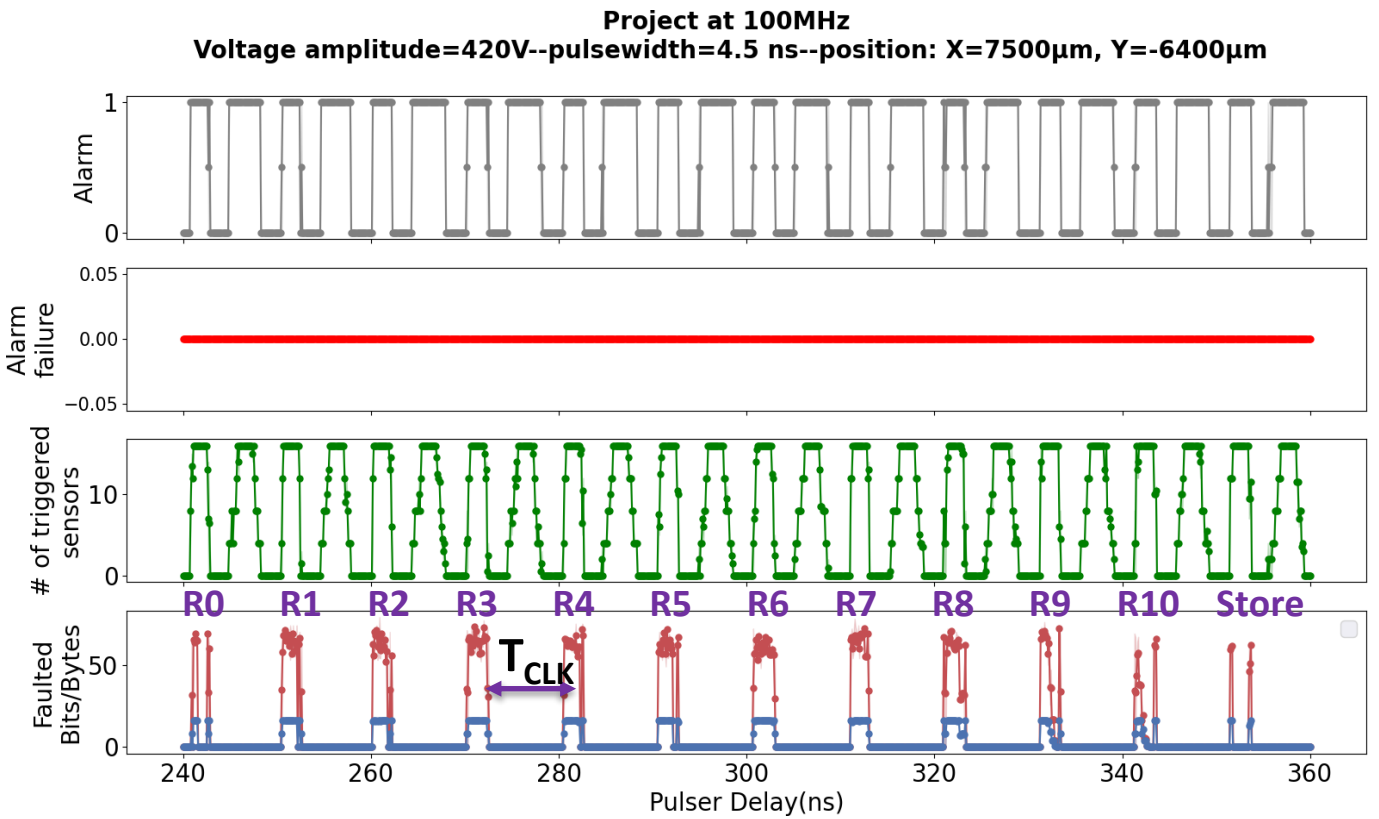


- No alarm failure → All injected faults are detected.

- Width of the detection windows *(Sensors):* 7 ns.
- Number of the triggered sensors: 12-16.
- Width of the injection windows *(AES):* 2-3 ns.

- **Sampling fault model.**

EMFI results: project behavior at 100MHZ

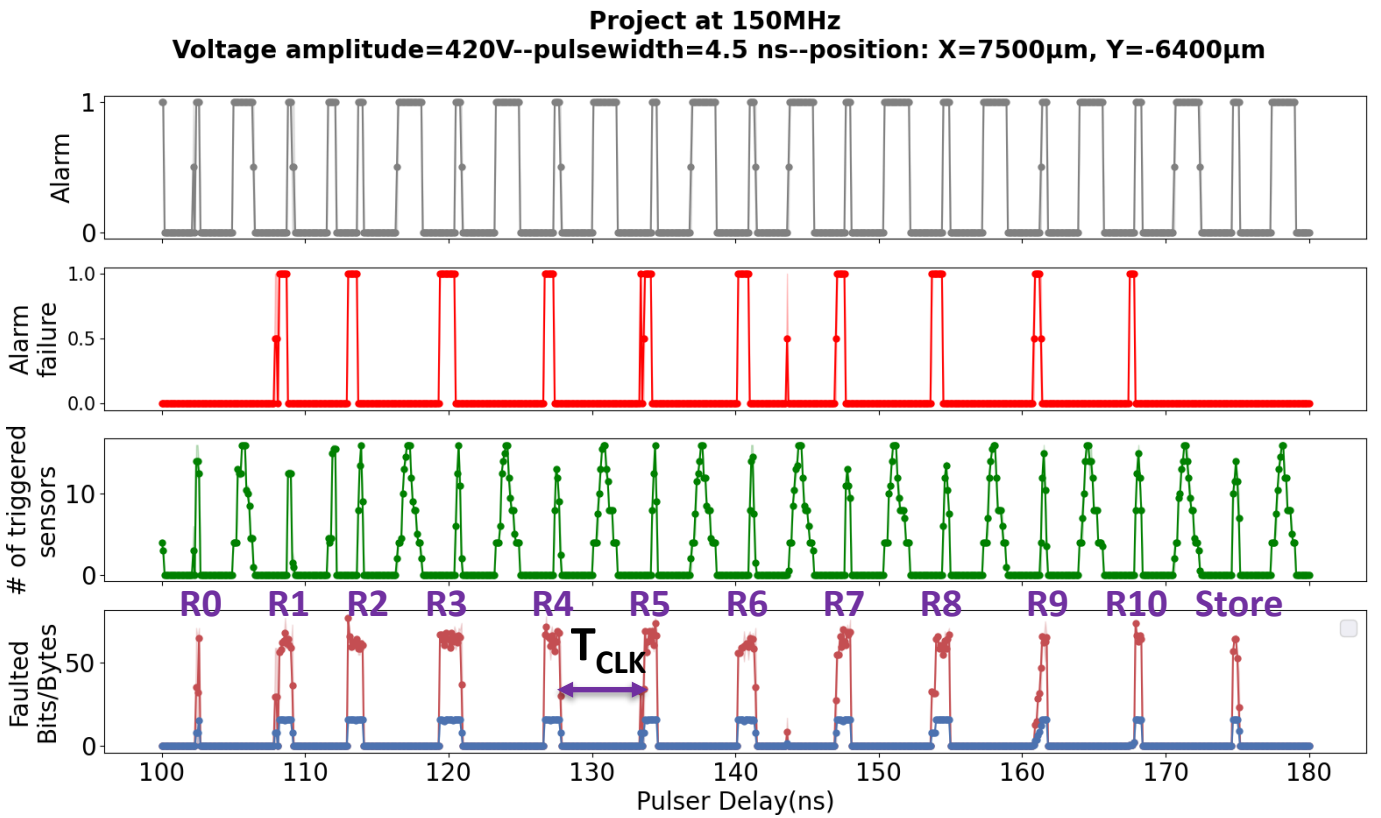


- No alarm failure →All injected faults are detected.
- Effect of the temporal step on the number of triggered sensors.

- Width of the detection windows: 2-3ns.
- Number of the triggered sensors: 8-16.
- Width of the injection windows: 1,5-2,2 ns.

- **Sampling fault model.**

EMFI results: project behavior at 150MHZ

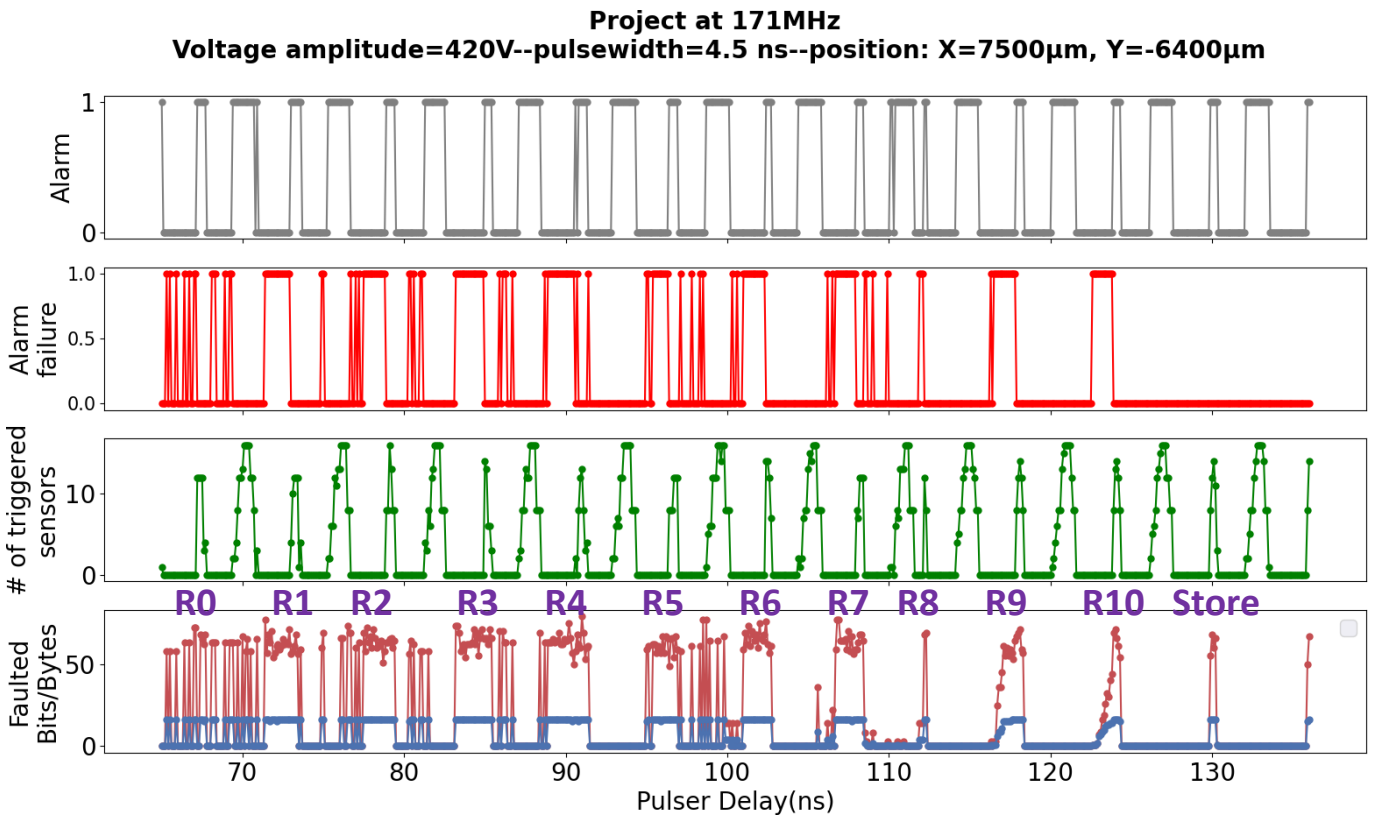


- Appearance of undetected fault windows.

- Width of the detection windows: 0,6-1,2 ns.
- Number of the triggered sensors: 8-16.
- Width of the injection windows: 1,1 ns.

- **Is there only sampling fault model or are there others?**

EMFI results: project behavior at 171MHZ

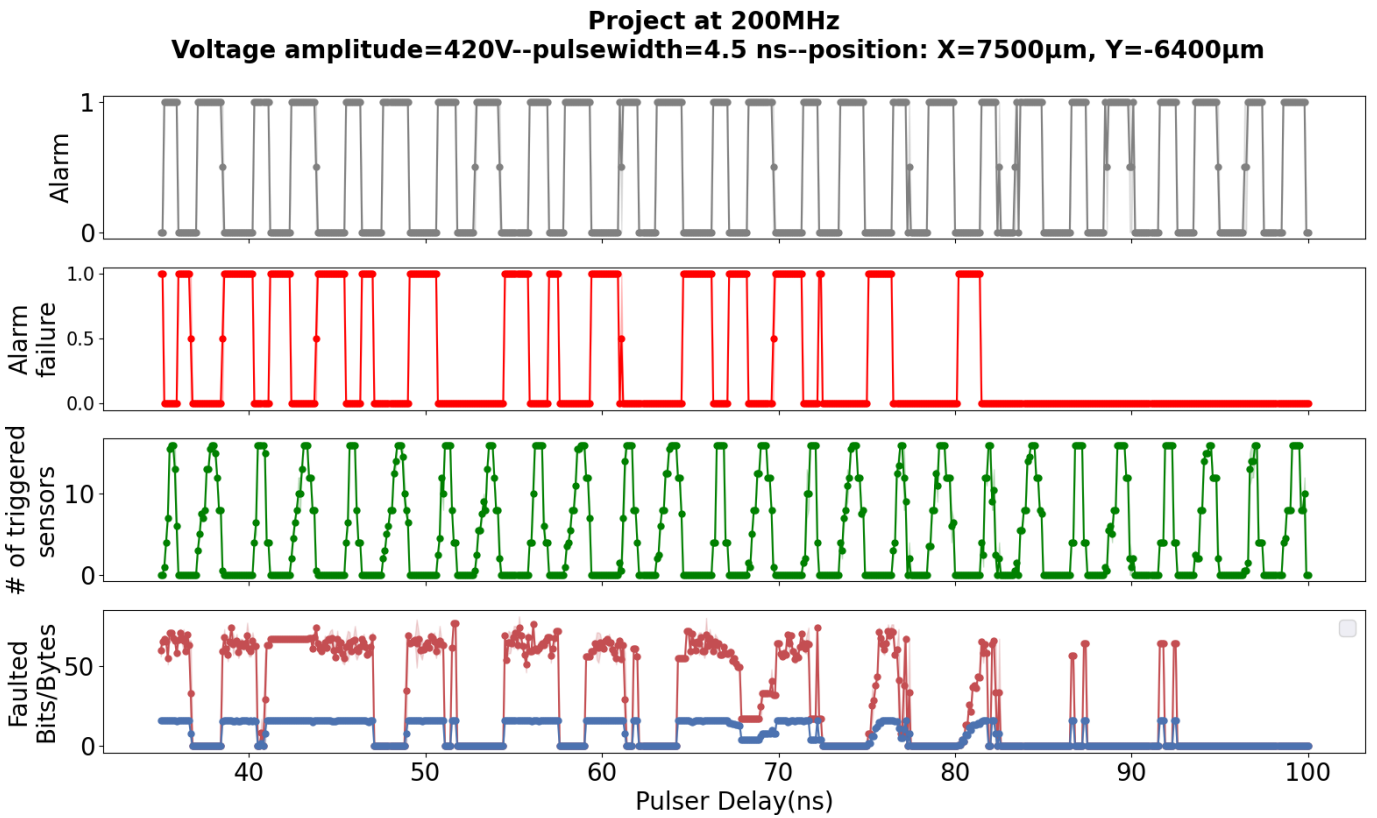


- Obtaining undetected fault windows →**limitation in the performance of these sensors.**
- The repeatability and properties of these faults match the principle of **timing faults violation**.

- Width of the detection windows: 0,4-1,1 ns.
- Number of the triggered sensors: 8-16.
- Width of the injection windows: 1,2-2.5 ns.

- **Timing fault model in addition to sampling fault model.**

EMFI results: project behavior at 200MHZ

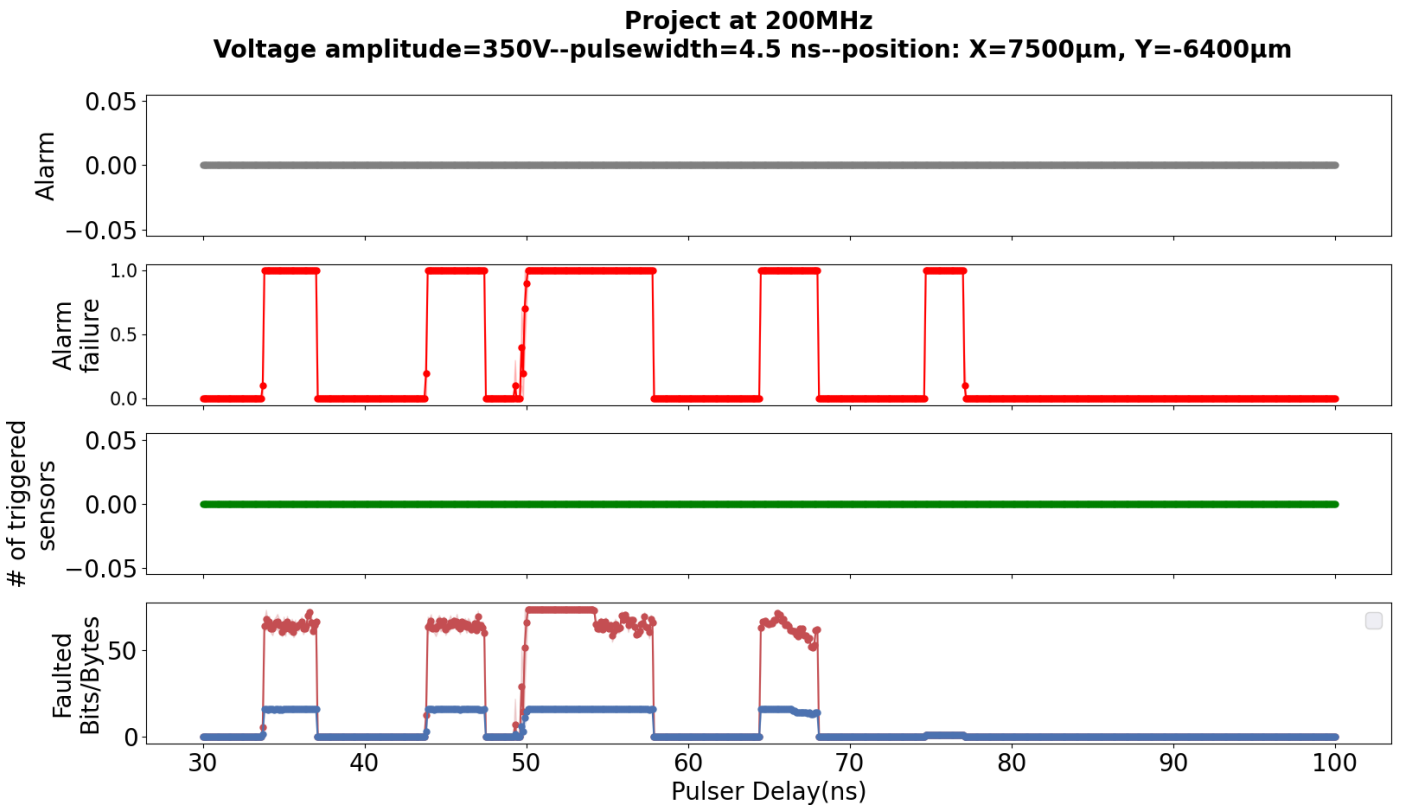


- Critical path of the DUT < 5 ns.
- Study the project behavior close to the DUT max frequency.
- Bad detection rate for these sensors at high clock frequency.

- Width of the detection windows: 0,6-1 ns.
- Number of the triggered sensors: 8-16.

- **Timing fault model in addition to sampling fault model.**
- **No need for a strong EM stress to inject faults.**

EMFI results: project behavior at 200MHZ

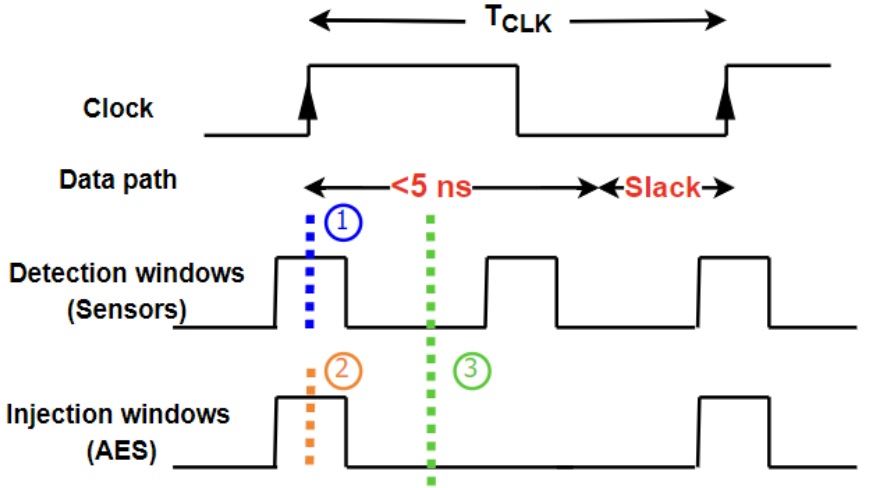


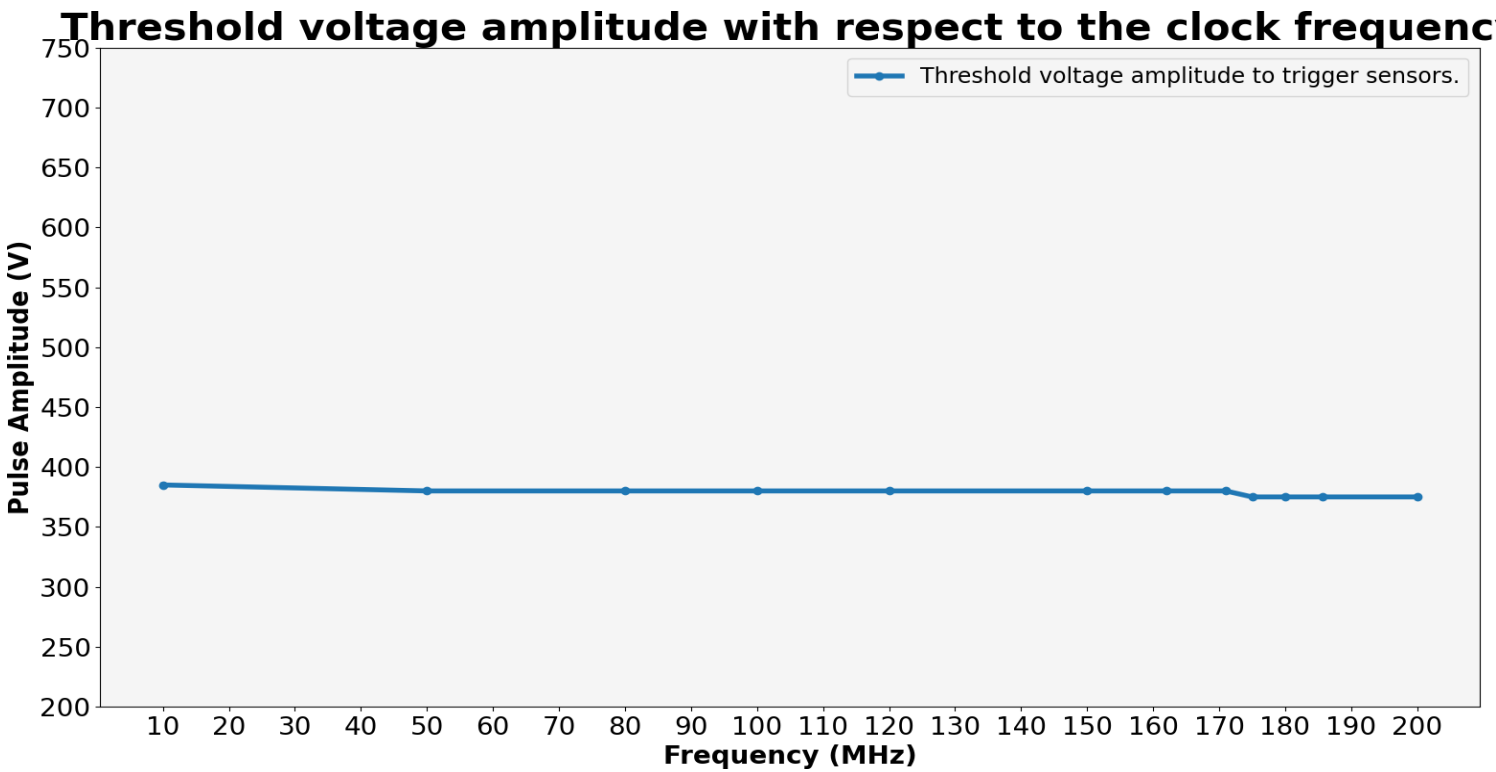
- Decreasing the voltage amplitude from 420V to 350V.

- None of these sensors are triggered.
- Timing fault model only.

Discussions (1)

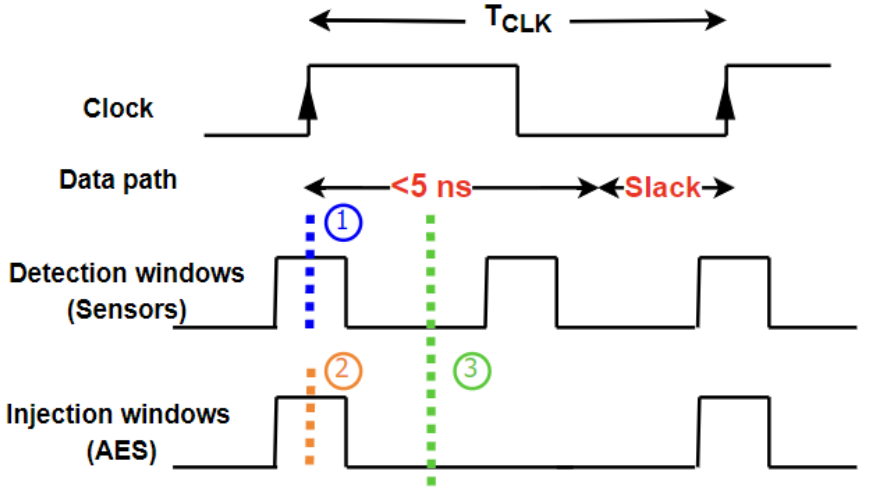
Threshold voltage amplitude required to inject sampling faults in the detectors.

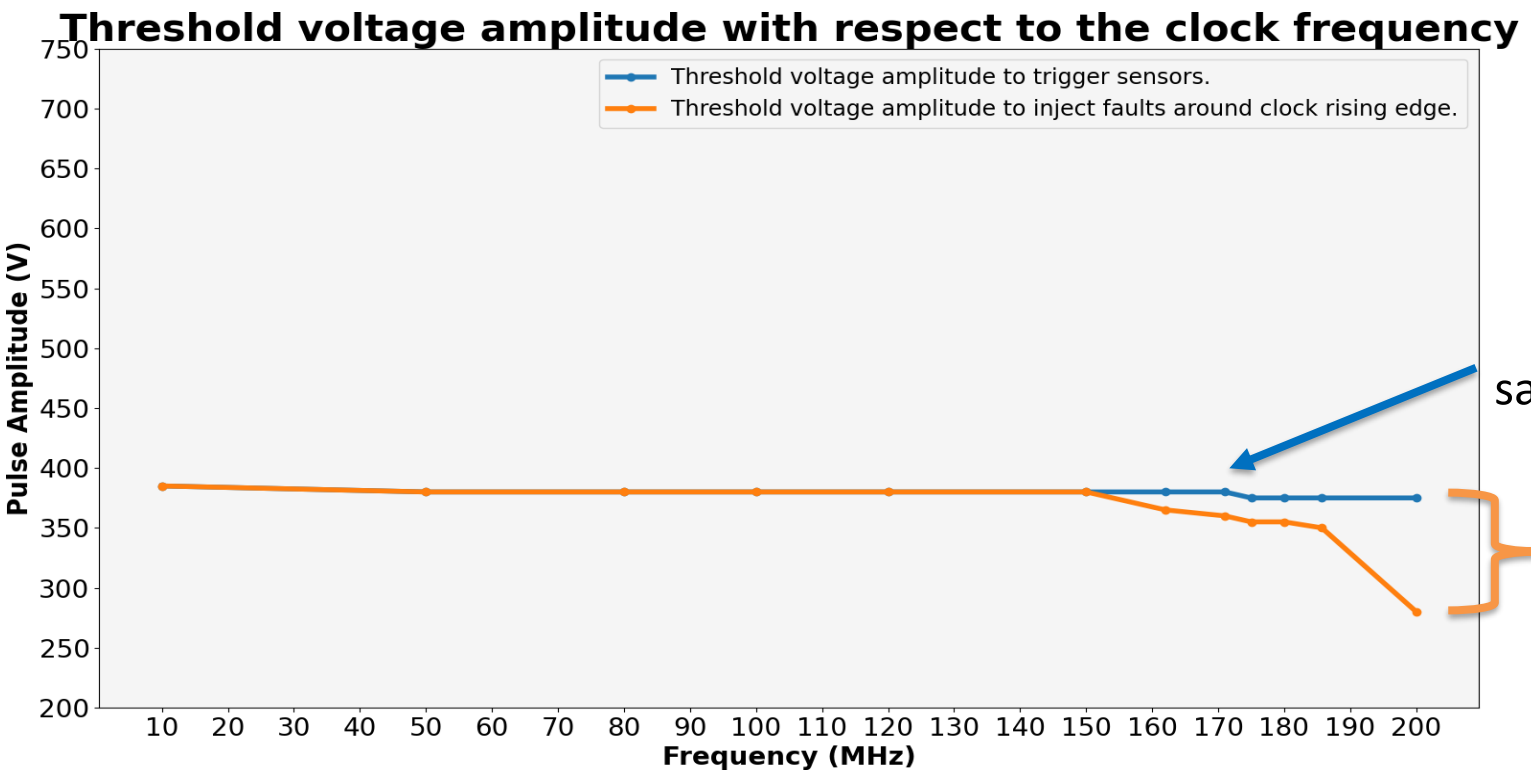




Discussions (2)

Threshold voltage amplitude required to inject faults in the AES around the CLK rising edge.



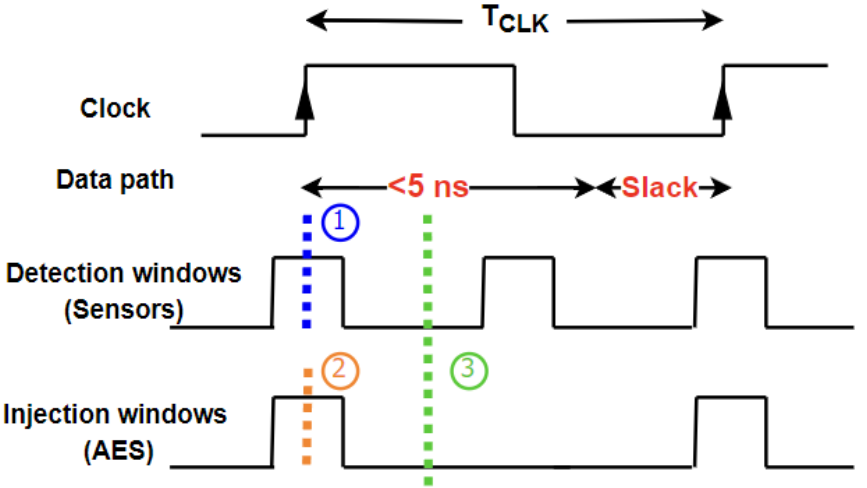


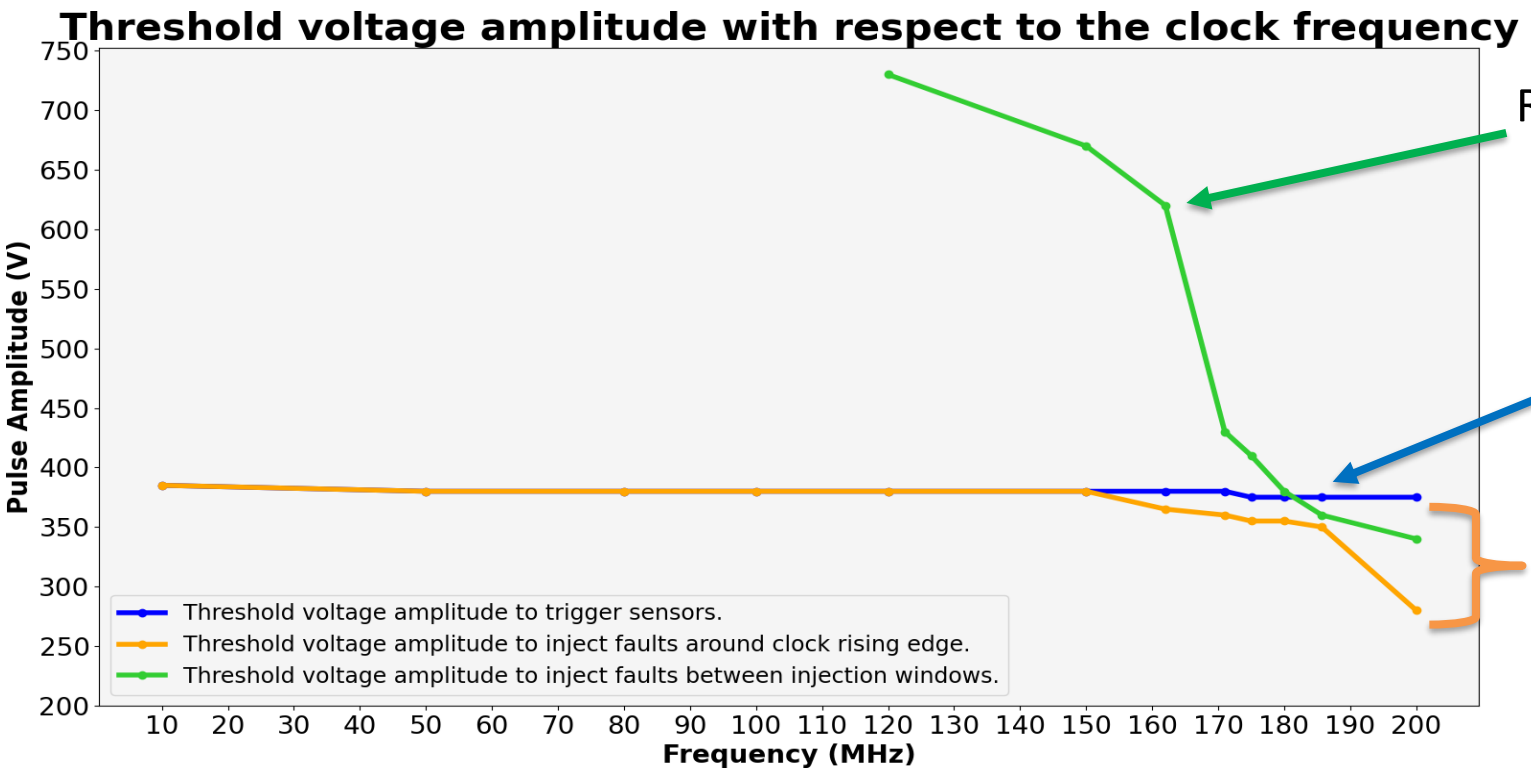
Threshold of the sampling fault model

Timing fault model only.

Discussions (3)

Threshold voltage amplitude required to inject faults in the AES between injection windows.



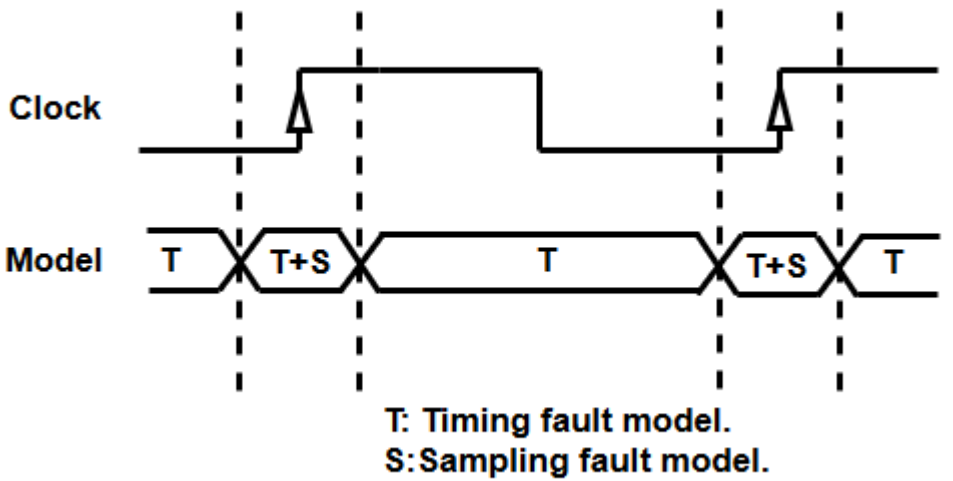


Reflection of the timing slack

Threshold of the sampling fault model

Timing fault model only

Synthesis: EMFI model



- Evidence of the coexistence between sampling and timing fault models:
  - ✓ Timing Faults could be injected anywhere during the clock period.
  - ✓ Sampling Faults could be injected only around the clock rising edge.

Synthesis: Fully digital detector effectiveness

- High detection of sampling fault model at low frequencies *(f<150 MHz)* by the current sensor.
- No detection of timing fault model obtained at high frequencies *(150 MHz<F<200MHz).*

Further works

- Study the existence of others EMFI models.
- Examine the EMFI types (bit set, reset, flip…).
- Development of a new sensor that detects both fault models.
- Design of a sensor embedded in a 22 nm ASIC.

MINES Saint-Étienne
Une école de l'IMT

APRIORI

Questions

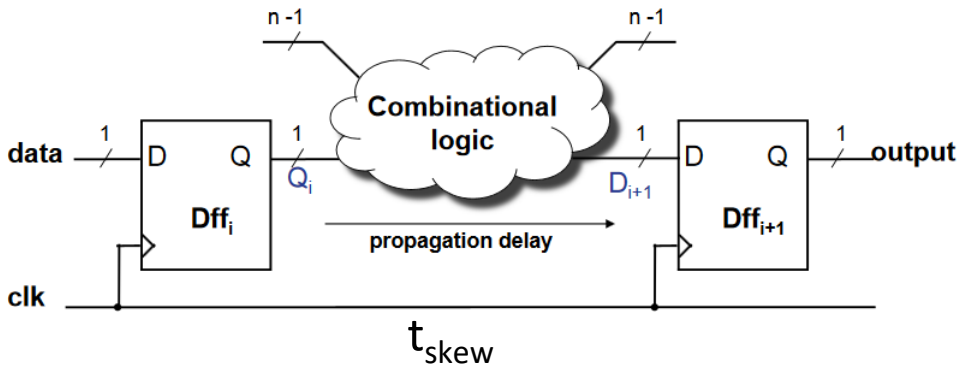
Contact: roukoz.nabhan@emse.fr

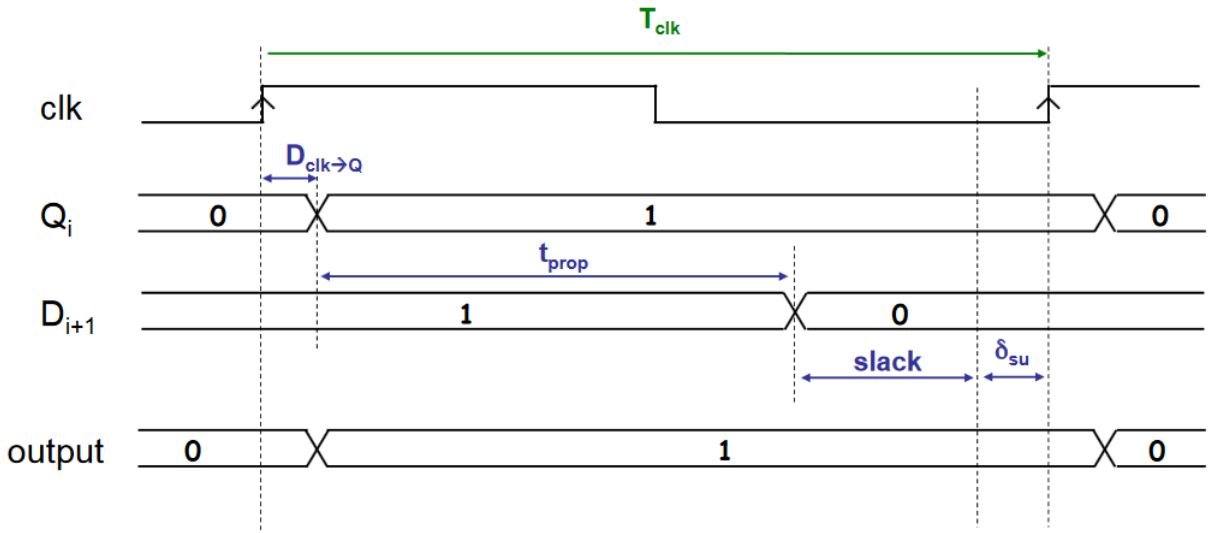
MINES Saint-Étienne
Une école de l'IMT

TELECOM ParisTech
Une école de l'IMT

Institut Mines-Télécom

Internal architecture of combinatorial logics





$$T_{CLK} = D_{CLK \to Q} + t_{prop\ delay} + \delta_{su} - t_{skew} + Slack$$

$$T_{CLK} = Length\ of\ the\ critical\ path\ + Slack$$