

Injection EM: du modèle de faute à une contremesure

P. Maurine

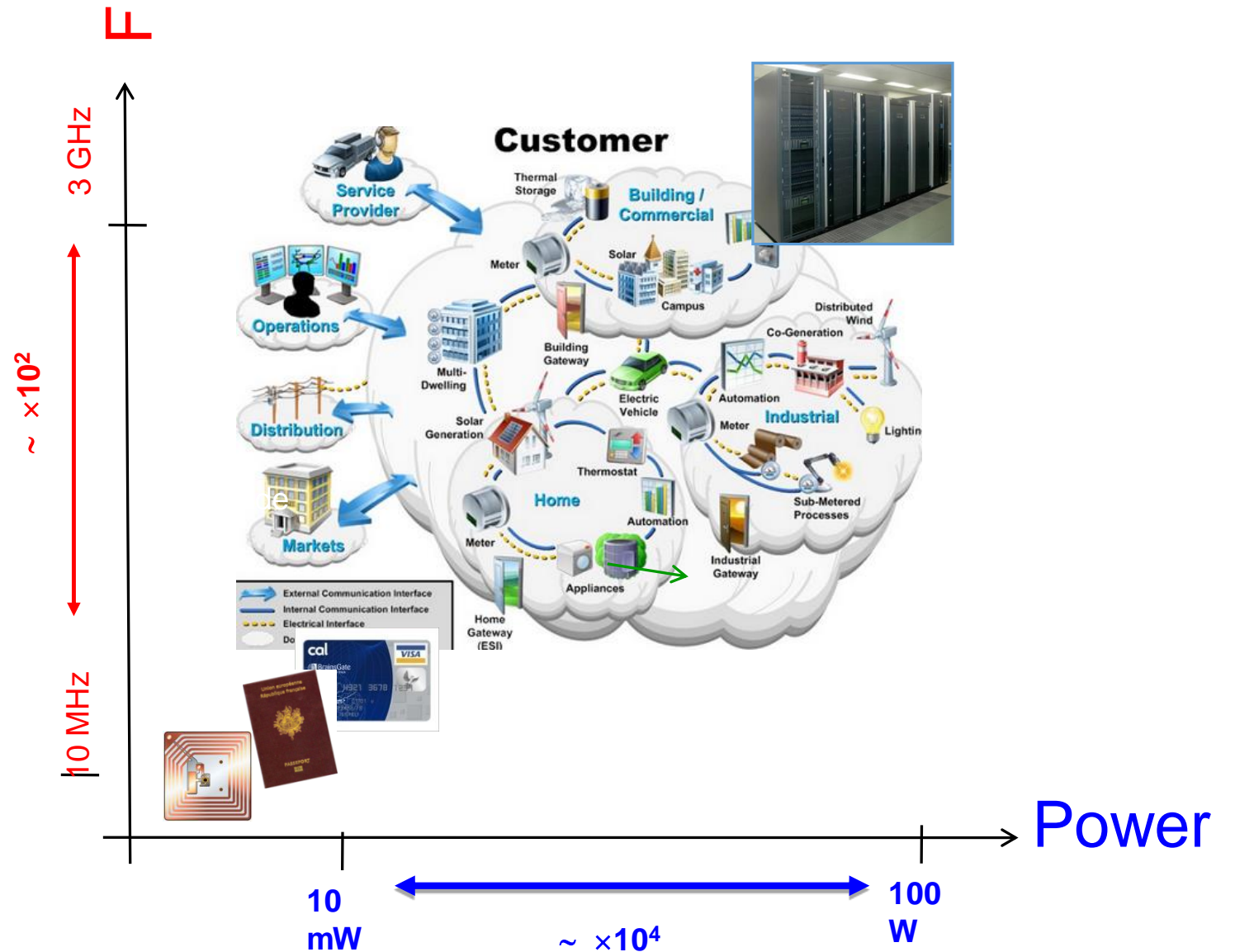


Menaces **concrètes** sur les biens et les personnes

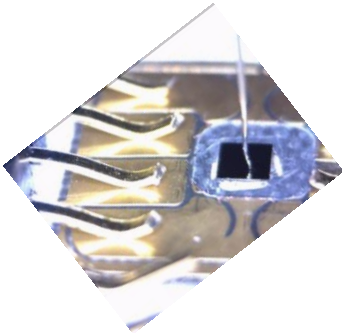
Usage massif de cryptographie (légère ou non) pour garantir la sécurité et la sûreté de fonctionnement

Les circuits et systèmes intégrés sont LE support de l'information et de la cryptographie

Facteur de forme (taille et encapsulation) divers, performance et complexité diverses !

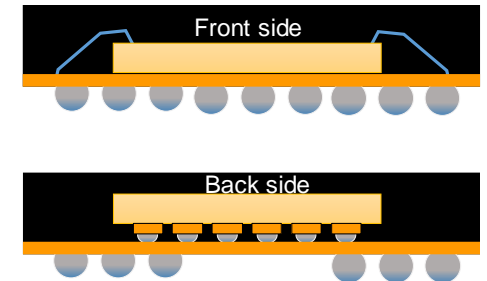


Motivation initiale pour l'injection EM (2009-2010)



~100 kgates, ~ 30 MHz, ~ 2 mm²
~ 90 nm / 4-5 metal Layers
~ 2-3 domaines d'horloge
~ 1 domaine d'alimentation
+ Contremesures dont des capteurs de tirs laser

~ 1 M gates, ~ 1 GHz, ~ **25 mm²**
~ 32-28 nm / 7-12 metal layers
~ 10 domaines d'horloge
~ 2-4 domaines d'alimentation
~ bulk -- FDSOI



Comment injecter des fautes efficacement et simplement dans de tels dispositifs ?

2002

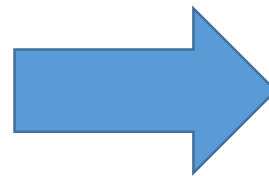
[1] J.J. Quisquater, D. Samyde
'Eddy current for Magnetic Analysis with Active Sensor' (Esmart 2002)

2007

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

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)



ANR ARPEGE EMAISECi
(faisabilité de l'injection EM)

Complexe à maîtriser dans le temps
Faible précision temporelle

2002

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

2007

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

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)

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)

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)

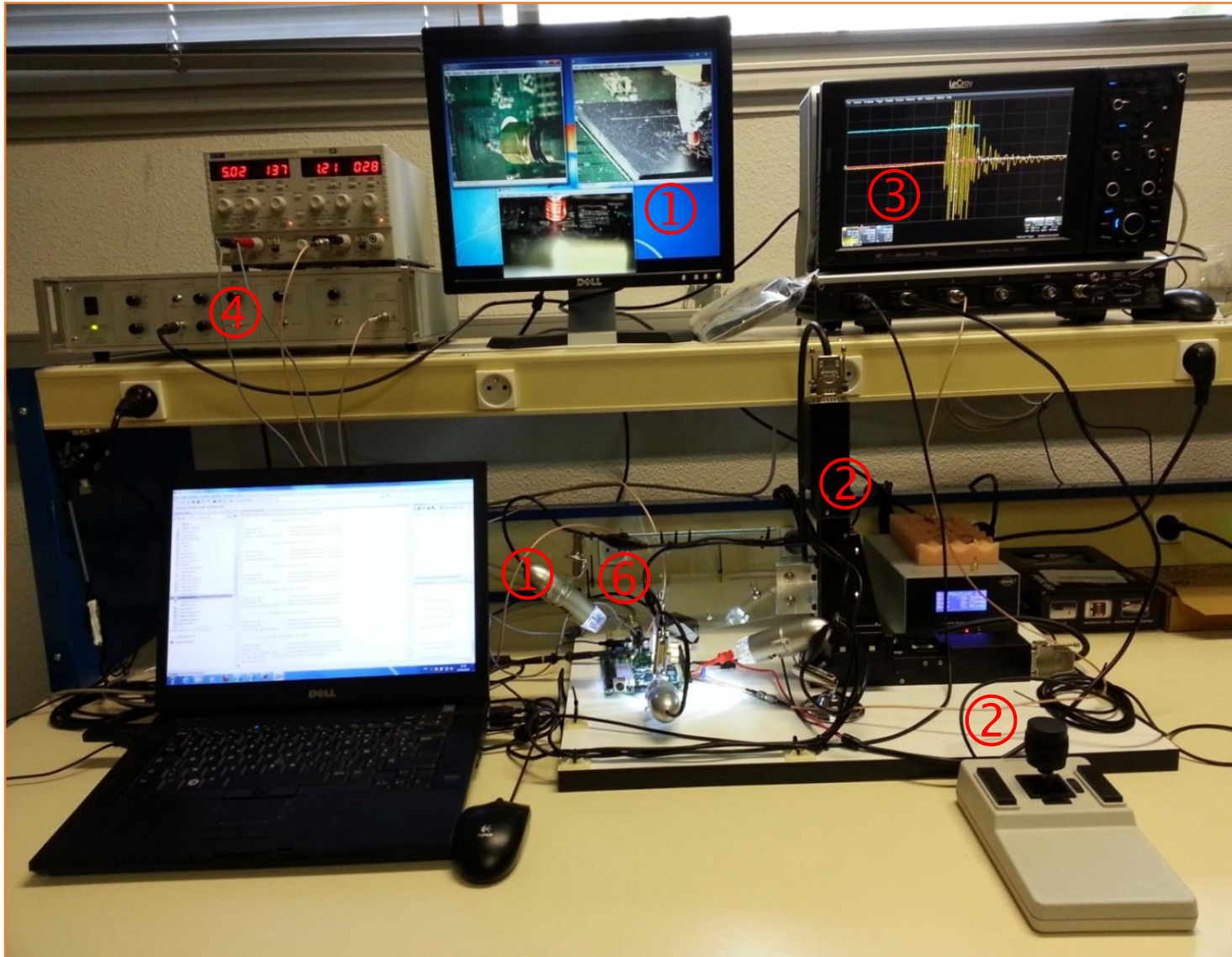
2012

[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)

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)

ANR ARPEGE EMAISECi



① 3-axes vision system

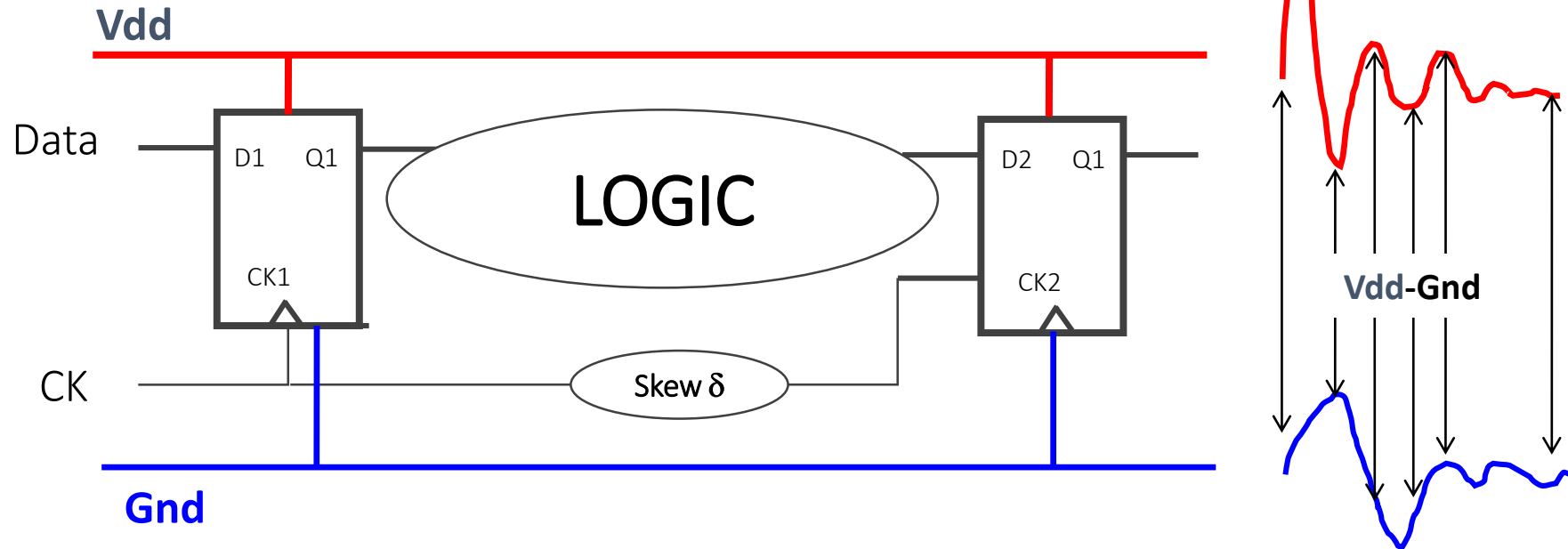
② 3-axes positioning system

③ Oscilloscope

④ High speed voltage pulse generator (200V-8A)

⑥ Basic EM injectors

⑦ a laptop



$$[\underbrace{CK1}_{/} - \overset{\nearrow}{>} \underbrace{Q1}_{/}] + [\underbrace{Q1}_{/} - \overset{\nearrow}{>} \underbrace{D2}_{/}] < T_{CK} - \delta - T_{SETUP2}$$

L'injection EM induit des fautes de timing

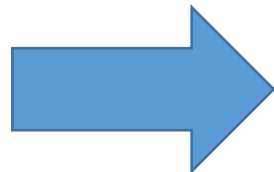
(violations de la contrainte de setup)

Est-ce que l'injection EM n'induit que des fautes de timing ?

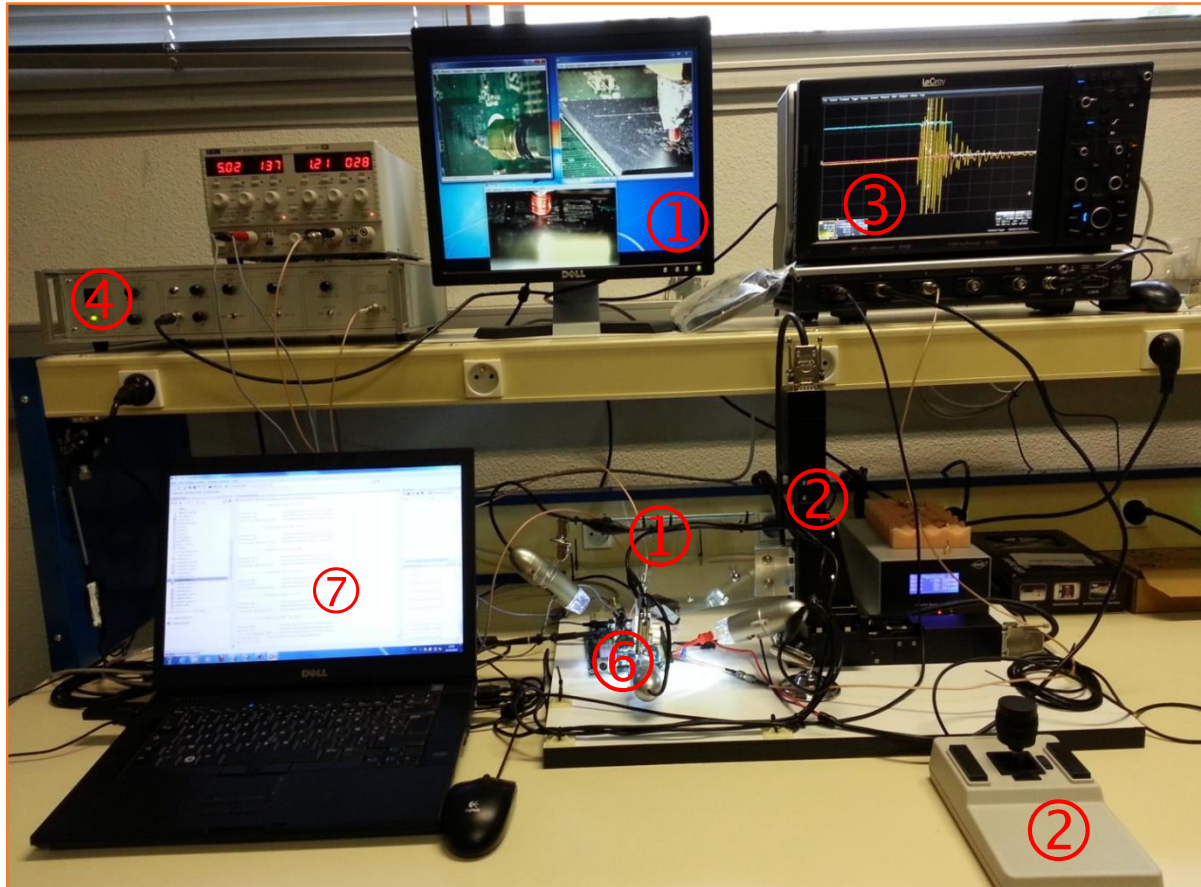
$$\underbrace{[CK1 \rightarrow Q1]}_{/} + \underbrace{[Q1 \rightarrow D2]}_{/} < T_{CK} - \delta - T_{SETUP2}$$

Dans ce cas, c'est une technique limitée ...

Objectif : démontrer que l'injection EM peut induire des bitsets et bitresets !



ANR e-Matahari
(Optimisation des sondes d'injection)



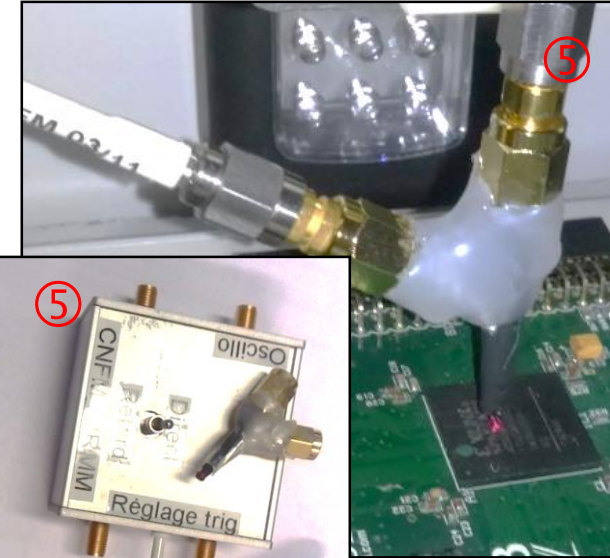
- ① 3-axes vision system
- ② 3-axes positioning system
- ③ Oscilloscope

④ High speed voltage pulse generator (400V-16A)

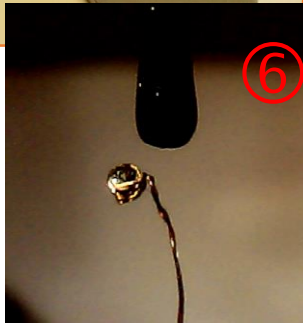
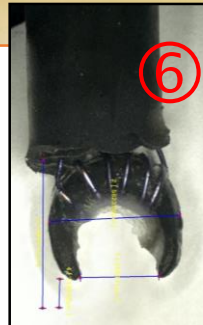
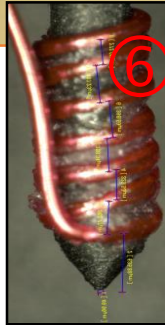
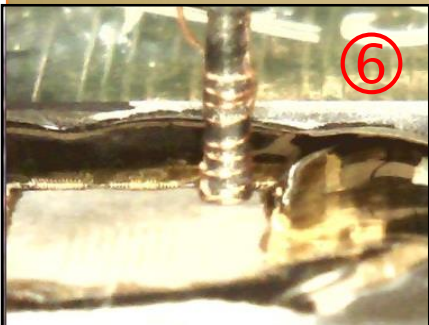
⑤ EM analysis and EMFI coupling system

⑥ Enhanced EM injectors

⑦ a laptop

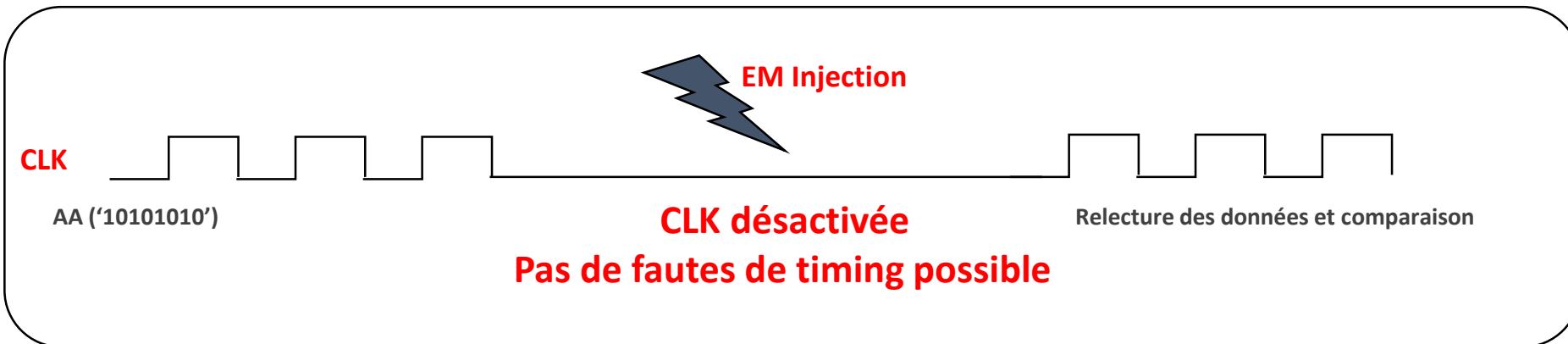
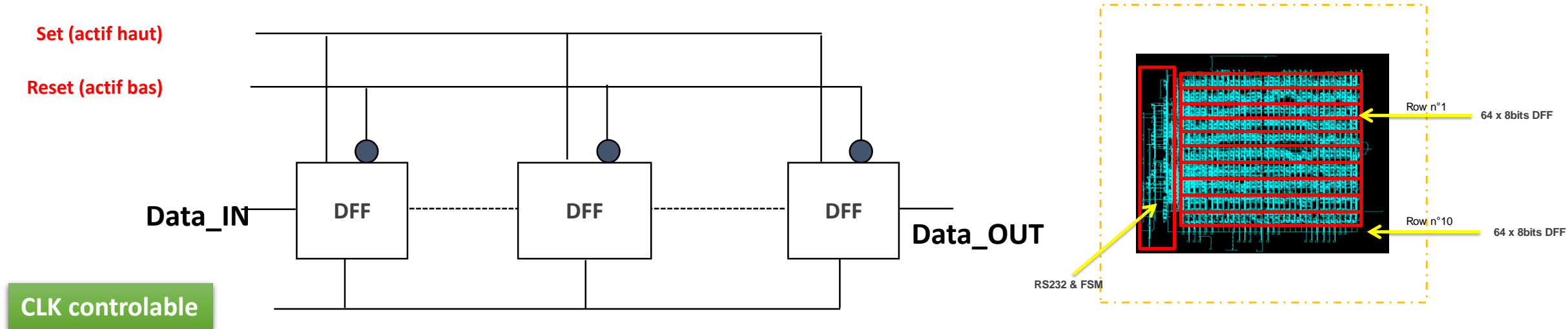


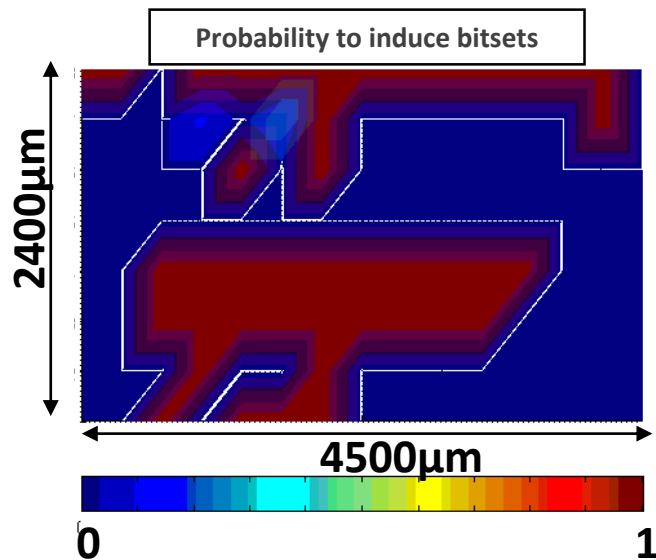
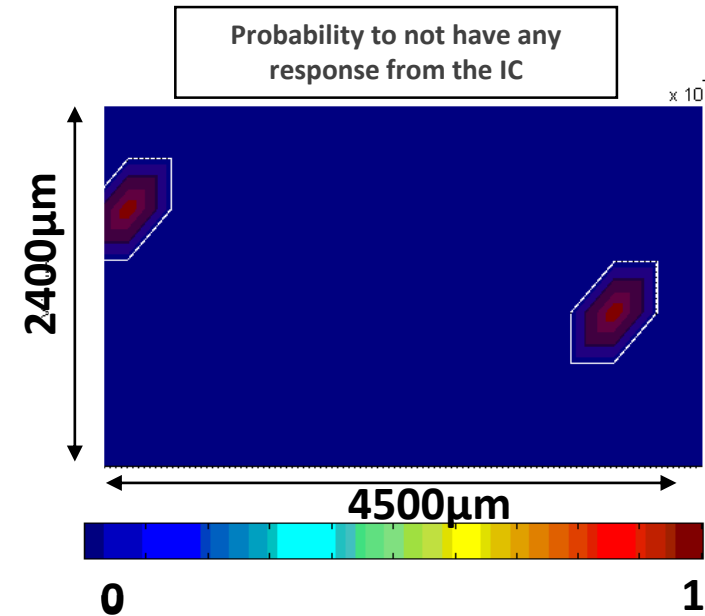
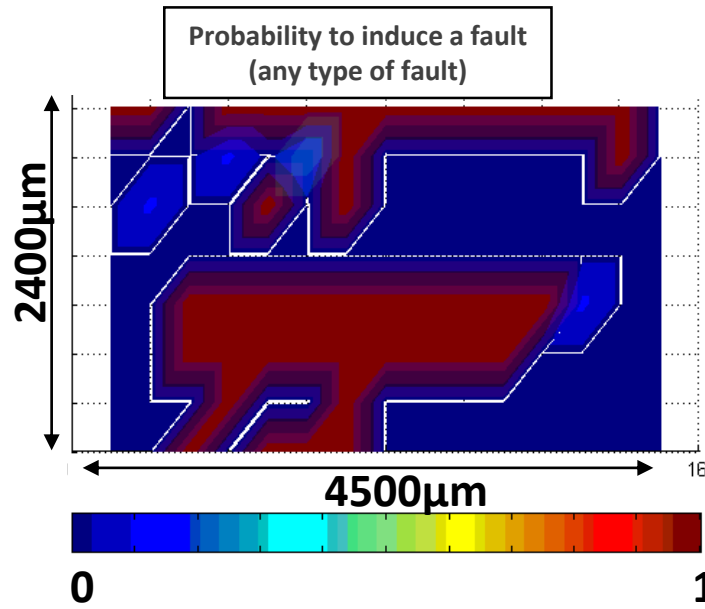
ANR e-Matahari



Bitset et bitresets ?

Nécessité d'éviter l'apparition de fautes de timing pour démontrer que l'EMFI est capable de produire des bitsets et bitresets

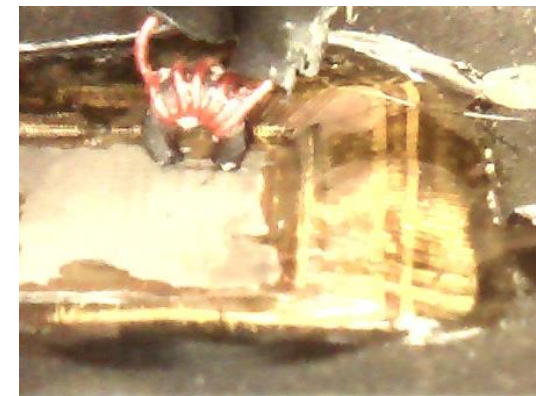


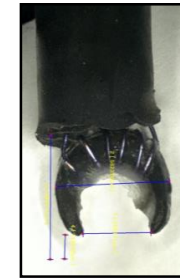
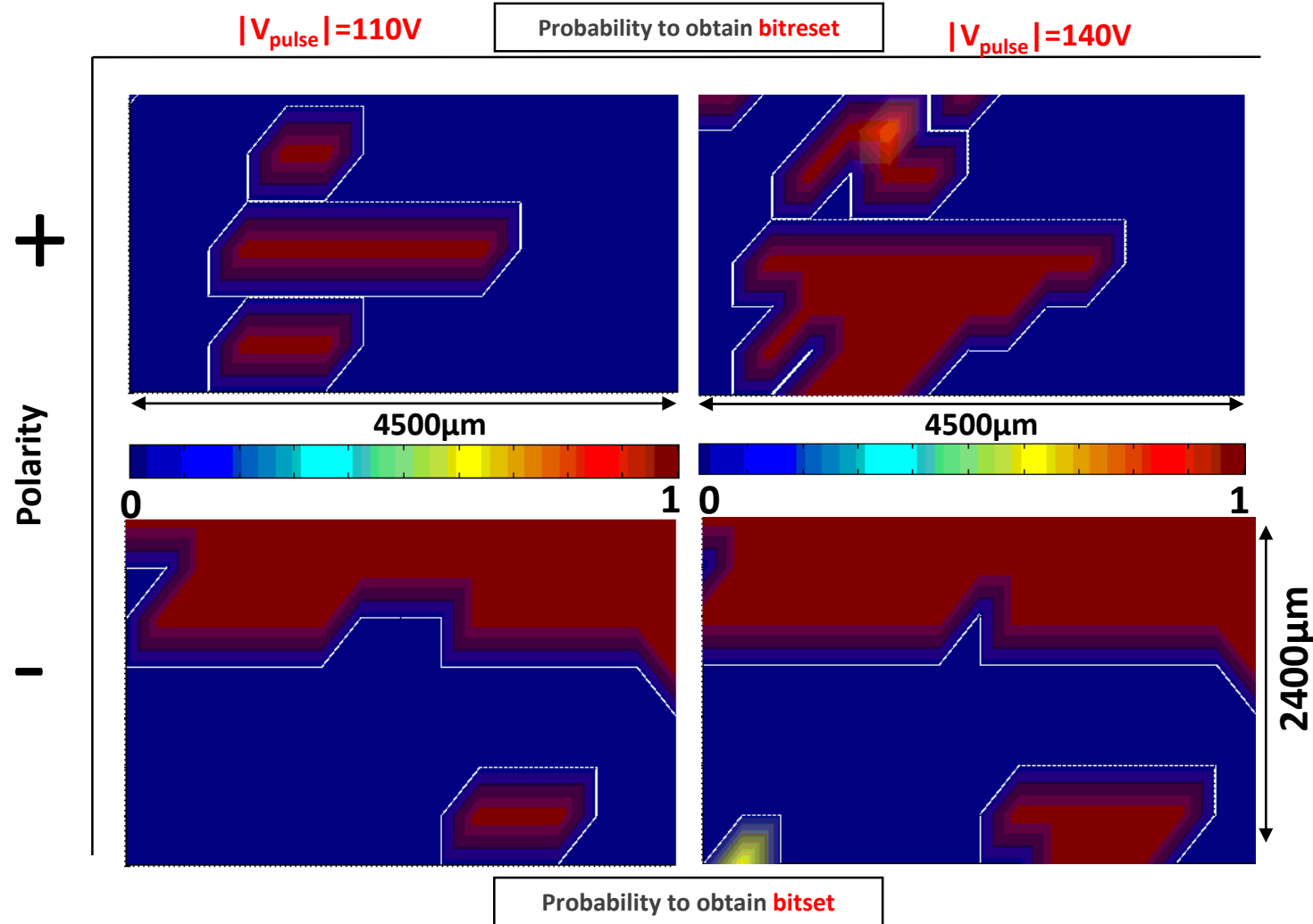


Pulse width = 8ns
Pulse amplitude = 170V
Polarity = Positive

2 types de fautes:

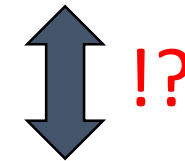
- Bitsets
- Pas de réponse
- No Bitresets ???





Probability to obtain a bitset = 0

Set signal active high



Probability to obtain a bitreset=0

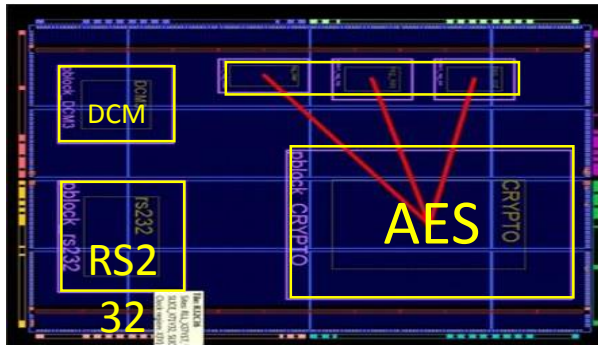
Reset signal active low

L'injection EM ne produit pas uniquement des fautes de timing

L'injection EM est capable d'inverser le contenu d'une DFF au repos

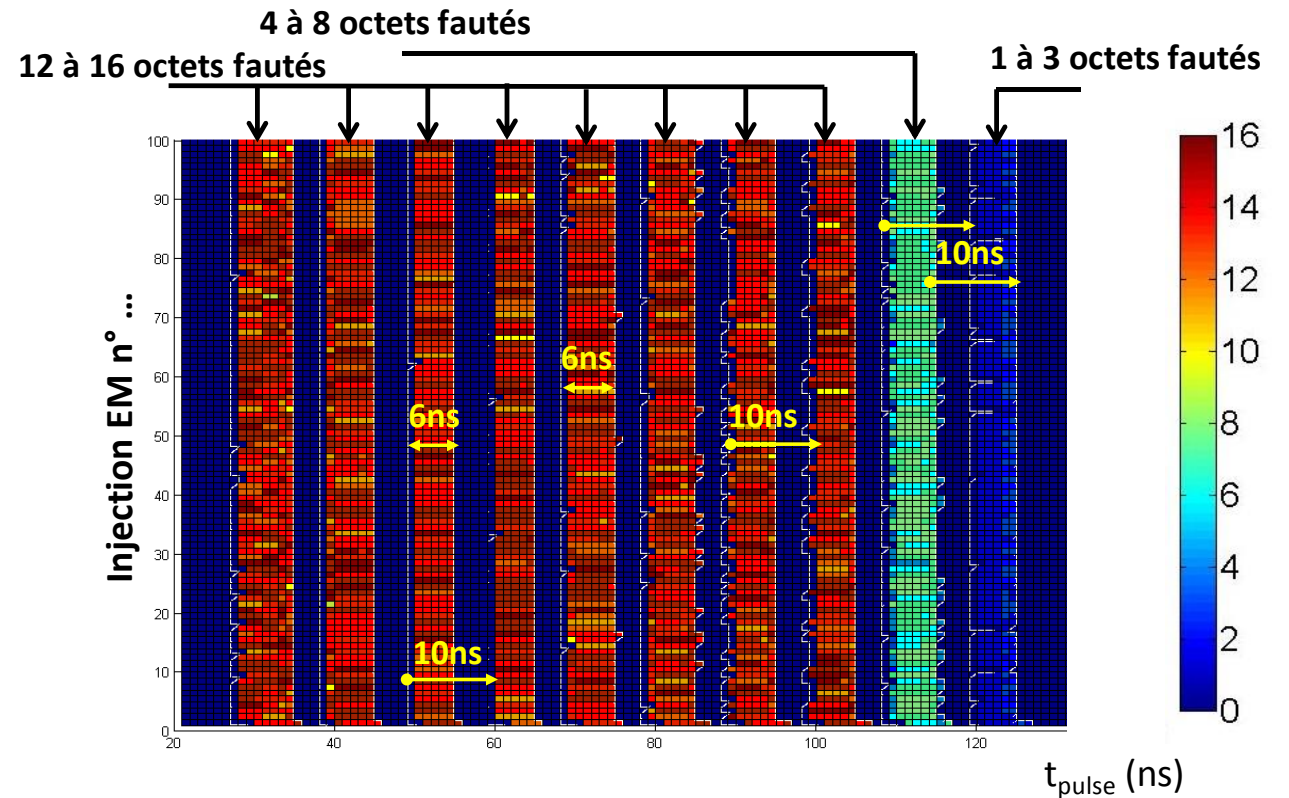
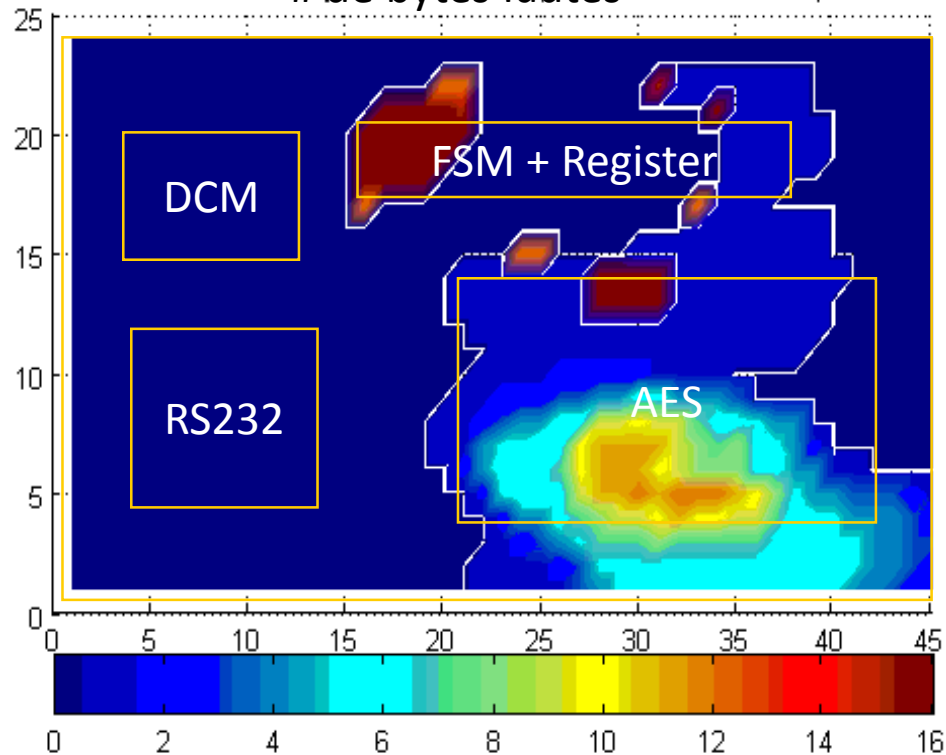
Quel modèle de faute pour l'injection EM ?

Modèle de fautes ?



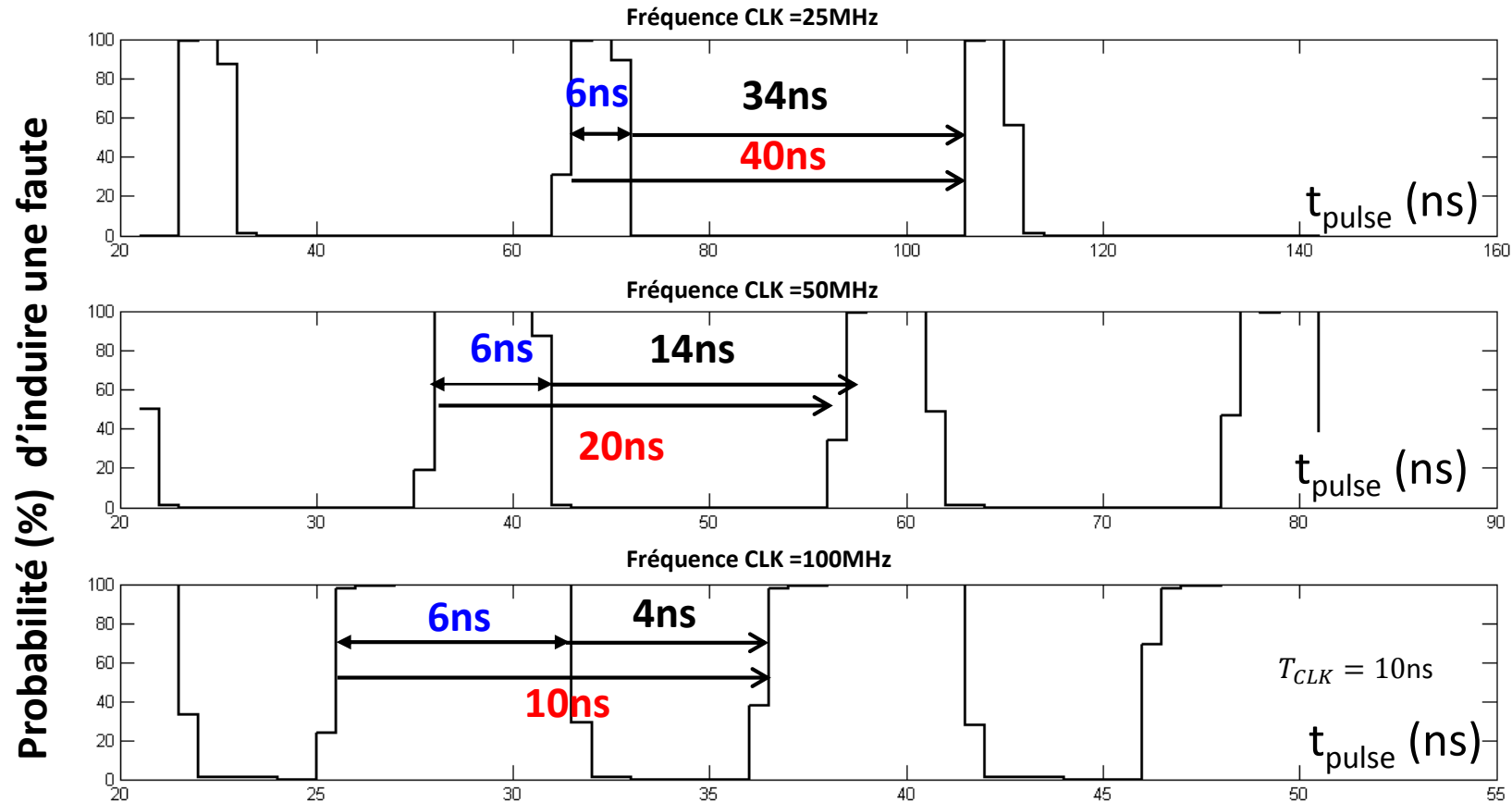
FPGA Xilinx Spartan 3
Vdd= 1.2V
Fréquence : 100MHz
Pas de la Cartographie : 200 μ m
Vpulse = 44V << 110V
100 tirs / position
Tirs durant la 9^{ème} ronde de l'AES

de bytes fautés

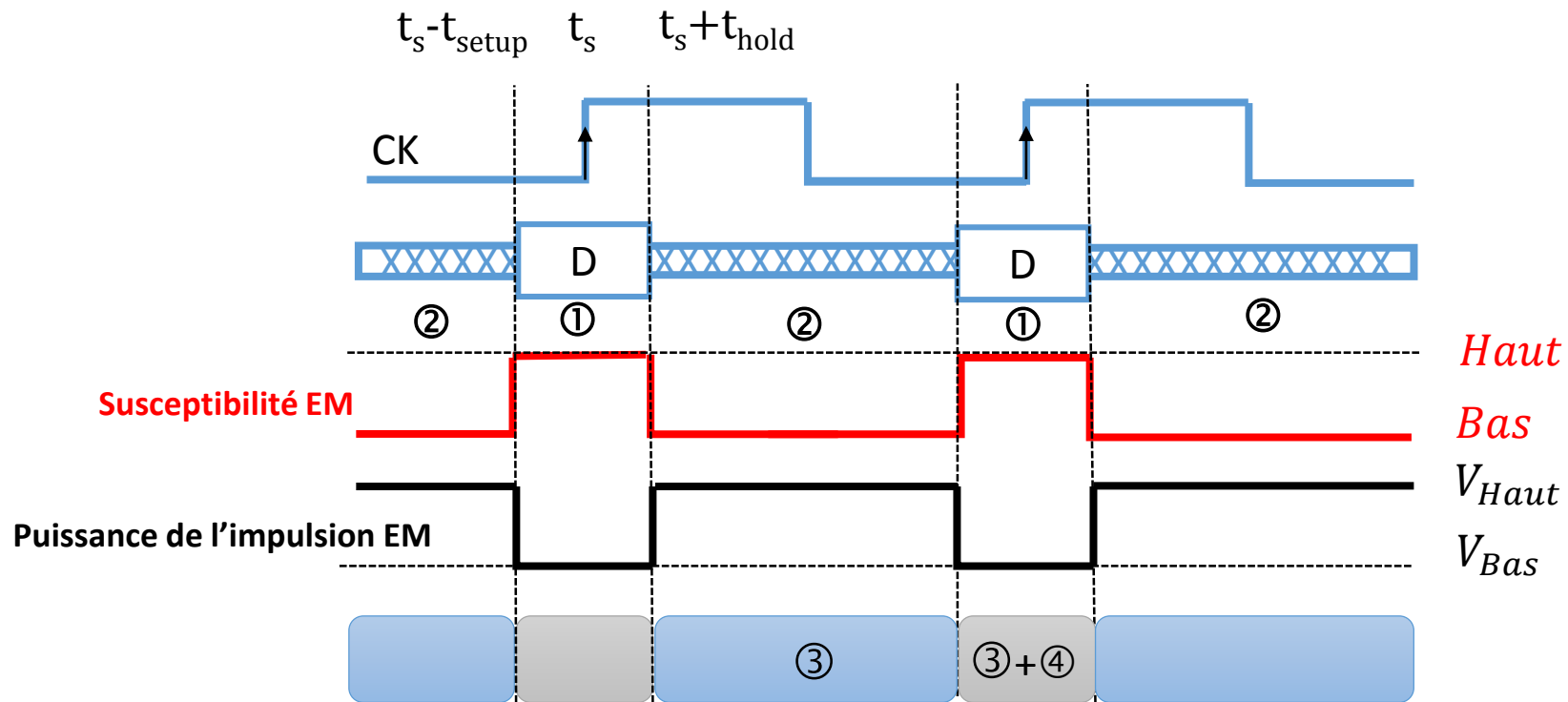


Dépendance avec la fréquence?
Dépendance avec le signal d'horloge ?

Modèle de fautes ?



Pas de dépendance avec la fréquence
Pas de fautes de timing

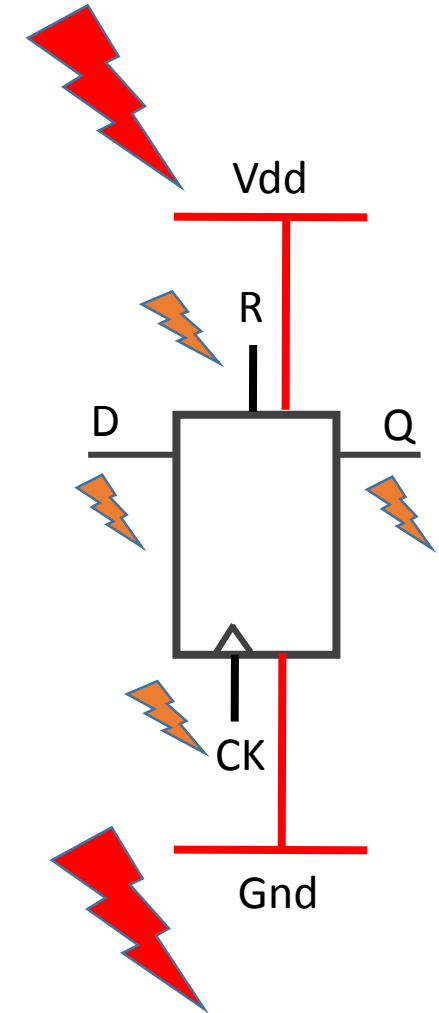


① : Fenêtre de stabilité

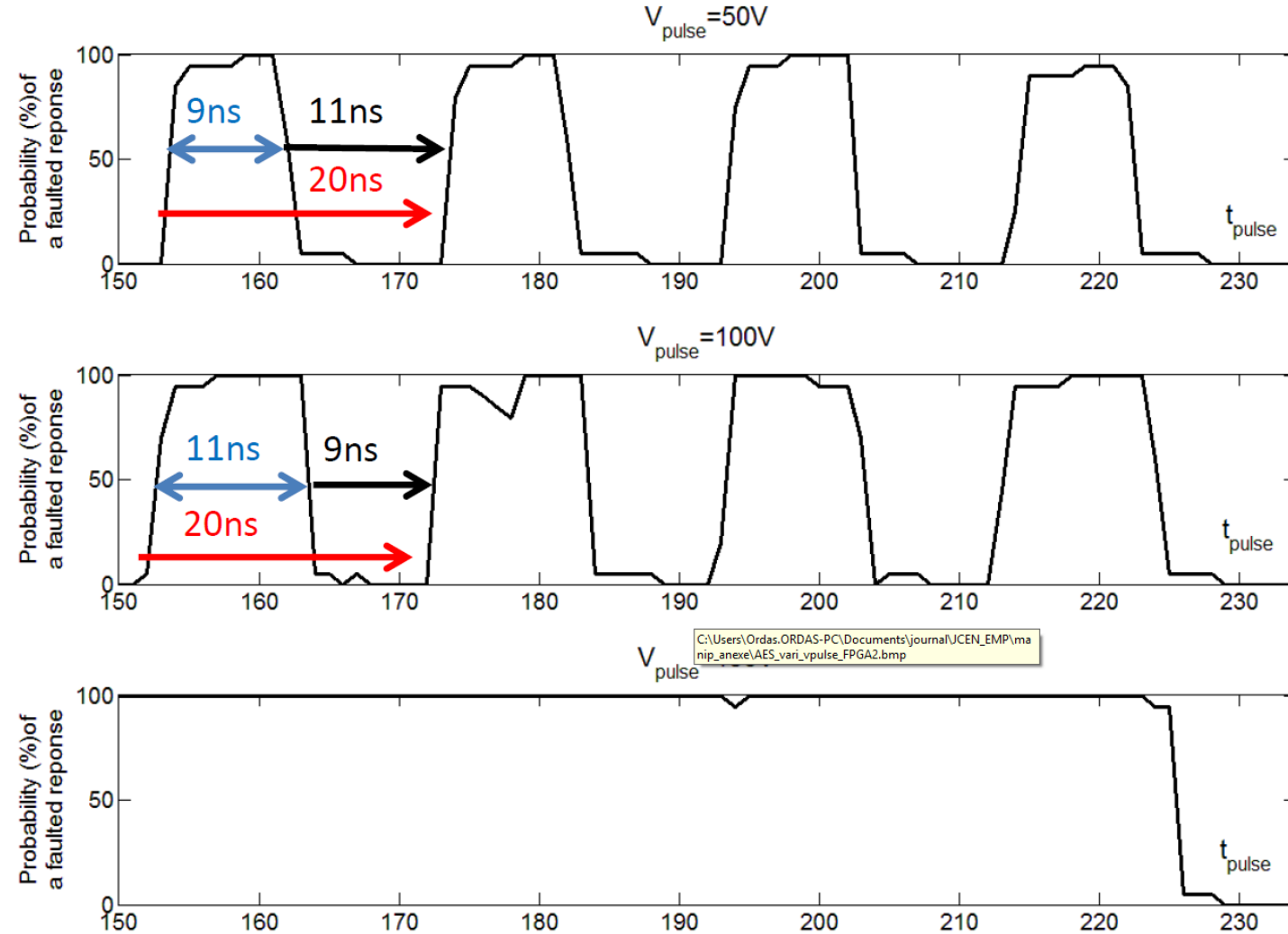
② : Fenêtre de calcul

③ : Bitset ou bitreset généré

④ : Faute d'échantillonnage générée



**Probabilité d'injecter
une faute en fonction
de l'instant d'injection
et de la puissance du tir**



Comment étayer ce modèle ?

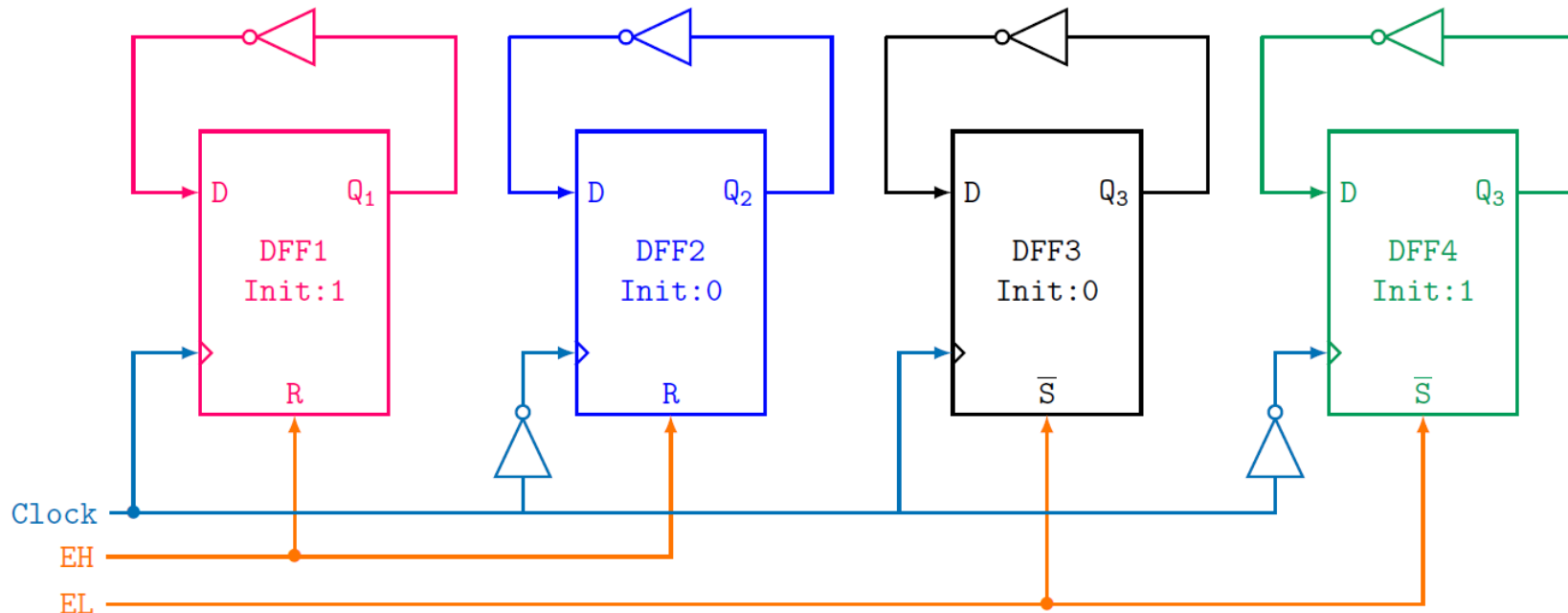
(Difficile d'observer les signaux d'entrée d'une DFF pendant une injection !)

Développer une contremesure sur la base du modèle et vérifier son efficacité !

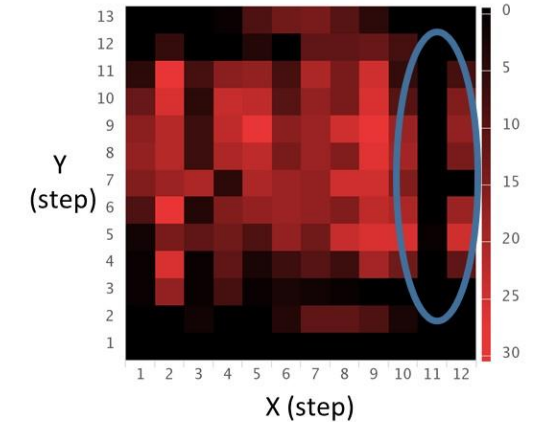
Détecteur standard cell d'impulsions EM

4 DFF rebouclées
Initialisation spécifique
Réseau de set & reset

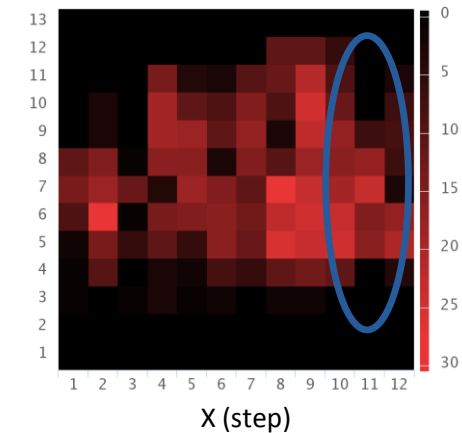
Toutes les transitions couvertes
Actif front montant et descendant



Number of detections by firing position



Number of faulted ciphers by firing position



Capable de détecter les injections BBI !
Capable de détecter les glitch d'alim (en partie) !
Capable de détecter des tirs laser ?

EMFI @ die level
34 détecteurs couvrant la totalité de la surface

De 2009
à 2016

Développement et optimisation des plateformes d'injection EM

Définition d'un modèle de faute pour l'injection EM (modèle de susceptibilité EM)

Validation du modèle par la définition d'un capteur numérique d'impulsion EM (efficace contre BBI, power glitches et potentiellement laser)

Perspectives

Augmenter les résolutions spatiales et temporelles des plateformes (FUI CSAFE+)

Raffiner le modèle de faute (mémoire, blocs analogiques ...)

Comprendre le lien entre émission EM et susceptibilité EM (guider l'injection EM)

Effets de l'injection EM au niveau architecture

Somme toute : l'injection EM est un outil récent / Laser !