DE LA RECHERCHE À L'INDUSTRIE

cea

www.cea.fr

Extending the EM injection fault model

S. Ordas[1], L. Guillaume-Sage[1], K. Tobich[1], P. Maurine[2,1]

[1] LIRMM
[2] CEA-TECH

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

CryptArchi 2014

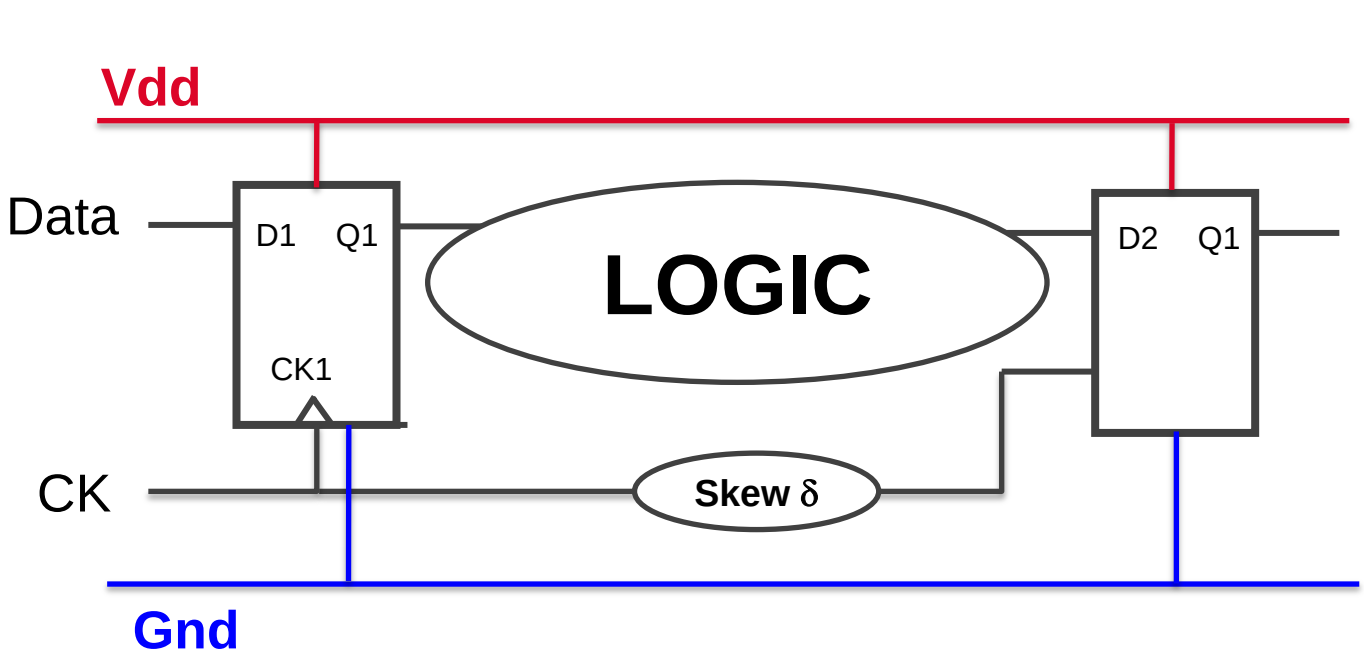
Outline

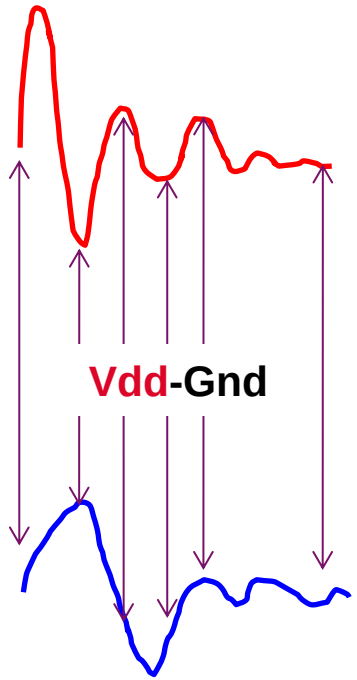
1. State of the Art
2. Timing faults
3. Motivations
4. Enhancing EM injectors
5. Experimental results
6. Conclusions

State of the Art

2002	**[1]** J.J. Quisquater, D. Samyde **'Eddy current for Magnetic Analysis with Active Sensor' (Esmart 2002)**	EM injection allows disrupting the behavior of embedded memories
2007	**[2]** J.-M. Schmidt, M. Hutter **'Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results' (Austrochip 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)**	Harmonic EM Injection modifies the ***propagation delays*** of logical paths
2011	**[4]** F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine "**Local and Direct EM Injection of Power Into CMOS Integrated Circuits (FDTC 2011)**	Harmonic EM Injection modifies the behavior of clock generator **(frequency)**
2012	**[5]** P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine '**Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator' (COSADE 2012)**	Harmonic EM Injection modifies the behavior or RO based TRNG **(phase locking)**
2012	**[6]** A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria '**Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system' (ePrint 2012)**	Pulsed EM Injection produces ***timing faults*** during the course of hardware cryptographic modules
2012	**[7]** A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria '**Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES' (FDTC2012)**	Pulsed EM Injection produces ***timing faults*** during the course of hardware and software …
2014	**[8]** 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)**	Evaluation of a countermeasure based on the ***timing slack monitoring***

EM Injection





$$[CK1 \nearrow > Q1 \nearrow] + [Q1 \searrow > D2 \nearrow] < T_{CK} - \delta \searrow - T_{SETUP2} \nearrow$$

EM Injection produces Setup time constraint violations

Motivations

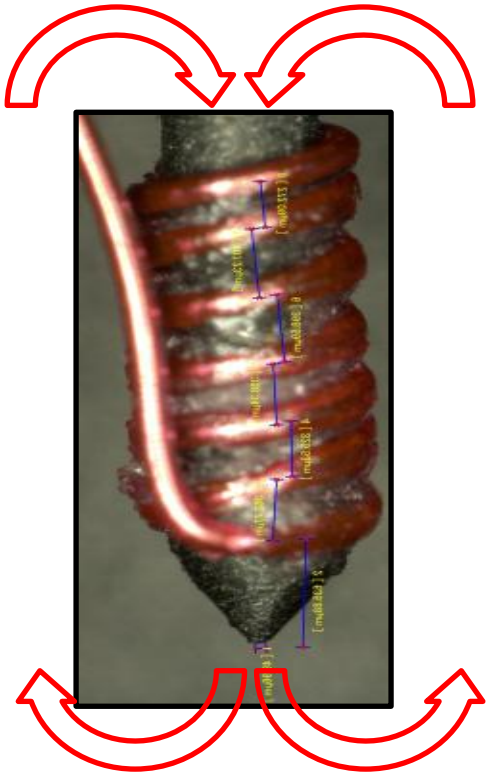
Does EM injection only produce timing faults ?

In that case EM Injection has a limited interest for smartcard evaluation !

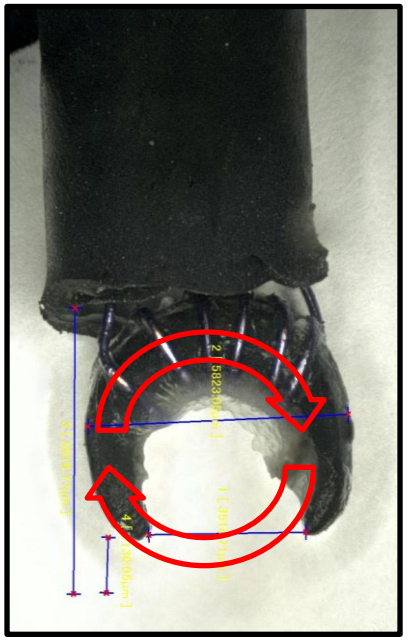
Does EM injection produce bitsets and bitresets ?

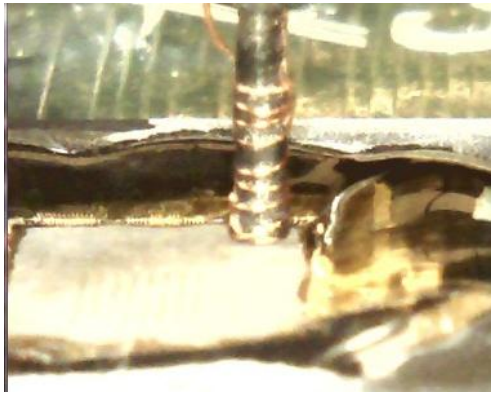
In that case EM Injection has much more interest for smartcard evaluation !

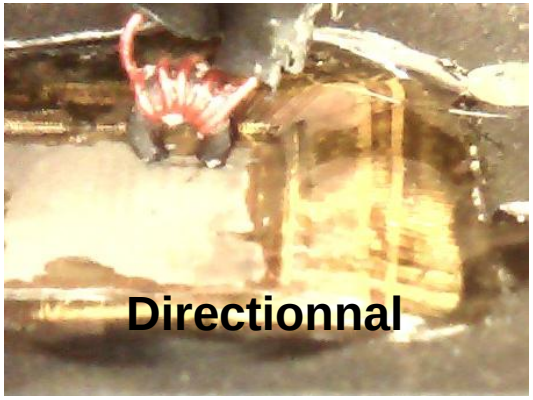
EM Injection Platform : probe



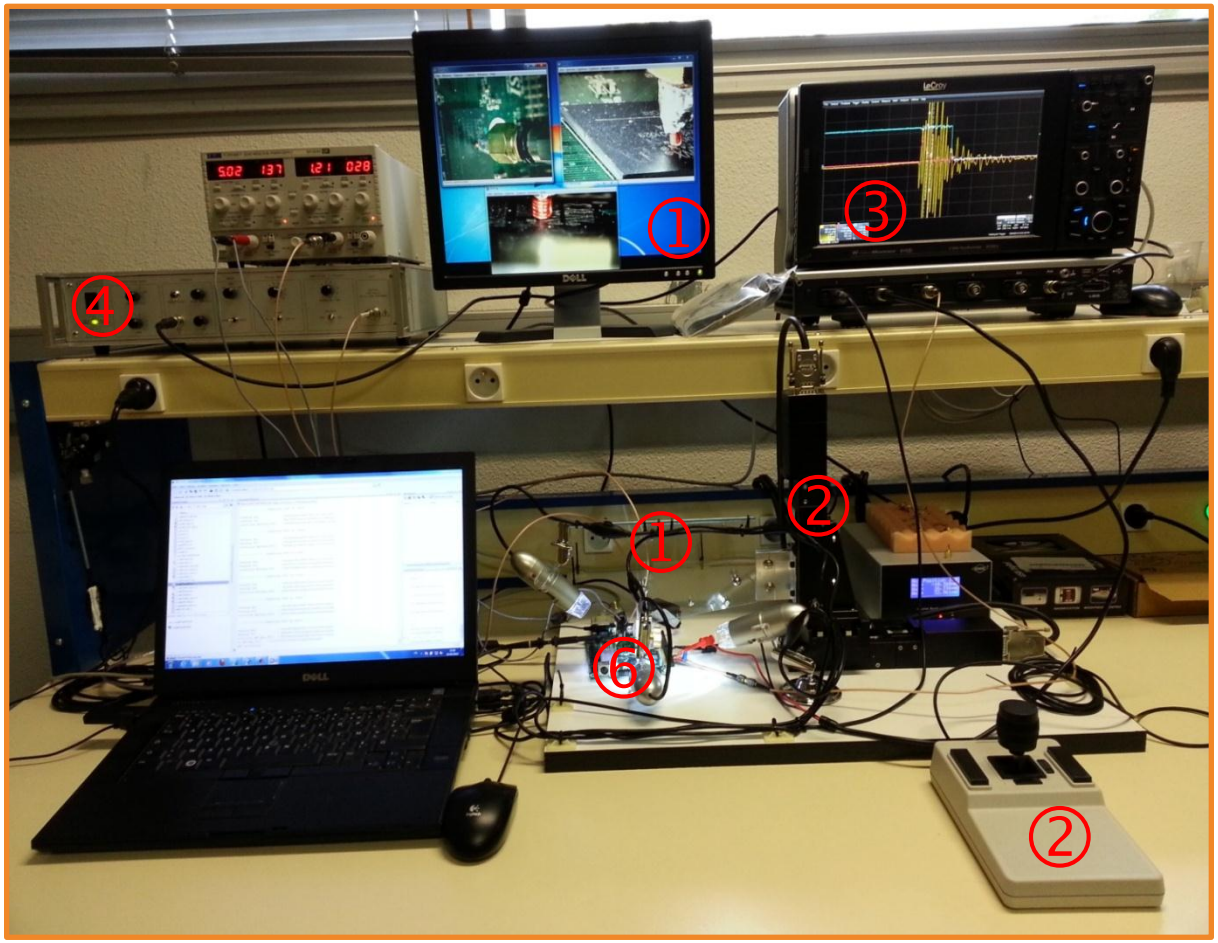
Concentrate the magnetic field lines on a reduced area of the IC surface using concentric field lines







EM Injection Platform : overview



① 3-axes vision system

② 3-axes positioning system

③ Oscilloscope

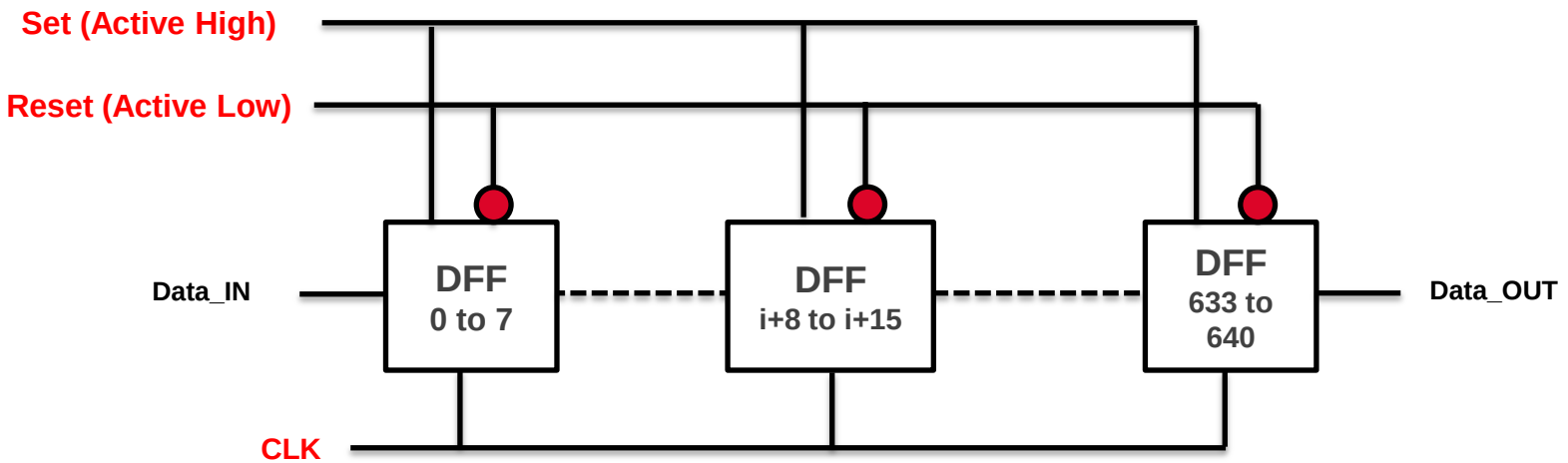
④ Pulse generator

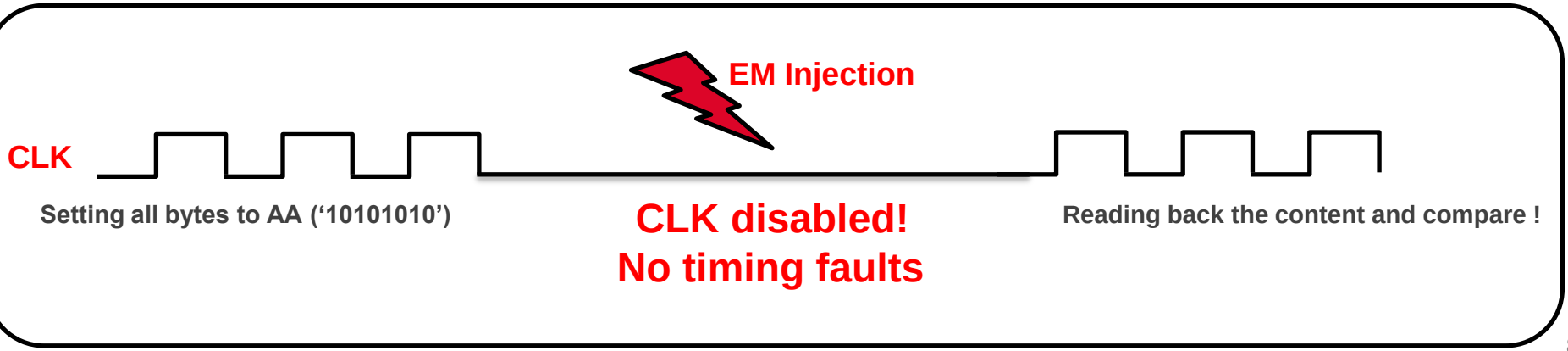
⑥ Hand made injection probes

⑦ a laptop

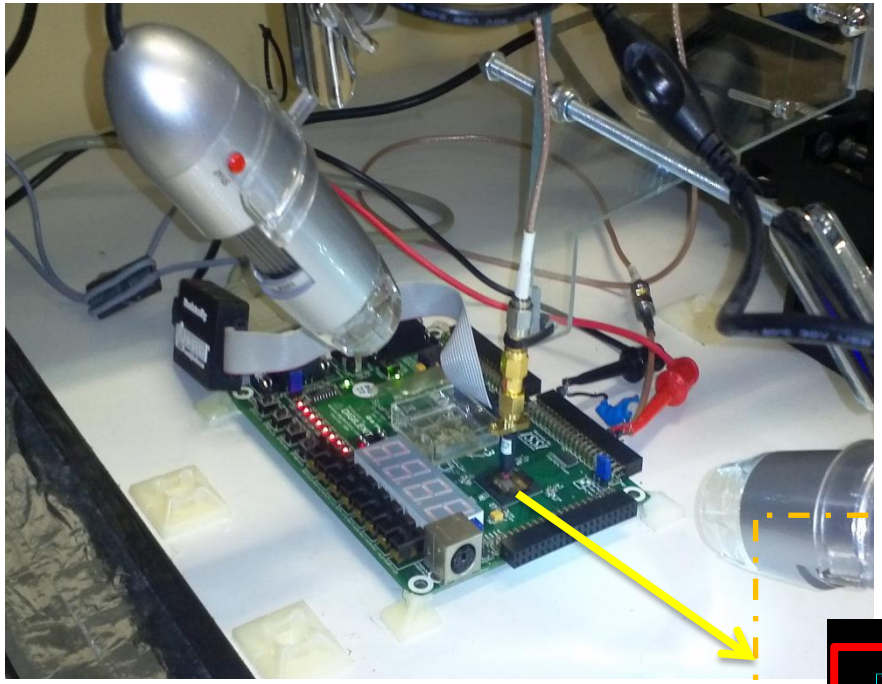
Bitsets and Bitresets ?

To evaluate if EM pulsed Injection may produce some Bitsets and Bitresets requires avoiding the occurrence of EM timing fault !





Bitsets and Bitresets ?



FPGA xilinx

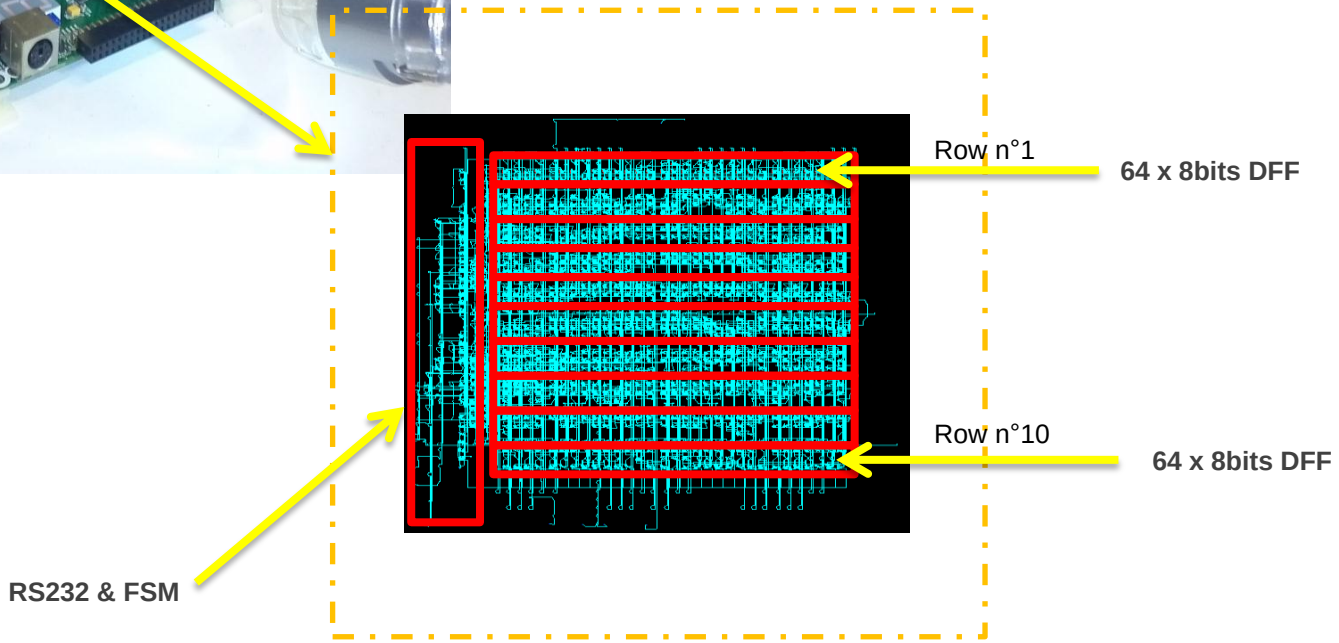
Fck = 50MHz when active !!

Vddcore = 1.2 V (nominal)

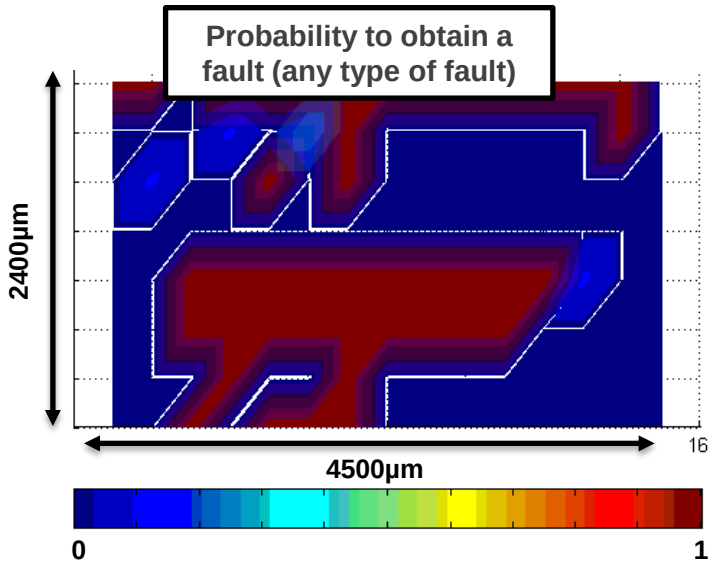
Decapsulated IC

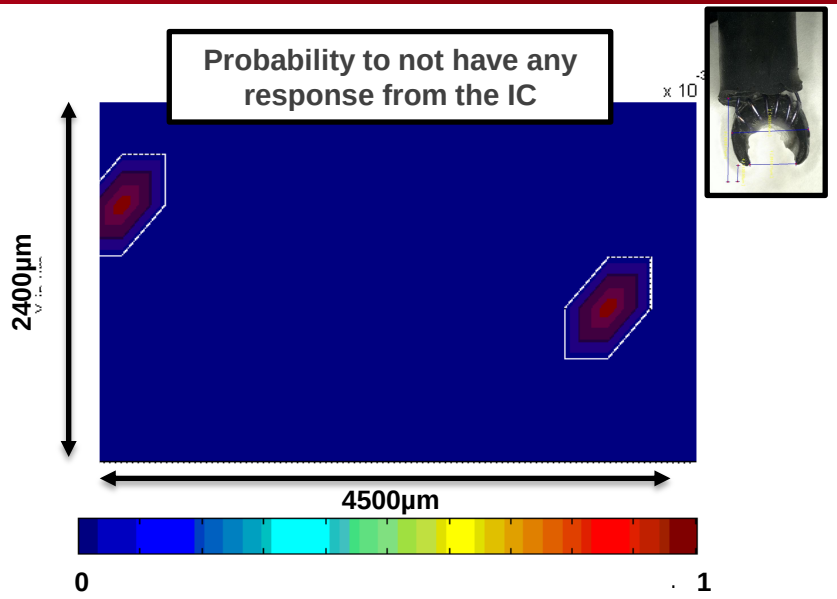
Handmade probe (with a ferrite core)

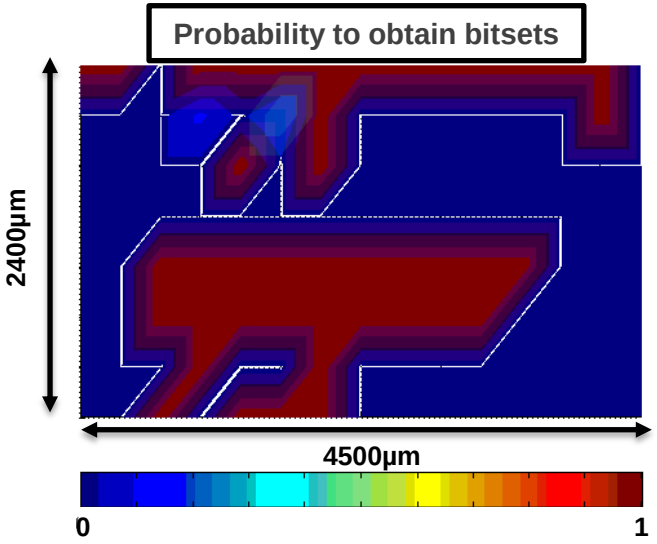
Injection probe in contact with the IC surface



Bitsets and Bitresets ? 1st Cartographies



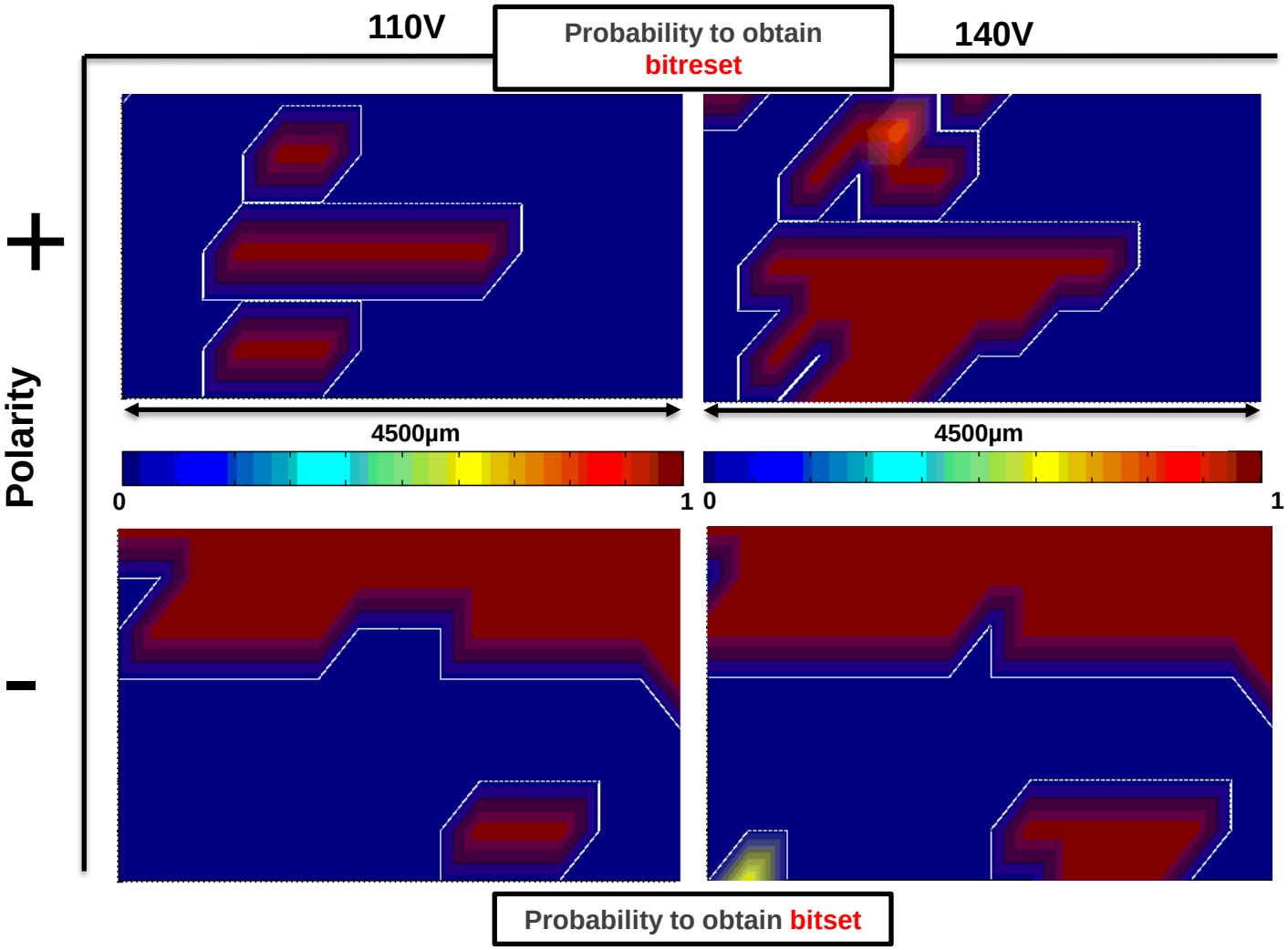


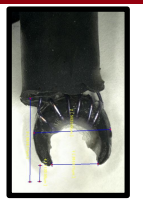


Pulse width = 8ns
Pulse amplitude = 170V
Polarity = Positive

2 types of faults:
- **Bitsets**
- **No response**

Bitsets and Bitresets : effect of pulse polarity !





Probability to obtain a bitset =0

Set signal active high

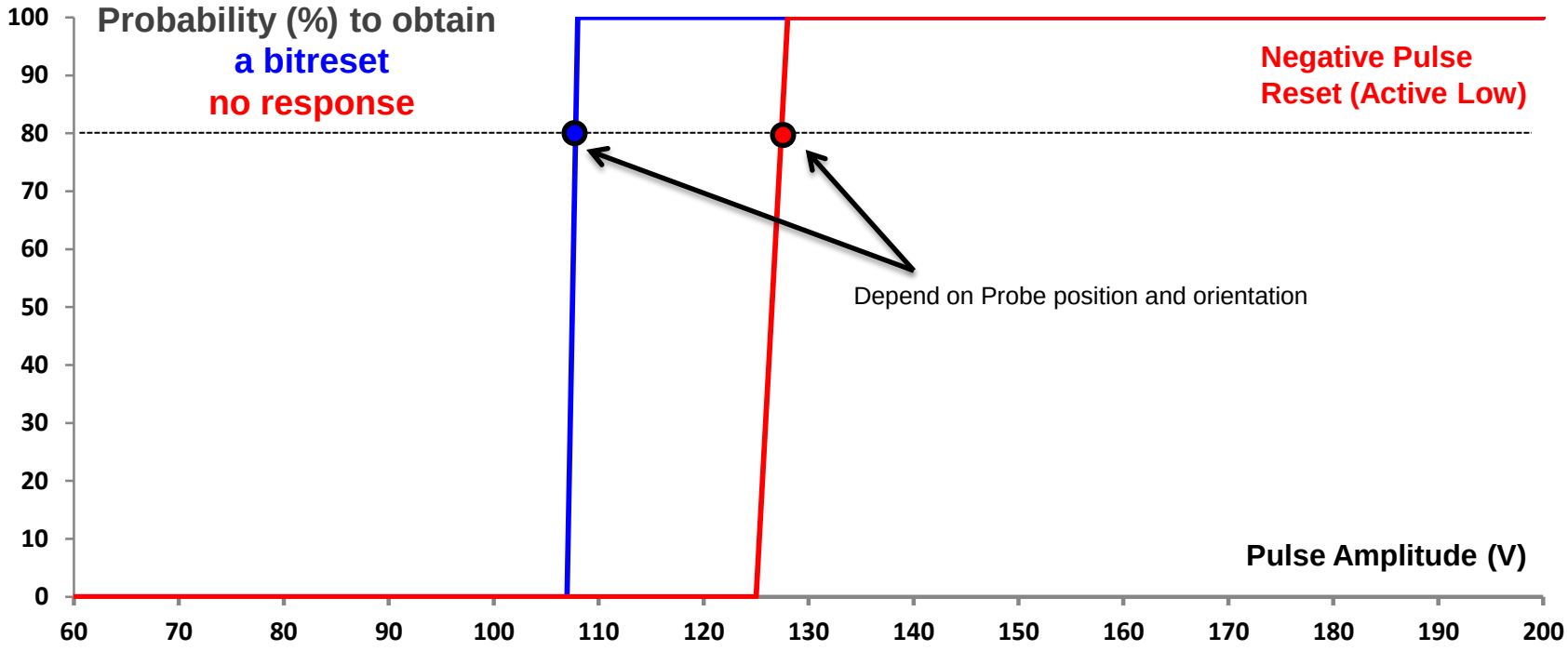
Probability to obtain a bitreset=0

Reset signal active low

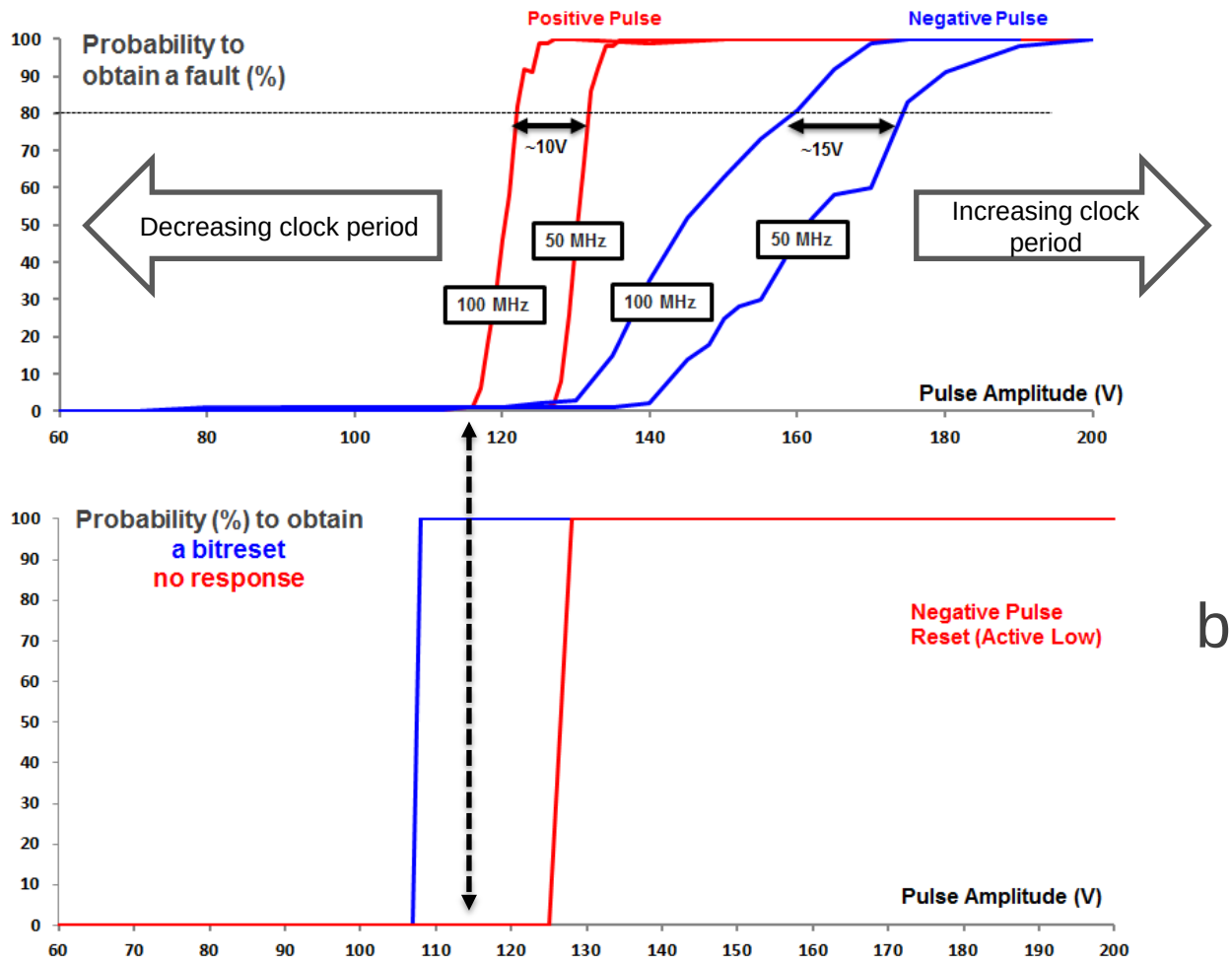
Overshoots on Gnd and Undershoots Vdd ?

Bitsets and Bitresets : pulse amplitude!

FPGA xilinx
Fck = 50MHz when active !!
Vddcore = 1.2 V (nominal)
Decapsulated IC
Handmade probe (with a ferrite core)
Injection probe in contact with the IC surface



Bitsets and Bitresets and timing faults ?



It is not so clear that timing faults appear before bitsets and bitsets !

Conclusions

1. Polarity of EM injection is important
2. EM injection has a local effect
3. EM injection produces timing faults
4. EM injection also produces bitsets and bitresets
5. It is not so clear that bitsets and bitresets appear after or before timing faults (it should depend on timing slack)