A Fully-digital EM-Pulse (EMP) Detector

David El-Baze[1] Jean-Baptiste Rigaud[1] Philippe Maurine[2,3]

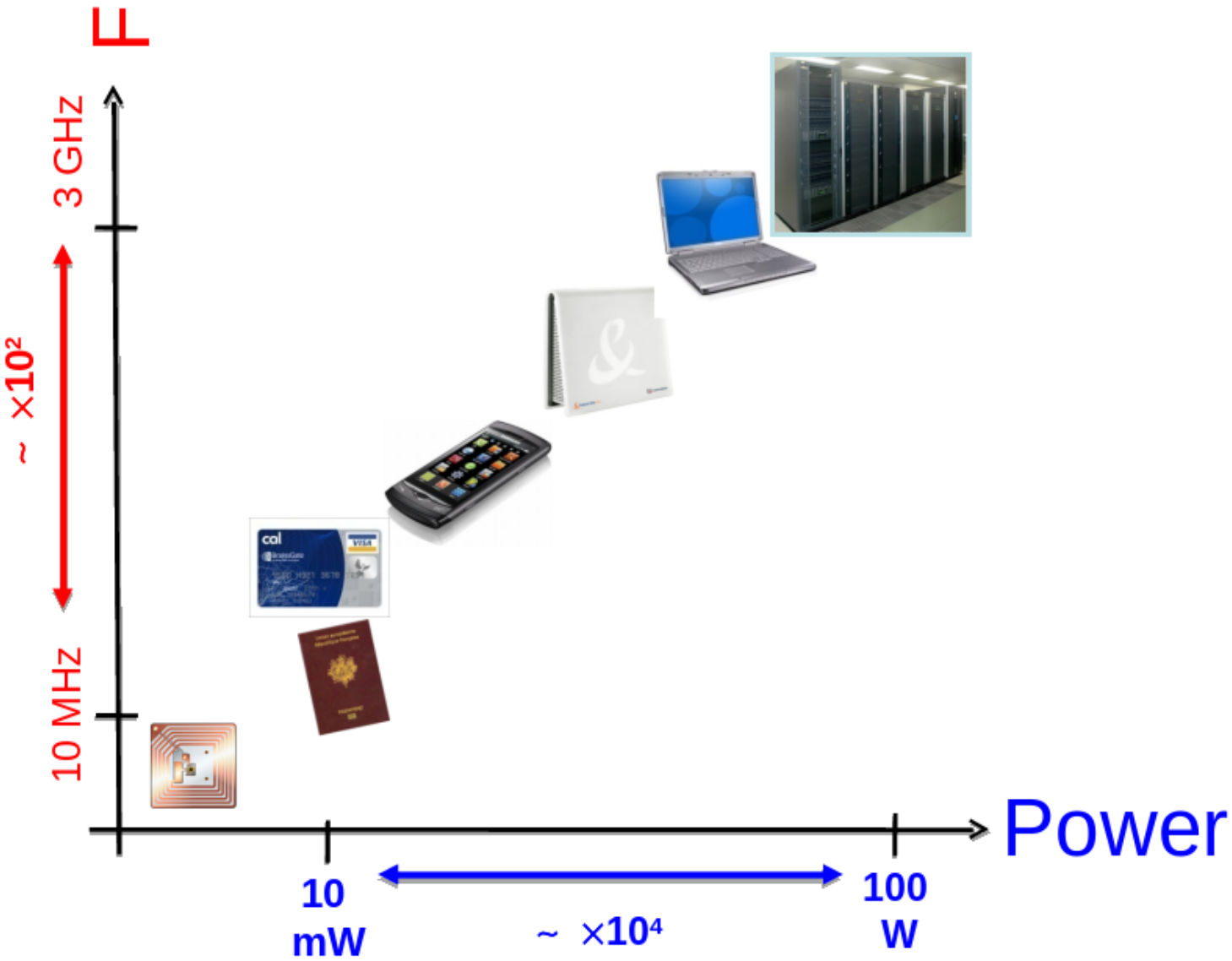
[1]Mines Saint-Etienne

[2]CEA

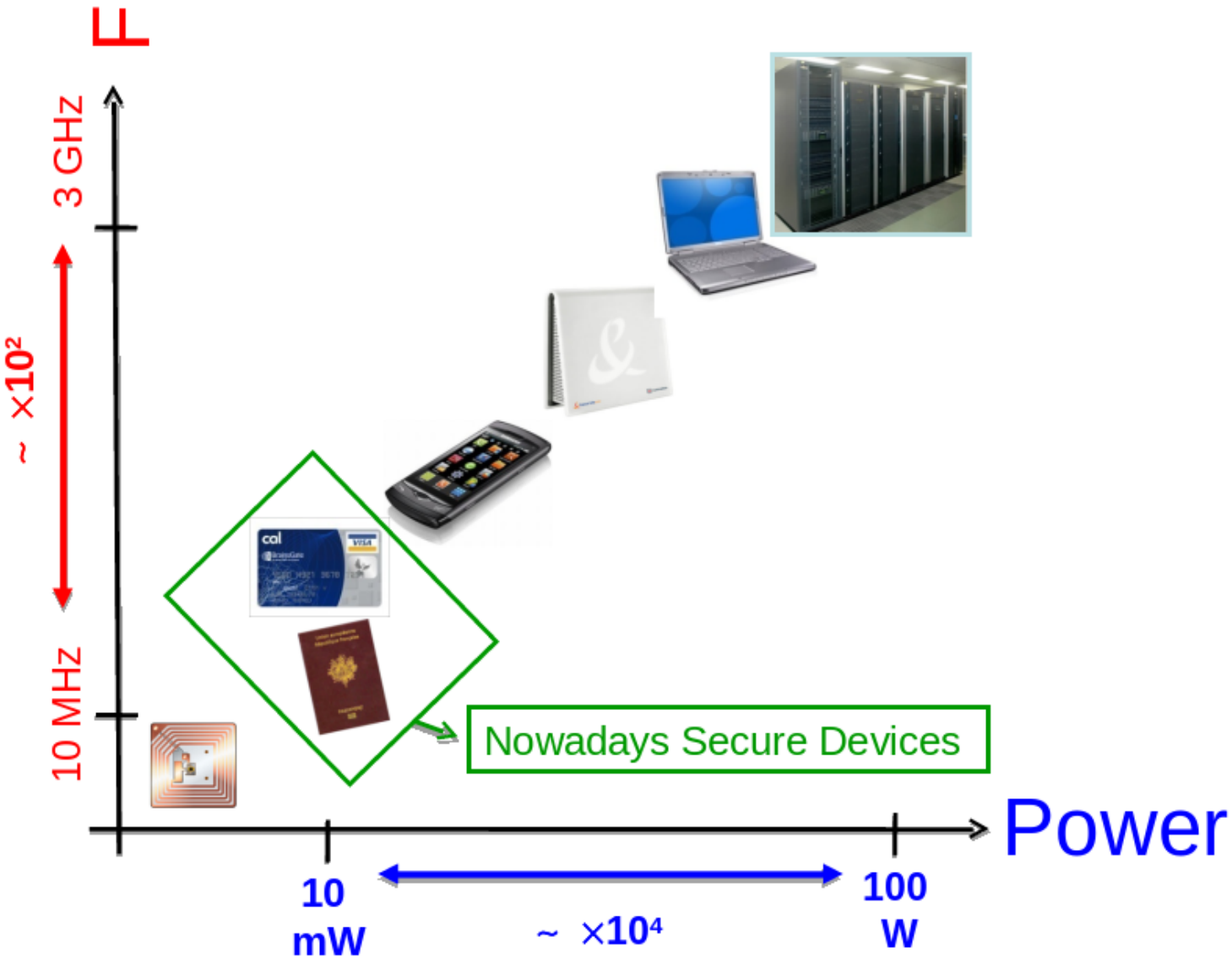
[3]LIRMM

June 29, 2015

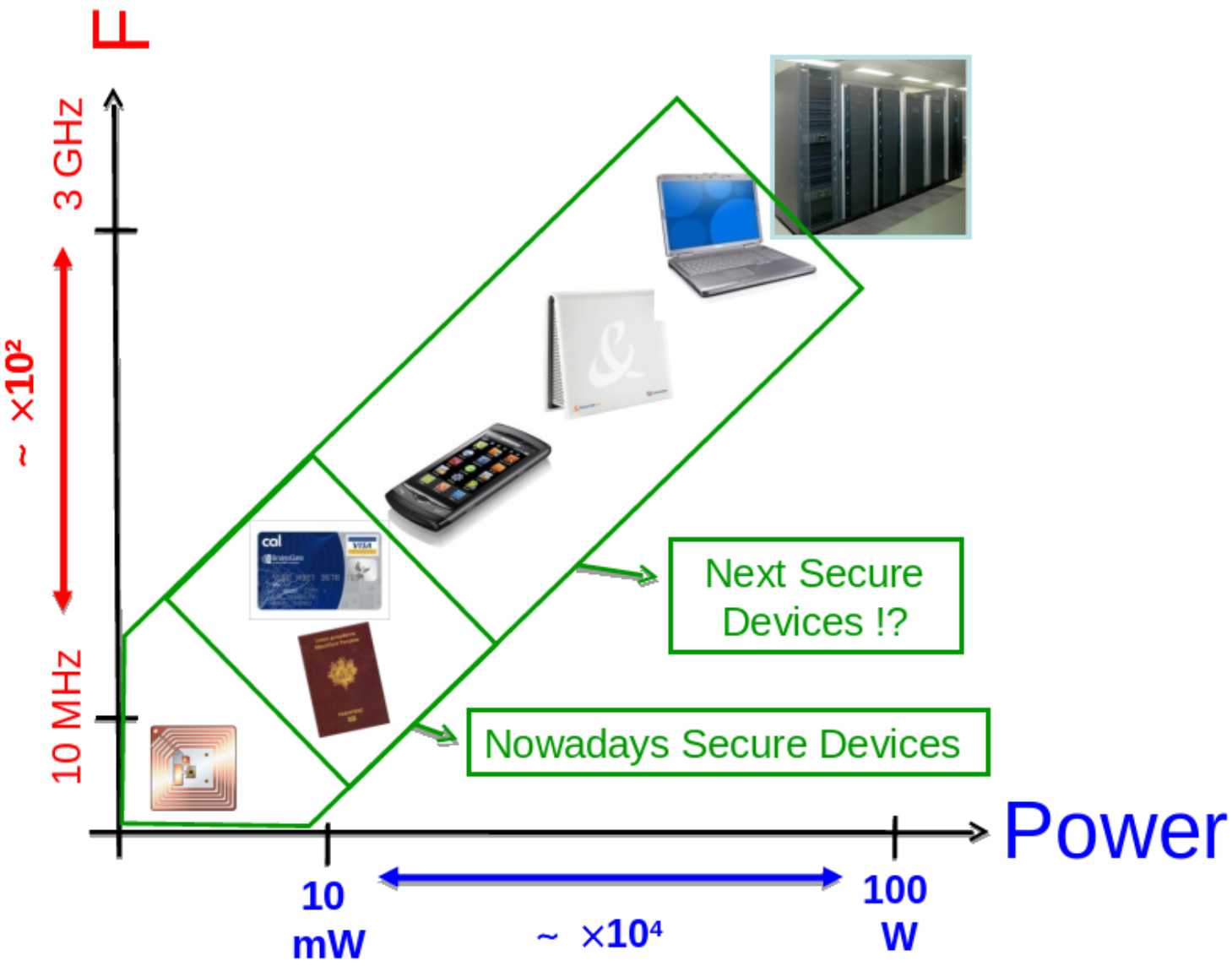
Current devices in IoT



Current devices in IoT



Current devices in IoT



Outline

1. State of the Art
2. The concept
3. Test Platform and Results

State of the Art

State of the Art

2002 [1] J. Quisquater, D. Samyde
'Eddy current for Magnetic Analysis with Active Sensor' (Esmart 2002)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 [2] J.-M Schmidt, M. Hutter
'Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results' (Austrochip 2007)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 [3] A. Alaeldine, T. Ordas, R. Perdriau, P. Maurine, M. Ramdani, L. Torres, M. Drissi
'Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection' (EMC-Zurich 2009)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 [4] F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine
'Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system' (ePrint 2012)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 [5] A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
'Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES' (FDTC2012)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 [6] L. Zussa, A. Dehbaoui, K. Tobich, J-M Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, A. Tria
'Efficiency of a Glitch Detector against Electromagnetic Fault Injection' (DATE 2014)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 **Evaluation of a countermeasure based on timing slack monitoring**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 **Evaluation of a countermeasure based on timing slack monitoring**

2014 [7] S. Ordas, L. Guillaume-Sage, K. Tobich, J.M. Dutertre, P. Maurine **'Evidence of a Larger EM induced Fault Model' (CARDIS 2014)**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 **Evaluation of a countermeasure based on timing slack monitoring**

2014 **EM Injection induces bitsets and bitresets (and not only timing faults)**

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 **Evaluation of a countermeasure based on timing slack monitoring**

2014 **EM Injection induces bitsets and bitresets (and not only timing faults)**

2015 [8] S. Ordas, L. Guillaume-Sage, P. Maurine
'EM Injection: Fault Model and Locality' (to appear FDTC 2015)

State of the Art

2002 **Embedded memories can be disrupted by EM Injection**

2007 **EM Injection allows disrupting the course of a RSA algorithm**

2009 **EM Injection modifies the propagation delays of logical paths**

2011 **EM Injection modifies the oscillating frequency of an internal clock generator**

2012 **EM Injection induces timing faults during the course of hardware and software cryptographic modules**

2014 **Evaluation of a countermeasure based on timing slack monitoring**

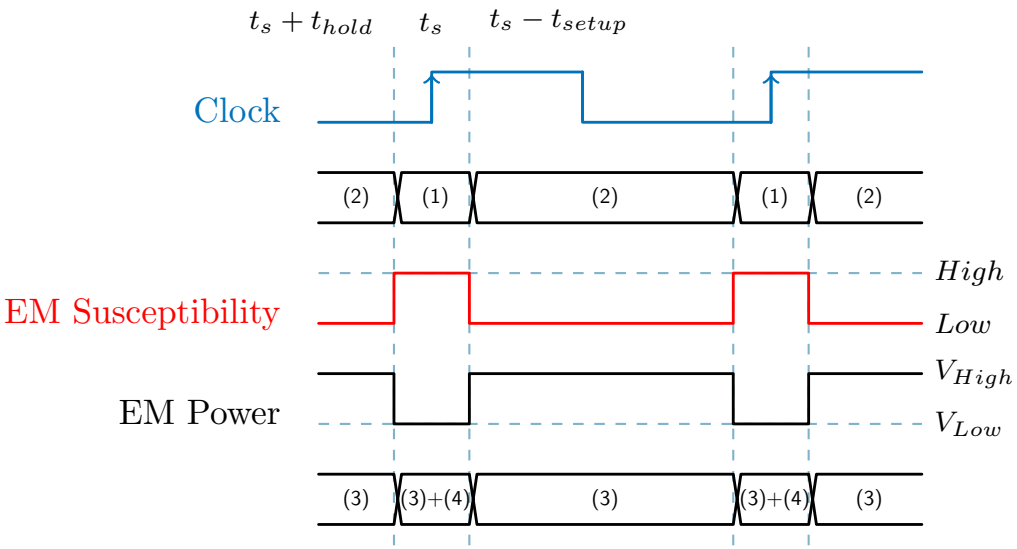
2014 **EM Injection induces bitsets and bitresets (and not only timing faults)**

2015 **DFFs are one of most sensible gates in a design**

The concept

DFF Susceptibility

Power Needed to fault a D Flip Flop



(1) : Stability Window
(2) : Processing Window

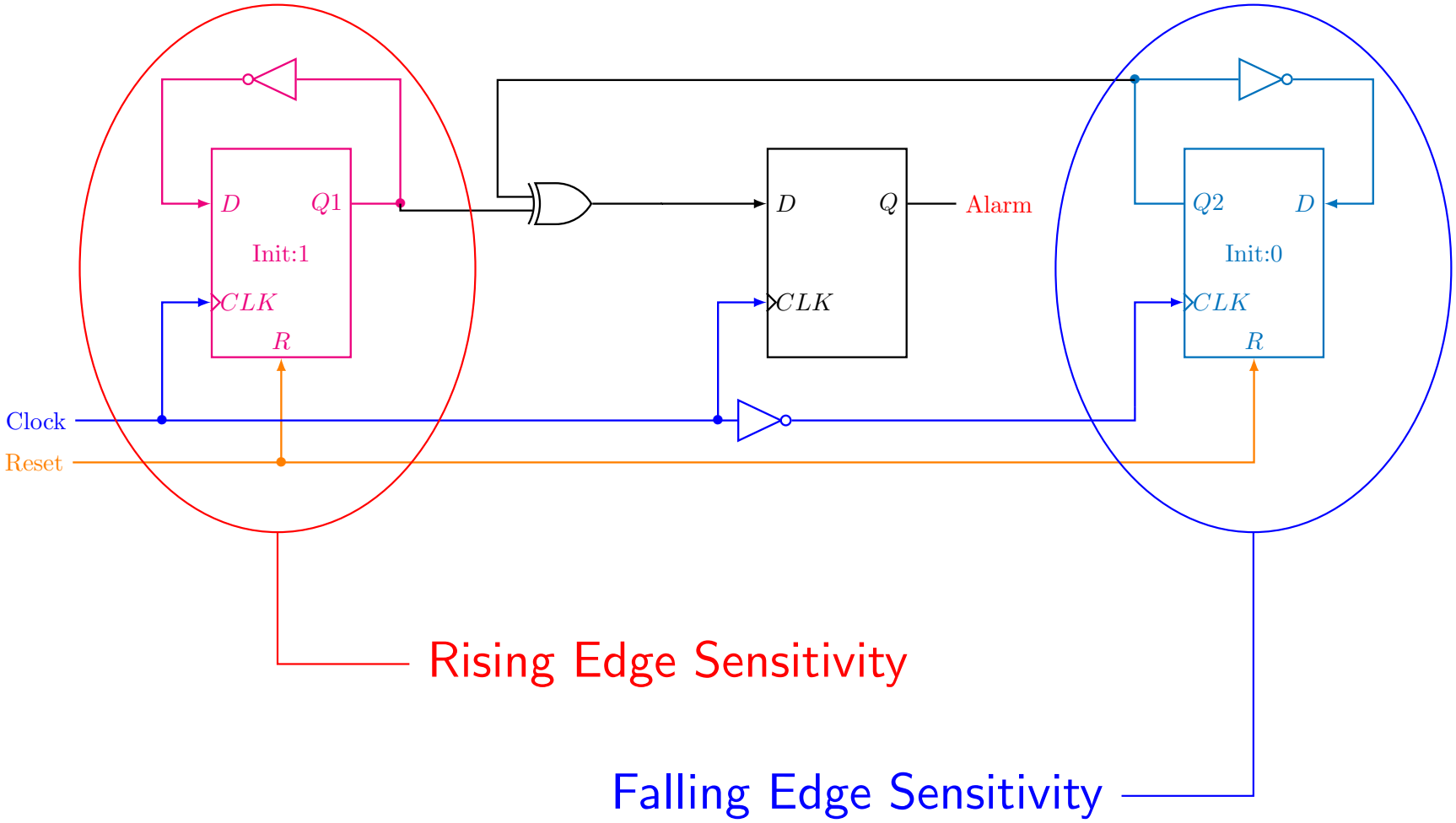
(3) : Bitset or bitreset produced
(4) : Sampling fault produced

- DFF are the more susceptible gates in a design (except maybe Memory Sense Amplifiers).
- Susceptibility of DFF is higher on rising edges.

$\Rightarrow$ use of DFF to design a fully digital EMP detector.

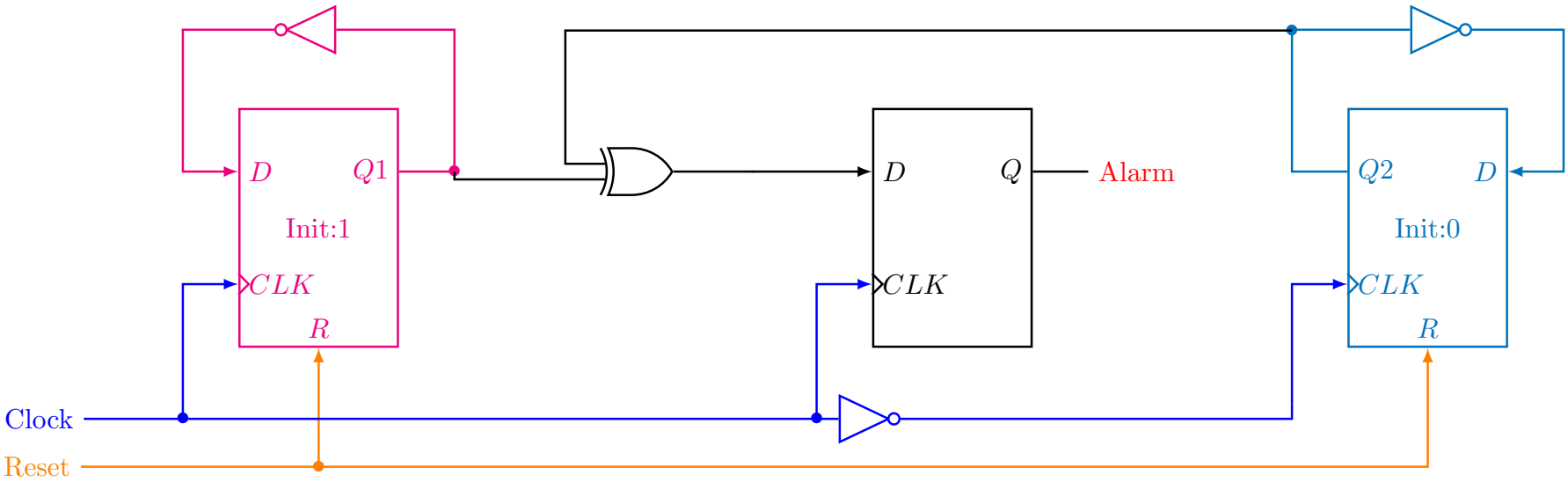
S. Ordas: CARDIS 2014, PHISIC 2015, FDTC 2015

Architecture of the Half-Detector

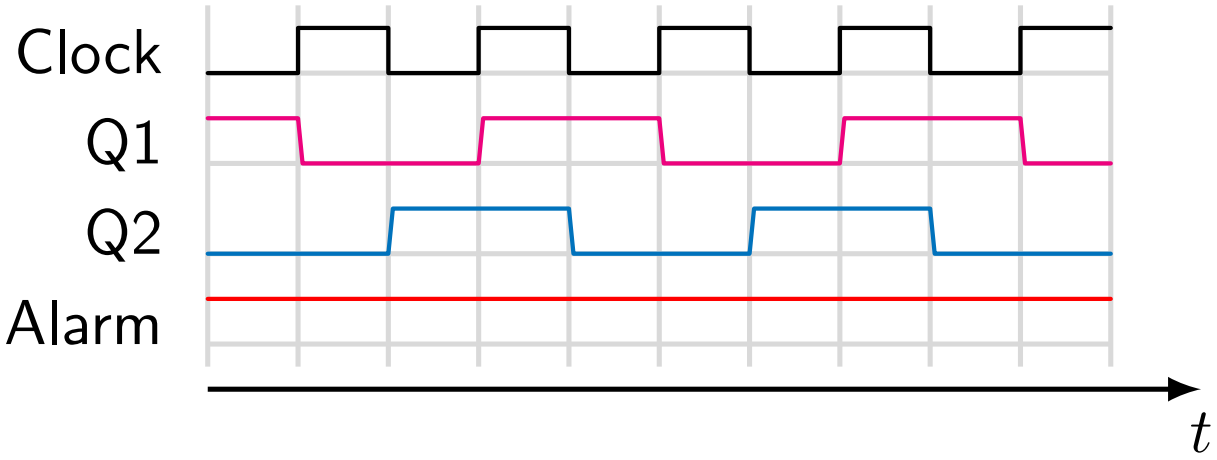


DFFs' outputs are set to 1 when reset net is high.

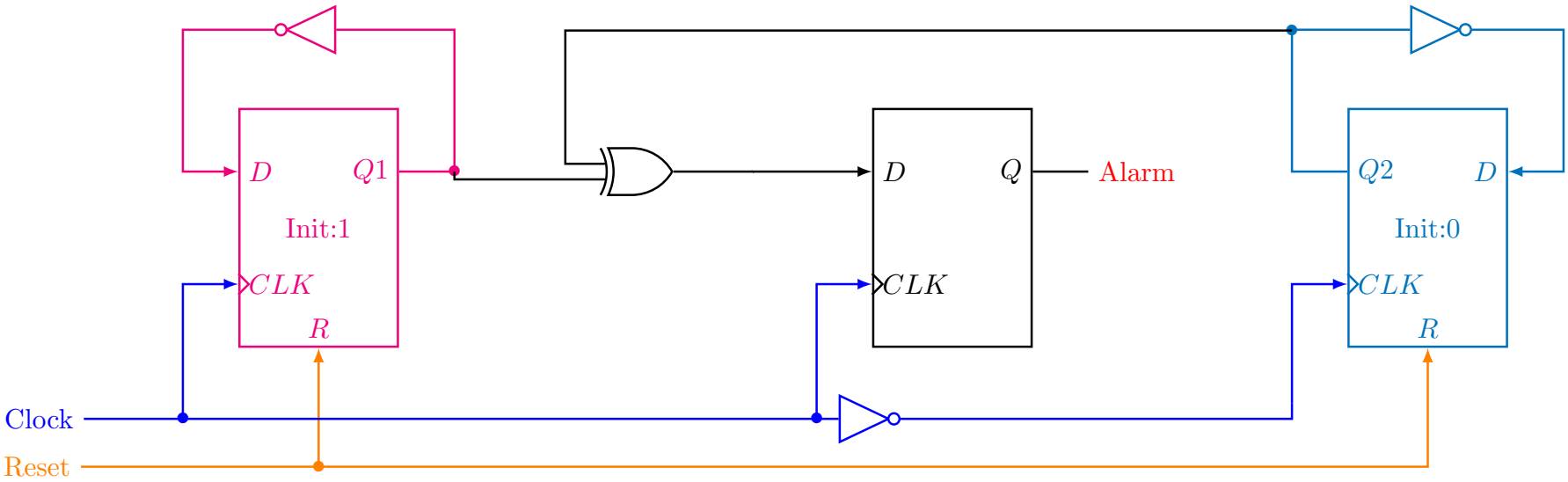
Half-Detector Timing Diagram



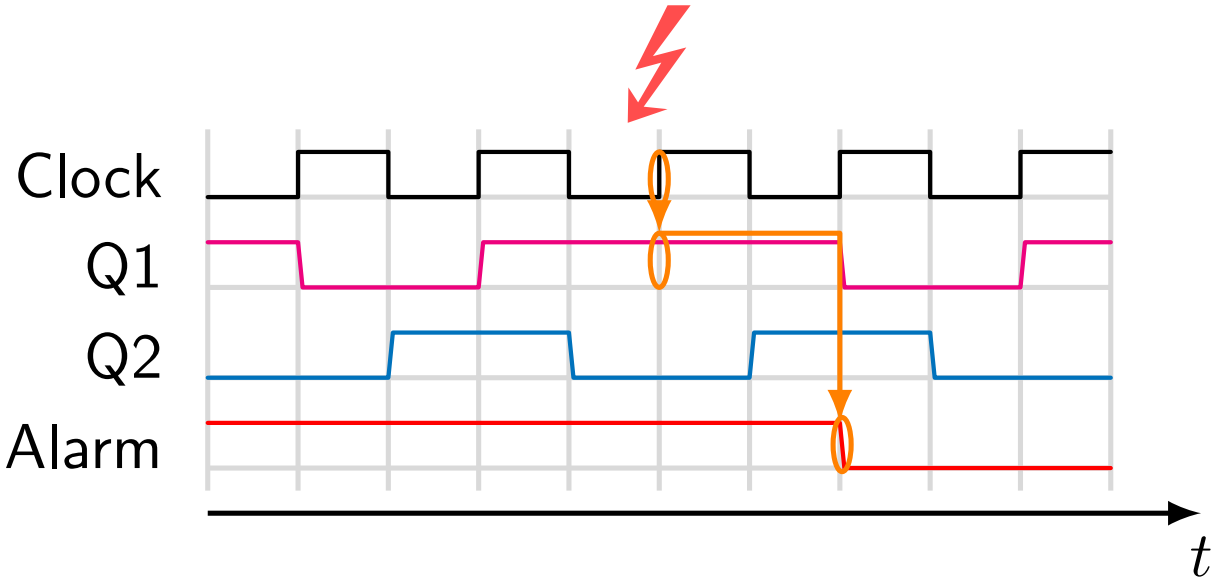
When operates normally :



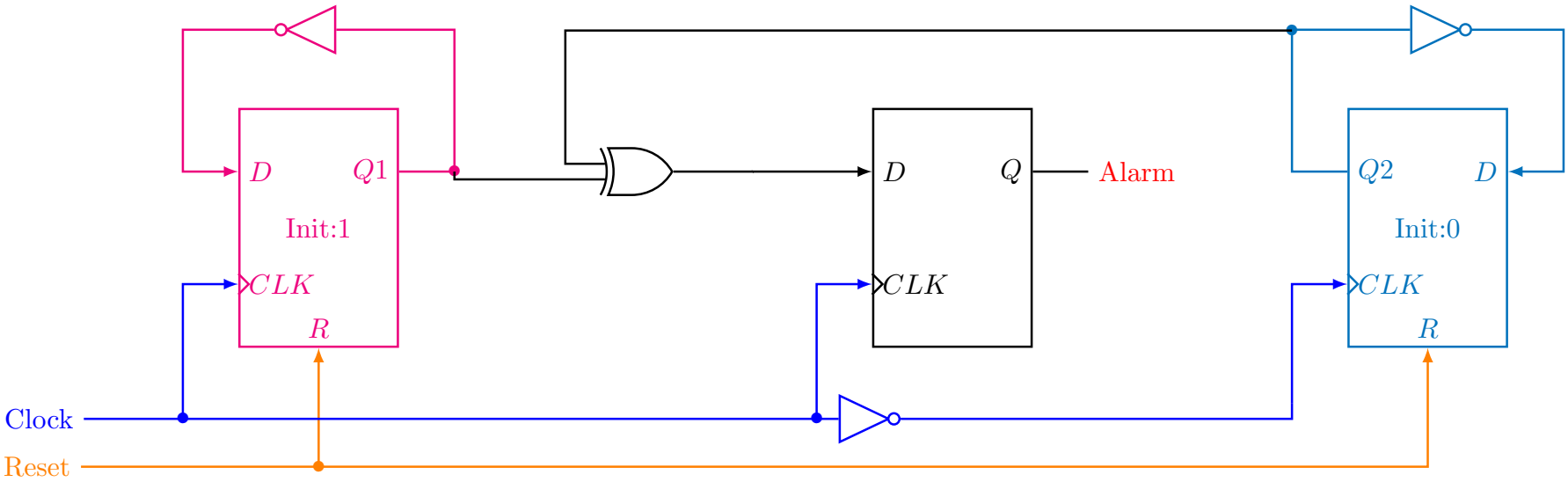
Half-Detector Timing Diagram



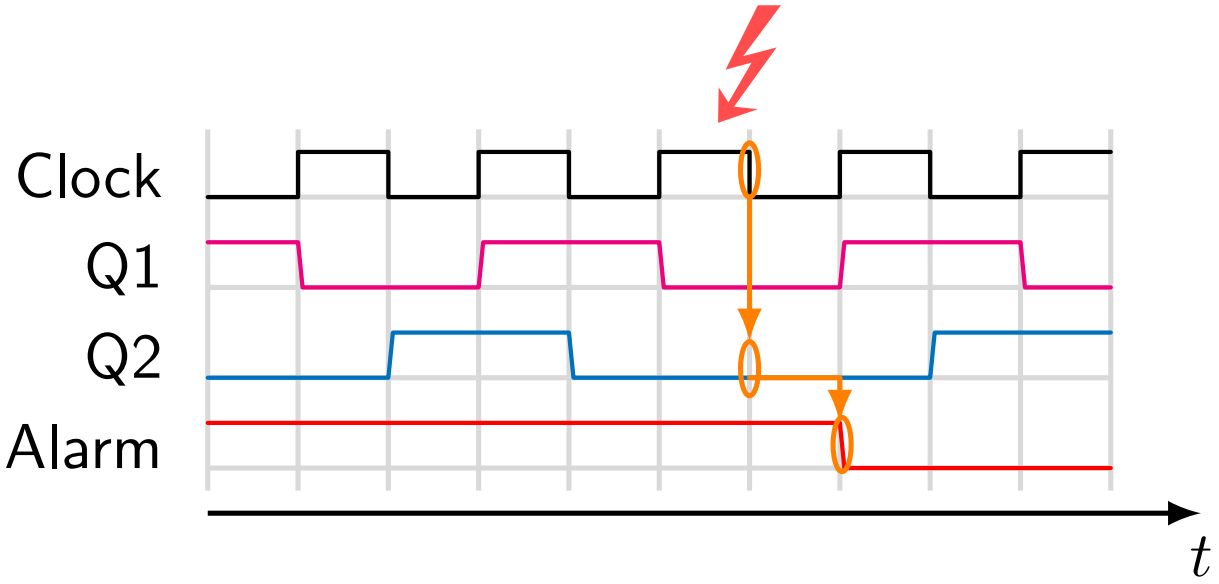
EMP at rising edge :



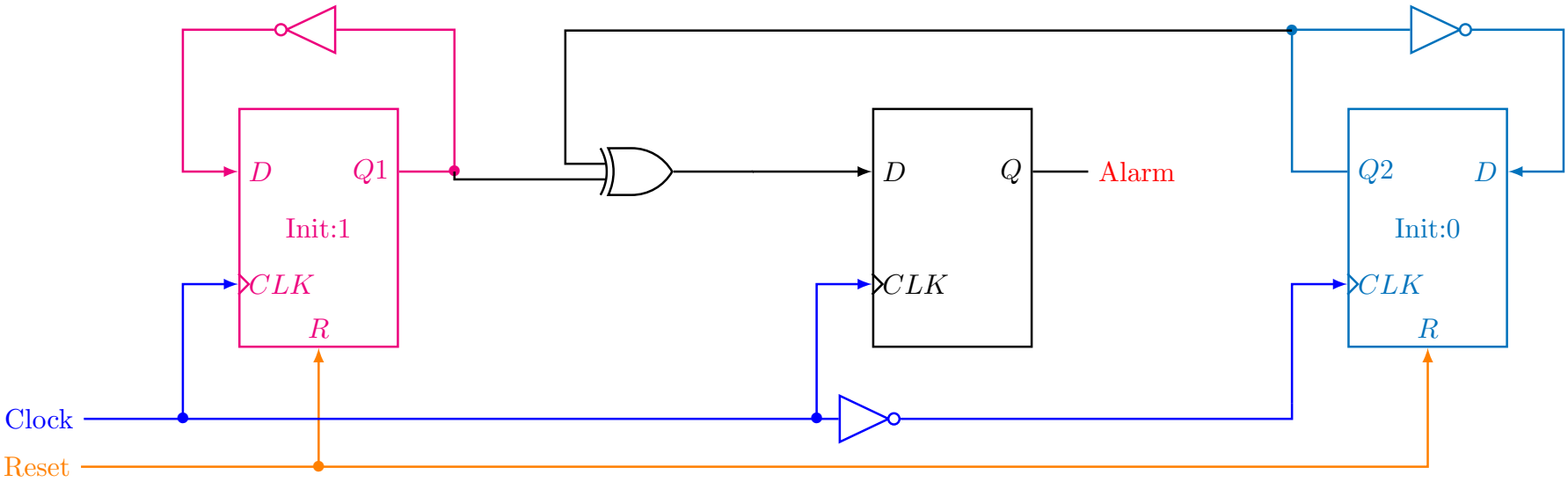
Half-Detector Timing Diagram



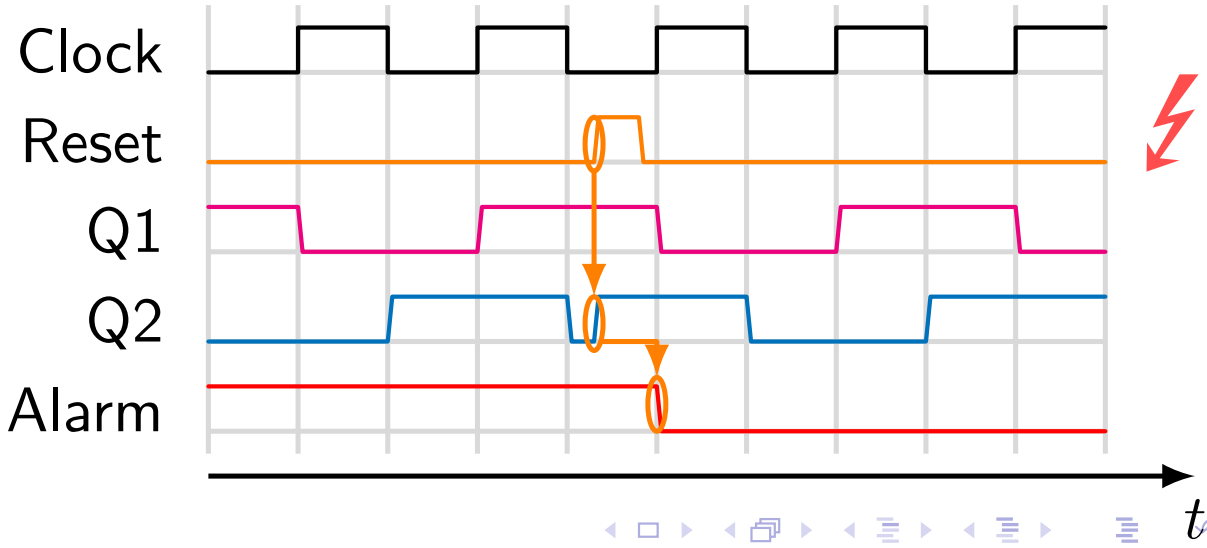
EMP at falling edge :



Half-Detector Timing Diagram

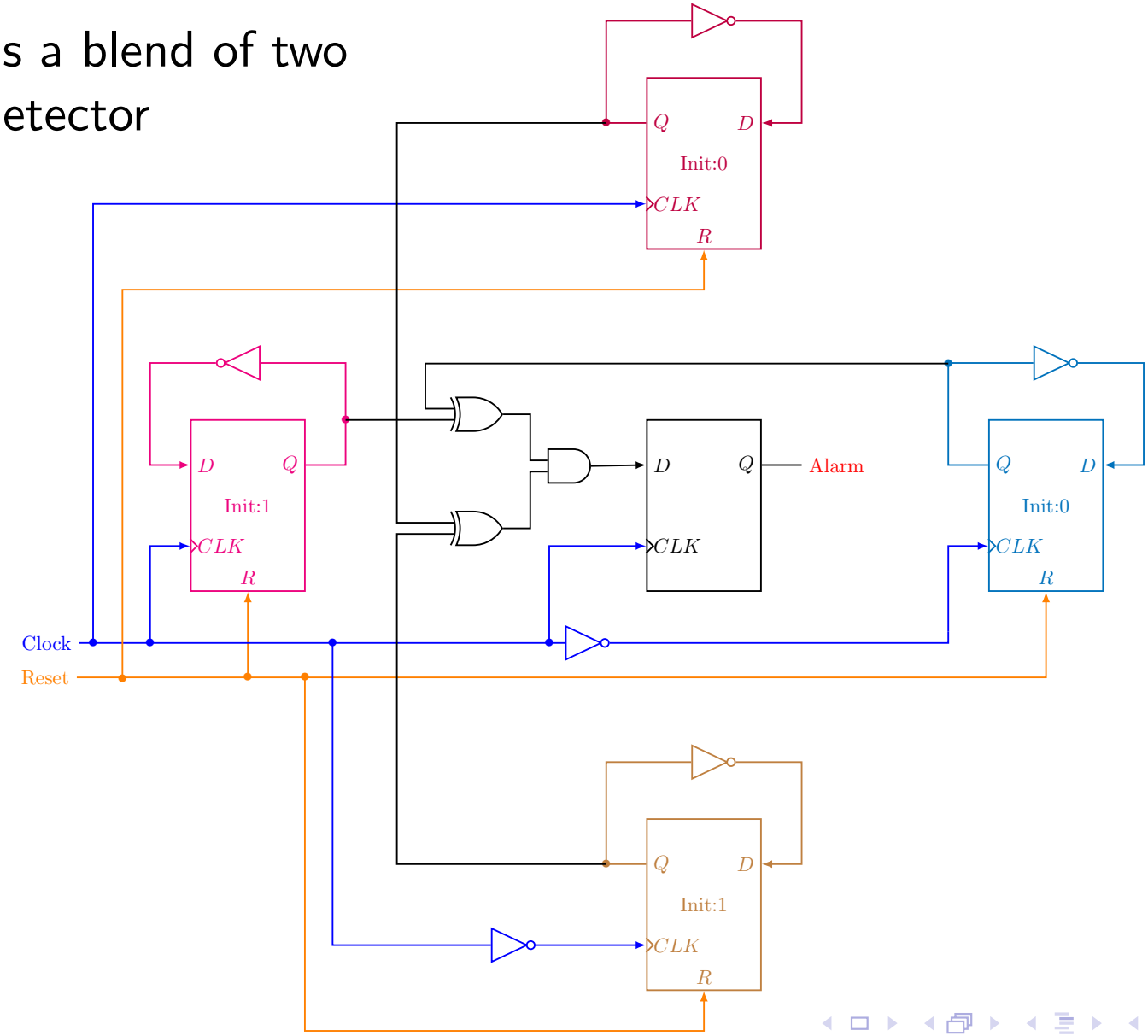


When EMP creates a reset glitch :



Full Detector Design

This is a blend of two half-detector



Test Platform and Results

Test Platform

Composition

The Test Platform we developped is composed of

- EM Glitch Generator ($\pm$ 400V 16A),
- A probe for fault injection,
- A motorized stage (for probe positionning),
- FPGA Xilinx Spartan 3 : 1000 gates programmed with a Design (AES, UART, mesh of detectors).

Experiments

- 2 designs : one with a common reset (1R) shared by AES and the detectors and another with a separate reset net (2R).
- 3 maps for both, with a FPGA powered at 1.1V, 1.2V (normal supply voltage of the card) and 1.3V.

Experiment overview

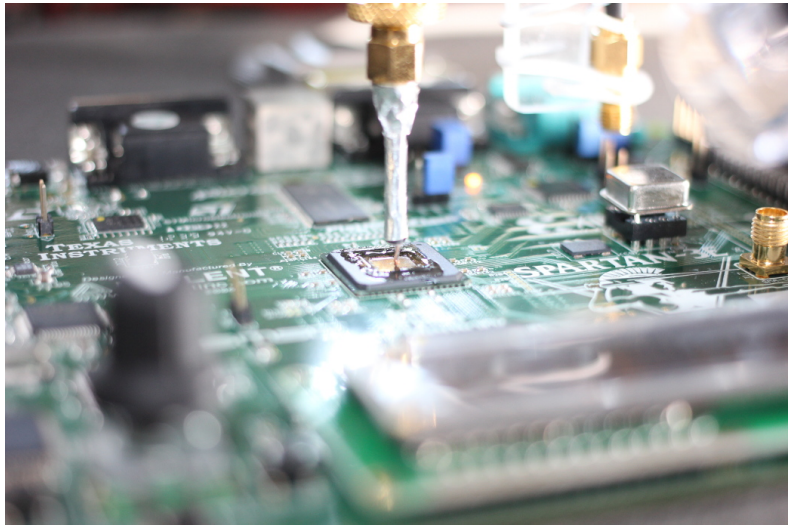


Figure: EM injection probe

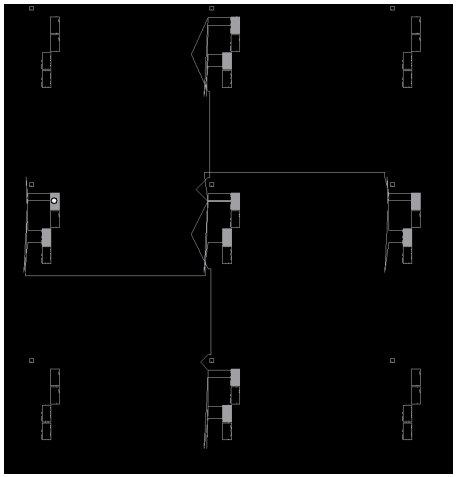


Figure: Detector Hard Macro

- 34 nand eq.

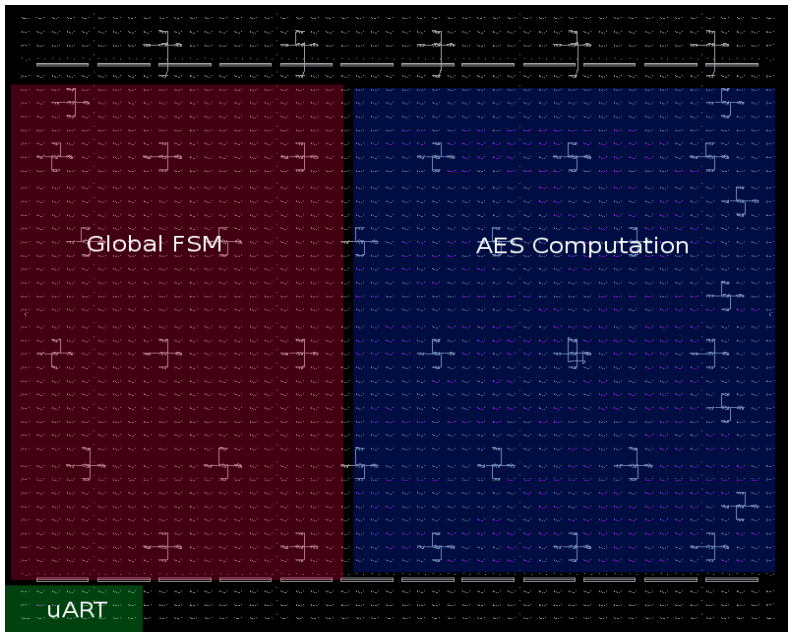
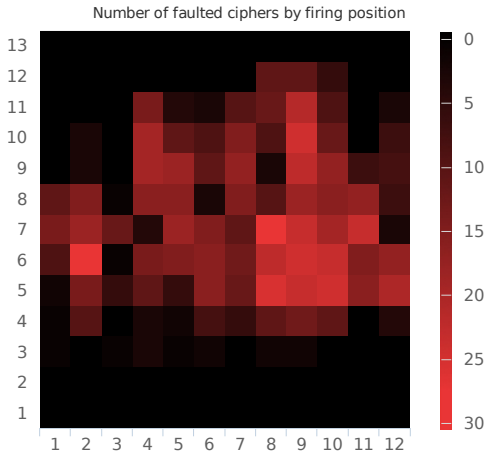
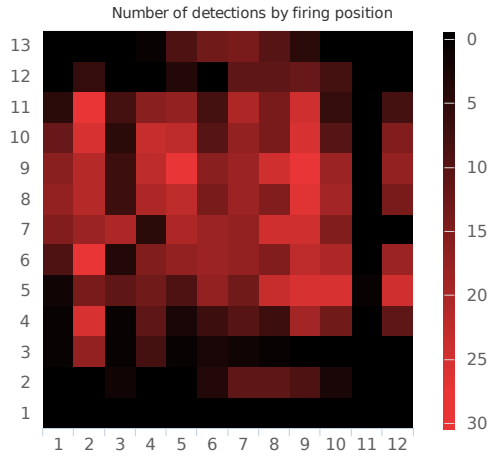


Figure: Floorplan

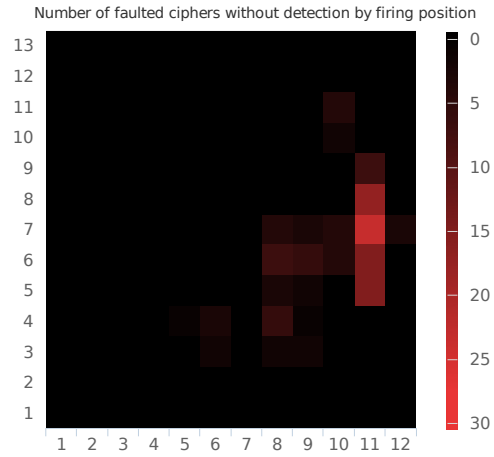
First Results



AES Sensitivity



Detector Sensitivity



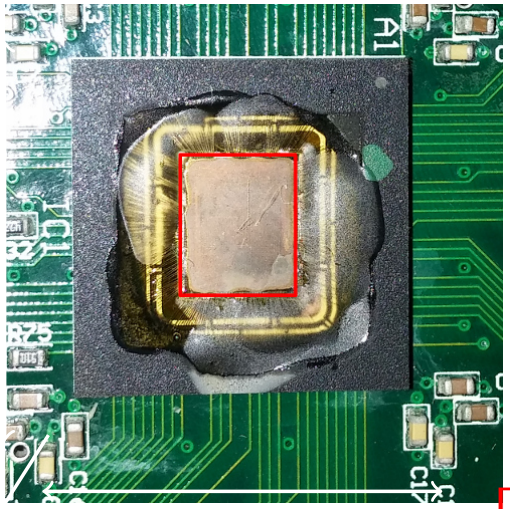
Results

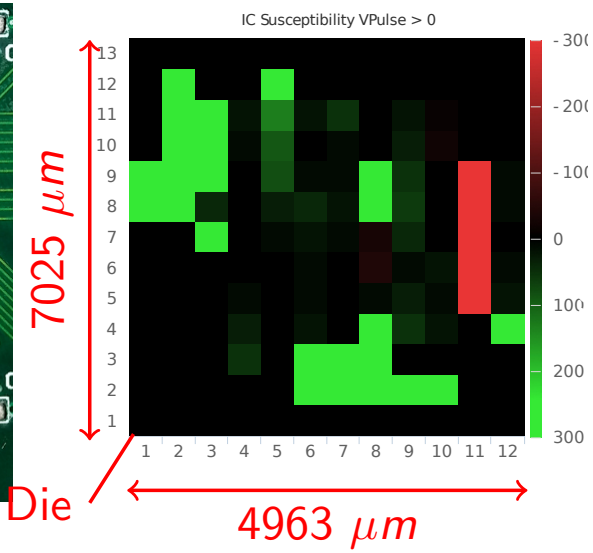
One Position = One Category

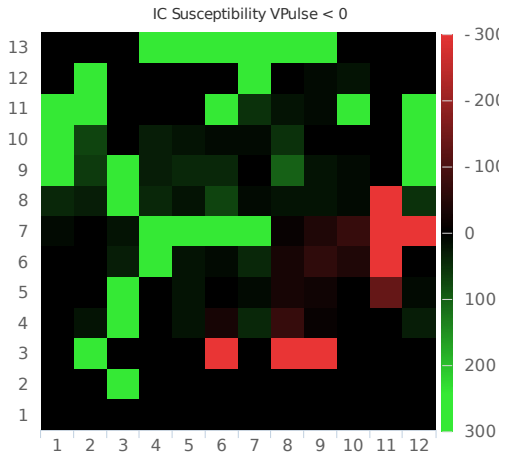
- Category *AF* : When detectors are more sensitive than the AES (looks good),
- Category *CF* : When the AES is more sensitive than detectors (looks bad),
- Category *Idem* : When detectors have the same sensitivity than the AES (fairly good).

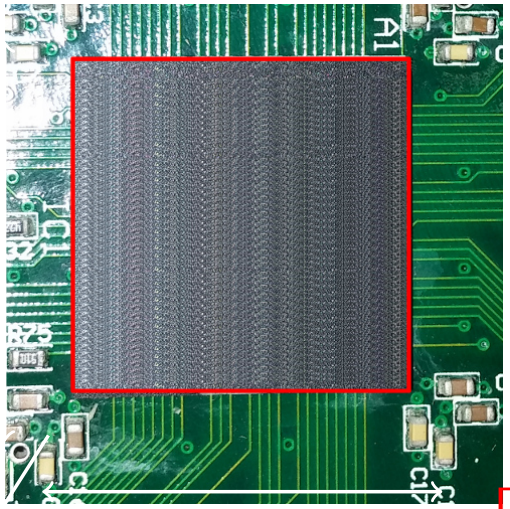
A Detection rate formula : $$\frac{\mathrm{Card}(AF) + \mathrm{Card}(Idem)}{\mathrm{Card}(AF) + \mathrm{Card}(CF) + \mathrm{Card}(Idem)}$$

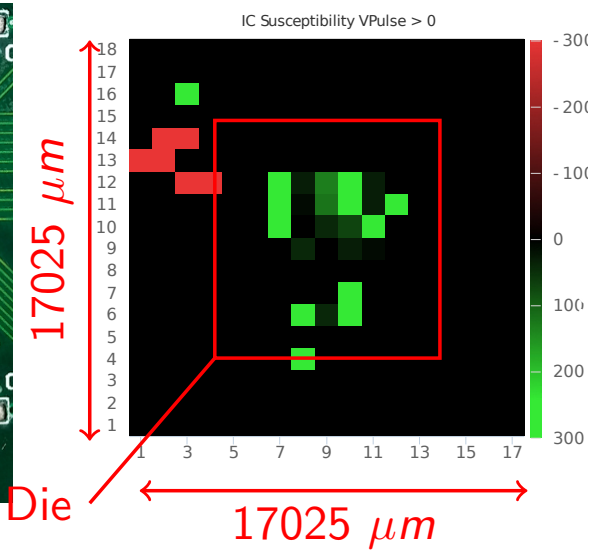
Results: 1.2V and common reset nets

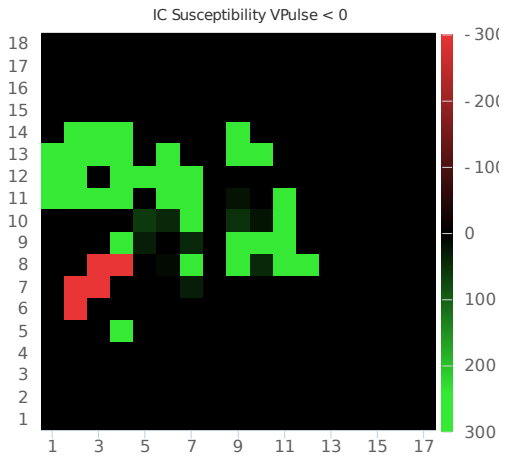




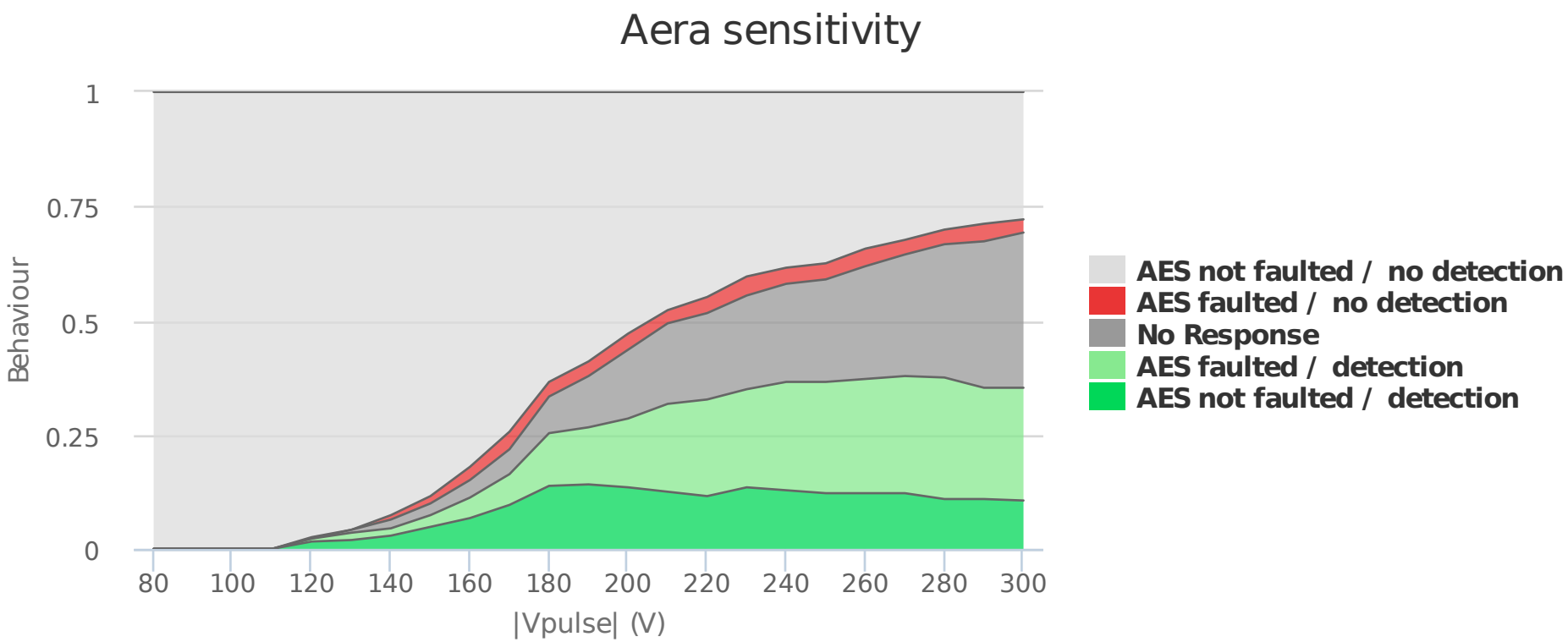








Results



	Common Reset	Separated Reset
1.1 V	85 %	84 %
1.2 V	86 %	79 %
1.3 V	85 %	79 %

Conclusion

First Results

- Detector against EM Injection
  - From a Fault Model established by Sebastien Ordas (FDTC2015 to appear)
  - Fully Digital
  - Low-Cost
  - Fully compliant with design flow
- Detection efficiency > 85 % in our test

Further works

- Assessment of the detector against Voltage Glitch and Laser Injection
- Development of a demonstrator on ASIC

Thank you !

Thank you for your attention.
Any questions ?