November 19th, 2025

European Cyber Week

THE SOVEREIGN CYBER & DEFENCE AI FORUM

Fault Injection – Keynote 2

BITFLIP Conference

Fault Injection Keynote 2

November 19th, 2025
13:30

Le Refectoire

Jean-Max DUTERTRE

Professor, Mines Saint-Etienne

Monitoring Fault Injection Attacks with Sensors Lessons Learned

Equipe Commune Systèmes et Architectures Sécurisées
Mines Saint-Etienne, CEA, Leti, Centre CMP
13541 Gardanne FRANCE

Context – Hardware security

- Hardware security (ICs) – hardware attacks
- Secure HW: integrated circuits implementing security features
  - ✓ MCU/SoC with hardware cryptographic accelerator
  - ✓ Memory readback protection (IP & user data protection)

- Fault Injections Attacks (FIA)
  - ✓ Active/Perturbation attacks

  Attack objectives:
  - ✓ Information leakage (DFA) → secret key extraction
  - ✓ Control flow attacks (e.g., test inversion → memory extraction)

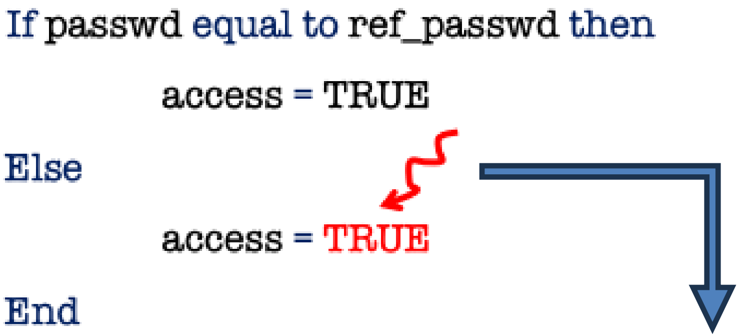
Context – Fault Injection Attack example

- Control Flow attack on a password verification routine
  - ✓ Test inversion through instr. modification / data corruption

```
If passwd equal to ref_passwd then
        access = TRUE
Else
        access = TRUE
End
```

Applied stress
→ FIA

Context – Monitoring FIA with sensors



```
If passwd equal to ref_passwd then
        access = TRUE
Else
        access = TRUE
End
```

Fault induced through the application of a **stress**

→ can be monitored and detected using **sensors**

- This talk
  - ✓ Monitoring FIA with digital sensors
  - ✓ Sensor principles
  - ✓ FIA mechanisms
  - ✓ Lessons learned designing and testing various sensors

    why many fail and others succeed

Monitoring FIA with Sensors – Lessons Learned

- Monitoring FIA with digital sensors – basics/principles

- Fault Injection Attacks
- EMFI detection sensors
- LFI detection sensors
- Conclusion

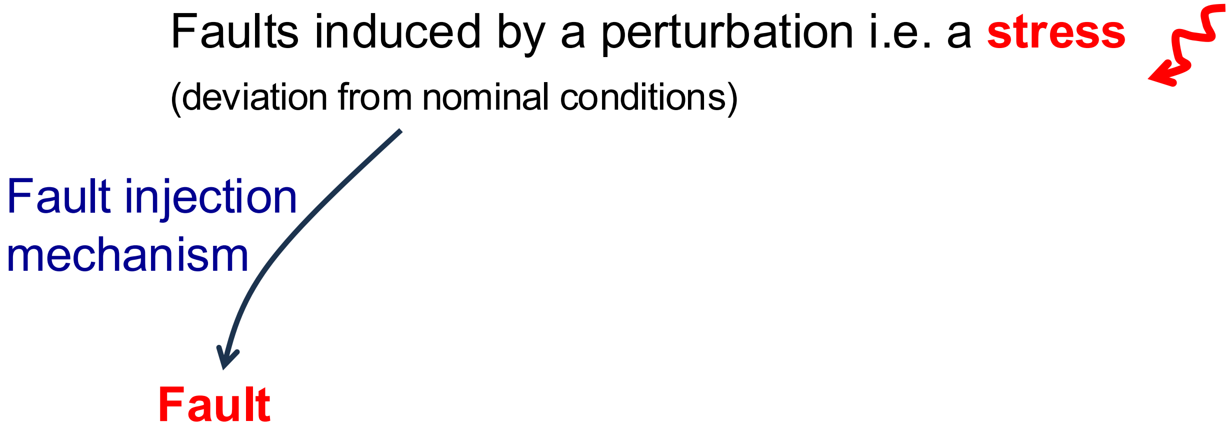
Monitoring FIA with digital sensors – basics/principles

- Digital sensors built from digital gates
  - ✓ Easier to design and to adapt to various technology nodes and manufacturers
  - ✓ Integration into ASIC and FPGA
  - ✓ Digital but based on analog mechanisms

- Analog sensors: custom analog design
  - ✓ Not addressed in this talk …
  - ✓ … not because they are less efficient but because not the speaker's expertise

Monitoring FIA with digital sensors – basics/principles

- Detection principle → monitoring the applied stress



Faults induced by a perturbation i.e. a **stress**

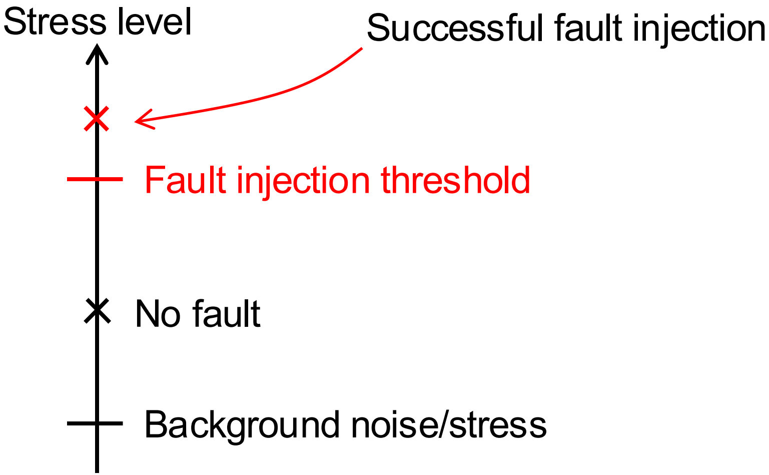
(deviation from nominal conditions)

Fault injection mechanism

Fault

Monitoring FIA with digital sensors – basics/principles

- Fault injection depends on the level of applied stress



Stress level

Successful fault injection

Fault injection threshold

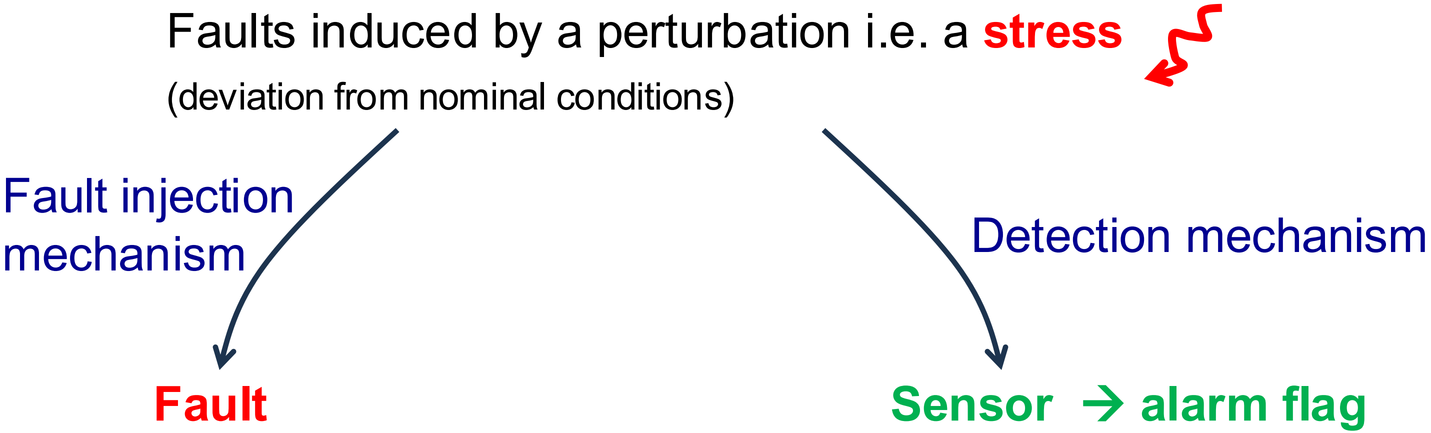
No fault

Background noise/stress

⇨ A certain level of stress has to be reached: Fault injection threshold

Monitoring FIA with digital sensors – basics/principles

- Detection principle → monitoring the applied stress



Faults induced by a perturbation i.e. a **stress**

(deviation from nominal conditions)

Fault injection mechanism

Detection mechanism

Fault

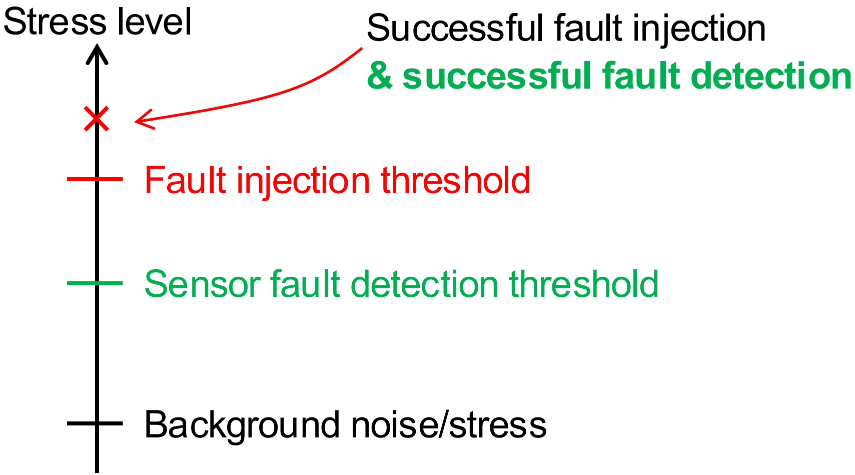
Sensor → alarm flag

Main principle: detect the applied stress and raise an alarm flag

! a security policy has then to be applied, a sensor by itself is not a countermeasure …
(discussion out of the scope of this talk)

Monitoring FIA with digital sensors – basics/principles

- Sensor detection threshold vs fault injection threshold



Stress level
Successful fault injection
& successful fault detection
Fault injection threshold
Sensor fault detection threshold
Background noise/stress

- Setting the detection threshold below the fault threshold ensures an efficient detection of FIA

Monitoring FIA with digital sensors – basics/principles

- Sensor design and evaluation metrics

- 2-step process
  - ✓ Sensor design, based on a detection mechanism (addressed later)
  - ✓ Sensor evaluation → on experimental basis

- Metrics
  - ✓ Type of monitored stress (Voltage, Temperature, Frequency, EMFI, LFI sensors)
  - ✓ Size
  - ✓ Power consumption
  - ✓ Latency
  - ✓ Detection threshold & area
  - ✓ Efficiency → sensor’s response to be tested experimentally

Monitoring FIA with digital sensors – basics/principles

- Sensor response classification → 2-letter code TP/TN/FP/FN

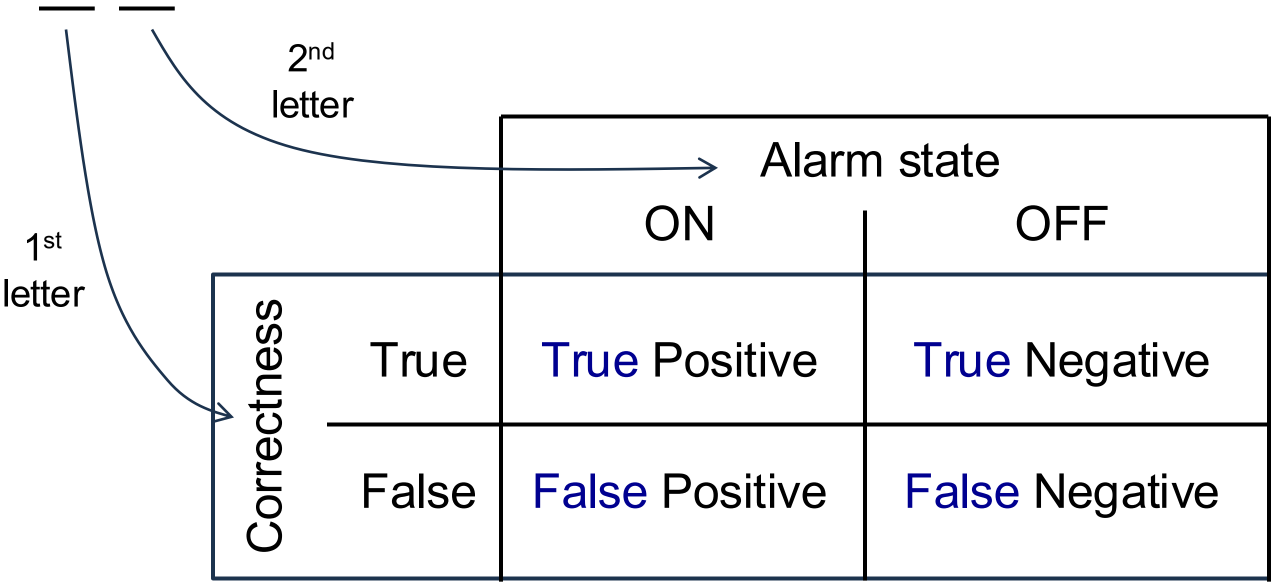
__ __

2^{nd} letter

		Alarm state	
		ON	OFF
Correctness	True	True Positive	True Negative
	False	False Positive	False Negative

Monitoring FIA with digital sensors – basics/principles

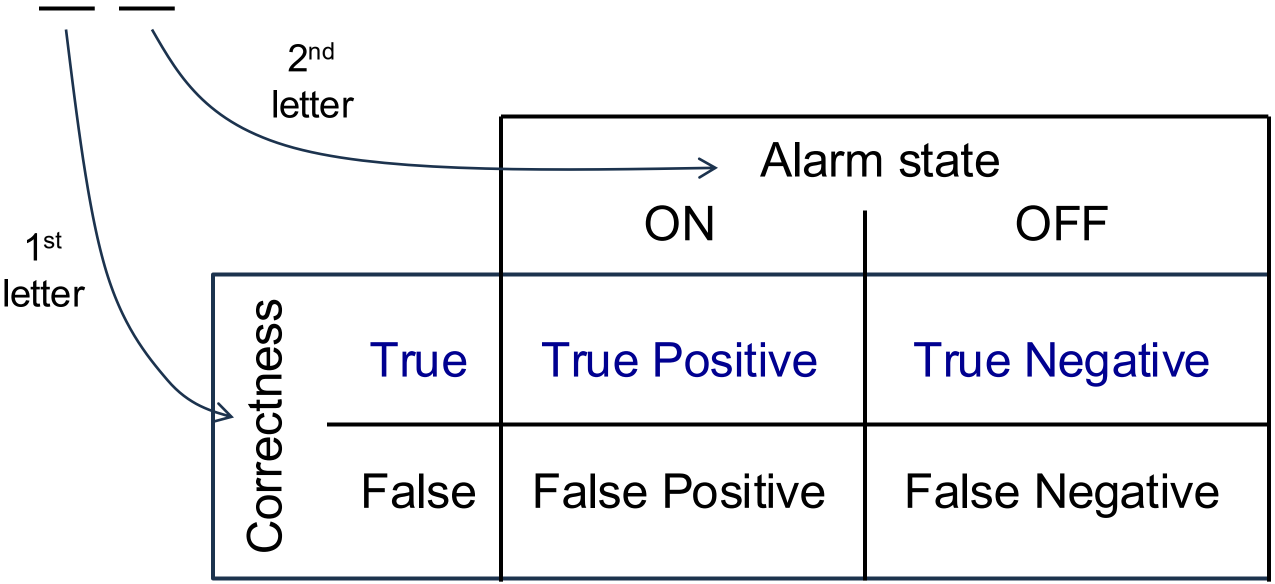
- Sensor response classification → 2-letter code TP/TN/FP/FN



		Alarm state	
		ON	OFF
Correctness	True	True Positive	True Negative
	False	False Positive	False Negative

Sensor response classification

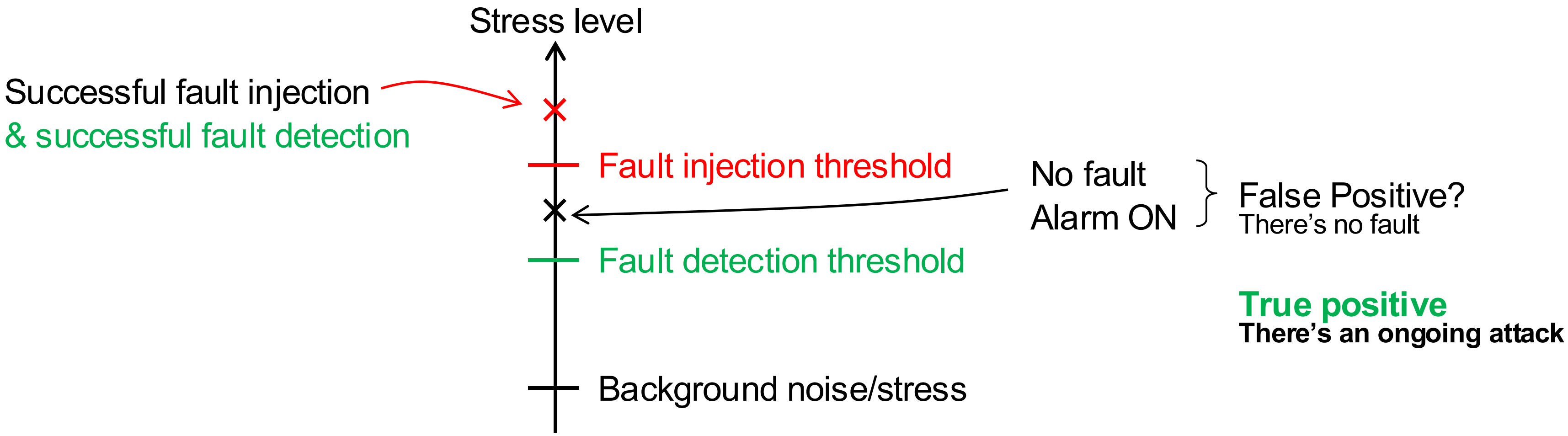
- Two ideal cases: True Positive & True Negative



		Alarm state	
		ON	OFF
Correctness	True	True Positive	True Negative
	False	False Positive	False Negative

Sensor response classification

- Definition of a True Positive



Stress level

Successful fault injection
& successful fault detection

Fault injection threshold

Fault detection threshold

Background noise/stress

No fault
Alarm ON

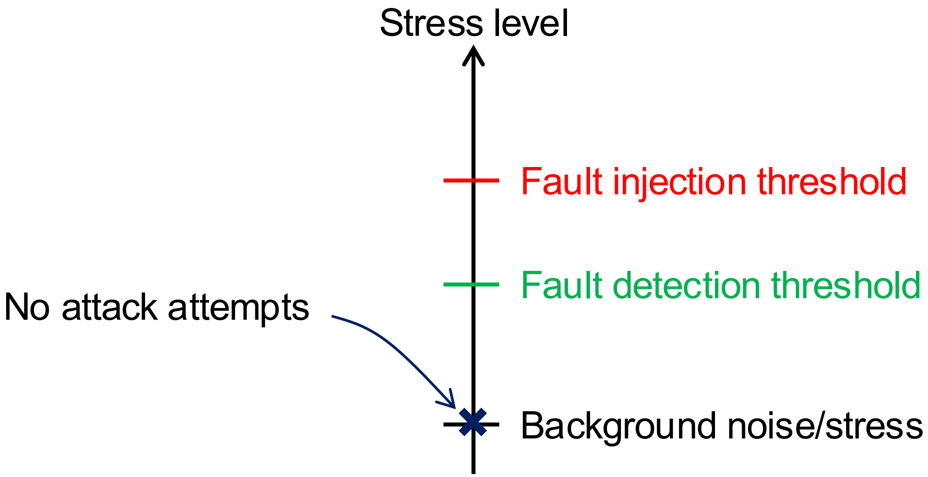
False Positive?
There’s no fault

True positive
There’s an ongoing attack

⇒ FIA sensor = stress/attack detector, not a fault detector (based on information redundancy)

Sensor response classification

- True Negative case: presence of a background noise or stress

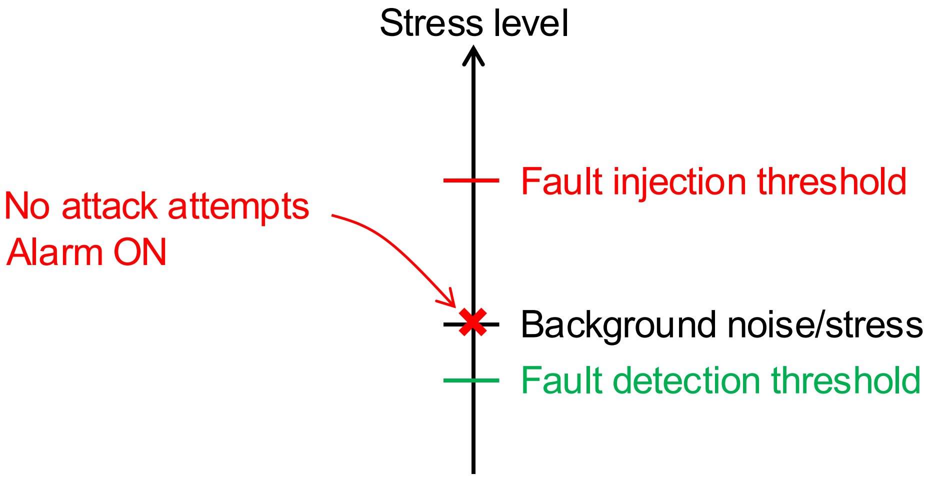


- However
  - ✓ Background noise/stress is not constant
  - ✓ The Fault detection threshold can be set low

→ They may cross leading to a False Positive sensor response

Sensor response classification

- False Positive case

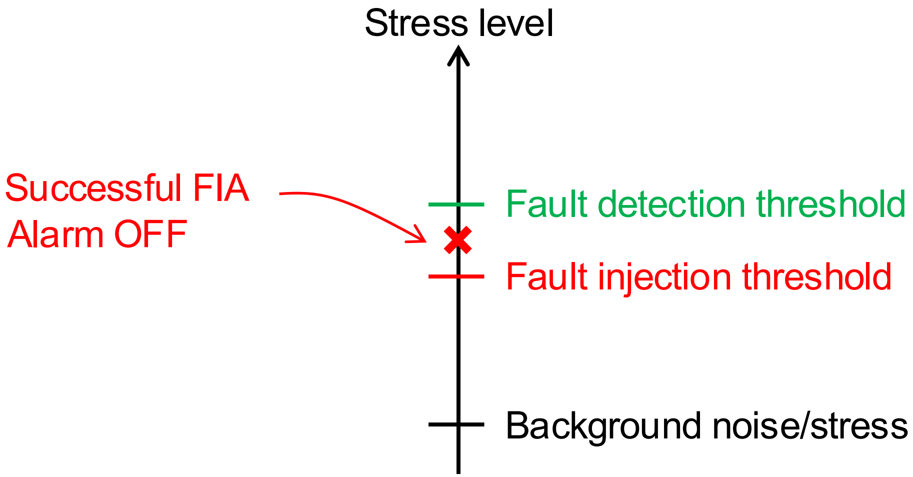


⇨ False Positive to be (absolutely) avoided → security policy is triggered

Key/data erasure, etc.
Similar to a denial of service

Sensor response classification

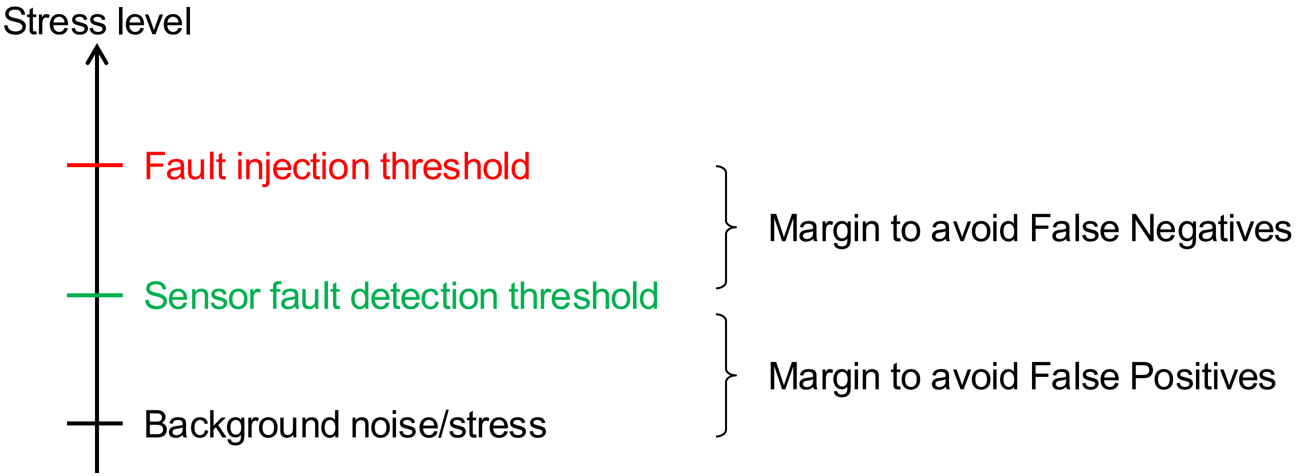
- False Negative case – Faull injection threshold < Fault detection threshold



- Injection/detection thresholds are not constant
  - ✓ Characteristics of the applied stress (duration, location, etc.)
  - ✓ Environmental conditions

Monitoring FIA with digital sensors – basics/principles

- Sensor detection threshold vs fault injection threshold


Stress level
Fault injection threshold
Sensor fault detection threshold
Background noise/stress
Margin to avoid False Negatives
Margin to avoid False Positives

Monitoring FIA with Sensors – Lessons Learned

- Monitoring FIA with digital sensors – basics/principles

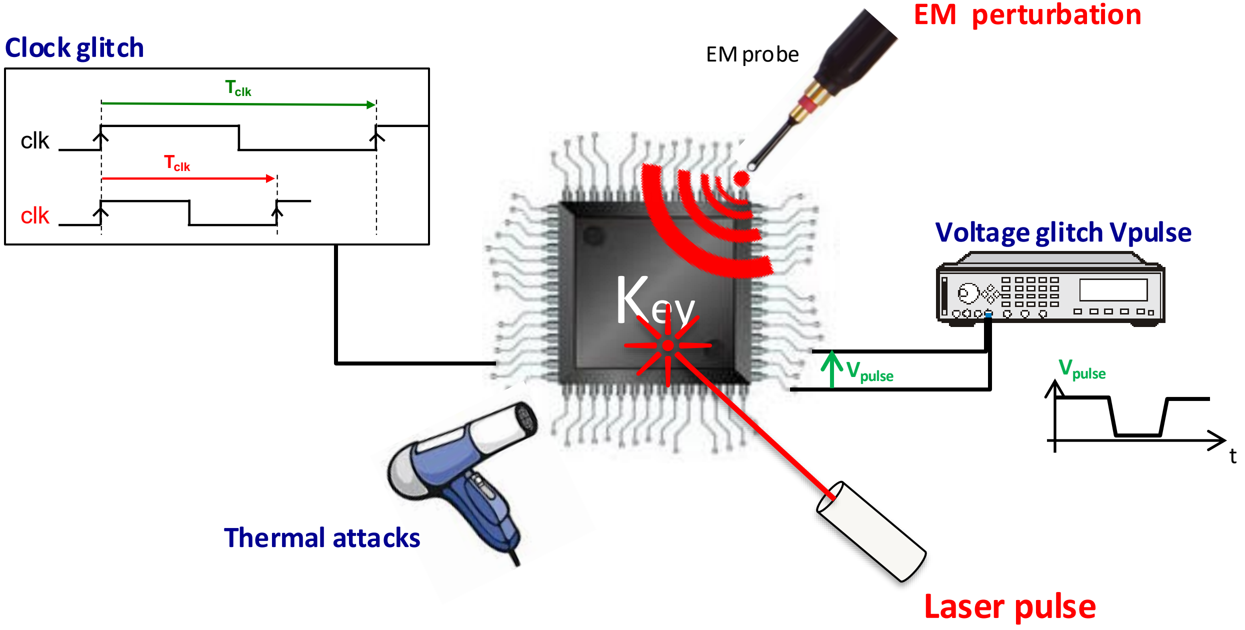
- Fault Injection Attacks

- EMFI detection sensors
- LFI detection sensors
- Conclusion

Fault Injection Attack basics

- Fault injection techniques

→ Disturbance of nominal operating conditions of a device target (ie stress attack)

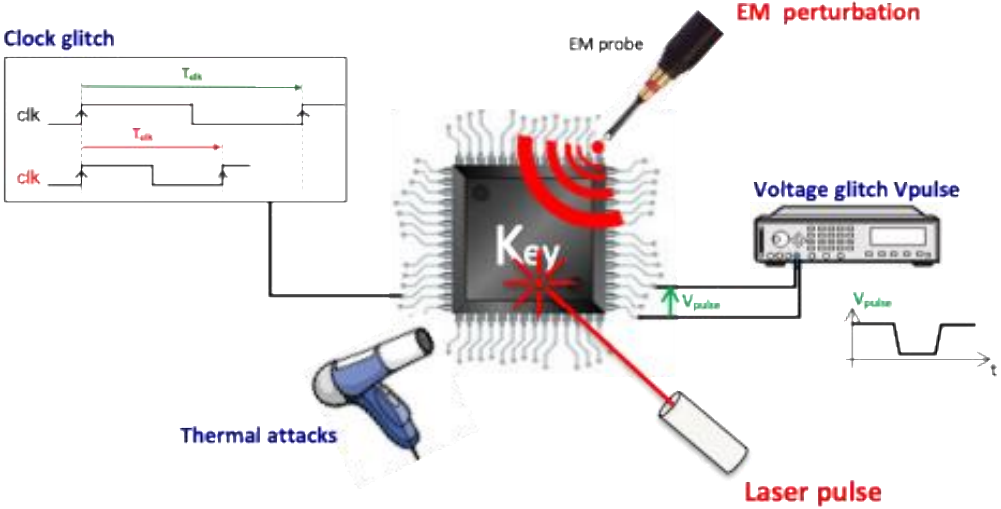


Fault Injection Attack basics

- Fault injection techniques

→ Disturbance of nominal operating conditions of a device target (ie stress attack)

  - Global effect, timing violation: clock, voltage supply, thermal perturbations
  - EMFI: local, timing violation
  - LFI: local
  - Radiation effects



Monitoring FIA with Sensors – Lessons Learned

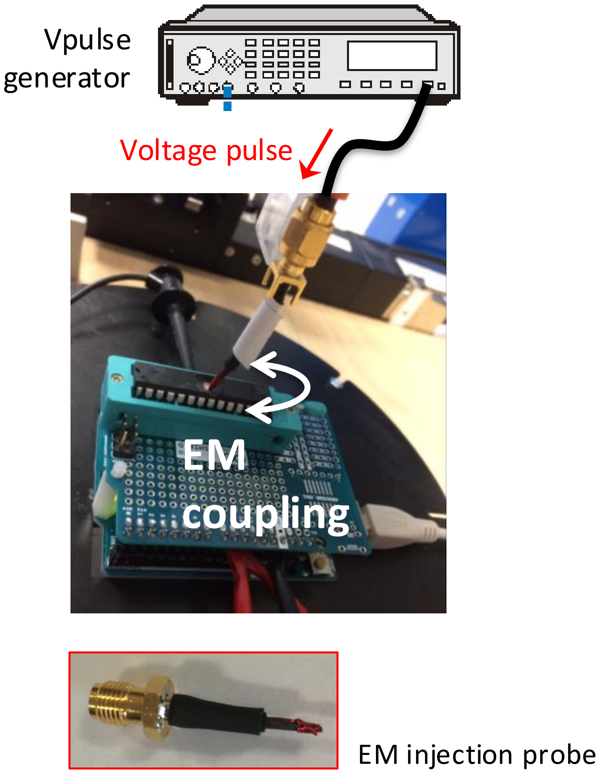
- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks

- EMFI detection sensors
  - EMFI mechanism
  - Delay-based sensor
  - DFF-based sensor
  - TDC-based sensor

- LFI detection sensors
- Conclusion

EMFI detection sensors

- EMFI mechanism



EM pulse induced by Vpulse (rising and falling edges) through currents variations in the injection probe

⇩

EM coupling with the target’s power/clock network

⇩

Induced transient in the target’s power/clock network

⇩

Voltage and/or clock glitches

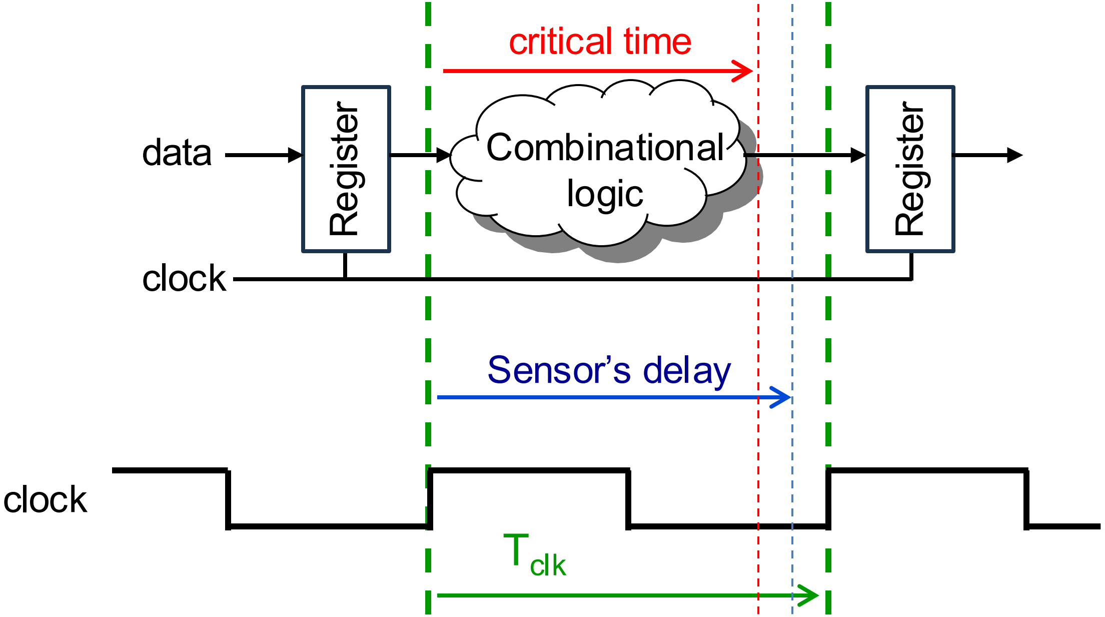
⇩

Timing constraints violation and faults!

R. Nabhan et al., Highlighting two EM fault models …, DATE 2023

EMFI detection sensors

- Delay-based sensor → Timing constraints monitoring of digital synchronous circuits
  - ✓ Idea: power supply and clock network stress can be monitored with a delay element

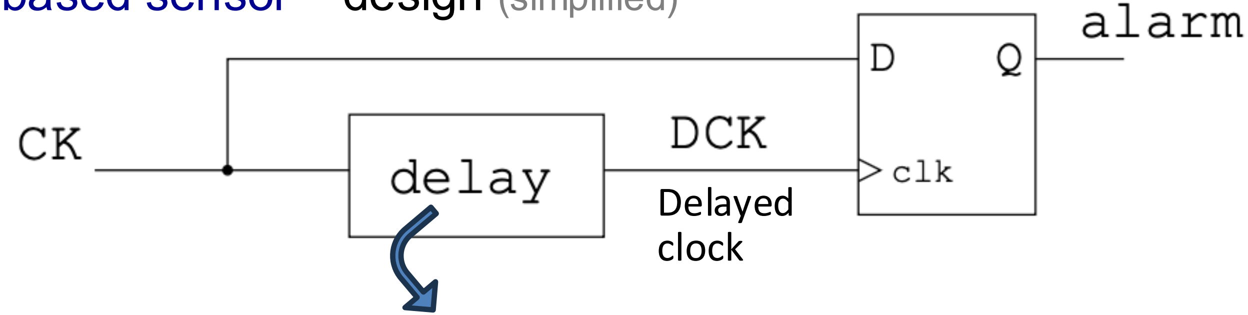


$\text{Logic}_{\text{critical time}} < T_{clk}$

$\text{Logic}_{\text{critical time}} < \text{delay} < T_{clk}$

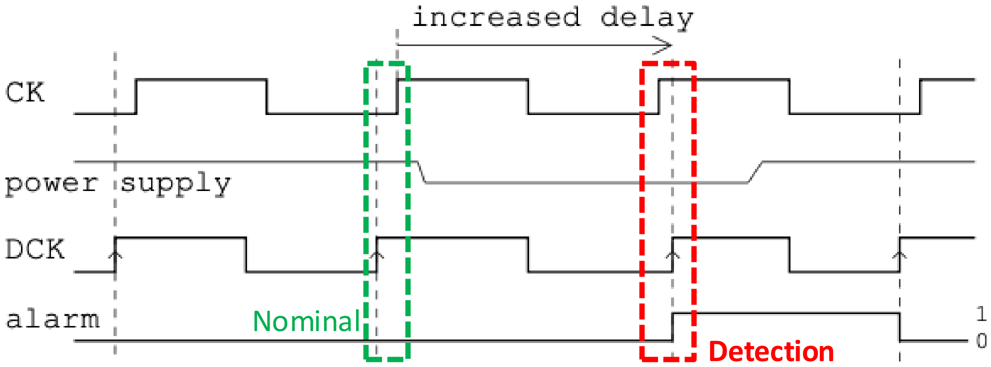
EMFI detection sensors

- Delay-based sensor – design (simplified)



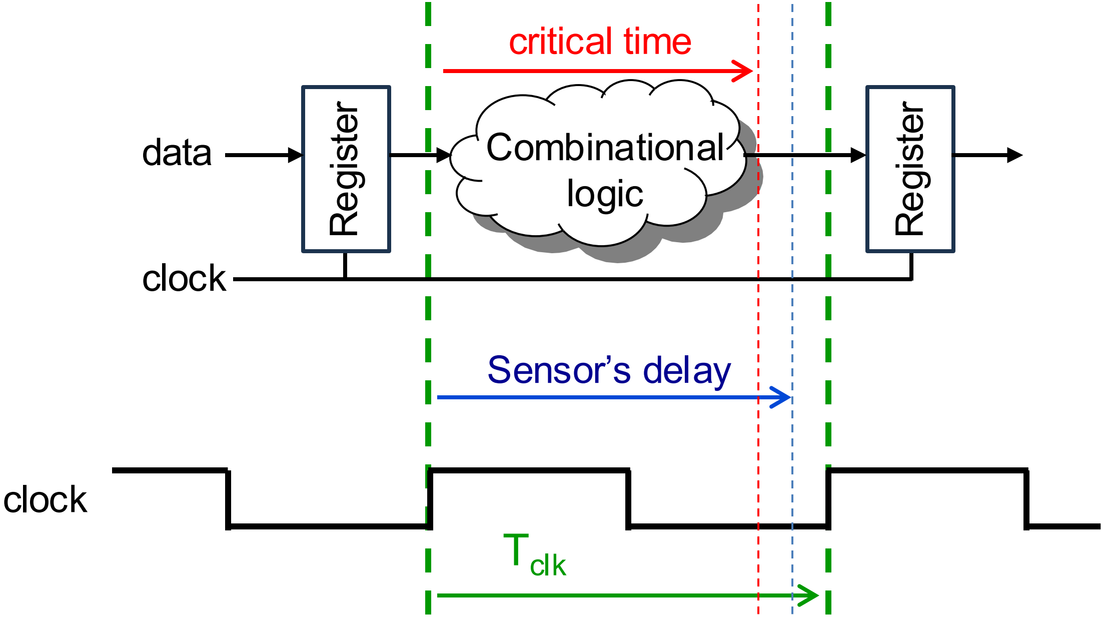
✓ Delay: increases with T° and voltage drop (also works for clock glitches)

→ Inversion of phase skew between CK and DCK → trigger the alarm



EMFI detection sensors

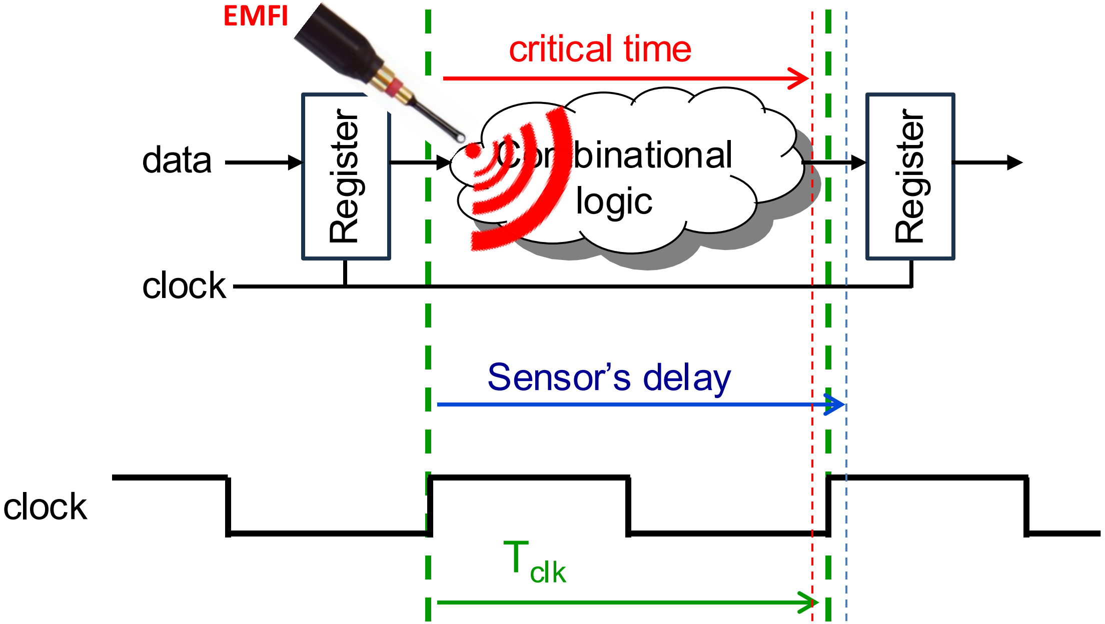
- Delay-based sensor → detection of an EMFI-induced voltage glitch



Logic $_{\text{critical time}}$ > delay > T_{clk}

EMFI detection sensors

- Delay-based sensor → detection of an EMFI-induced voltage glitch
  → Similar for detection of an EMFI-induced clock glitch

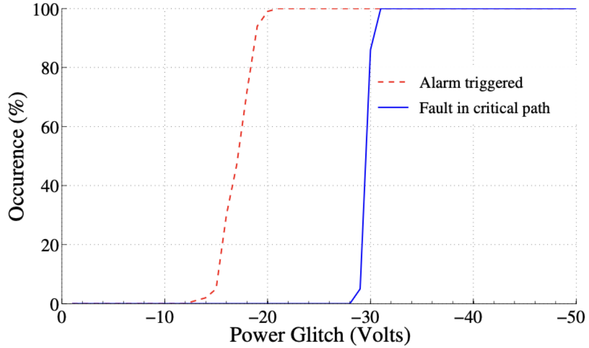


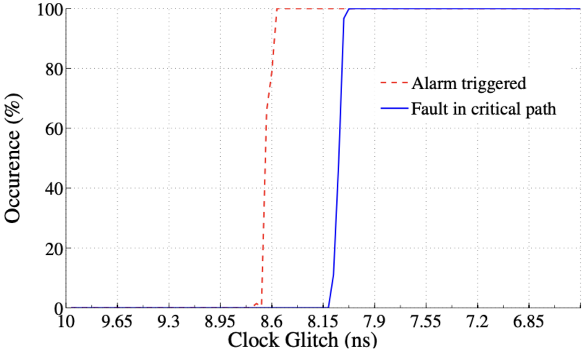
$\text{Logic}_{\text{critical time}} > \boxed{T_{clk} > \text{delay}}$

→ Alarm triggered

EMFI detection sensors

- Delay-based sensor – Exp. validation
  - ✓ Test vehicle: Delay-based sensor + AES accelerator on FPGA





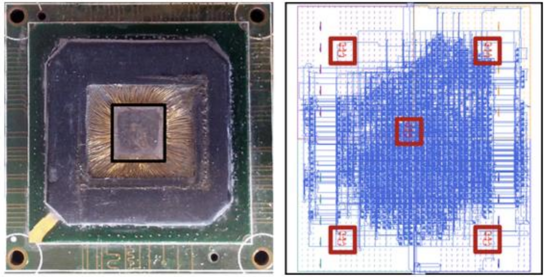
Voltage & clock glitches test series:
(applied externally)

- 100% detection rate
- No False Positive
- No Undetected fault

⇨ Fully efficient against global stress
Voltage, clock, temperature

EMFI detection sensors

- Delay-based sensor – Exp. validation
  - ✓ EMFI test series → EMFI has a local effect

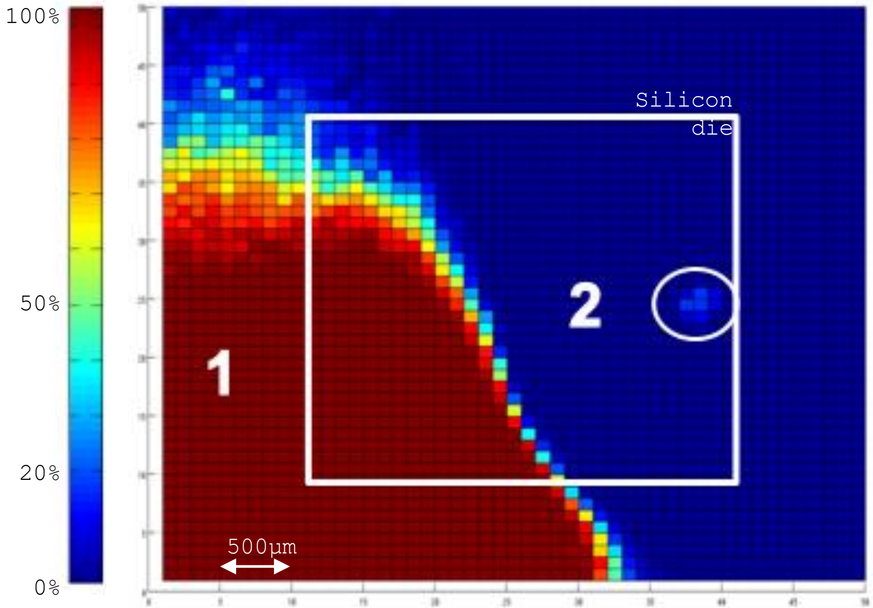


AES + 5 delay-based sensors

L. Zussa, et al., Efficiency of a Glitch Detector against Electromagnetic Fault Injection, DATE 2014

EMFI detection sensors

- Delay-based sensor – Exp. validation
  - ✓ EMFI test series → EMFI has a local effect



Single sensor test series

- Area 1 → Alarm triggered
- Area 2 → Fault injection

⇨ A delay-based sensor has a limited detection area

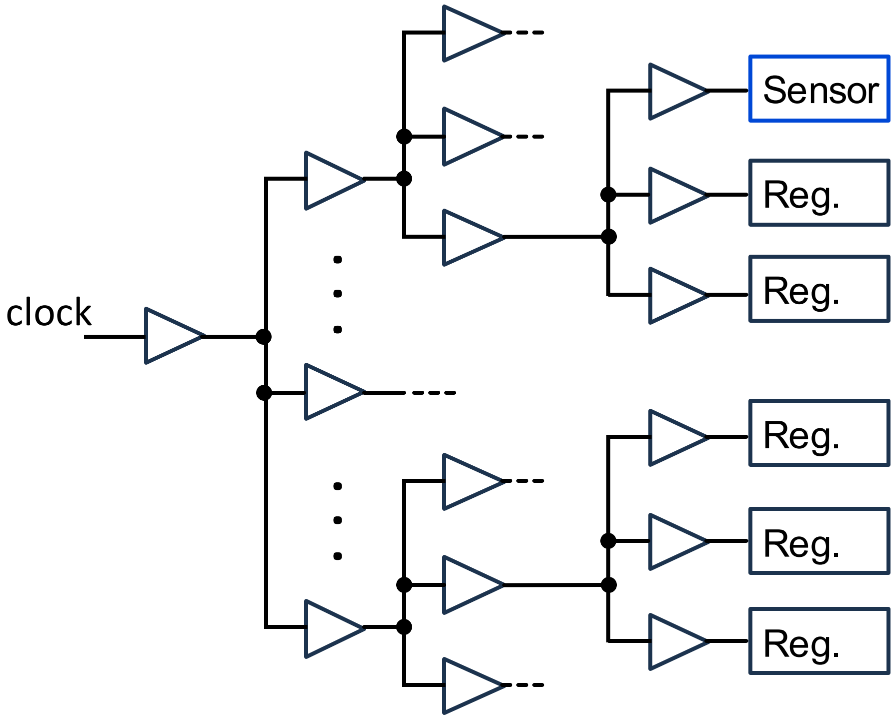
With 5-sensor configuration

Up to 10% of injected faults were undetected (depending of EMFI parameters)

L. Zussa, et al., Efficiency of a Glitch Detector against Electromagnetic Fault Injection, DATE 2014

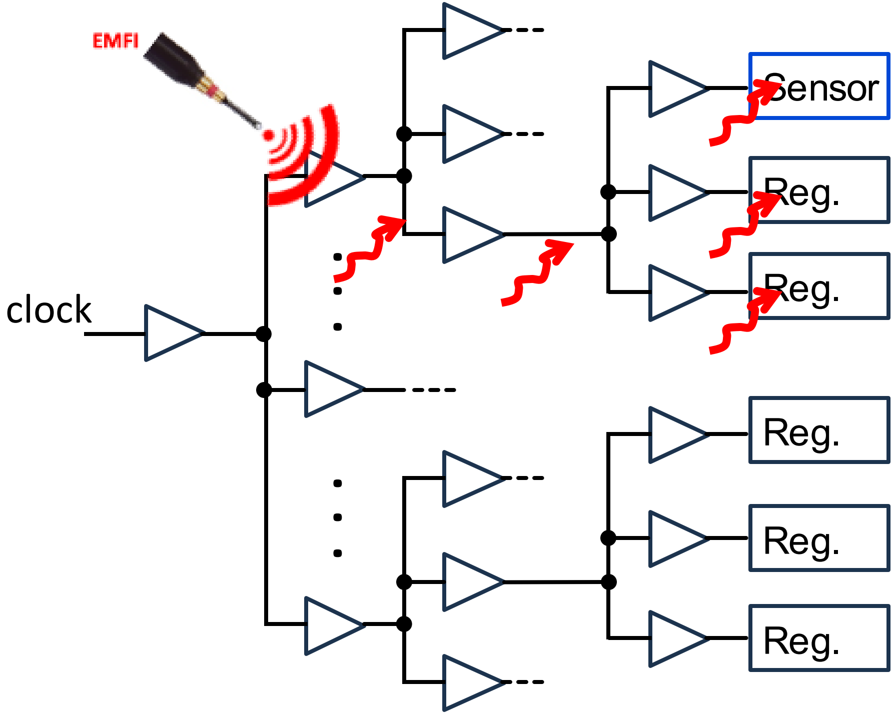
EMFI detection sensors

- Delay-based sensor – Weakness analysis (assumption)
  - ✓ EMFI-induced clock glitch propagation in clock network/tree



EMFI detection sensors

- Delay-based sensor – Weakness analysis (assumption)
  - ✓ EMFI-induced clock glitch propagation in clock network/tree

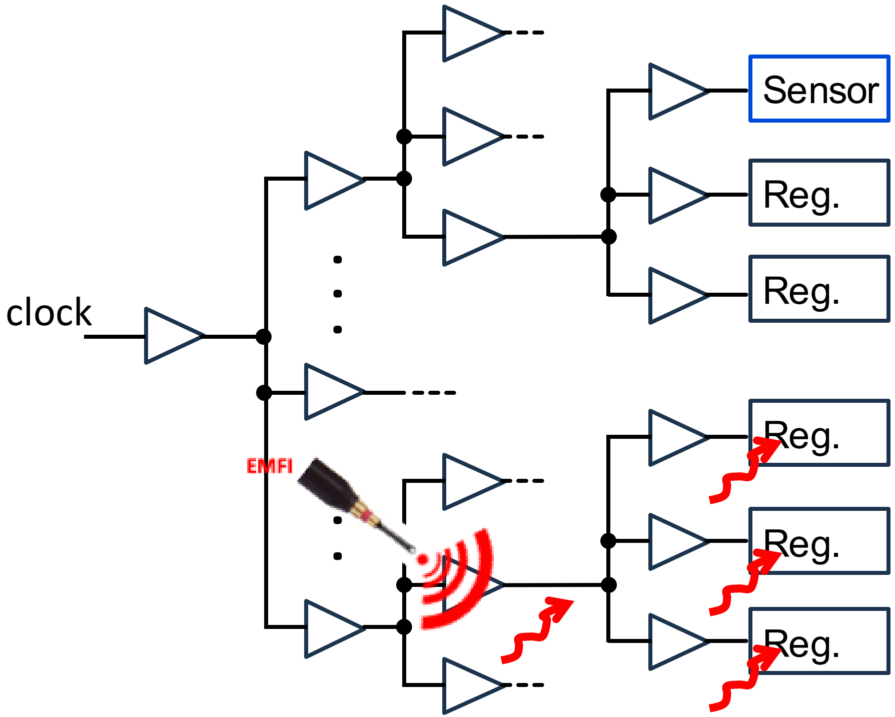


Clock path leading to a sensor

- Fault injection
- Fault Detection

EMFI detection sensors

- Delay-based sensor – Weakness analysis (assumption)
  - ✓ EMFI-induced clock glitch propagation in clock network/tree



Clock path leading to a sensor

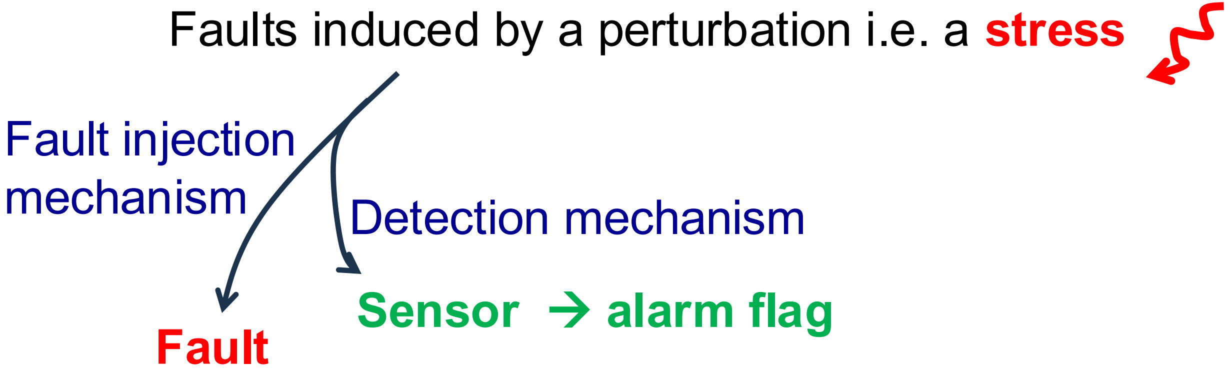
- Fault injection
- Fault Detection

Clock path with no sensor

- Fault injection
- Fault not detected

EMFI detection sensors

- Delay-based sensor
  - ✓ 100% effective to detect global T°, voltage and clock stresses



Faults induced by a perturbation i.e. a **stress**

Fault injection mechanism

Detection mechanism

Fault

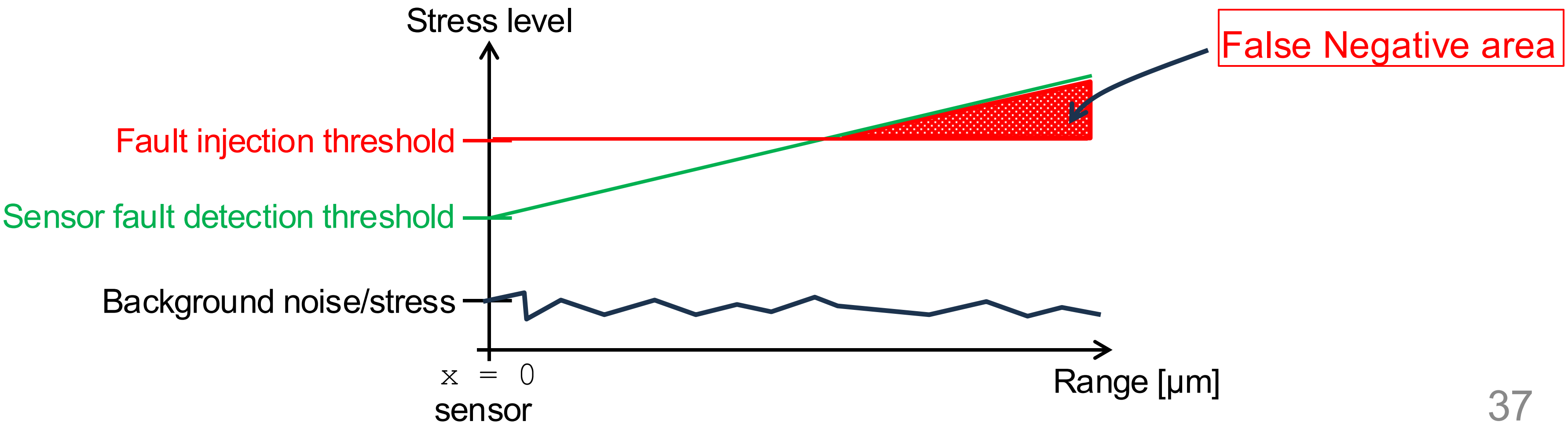
Sensor → alarm flag

⇨ Optimal efficiency when detection & fault injection mechanisms match

EMFI detection sensors

- Delay-based sensor
  - ✓ 100% effective to detect global T°, voltage and clock stresses
  - ✓ Limited detection range against EMFI – local stress
  - ✓ Not designed to detect LFI

- Sensor detection range



Monitoring FIA with Sensors – Lessons Learned

- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks

- EMFI detection sensors
    - EMFI mechanism
    - Delay-based sensor
    - DFF-based sensor
    - TDC-based sensor

- LFI detection sensors
- Conclusion

EMFI detection sensors

- DFF-based sensor (El Baze et al. 2016)

→ EMFI Sampling fault model

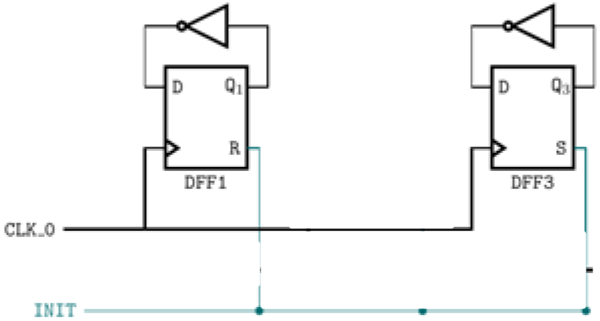
  - ✓ Faults are induced at sampling time
  - ✓ Recovery race between DFF input and clock signals

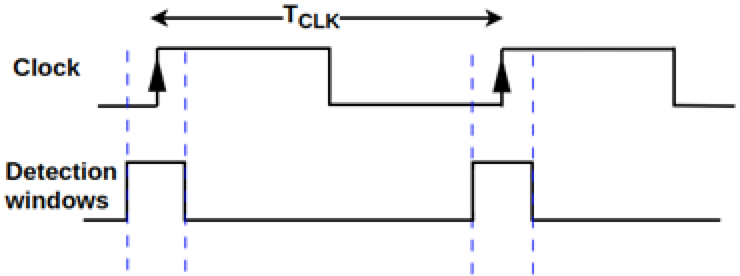
El Baze et al. A fully-digital EM pulse detector, DATE 2016
S. Ordas, et al., Electromagnetic fault injection: the curse of flip-flops, Journal of Cryptographic Engineering 2017

EMFI detection sensors

- DFF-based sensor – Design

→ Using toggling DFF to monitor and detect fault injection



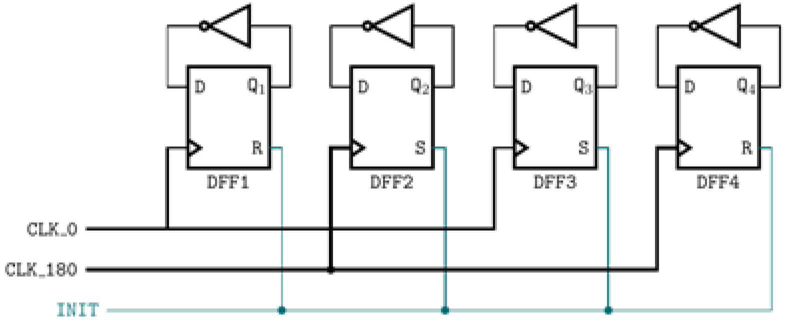


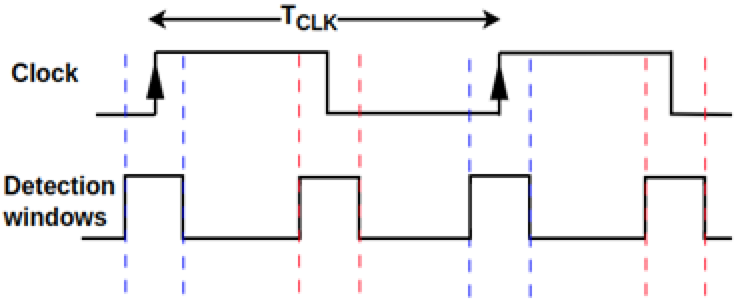
El Baze et al. A fully-digital EM pulse detector, DATE 2016

EMFI detection sensors

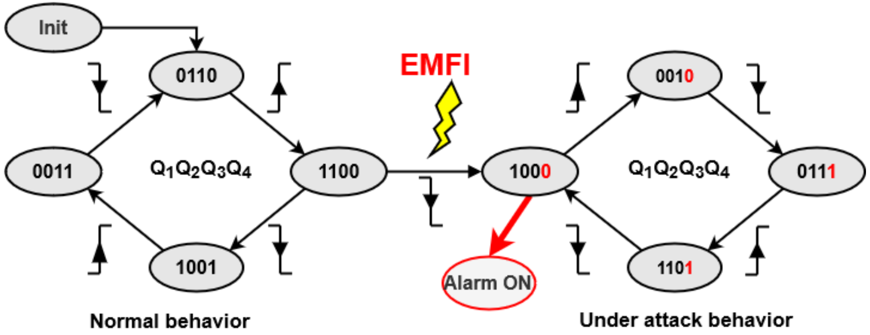
- DFF-based sensor – Design

→ Using toggling DFF to monitor and detect fault injection





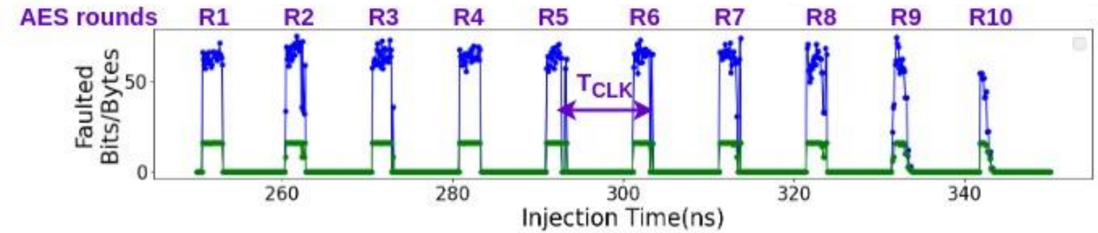
- Faulting a DFF modifies the toggling pattern → EMFI detection



El Baze et al. A fully-digital EM pulse detector, DATE 2016

EMFI detection sensors

- DFF-based sensor – Exp validation
  - ✓ EMFI test series on FPGA: AES (max. freq. 200 MHz) + sensors
  - ✓ At 100 MHz, 420V (Vpulse amplitude given as a measure of applied stress)

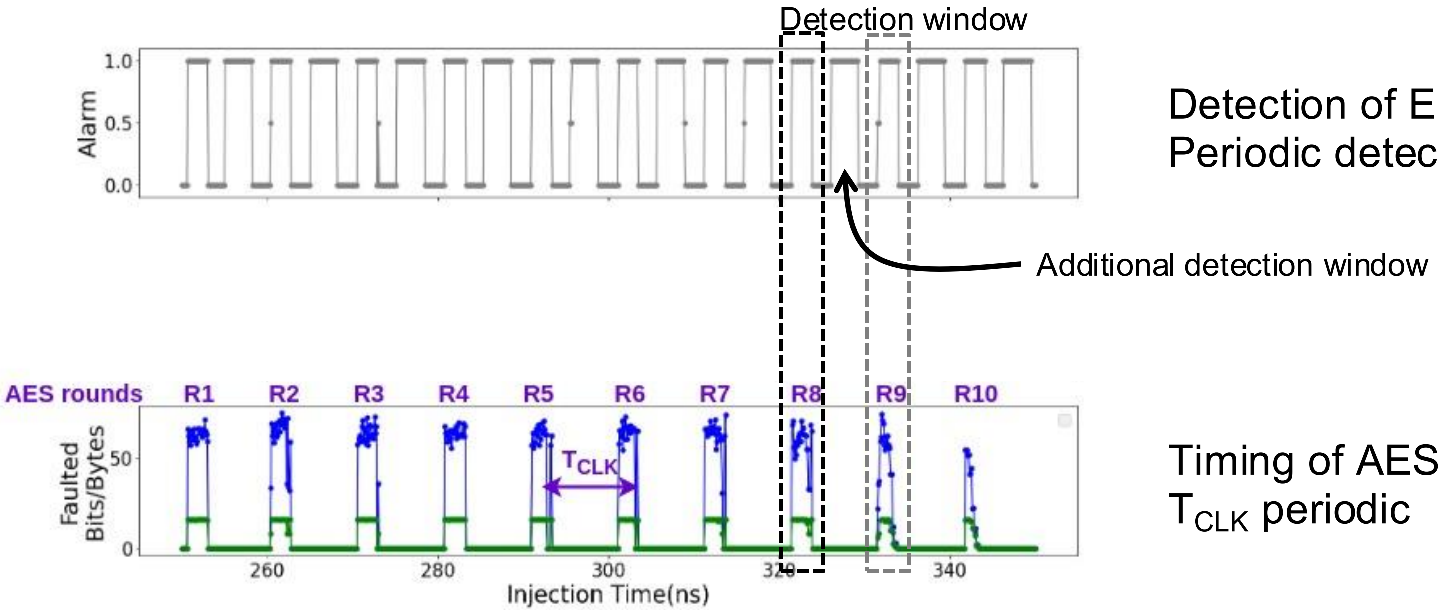


Timing of AES faults
T_{CLK} periodic

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

- DFF-based sensor – Exp validation
  - ✓ EMFI test series on FPGA: AES (max. freq. 200 MHz) + sensors
  - ✓ At 100 MHz, 420V (Vpulse amplitude given as a measure of applied stress)



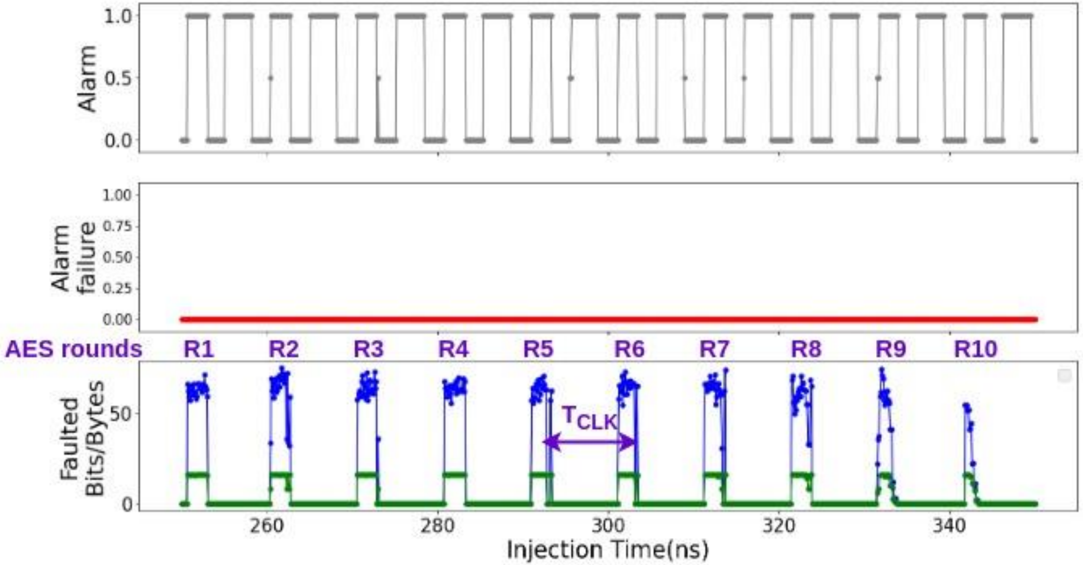
Detection of EMFI
Periodic detection windows

Timing of AES faults
T_{CLK} periodic

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

- DFF-based sensor – Exp validation
  - ✓ EMFI test series on FPGA: AES (max. freq. 200 MHz) + sensors
  - ✓ At 100 MHz, 420V (Vpulse amplitude given as a measure of applied stress)



Detection of EMFI
Periodic detection windows

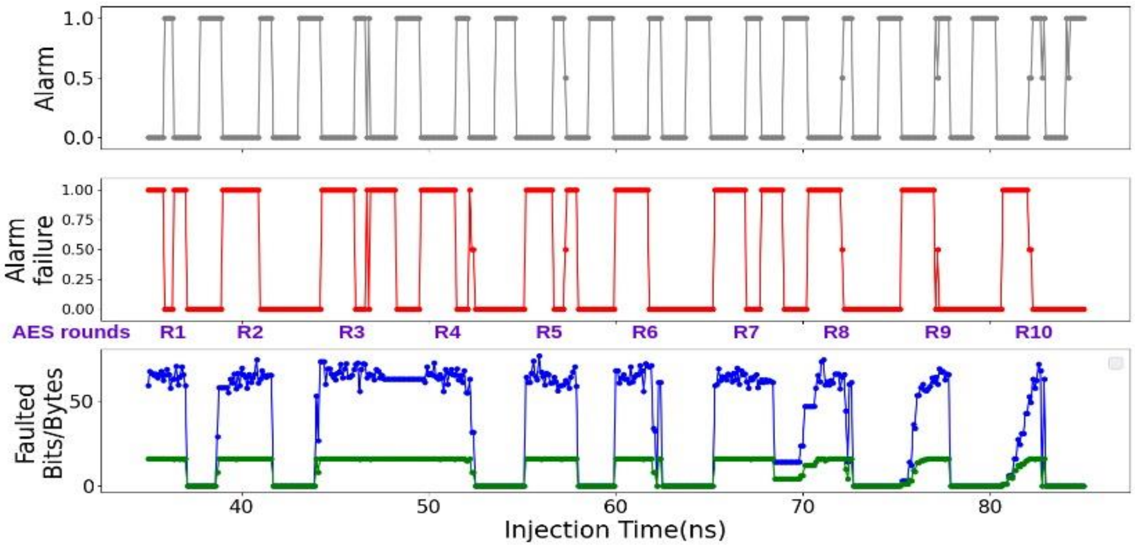
No alarm failure

Timing of AES faults
T_{CLK} periodic

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

- DFF-based sensor – Exp validation
  - ✓ EMFI test series on FPGA: AES (max. freq. 200 MHz) + sensors
  - ✓ At **200 MHz**, 420V (Vpulse amplitude given as a measure of applied stress)



Detection of EMFI

⇨ Undetected FIA

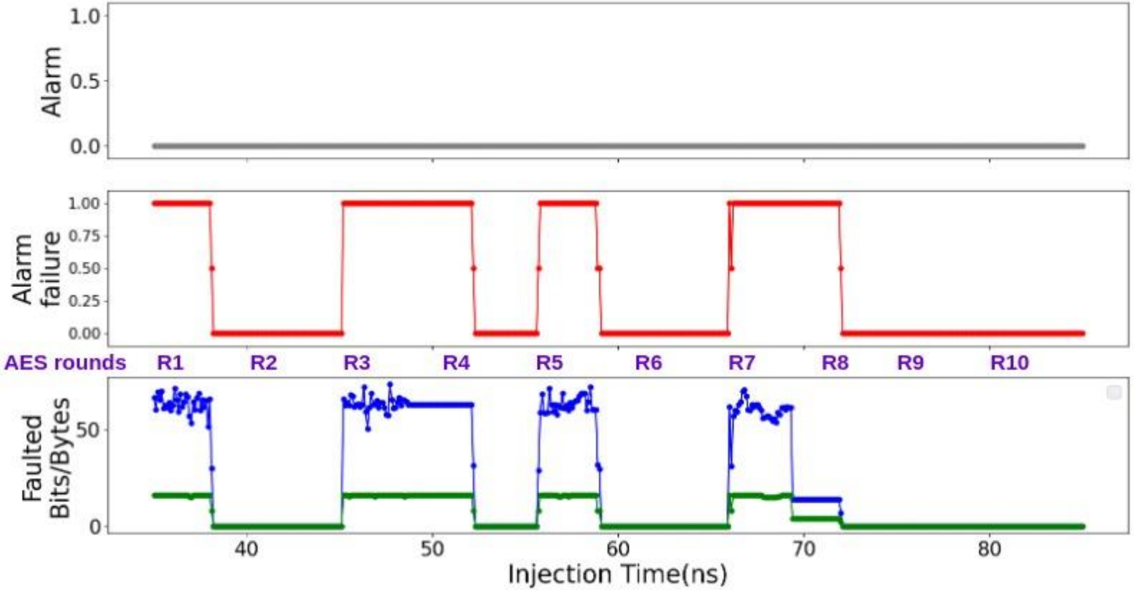
Timing of AES faults

Enlarged fault windows

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

- DFF-based sensor – Exp validation
  - ✓ EMFI test series on FPGA: AES (max. freq. 200 MHz) + sensors
  - ✓ At **200 MHz**, **350V** (Vpulse amplitude given as a measure of applied stress)



No detection of EMFI

Undetected FIA

Timing of AES faults

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

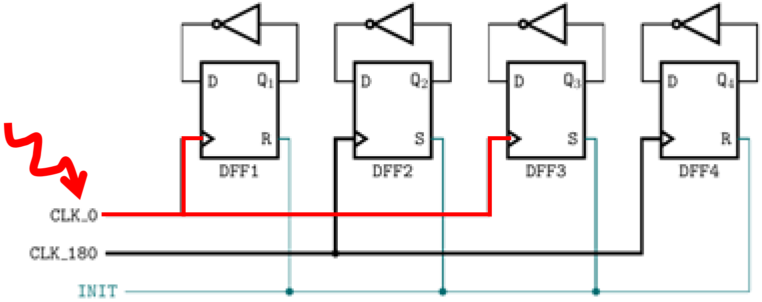
- DFF-based sensor – Analysis
  - ✓ EMFI at 420V → clock + voltage glitches
  - ✓ EMFI at 350V → voltage glitch only

EMFI detection sensors

- DFF-based sensor – Analysis
  - ✓ EMFI at 420V → clock + voltage glitches
  - ✓ EMFI at 350V → voltage glitch only

  - ✓ At 100 MHz, 420V → clock glitch induced faults → successful detection

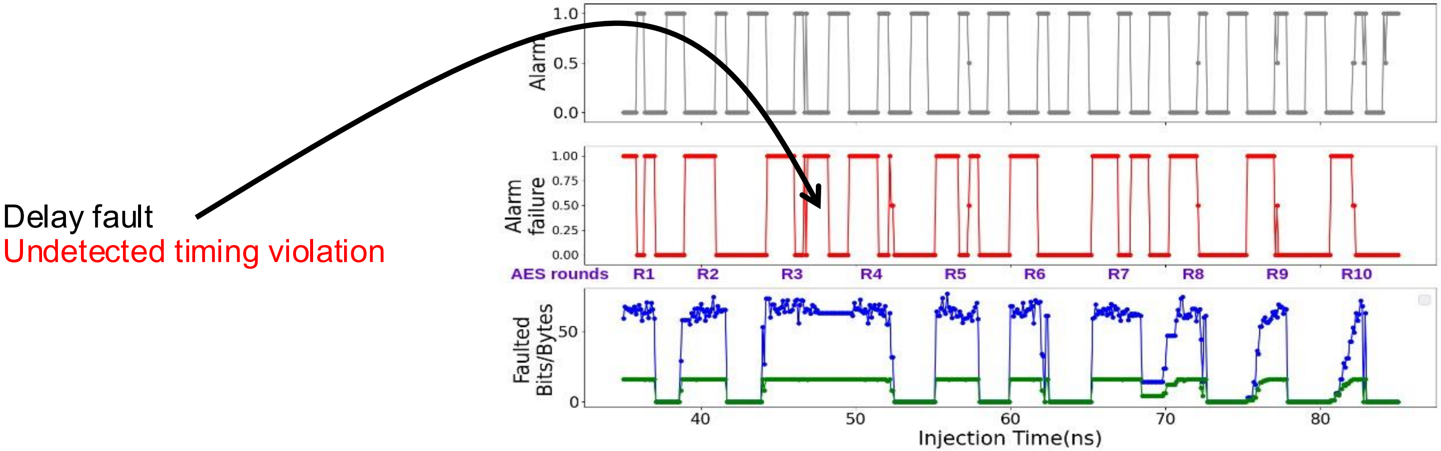
    Modification of DFFs toggling pattern



R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

- DFF-based sensor – Analysis
  - ✓ EMFI at 420V → clock + voltage glitches
  - ✓ EMFI at 350V → voltage glitch only
  - ✓ At **200 MHz**, 420V → clock + voltage glitches induced faults → partial EMFI detection
    Low slack



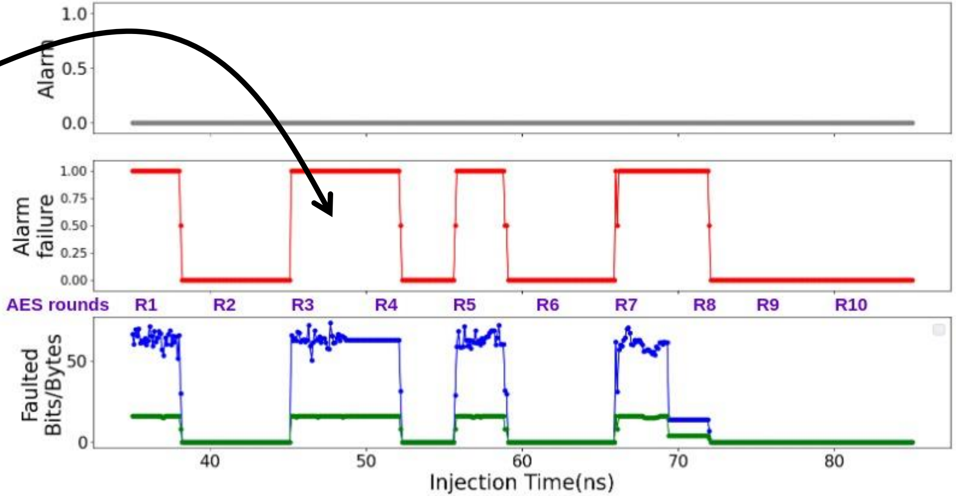
Delay fault
Undetected timing violation

R. Nabhan, Mitigation et compréhension de l'injection de fautes EMFI au moyen de capteurs numériques, PhD 2024

EMFI detection sensors

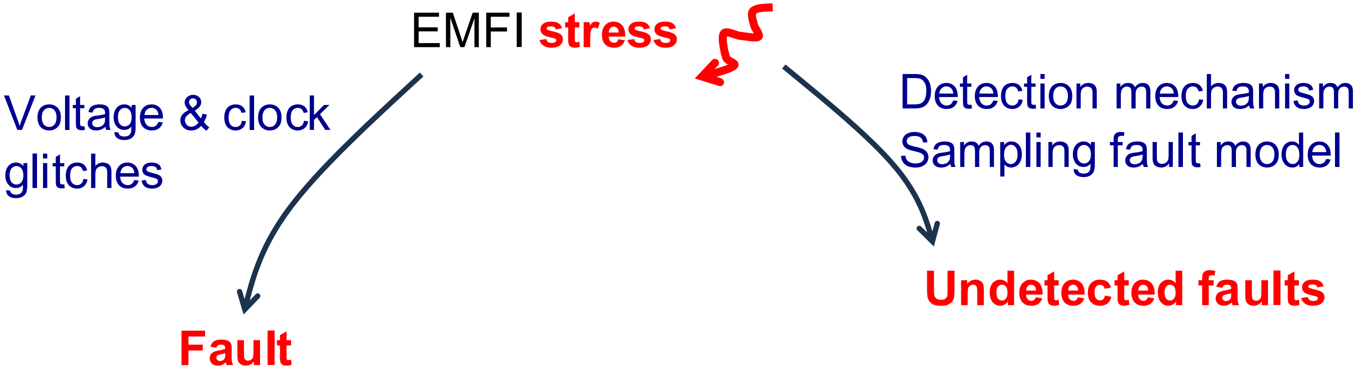
- DFF-based sensor – Analysis
  - ✓ EMFI at 420V → clock + voltage glitches
  - ✓ EMFI at 350V → voltage glitch only
  - ✓ At **200 MHz**, **350V** → voltage glitches induced faults → No EMFI detection
    Low slack

Delay fault
Undetected timing violation



EMFI detection sensors

- DFF-based sensor – Analysis
  - ✓ High risk of undetected faults when fault and detection mechanisms are different



EMFI **stress**

Voltage & clock glitches

Fault

Detection mechanism
Sampling fault model

Undetected faults

Monitoring FIA with Sensors – Lessons Learned

- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks

- EMFI detection sensors
  - EMFI mechanism
  - Delay-based sensor
  - DFF-based sensor
  - TDC-based sensor

- LFI detection sensors
- Conclusion

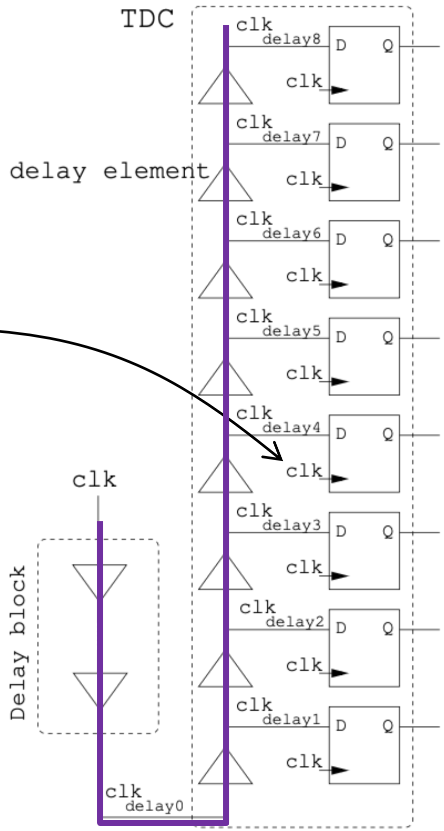
EMFI detection sensors

- TDC-based sensor – theory
  - ✓ Delay-based

→ Output: a digital image of the delay

Main clock

- ✓ Sampling clock of DFFs
- ✓ Delayed and sampled —



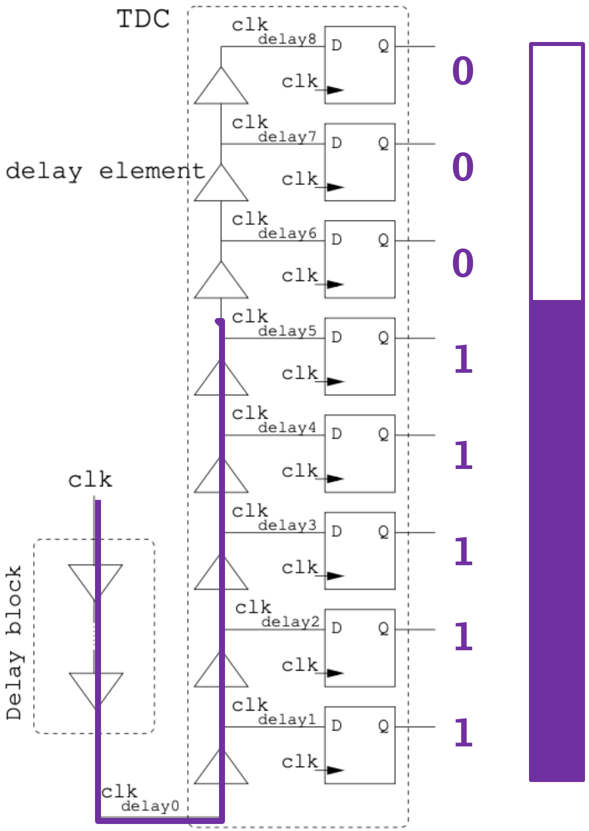
TDC = Time to Digital Converter

EMFI detection sensors

- TDC-based sensor – theory
  - ✓ Delay-based

→ Output: a digital image of the delay

  - ✓ Thermometer code



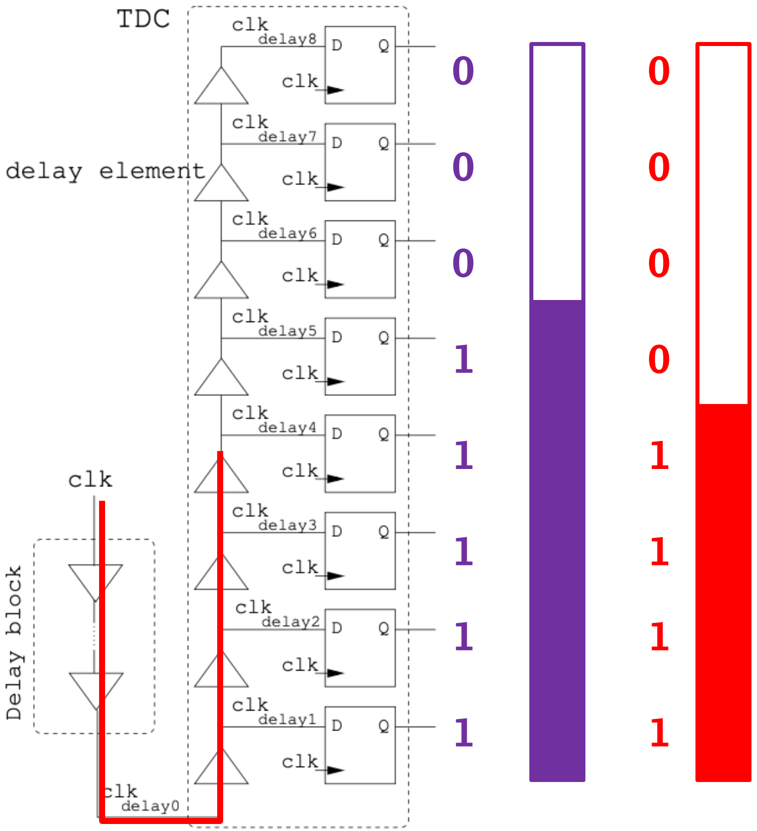
EMFI detection sensors

- TDC-based sensor – theory
  - ✓ Delay-based

→ Output: a digital image of the delay

  - ✓ Thermometer code

- EMFI-induced voltage glitch
  - ✓ Increased delay



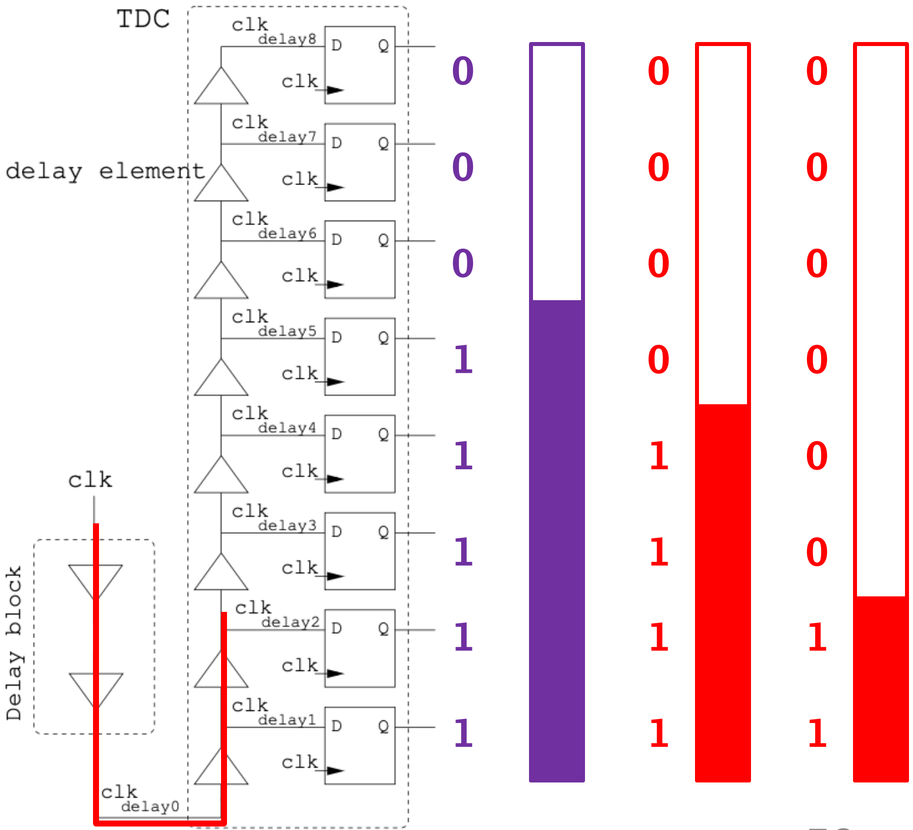
EMFI detection sensors

- TDC-based sensor – theory
  - ✓ Delay-based

→ Output: a digital image of the delay
  - ✓ Thermometer code

- EMFI-induced voltage glitch
  - ✓ Increased delay
- EMFI-induced clock glitch
  - ✓ Early sampling

⇨ EMFI detection through TDC output monitoring



EMFI detection sensors

- TDC-based sensor – Tested design
  - ✓ FPGA: AES + 3 TDC sensors

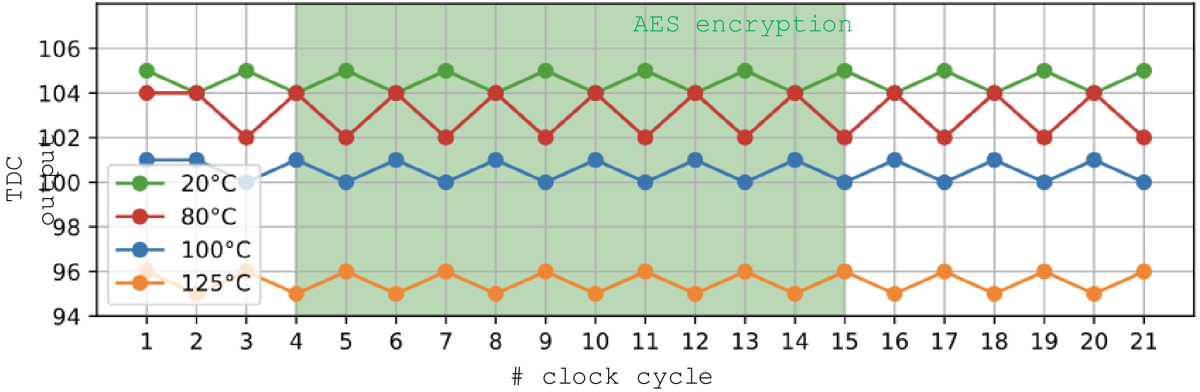
- Test of operating conditions
  - ✓ T° and voltage supply both affect the measured propagation delays

  → Relevant alarm triggering strategy?

R. Nabhan, et al., HEED: A Highly Efficient Electromagnetic Fault Detection Scheme, DATE 2026

EMFI detection sensors

- TDC-based sensor – Effect of temperature variations
  - ✓ TDC output on the -40°C – 140°C temperature range



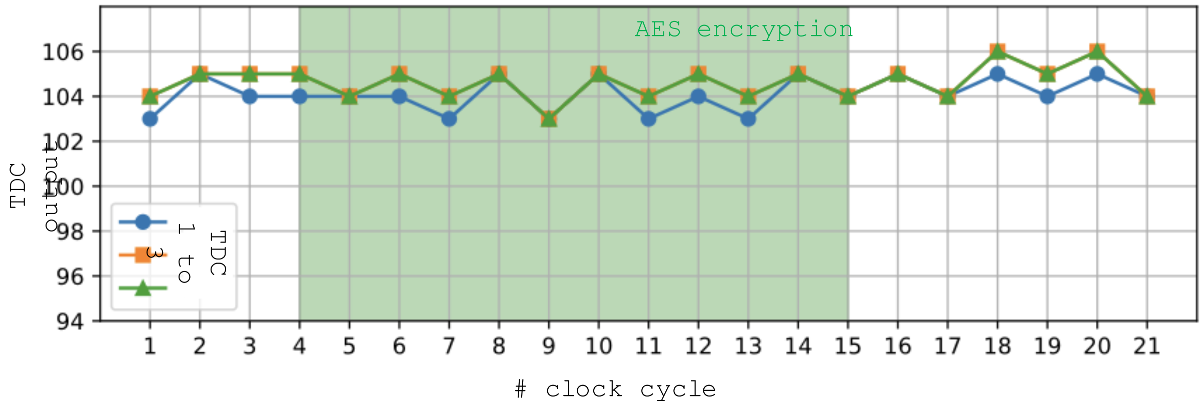
Thermal chamber

- TDC output
  - ✓ 104-106 at 20°C
  - ✓ 95-96 at 125°C

R. Nabhan, et al., HEED: A Highly Efficient Electromagnetic Fault Detection Scheme, DATE 2026

EMFI detection sensors

- TDC-based sensor – Effect of power supply noise
  - ✓ Dynamic noise generated by switching ON/OFF dedicated noise IPs

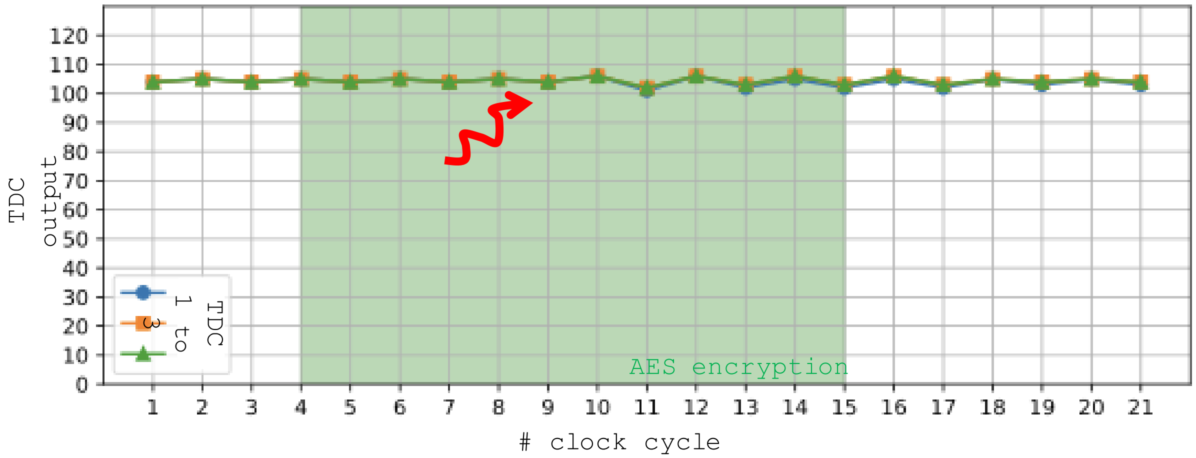


- TDC output variations (at room temperature)
  - ✓ $|\text{TDC Output}_n - \text{TDC Output}_{n-1}| \leq 2$

R. Nabhan, et al., HEED: A Highly Efficient Electromagnetic Fault Detection Scheme, DATE 2026

EMFI detection sensors

- TDC-based sensor – EMFI experiments
  - ✓ For EMFI parameters resulting in successful fault injection into the AES computations

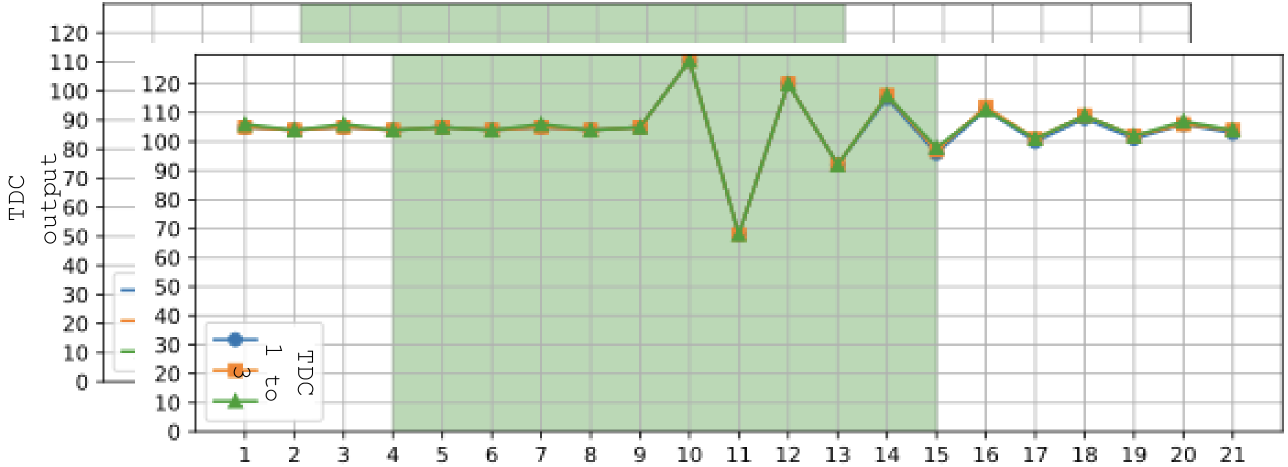


EMFI at the fault threshold

- TDC output variations leading to fault injection
  - ✓ $|\mathrm{TDC\ Output}_n - \mathrm{TDC\ Output}_{n-1}| \geq 3$

EMFI detection sensors

- TDC-based sensor – EMFI experiments
  - ✓ For EMFI parameters resulting in successful fault injection into the AES computations

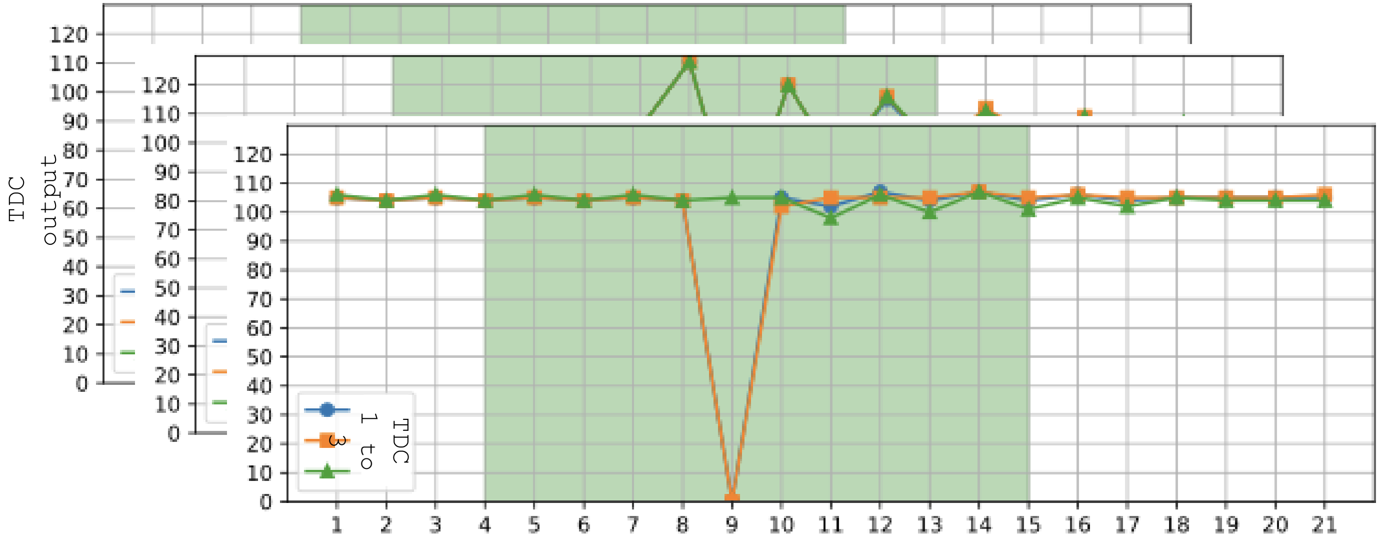


Strong EMFI

- TDC output variations leading to fault injection
  - ✓ $|\text{TDC Output}_n - \text{TDC Output}_{n-1}| \geq 3$

EMFI detection sensors

- TDC-based sensor – EMFI experiments
  - ✓ For EMFI parameters resulting in successful fault injection into the AES computations

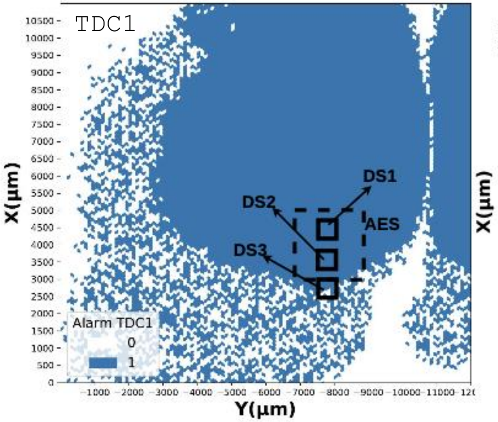


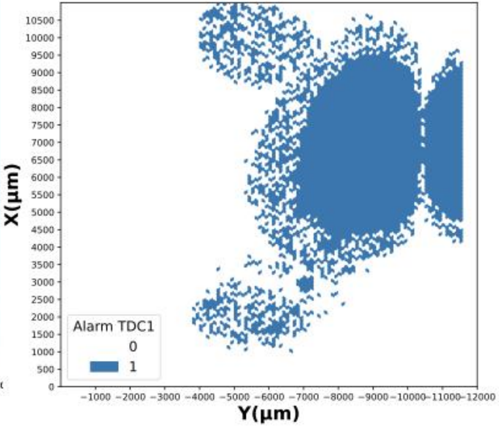
EMFI induced clock glitch

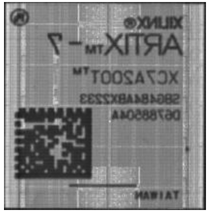
- TDC output variations leading to fault injection
  - ✓ $|\text{TDC Output}_n - \text{TDC Output}_{n-1}| \geq 3$

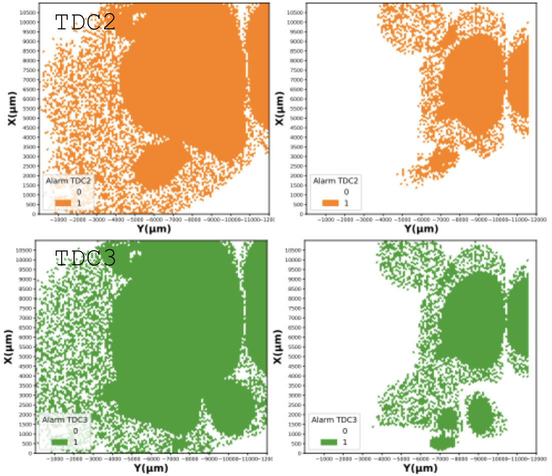
EMFI detection sensors

- TDC-based sensor – Detection strategy
  - ✓ Alarm triggered for $|\text{TDC Output}_n - \text{TDC Output}_{n-1}| > 2$
  - → 100% fault detection rate
  - → 1% False Positive (unwanted alarms due to noise ; 17 FP out of 1,650 tests)
- Large detection area – drawn for various EMFI parameters









R. Nabhan, et al., HEED: A Highly Efficient Electromagnetic Fault Detection Scheme, DATE 2026

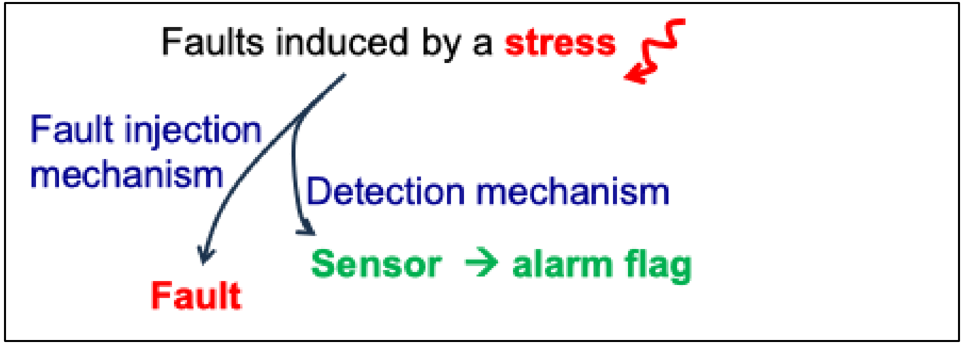
EMFI detection sensors

- Conclusion

✓ EMFI detection = still an open subject

✓ Exp. testing is mandatory (including at various nominal and stress conditions)

✓ Choose a detection mechanism matching the fault injection mechanism



Faults induced by a **stress**

Fault injection mechanism

Detection mechanism

Fault

Sensor → alarm flag

Monitoring FIA with Sensors – Lessons Learned

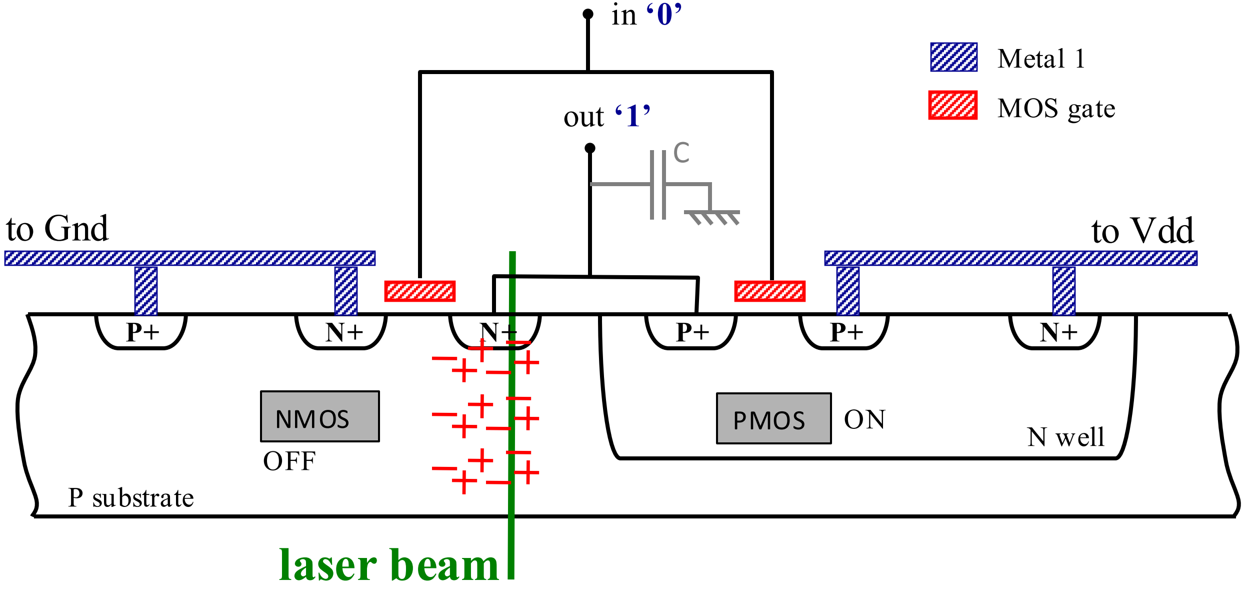
- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks
- EMFI detection sensors

- LFI detection sensors
  - LFI mechanism
  - TDC-based sensor
  - BBICS Bulk Built-In Current Sensor

- Conclusion

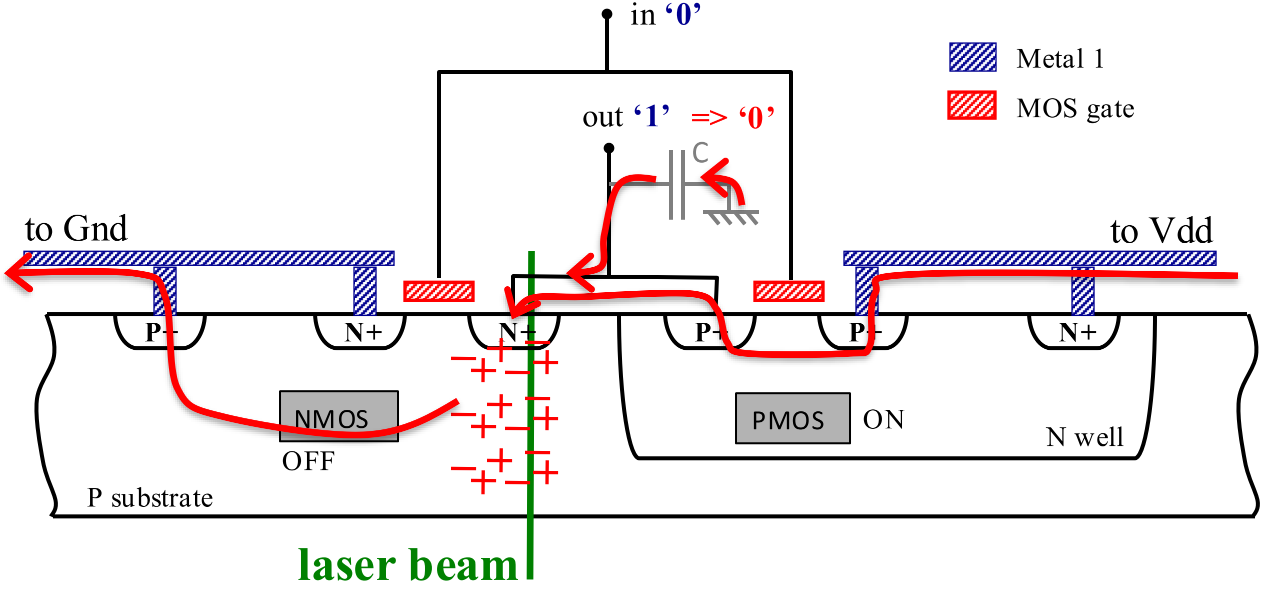
LFI detection sensors

- LFI mechanism – Laser induced photocurrent $(\lambda \leq 1{,}100\ nm)$
  - ✓ Inverter cross section



LFI detection sensors

- LFI mechanism – Laser-induced photocurrent $(\lambda \leq 1{,}100\ nm)$
  - ✓ Inverter cross section



⇨ Laser-induced I_{ph} ⇨ Logical faults

Monitoring FIA with Sensors – Lessons Learned

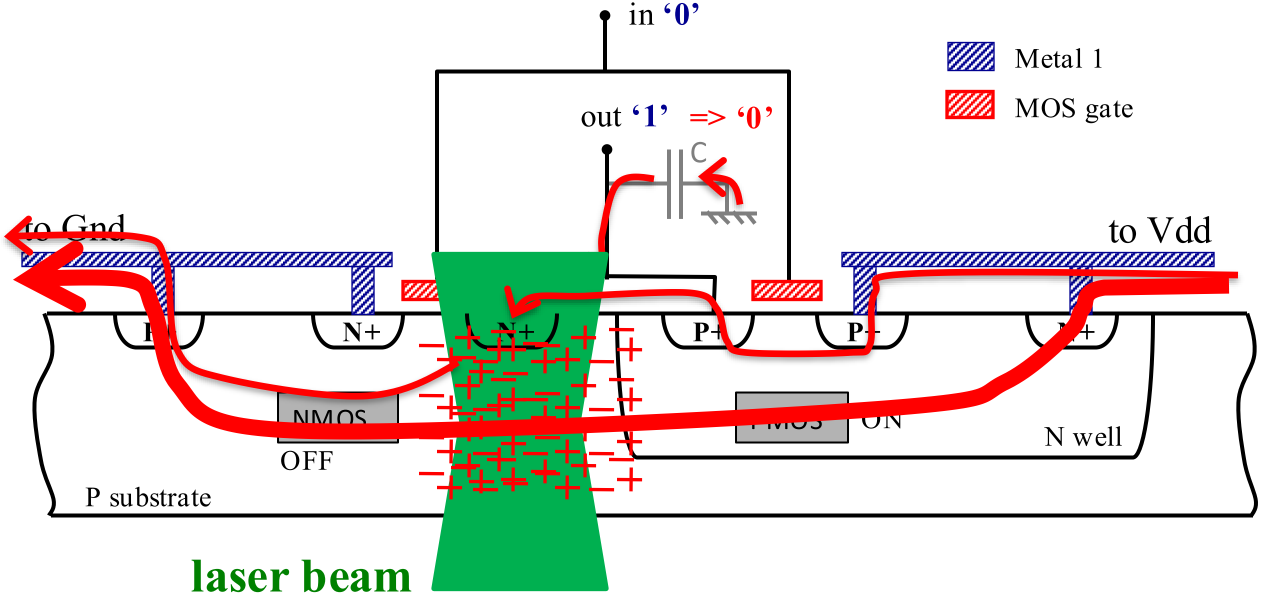
- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks
- EMFI detection sensors

- LFI detection sensors
  - LFI mechanism
  - TDC-based sensor
  - BBICS Bulk Built-In Current Sensor

- Conclusion

LFI detection sensors

- TDC-based sensor – Principle



Laser-induced Vdd to Gnd current (large)

⇩

IR-drop

⇩

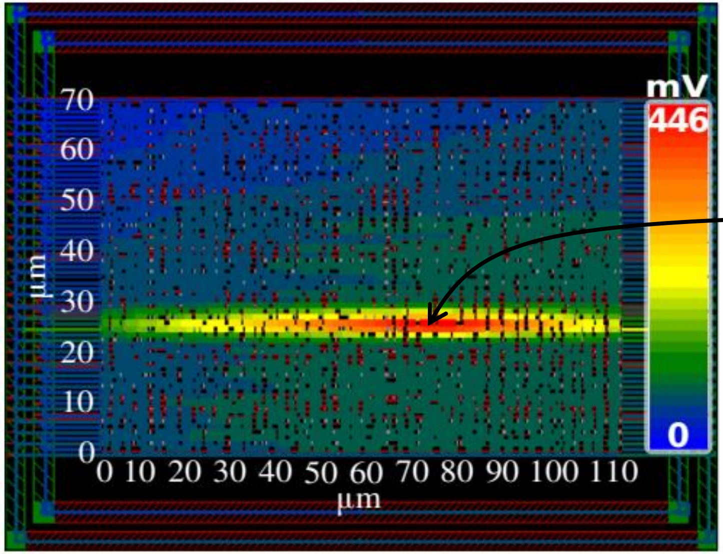
Increase of logic propagation times

⇩

Detection by TDC-based sensor

LFI detection sensors

- TDC-based sensor – Principle
  - ✓ Laser-induced IR-drop (simulation, 5 µm laser spot)
  - → Propagation of a significant IR-drop at a large distance

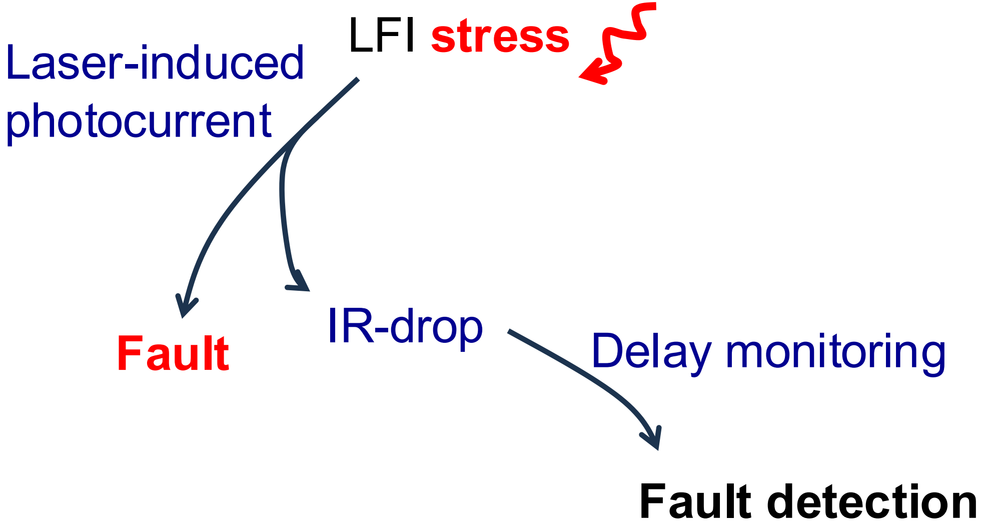


ARM7 CPU, CMOS 28nm, 5k+ gates

R. Viera et al., Simulation and experimental demonstration of the importance of IR-drops during laser fault-injection, IEEE TCAD 2019

LFI detection sensors

- TDC-based sensor – Universal fault detection sensor?
  - ✓ Ability to detect LFI/EMFI/voltage/temperature/frequency stress
  - ✓ Detection mechanism → 2-step mechanism



LFI **stress**

Laser-induced photocurrent

Fault

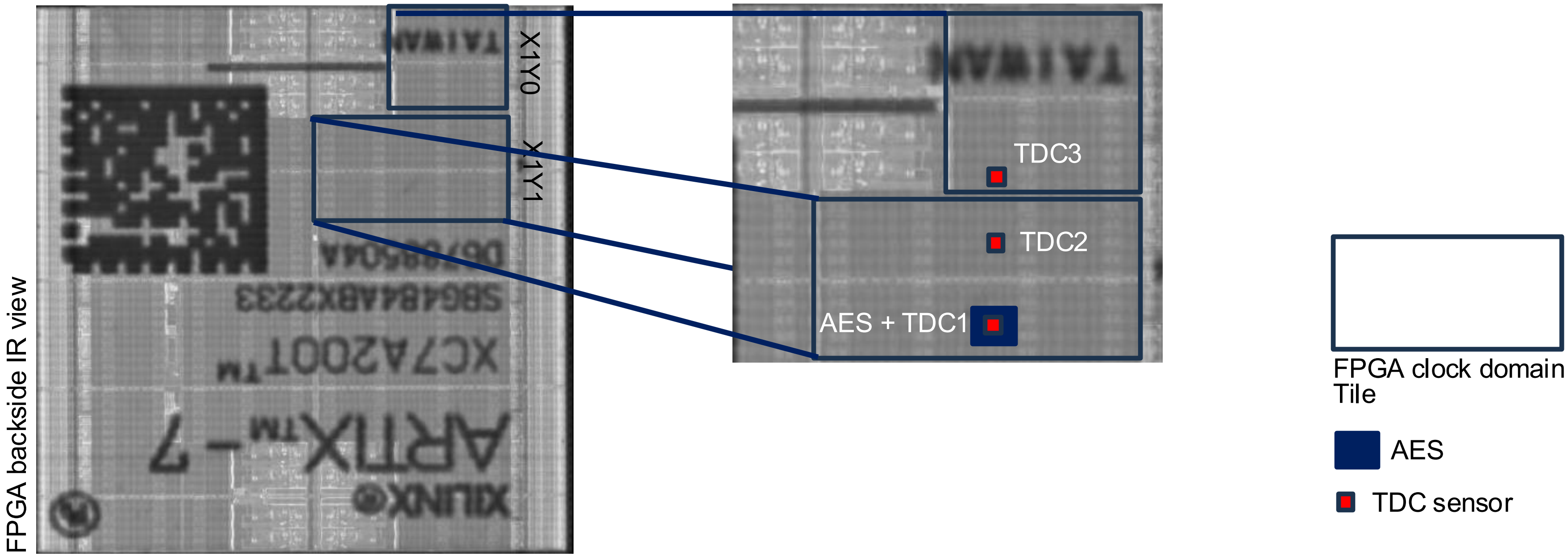
IR-drop

Delay monitoring

Fault detection

LFI detection sensors

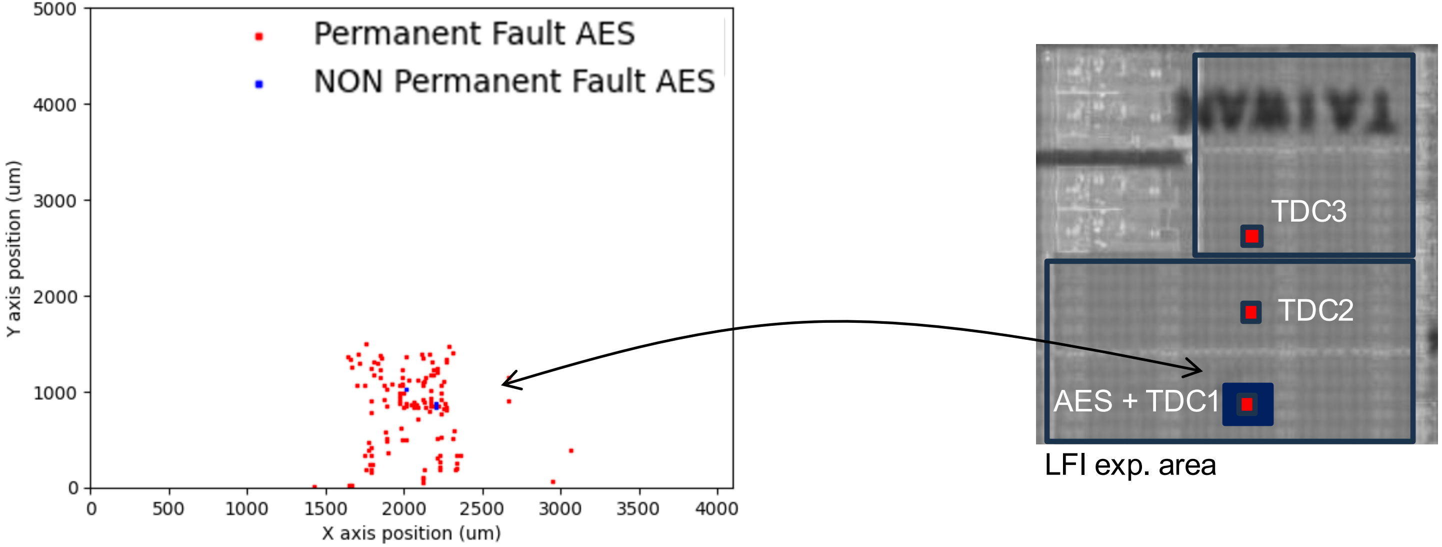
- TDC-based sensor – Tested design
  - ✓ FPGA: AES + 3 TDC sensors



M. Ebrahimabadi et al., Multi-Sensor Data Fusion for Enhanced Detection of Laser Fault Injection Attacks in Cryptographic Hardware: Practical Results, DATE 2025

LFI detection sensors

- TDC-based sensor – LFI experiments
  - ✓ Fault injection (AES)
  - ✓ Laser FI threshold 20 ns, 1.3 W, 5 µm ∅, 1,064nm

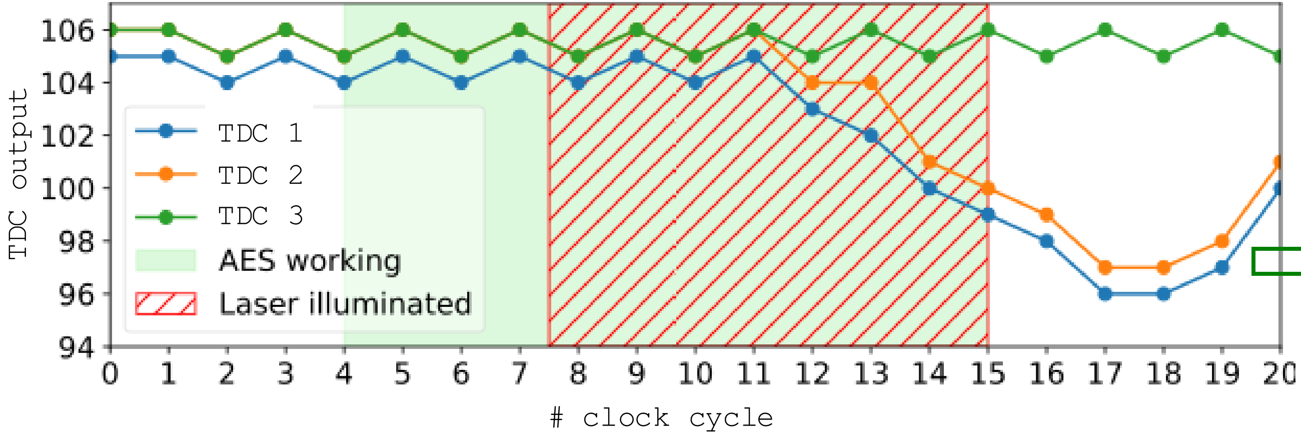


LFI exp. area

M. Ebrahimabadi et al., Multi-Sensor Data Fusion for Enhanced Detection of Laser Fault Injection Attacks in Cryptographic Hardware: Practical Results, DATE 2025

LFI detection sensors

- TDC-based sensor – LFI experiments
  - ✓ Fault Detection (TDC sensor)
  - ✓ Laser parameters 150 ns, 1.6 W, 5 µm ∅, on AES → significant effect on TDC 1 & 2

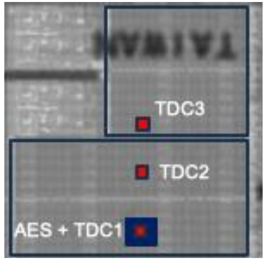


⇨ Fault detection

M. Ebrahimabadi et al., Multi-Sensor Data Fusion for Enhanced Detection of Laser Fault Injection Attacks in Cryptographic Hardware: Practical Results, DATE 2025

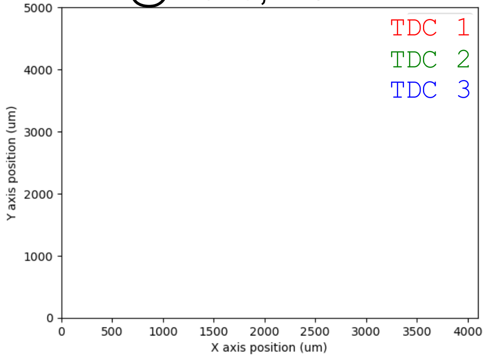
LFI detection sensors

- TDC-based sensor – LFI experiments
  - ✓ Fault Detection (all 3 TDC sensors)
  - → No LFI at 20ns laser pulse
  - → Good LFI detection at 150ns

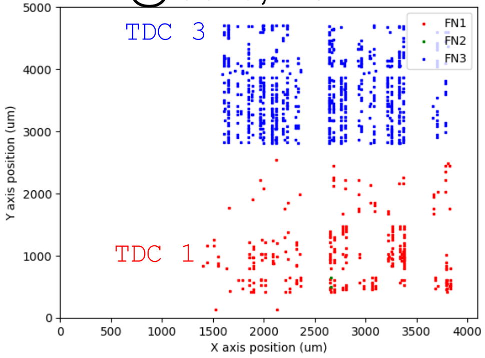


LFI exp. area

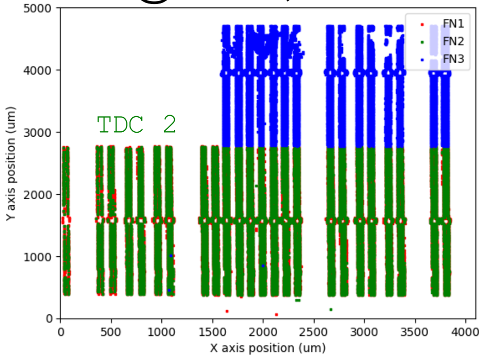
LFI @ 20ns, 1.3W



LFI @ 50ns, 1.3W



LFI @ 150ns, 1.3W

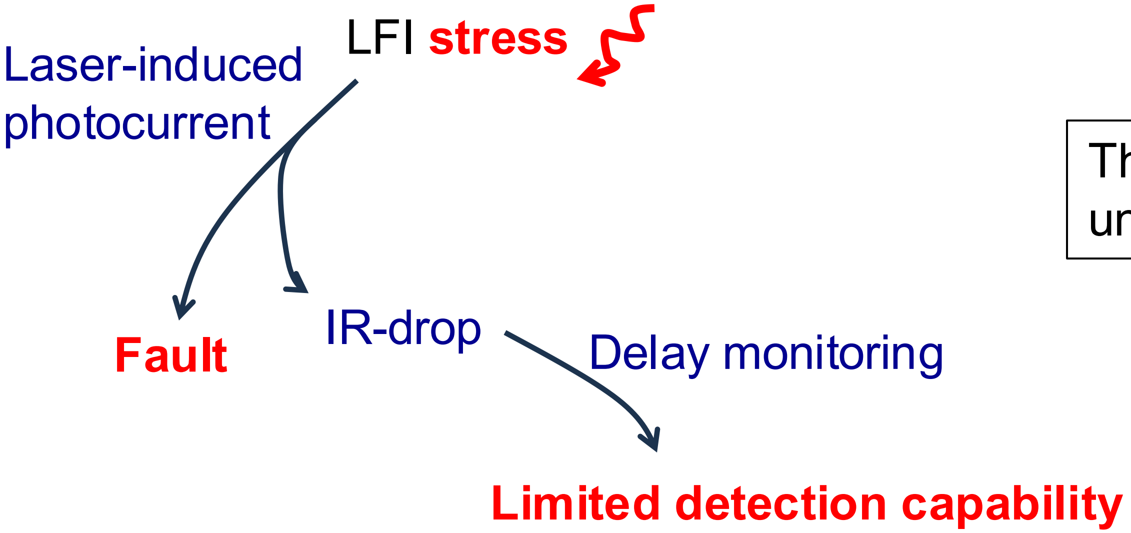


M. Ebrahimabadi et al., Multi-Sensor Data Fusion for Enhanced Detection of Laser Fault Injection Attacks in Cryptographic Hardware: Practical Results, DATE 2025

LFI detection sensors

- TDC-based sensor – Discussion
  - ✓ 75% detection rate at 150ns laser pulse duration (for AES transient faults)
  - ✓ 0% detection at 20ns,which is above the FI threshold

→ Using a 2-step detection mechanism limits sensor detection capability



This questions the idea of a universal sensor

Monitoring FIA with Sensors – Lessons Learned

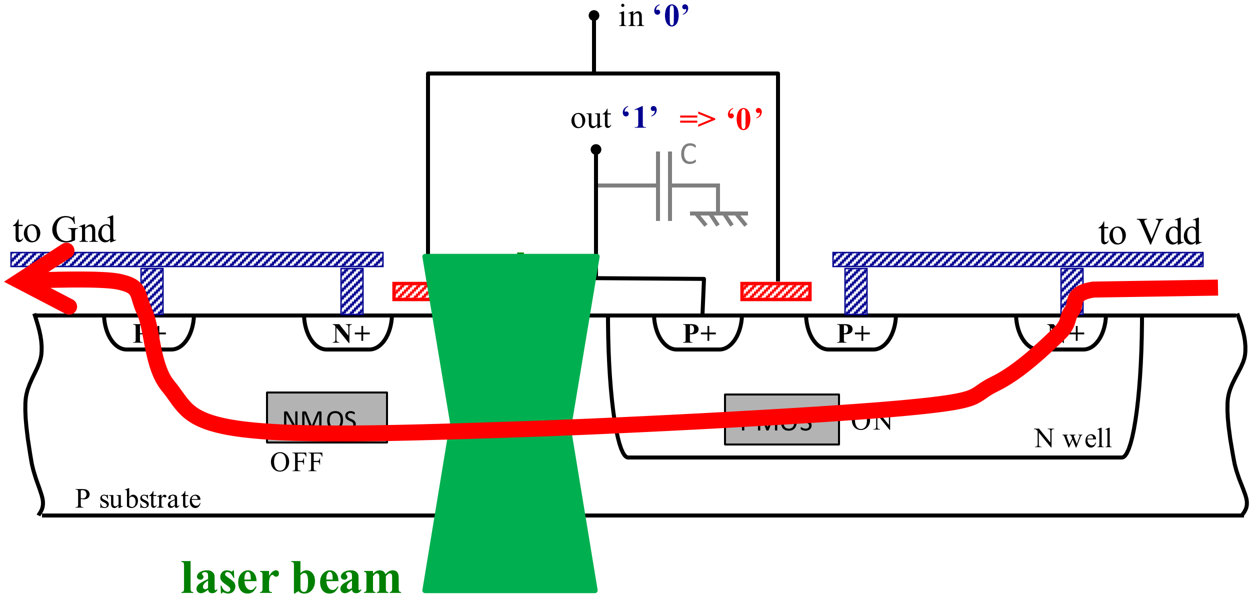
- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks
- EMFI detection sensors

- LFI detection sensors
  - LFI mechanism
  - TDC-based sensor
  - BBICS Bulk Built-In Current Sensor

- Conclusion

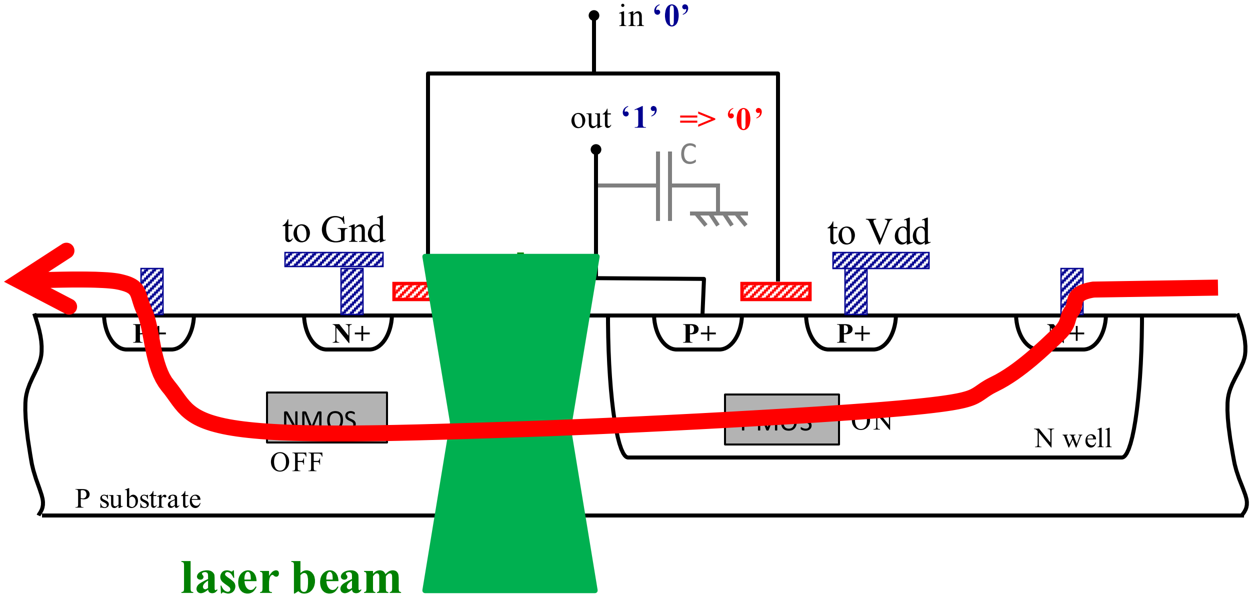
LFI detection sensors

- Bulk Built-In Current Sensor, BBICS – Principle
  - ✓ Monitoring of laser-induced bulk currents which is ~0 in nominal condition
  - ✓ Large Vdd to Gnd current component



LFI detection sensors

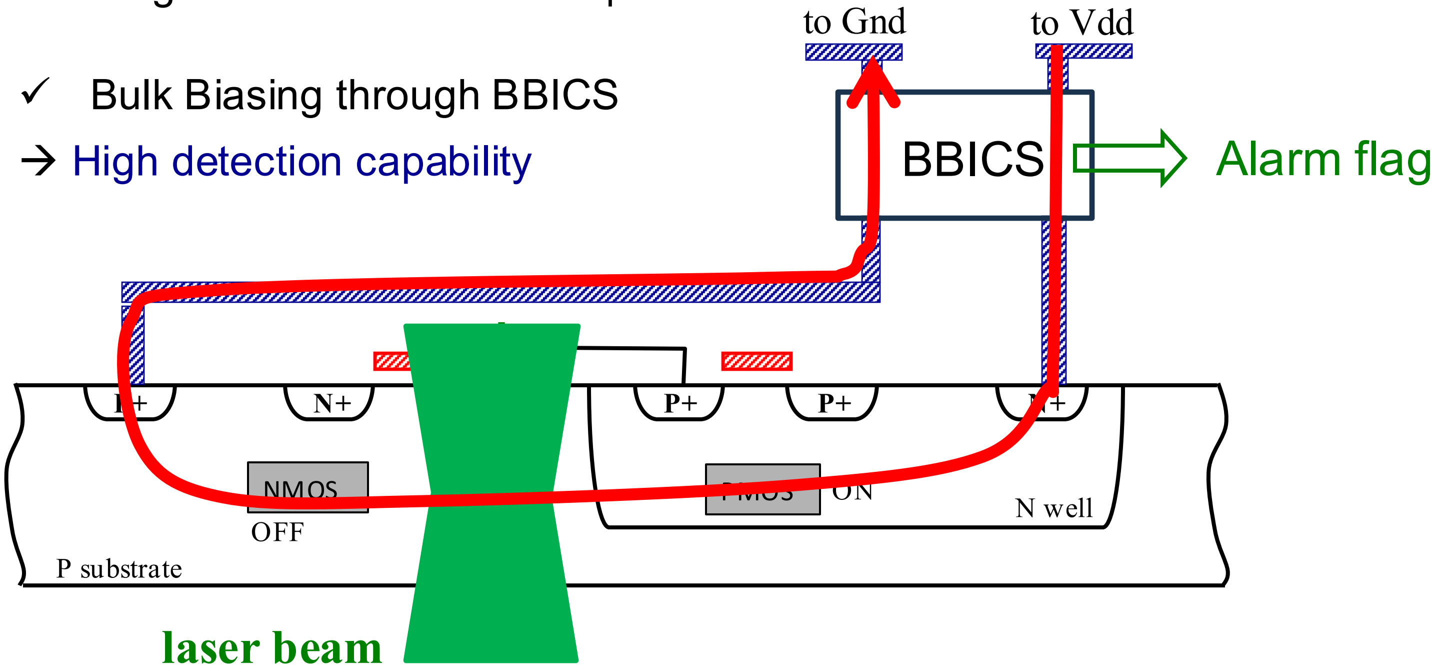
- Bulk Built-In Current Sensor, BBICS – Principle
  - ✓ Monitoring of laser-induced bulk currents which is ~0 in nominal condition
  - ✓ Large Vdd to Gnd current component



LFI detection sensors

- Bulk Built-In Current Sensor, BBICS – Principle
  - ✓ Monitoring of laser-induced bulk currents which is ~0 in nominal condition
  - ✓ Large Vdd to Gnd current component
  - ✓ Bulk Biasing through BBICS

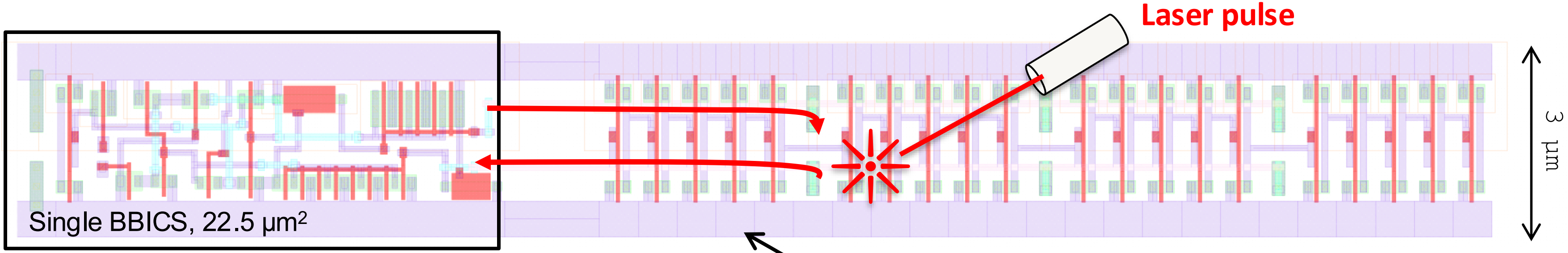
→ High detection capability

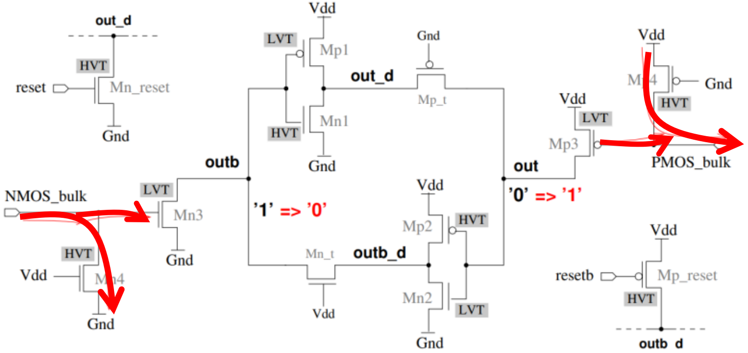


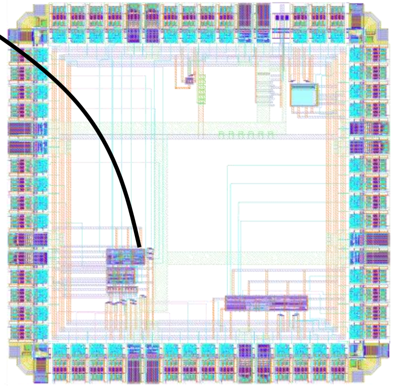
LFI detection sensors

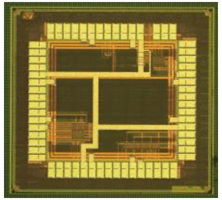
- BBICS – Tested design
  - ✓ ASIC CMOS 65 nm, several BBICS and logic blocks

Bulk laser-induced I_{PH}





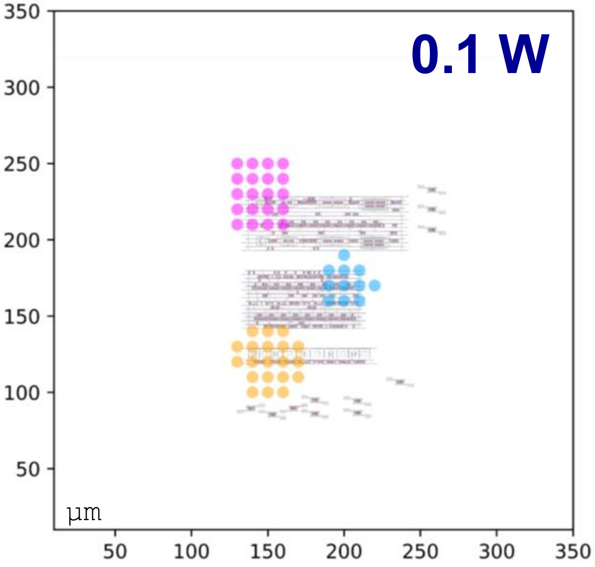


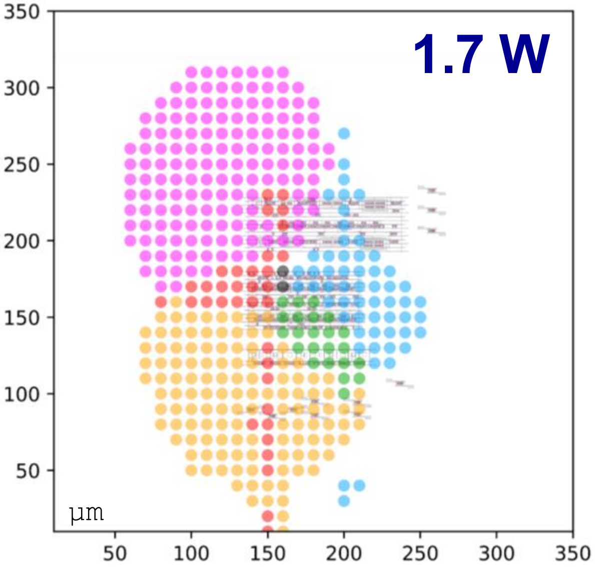


JM Dutertre et al., Improving the ability of bulk built-in current sensors to detect single event effects by using triple-well CMOS, MR 2014

LFI detection sensors

- BBICS – LFI exp.
  - ✓ Laser Fault Injection threshold: **1.9 W** at 50 ns, 5 µm Ø, 1,064 nm (DFF bit flip)
  - ✓ LFI detection 50 ns, 5 µm Ø, 1,064 nm





A. Guichaoua et al., Experimental Investigation of the pico-range LFI detection capabilities of Single Bulk Built-In Current Sensor, JAIF 2025

LFI detection sensors

- BBICS – LFI exp.
  - ✓ Laser Fault Injection threshold: **1.9 W** at 50 ns, 5 µm ∅, 1,064 nm (DFF bit flip)
  - ✓ LFI detection 50 ns, 1,064 nm

Laser spot diameter	Fault threshold	Detection area at FIA threshold	Detection area at half FIA threshold
5 µm	1.9 W	1,800 µm2 1.9W	950 µm2 0.95W
1 µm	1.7 W	900 µm2 1.7W	600 µm2 0.85W

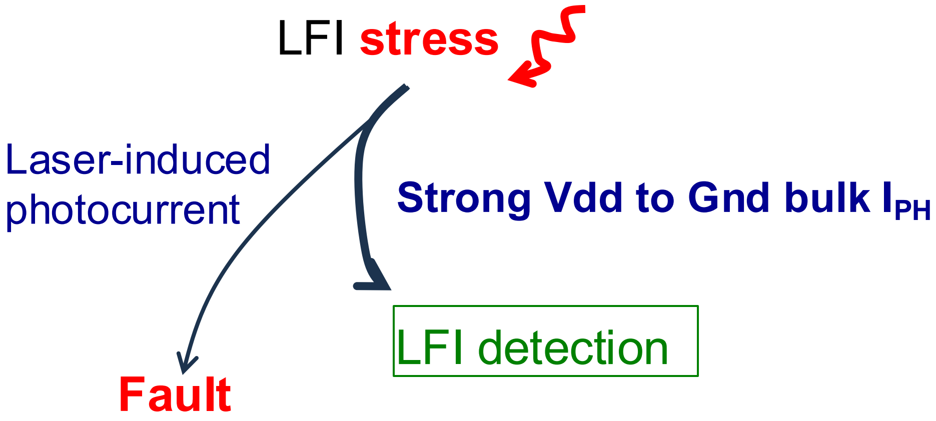
Single BBICS area 22.5 µm^2

A. Guichaoua et al., Experimental Investigation of the pico-range LFI detection capabilities of Single Bulk Built-In Current Sensor, JAIF 2025

LFI detection sensors

- BBICS – Discussion
  - ✓ Fully efficient at detecting LFI attacks
  - ✓ Based on a sound detection mechanism

Matsuda et al., A 286 f2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor, IEEE JSSC 2018



LFI **stress**

Laser-induced photocurrent

Strong Vdd to Gnd bulk I_{PH}

Fault

LFI detection

Monitoring FIA with Sensors – Lessons Learned

- Monitoring FIA with digital sensors – basics/principles
- Fault Injection Attacks
- EMFI detection sensors
- LFI detection sensors

- Conclusion

Monitoring FIA with Sensors – Lessons Learned

- Conclusion – A few advices

- Test, test, and test again
  - ✓ There is always something to be forgotten …

- Design a sensor with a detection mechanism matching that on the FIA it is supposed to detect
  - ✓ EMFI and LFI belongs to two distinct FIA families
  - ✓ There is (to date) no fully efficient universal detection sensor

Monitoring FIA with Sensors – Lessons Learned

- Conclusion – A few advices

- Delay-based sensors are good at monitoring stress-induced timing constraint violation
  - ✓ EMFI + T° stress + Voltage & clock glitches
- LFI detection sensors
  - ✓ BBICS work well
  - ✓ Delay-based sensors may miss many LFI

- FIA can be (very) efficiently monitored and detected
  - ✓ To be used as a 1st line of defense (no warranty of 100% efficiency)

Monitoring FIA with Sensors – Lessons Learned

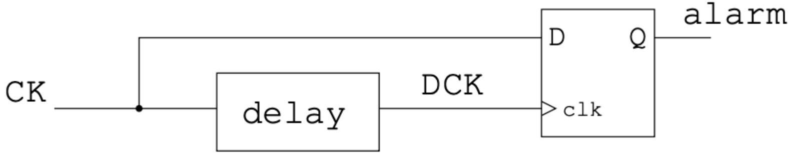
- Conclusion – One last warning

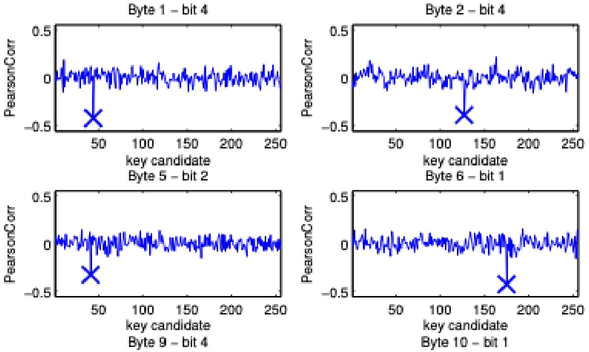
- Delay-based sensors are also used to conduct remote SCA attacks

→ J. Gravellier et al., Remote side-channel attacks on heterogeneous SoC, Cardis 2019

- Delay-based sensor successfully used to retrieve the secret key of the AES crypto-accelerator it was monitoring against FIA (FPGA)

→ L. Zussa, Evidence of an information leakage between logically independent blocks, CS2 2015





European Cyber Week

THE SOVEREIGN CYBER & DEFENCE AI FORUM

Contact:

dutertre@emse.fr

Institut Mines-Télécom

Equipe Commune Systèmes et Architectures Sécurisées
Mines Saint-Etienne, CEA, Leti, Centre CMP
13541 Gardanne FRANCE