
MINES Saint-Étienne

1816 2016

LIRMM

# An Embedded Digital Sensor Against EM and BB Fault Injection

David El-Baze, Jean-Baptiste Rigaud, Philippe Maurine

INSPIRING INNOVATION SINCE 1816

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Agenda

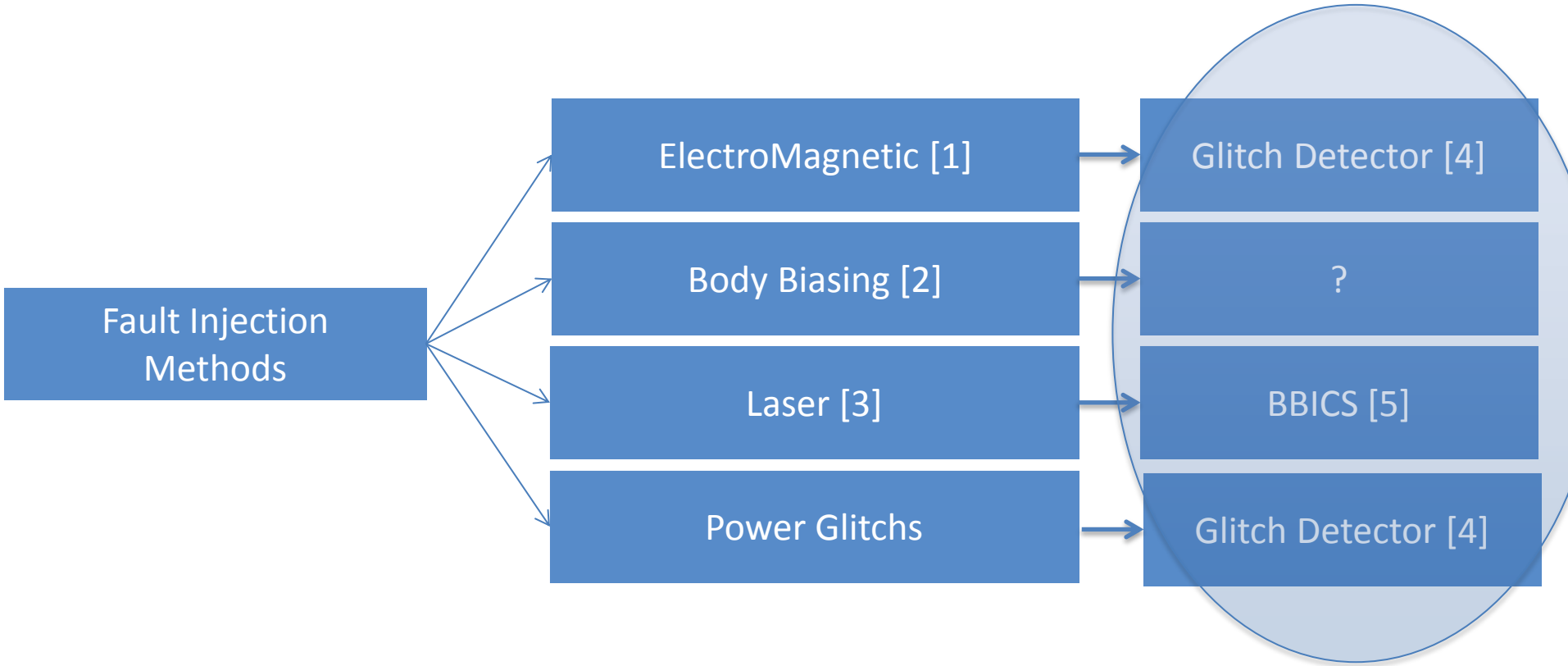
- **Context**

- Fault Model
- Detector Design
- EM and BB Detection Results
- Optimisation

- Next Steps
- Conclusion

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Context




[1] A. Dehbaoui et al. Injection of transient faults using electromagnetic pulses - Practical results on a cryptographic system, IACR 2012
[2] K. Tobich et al. Yet Another Fault Injection Technique: by Forward Body Biasing Injection
[3] S. P. Skorobogatov et R. J. Anderson Optical fault induction attacks, CHES 2002
[4] L. Zussa et al. "Efficiency of a glitch detector against electromagnetic fault injection," in Proceedings of DATE 2014
[5] Possamai Bastos et al. A bulk built-in sensor for detection of fault attacks. In *HOST 2013*

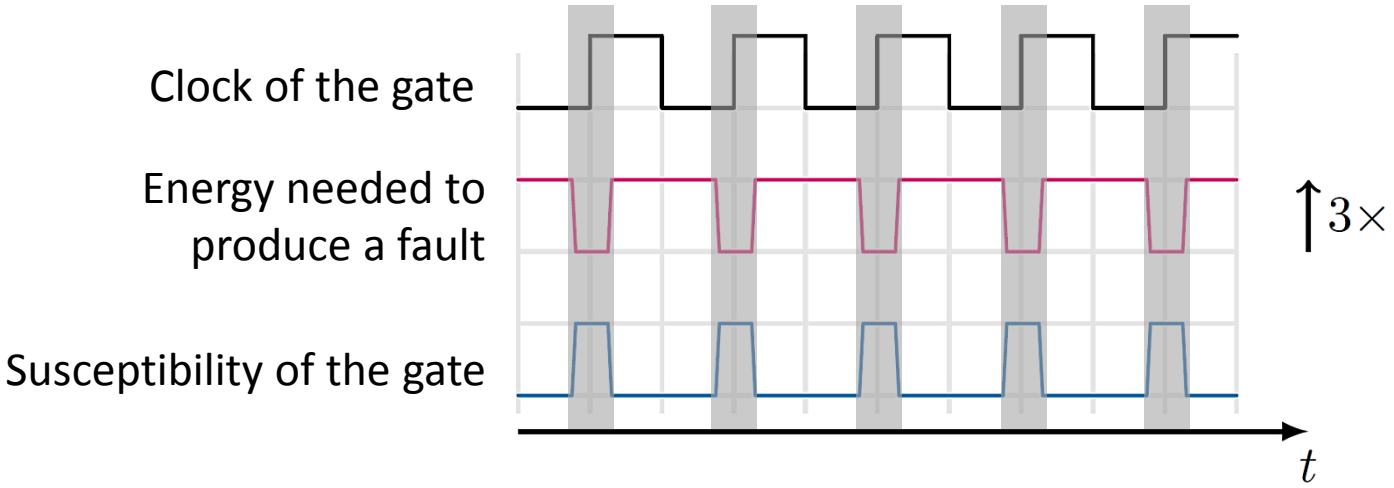
MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Agenda

- **Context**
- **Fault Model**
- **Detector Design**
- **EM and BB Detection Results**
- **Optimisation**
- **Next Steps**
- **Conclusion**

# Fault Model

- D-type Flip Flops are one of the most sensitive gates against ElectroMagnetic Attacks [6]



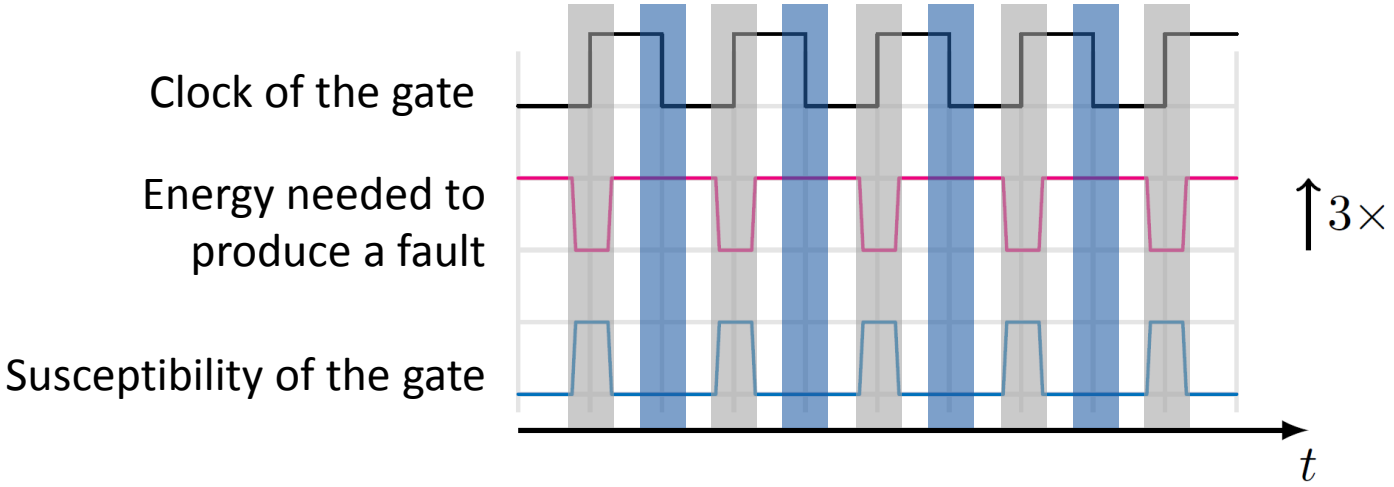

Windows where D-type Flip Flop are the most sensitive.

[6] S. Ordas, CARDIS 2014, PHISIC 2015, FDTC 2015

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Fault Model

- D-type Flip Flops are one of the most sensitive gates against ElectroMagnetic Attacks [6]




Windows where DFF of the detector are the most sensitive.

Windows where DFF of the protected circuit are the most sensitive.

[6] S. Ordas, CARDIS 2014, PHISIC 2015, FDTC 2015

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Agenda

- **Context**

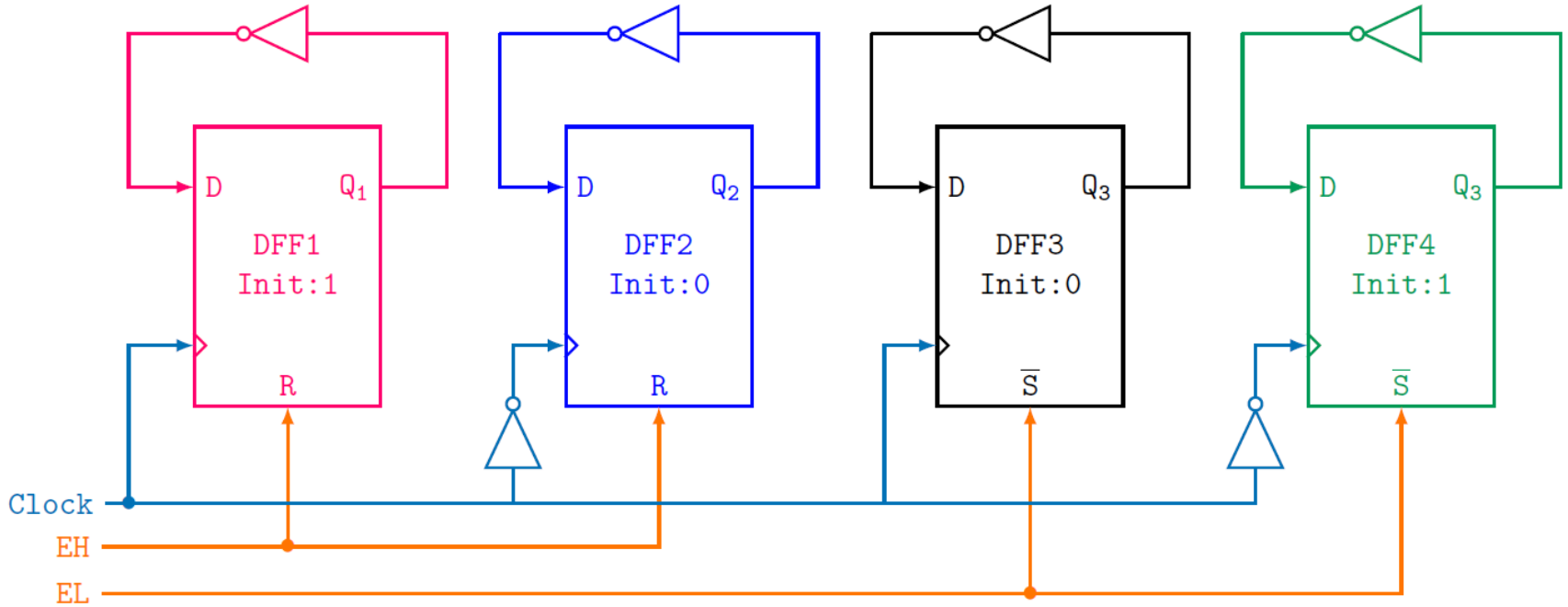
- **Fault Model**
- **Detector Design**
- **EM and BB Detection Results**
- **Optimisation**

- **Next Steps**
- **Conclusion**

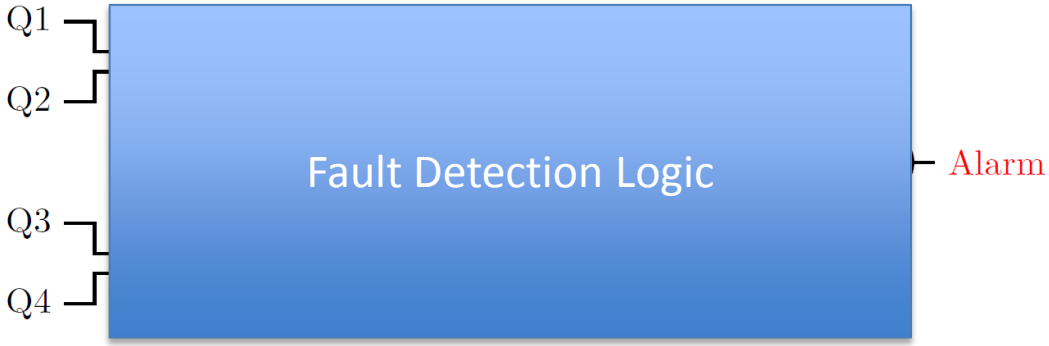
# Detector 1/2

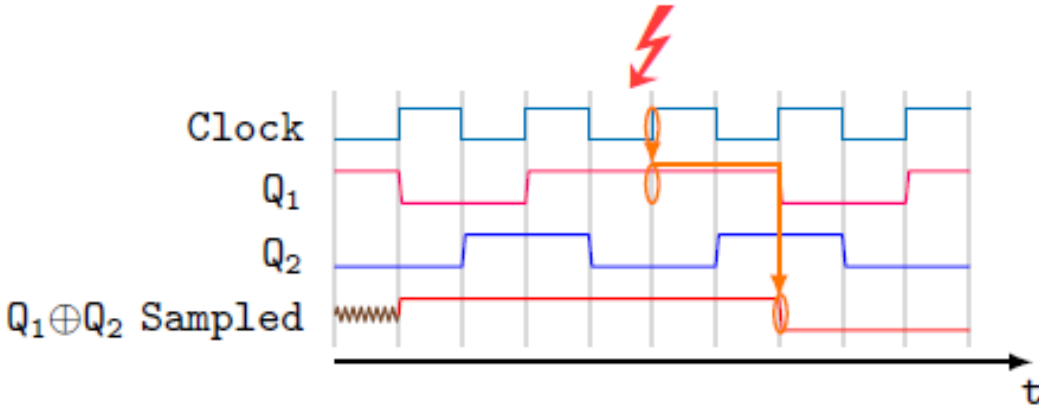
- 4 self looped DFFs
- Specific initialisation values
- A set and a reset network

Cover all the transitions and phase opposition



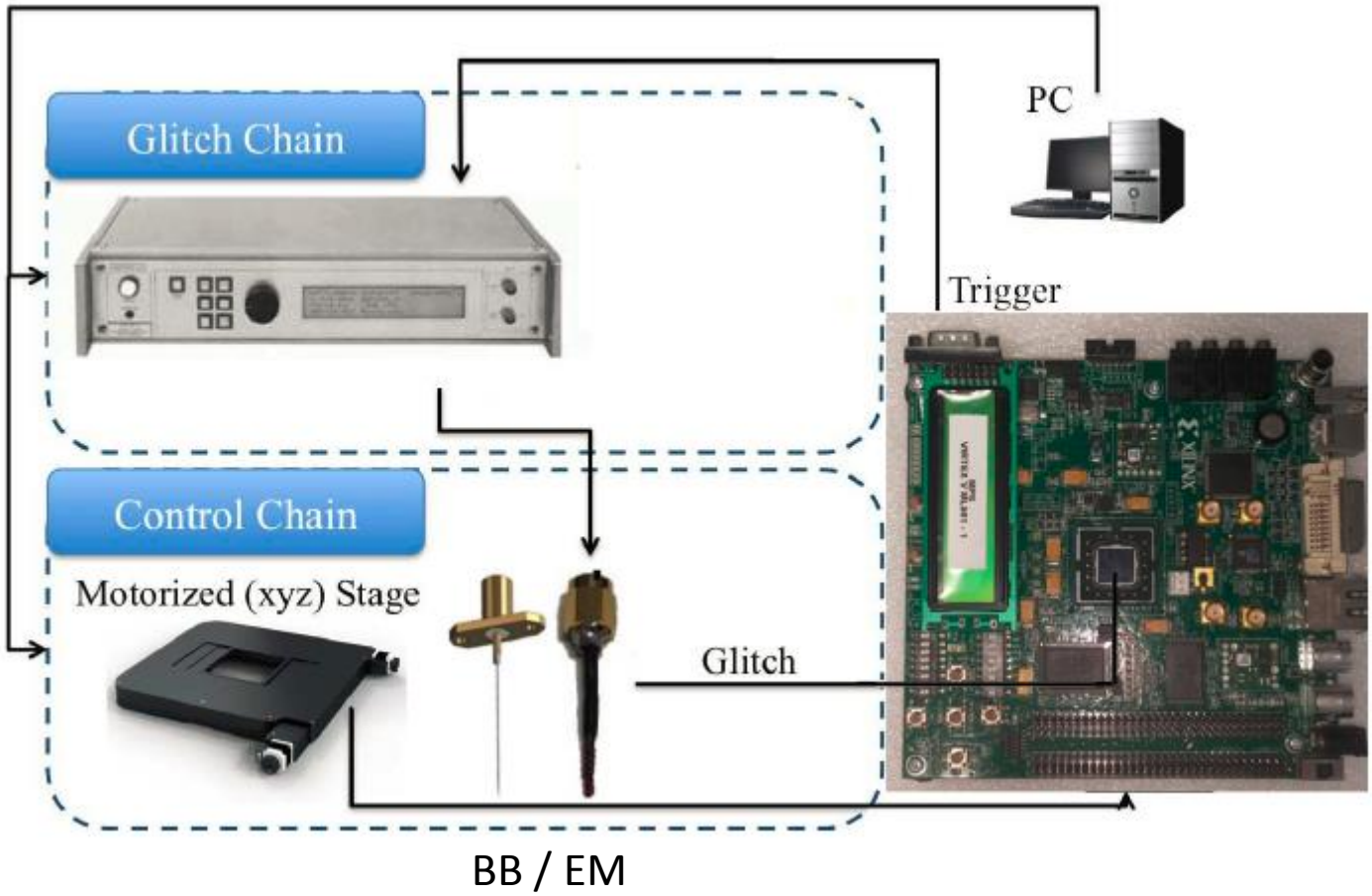
# Detector 2/2


Q1
Q2
Q3
Q4
Fault Detection Logic
Alarm


Clock
Q1
Q2
Q1⊕Q2 Sampled
t

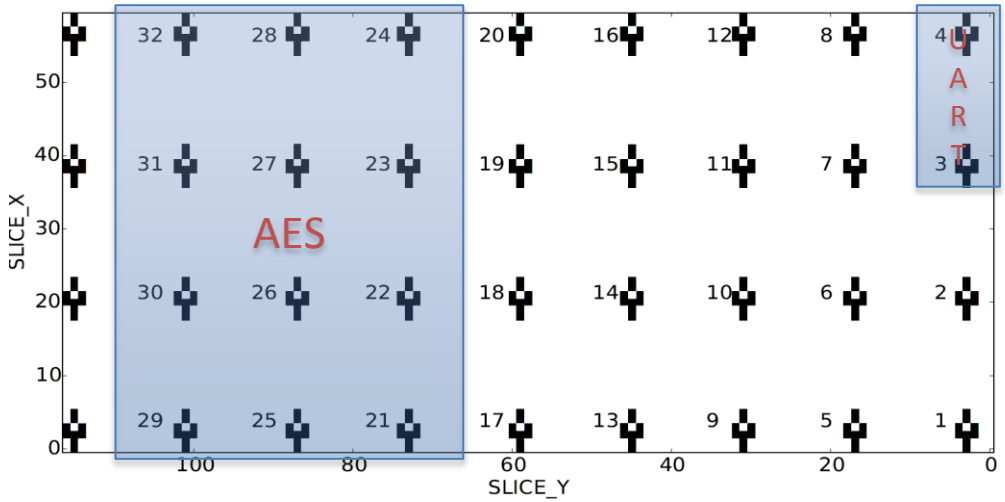
MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# EM & BB Test Bench



# Test Bench

| FPGA (Xilinx) | Tech. Node | Frequency (Period) | # of detectors |
|---|---|---|---|
| Virtex 5 | 65 nm | 100 MHz (10ns) | 36 |
| Virtex II Pro | 90 nm | 100 MHz (10ns) | 34 |
| Spartan 3E 1600 | 90 nm | 50 MHz (20ns) | 36 |



Spartan3 1600E Floorplan

- 34 detectors regulary spreading
- AES as a circuit to protect
- UART as communication system

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Agenda

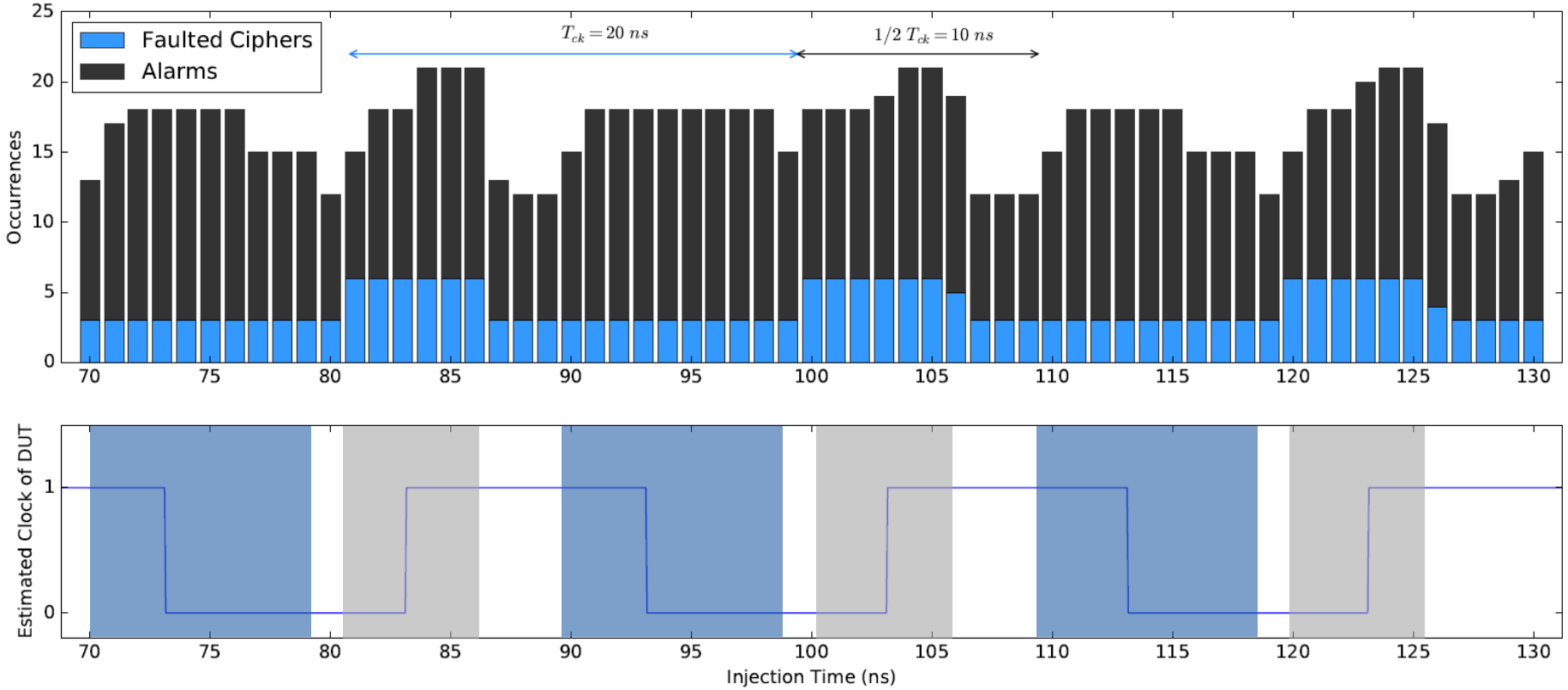
- **Context**

- **Fault Model**
- **Detector Design**
- **EM and BB Detection Results**
- **Optimisation**

- **Next Steps**
- **Conclusion**

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# EM Results




Probability to inject a fault in AES or in detectors
Spartan3 1600E / 50 Mhz

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Success Rate

- **GP** (Good Position) : # of positions where the detectors are efficient : the detection could block the output of the cipher (faulted or not).

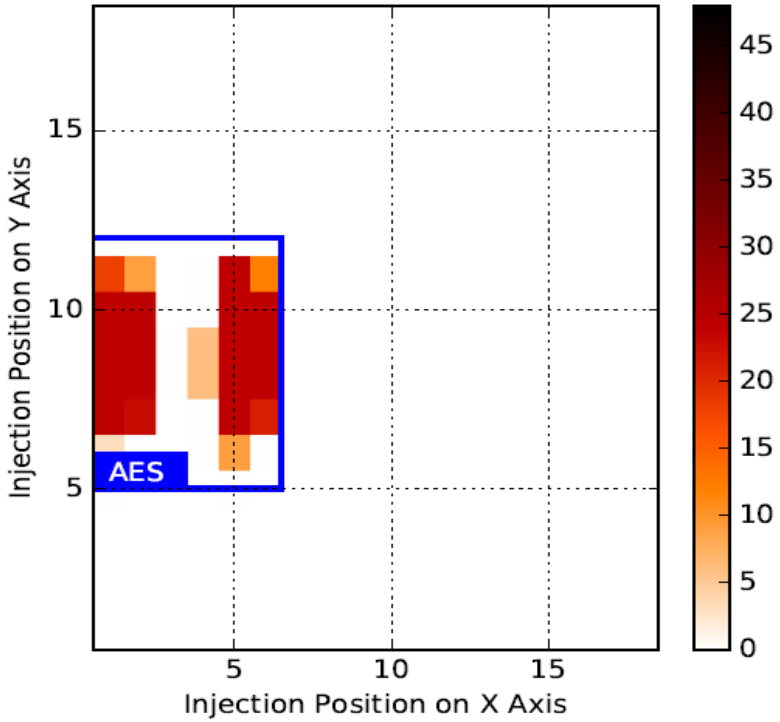
- **BP** (Bad Position) : # of positions where the AES can be faulted without triggering alarm.

- **SR** (Success Rate) : Ratio of Good Positions over the total # of active positions = where something happens.

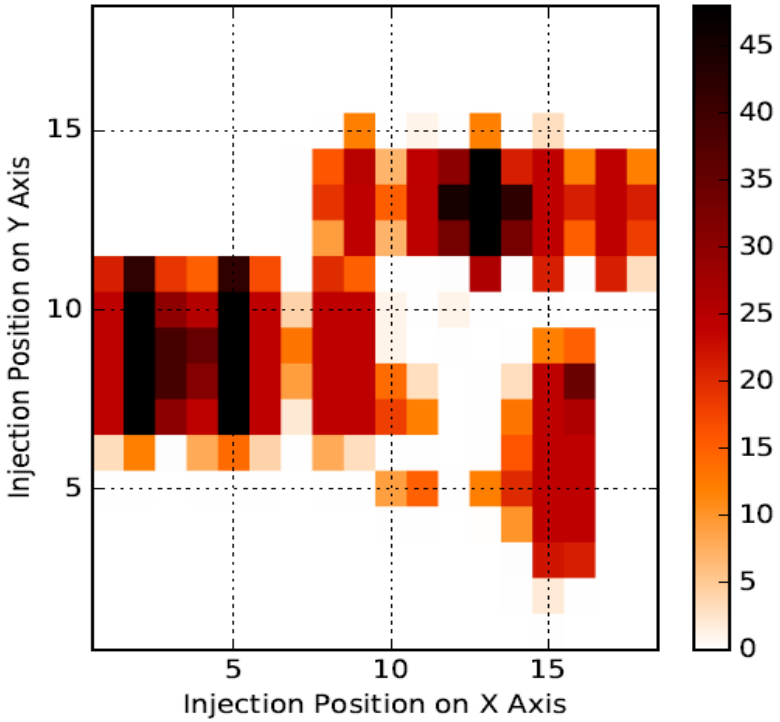
$$SR = \frac{GP}{GP + BP}$$

# EM Results (here on Virtex 5)

**# of faulted ciphers by firing position**




**# of detections by firing position**

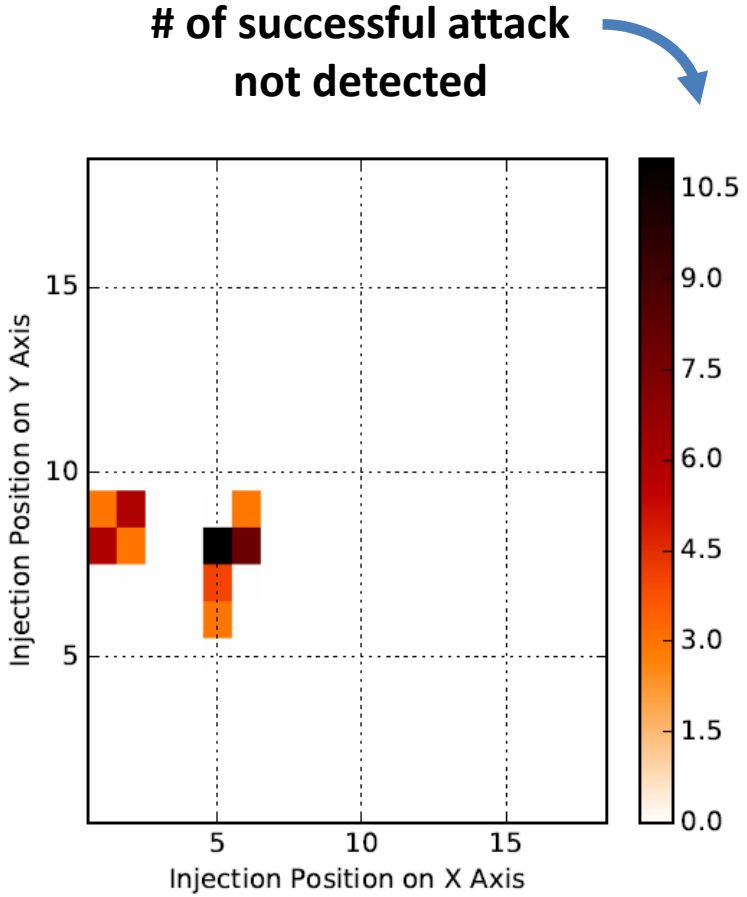



- Wide Detection Area, **no sensor detection range**.

SR = 94%

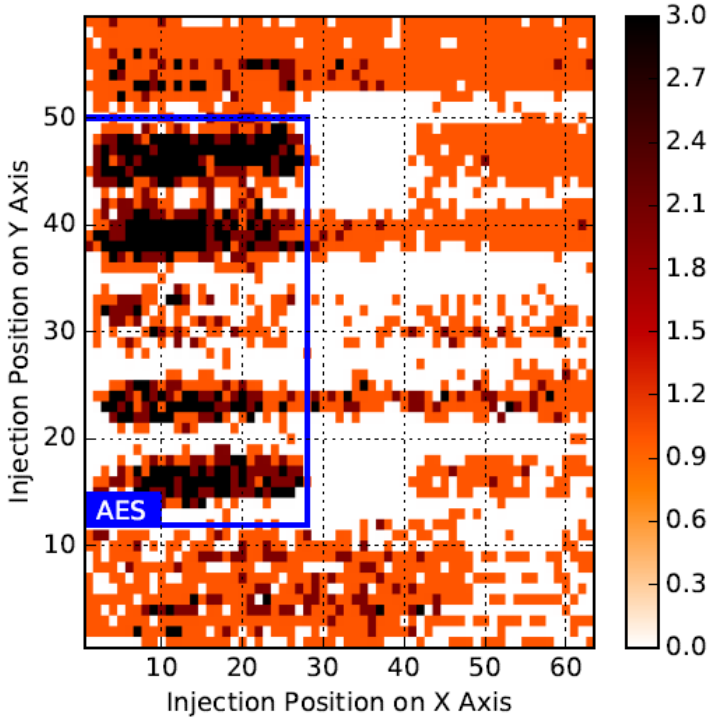
# EM Results (Virtex 5)

Successful attacks not detected : 47/467 = 10%

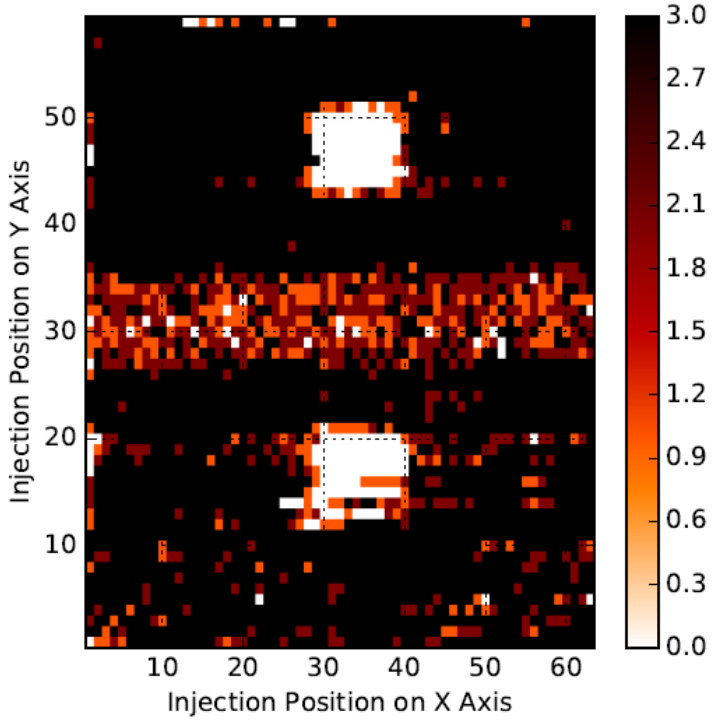


# BB Results (Virtex 2)

**# of faulted ciphers by firing position**




**# of detections by firing position**




- Wide Detection Area, **NO undetected faults**.

SR = 100%

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Synthesis

Table summarizing the success rates by attack and model of FPGA:

| | Injection at rising edge | | | Injection at falling edge | | |
|---|---|---|---|---|---|---|
| | Spartan3 1600E | Virtex 5 | Virtex II Pro | Spartan3 1600E | Virtex 5 | Virtex II Pro |
| EM Front-side | 78 % | | | 88 % | | |
| EM Back-side | | 94 % | 86 % | | 95 % | 94 % |
| RBBI | | 100 % | 100 % | | 100 % | 100 % |

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

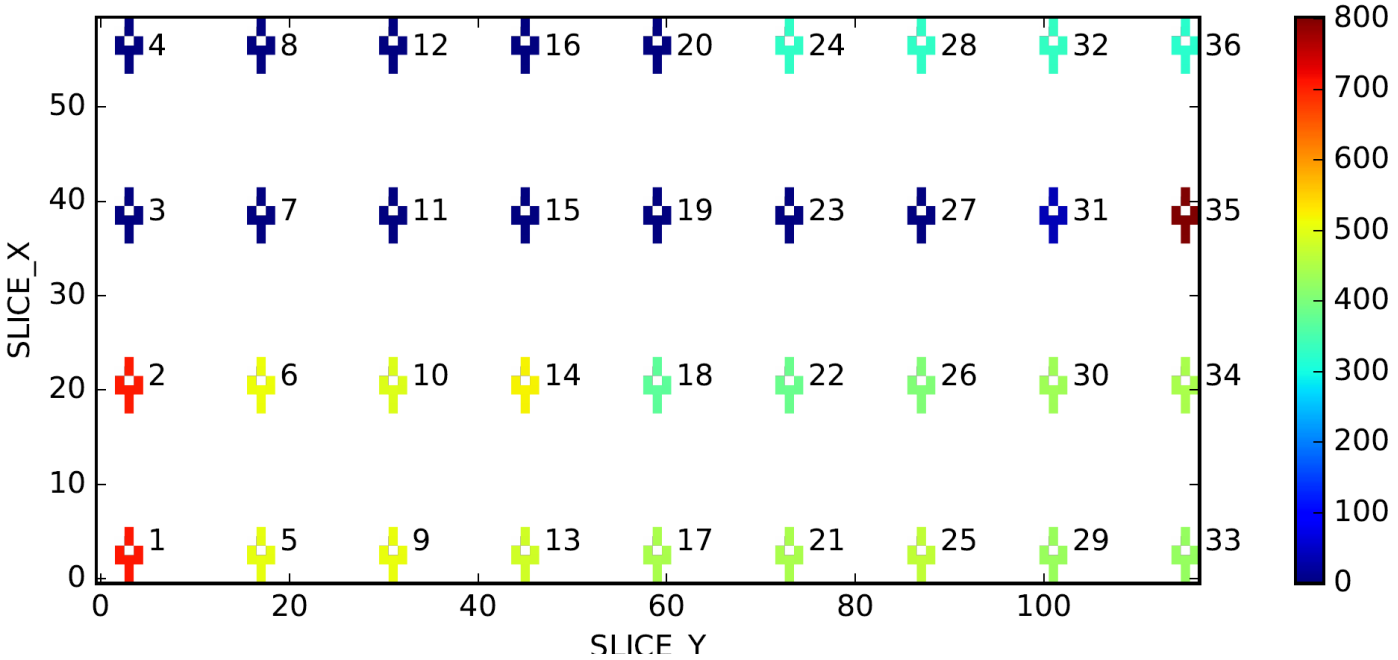
# Agenda

- **Context**

- **Fault Model**
- **Detector Design**
- **EM and BB Detection Results**
- **Optimisation**

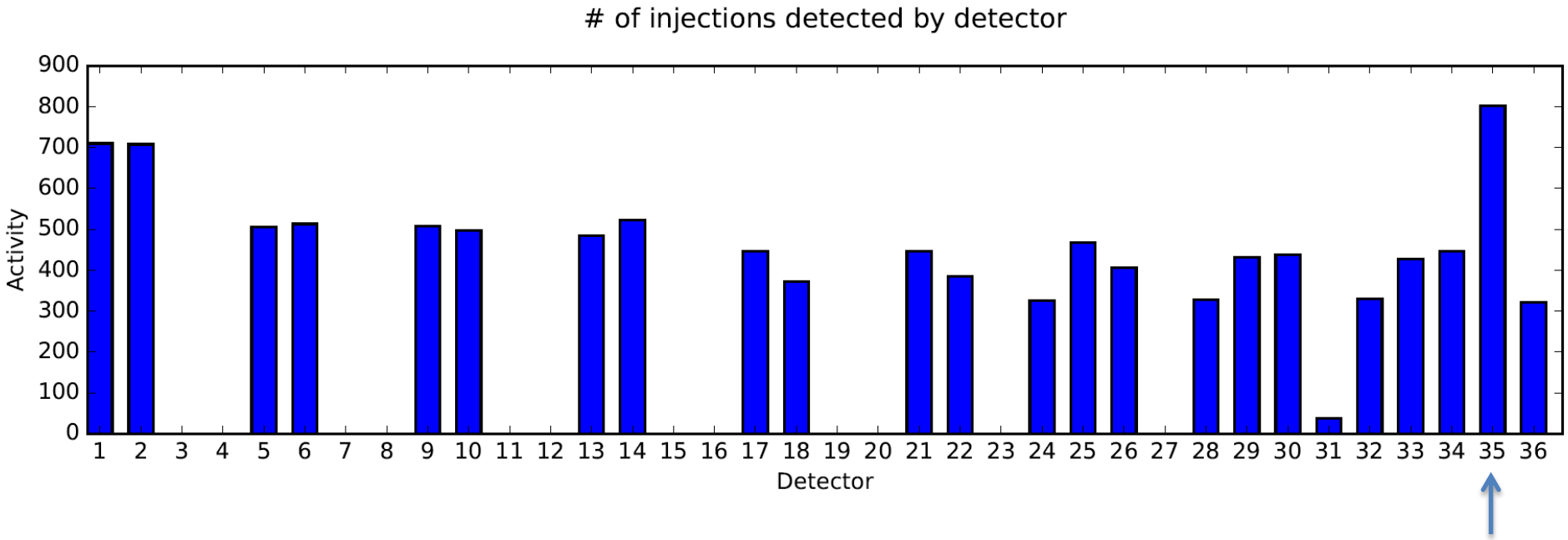
- **Next Steps**
- **Conclusion**

# Impact of the detectors' location



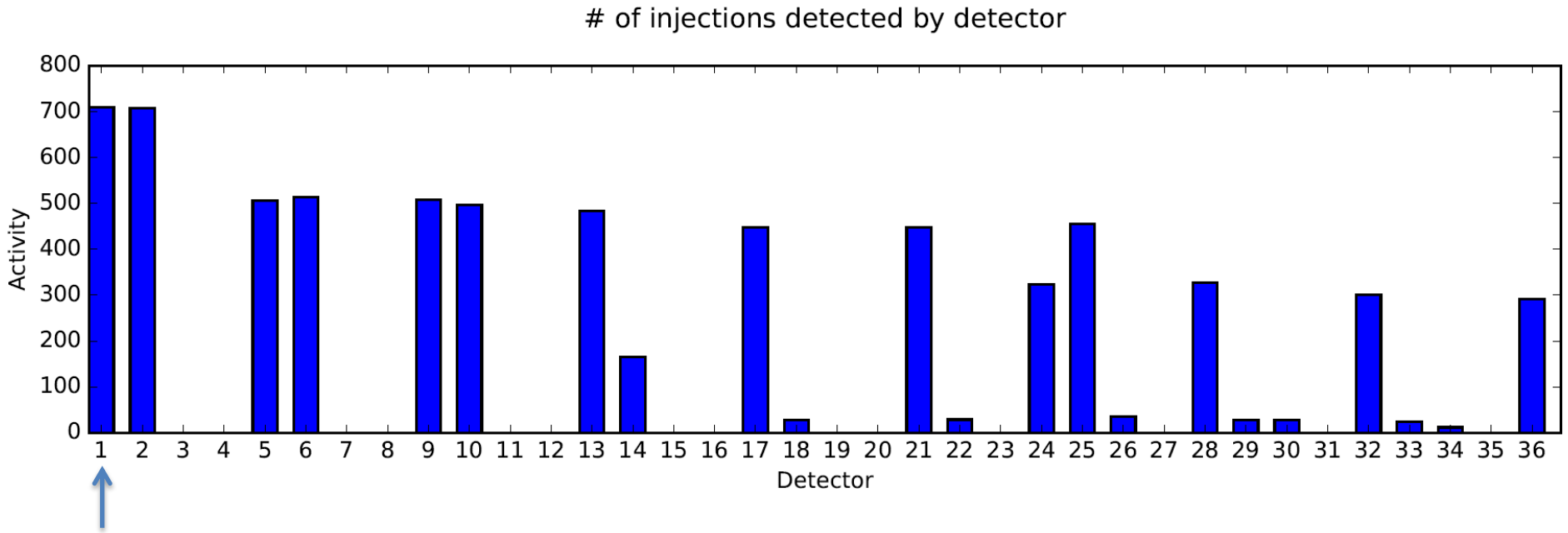

Virtex 5 Floorplan. Colors means number of triggering per sensor for a full map.

# Impact of the detectors' location



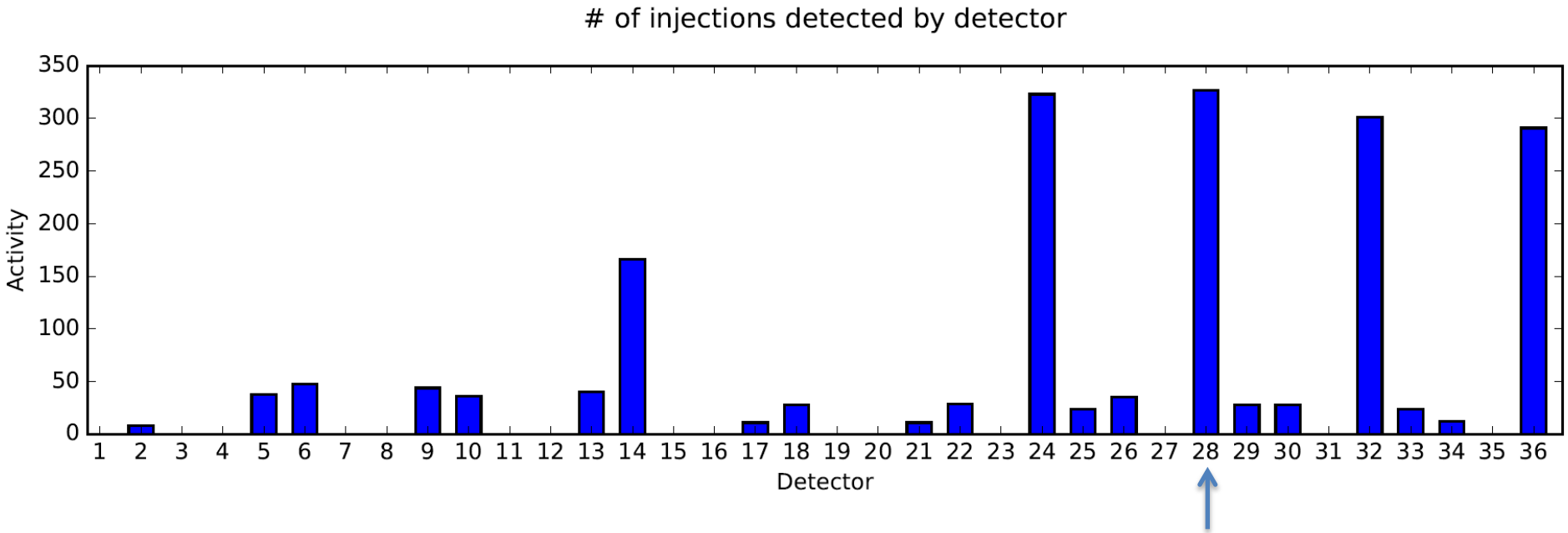

- **Selecting the most active detector**

# Impact of the detectors' location




- **Generation of the histogram of activity by ignoring the attacks detected by the previous sensors "fixed"**

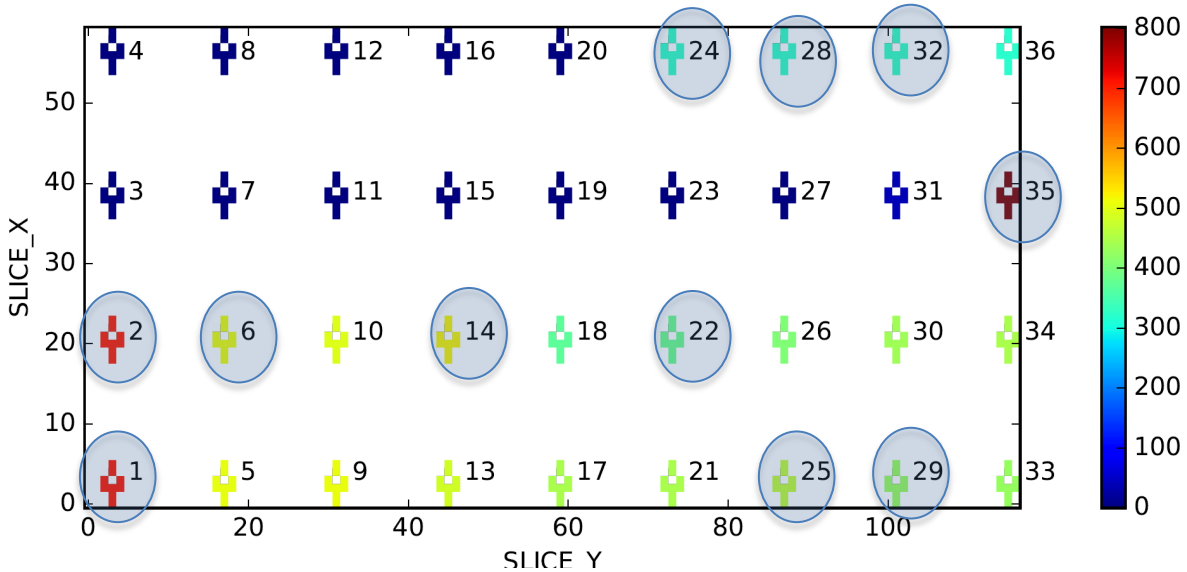
# Impact of the detectors' location




- **Iterate again until all the detections are catched.**

# Impact of the detectors' location

- **Results of optimisation against EM Injections:**
  - **11 detectors / 36 are enough to detect a the attacks**



MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Next Steps

- **Tests against Power Glitches Injections (finalizing the experiments)**
- **Tests against Laser Injections**
- **Development of a Test Chip (ASIC).**

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816 |

# Conclusion

- **Proposal of an enhanced detector**
  - **Fully Digital and fully compliant with ASIC design flow**
  - **Small : 35 nand eq. / detector**
- **Efficient against at least two injection fault methods:**
  - **ElectroMagnetic Injections**
  - **Body-Biasing Injections**
  - **Power Glitch Injections (First results being analyzed)**

MINES Saint-Étienne | INSPIRING INNOVATION SINCE 1816

# Thank you !