# Electromagnetic Transient Faults Injection

- **Amine Dehbaoui**
- Bruno Robisson
- Assia Tria

- Jean-Max Dutertre

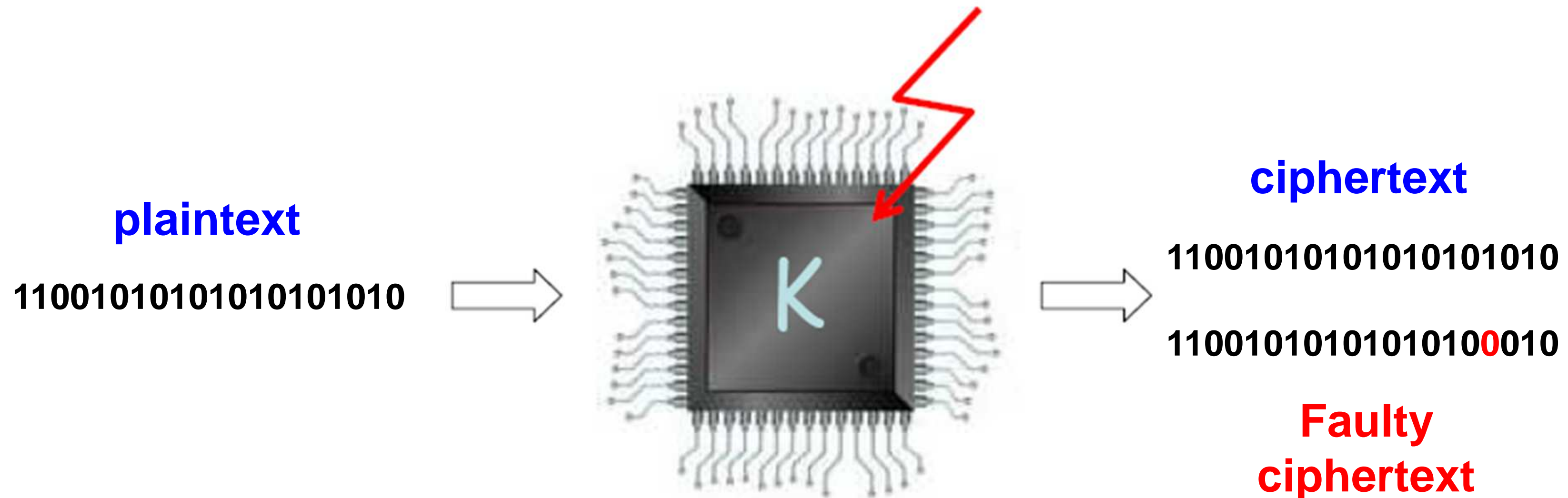
- François Poucheret
- Philippe Maurine

amine.dehbaoui@cea.fr



International Workshops on
Cryptographic Architectures Embedded in Reconfigurable Devices
Chateau de Goutelas, Marcoux, France - June 19-22 2012

# Fault Attacks




- **Modifying the behavior** of the chip and recovering sensitive data
- Various experimental setups are used
- **Underpowering** / **overclocking** a device
- A **rise in temperature** may also induce faults
- The use of **optical radiations** : flash bulb, laser beam

# Motivations for EMP Injection

- Does not require depackaging the target
- Does target the upper metal Layer (Vdd, Gnd, Clk)
- May bypass some countermeasures (light sensors, global power filtering …)

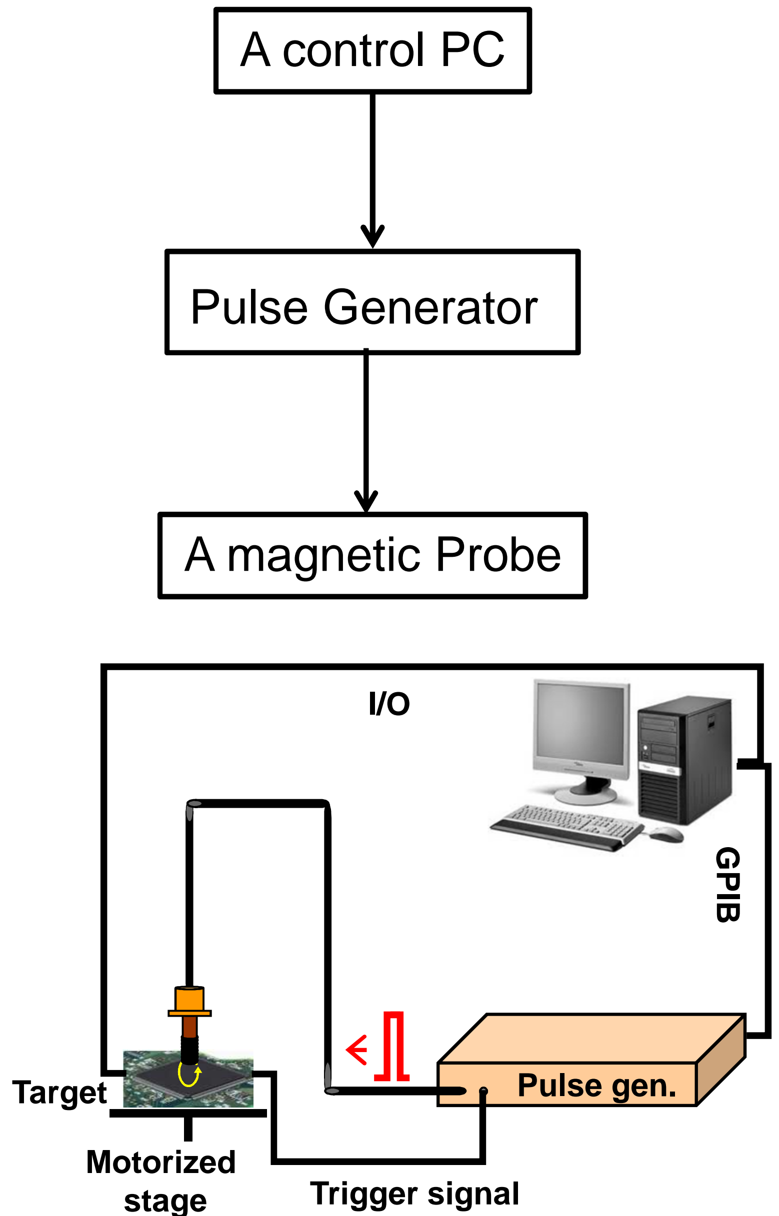
Seems adequate to inject fault
in Secure SoC designed with
advanced technologies !

Access to backside is
difficult !
BGA packages !!!

# Agenda

- What is an EMP platform ? Is it low Cost ?
- Does it always work ?
- What is the effect of an EMP on IC?
- What is the resolution of an EMP ?

# EMP platforms




**Low Amplitude Pulses (CEA-EMSE)**

- Amplitude : 1 V - 100 V
- Pulse width : 1ns – 1 ms
- rising / falling times : 5 ns
- Very low jitter : < 45 ps

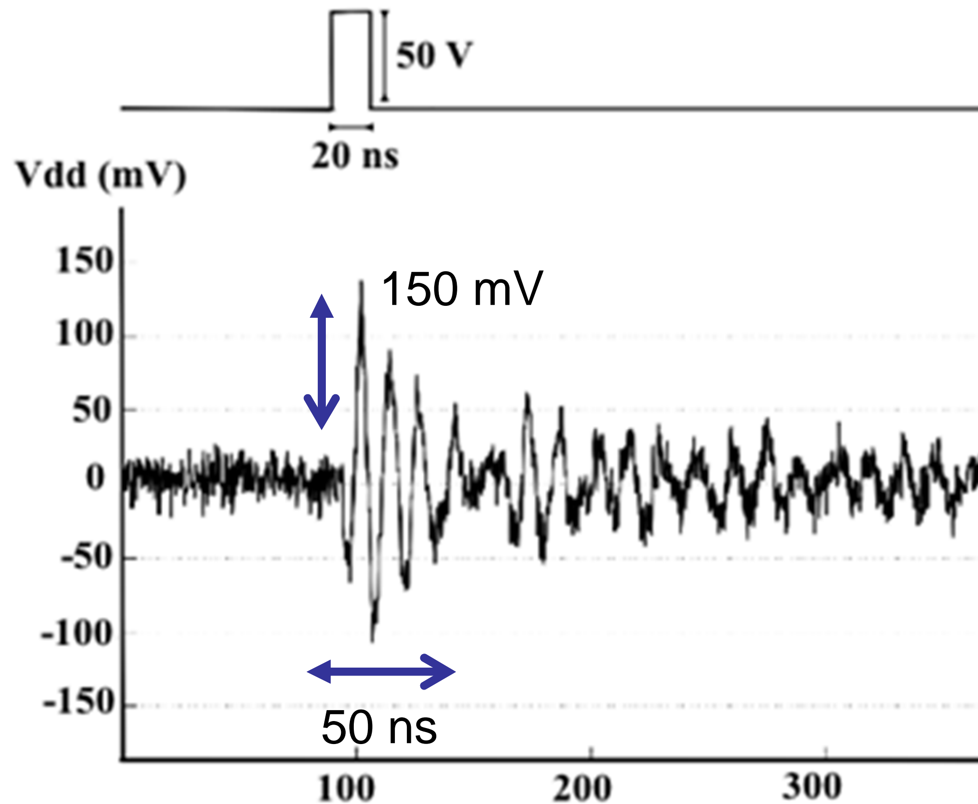
- Rohde & Schwartz magnetic antenna (500µm diameter)

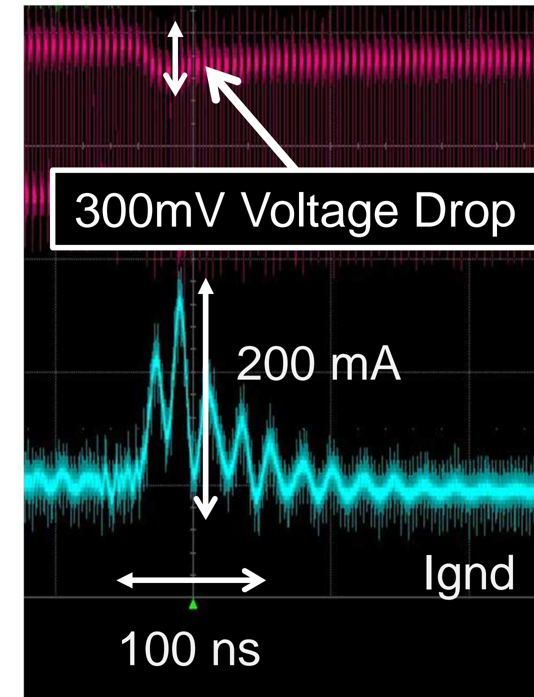
**High Amplitude Pulses (LIRMM)**

- Amplitude : 100 V – 1.2 KV
- Not Available on the market
- Must be home made

According to the forwarded power

# EMP Injection : Observation




Low Amplitude Pulses :

- DeltaV= 50V
- Width = 20 ns
- 150 mV Voltage Drop

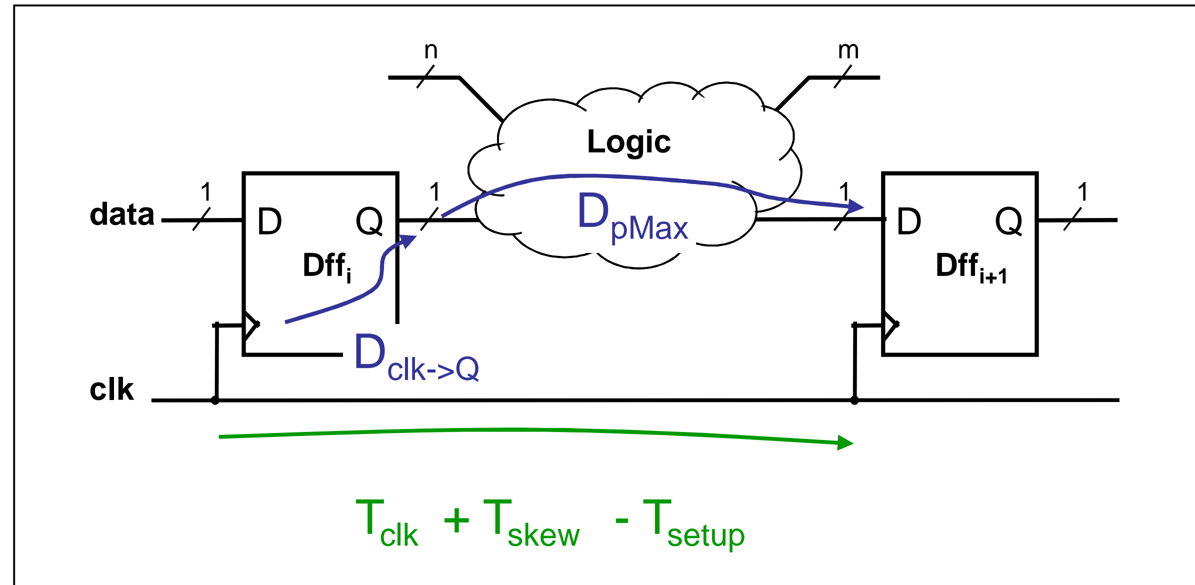
High Amplitude Pulses :

- DeltaV= 900V
- Width = 250 ns
- 300 mV Voltage Drop

Are these voltage drops sufficient to induce faults into calculations ?

# EMP Injection : Design considerations

$$Delay \approx a \cdot \tau \cdot \frac{C_L}{C_{IN}} \qquad \tau = \frac{2 \cdot L^2}{\mu \cdot} \cdot \frac{V_{DD}}{(V_{DD} - V_t)^2}$$




data arrival time $= D_{clk\text{->}Q} + D_{pMax}$

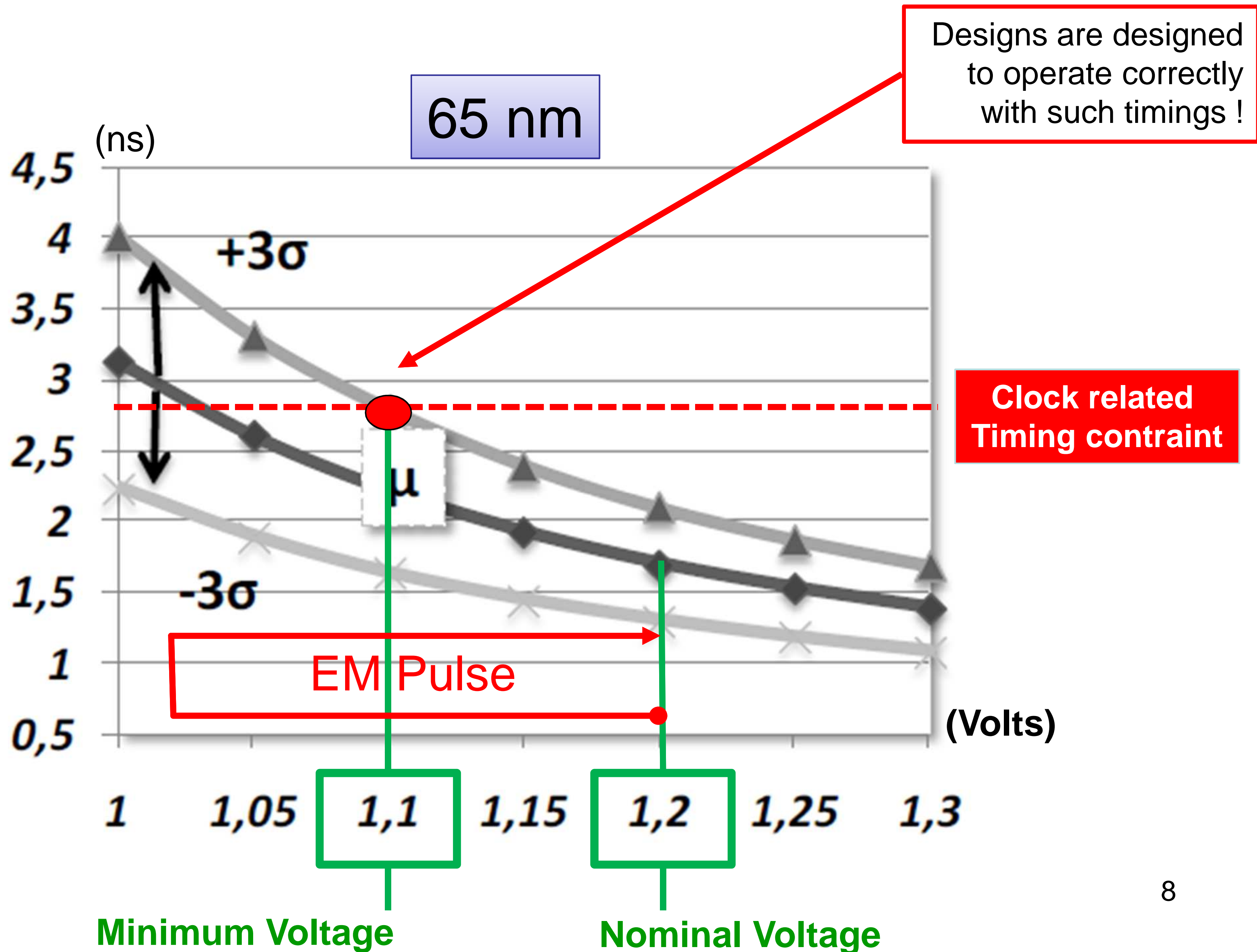
data required time $= T_{clk} + T_{skew} - T_{setup}$

$\Rightarrow$ $T_{clk} > D_{clk\text{->}Q} + D_{pMax} - T_{skew} + T_{setup}$

$T_{slack} = T_{clk} - ( D_{clk\text{->}Q} + D_{pMax} - T_{skew} + T_{setup} )$

Violating this timing constraint results in fault injection.
Usually IC are designed to tolerate : **Vdrops < 0.1 x Vdd !!**

# EMP Injection: Effect

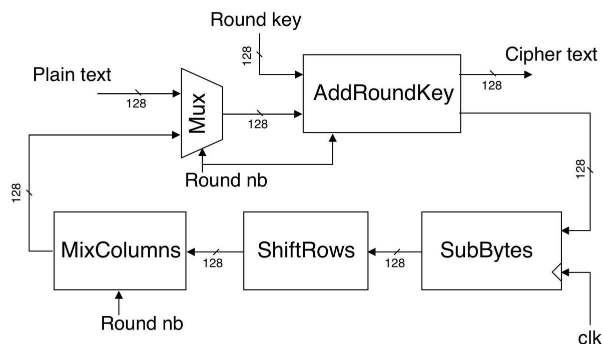


# Validations & Experimental Results

## Experiments

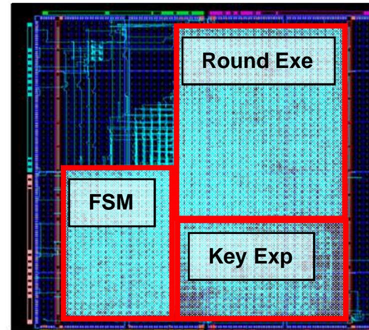
### 1. Hardware AES 100 MHz

- Xilinx Spartan 3
- Core supply : 1.2 Volts
- Clock speed : 100 MHz
- **Tslack = 2 ns**



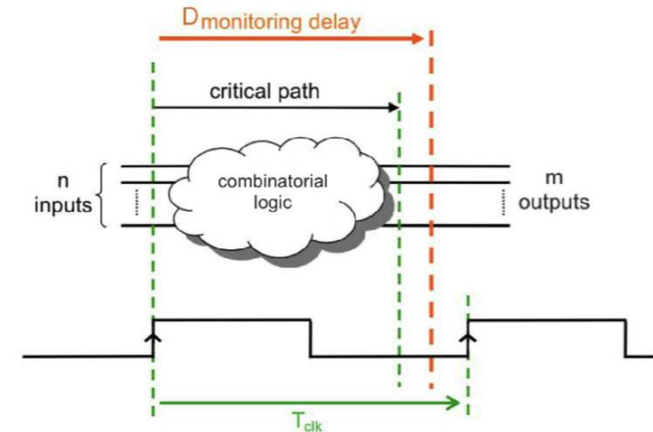

### 2. Hardware AES 50 MHz

- Xilinx Spartan 3
- Core supply : 1.2 Volts
- Clock speed : 50 MHz
- **Tslack = 10 ns**




### 3. Hardware AES 100 MHz + CM

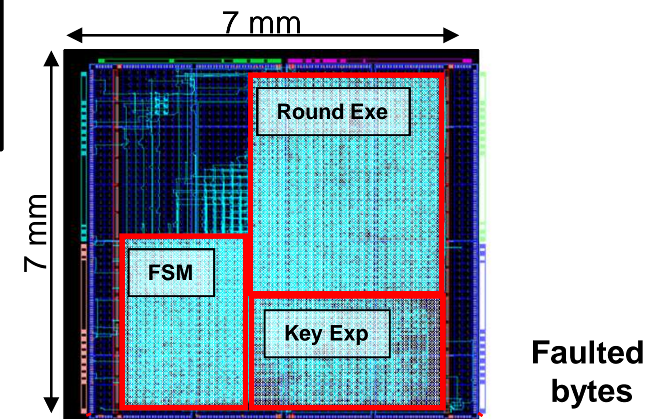
- Xilinx Spartan 3
- Core supply : 1.2 Volts
- Clock speed : 100 MHz
- **Tslack = 2 ns**
- Embedded countermeasure
- Detection of timing violations



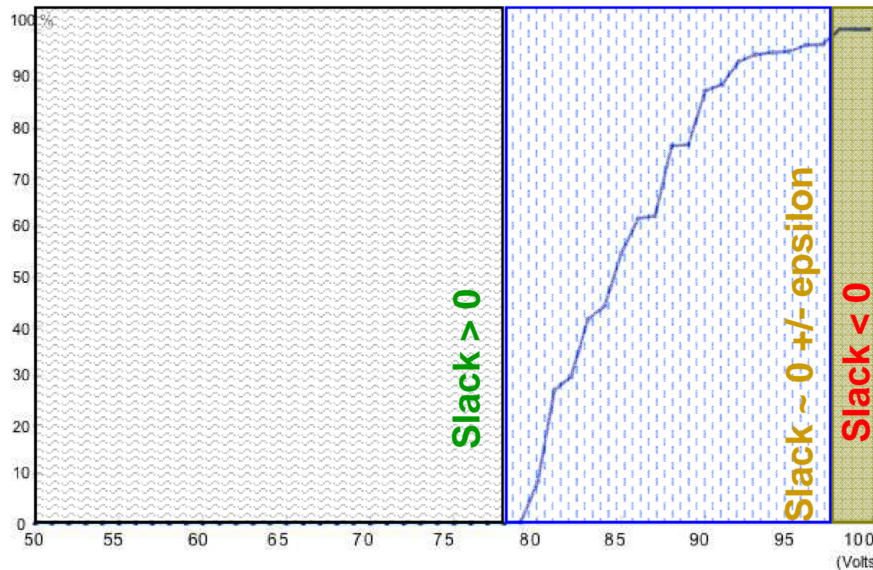
# EMP Injection Cartography

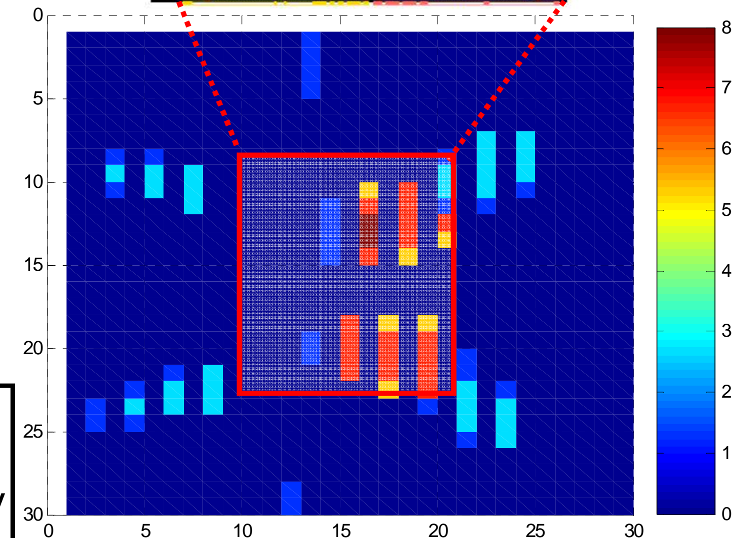
- At each position, an **EMP** is injected **100V-10ns**
- The corresponding faulted ciphertext is retrieved
- **1,000 encryptions** of the same plaintext
- 30x30 different locations
- Antenna **diameter** : **500 µm**
- Displacement **step** : **500 µm**

**Design 1**
**Tslack = 2 ns**




**Occurrence rate of the induced faults versus EMP amplitude**

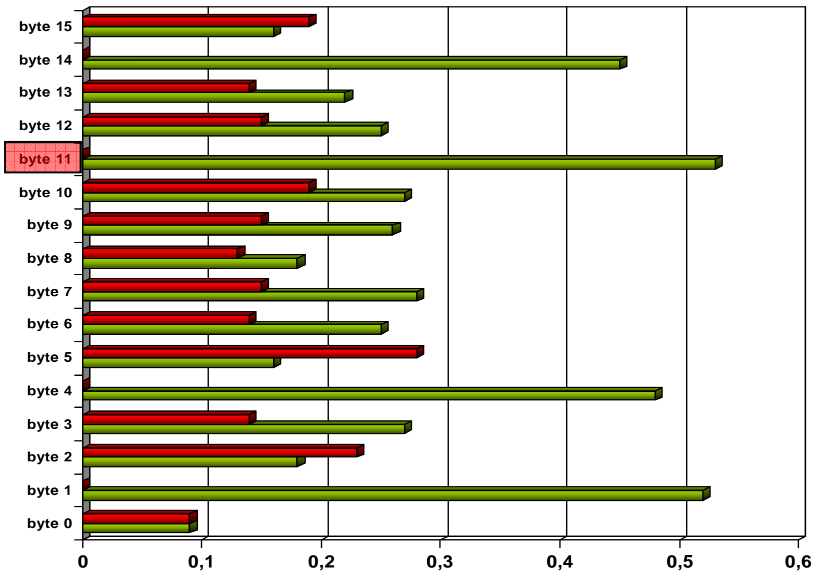


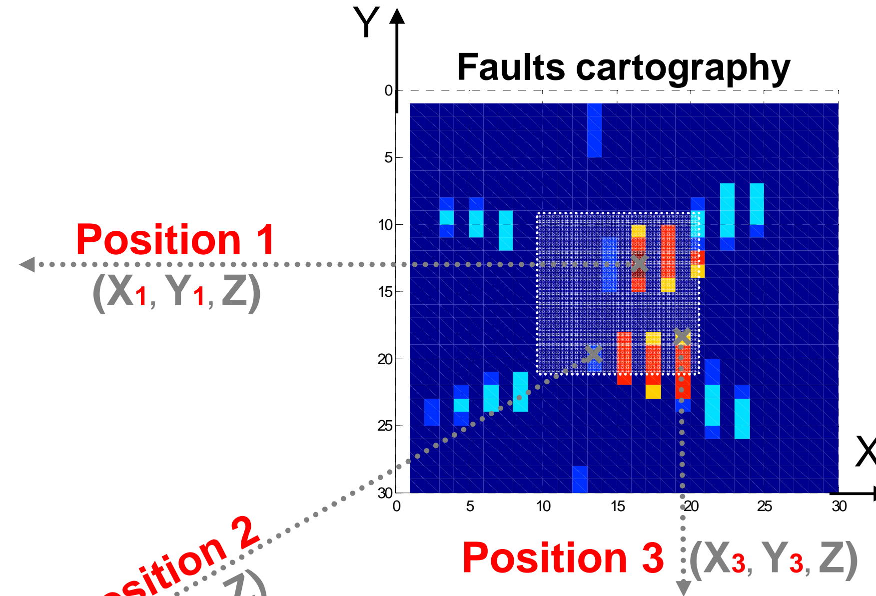



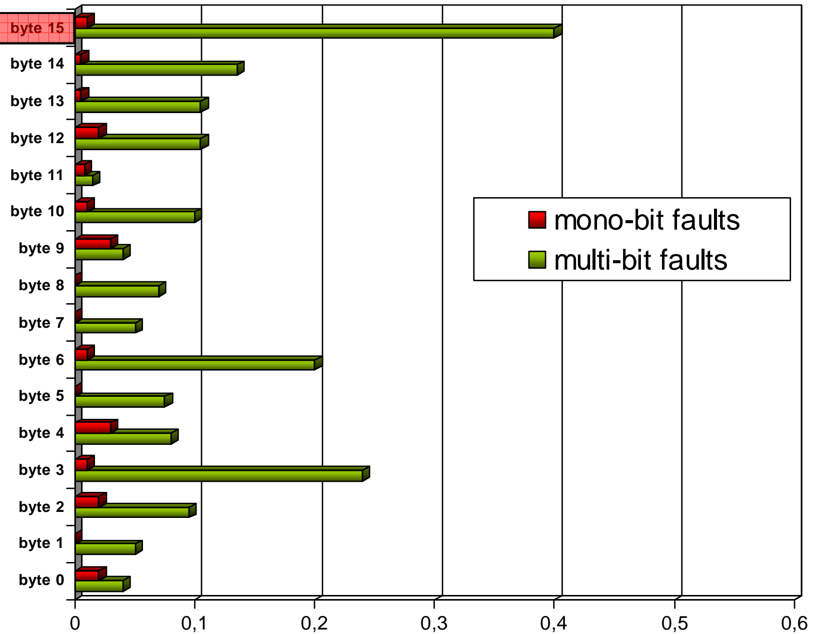

**Faults cartography**

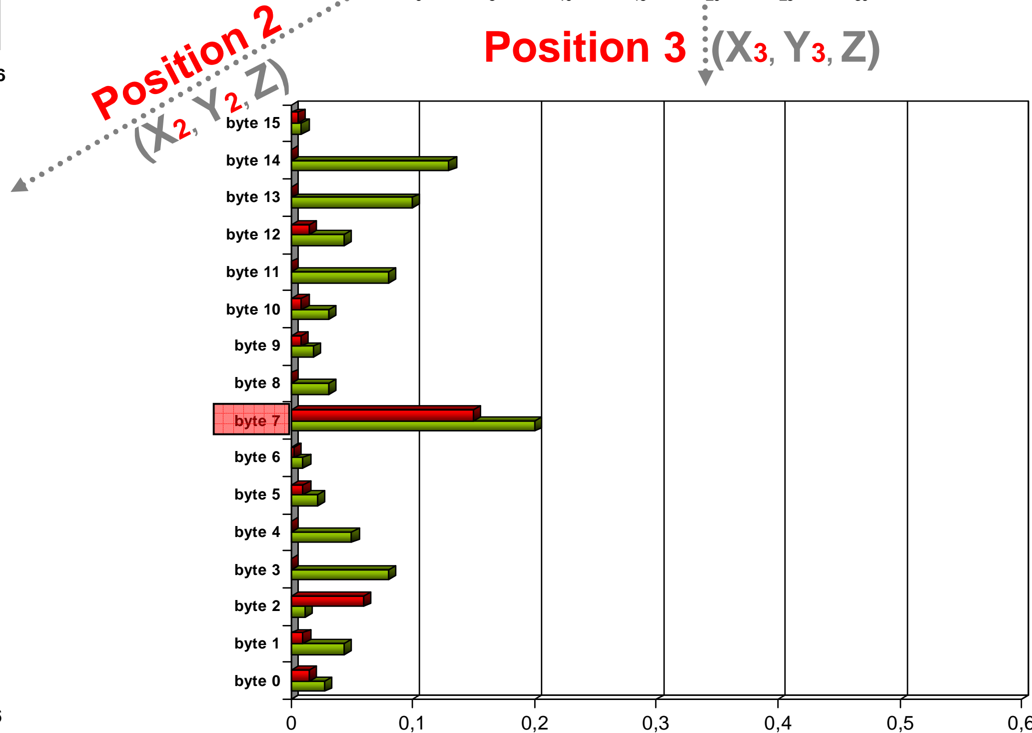
- Localized effect of the **EMP**
- Good correlation between the Floorplan and the cartography
- Deterministic and **reproducible effect**

# Localized Effect of the Voltage Drops



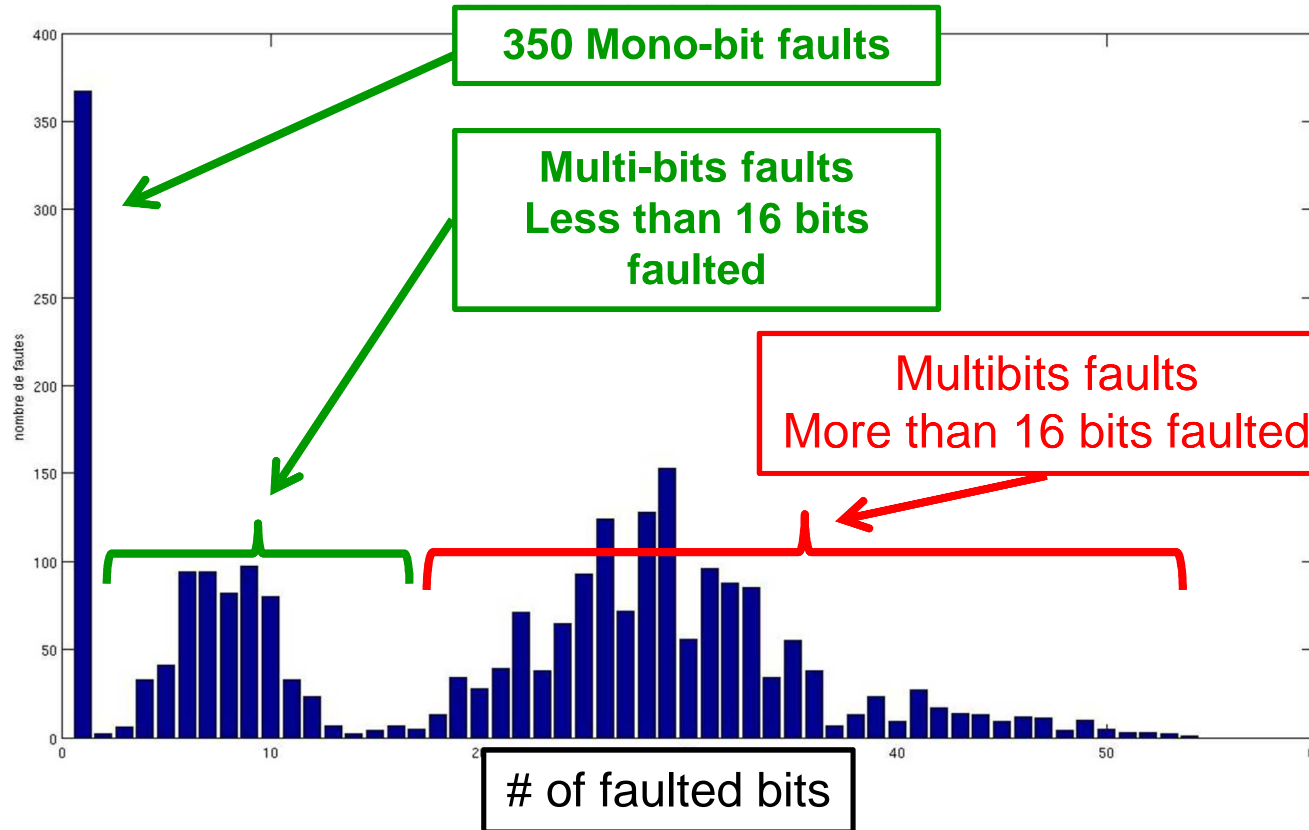



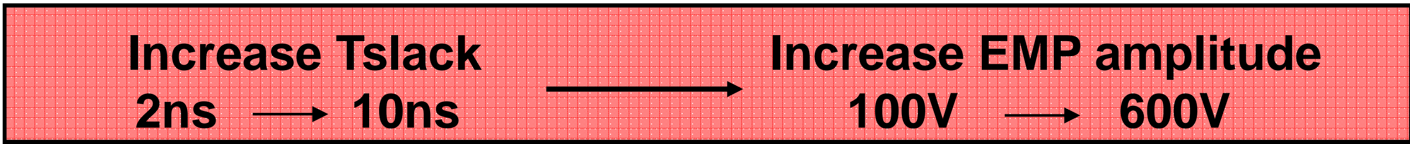



# Validation & Experimental Results

- Xilinx Spartan 3
- Core supply : 1.2 Volts
- Clock speed : 50 MHz
- EMP : 600V

**Design 2**
**Tslack = 10 ns**

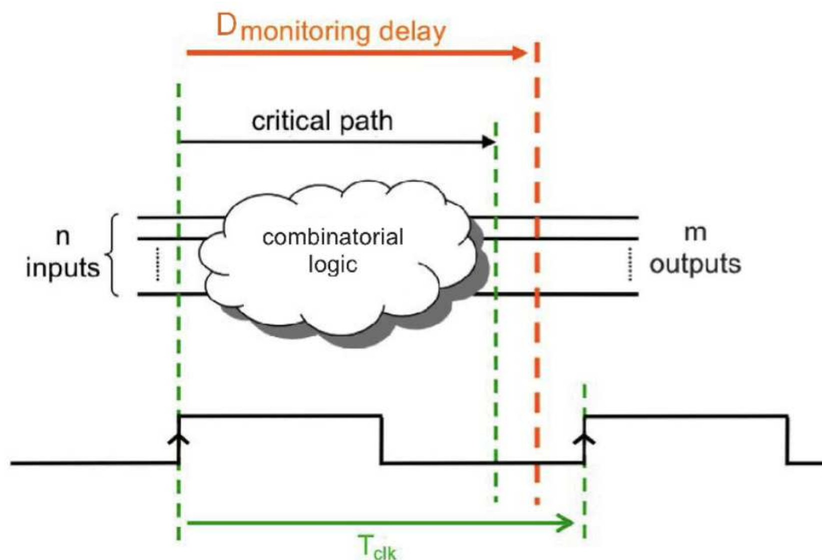


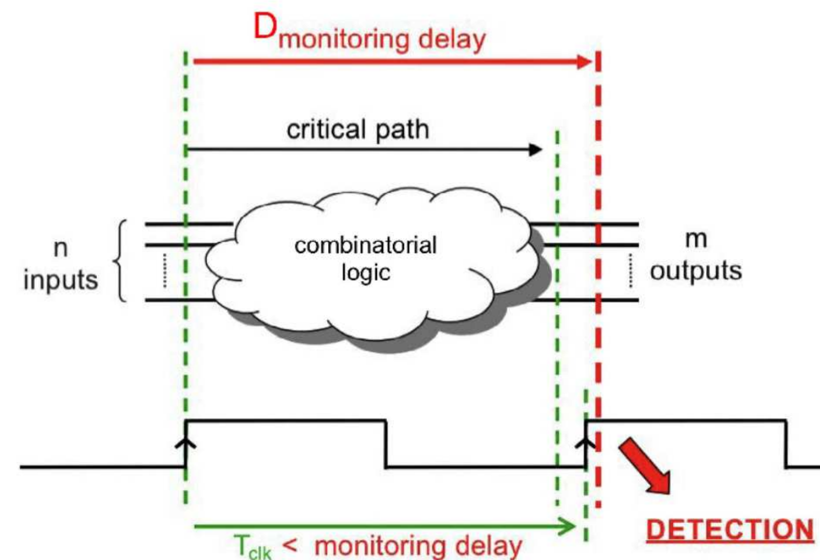



# Voltage Drops Detection

**Design 3**
**Tslack = 2 ns**

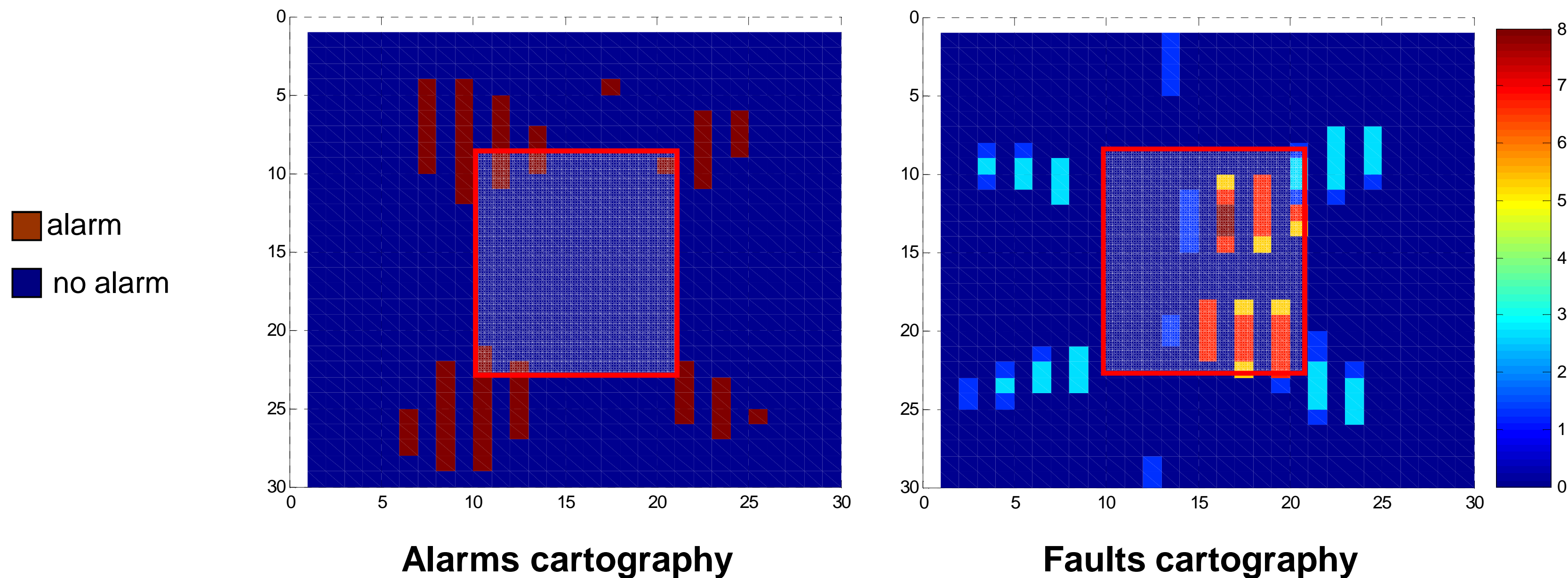
- FPGA Spartan 3 **XC3S1000 FT256**
- Techno **130nm**
- Operating voltage : **1.2 volts**
- Operating frequency : **100 MHz**
- **Hardware AES** implementation
- countermeasure : **monitoring the data path delay**)



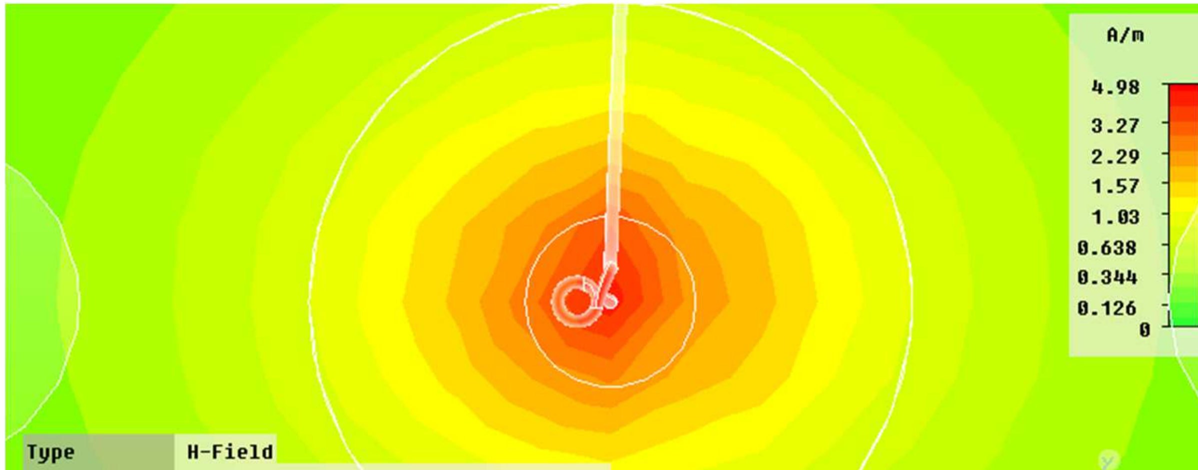
# Voltage Drops Detection

- At each position, an **EMP** is injected
- The corresponding faulted ciphertext (if any) is retrieved
- The value of the alarm flag is stored
- **1,000 encryptions** of the same plaintext
- **30x30 different locations** of the injection probe (step 500 µm)

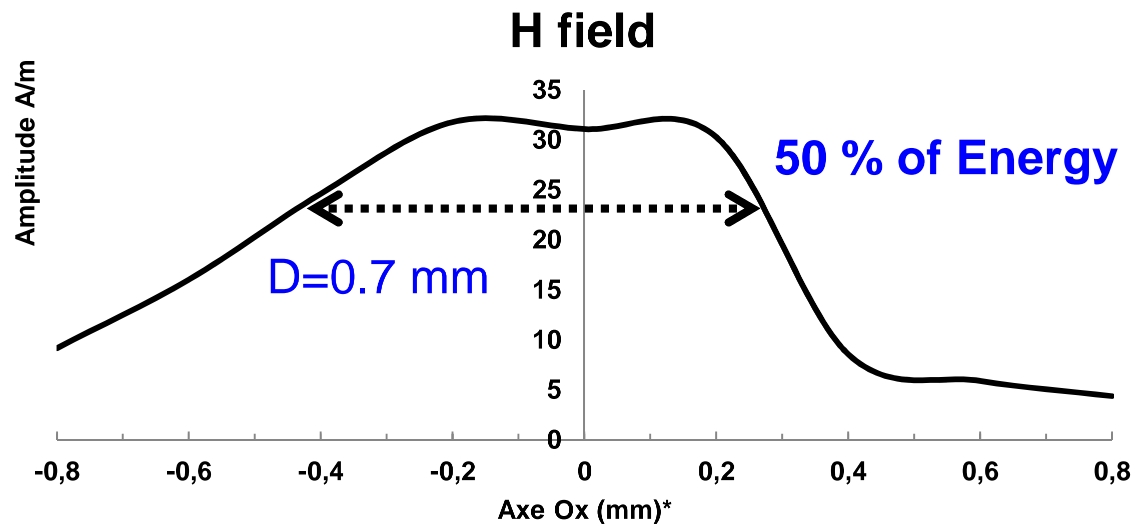



- Localized effect of the **EMP**
- The EMP is detected only in some positions
- Possibility to induce faults without triggerring the alarm

# Spatial Resolution ?




**CST simulations H field**
**1 turns / ∅ 100 µm**
**200 µm below the probe**




**Resolution of EMP Injection depends also on the IC !**

# Conclusion & Further works

- Ability to inject **single-bit** and **multi-bits** faults into AES calculations
- **Induced faults are timing faults due to voltage drops**
- **EMP amplitude depends on Timing slack (IC frequency and technology)**
- **Localized effect** : the coupling depends of the IC Layout
- May **bypass** power supply low-pass **filtering**
- May fault any paths (even non critical paths)