FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

A Tale of Two Models: Discussing the Timing and Sampling EM Fault Injection Models

Roukoz Nabhan*, **Jean-Max Dutertre***, **Jean-Baptiste Rigaud***, **Jean-Luc Danger†** and **Laurent Sauvage†**

*Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France
†LTCI, Télécom Paris, Institut Mines-Télécom, 91120 Palaiseau, France
*{roukoz.nabhan, dutertre, rigaud}@emse.fr
†{jean-luc.danger, laurent.sauvage}@telecom-paris.fr

MINES Saint-Étienne
Une école de l'IMT

TELECOM ParisTech
Une école de l'IMT

Institut Mines-Télécom

APRIORI

anr
ANR-20-CYAL-0007

Introduction

- Securing Integrated Circuit (IC) against fault injection attacks is an ongoing challenge
- Developing effective on-chip detection sensors as countermeasures against ElectroMagnetic Fault Injection (EMFI)
- Study the mechanism involved in injecting faults due to EM disturbances
- Test the effectiveness of the fully digital detector designed by *Elbaze et al.* embedded in an AES accelerator

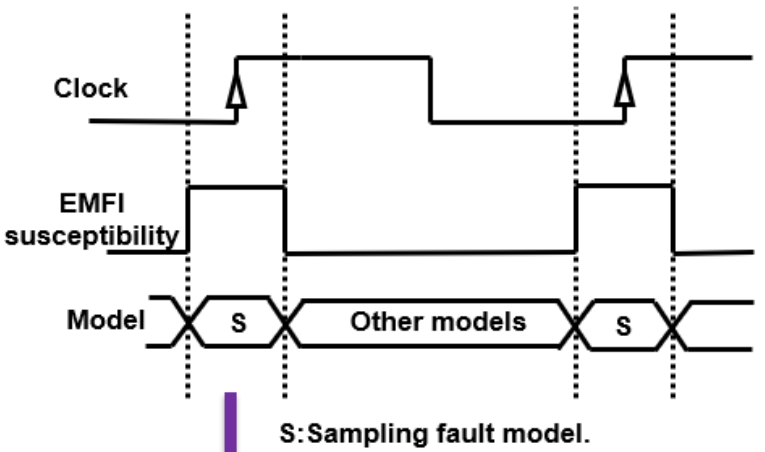
Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

Outline

- **Previous work**
  - **EMFI models**
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

EMFI models: sampling fault model



- Previous publications[1,2,3] explained EMFI models through **sampling fault models**:
  - Occurs around the clock rising edge within EMFI susceptibility windows
  - Fault windows width is constant and independent of the clock frequency
  - Bit-set or bit-reset depend on the polarity of the pulse
- Based on an experimental results and modeling of the EMFI effect on the Power Distribution Network (PDN) of a generic IC

[1] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 183–197, 2017.
[2] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital em pulse detector," in 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 2016, pp. 439–444.
[3] 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

EMFI models: timing violations fault model

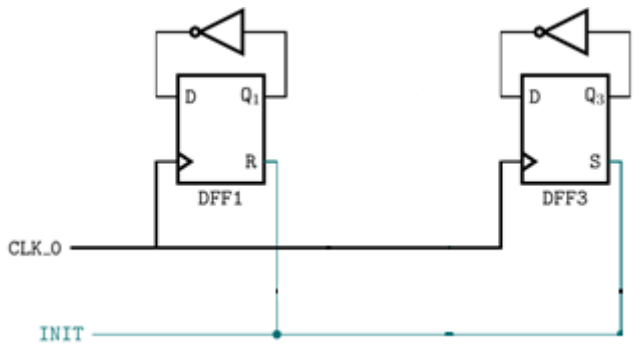
- Timing faults[1]
  - EM disturbances coupling with the target's PDN
  - Increased critical path surpassing the clock period
  - Bit flip
- EMFI-induced clock glitches[2]
  - EM disturbances coupling with the target's Clock Distribution Network (CDN)
  - Shortened clock period
  - Bit flip

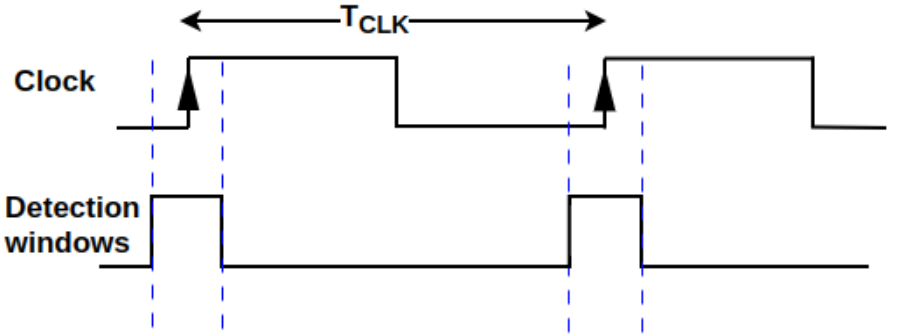
[1]A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012, 2012, pp. 7–15.
[2]M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, and P. Schaumont, "Inducing local timing fault through em injection," in 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC). IEEE, 2018, pp. 1–6

Outline

- Previous work
  - EMFI models
  - **Fully digital detector**
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

From sampling fault model to digital sensor

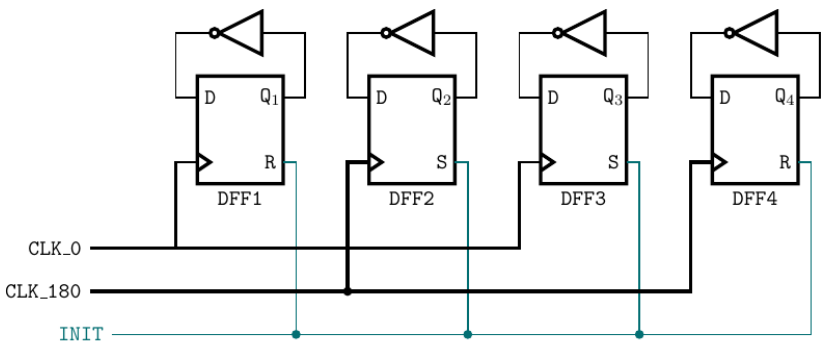


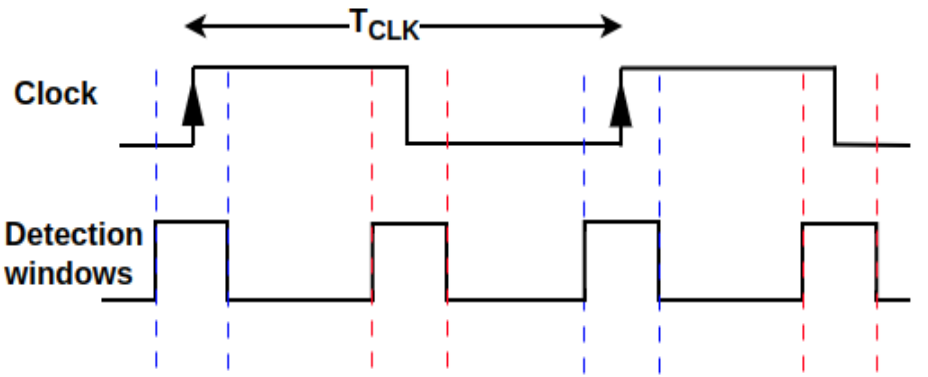


- **Two** DFF toggling on CLK rising edges
- Resp. initialized at 0 (DFF1) and 1 (DFF3) to monitor both 1→0 and 0→1 transitions

D. El-Baze, J. -B. Rigaud and P. Maurine, "An Embedded Digital Sensor against EM and BB Fault Injection," *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2016

From sampling fault model to digital sensor

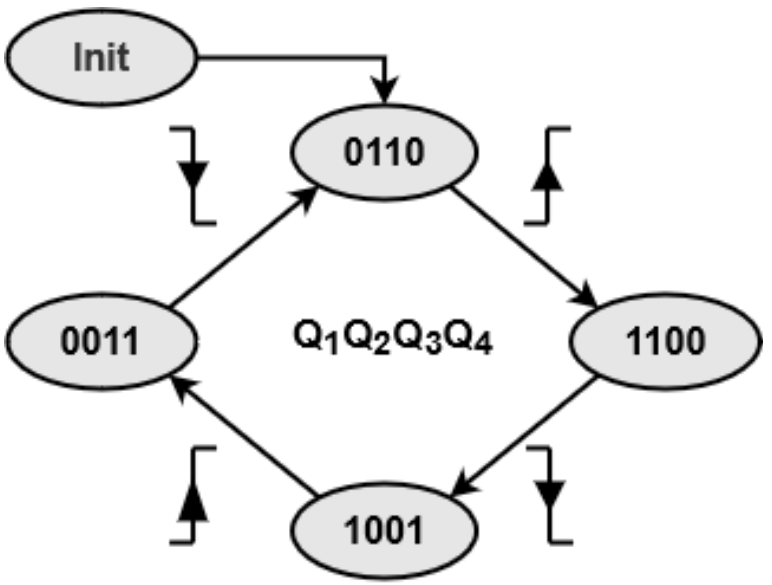




- **Four** DFF toggling on CLK rising and falling edges
- Goal: increase the faults detection windows

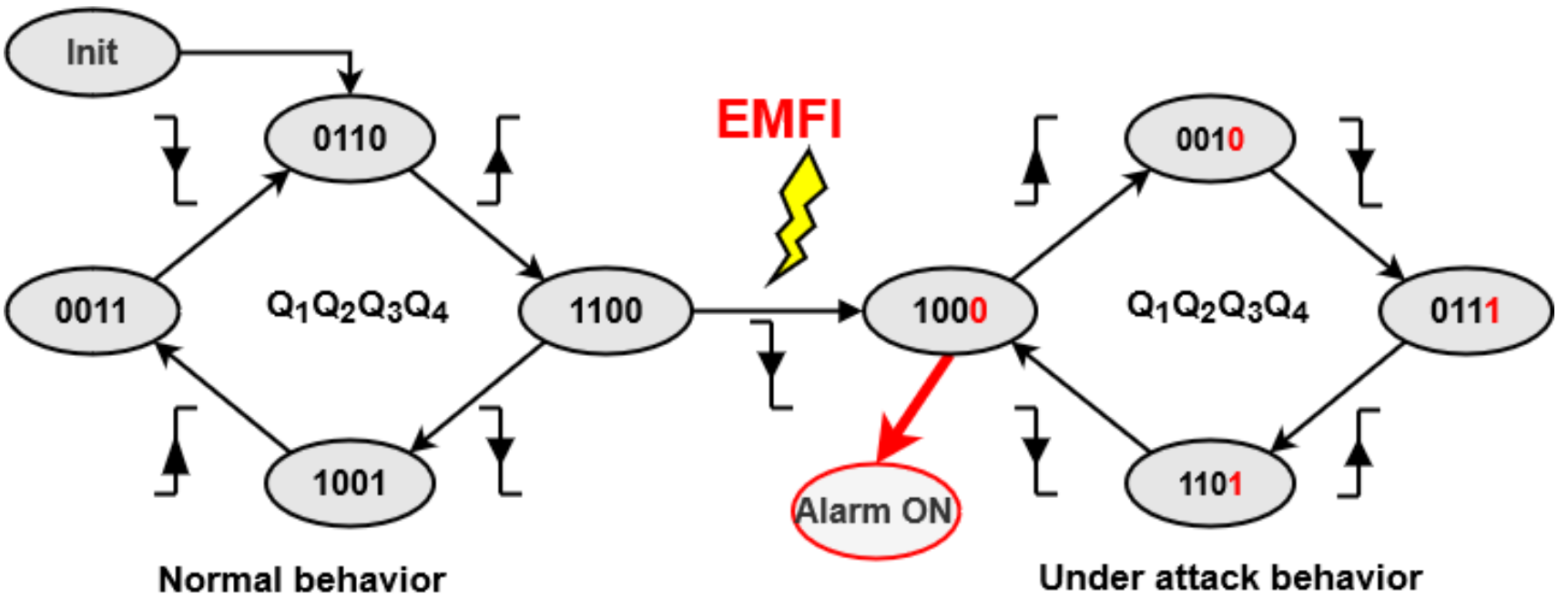
D. El-Baze, J. -B. Rigaud and P. Maurine, "An Embedded Digital Sensor against EM and BB Fault Injection," *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2016

How does this detector work?



Normal behavior

How does this detector work?

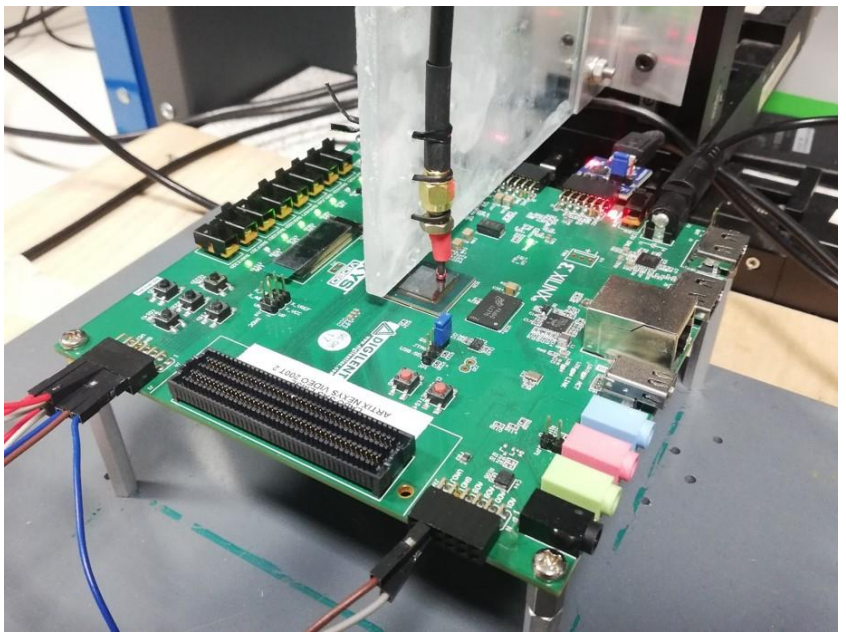


Alarm is raised for any deviation in $Q_1Q_2Q_3Q_4$ states from the normal behavior

Outline

- Previous work
  - EMFI models
  - Fully digital detector
- **Experimental setup**
  - **EMFI platform**
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

Experimental setup: EMFI platform



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

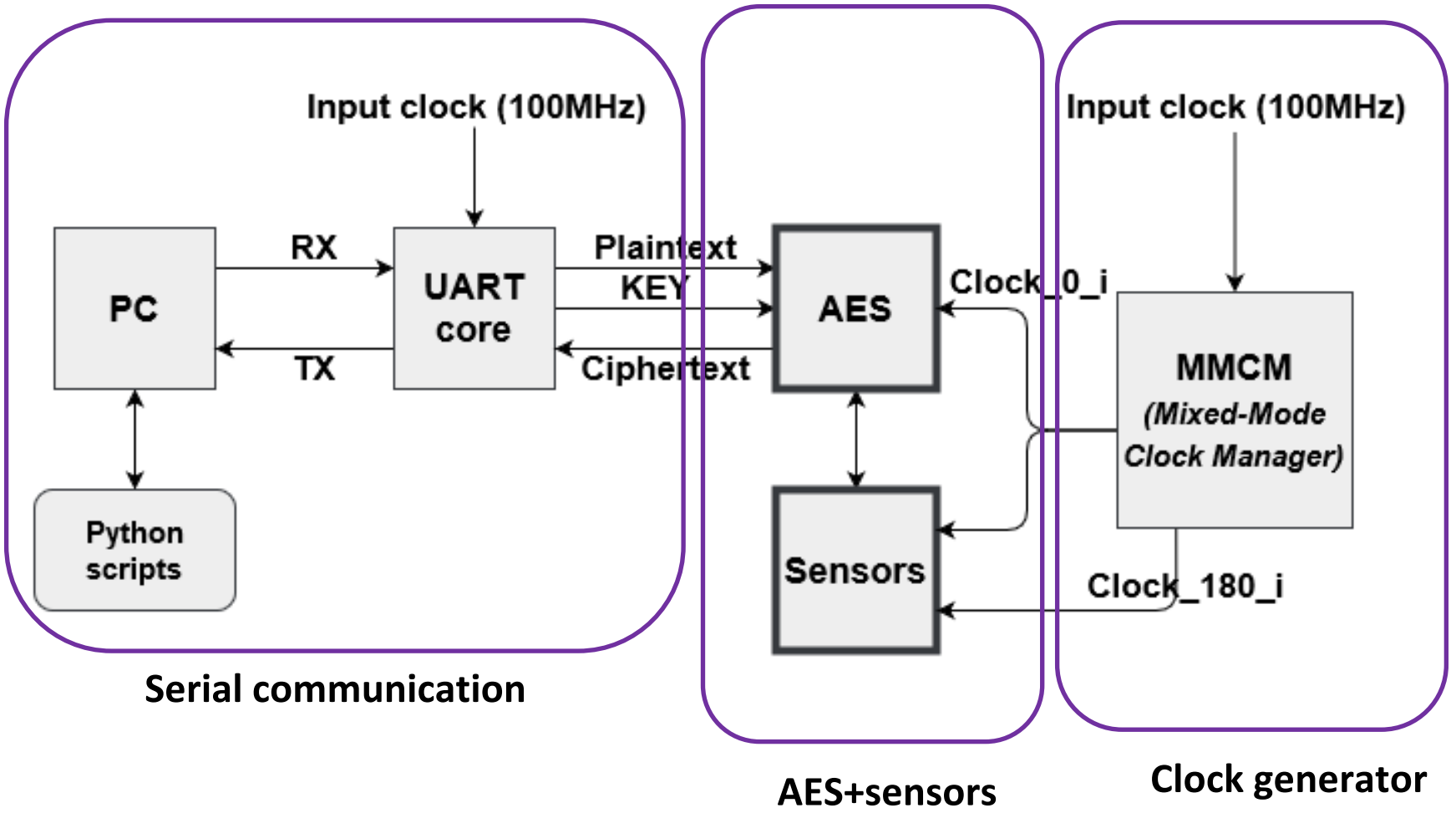
- AV-Tech voltage pulse generator
  - Pulse amplitude: up to +/- 750V
  - Pulse-width: 4.5-20ns
  - Pulse rise and fall time: 2 ns
  - Remotely controlled using the telnet protocol

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

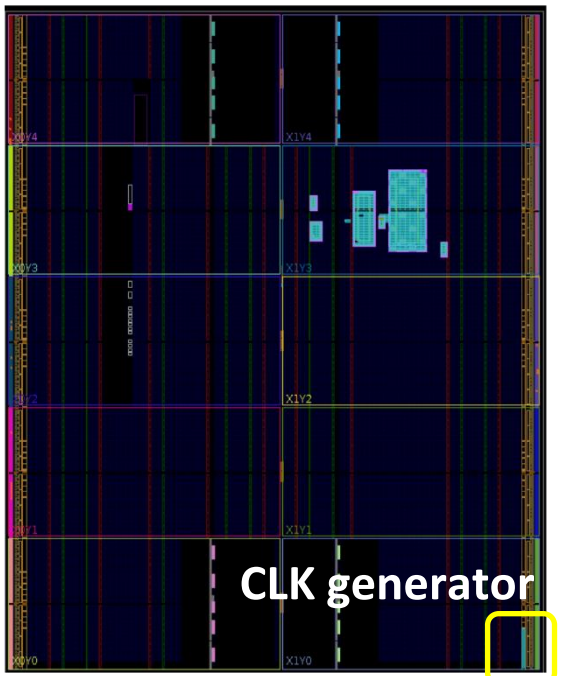
Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - **DUT block diagram**
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

DUT block diagram: AES + sensors.

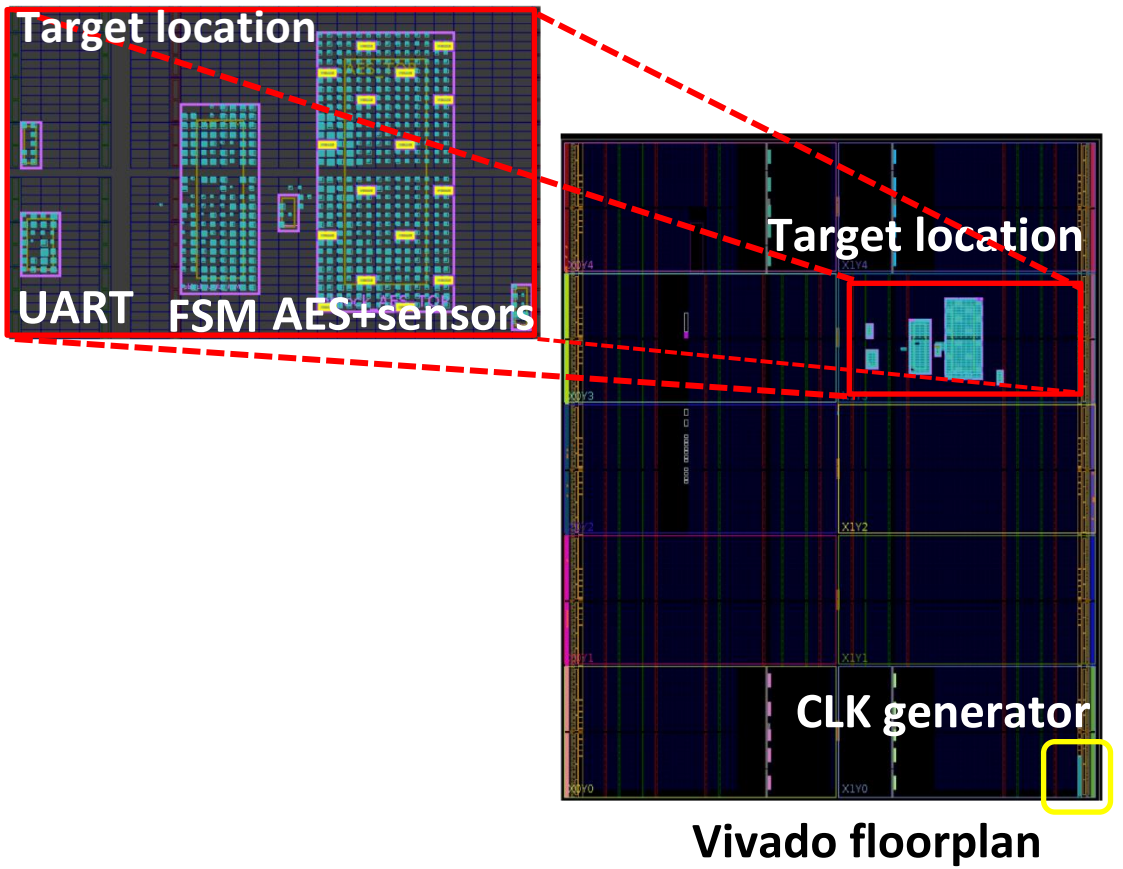


FPGA implementation: Floorplan



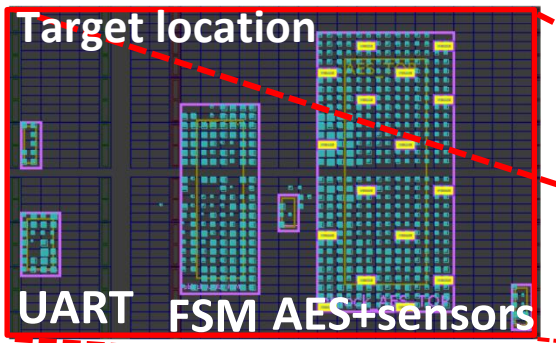
Vivado floorplan

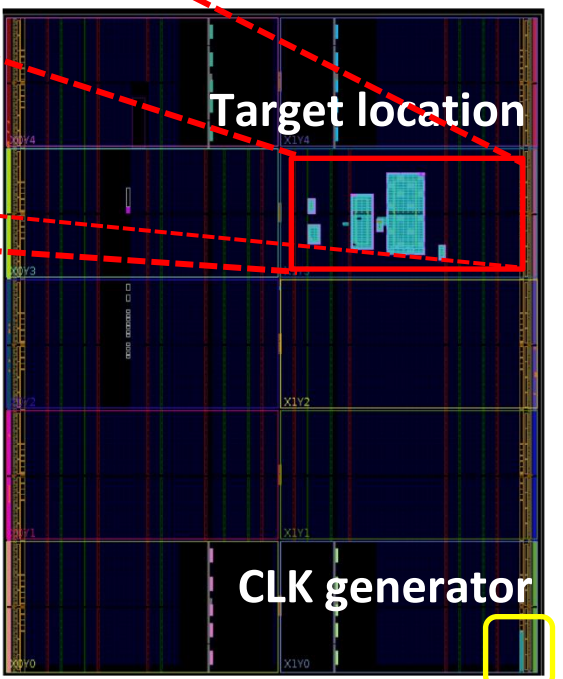
FPGA implementation: Floorplan



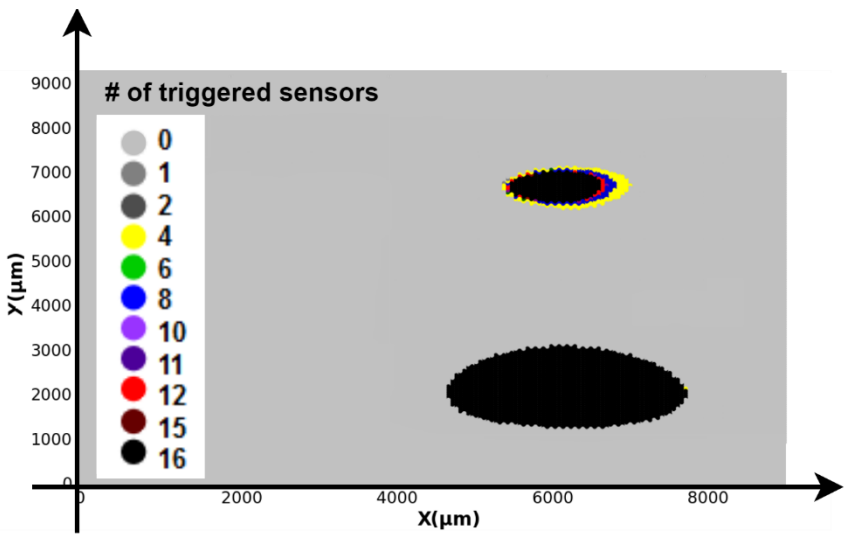
Vivado floorplan

FPGA implementation: Floorplan



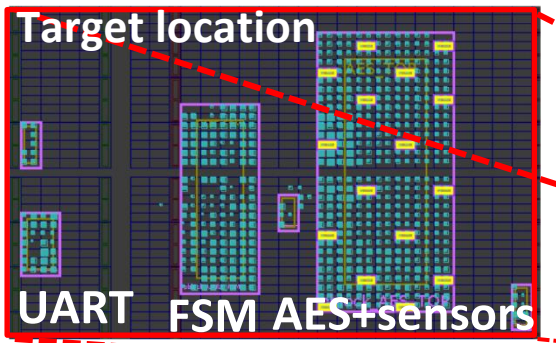


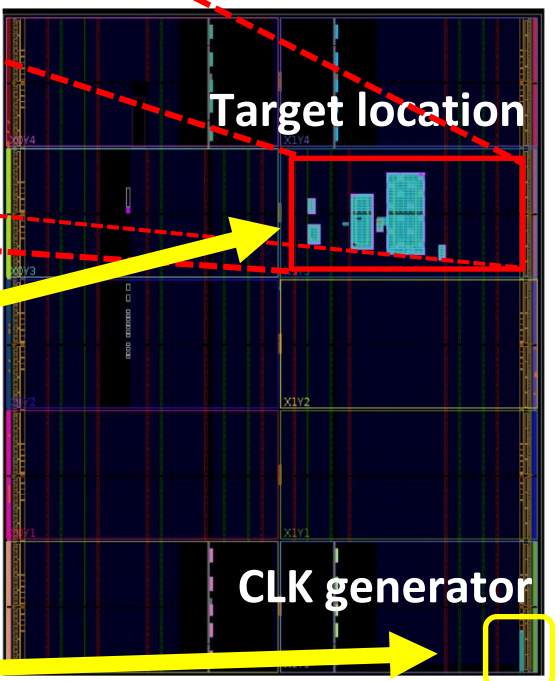
Vivado floorplan



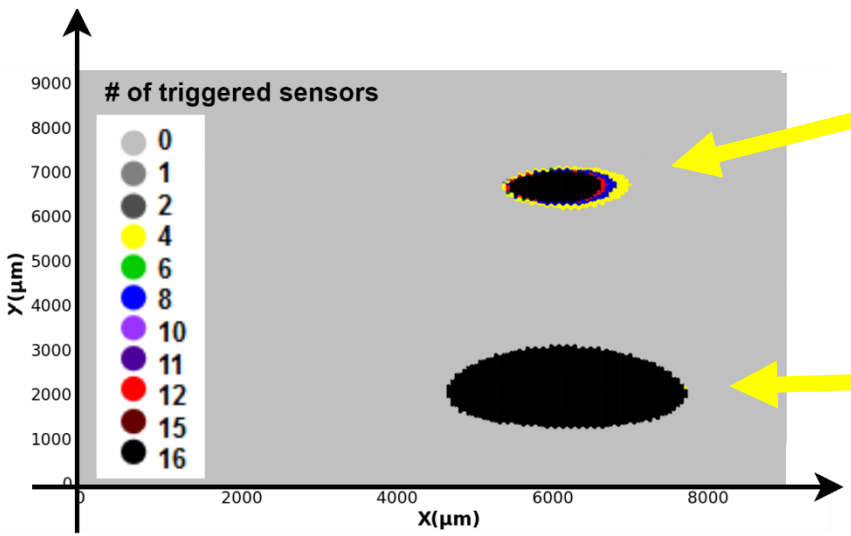
Sensors sensitivity map

FPGA implementation: Floorplan



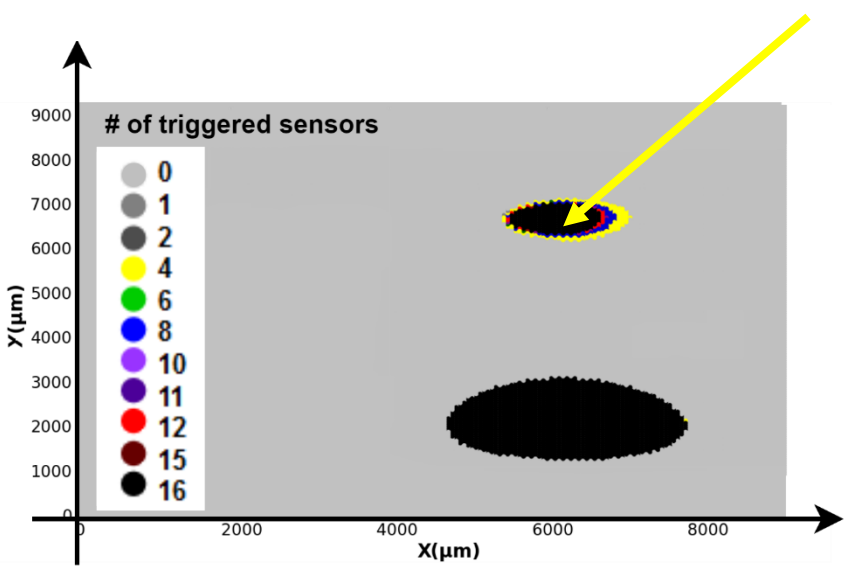


Vivado floorplan



Sensors sensitivity map

Experimental methodology



Sensors sensitivity map

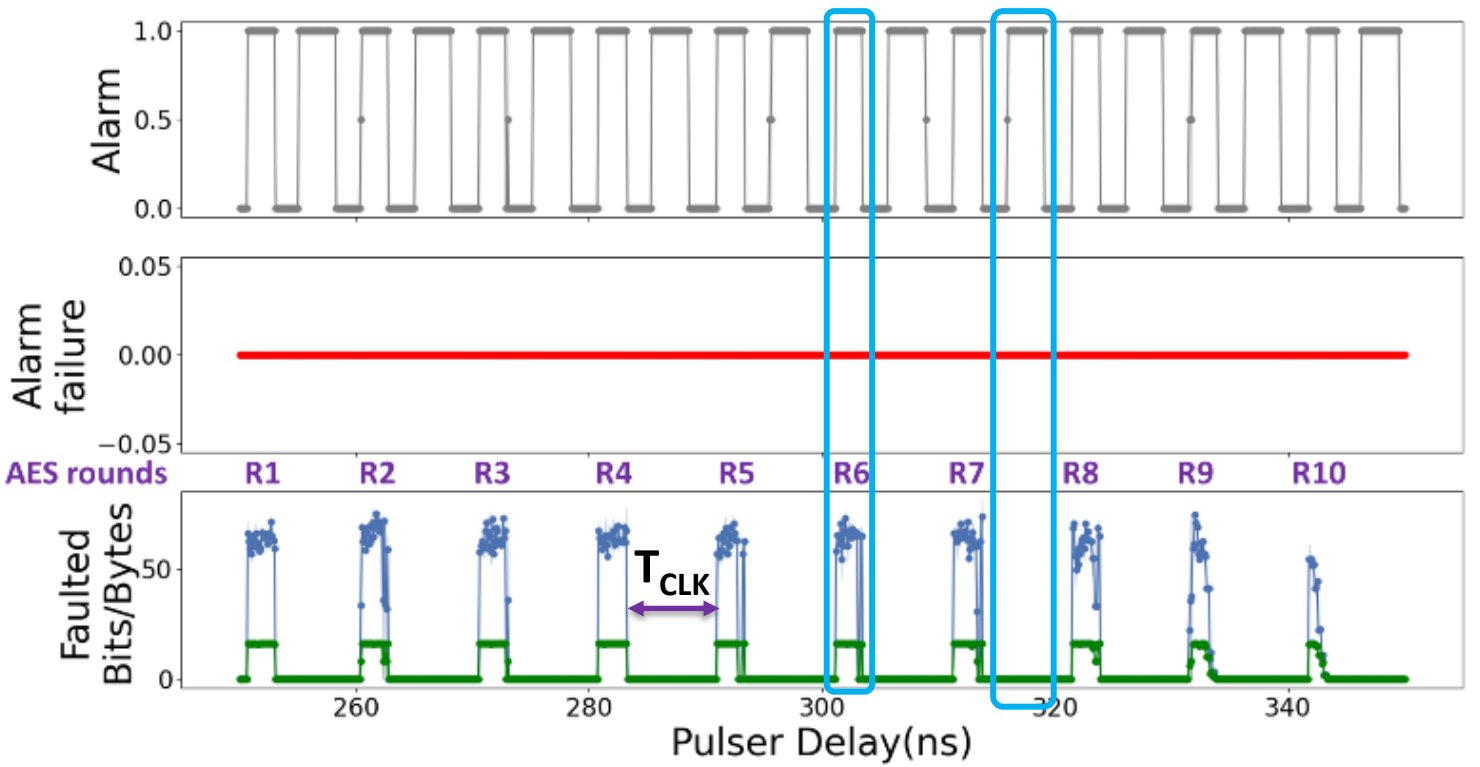
EM injection probe above the AES accelerator sensitive area

Focus on the intrinsic detection ability of the sensor all over the target‘s **full-frequency range**

Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- **Experimental results**
  - **EMFI results**
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

EMFI results: @100MHZ (+420V)

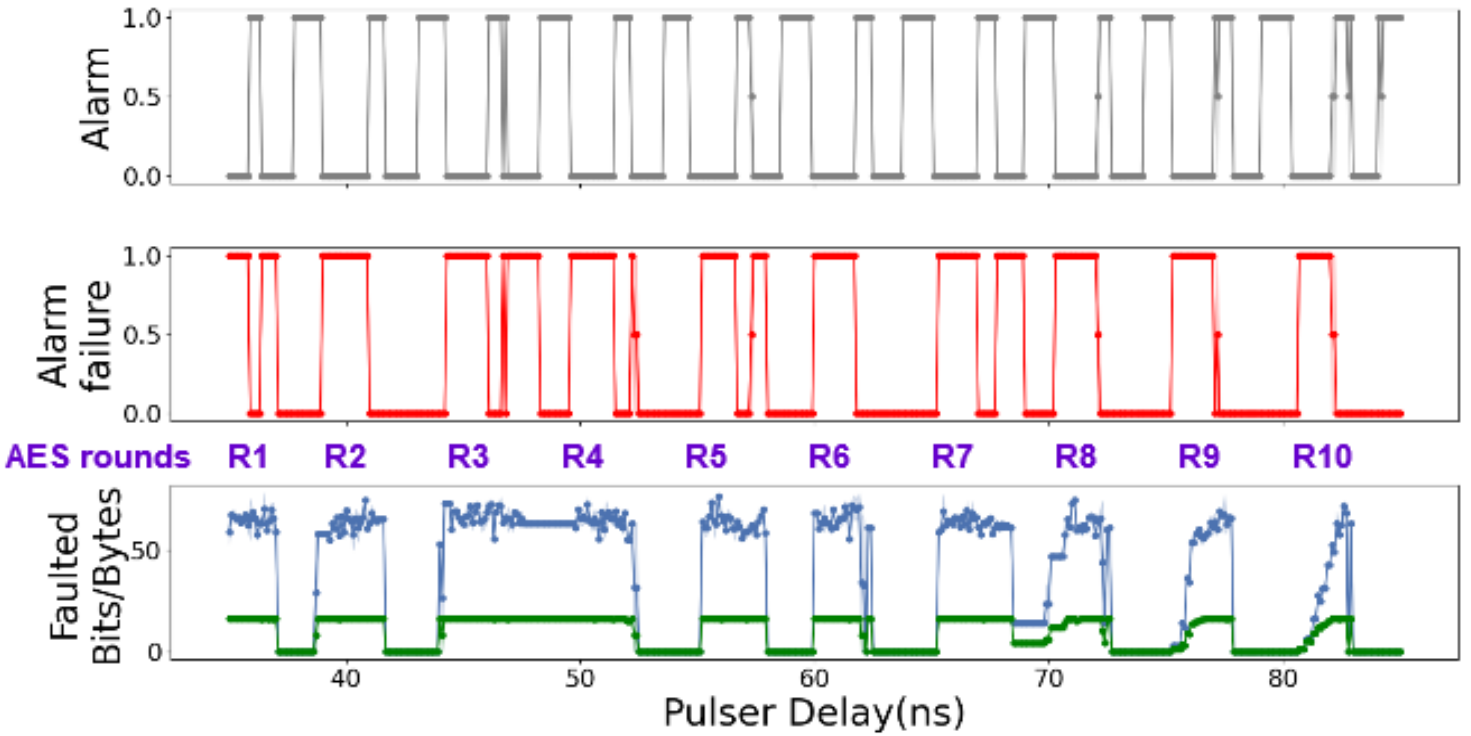


No alarm failure → All injected faults are detected

Faults windows were consistent to the sampling fault model

- Width of the detection windows *(sensors)*: 2-3ns.
- Width of the injection windows *(AES)*: 1.5-2.5 ns.

EMFI results: @200MHZ (+420V)



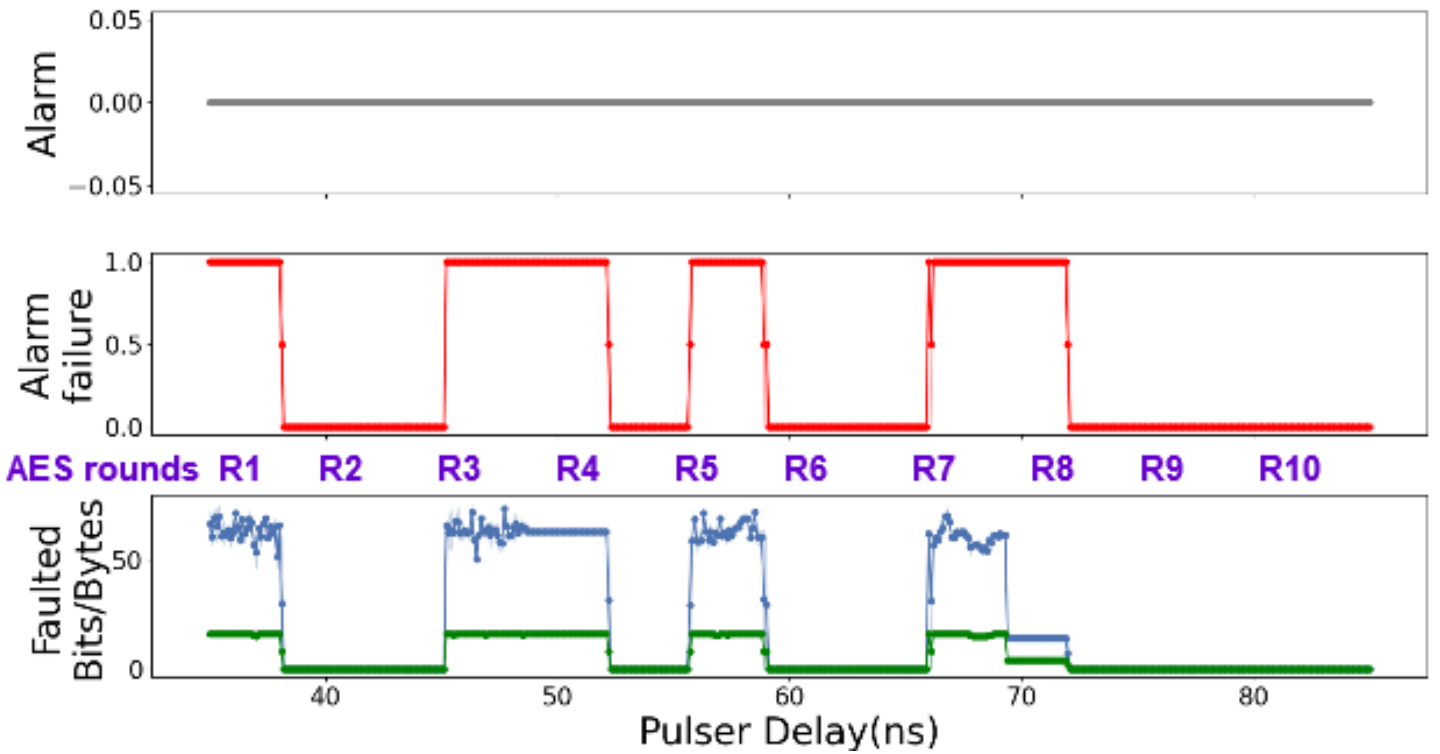
Study the project behavior close to the DUT max frequency

Bad detection rate for these sensors at high clock frequency

Timing fault model in addition to sampling fault model?

- Width of the detection windows: 0.6-1 ns.

EMFI results: @200MHZ (+350V)



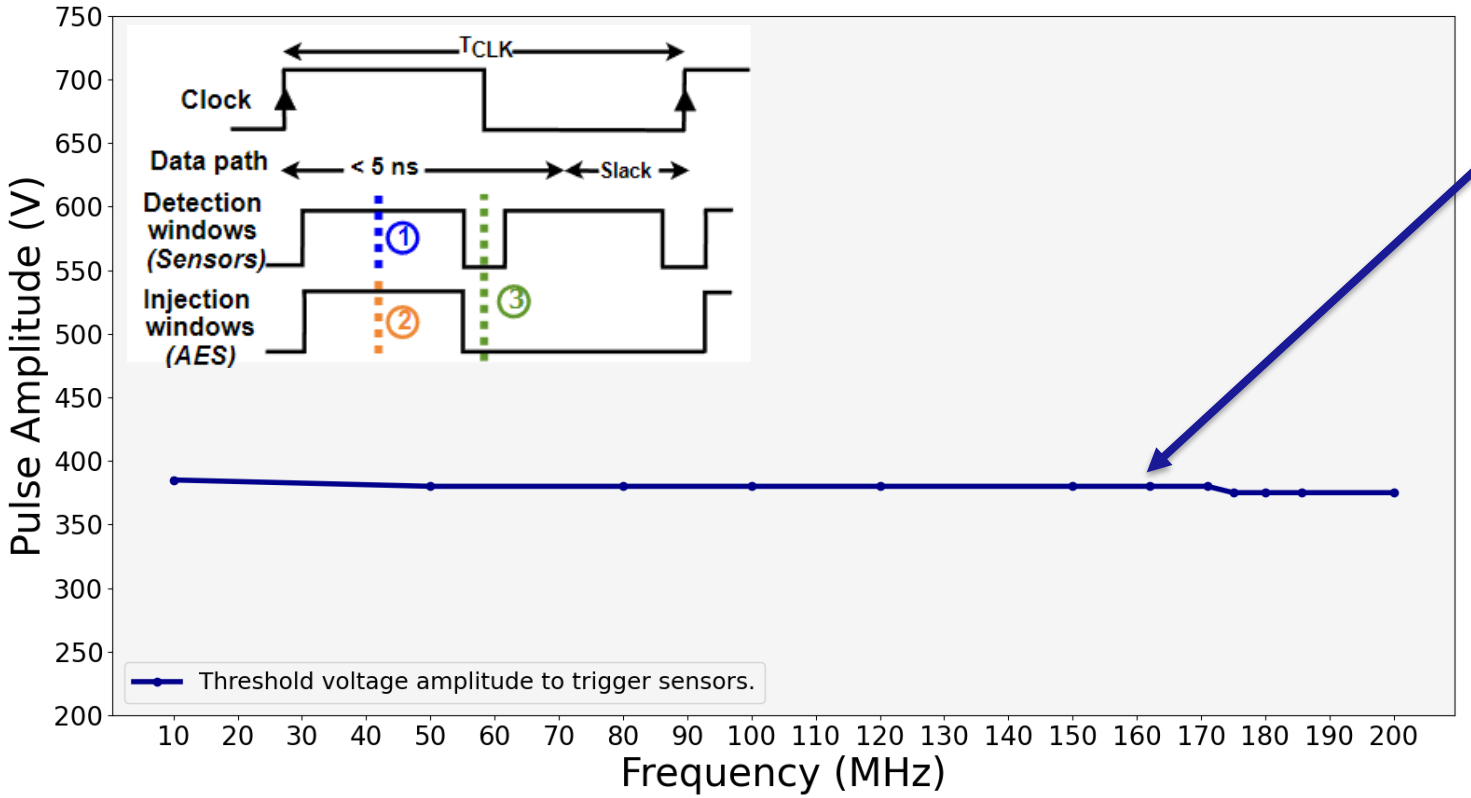
Decreasing the voltage amplitude from 420V to 350V

- None of these sensors are triggered
- Timing fault model induced (no sampling faults)

Outline

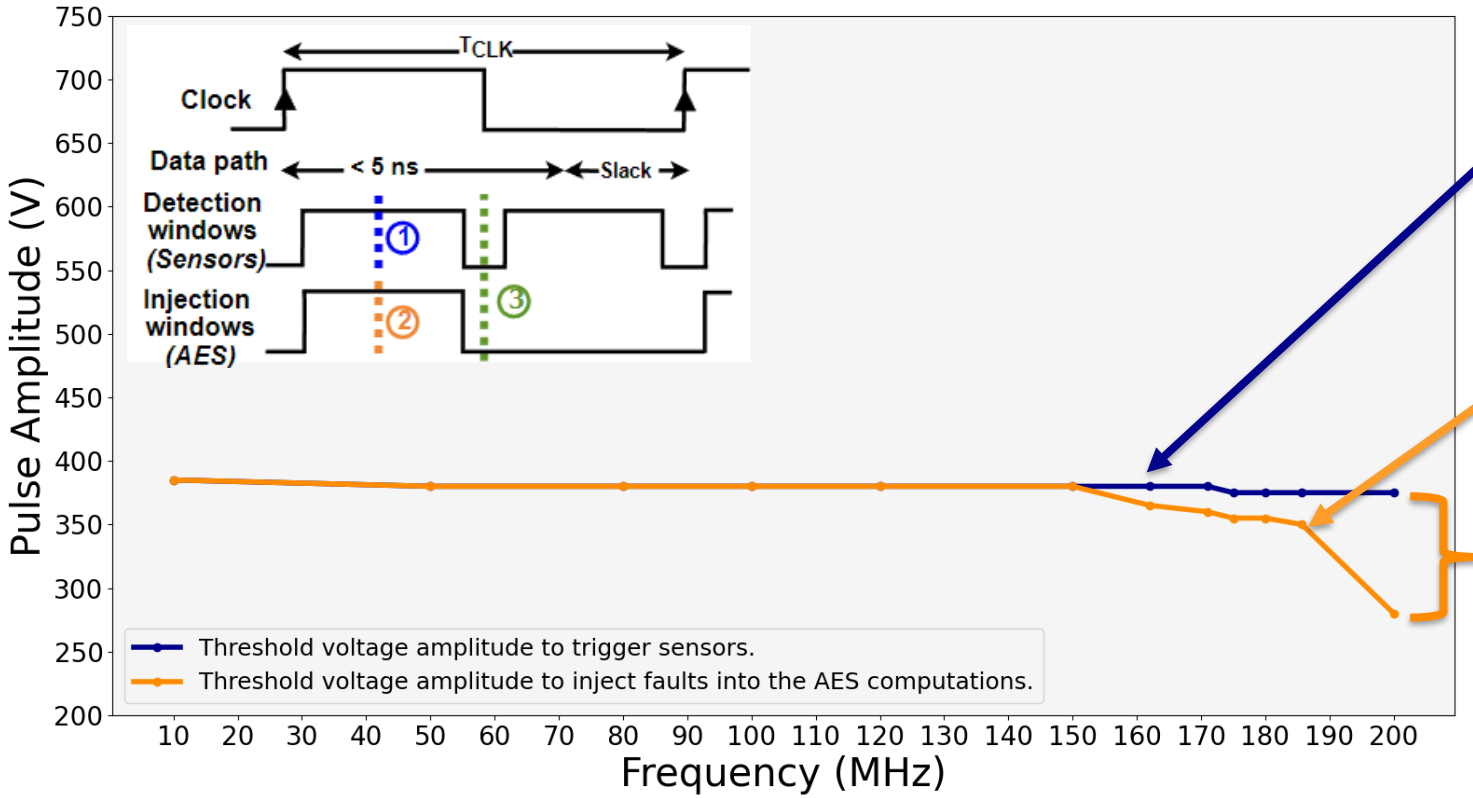
- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - **Deep exploration of EMFI mechanisms**
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

Deep exploration of EMFI mechanisms



Threshold to trigger sensors

Deep exploration of EMFI mechanisms

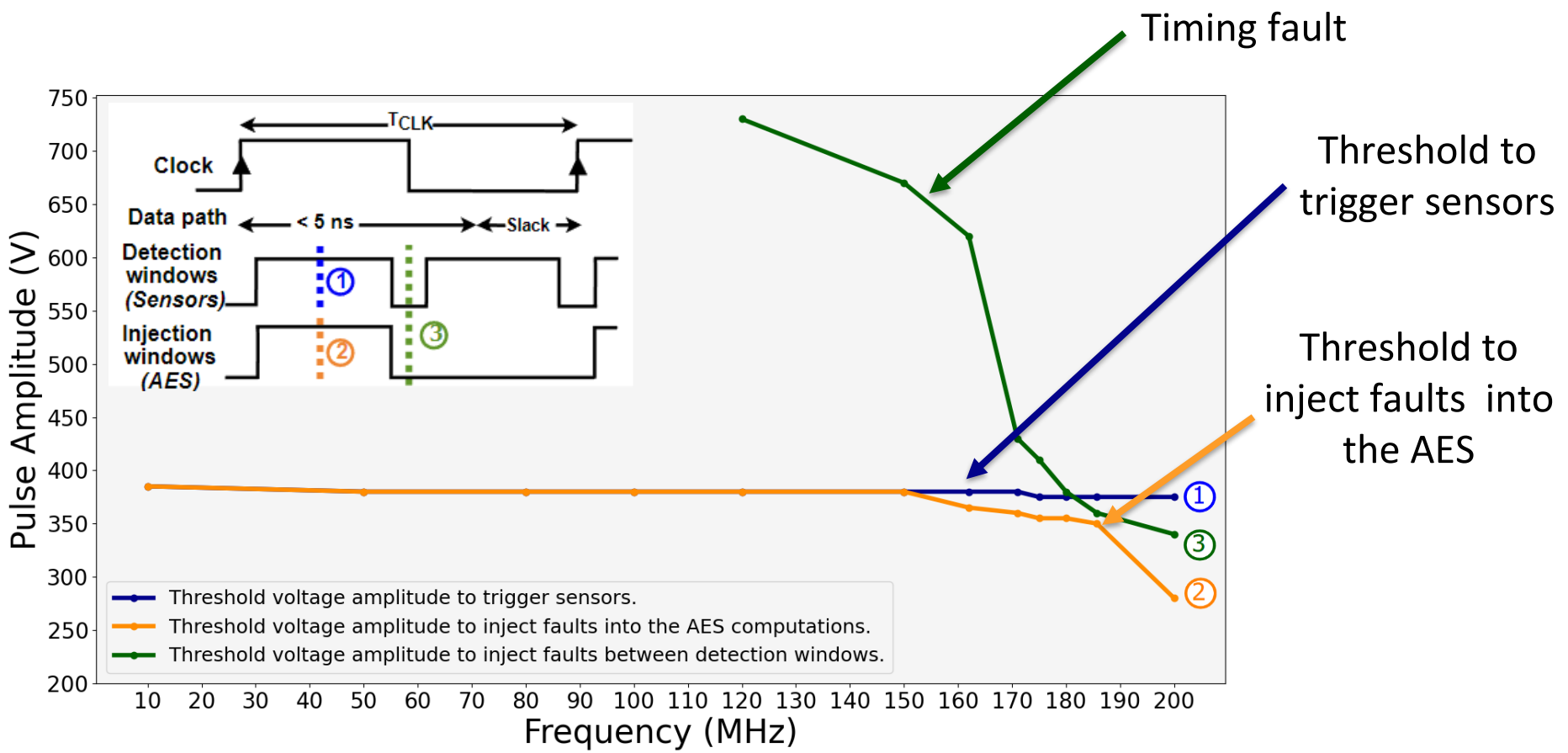


Threshold to trigger sensors

Threshold to inject faults into the AES

Sensor failed

Deep exploration of EMFI mechanisms



Coexistence of two distinct fault injection mechanisms to explain EMFI[1]

[1]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

Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - **Analysis of experimental results**
- In-depth analysis of EMFI-induced clock glitches
- Conclusion

Analysis of experimental results

	Impact on the detection window widths w.r.t	
	Sampling fault model[1,2,3]	**Our experimental results**
Clock frequency	Constant and independent	Decreased when the clock frequency increased
Input data	Independent	Dependent
Critical path	Independent	Reduced when shortening the propagation delay path
Fault logic model	Bit-set or bit-reset depend on the polarity of the pulse	Bit flip (Mix of bit-sets and bit-resets) No effect of the polarity pulse

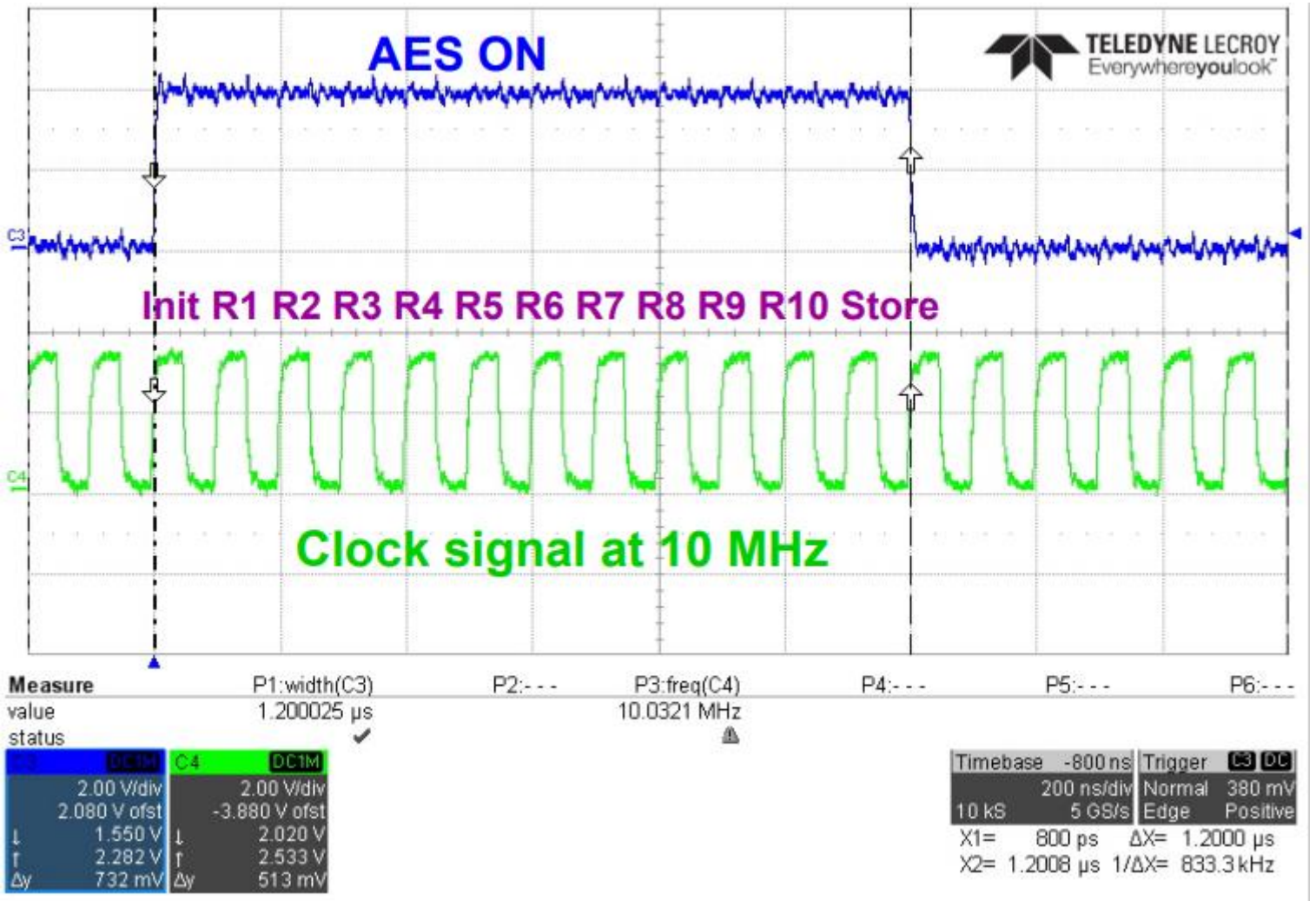
- The faults injected at low frequency
  - Broadly follow the sampling fault model
  - Some discrepancies from the theory cast doubts on its validity
  - Further exploration and tests are needed

[1] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 183–197, 2017.
[2] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital em pulse detector," in 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 2016, pp. 439–444.
[3] 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

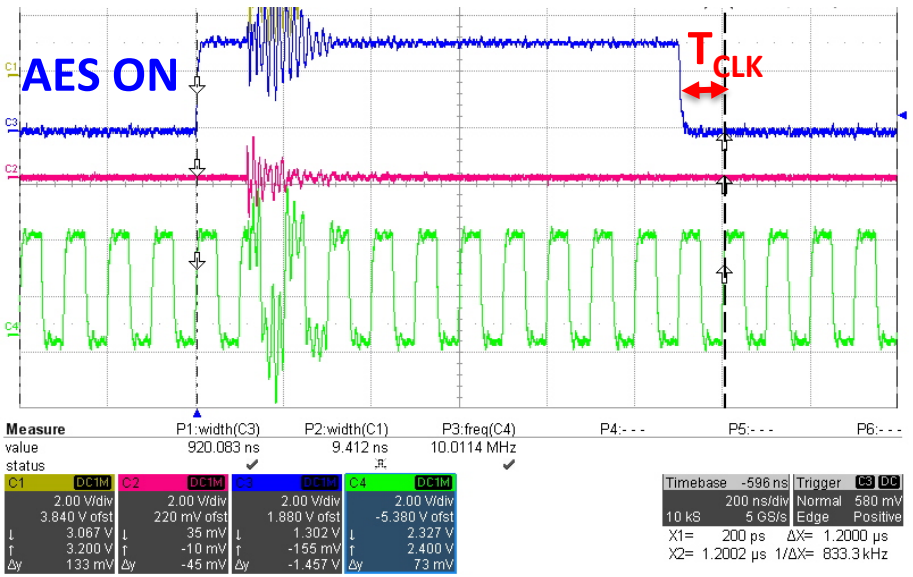
Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- **In-depth analysis of EMFI-induced clock glitches**
- Conclusion

Normal operation



EMFI effects on AES duration (+420V)

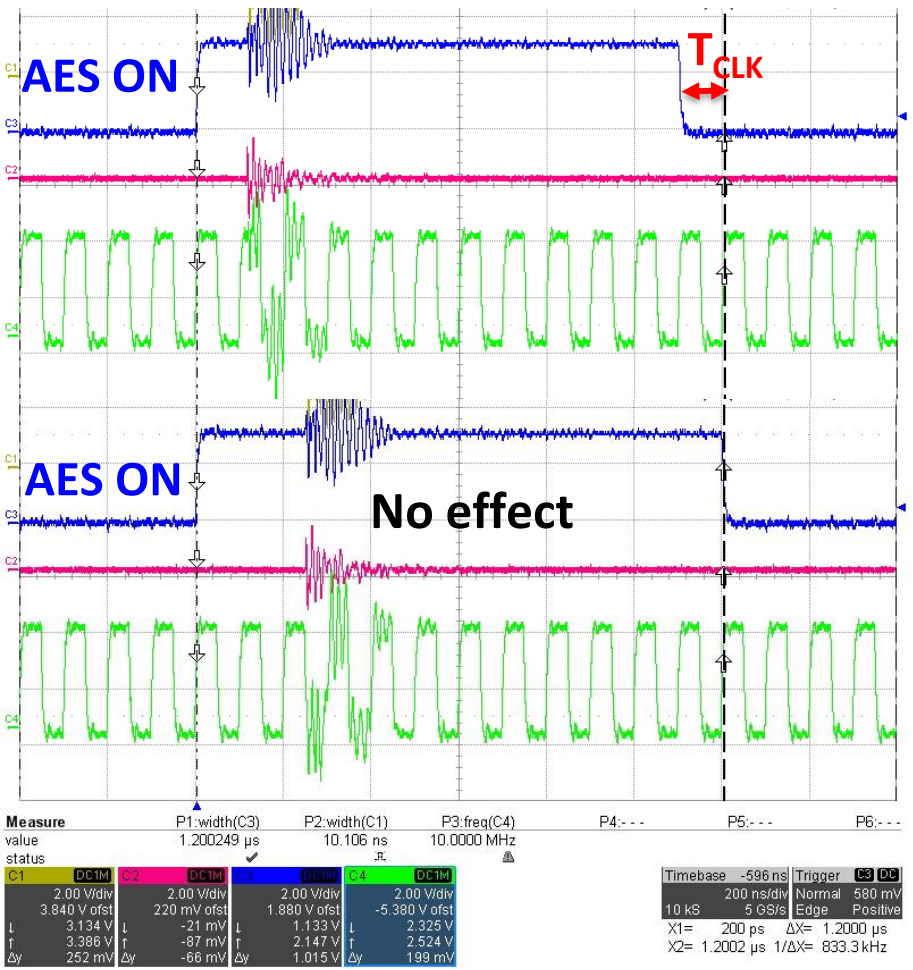


- The impact of EMFI attacks, induced by a positive pulse on the AES ON signal:
  - When the clock signal is ‘1’:

The width of the AES ON signal is reduced by one clock period

Ciphertext is correctly received

EMFI effects on AES duration (+420V)



- The impact of EMFI attacks, induced by a positive pulse on the AES ON signal:
  - When the clock signal is ‘1’:

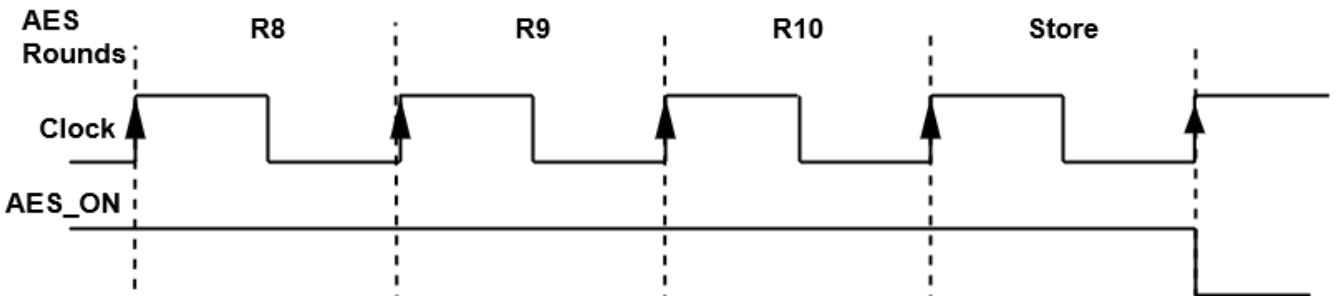
    The width of the AES ON signal is reduced by one clock period

    Ciphertext is correctly received
  - When the clock signal is ‘0’:

    No effect

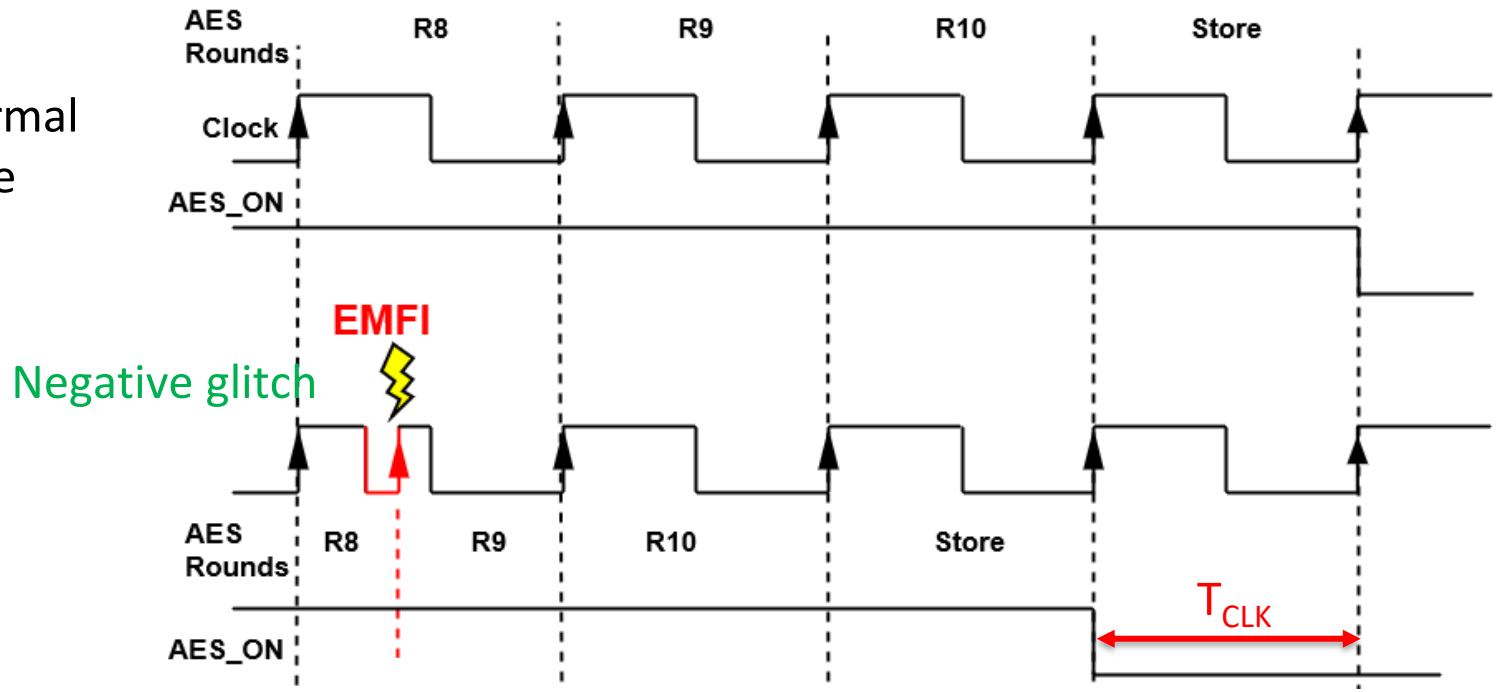
EMFI effects on AES duration (+420V)

Normal case



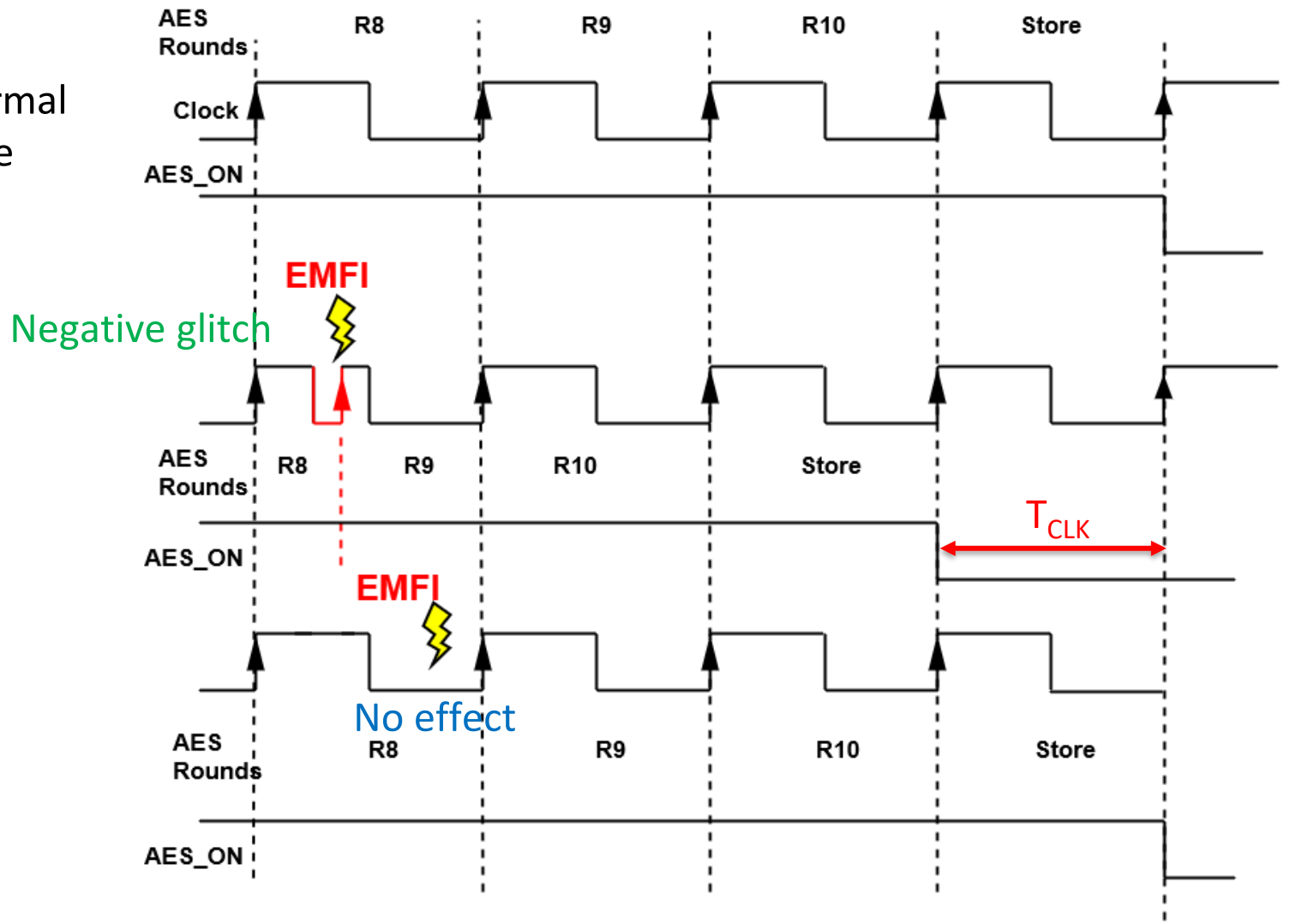
EMFI effects on AES duration (+420V)

Normal case

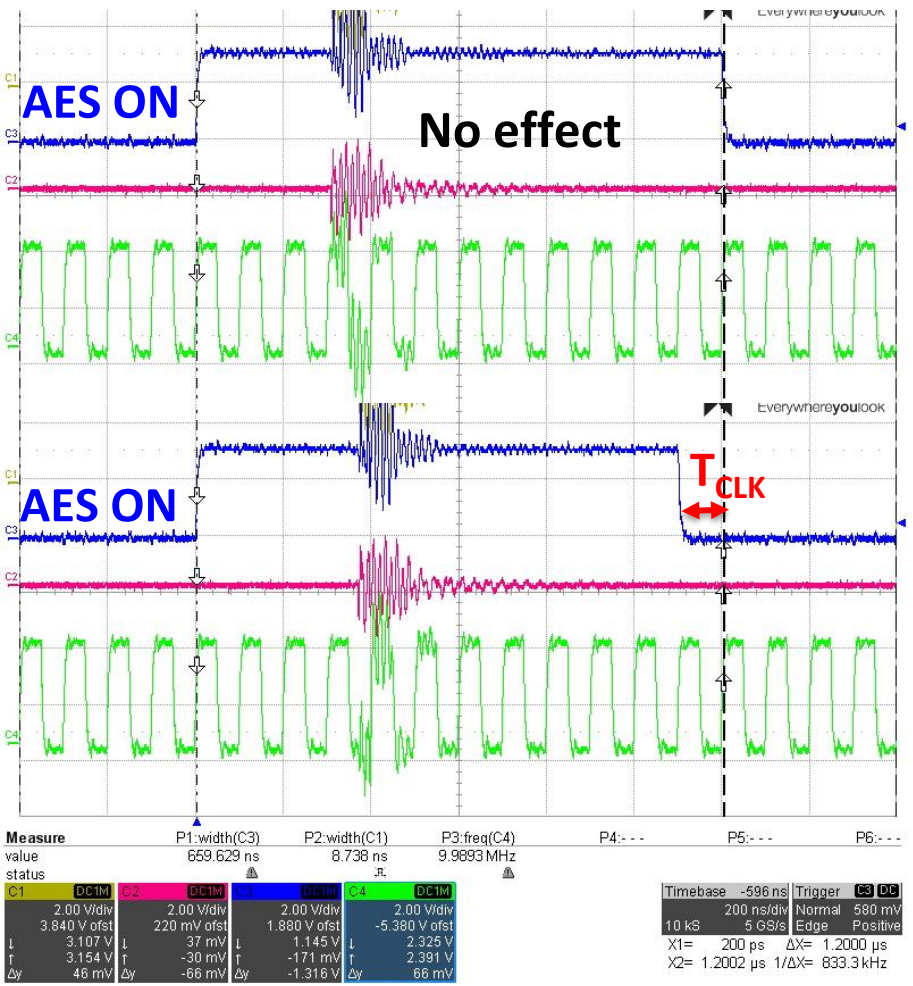


EMFI effects on AES duration (+420V)

Normal case



EMFI effects on AES duration (-420V)



- The impact of EMFI attacks, induced by a negative pulse on the AES ON signal:
  - When the clock signal is ‘1’:

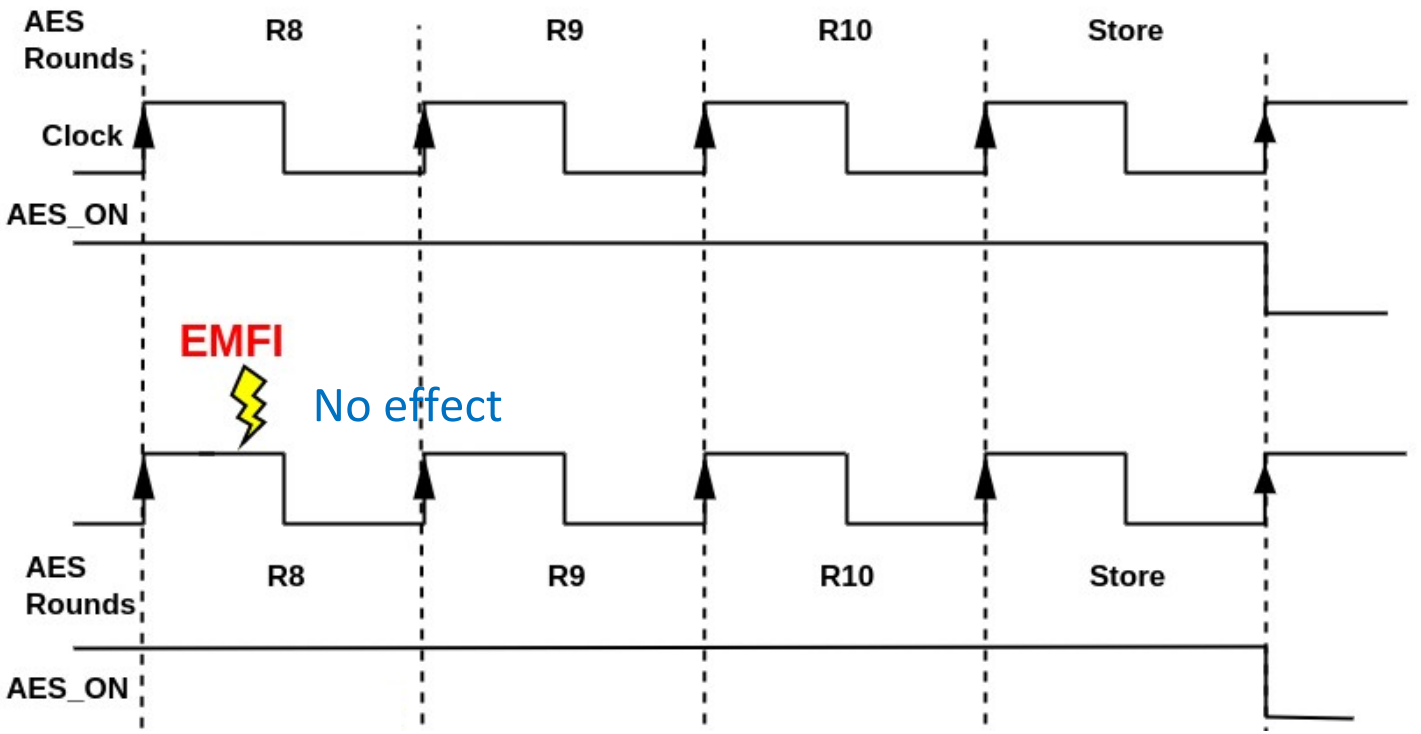
    No effect

  - When the clock signal is ‘0’:

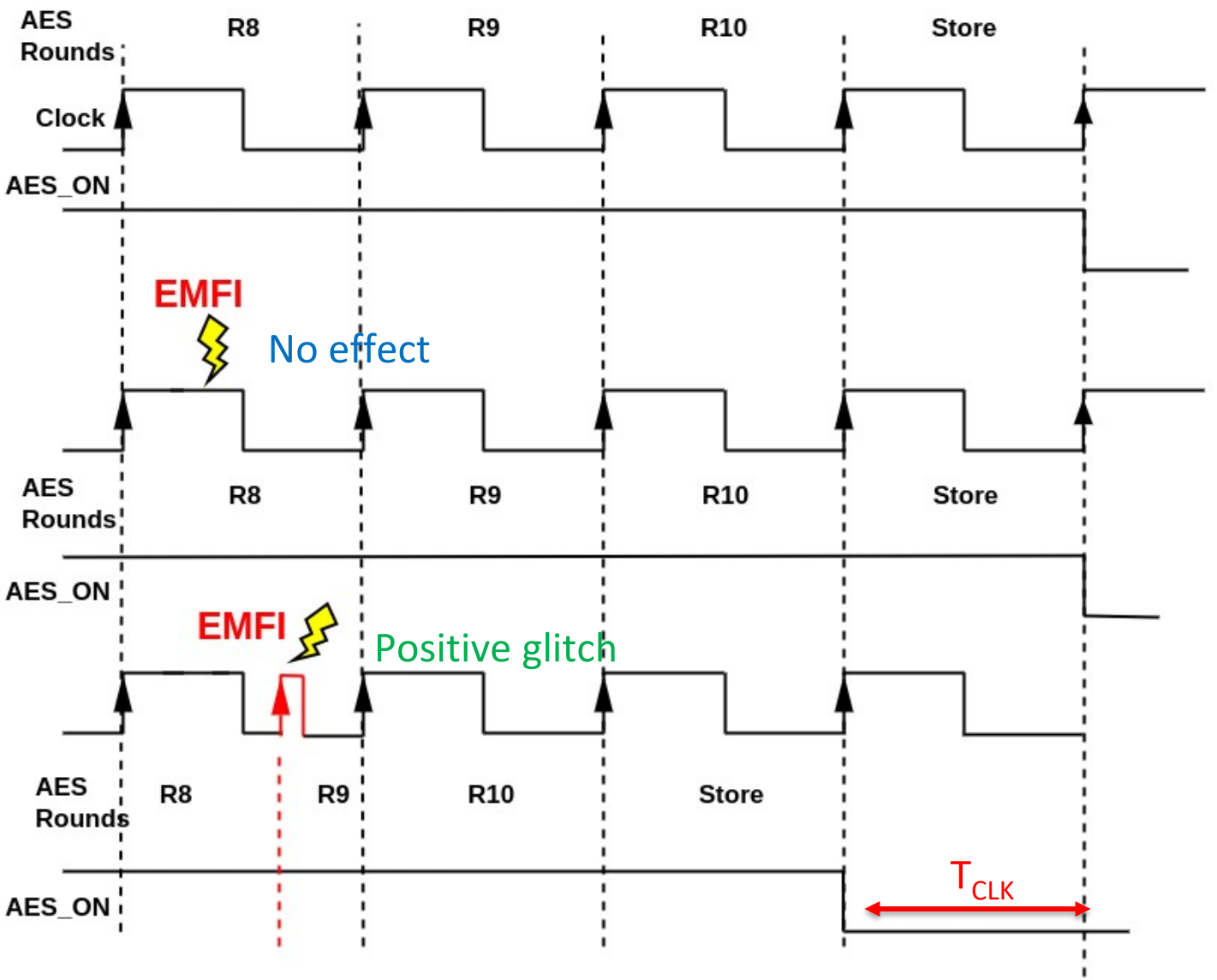
    The width of the AES ON signal is reduced by one clock period

Ciphertext is correctly received

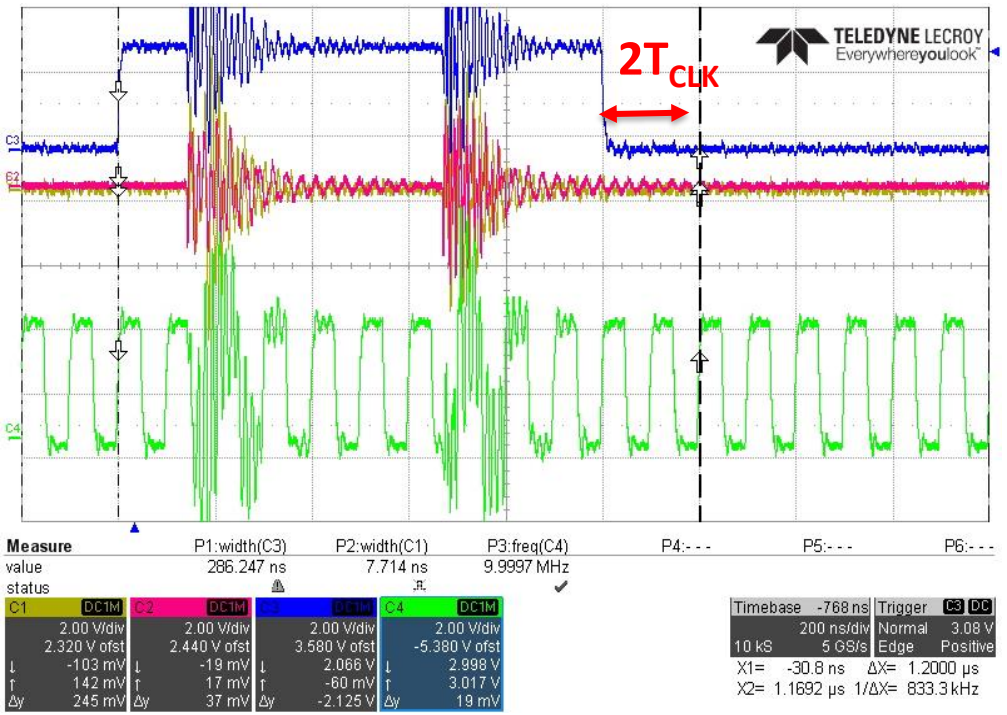
EMFI effects on AES duration (-420V)



EMFI effects on AES duration (-420V)



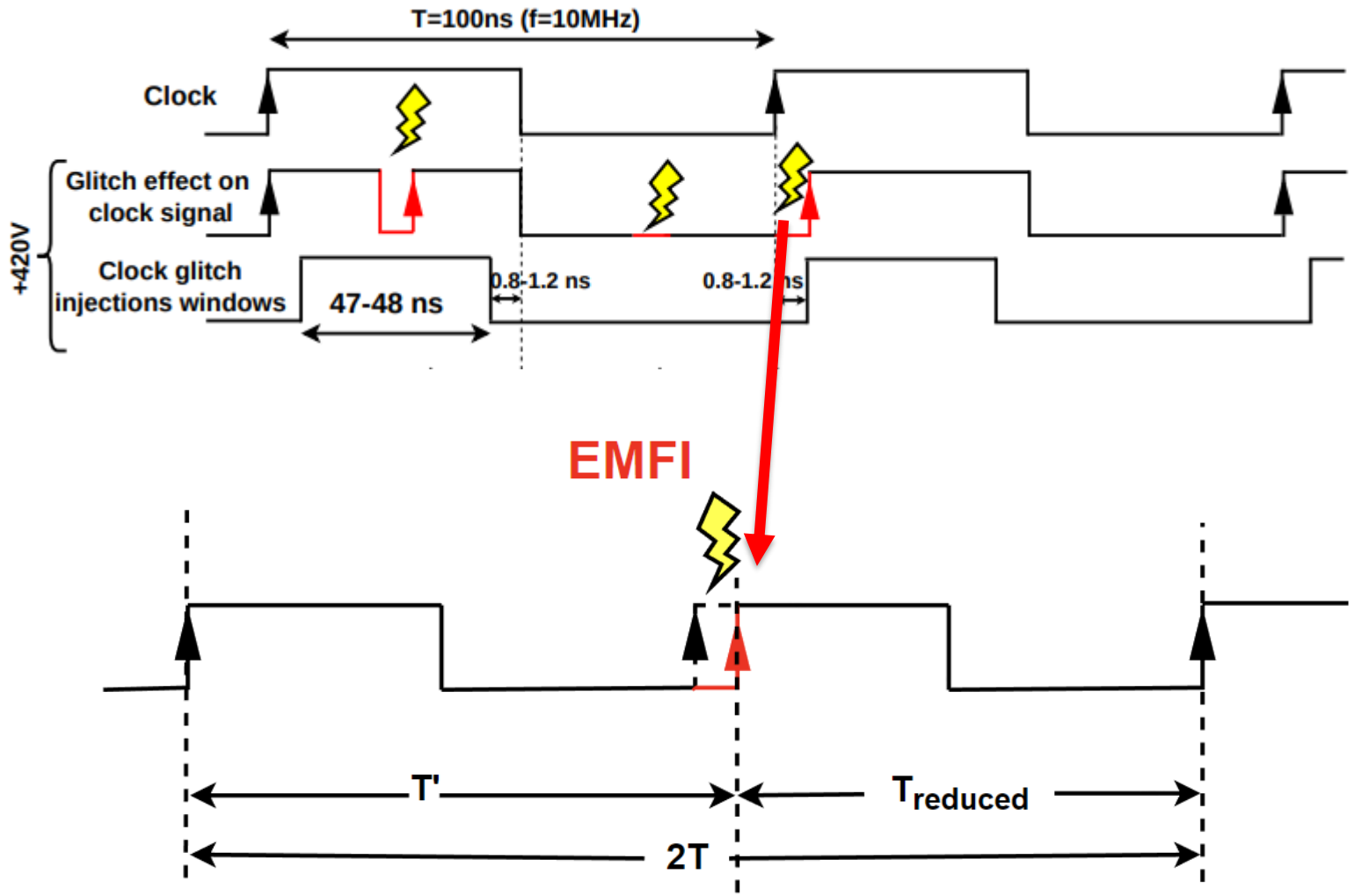
EMFI effects on AES duration



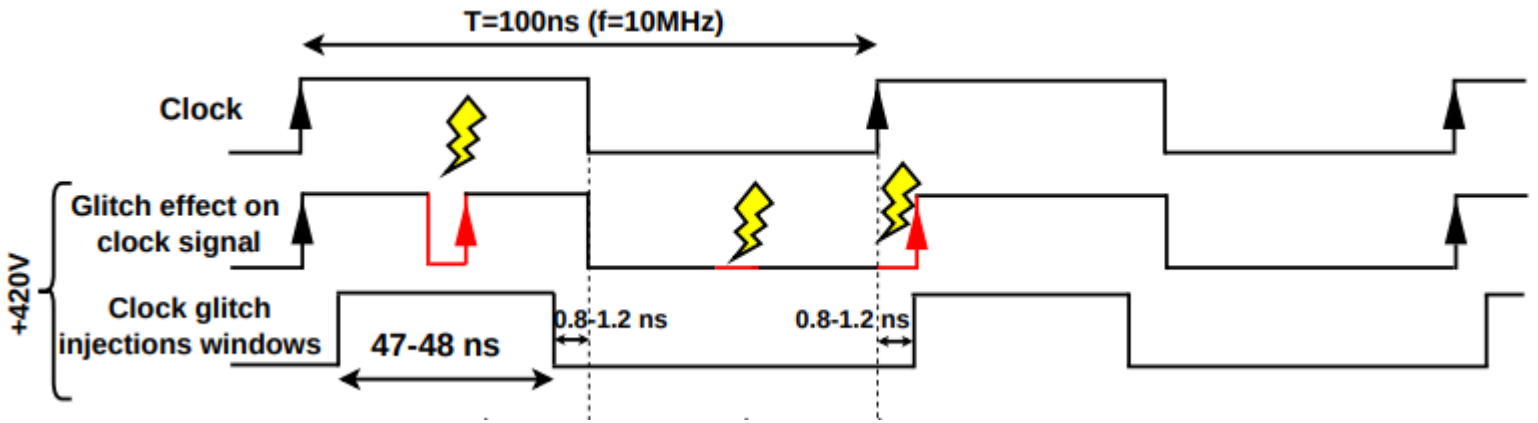
- Two EM disturbances induced two clock glitches
- Ciphertext is correctly received

EMFI does induce clock glitches in the target's CDN
It can replace genuine clock rising edges

EMFI-induced clock glitch principle (+420V)



EMFI-induced clock glitch principle (+420V)

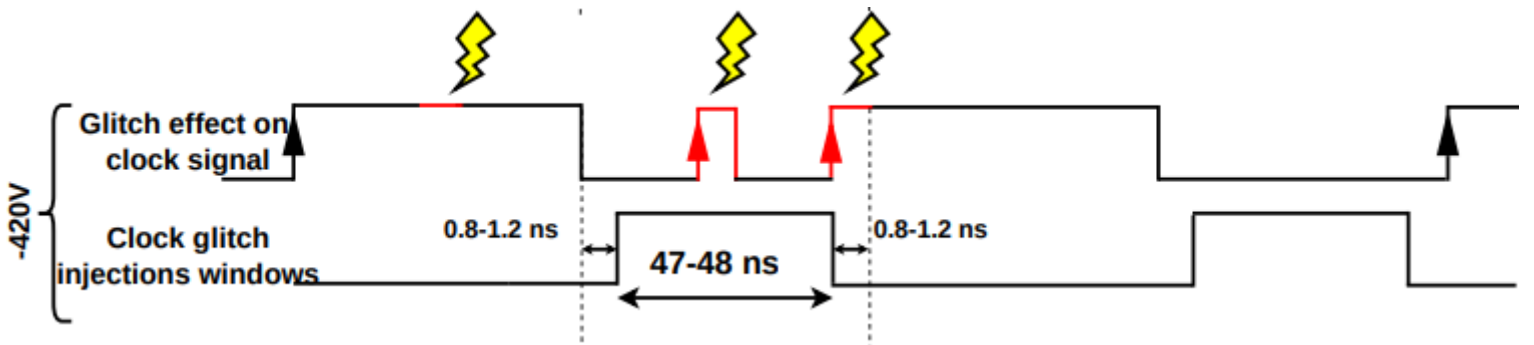


The width of the susceptibility window caused by EMFI-induced clock glitches:

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

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

EMFI-induced clock glitch principle (-420V)

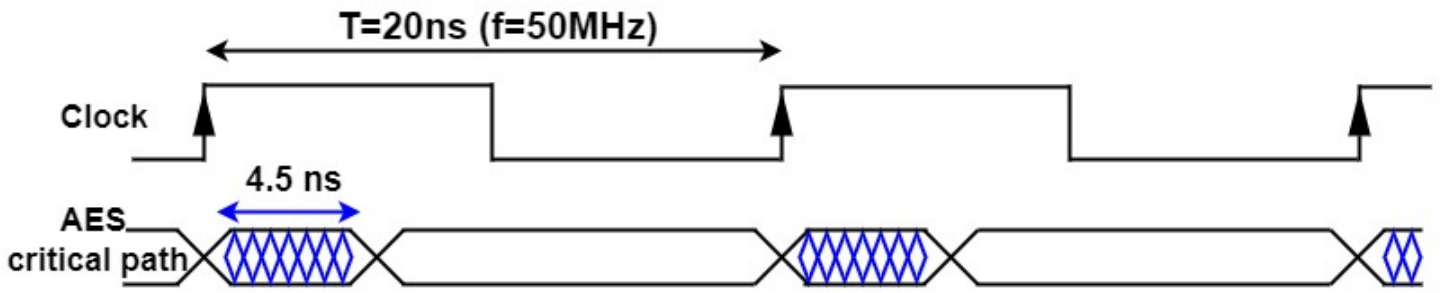


The width of the susceptibility window caused by EMFI-induced clock glitches:

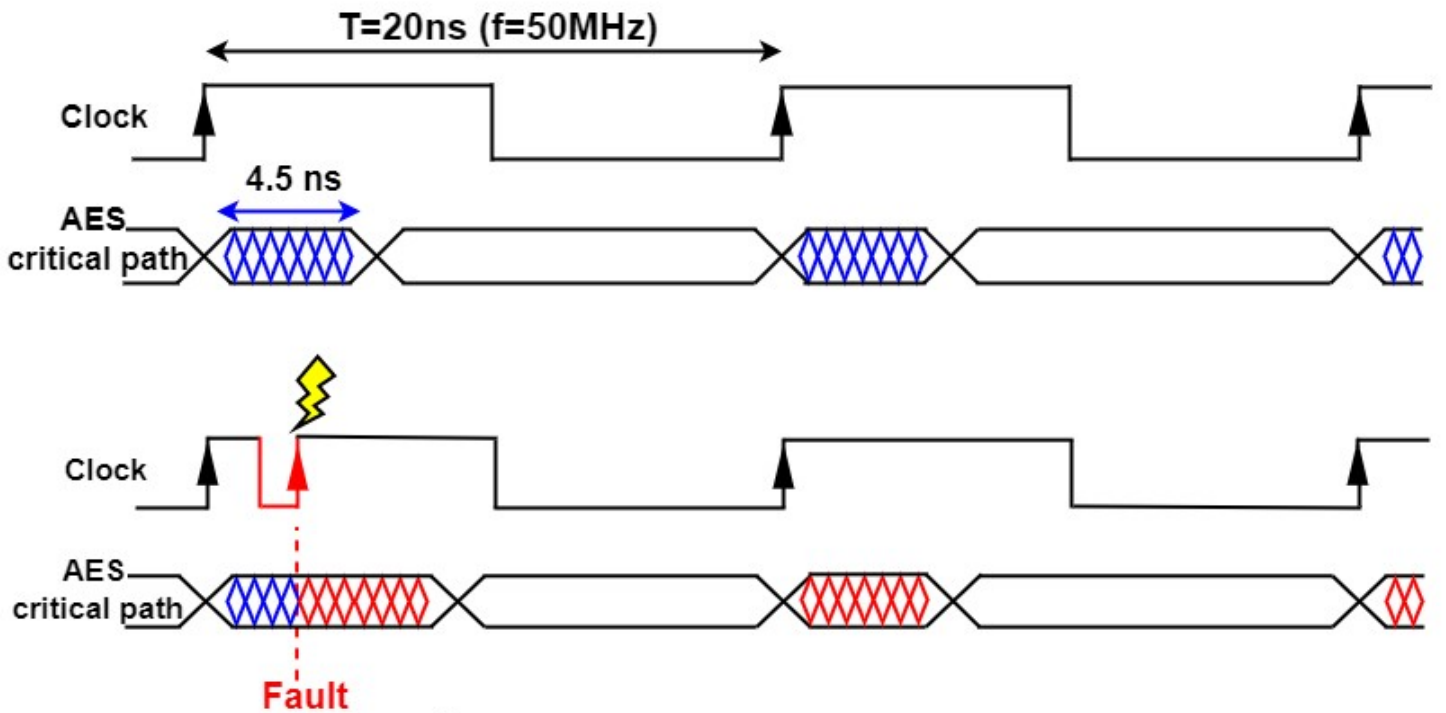
$$w_{EMFI} = \frac{T}{2} - 2k$$

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

EMFI-induced clock glitches ($t_{critical} < \frac{T}{2}$)

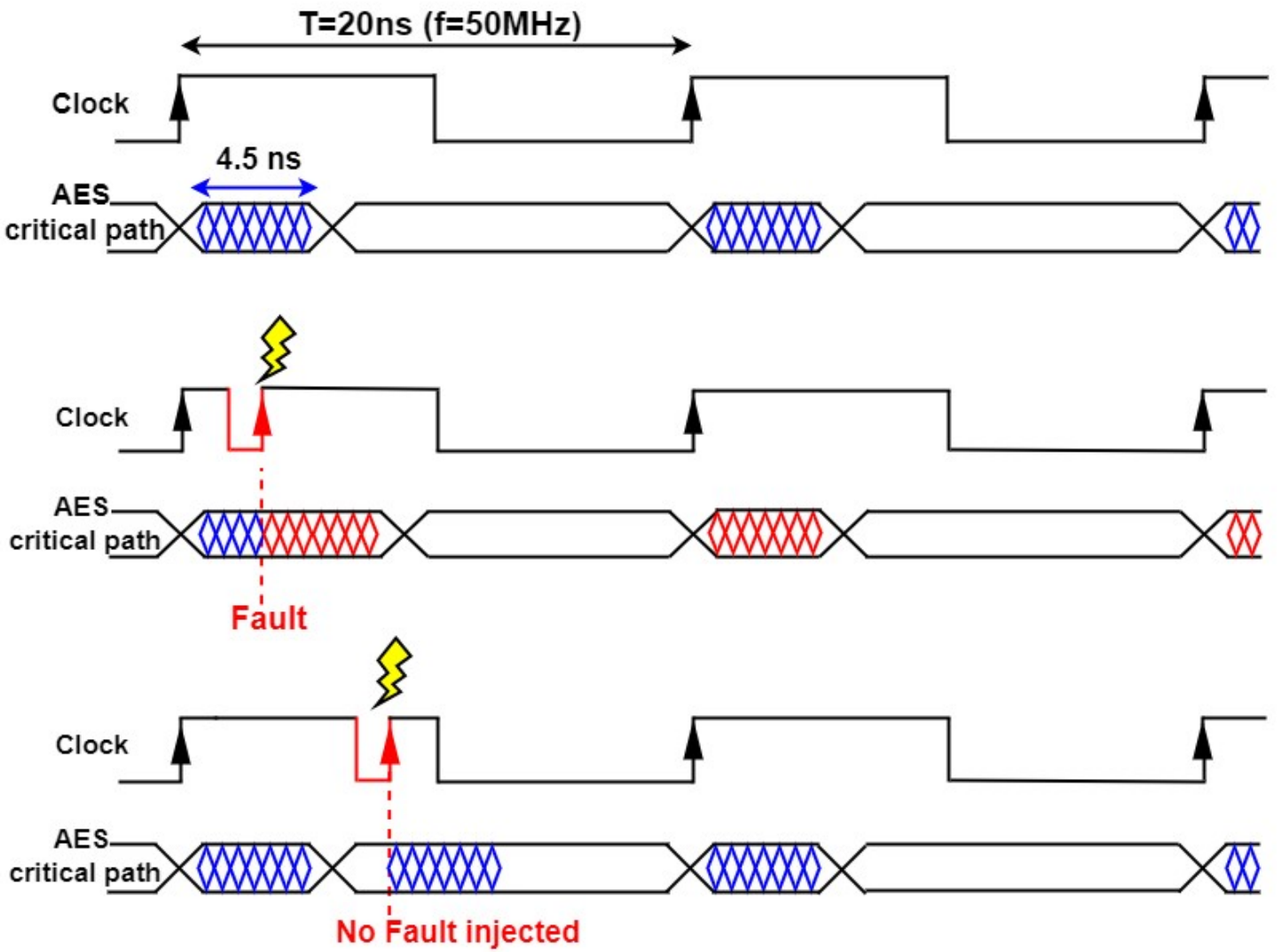


EMFI-induced clock glitches ($t_{critical} < \frac{T}{2}$)



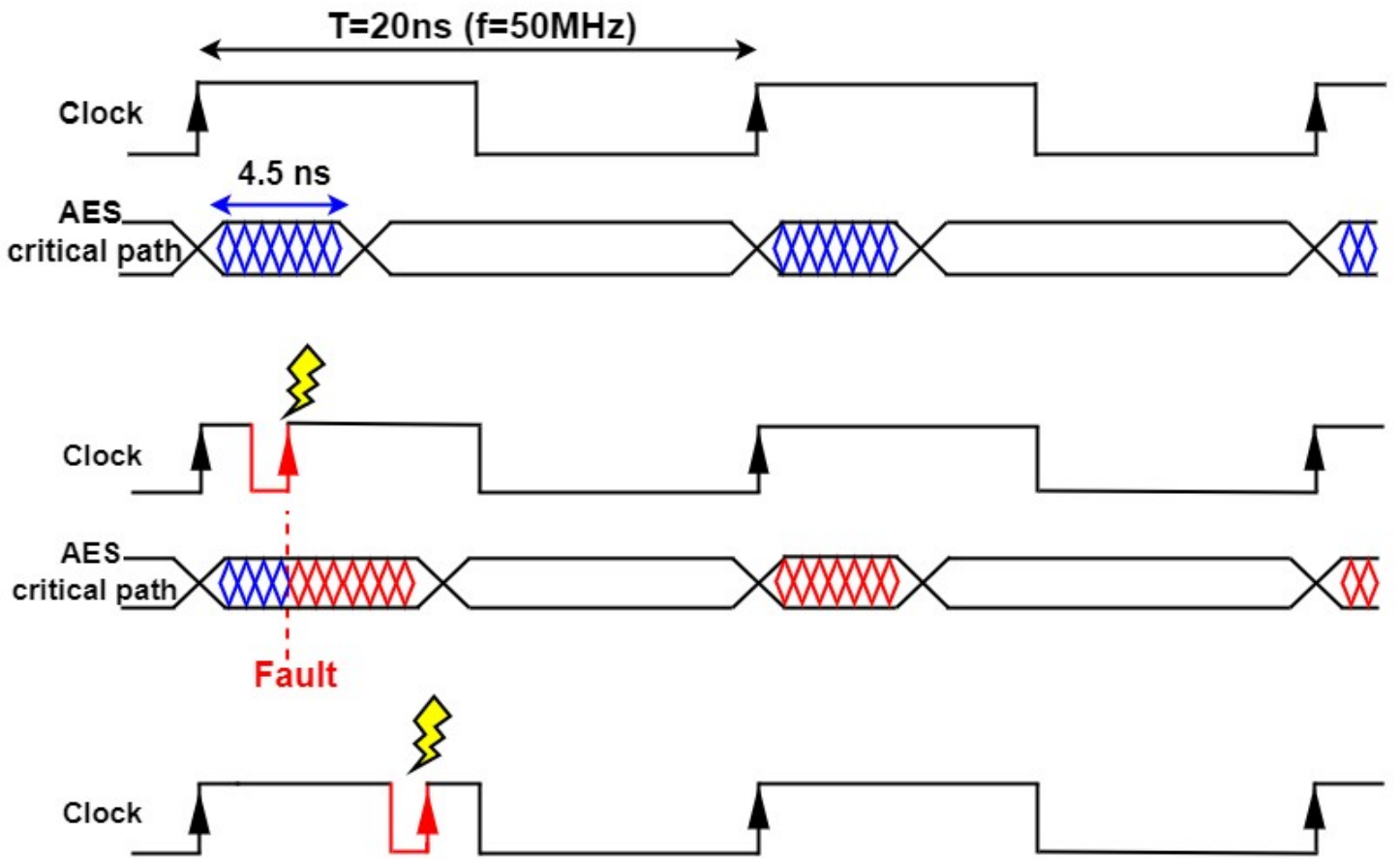
Timing violations

EMFI-induced clock glitches ($t_{critical} < \frac{T}{2}$)



Timing violations

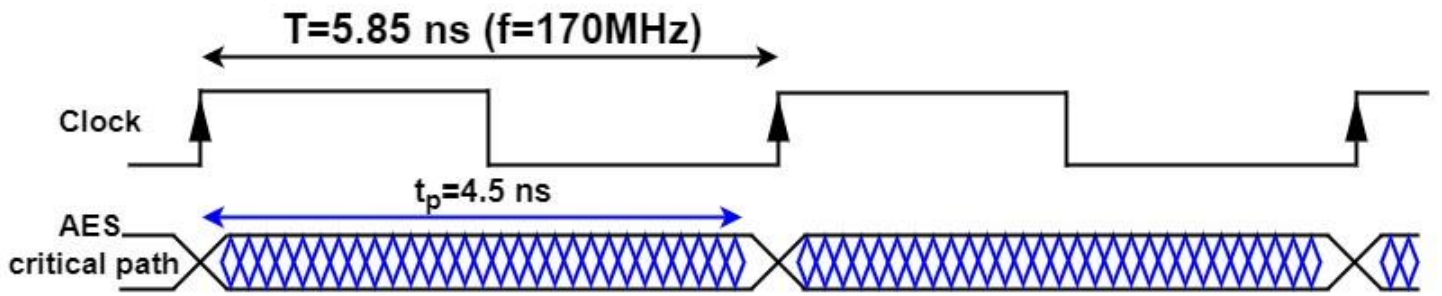
EMFI-induced clock glitches ($t_{critical} < \frac{T}{2}$)



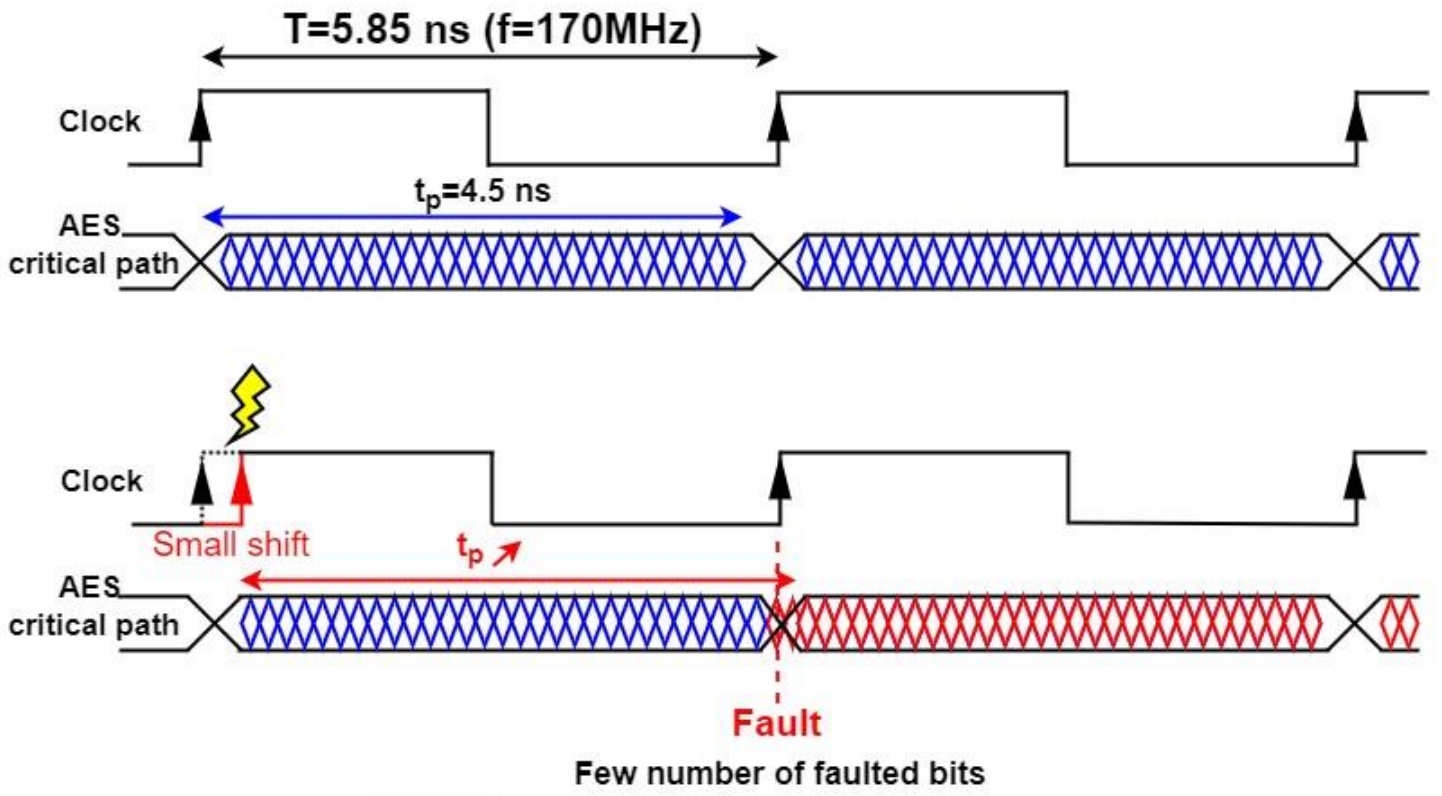
Timing violations

Width of injected faults windows depends on the critical path

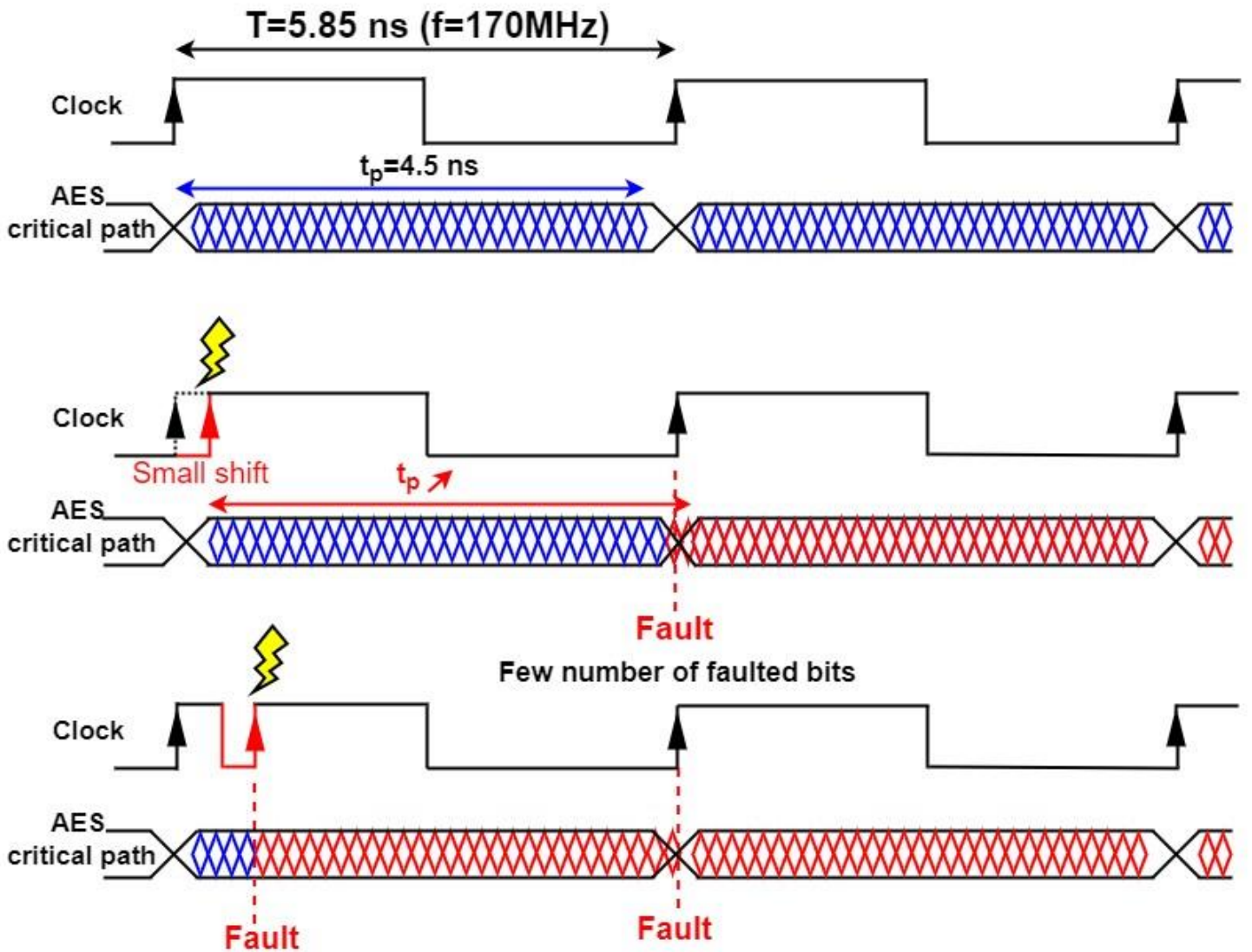
EMFI-induced clock glitches ($t_{critical} > \frac{T}{2}$)



EMFI-induced clock glitches ($t_{critical} > \frac{T}{2}$)

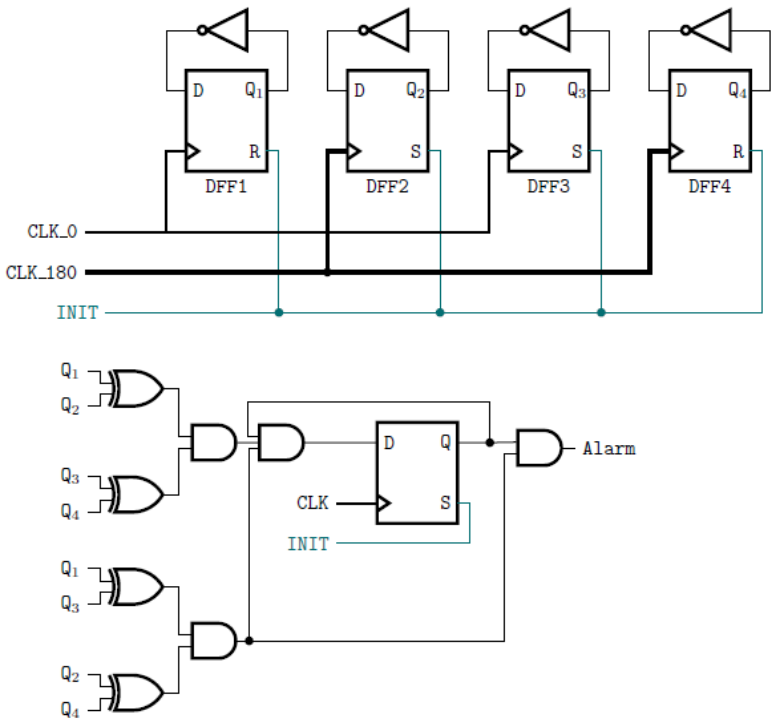


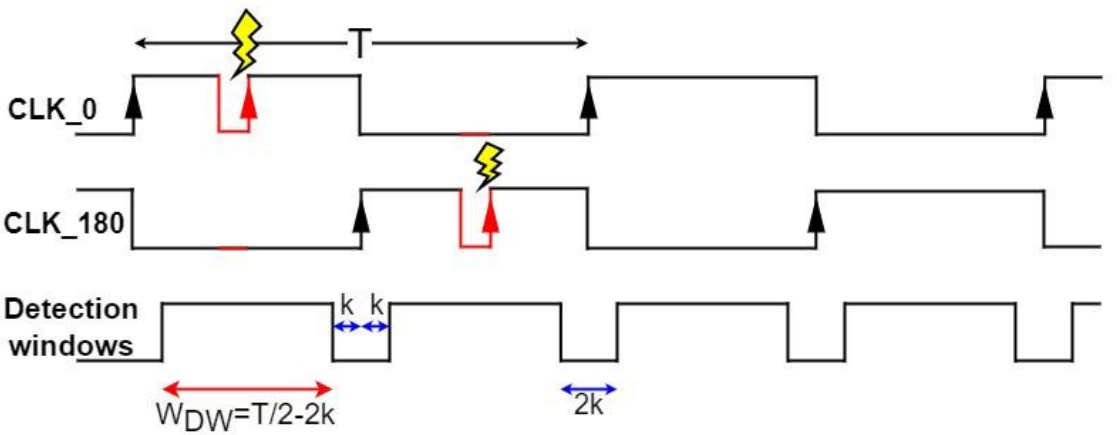
EMFI-induced clock glitches ($t_{critical} > \frac{T}{2}$)



Timing violations

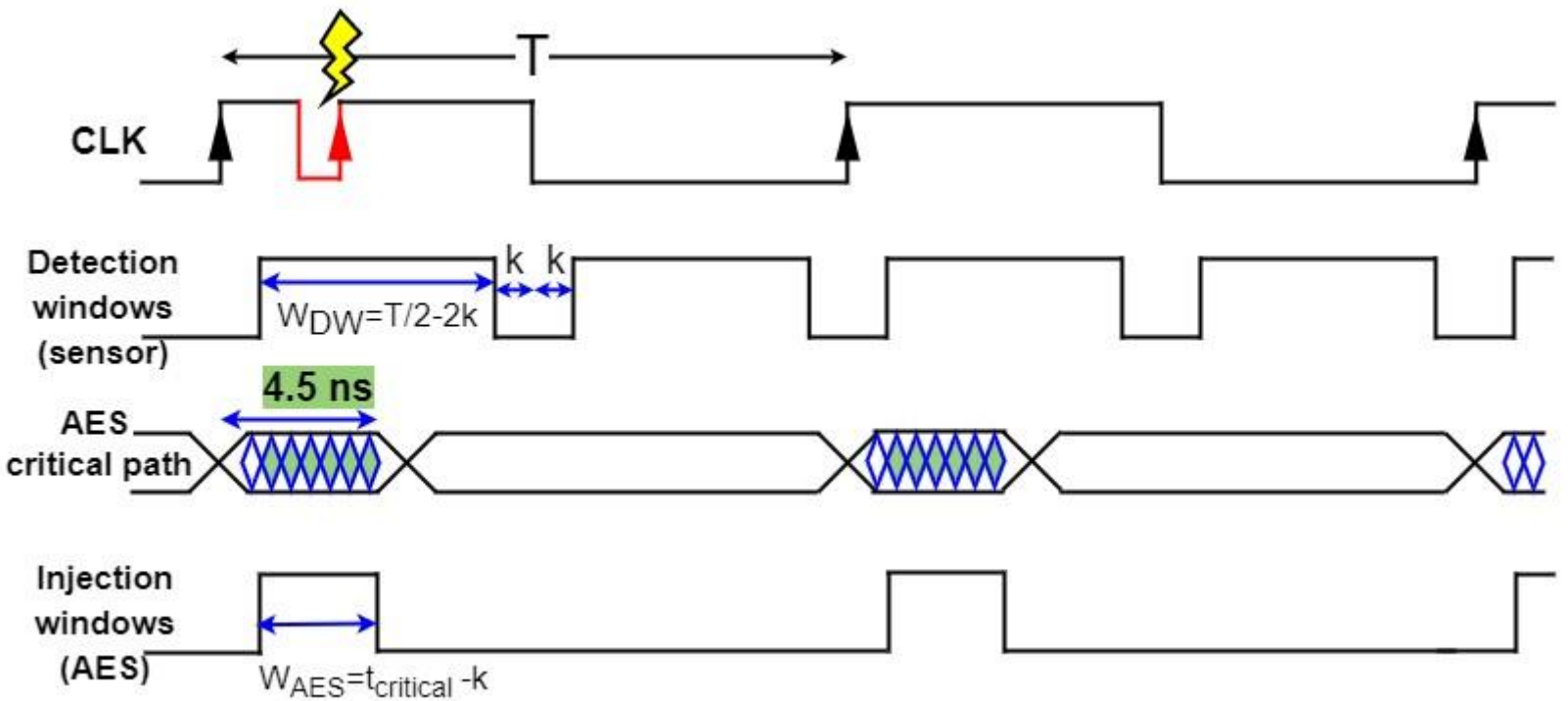
How does the mechanism of EMFI-induced clock glitch explain the triggering of the sensors?



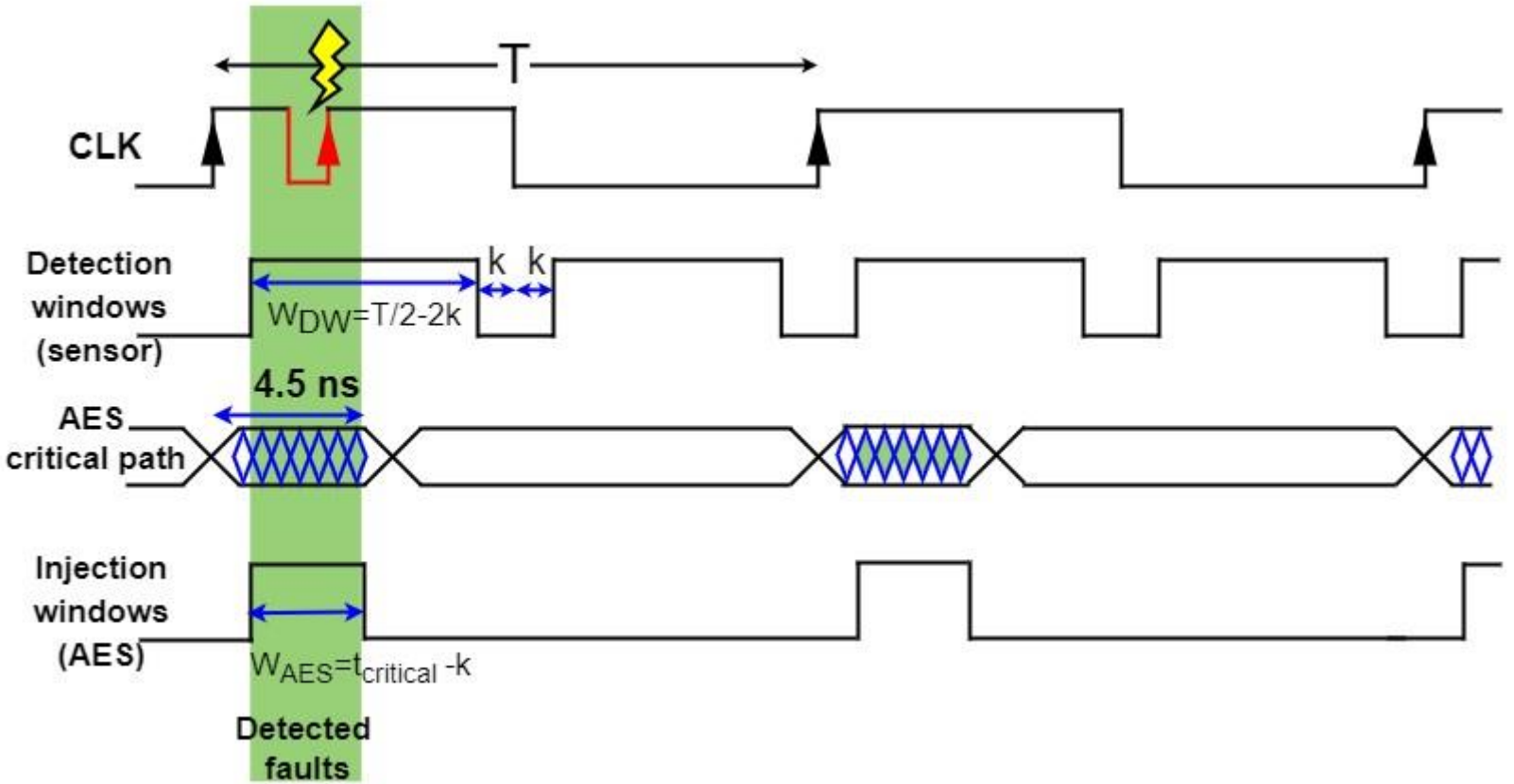


When frequency ↗, clock period ↘, the width of DWs for triggering sensors ↘

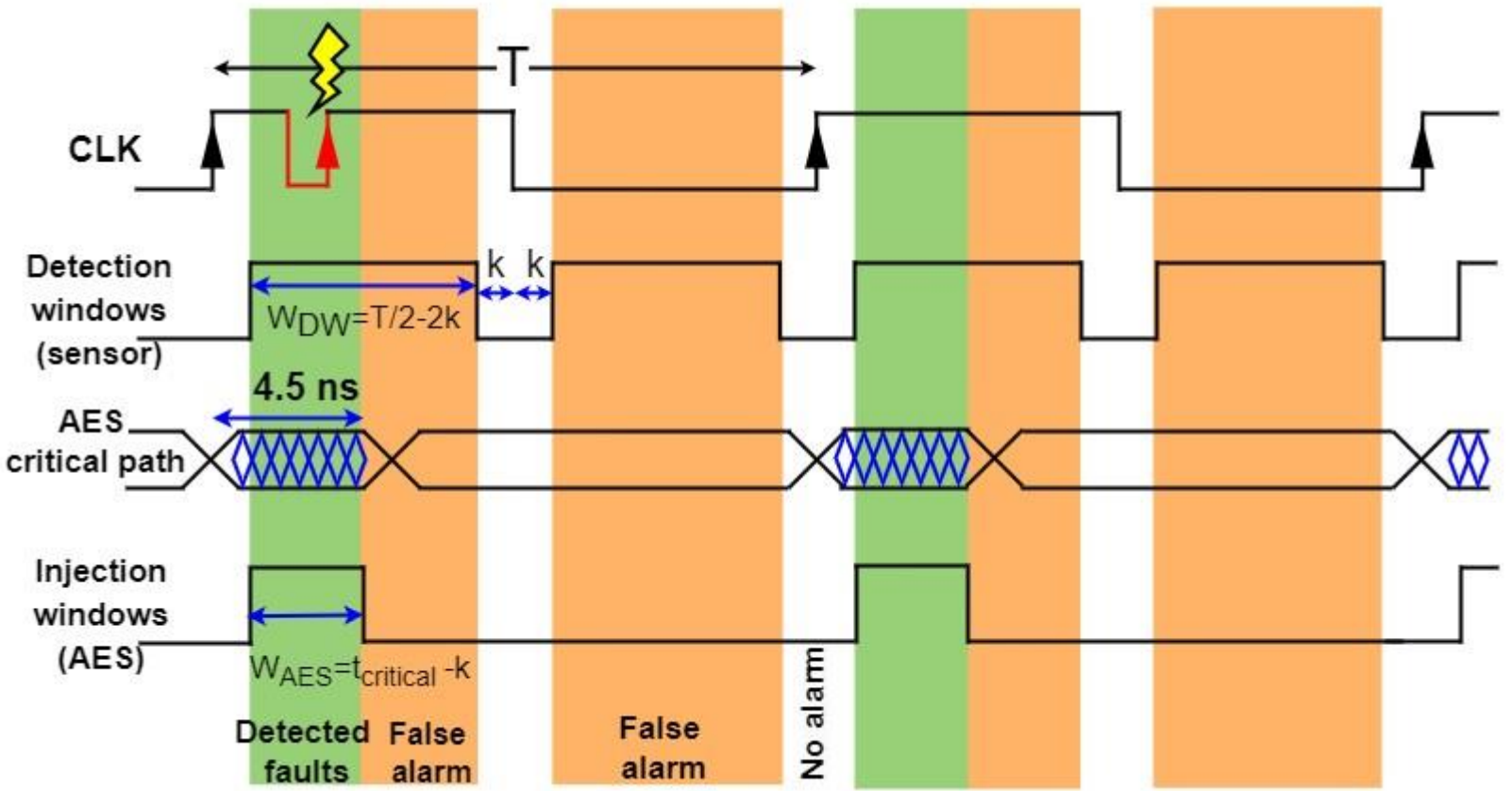
Study of the sensor's detection capability (when $t_{critical} < \frac{T}{2}$)



Study of the sensor's detection capability (when $t_{critical} < \frac{T}{2}$)



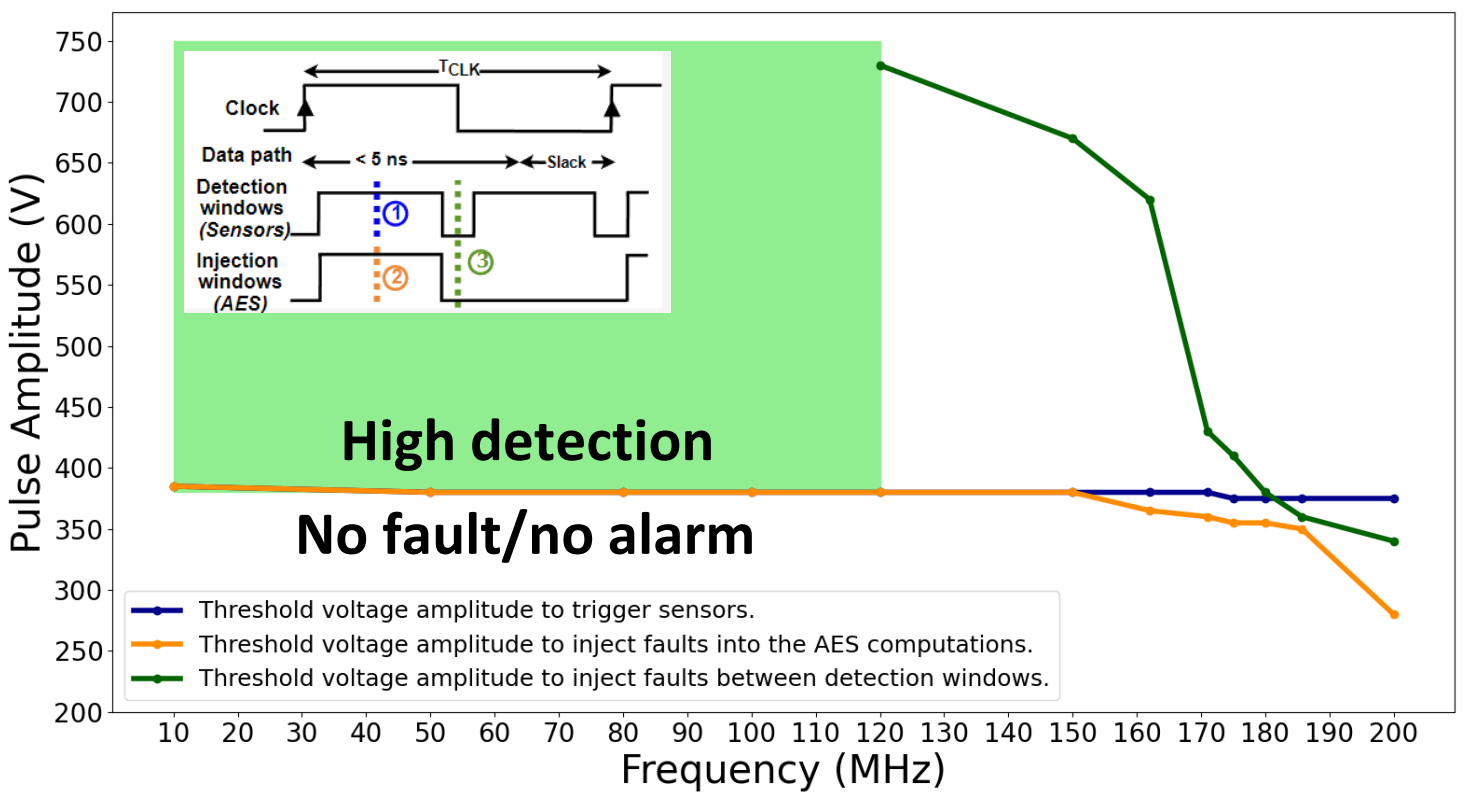
Study of the sensor's detection capability (when $t_{critical} < \frac{T}{2}$)



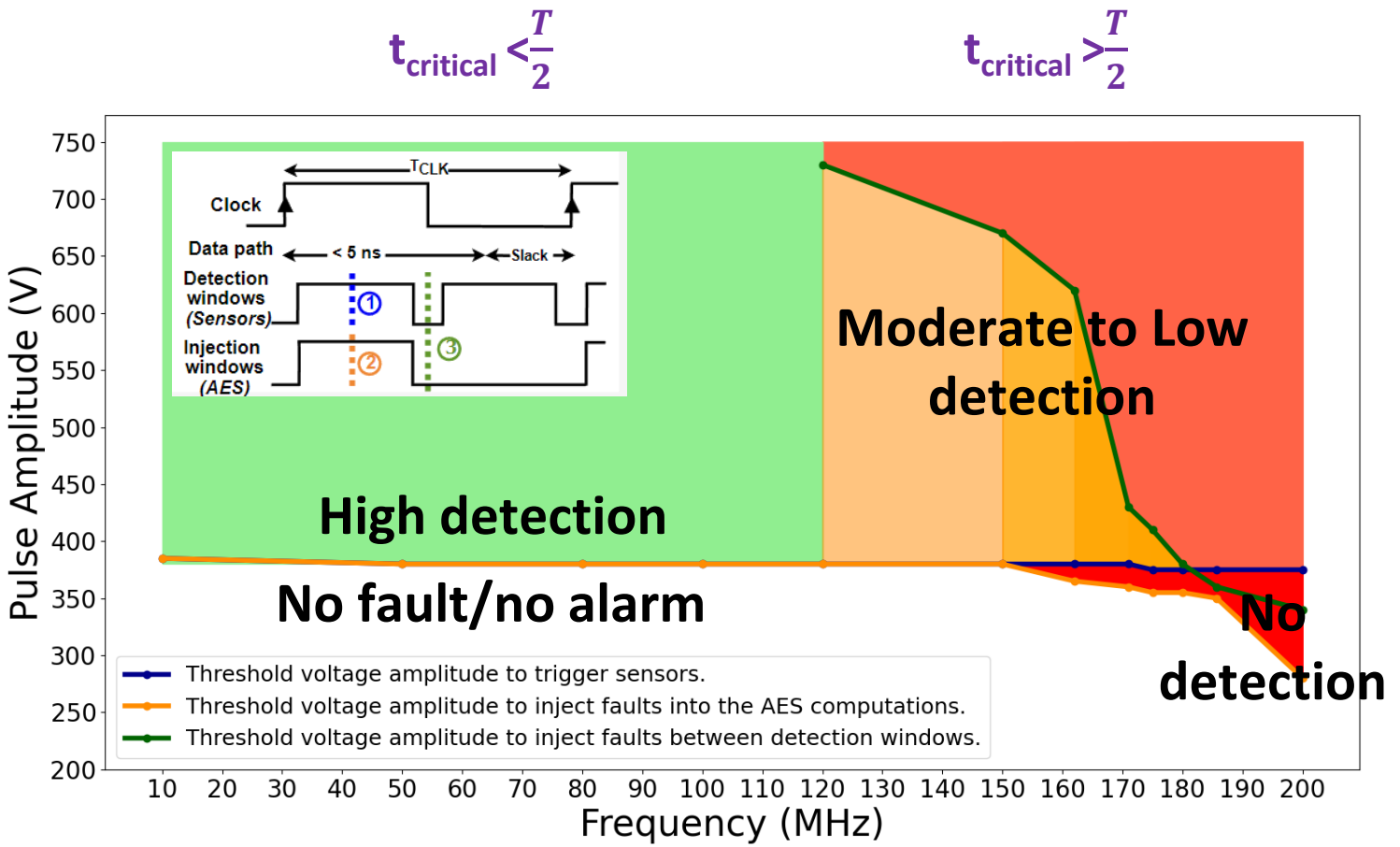
This explains why all injected faults are detected at low frequencies

Sensor's detection performance when changing clock frequency and pulse amplitude

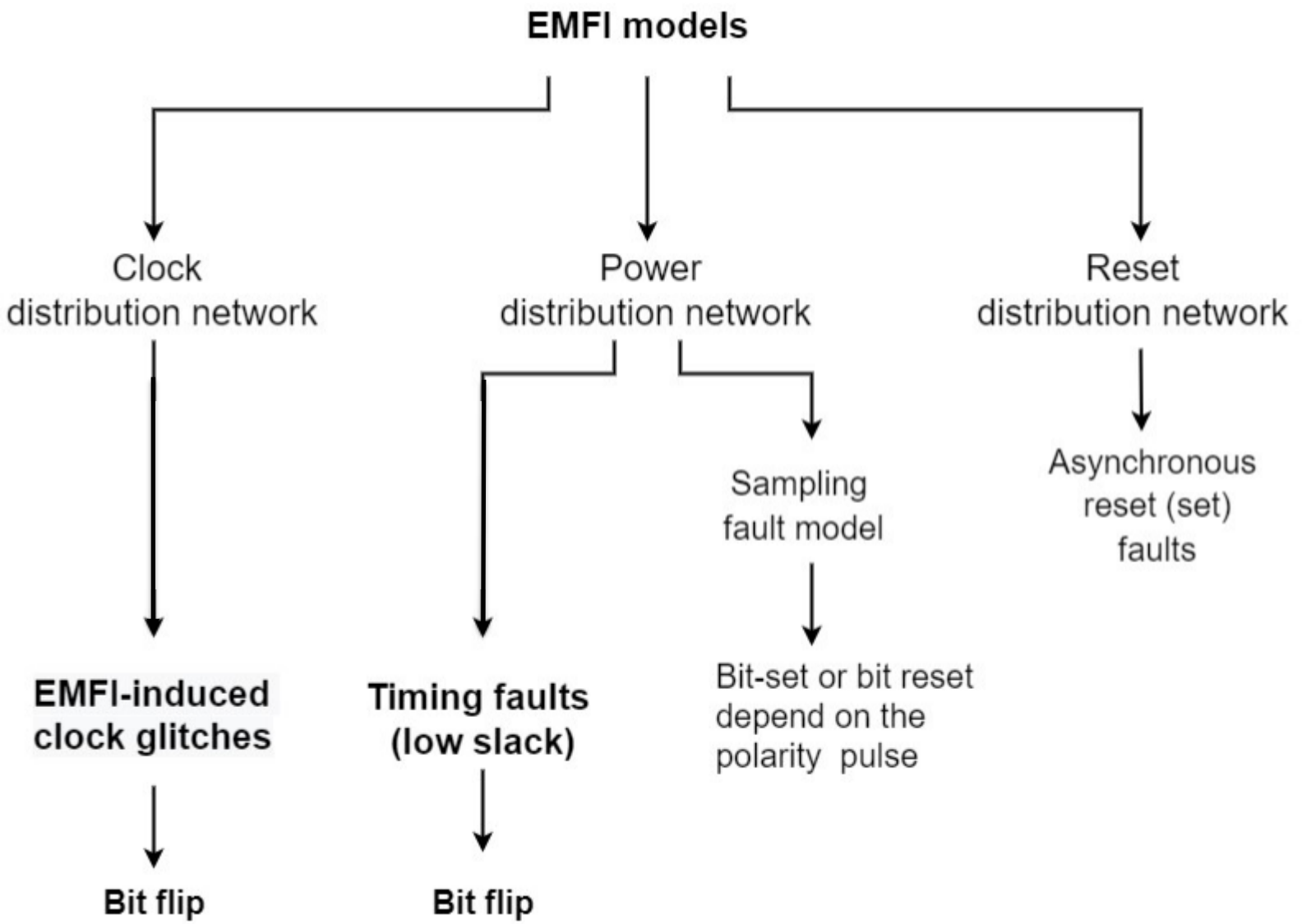
$t_{critical} < \frac{T}{2}$



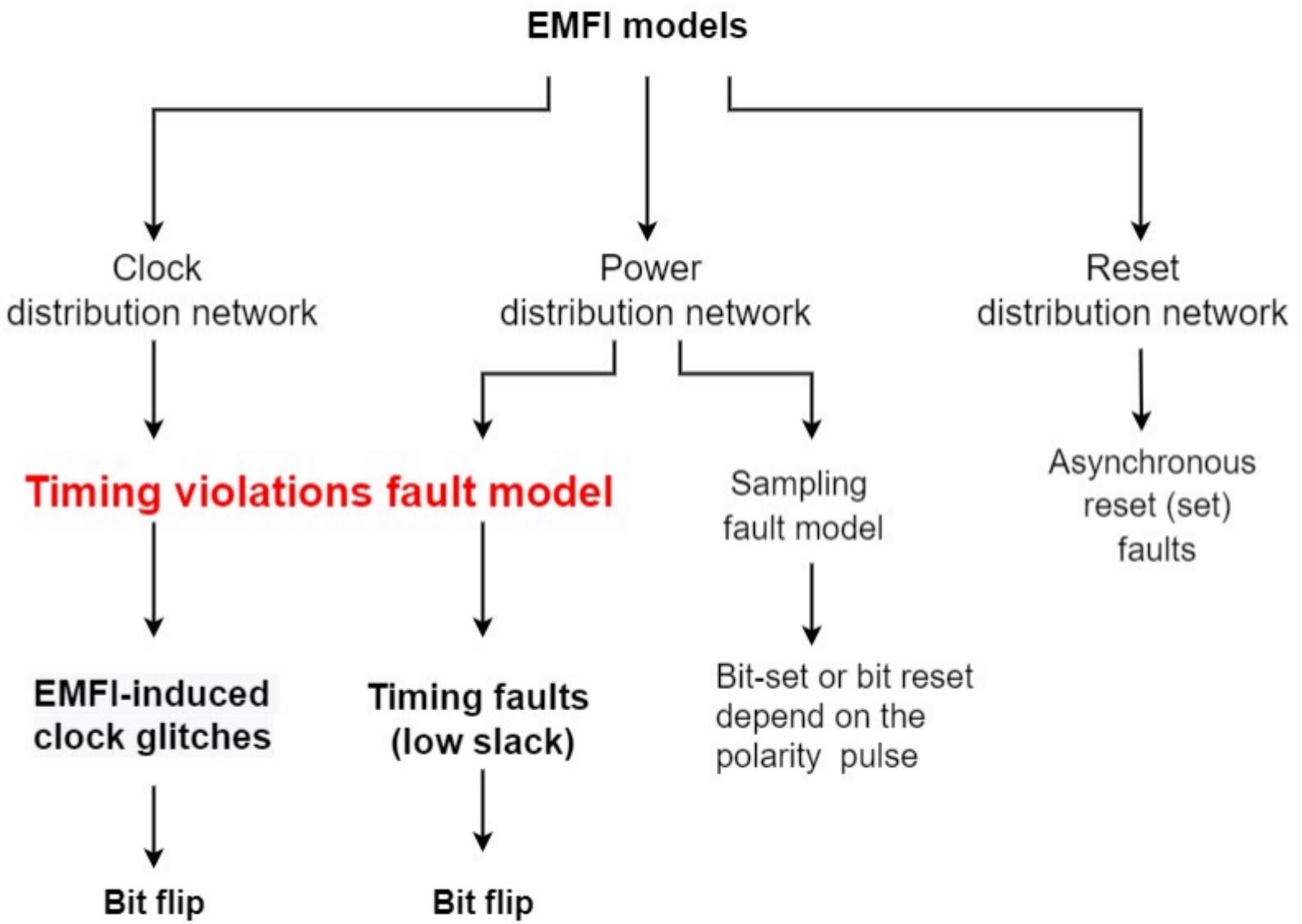
Sensor's detection performance when changing clock frequency and pulse amplitude



EMFI models: Timing violations fault model



EMFI models: Timing violations fault model



Outline

- Previous work
  - EMFI models
  - Fully digital detector
- Experimental setup
  - EMFI platform
  - DUT block diagram
- Experimental results
  - EMFI results
  - Deep exploration of EMFI mechanisms
  - Analysis of experimental results
- In-depth analysis of EMFI-induced clock glitches
- **Conclusion**

Conclusion

- EMFI models: timing violations fault model
  - EMFI-induced clock glitches within the clock network
  - Timing faults, which result from EM coupling with the PDN
- El-Baze sensor's efficiency
  - High detection at low frequencies
  - No detection of timing faults obtained at high frequencies
- The risk of using an EMFI detection sensor based on a single fault model
- An enhanced explanation of the EMFI models to aid designers in developing more effective detection sensors

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