FAULTING REAL-WORLD DEVICES WITH X-RAYS BEAMS?

ANR MITIX

CEA-CESTI / SIMAP

+ partenaires TIMA / CEA-LTSO / ONERA

Stéphanie Anceau / Sophie Bouat / Luc Salvo / Laurent Maingault / Gwendal Jugault / Pierre Lhuissier / Emrick Belliard / Rémi Tucoulou

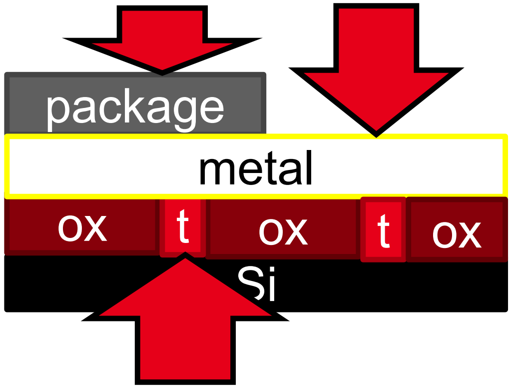
X-RAY ATTACKS

Laser perturbation (VIS-IR)

Resolution limited by its wavelength

(IR ~ 1 µm)

Unpackage the device / bakside illumination

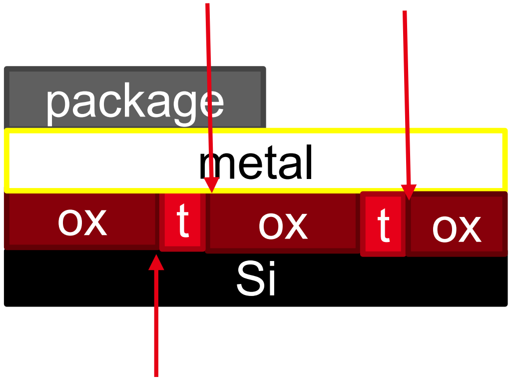


X (~ 10 keV)

Wavelength < 1 nm

Package, thin metal layers →

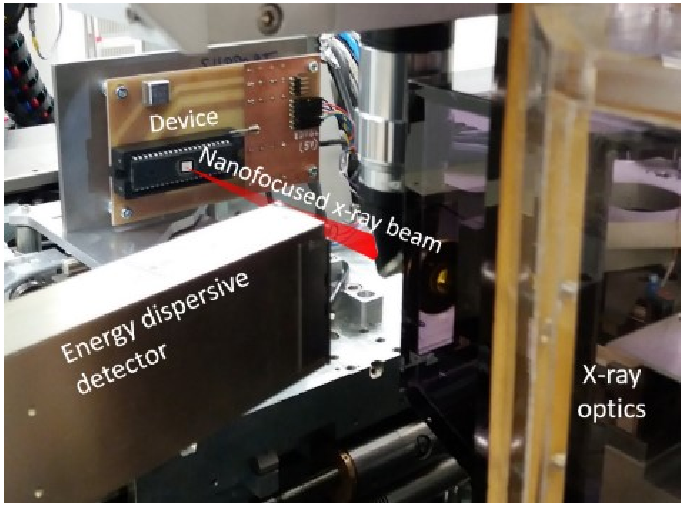
~ transparent



<u>Preuve de concept :</u>

Attaques sur transistor unique démontrée sur des cellules mémoires (RAM / FLASH) en technologie > 90 nm avec un faisceau synchrotron nano-focalisé.

CHES 2017, September 25-28, 2017, Proceedings, 2017, p. 1



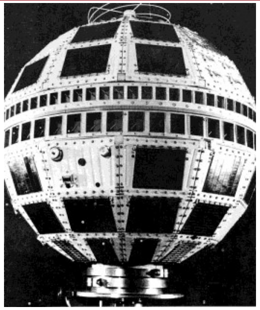
EFFET RAYONS X EN REALITE

Spatial
Années 60

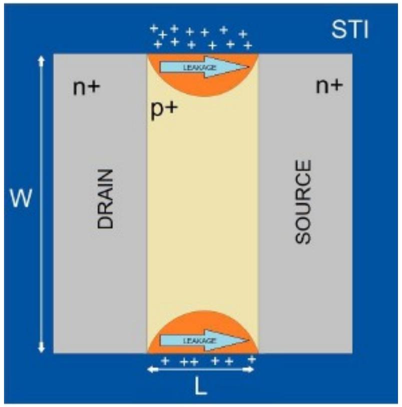
412 IEEE TRANSACTIONS ON ELECTRONIC COMPUTERS, VOL. EC-16, NO. 4, AUGUST 1967

Design and Use of Fault Simulation for Saturn Computer Design

FRED H. HARDIE AND ROBERT J. SUHOCKI



- **Perturbation des oxides de manière semi-permanente (TID)**



nMOS leak
pMOS are blocked

- **Recuit nécessaire pour enlever la faute**
- **Modification possible des cellules de Flash**
- **Faisceau petit mais difficile à focaliser (synchrotron)**

→ Nouveau type de fautes (Persistent Fault Attacks)

VERS DES ATTAQUES REELLES

Attaques sur transistor unique démontrée sur des cellules mémoires (RAM / FLASH) en technologie > 90 nm avec un faisceau

CHES 2017, September 25-28, 2017, Proceedings, 2017, p. 1

Minimum sur la technologie ?

Cellules logiques ?

I. Manip ESRF avec microcontrôleur 28 nm

Avec un générateur X de laboratoire ?

II. Masques sur tomographe (SIMAP)

GRENOBLE, FRANCE

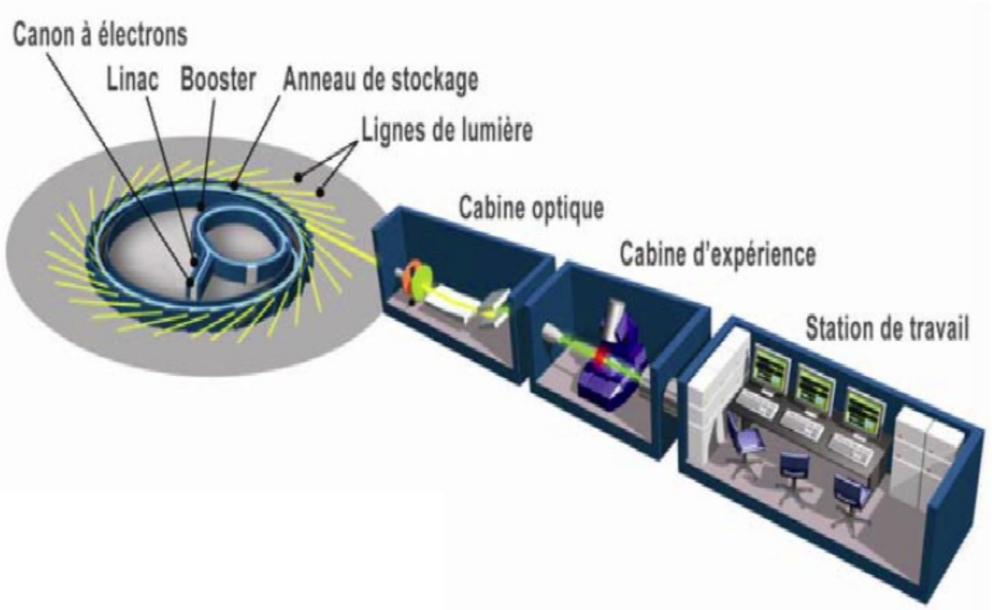
Léti ITSEF

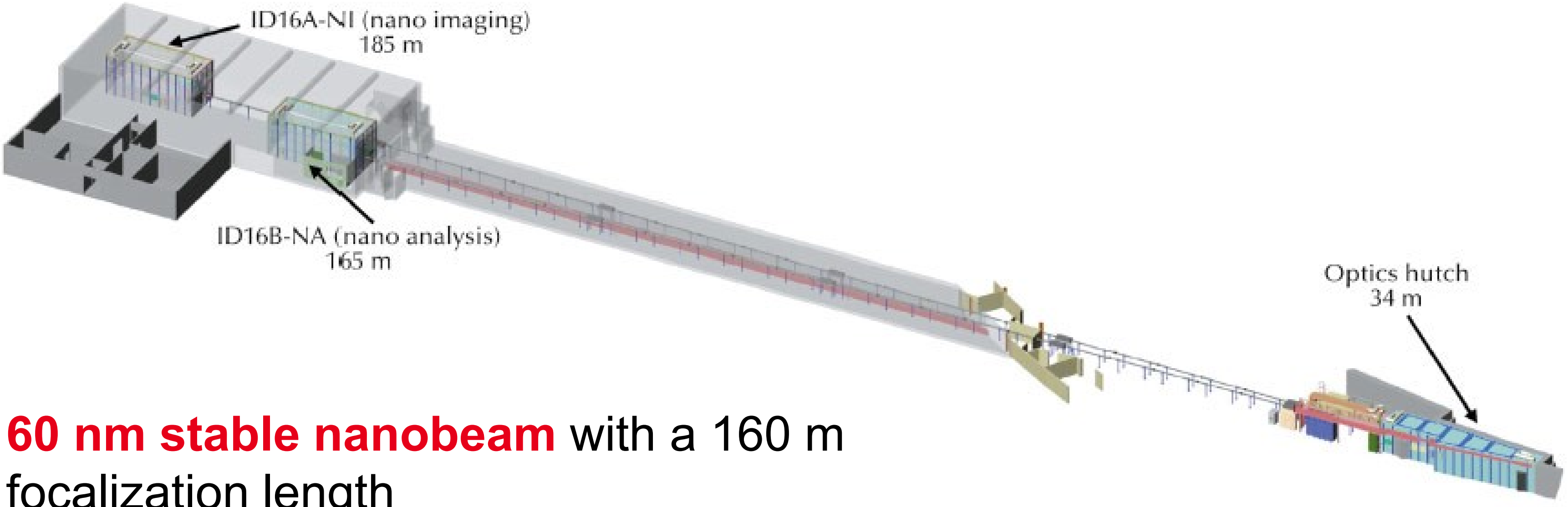
European Synchrotron Radiation Facility (ESRF)

500 m

SYNCHROTRON SETUP

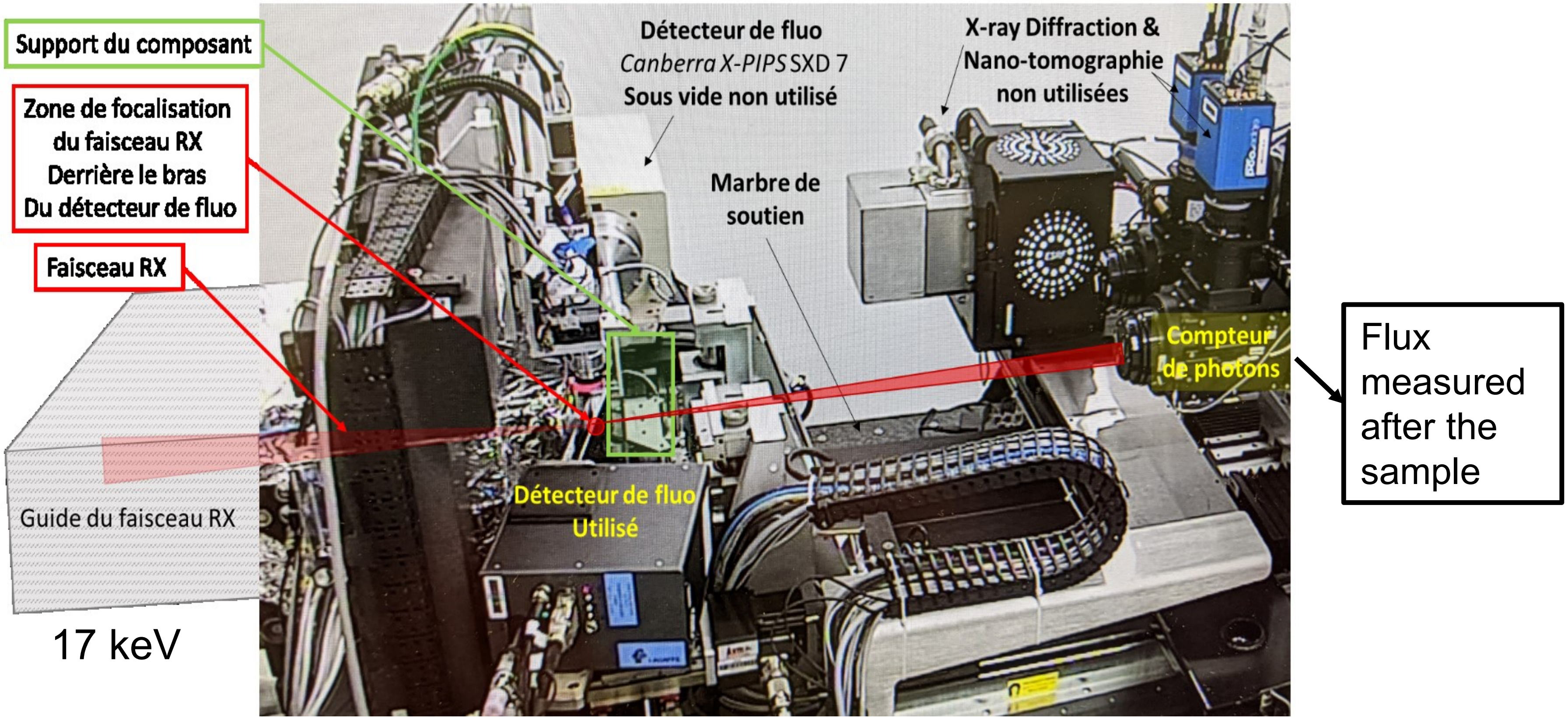
- Electron packets circulate in the loop
- Photon emitted w/h bending magnets and undulators





60 nm stable nanobeam with a 160 m focalization length

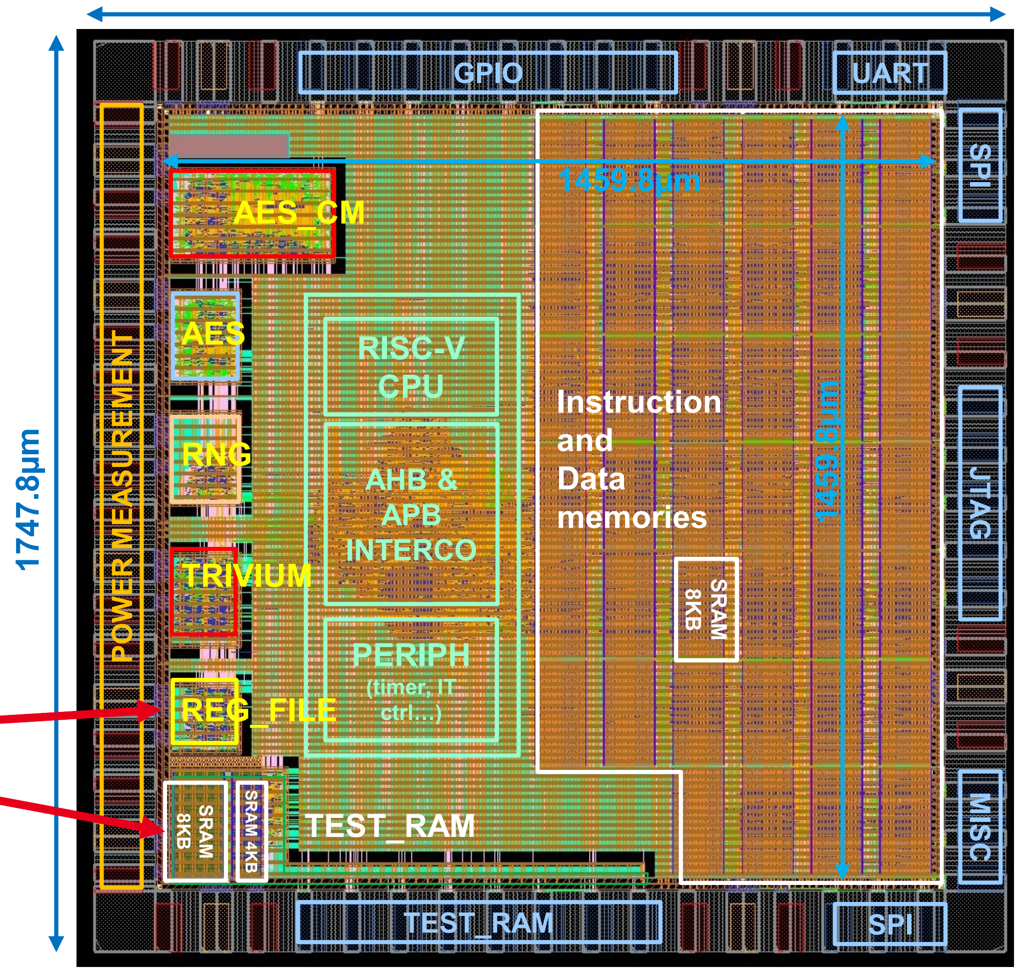
OVERVIEW


Support du composant
Zone de focalisation
du faisceau RX
Derrière le bras
Du détecteur de fluo
Faisceau RX
Guide du faisceau RX
17 keV
Détecteur de fluo
Canberra X-PIPS SXD 7
Sous vide non utilisé
Marbre de
soutien
X-ray Diffraction &
Nano-tomographie
non utilisées
Compteur
de photons
Détecteur de fluo
Utilisé
Flux
measured
after the
sample

Un faisceau lumineux guide le positionnement du composant dans le plan focal du faisceau RX

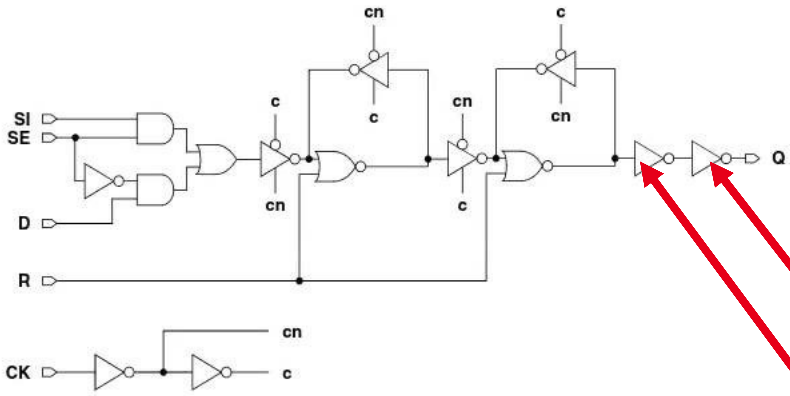
- **TEST COMPONENT : critical knowledge of the TOE**
  - BULK 28 nm technology node / RISC-V CPU
  - Gds2 available

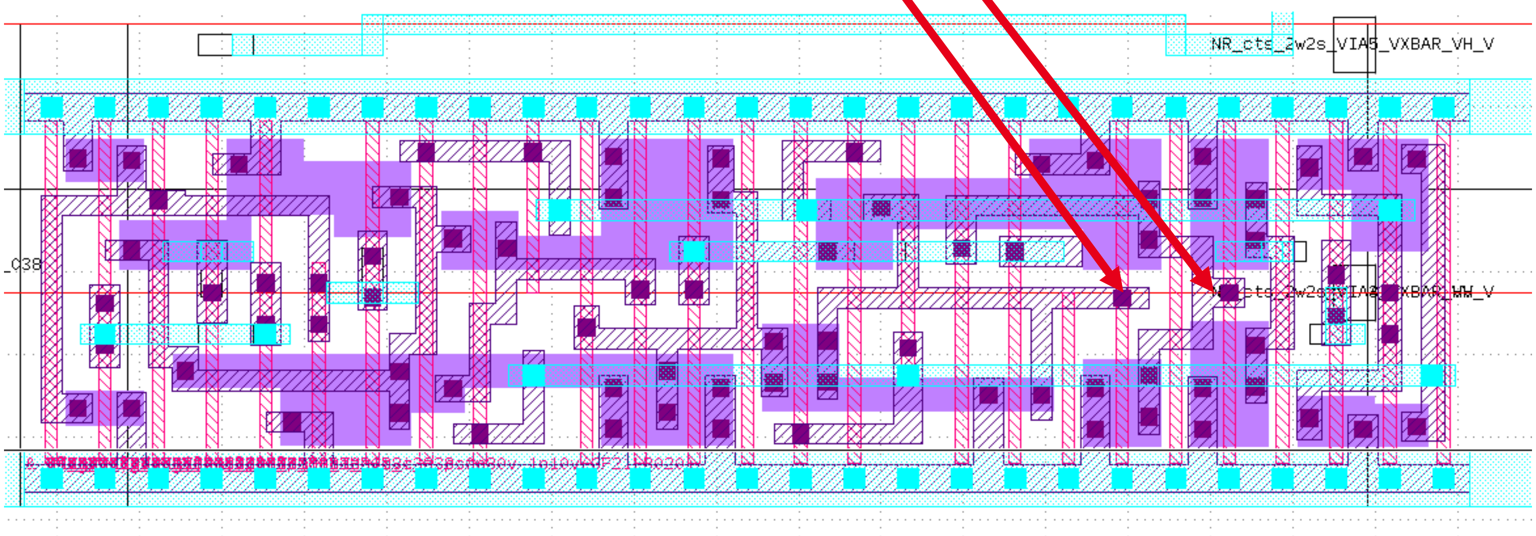
Targets
1. Registers
2. SRAM



EFFECT ON LOGICAL GATES

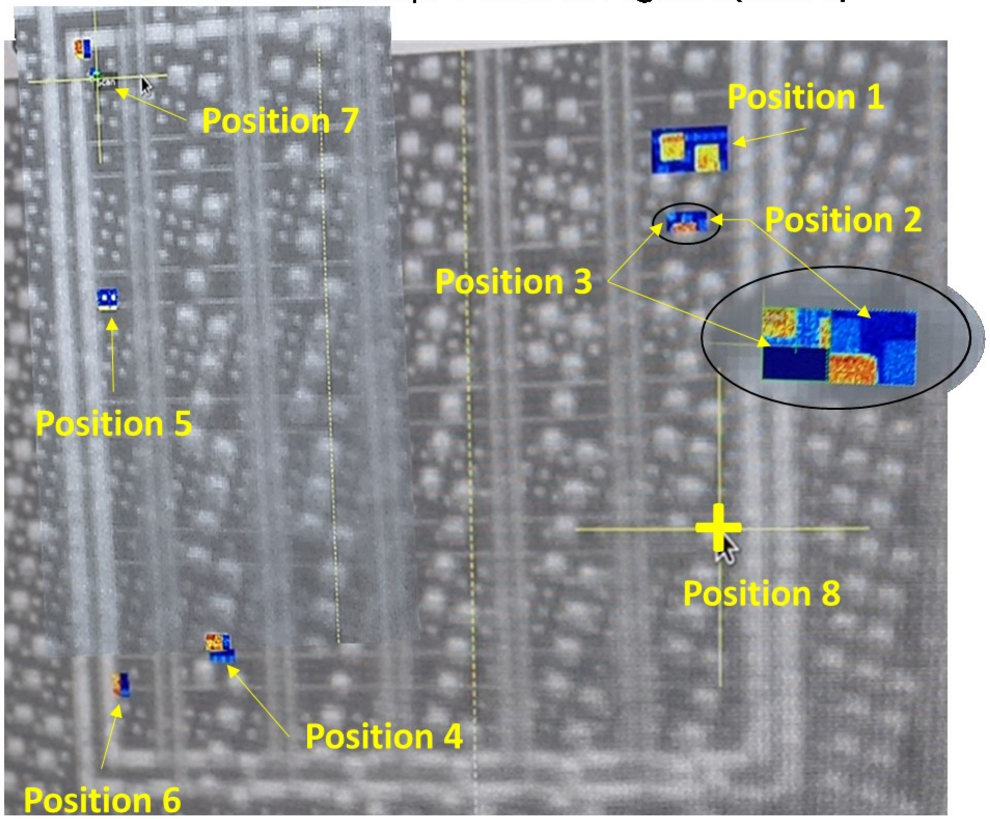
Flip-flop register





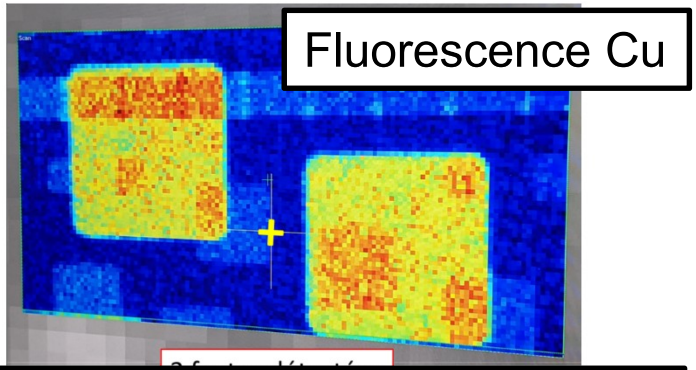
FIRST ATTACK ON LOGICAL GATES

Positions des attaques dans le registre (bloc 5)

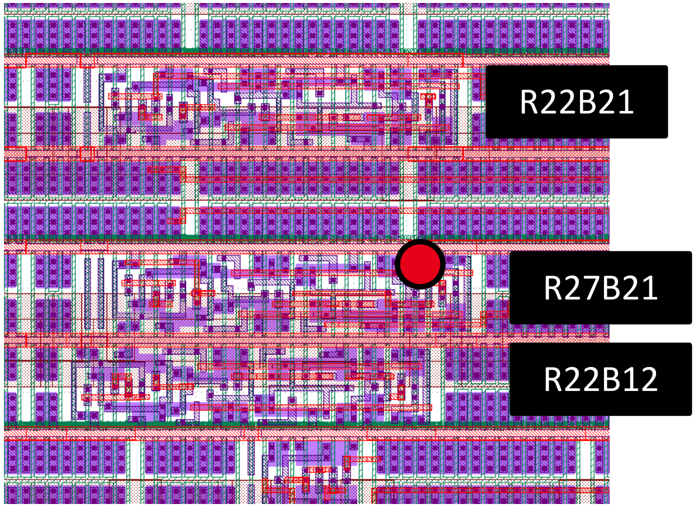


Images optiques

Position 1 – Registre (bloc 5) : 1 min – flux 2,3 x 10^8 photons/s (avec atténuateurs Si 3,5 mm)
+ 1 min – flux 6,6 x 10^{10} photons/s (sans atténuateur)

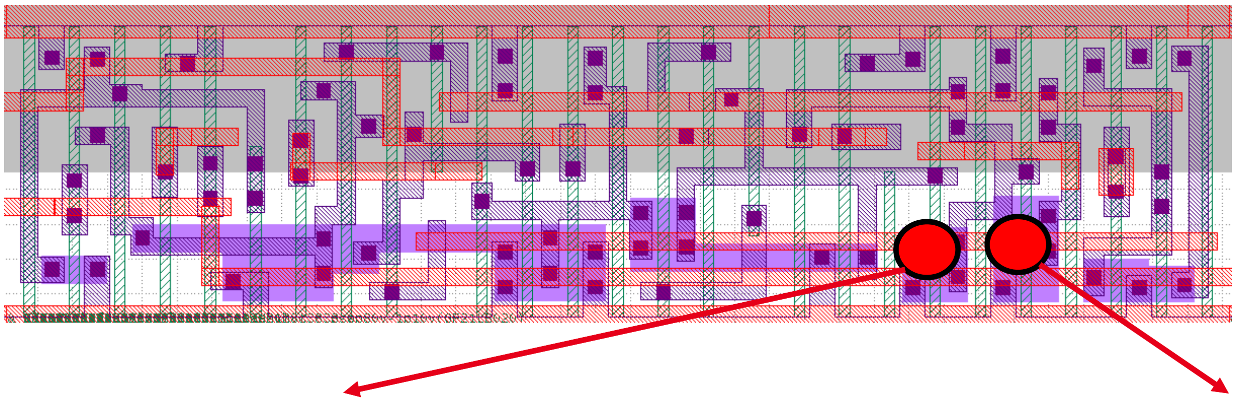


Localization thanks to M6-M7 dummies



pMOS

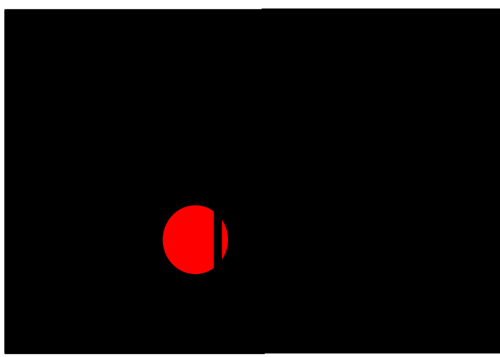
nMOS



$\approx 7 \times 10^{10}$ photons disappear after months

Stuck at 1

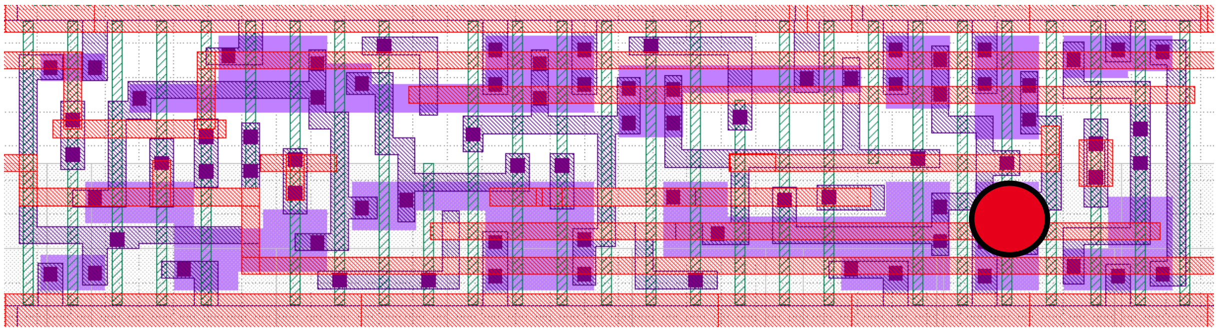
Stuck at 0



→1

→0

$\approx 3 \times 10^{11}$ photons
Stable after months



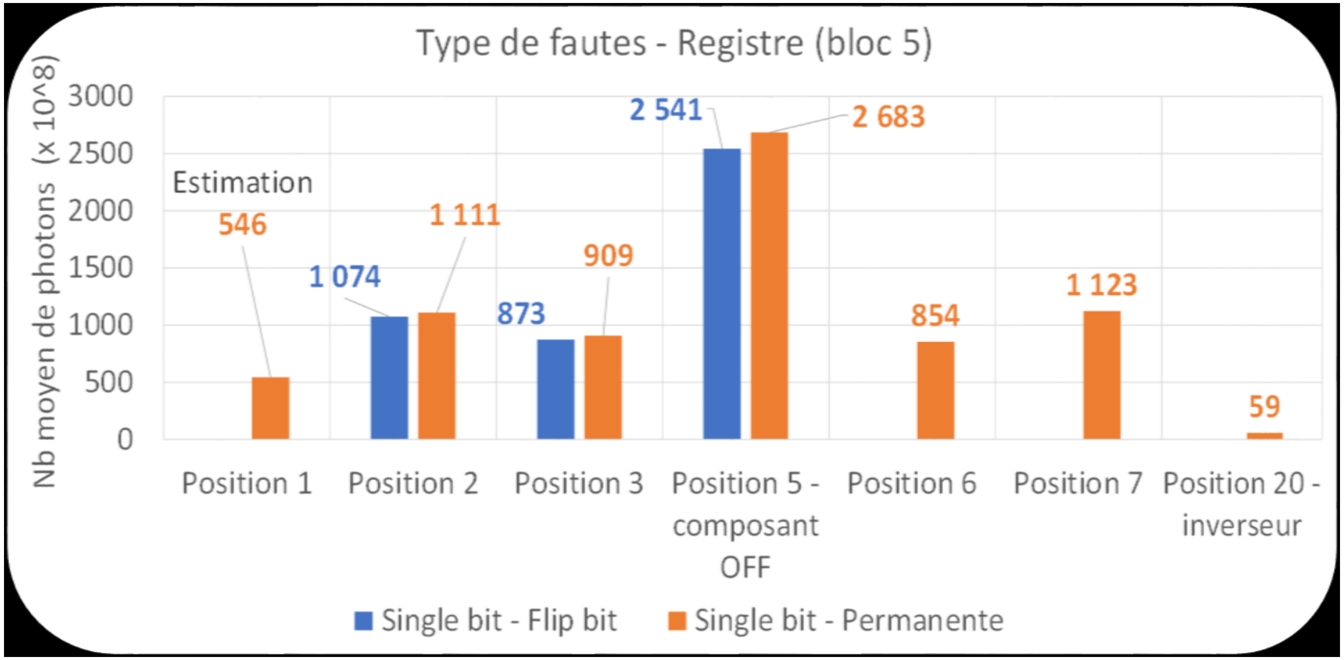
nMOS

pMOS

→ Impossible to reach ‘1’

DOSE TUNING

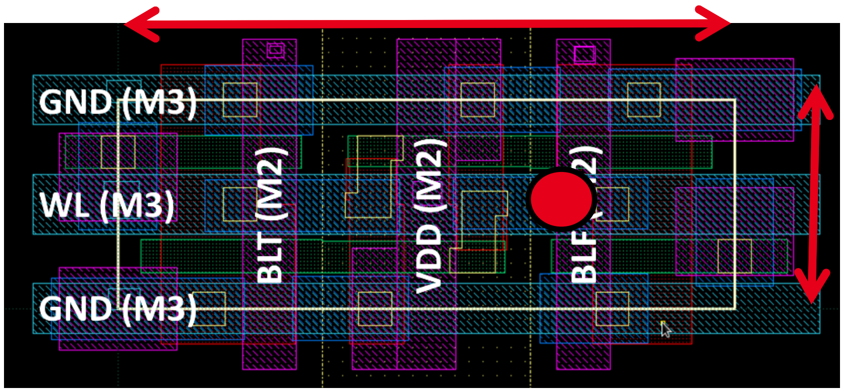
- Fine tuning => single bit fault made (power on and off)



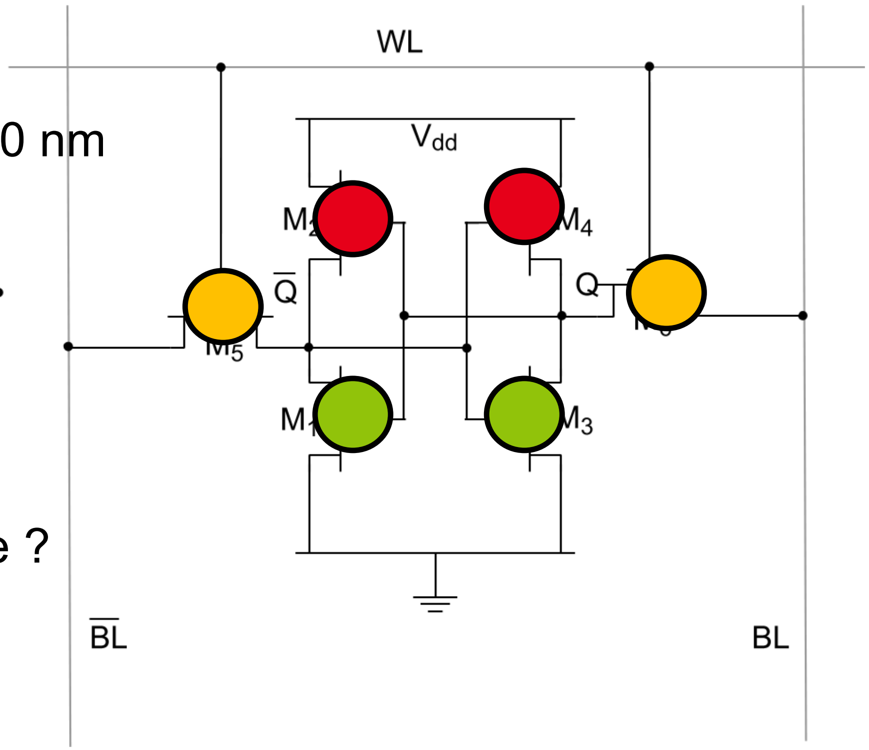
- Short term fault duration shall be investigated, on-off cycle, annealing.

6-T CLASSIC RAM

600 nm



220 nm



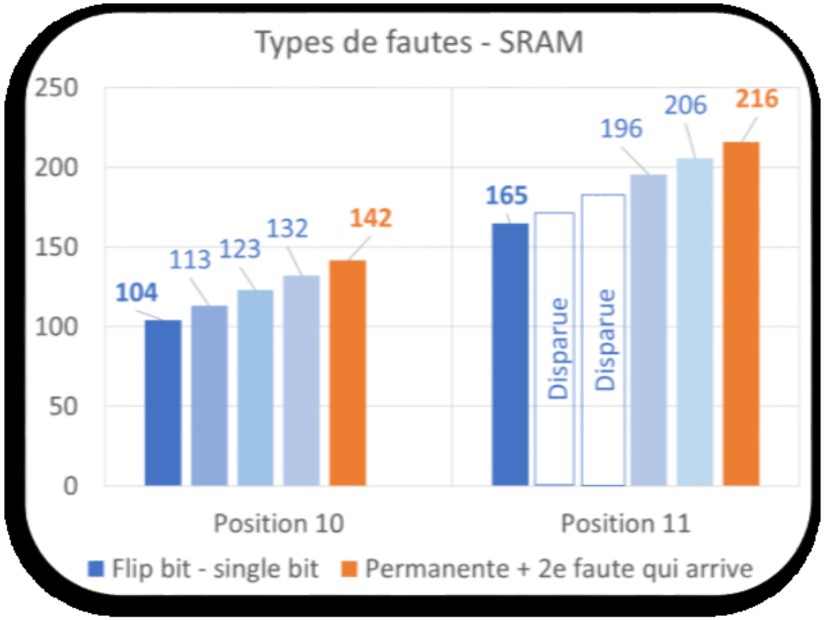
Bit set/reset nMOS

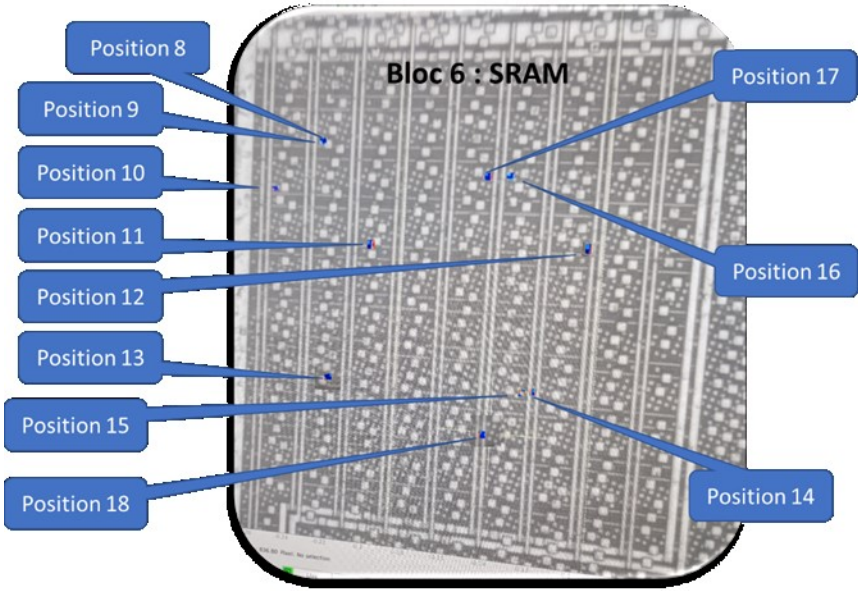
Bit set/reset pMOS possible ?

Whole line faulted behavior

FAULT IN SRAM

~ $150 - 200 \times 10^{18}$ photons pour Single bit fixé
Single bit possible





RESULTS AT ESRF

- Possible to modify single transistors with recent MCU technology nodes (28 nm)
- Targetting specific cells is easy with non destructive fluorescence imaging
- Multiple faults shall be simple

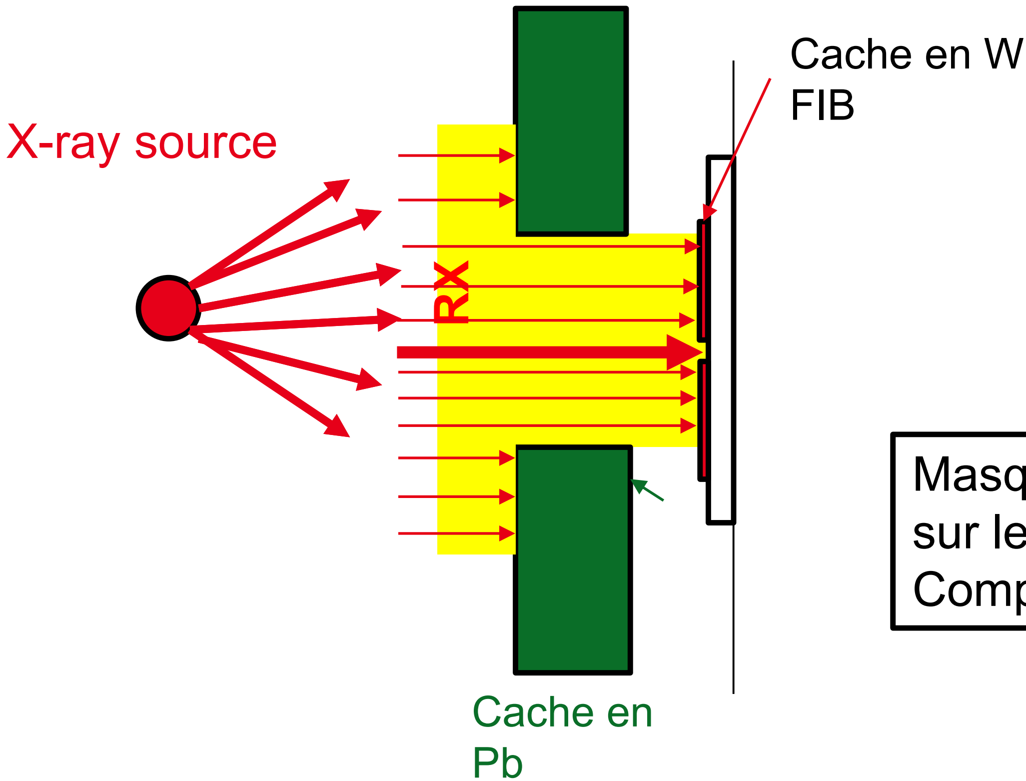
Future works (with high attack potential) :

- Demonstration of Persistent Fault Attacks on AES (PFA), new attacks in CPU logic…
- FDSOI 22 nm, lower technology nodes ?

VERS DES ATTAQUES REELLES : ~~ESRF~~

<u>Point de départ</u>: Fautes FLASH & SRAM sur ATMega 128 (0.35 µm) à l'ESRF

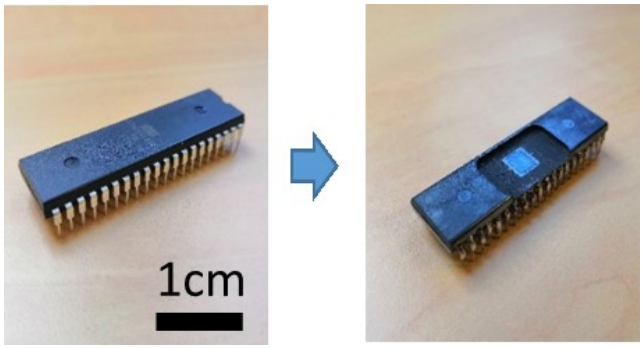
Avec un générateur X de laboratoire ? → II. Masques sur tomographe X (SIMAP)

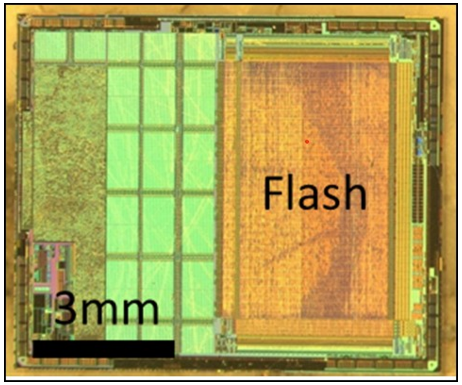


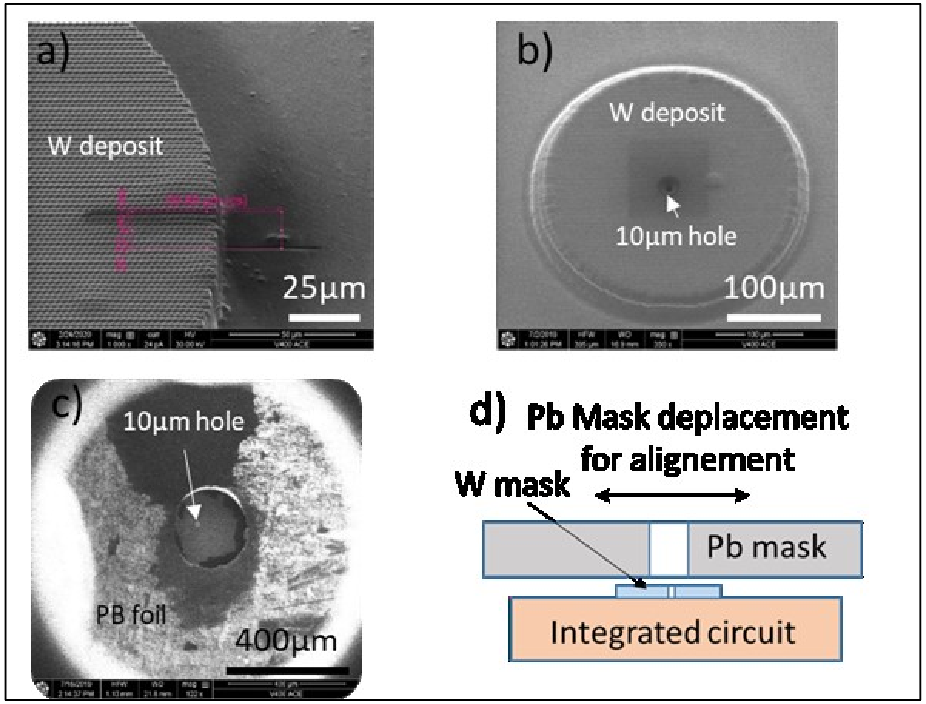
Masquage du flux X afin d'adresser un minimum de cellules

- Masque déposé sur le Composant
- Masque amovible

BACK IN 90' AND 2017 CHES => ATMEGA 128 FLASH PERTURBATION



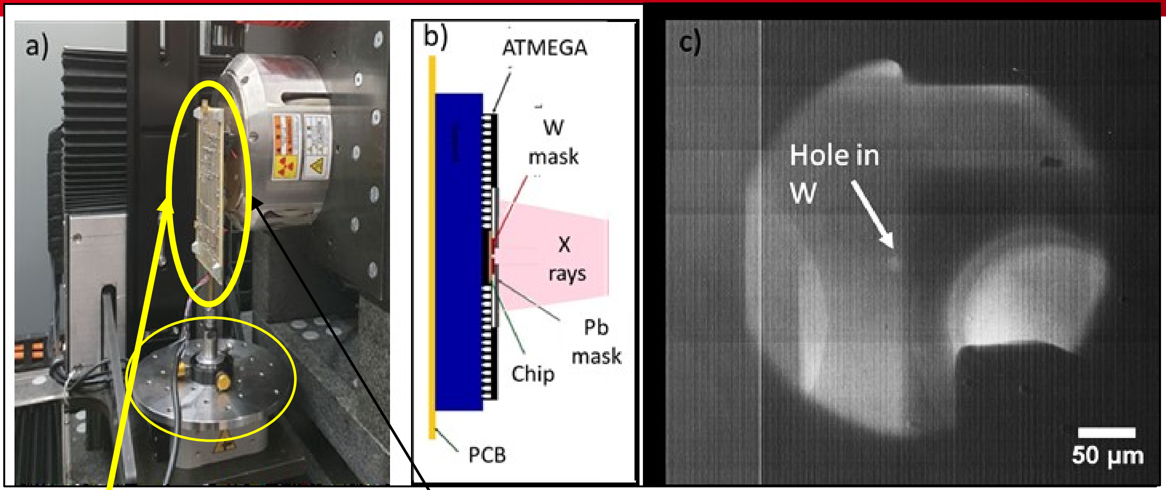




Etapes process:
a) Dépôt W (Ø 300 µm x ép. 20 µm) au FIB
b & c) avec un trou traversant creusé au FIB (Ø 10 µm)
d) recouvert par une feuille de Pb (ép. 300 µm) trouée (Ø 250 µm)

CARDIS 2021

REPRODUCTION MANIP CHES 2017

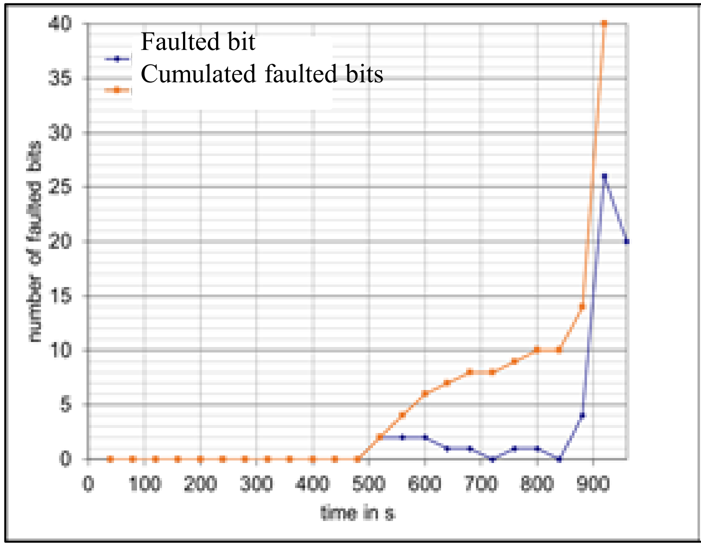


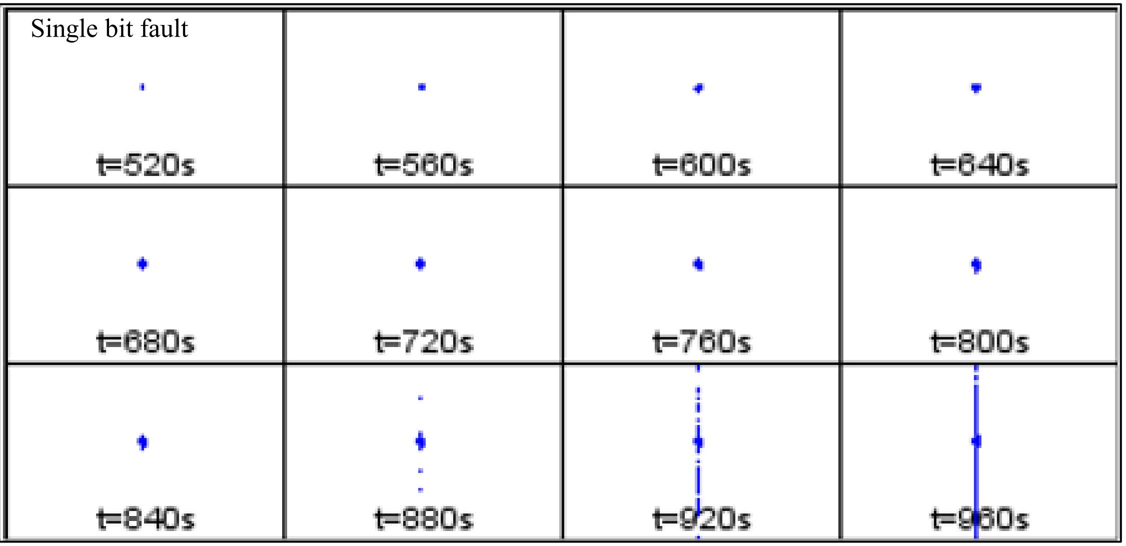
Composant

Source X

Trou ~ 10 µm²

Faute random single bit suivie par un accumulation de bits fautés



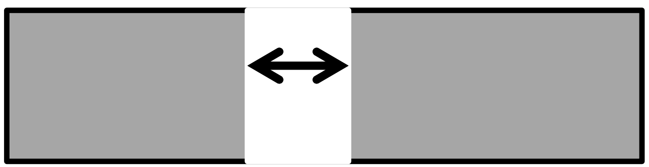


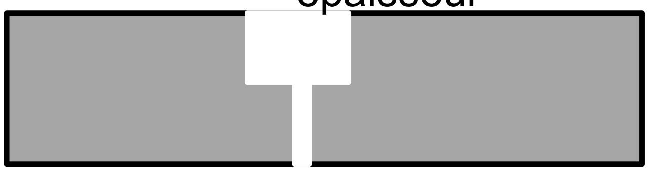
CONTRÔLE POSITION PERTURBATION CACHE AMOVIBLE

Feuille Pb :50 µm

Plusieurs possibilités

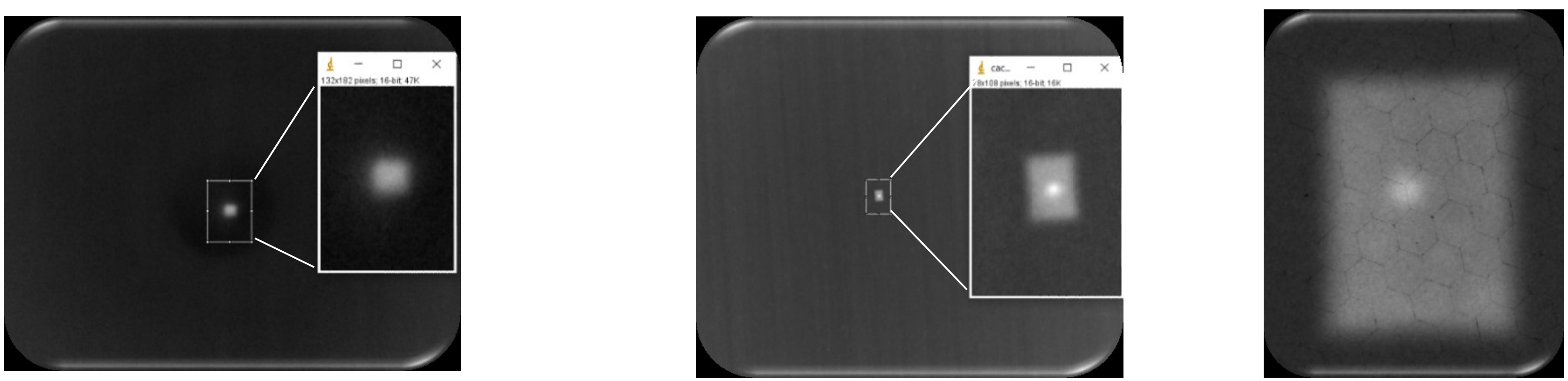
Trou large 30 µm² x 25 µm épaisseur





Trou FIB
10 µm

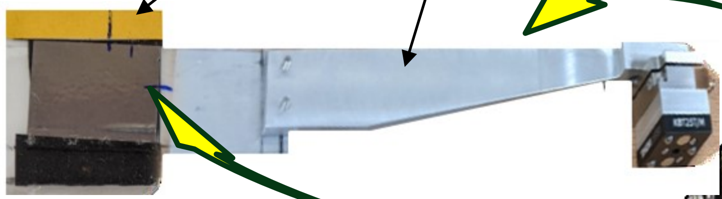
Trou 3 µm / Spot ~1 µm

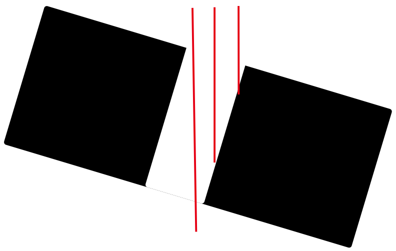


Transmission X

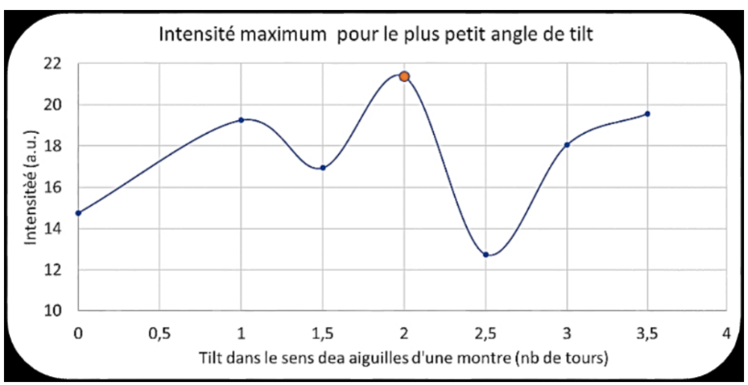
CACHE AMOVIBLE

Cache fixé sur le bras

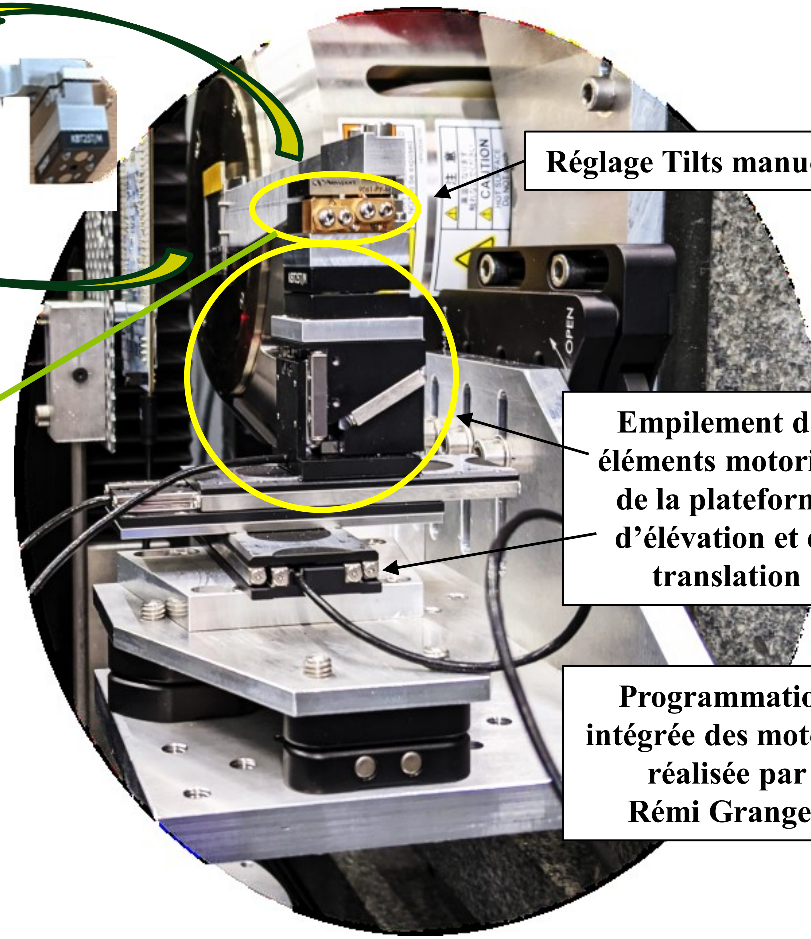




tilt critique



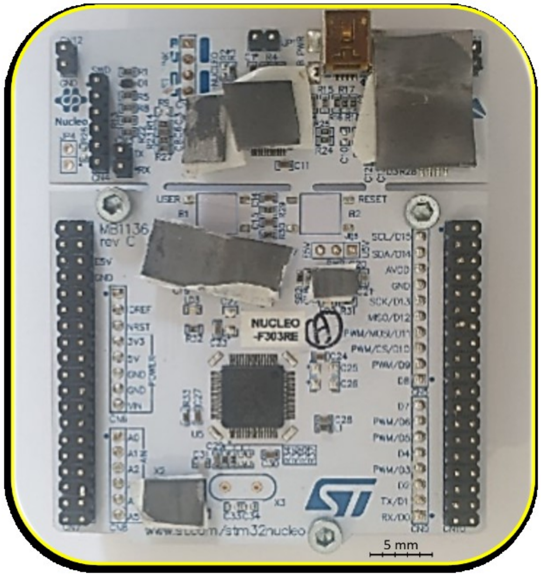
Tilt ⇔ Intensité maximale

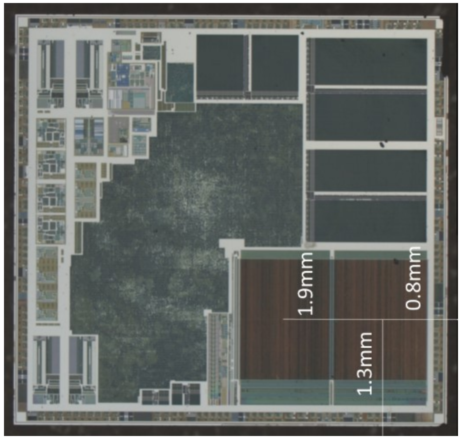


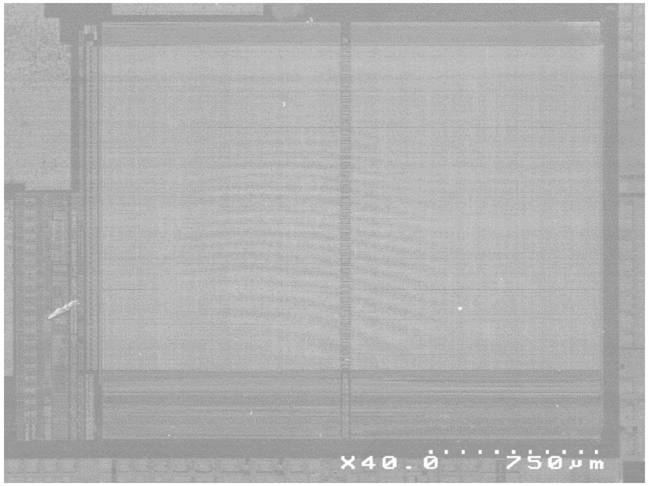
Réglage Tilts manuel

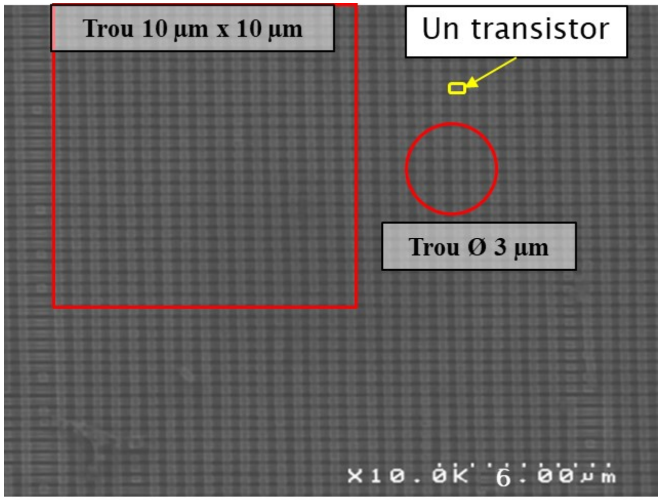
Empilement des éléments motorisés de la plateforme d'élévation et de translation

Programmation intégrée des moteurs réalisée par Rémi Granger


NUCLEO
-F303RE
5 mm


1.9mm
0.8mm
1.3mm

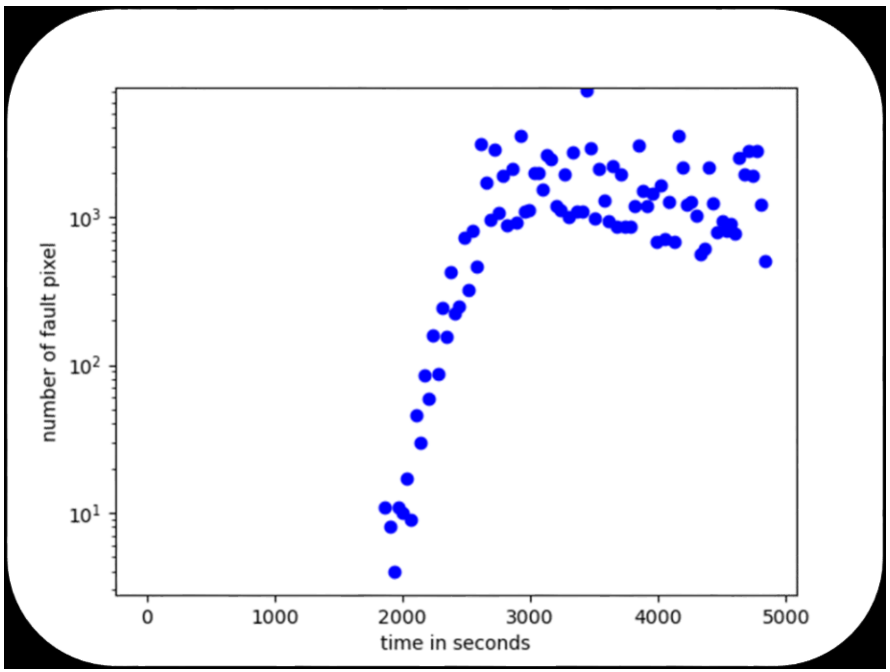

x40.0 750µm

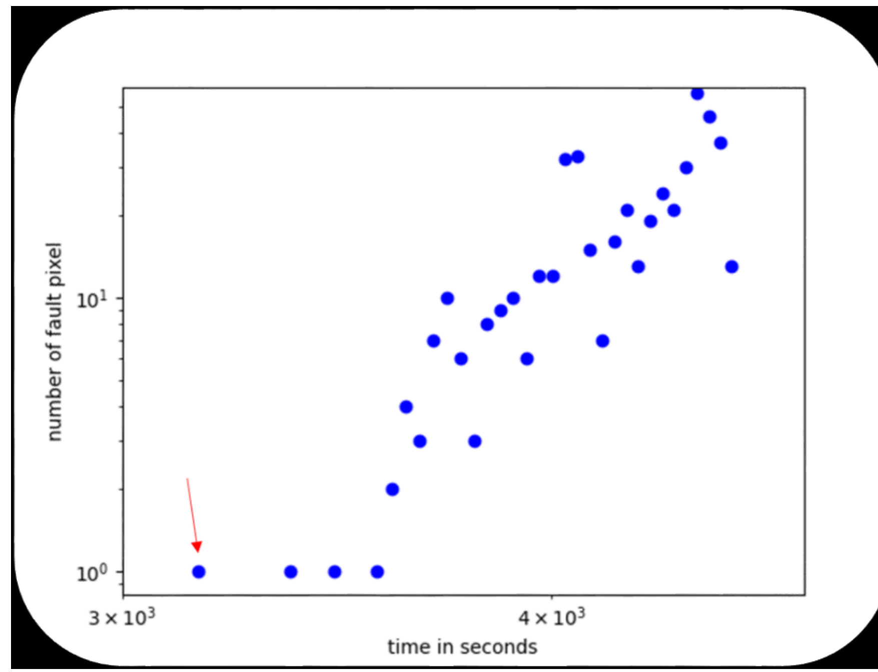

Trou 10 µm x 10 µm
Un transistor
Trou Ø 3 µm
x10.0k 6.00µm

RESULTATS

Attaque avec Cache Trou 10 µm x 10µm
11 fautes au bout de 30 minutes

Attaque avec Cache Trou Ø 3 µm
Faute random single Bit au bout de ~ 50 minutes





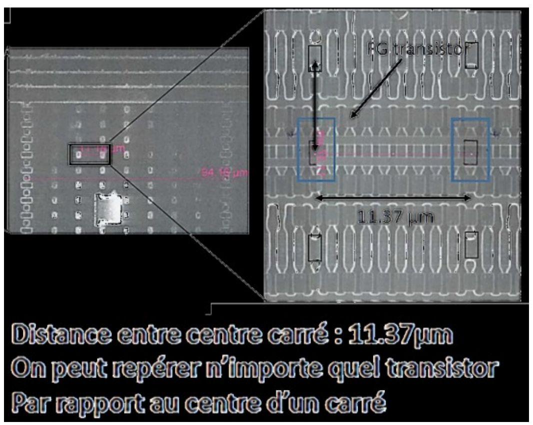
Facile à l'ESRF => images de fluorescence à bas flux !

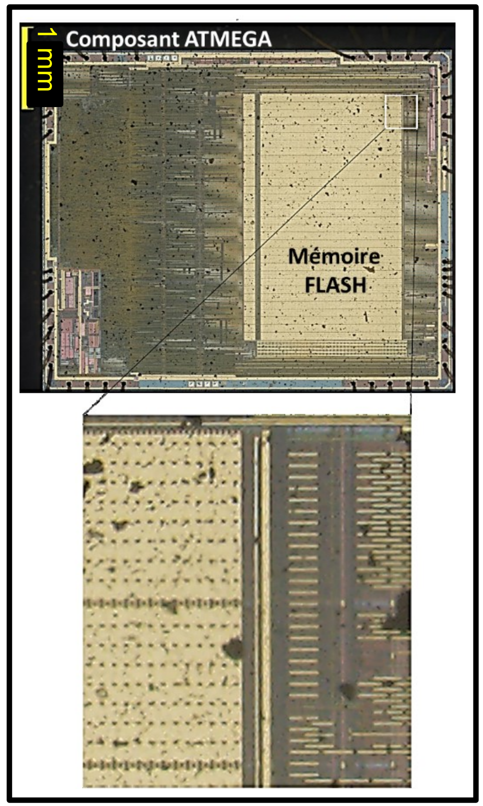
Tomo X =>

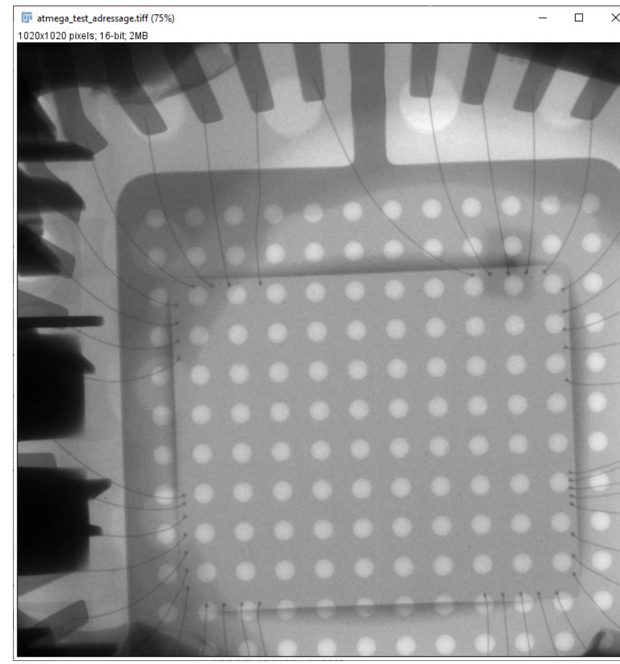
Optique

Transmission X

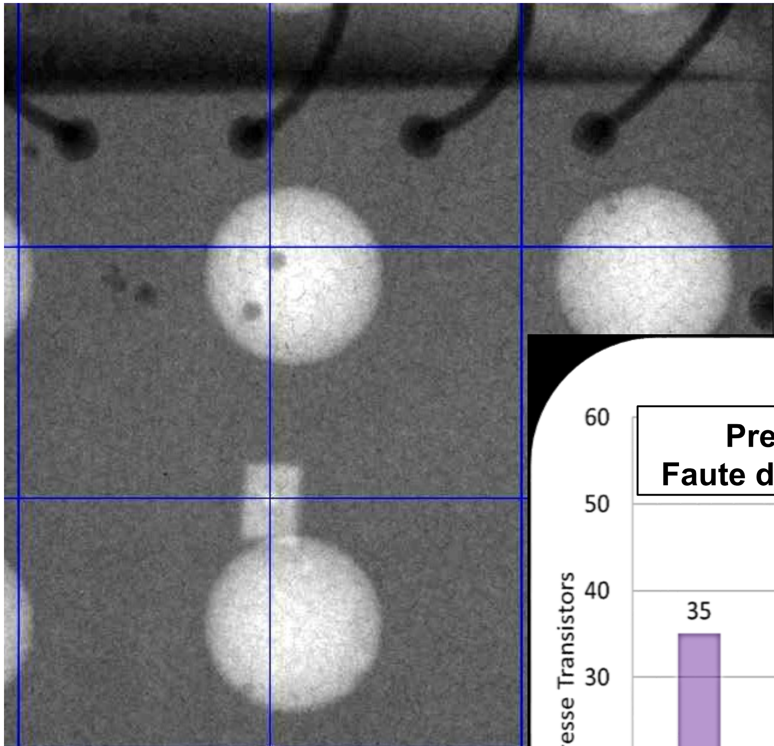
MEB

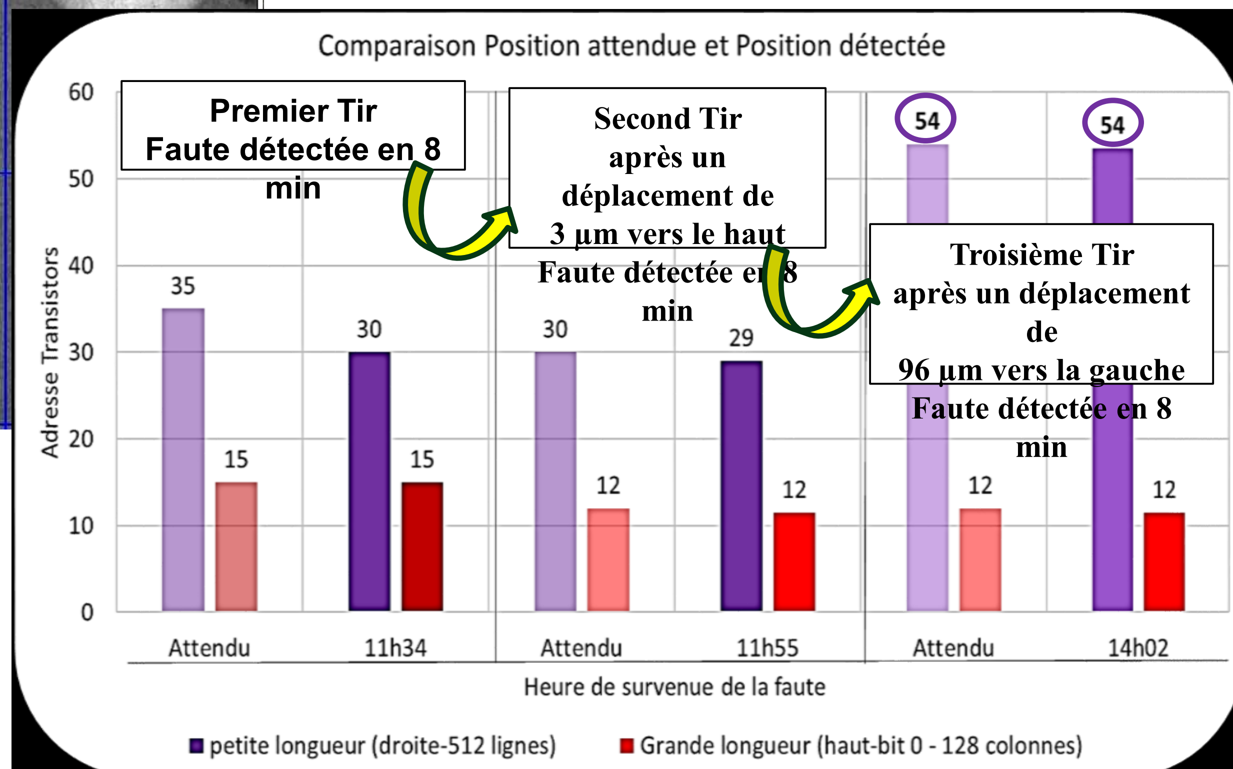






POSITIONNEMENT PRECIS
RESULTATS





LOW ATTACK POTENTIAL X RAY

- Single bit obtained on 90 nm MCU
- Difficult to target specific cells
- Fault takes time (10s minutes)

Future works :

- Impact if several transistors are perturbed ?
- Mechanical aspects : Better alignment / Smaller masks

ARE X-RAY A RELEVANT THREAT FOR SECURITY ?

- **With a synchrotron => clearly yes, with a high attack potential**
  - Expensive (but not so much indeed)
  - Access not easy
  - Lot of knowledge on the TOE

- **W/o synchrotron => not sure…**
  - Still work to do to obtain at least the same control as for laser fault injections

- **Questions ?**