SMACD'17
June 15, 2017

Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos

LIRMM

tima

MINES Saint-Étienne
Une école de l'IMT

SMACD'17
June 15, 2017

Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos

LIRMM

tima

MINES Saint-Étienne
Une école de l'IMT

Outline

Outline

Many Smart Cards among us nowadays

Many Smart Cards among us nowadays

Credit/Debit Card

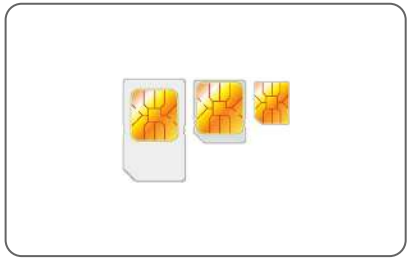
Passport

Company Badge

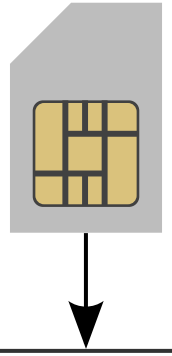
Health Insurance

ID Card

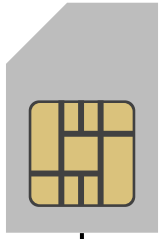
Phone SIM Card



And more...

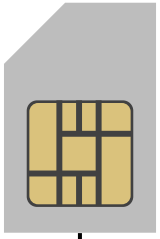


Smart Card is not only a data storage



Smart Card is not only a data storage

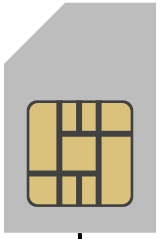
It's a secure **microcontroller**



Smart Card is not only a data storage

It's a secure **microcontroller**

Encryption algorithms such as AES, DES, 3DES, RSA and ECC

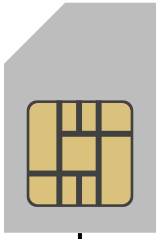


Smart Card is not only a data storage

It's a secure **microcontroller**

Encryption algorithms such as AES, DES, 3DES, RSA and ECC

Fault-based attack to extract confidential data



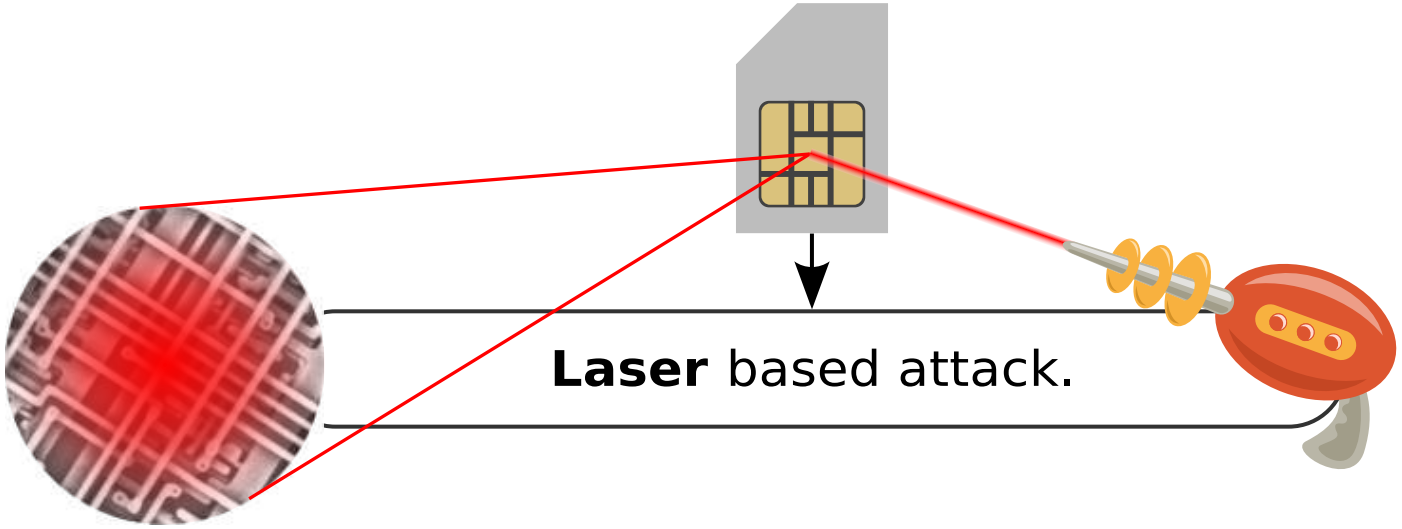
Smart Card is not only a data storage

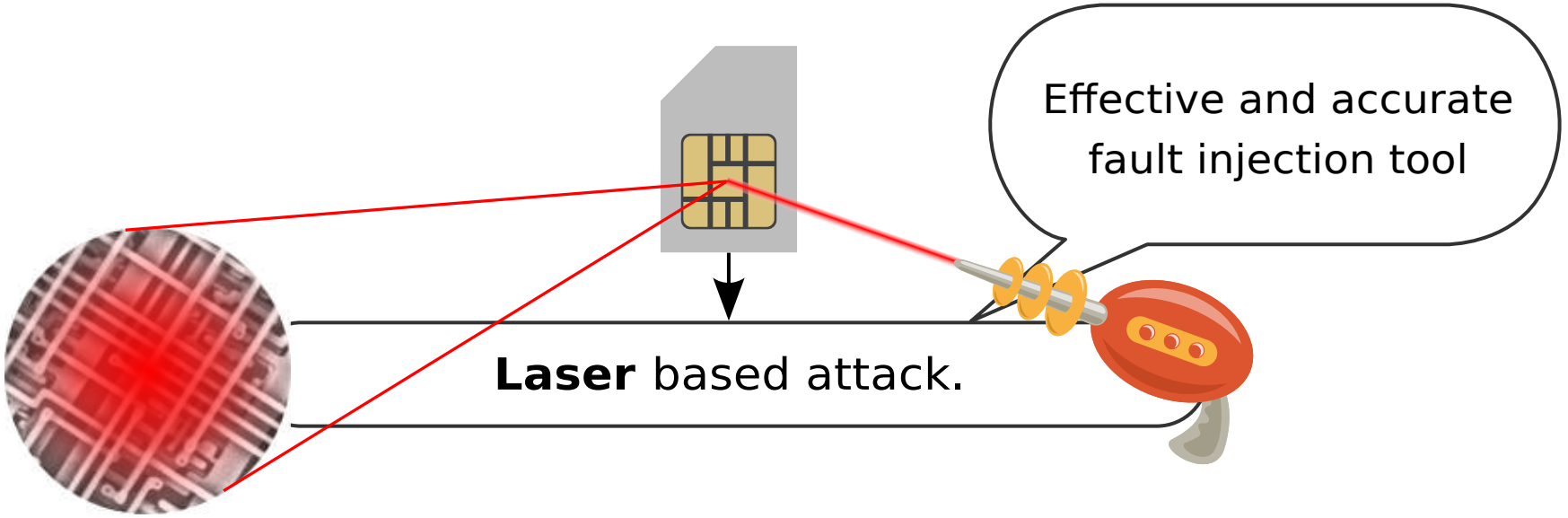
It's a secure **microcontroller**

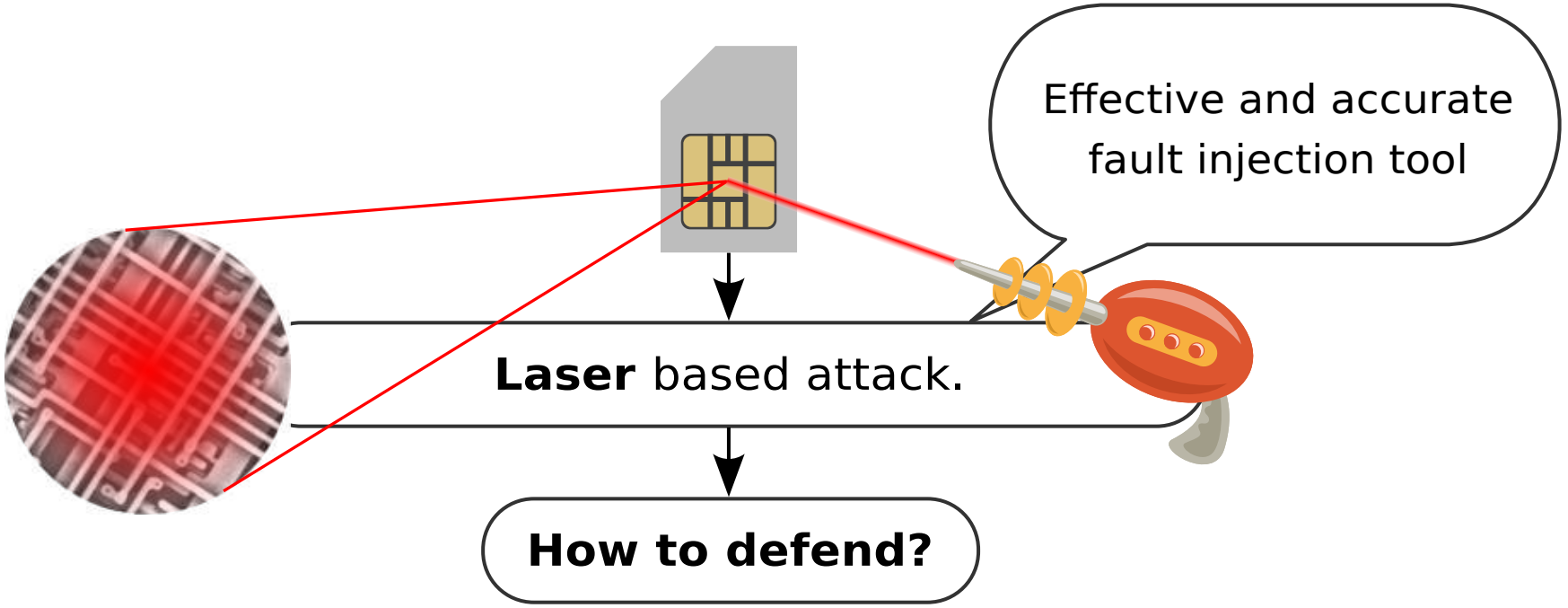
Encryption algorithms such as AES, DES, 3DES, RSA and ECC

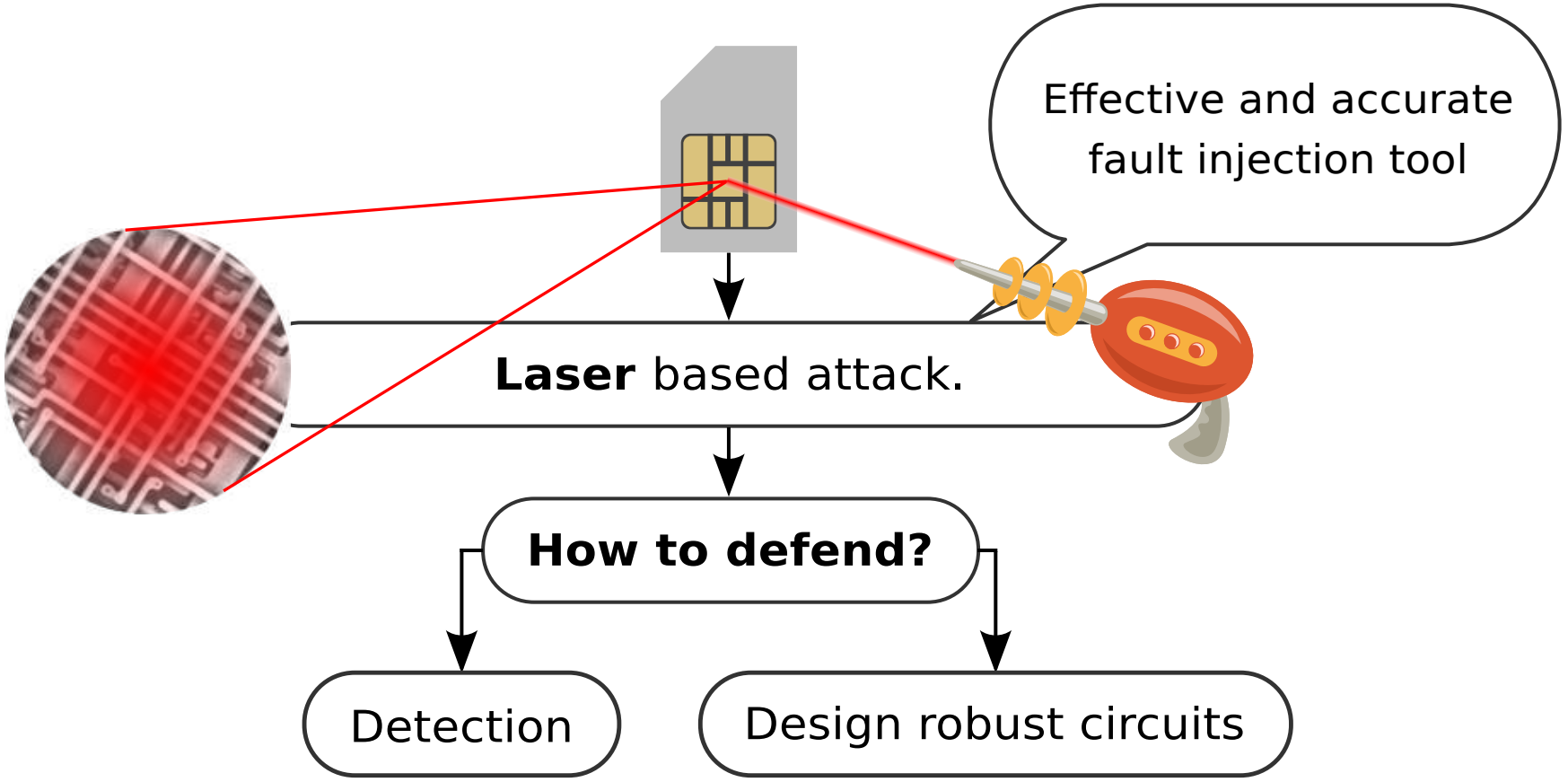
Fault-based attack to extract confidential data

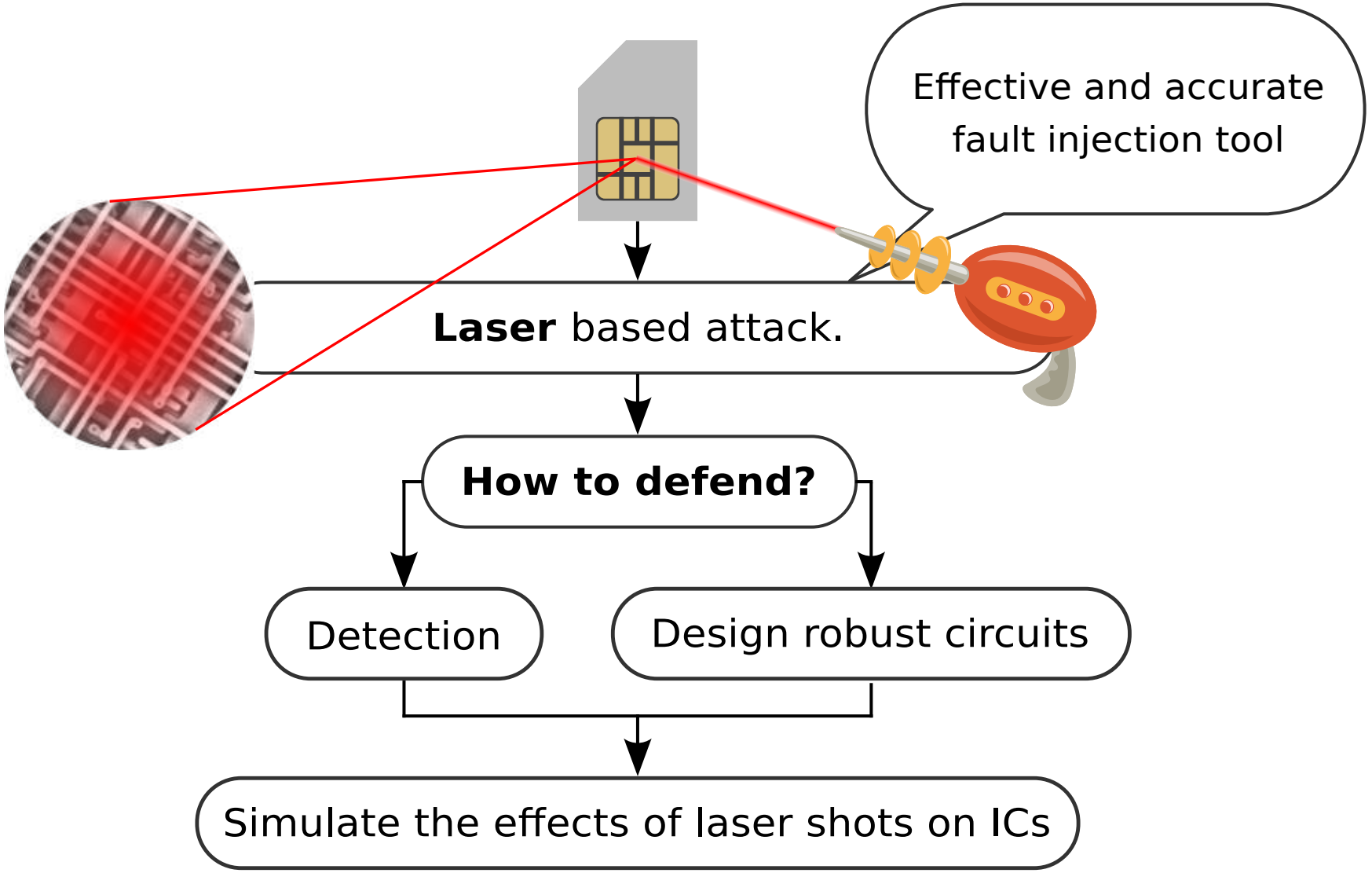
How to attack?

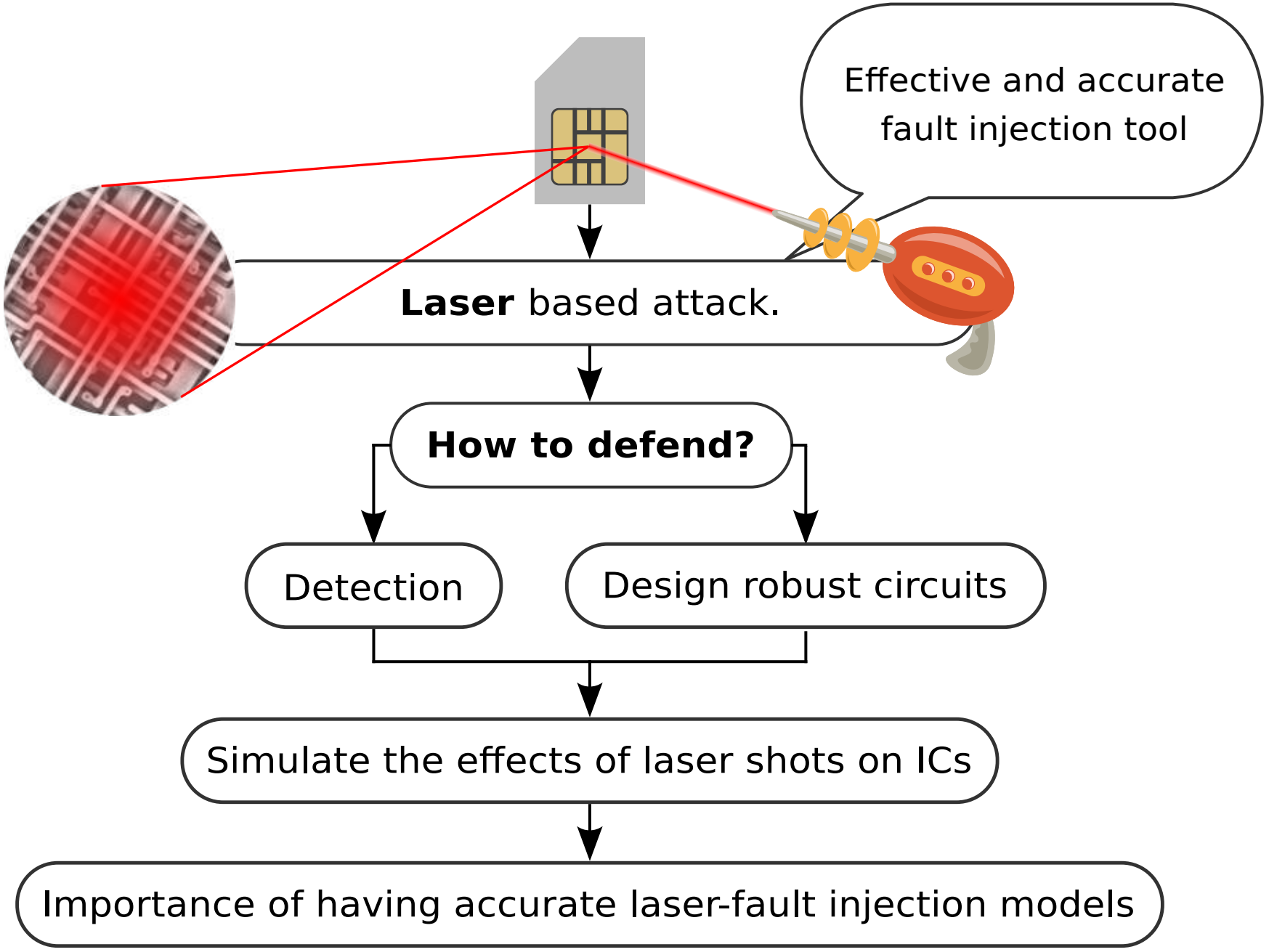

Laser based attack.


Effective and accurate fault injection tool
Laser based attack.


Effective and accurate fault injection tool
Laser based attack.
How to defend?

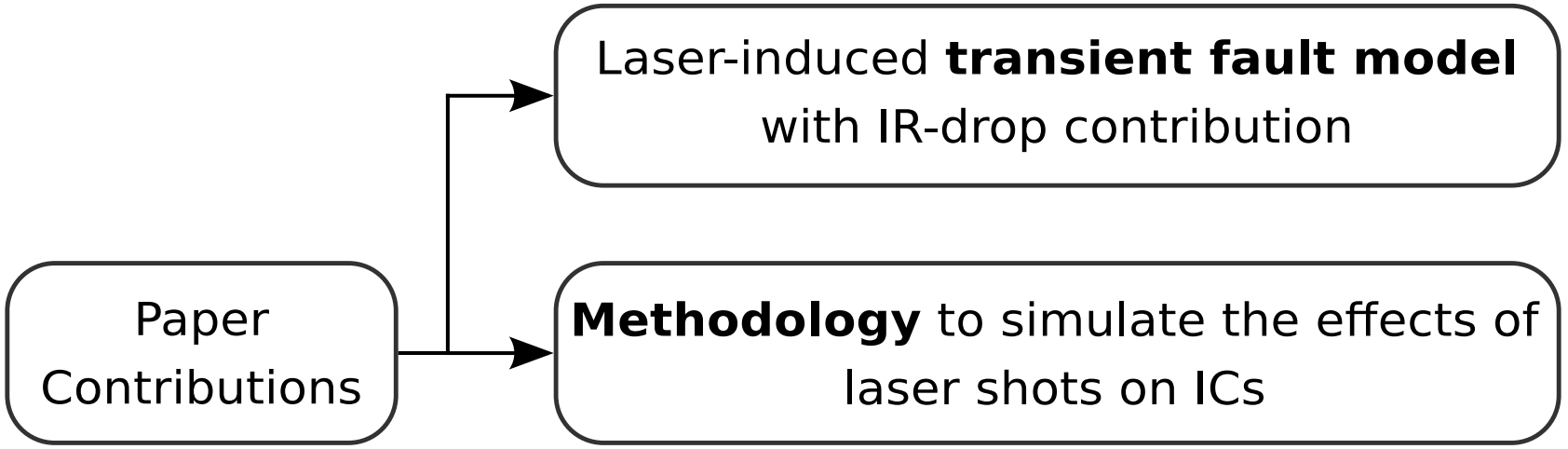

Effective and accurate fault injection tool
Laser based attack.
How to defend?
Detection
Design robust circuits


Effective and accurate fault injection tool
Laser based attack.
How to defend?
Detection
Design robust circuits
Simulate the effects of laser shots on ICs


Effective and accurate fault injection tool
Laser based attack.
How to defend?
Detection
Design robust circuits
Simulate the effects of laser shots on ICs
Importance of having accurate laser-fault injection models

Paper Contributions

Laser-induced **transient fault model** with IR-drop contribution


Paper Contributions
Laser-induced **transient fault model** with IR-drop contribution
Methodology to simulate the effects of laser shots on ICs

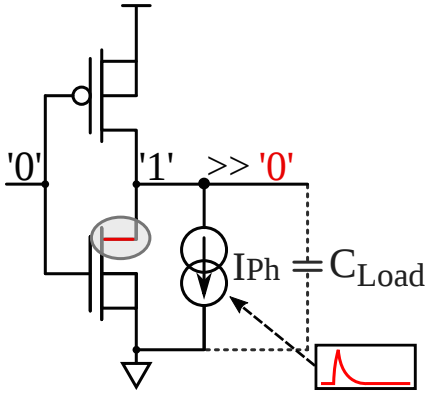
Paper Contributions

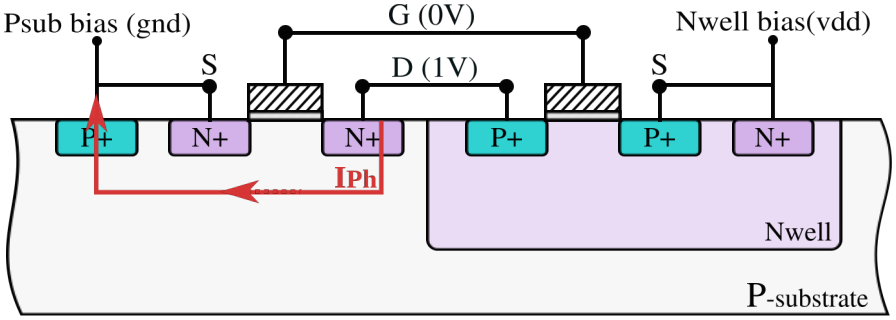
- Laser-induced **transient fault model** with IR-drop contribution
- **Methodology** to simulate the effects of laser shots on ICs
- Analyse the impact of laser-induced **IR-drop** in the fault injection process

Outline

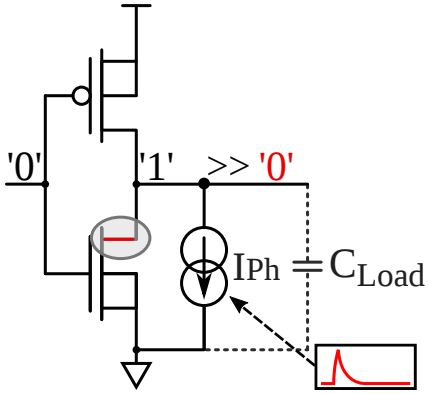
Outline

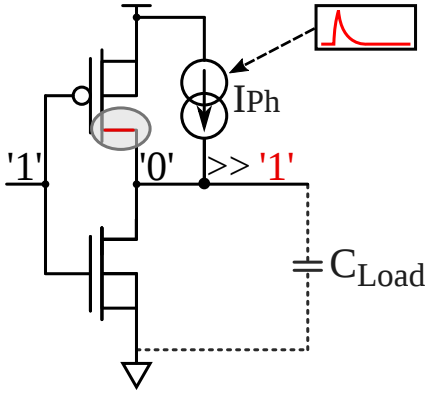
Classical model for simulating laser-induced transient currents on ICs

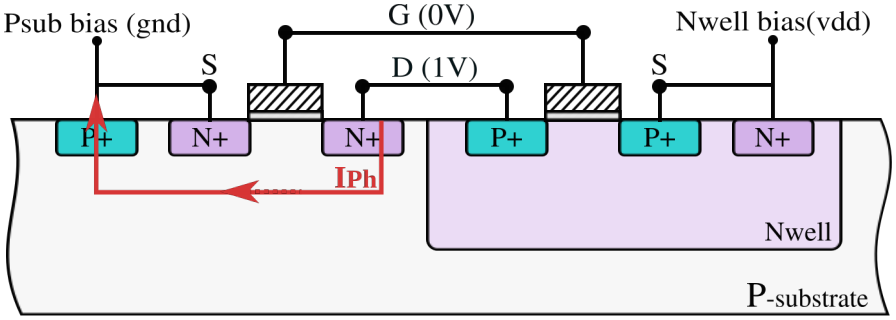


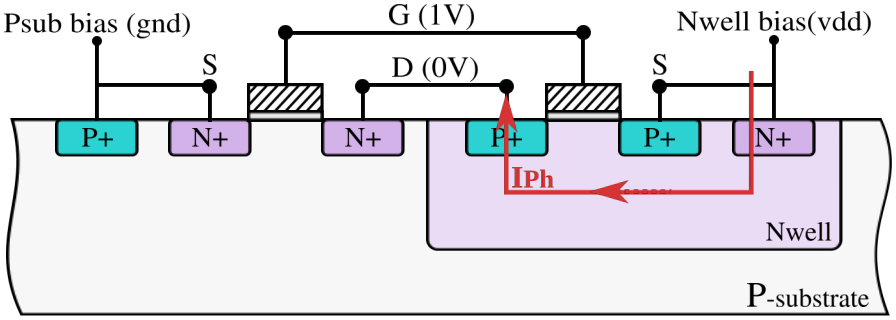


Classical model for simulating laser-induced transient currents on ICs

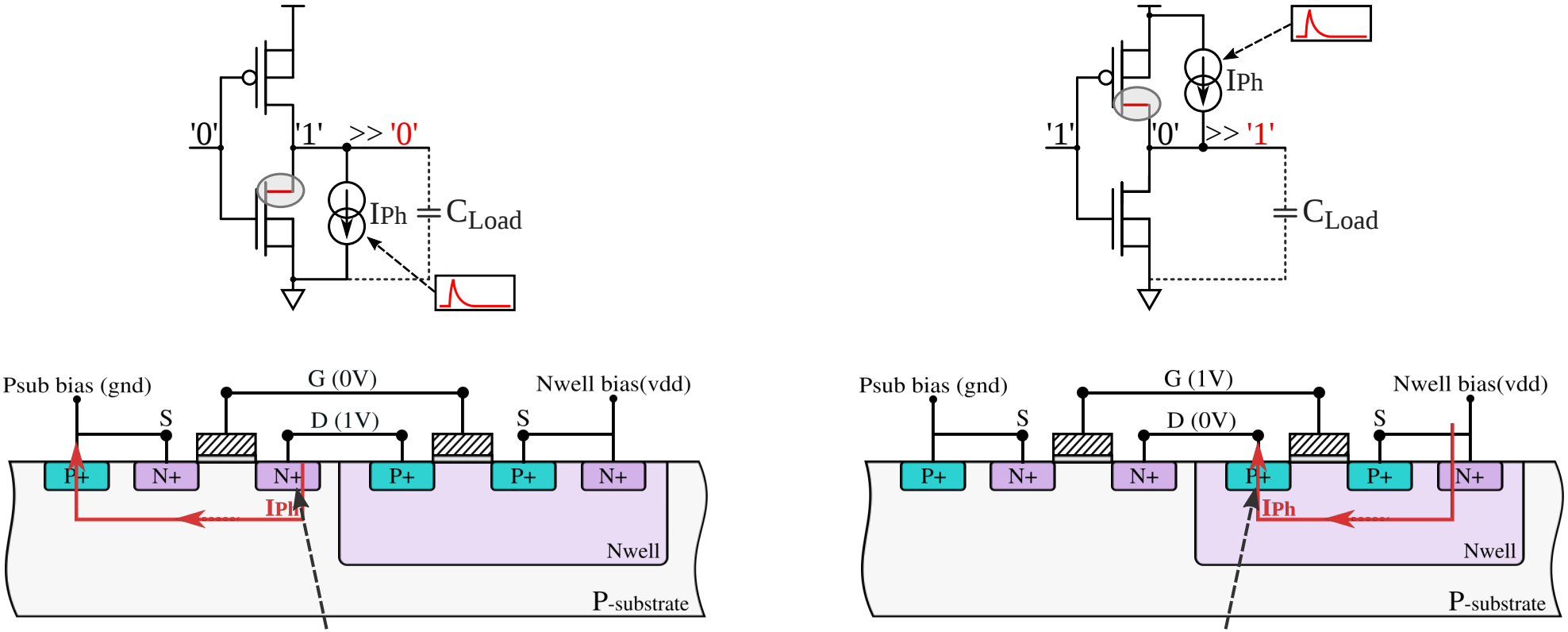






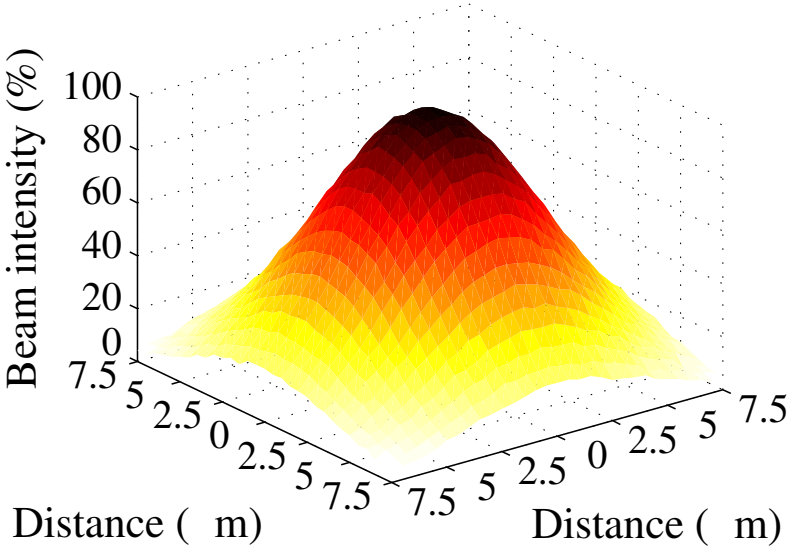


Classical model for simulating laser-induced transient currents on ICs



sensitive areas (reverse biased PN junction between the drain and the substrate)

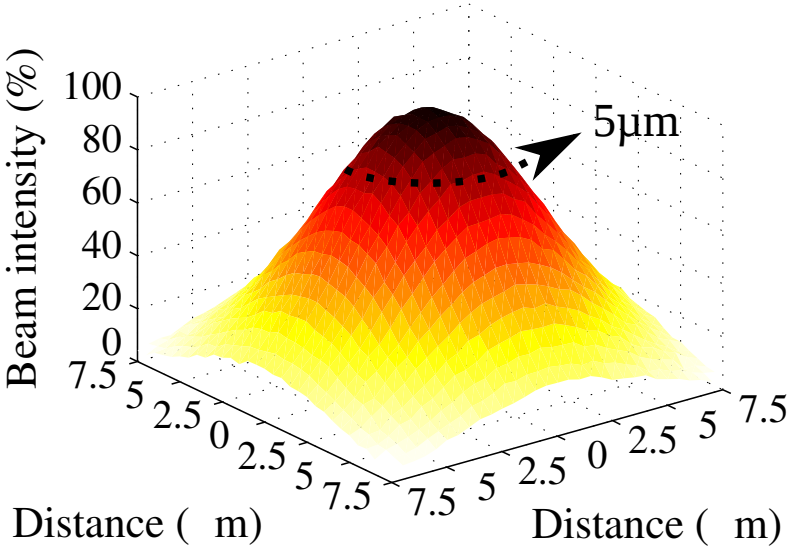
Spatial distribution of the laser-induced photocurrent



$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S$$

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”

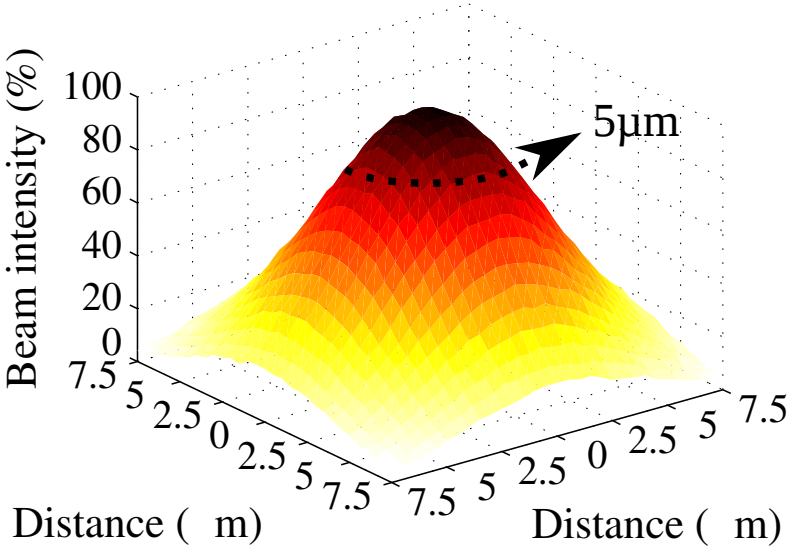
Spatial distribution of the laser-induced photocurrent

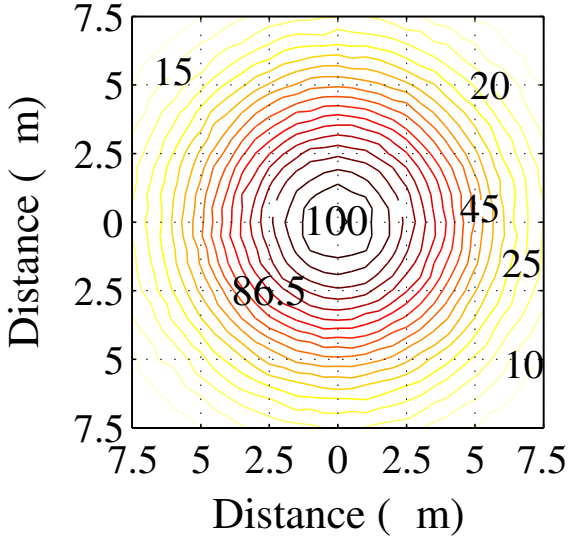


$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S$$

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”

Spatial distribution of the laser-induced photocurrent



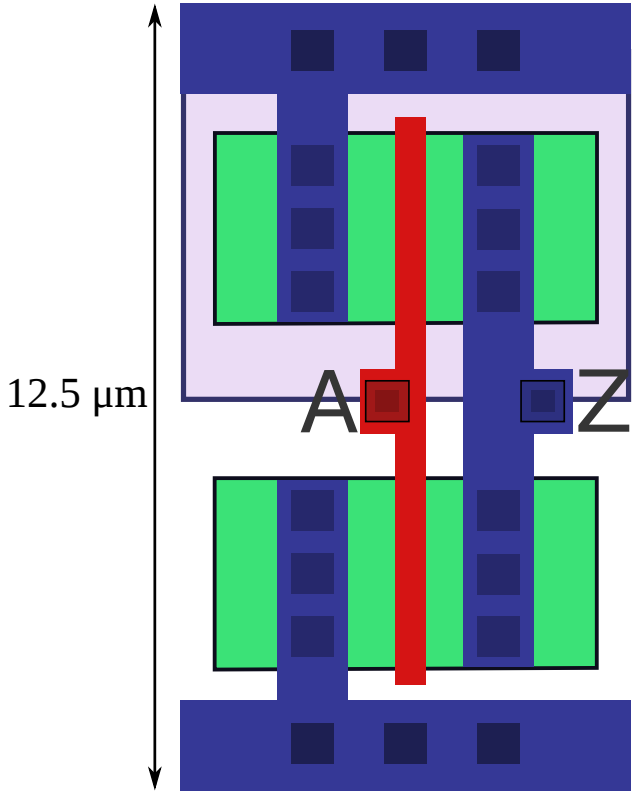


$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S$$

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”

2.2 - Limits of the classical transient fault model

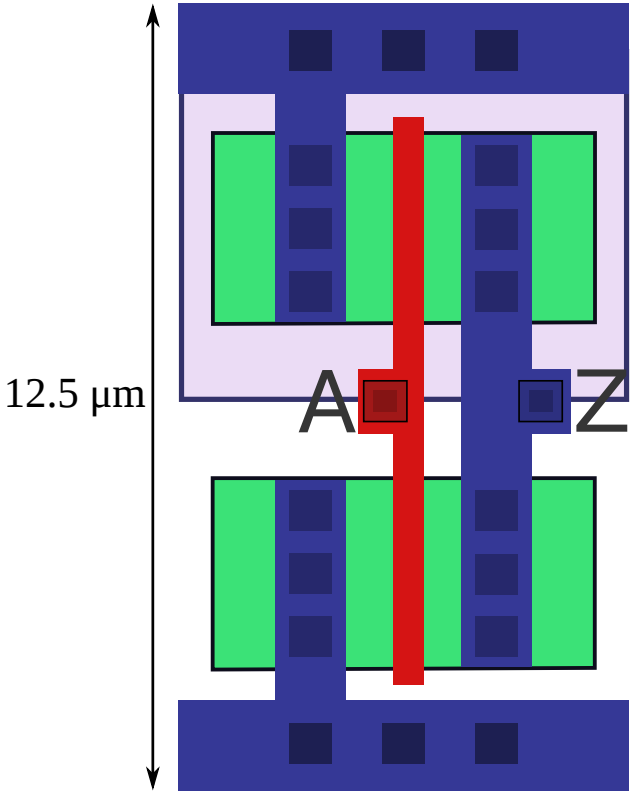
Standard cell(s) illuminated by a 5µm laser spot diameter



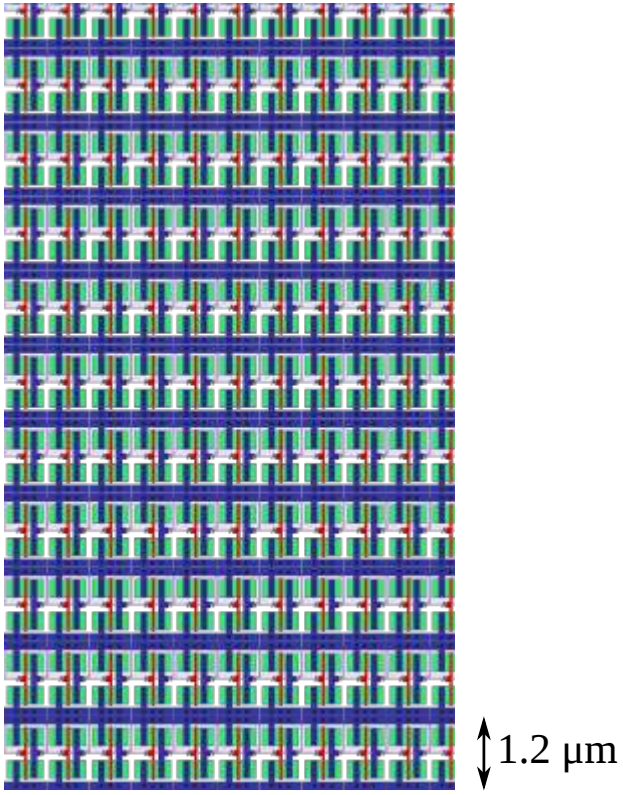
tech: 250 nm

2.2 - Limits of the classical transient fault model

Standard cell(s) illuminated by a 5µm laser spot diameter



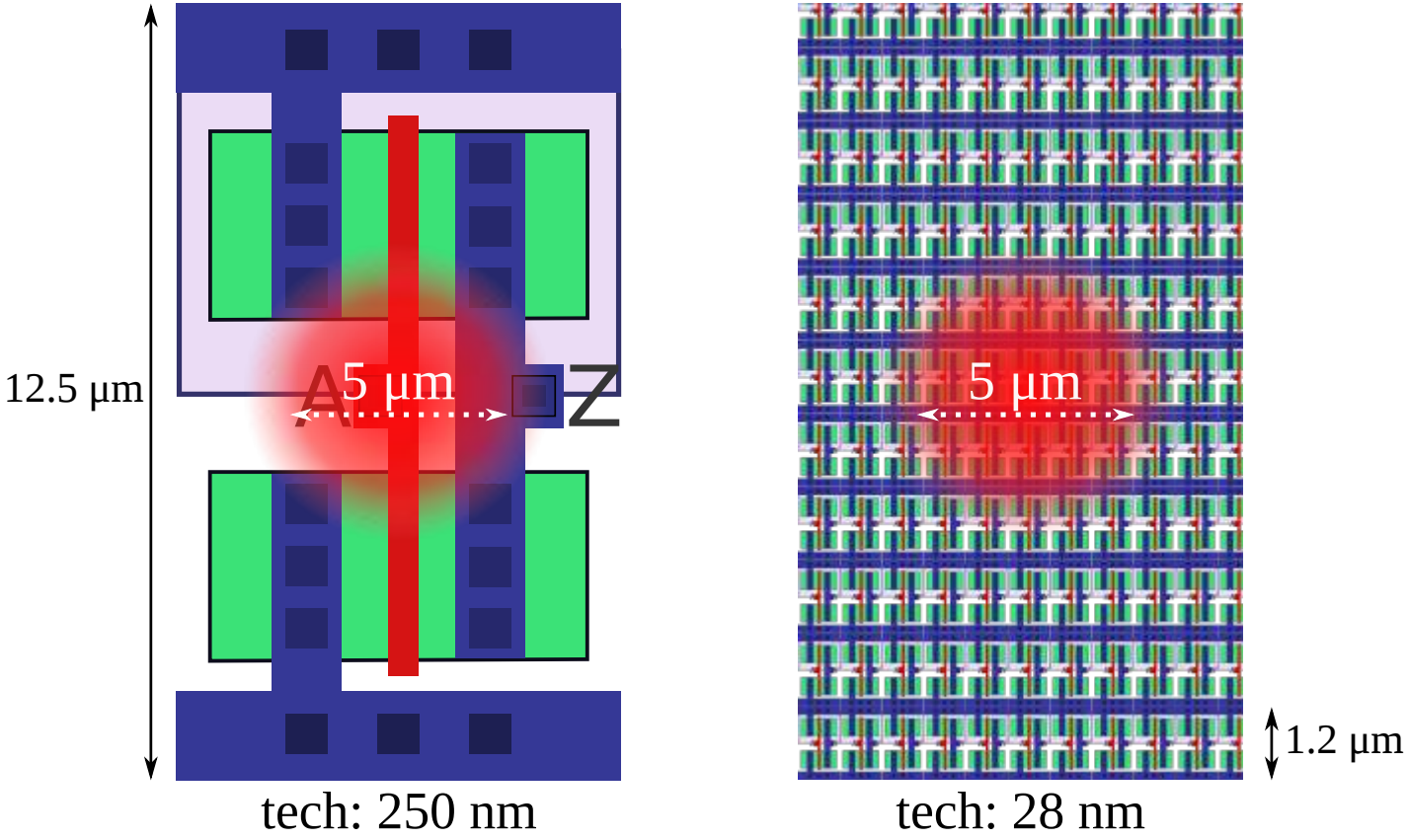
tech: 250 nm



tech: 28 nm

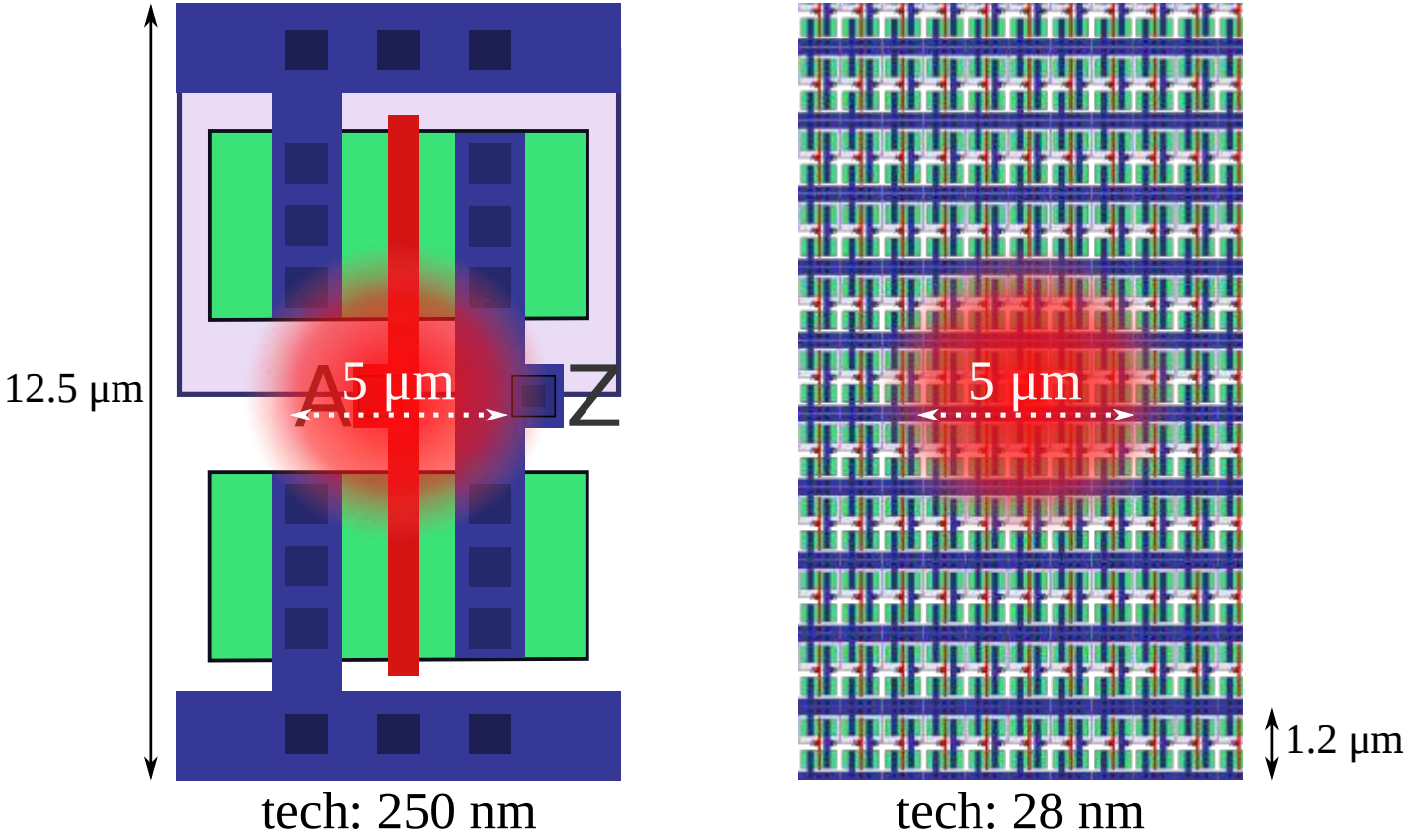
2.2 - Limits of the classical transient fault model

Standard cell(s) illuminated by a 5µm laser spot diameter



2.2 - Limits of the classical transient fault model

Standard cell(s) illuminated by a 5µm laser spot diameter

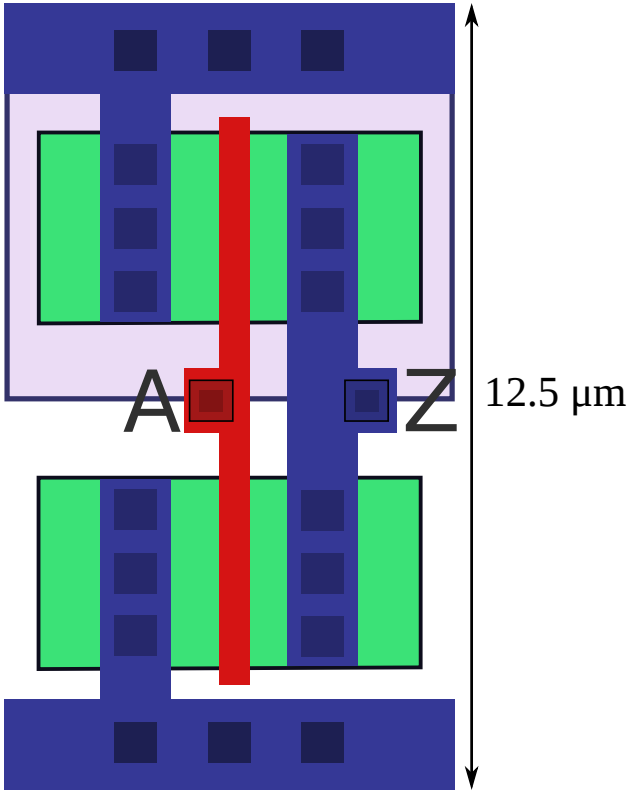


How does the standard cell height influence in the fault injection process?

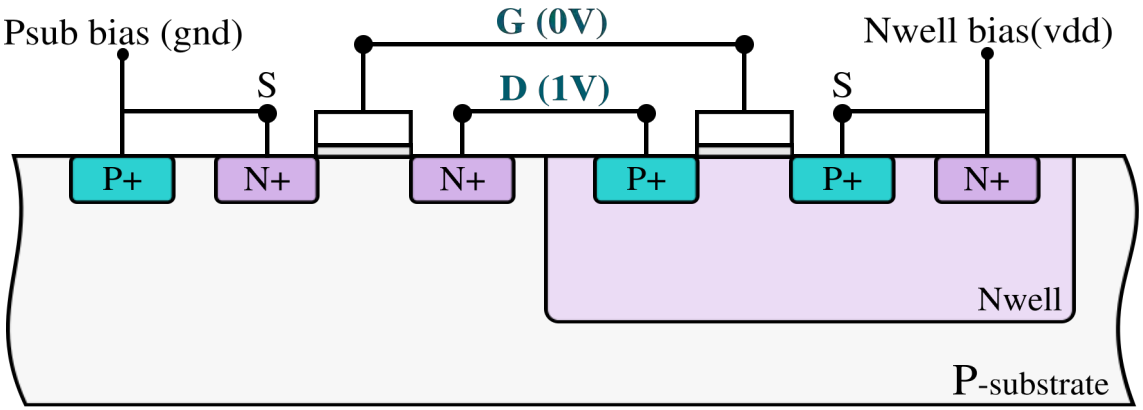
2.2 - Limits of the classical transient fault model

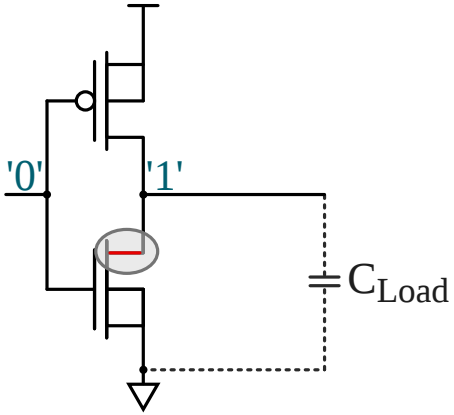
Case 1:

Only NMOS transistors are illuminated by the laser beam



tech: 250 nm

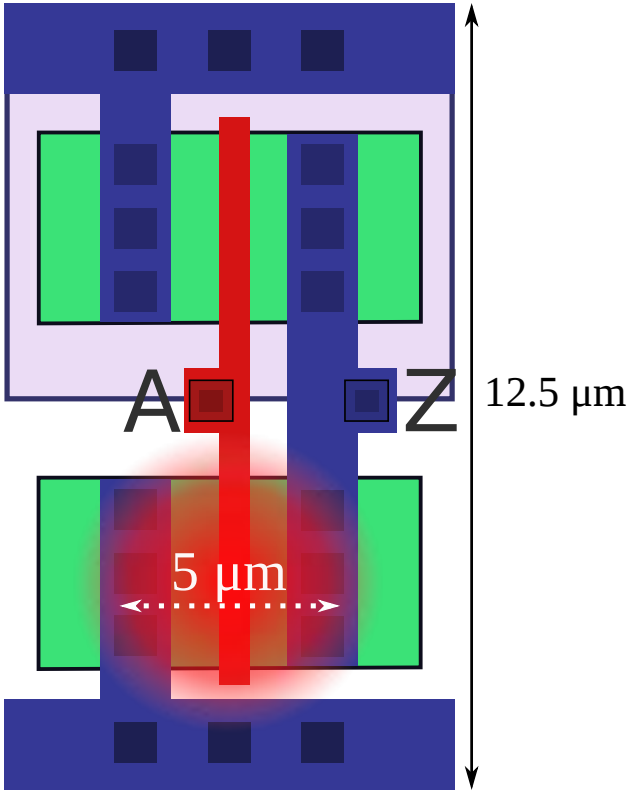




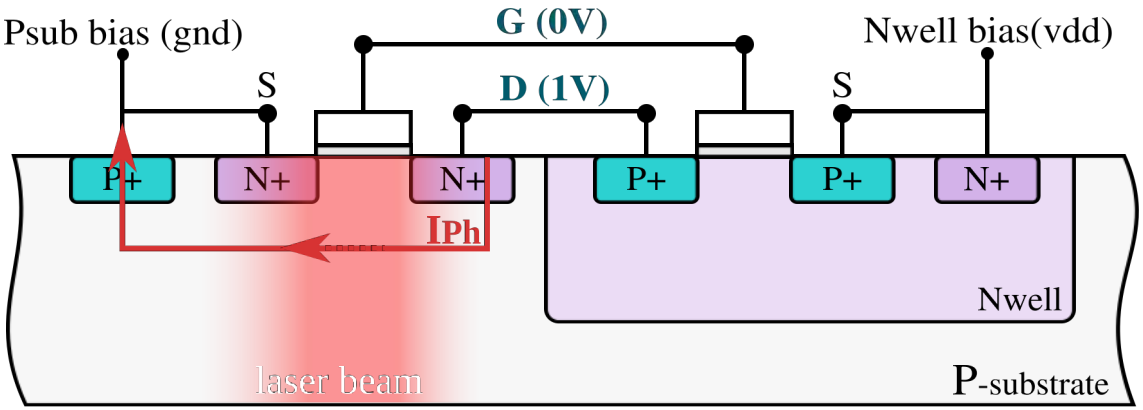
2.2 - Limits of the classical transient fault model

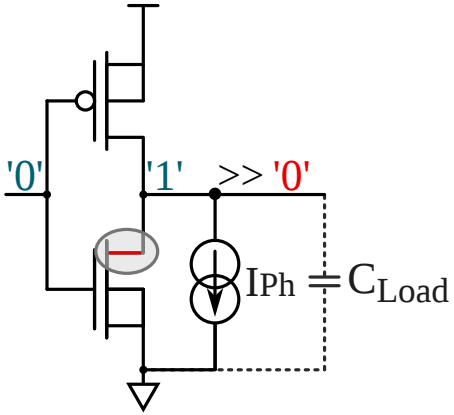
Case 1:

Only NMOS transistors are illuminated by the laser beam



tech: 250 nm

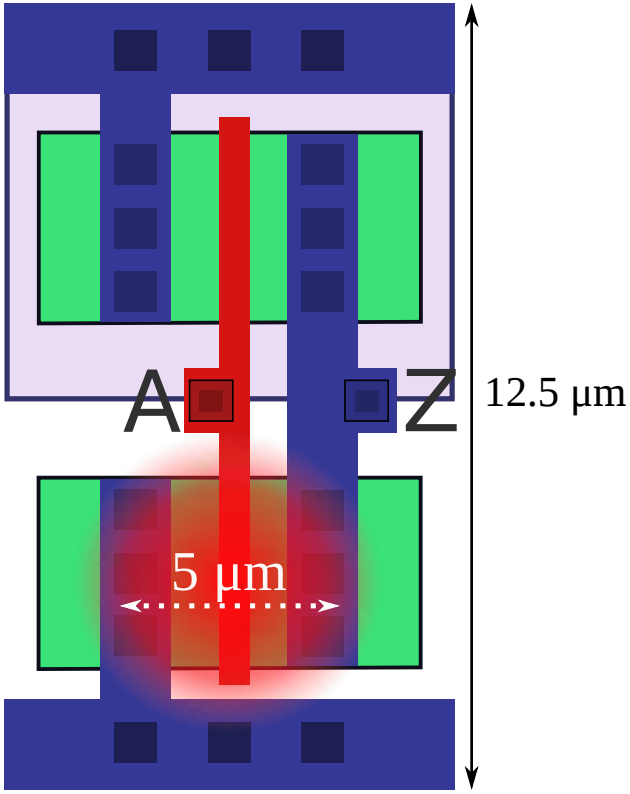




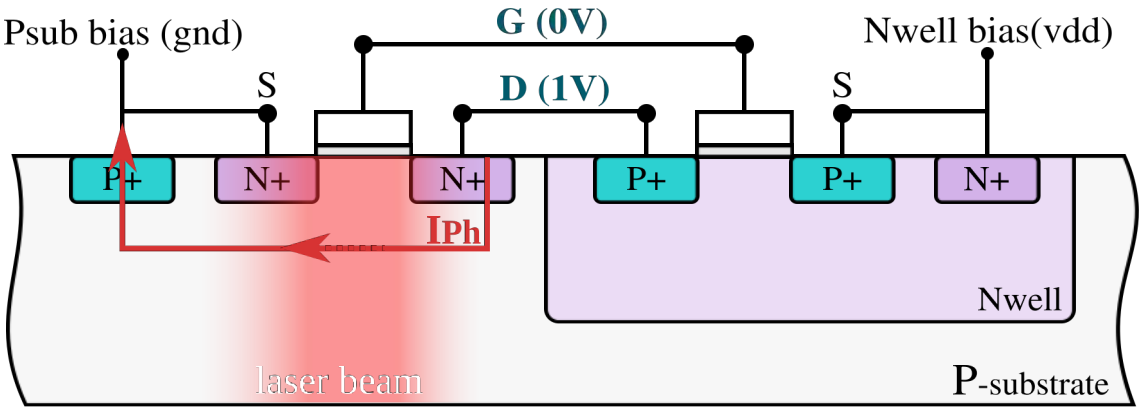
2.2 - Limits of the classical transient fault model

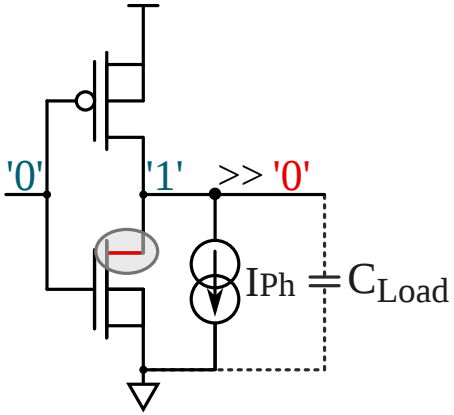
Case 1:

Only NMOS transistors are illuminated by the laser beam



tech: 250 nm



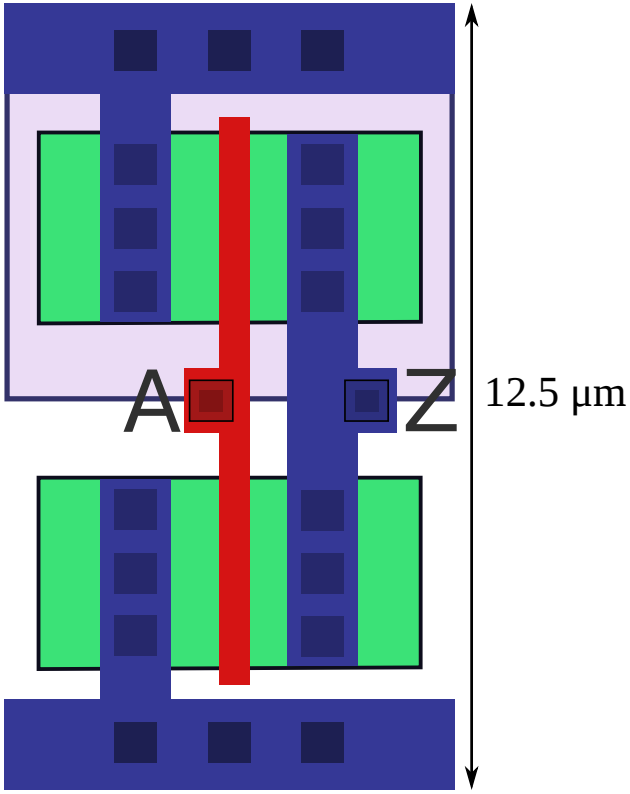


No laser-induced currents in the Nwell-Psub junction (classical model is OK)

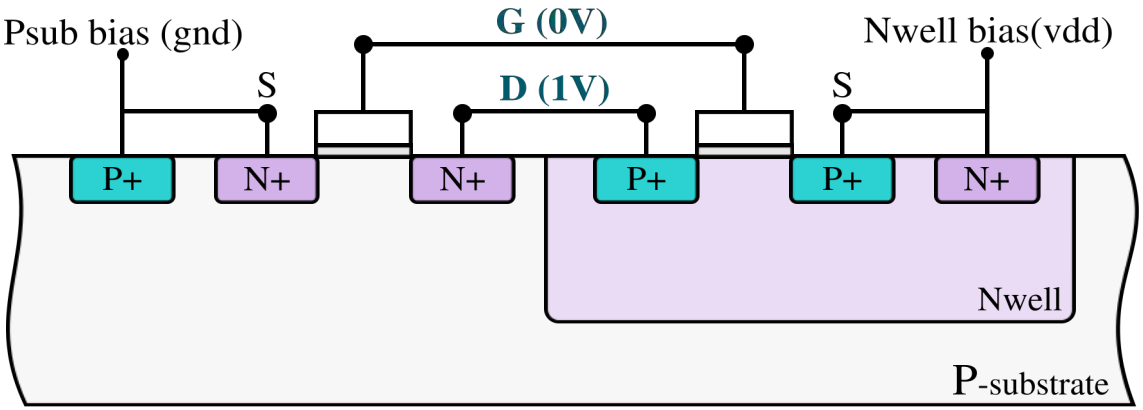
2.2 - Limits of the classical transient fault model

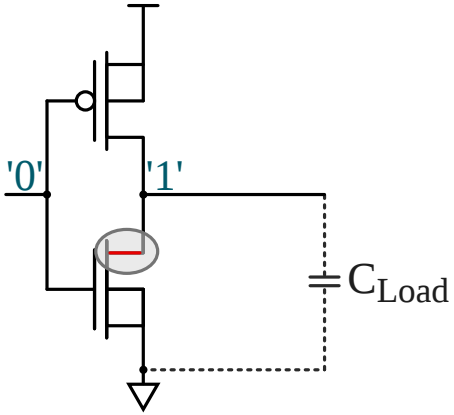
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam



tech: 250 nm

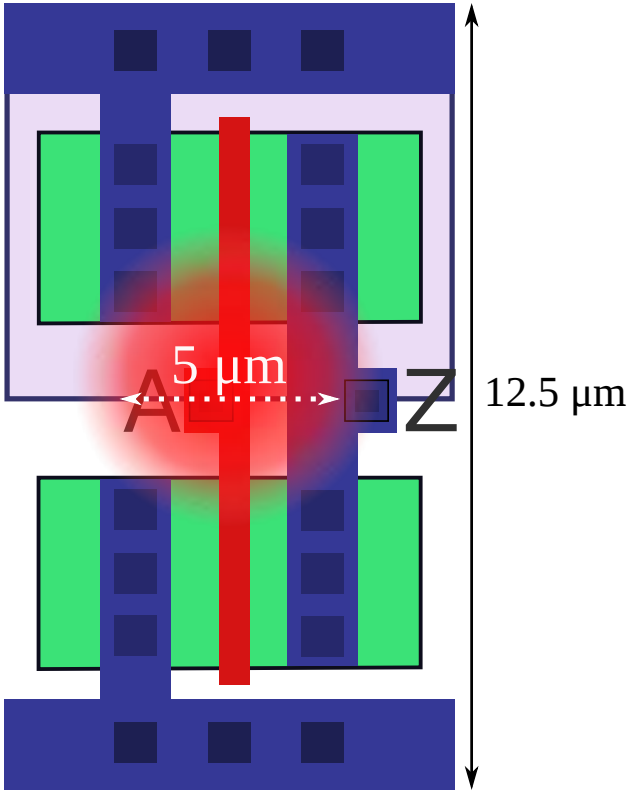




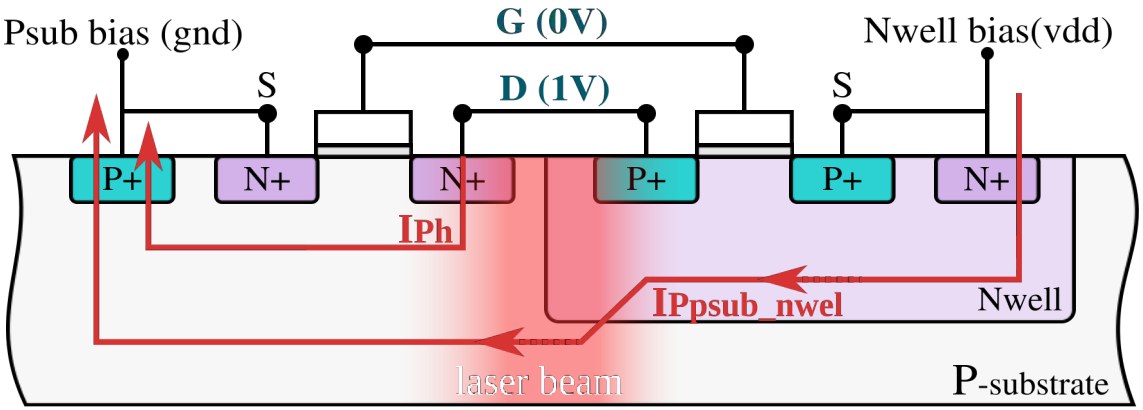
2.2 - Limits of the classical transient fault model

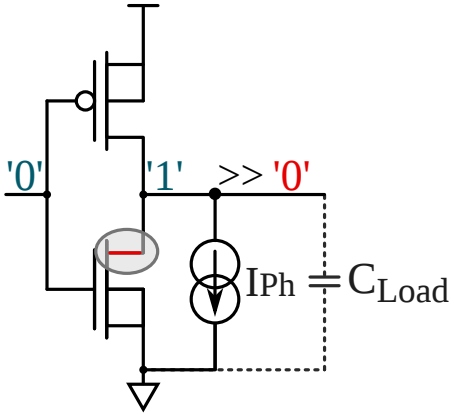
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam



tech: 250 nm

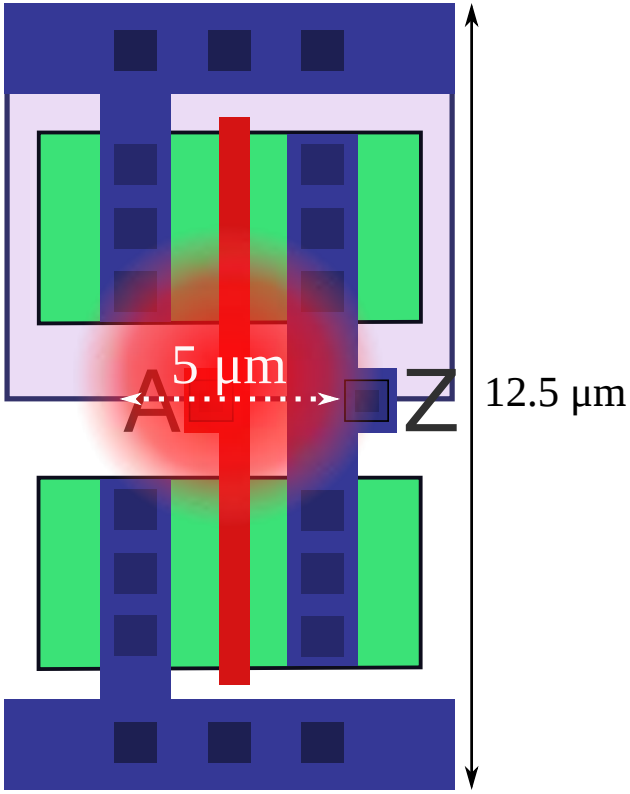




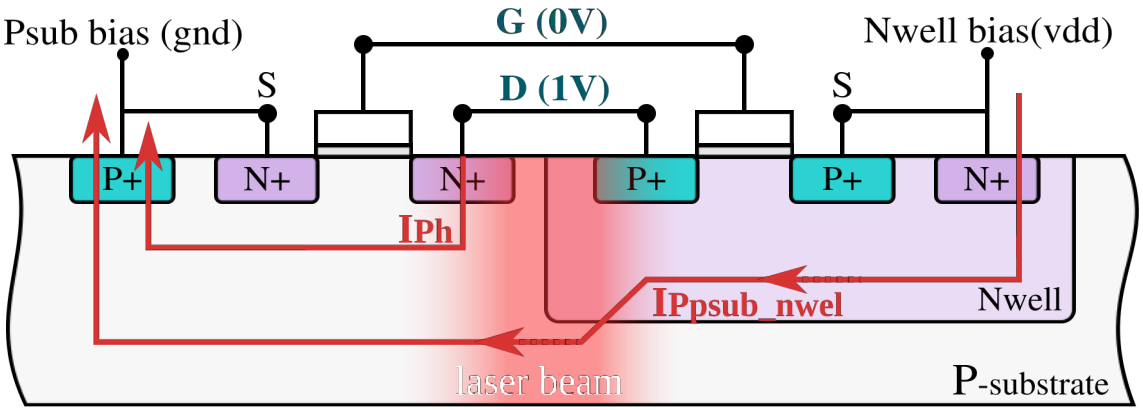
2.2 - Limits of the classical transient fault model

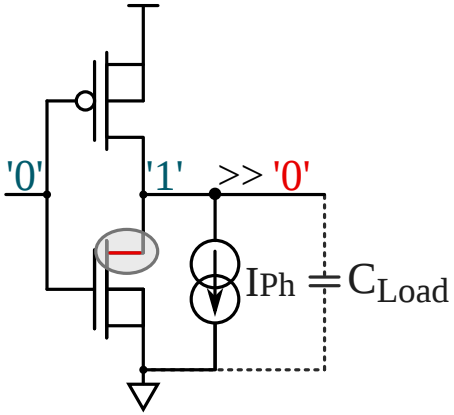
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam



tech: 250 nm



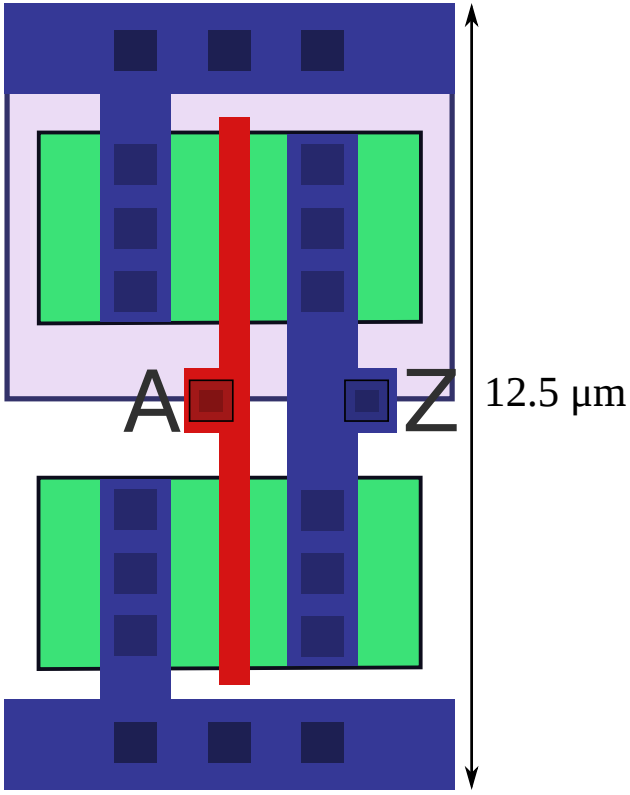


Laser-induced currents
in the Nwell-Psub junction
(classical model is **incomplete**)

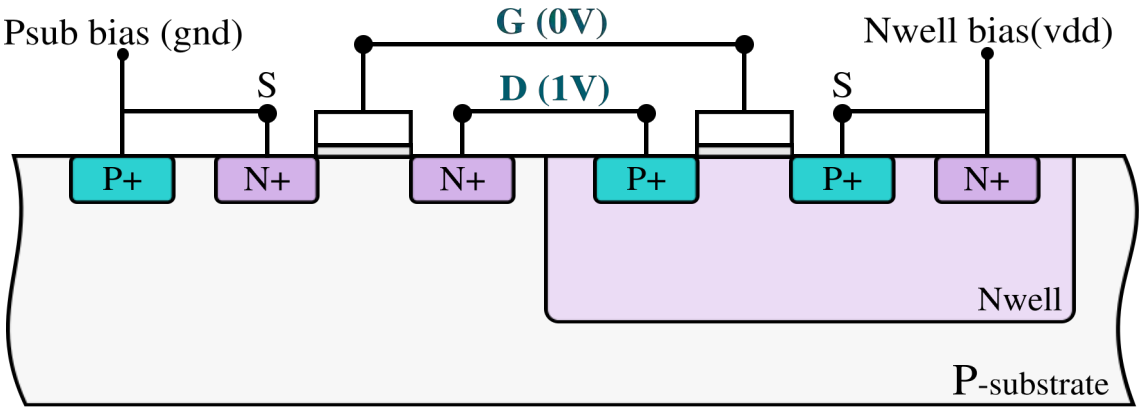
2.2 - Limits of the classical transient fault model

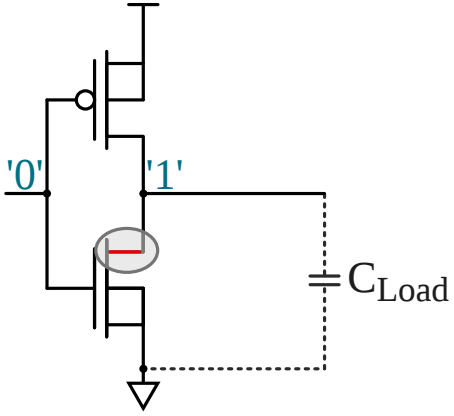
Case 3:

Only PMOS transistors are illuminated by the laser beam



tech: 250 nm

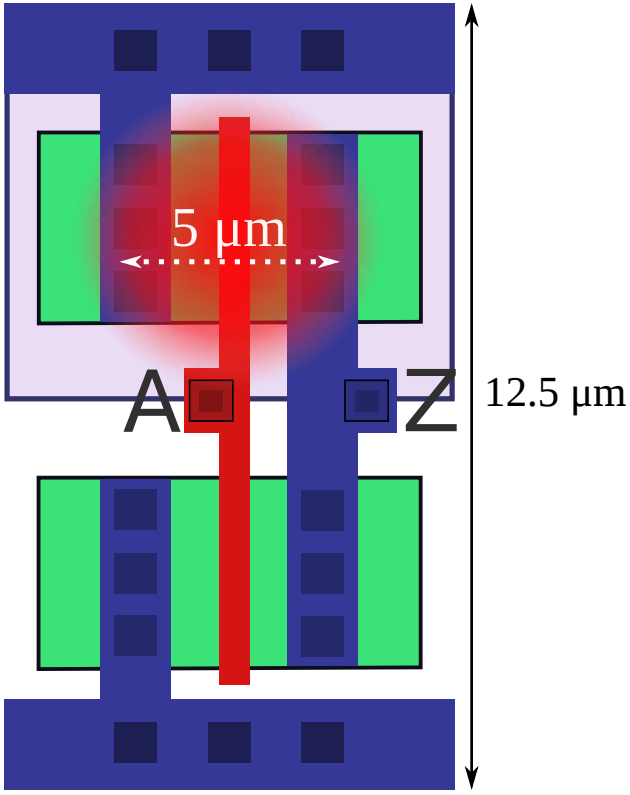




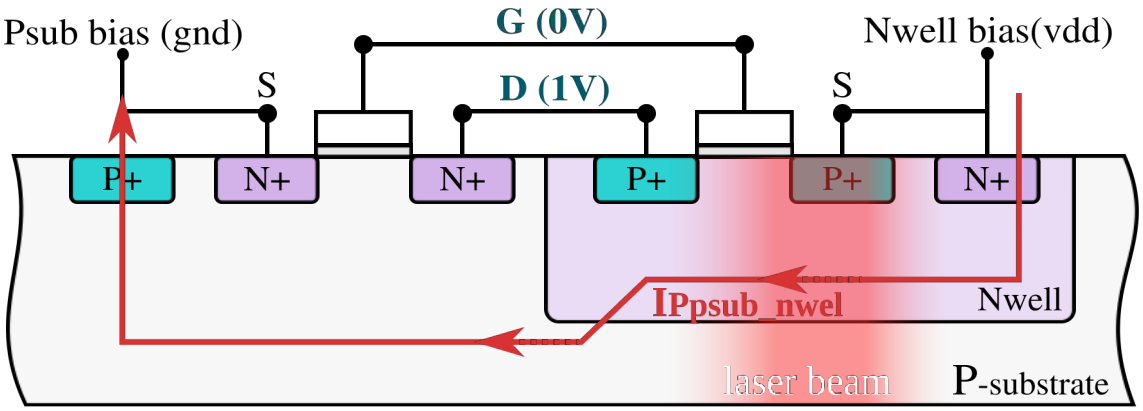
2.2 - Limits of the classical transient fault model

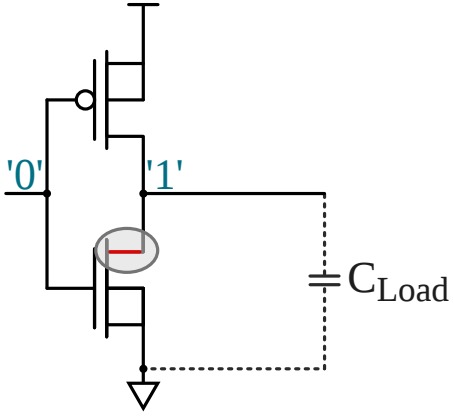
Case 3:

Only PMOS transistors are illuminated by the laser beam



tech: 250 nm

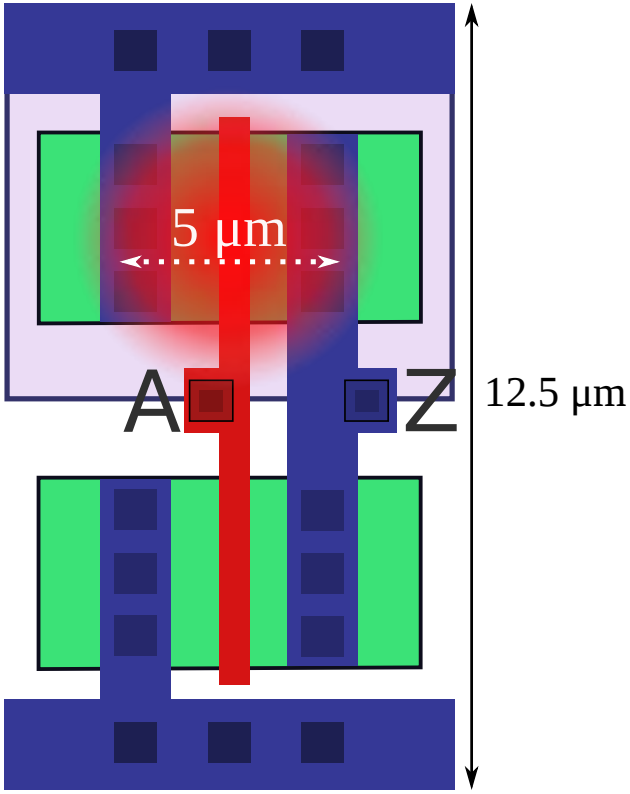




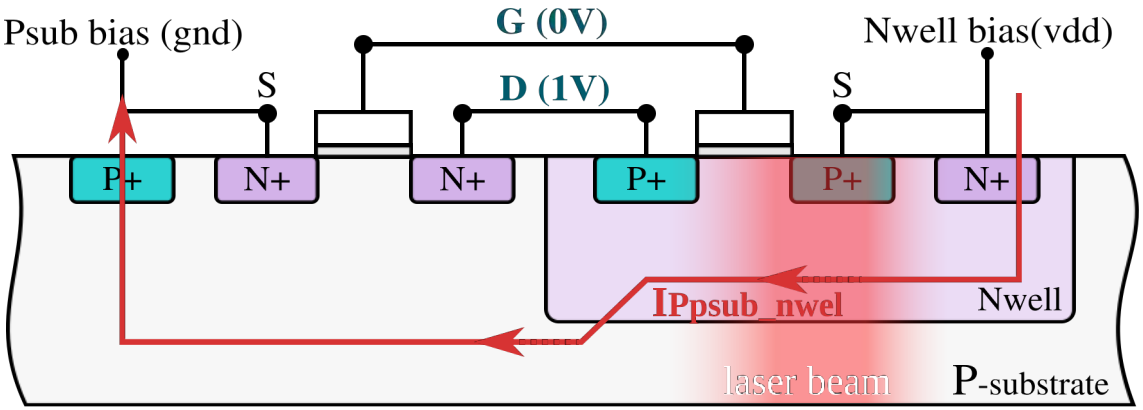
2.2 - Limits of the classical transient fault model

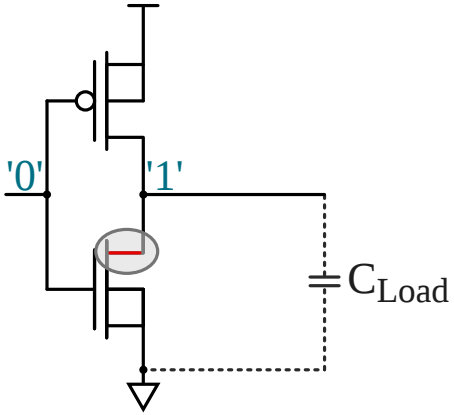
Case 3:

Only PMOS transistors are illuminated by the laser beam



tech: 250 nm



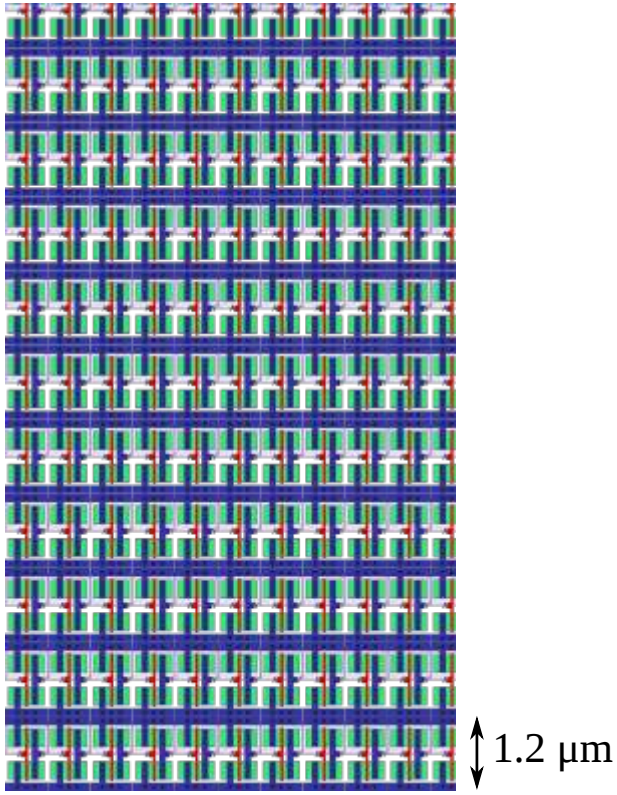


Laser-induced currents
in the Nwell-Psub junction
(classical model is **incomplete**)

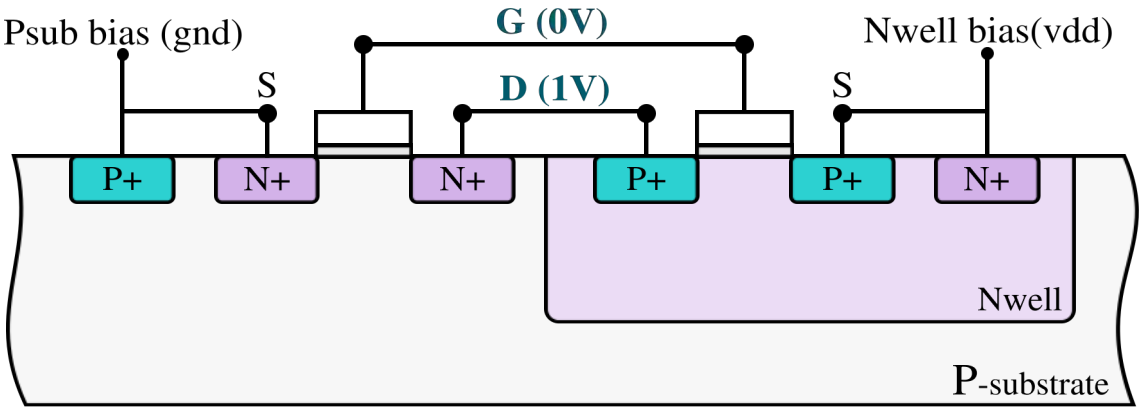
2.2 - Limits of the classical transient fault model

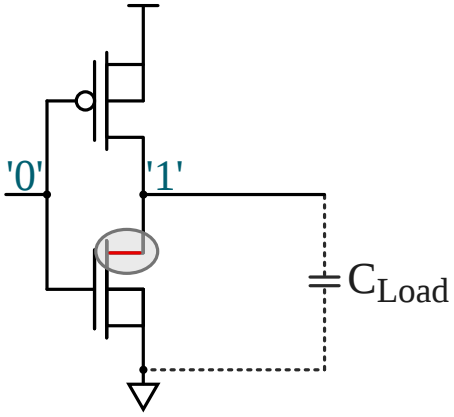
Case 4:

NMOS and PMOS transistors are **always** illuminated by the laser beam



tech: 28 nm

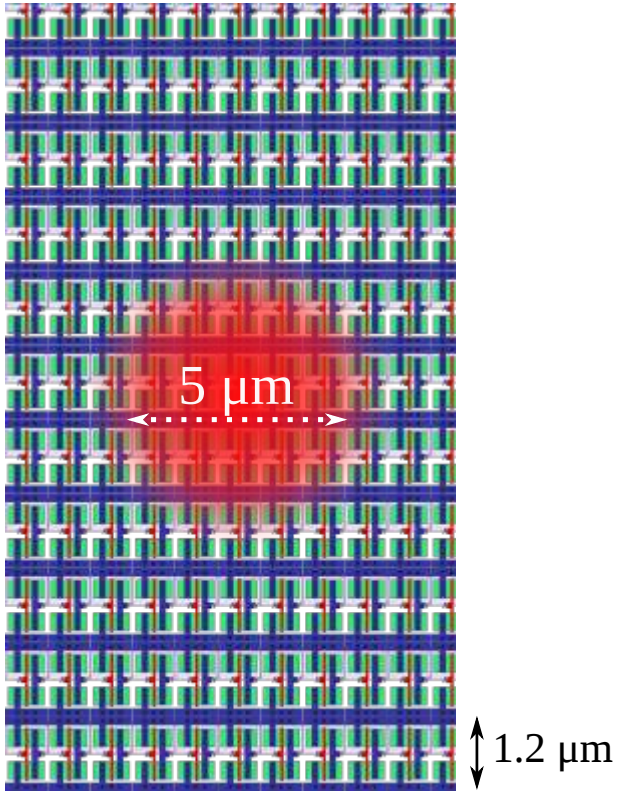




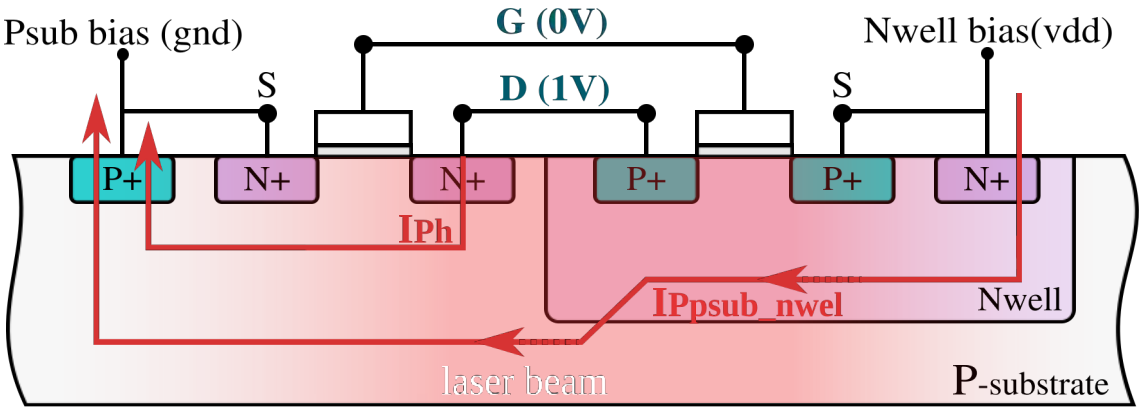
2.2 - Limits of the classical transient fault model

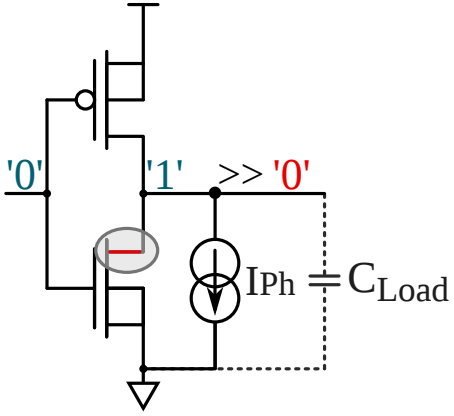
Case 4:

NMOS and PMOS transistors are **always** illuminated by the laser beam



tech: 28 nm

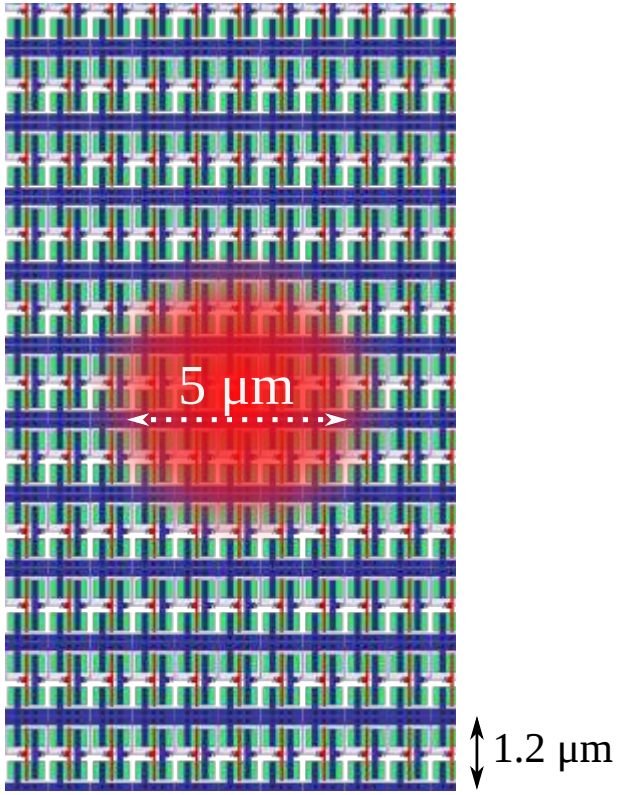




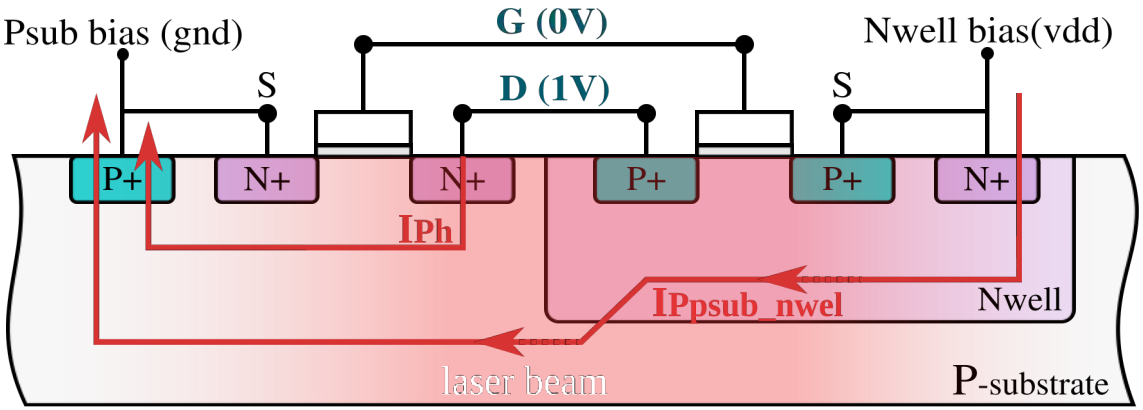
2.2 - Limits of the classical transient fault model

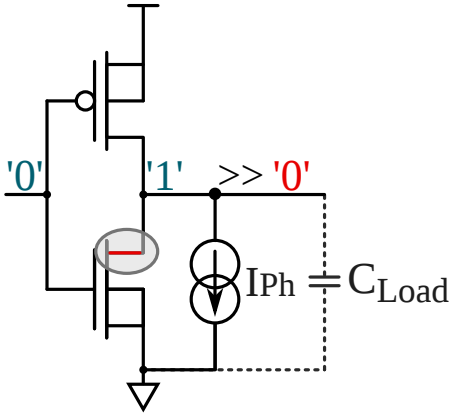
Case 4:

NMOS and PMOS transistors are **always** illuminated by the laser beam



tech: 28 nm





Laser-induced currents
in the Nwell-Psub junction
(classical model is **incomplete**)

Outline

Outline

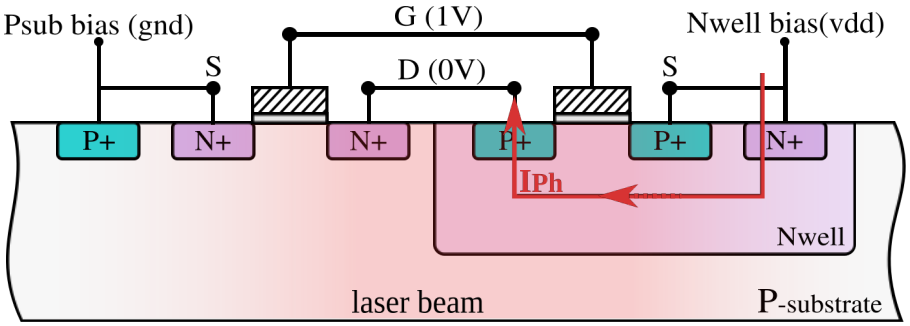
3.1 - Upgraded electrical model

Classical Model

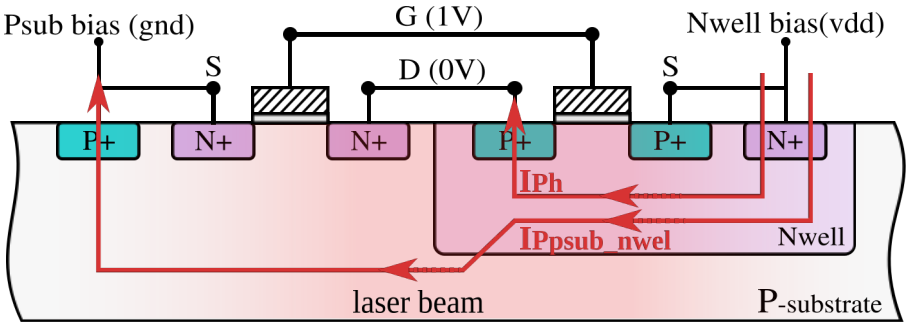
Upgraded Electrical Model

3.1 - Upgraded electrical model

Classical Model

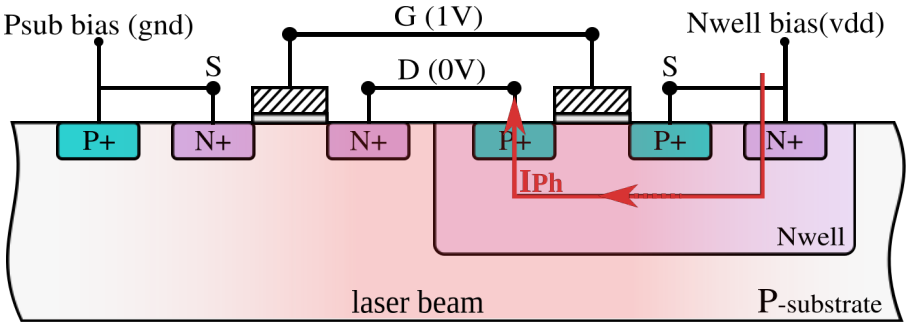


Upgraded Electrical Model

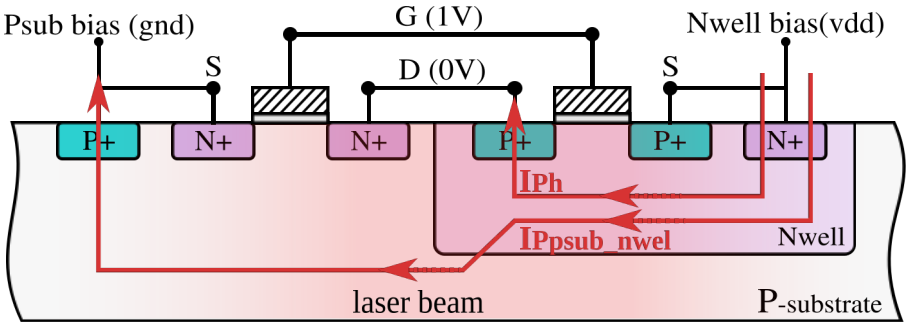


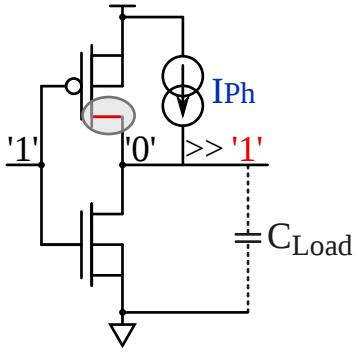
3.1 - Upgraded electrical model

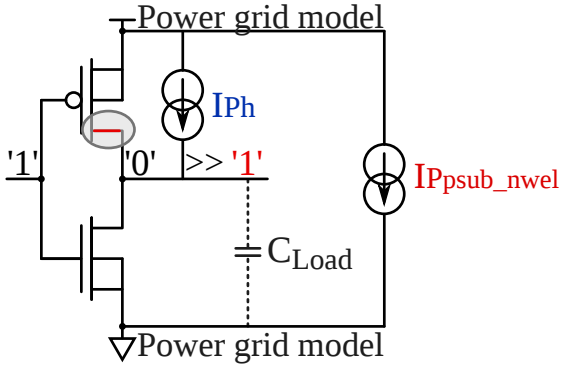
Classical Model



Upgraded Electrical Model





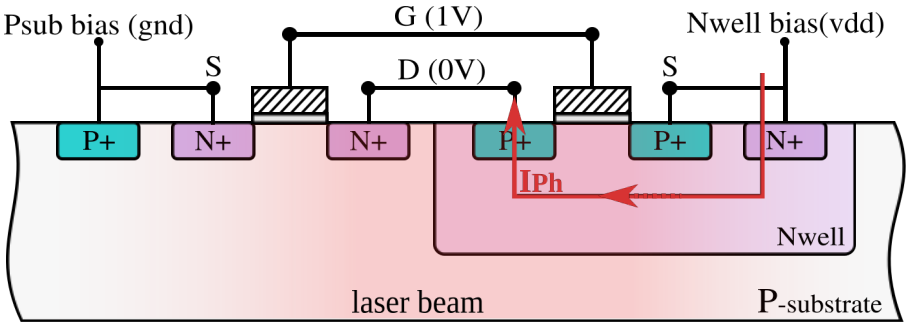


$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S$$

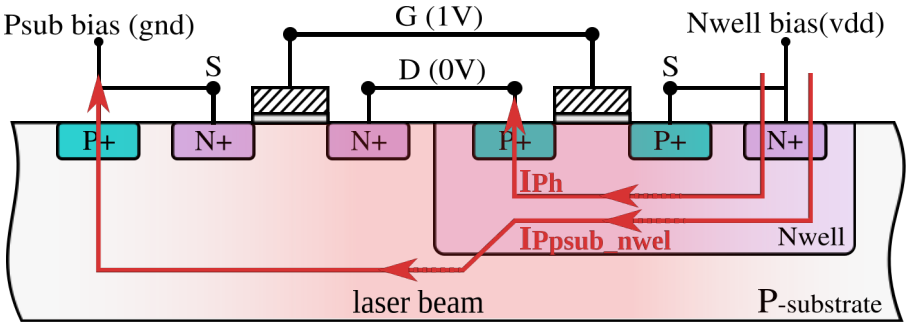
$$IP_{Psub\_nwell} = factor \times I_{ph}$$

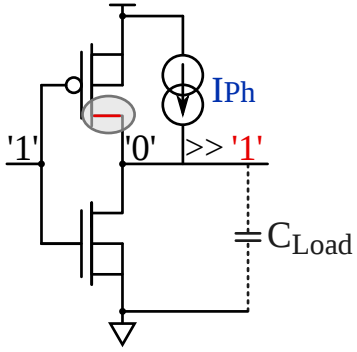
3.1 - Upgraded electrical model

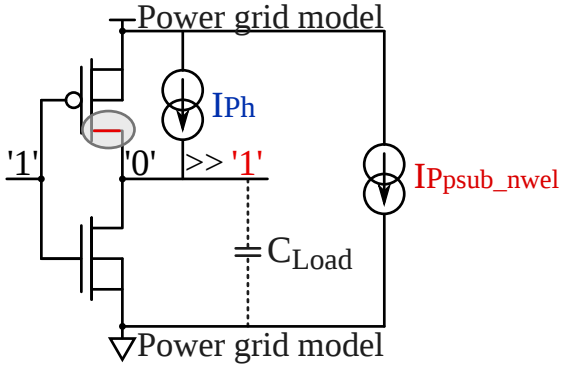
Classical Model



Upgraded Electrical Model







$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S$$

$$IP_{Psub\_nwell} = factor \times I_{ph}$$

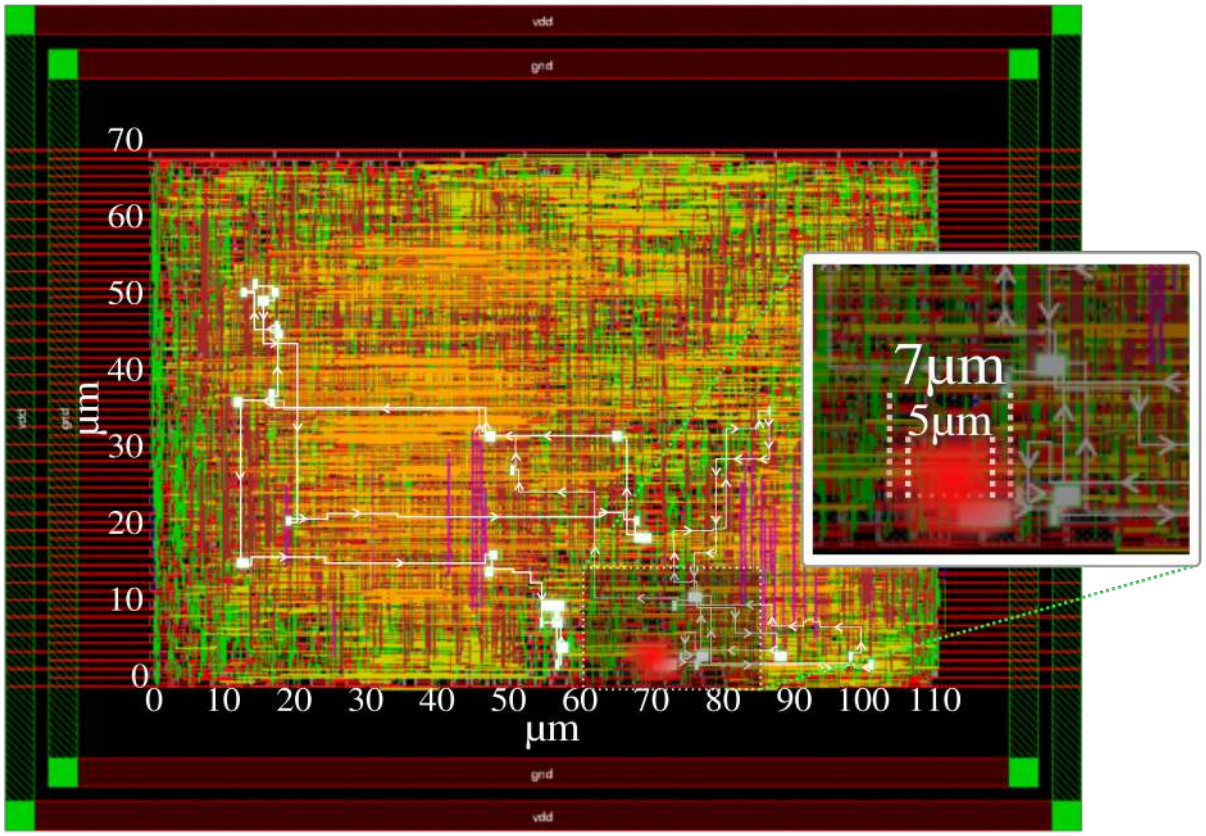
(>10)

J.M. Dutertre et al., “Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS

Outline

Outline

5.0 - Case study



ARM 7 processor

CMOS 28 nm

VDD = 1 V

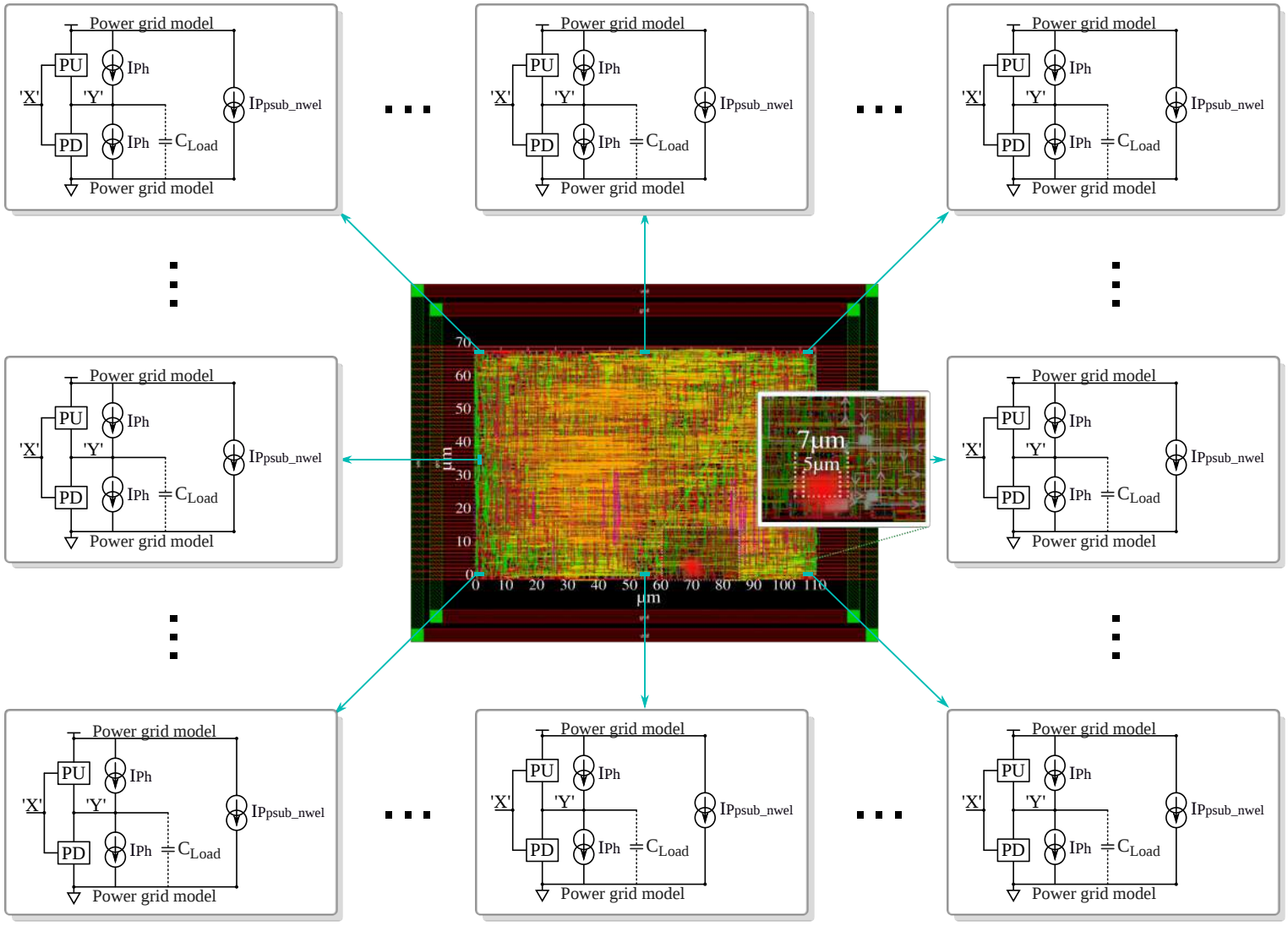
110 µm x 70 µm

Laser spot diameter = 5 µm

5.0 - Case study

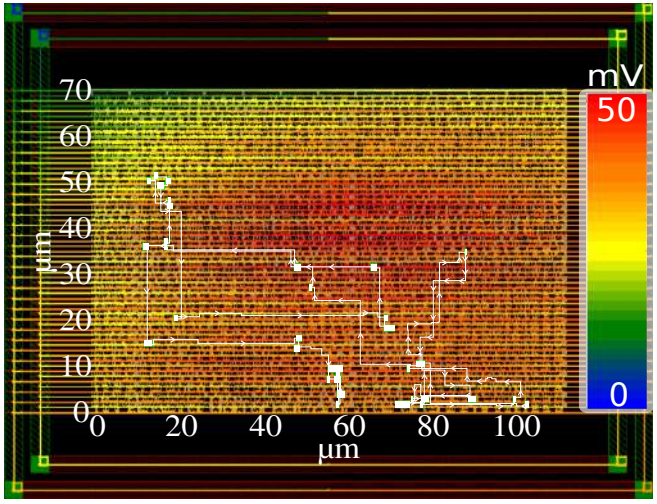
Set the amplitude of the exponencial currents according to:

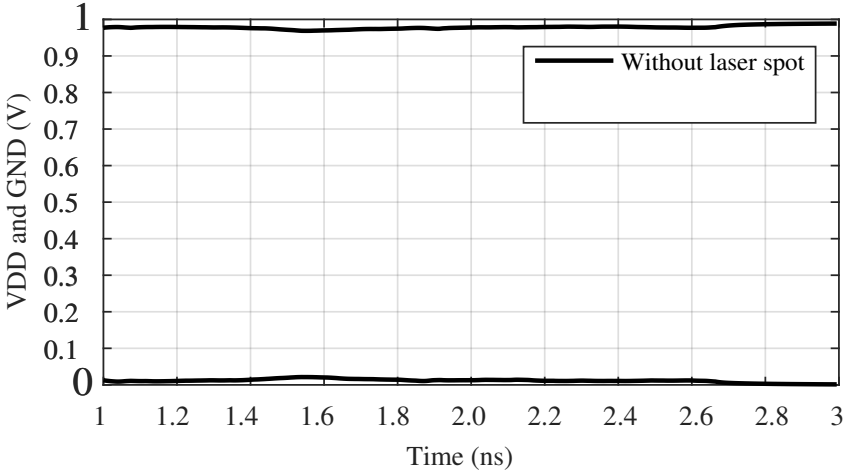
$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \qquad IP_{Psub\_nwell} = factor \times I_{ph}$$



5.1 - Maximum Voltage Drop Propagation

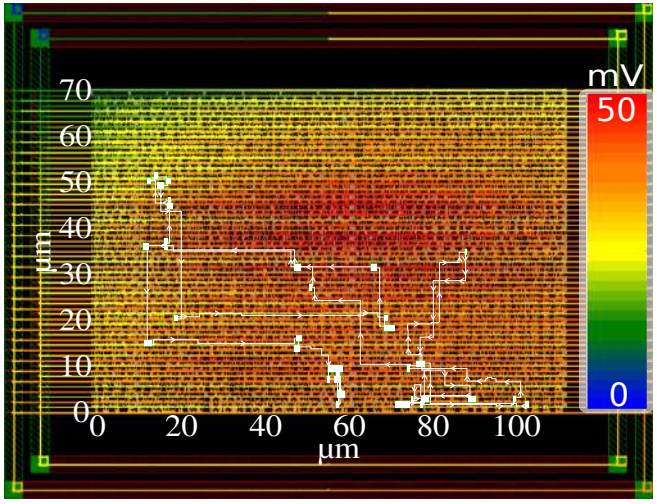
Without laser illumination



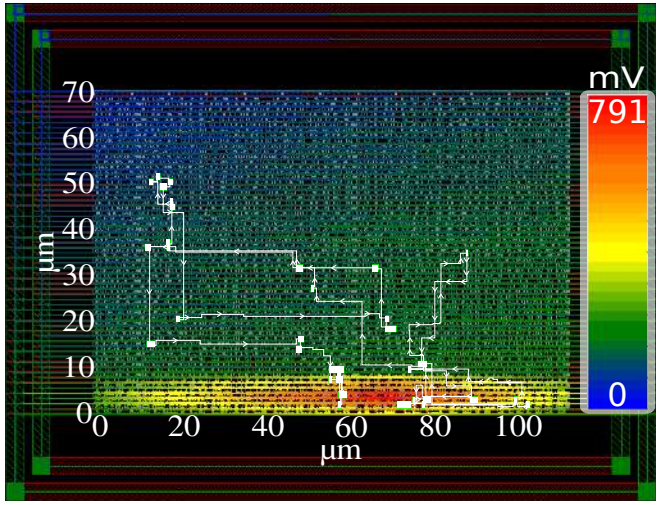


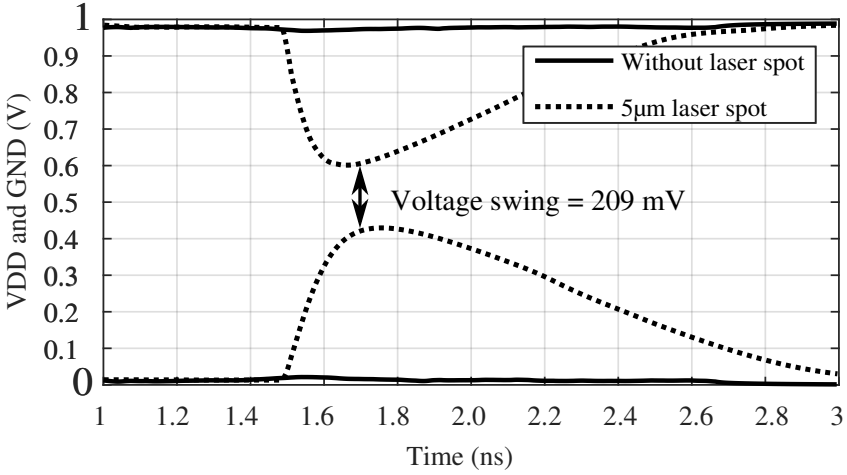
5.1 - Maximum Voltage Drop Propagation

Without laser illumination



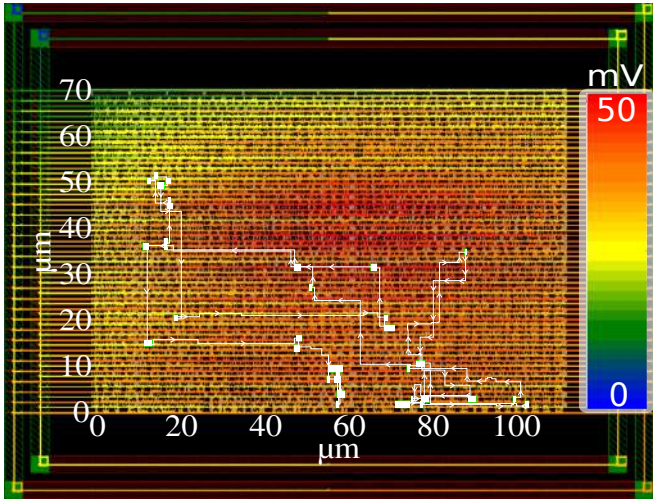
With laser illumination



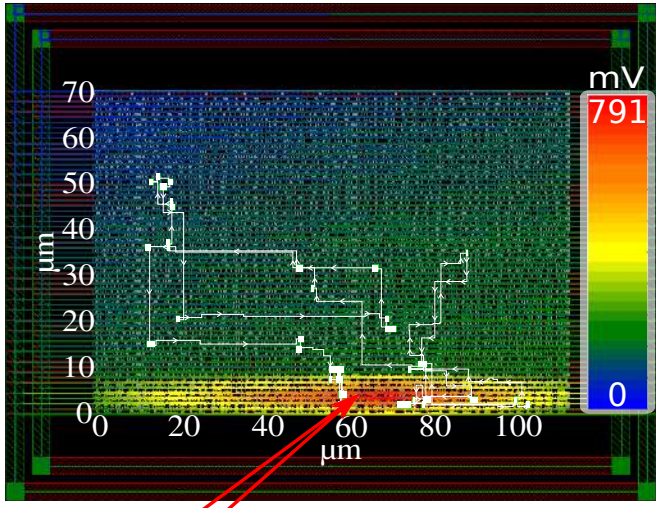


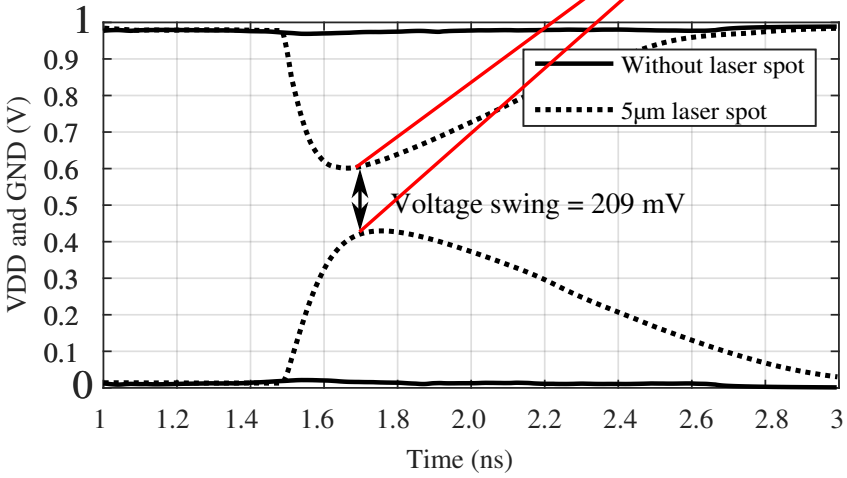
5.1 - Maximum Voltage Drop Propagation

Without laser illumination



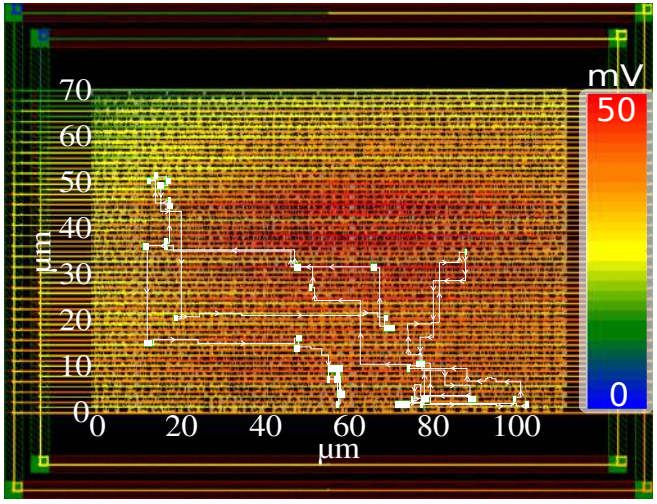
With laser illumination



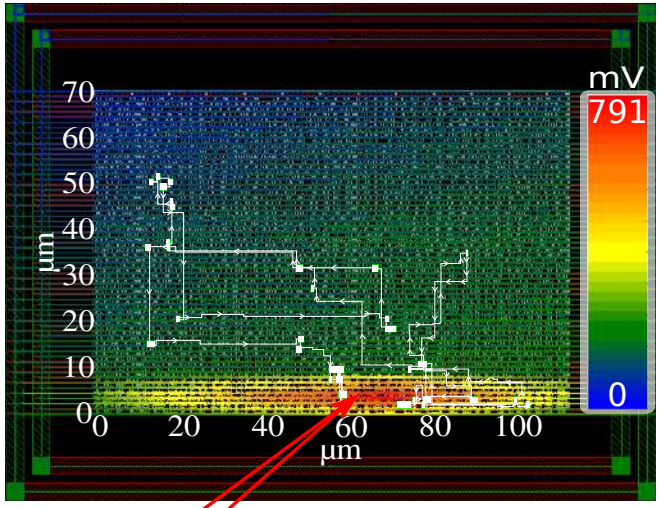


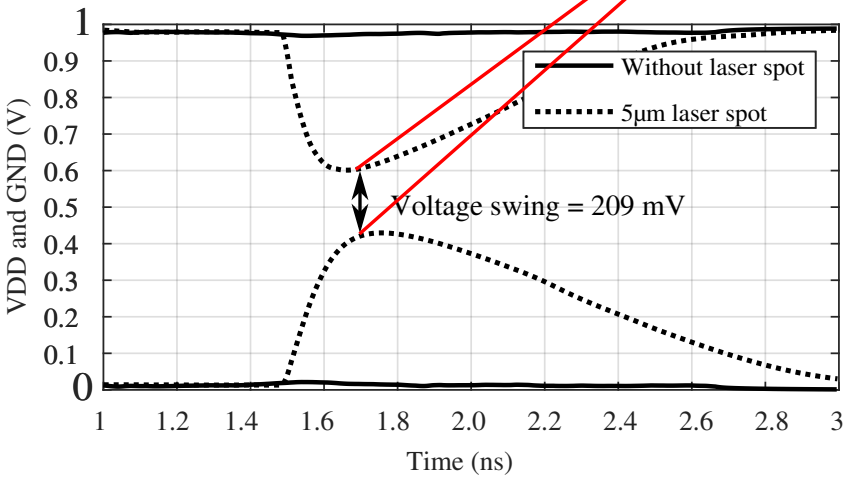
5.1 - Maximum Voltage Drop Propagation

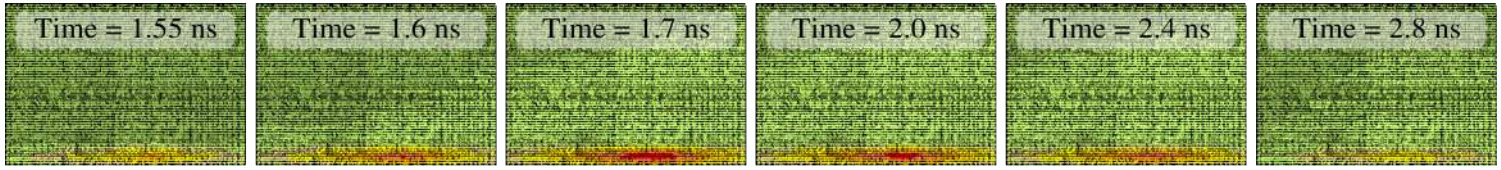
Without laser illumination



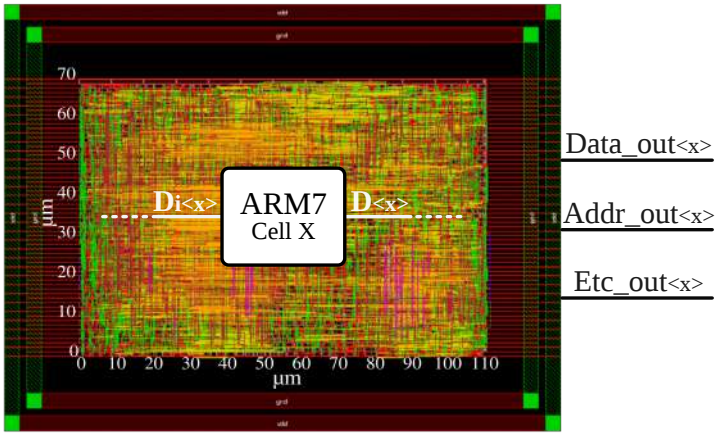
With laser illumination

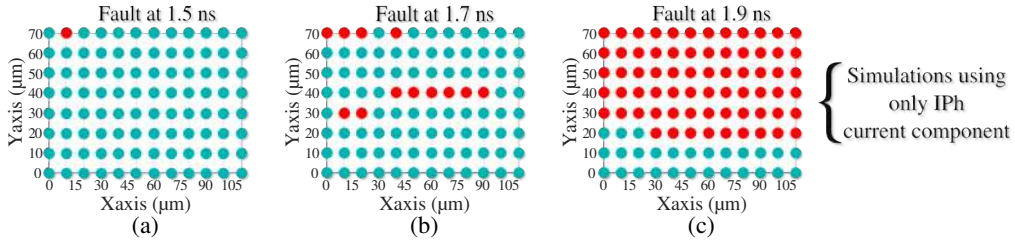


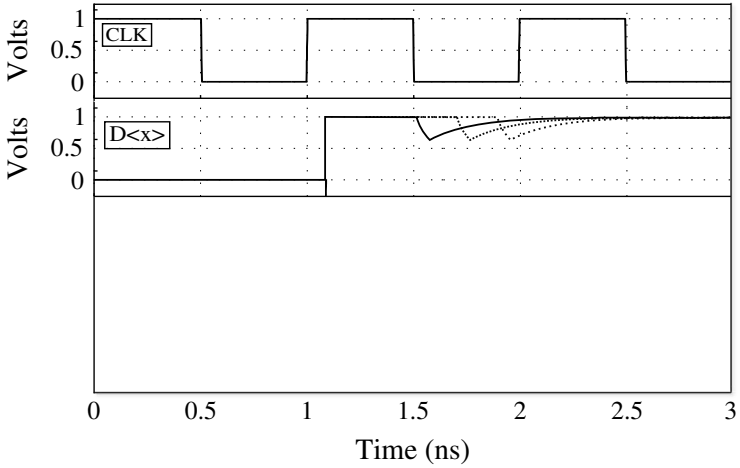


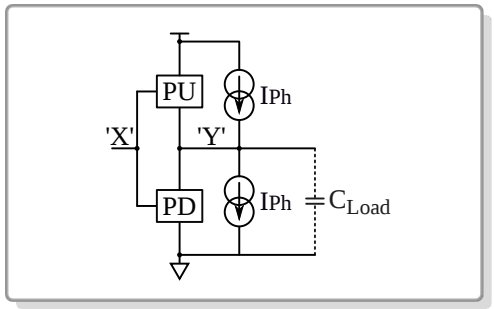


5.2 - Simulated Scenarios and Fault Injection Maps

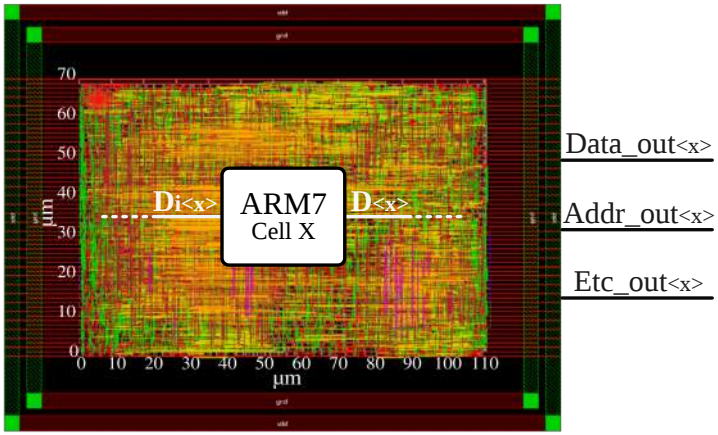


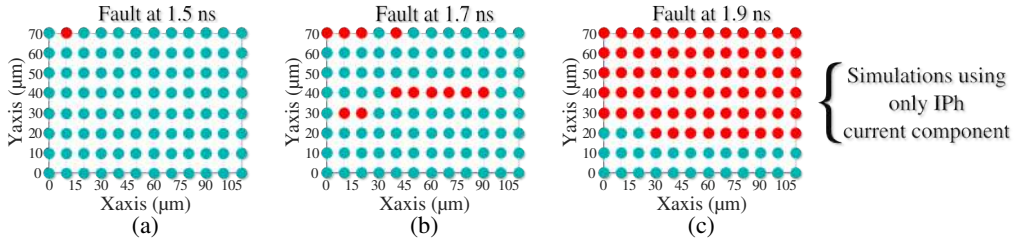


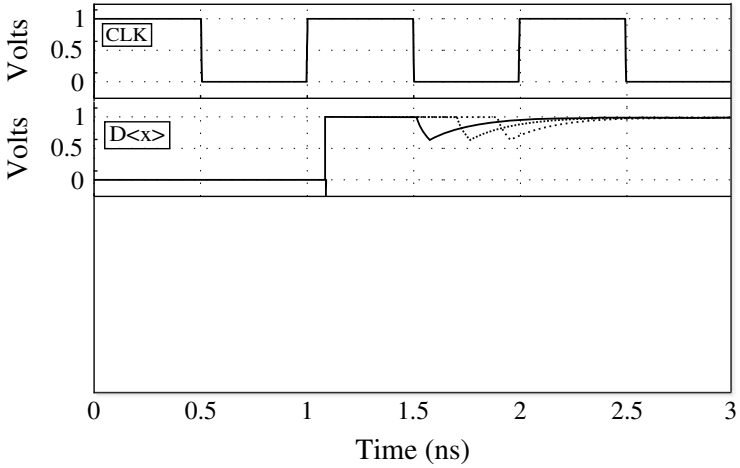


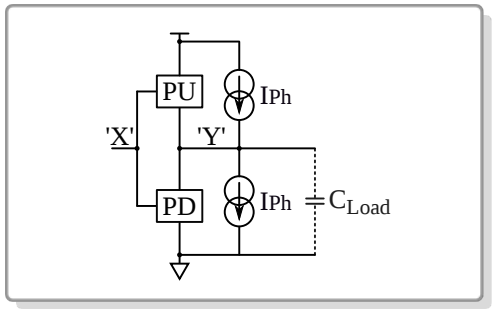


5.2 - Simulated Scenarios and Fault Injection Maps

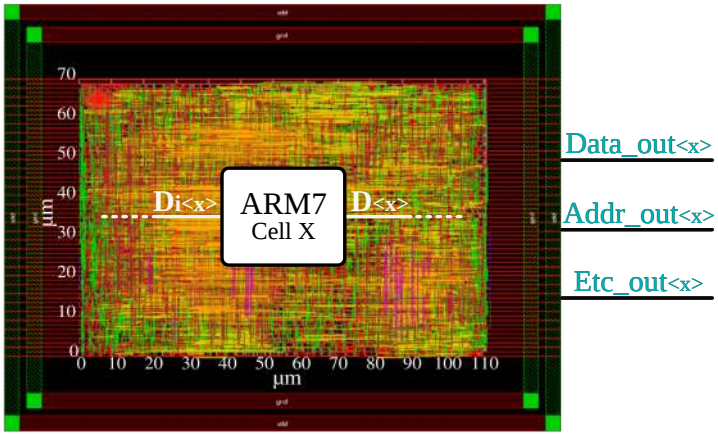


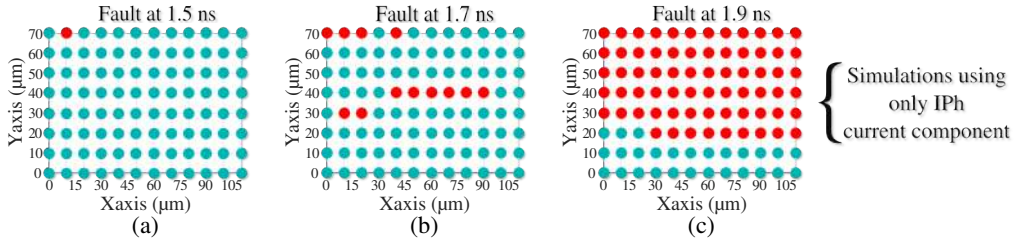


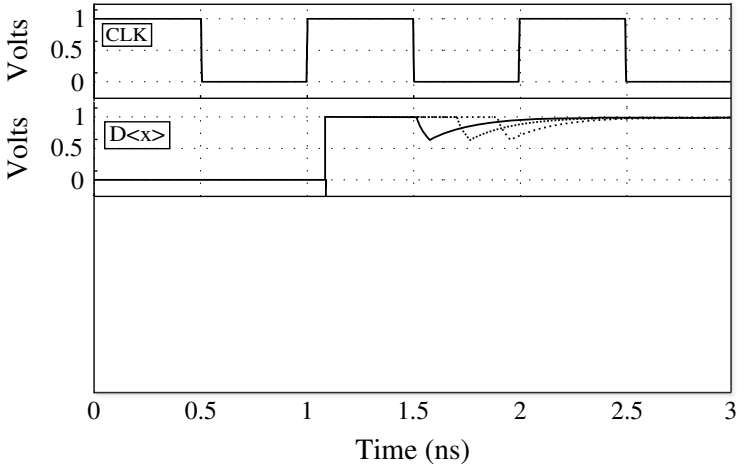


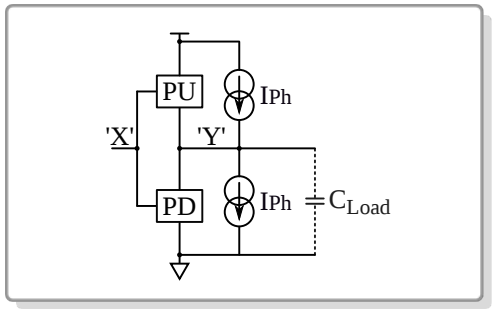


5.2 - Simulated Scenarios and Fault Injection Maps

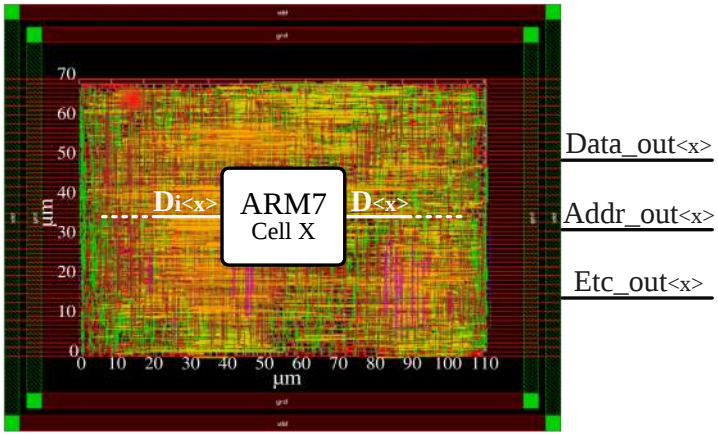


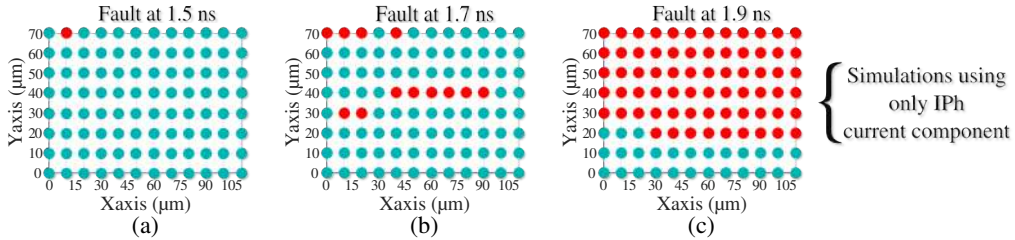


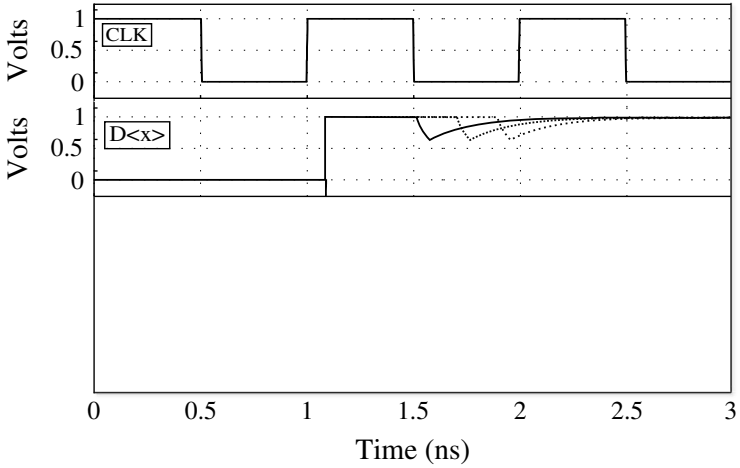


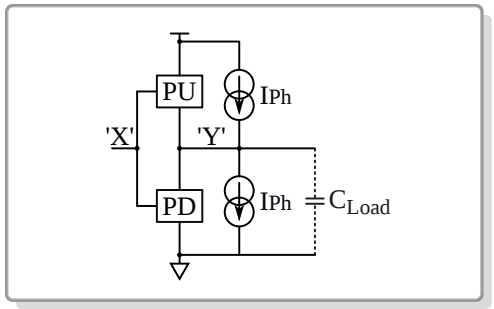


5.2 - Simulated Scenarios and Fault Injection Maps

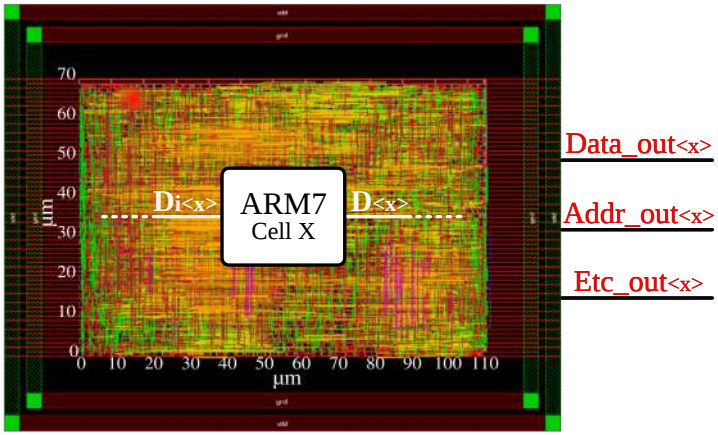


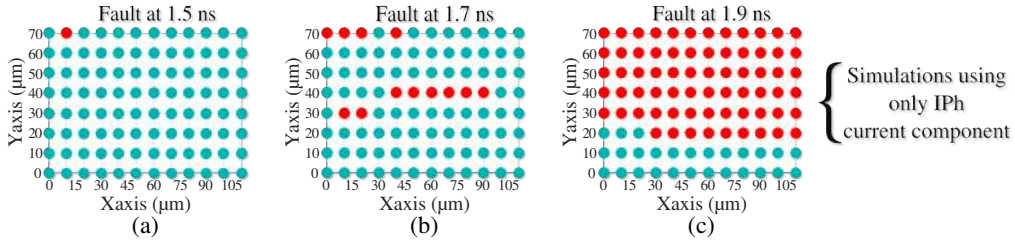


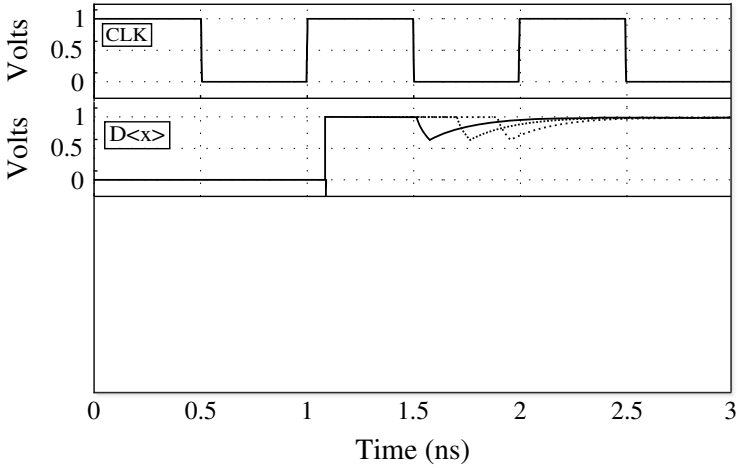


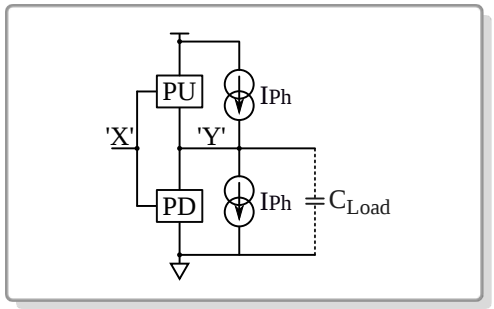


5.2 - Simulated Scenarios and Fault Injection Maps

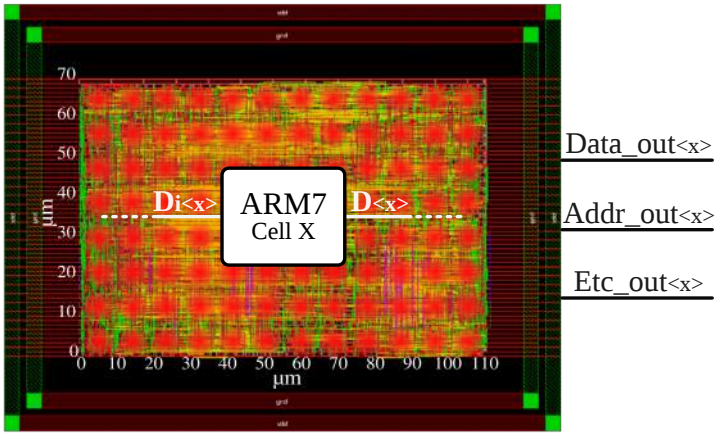


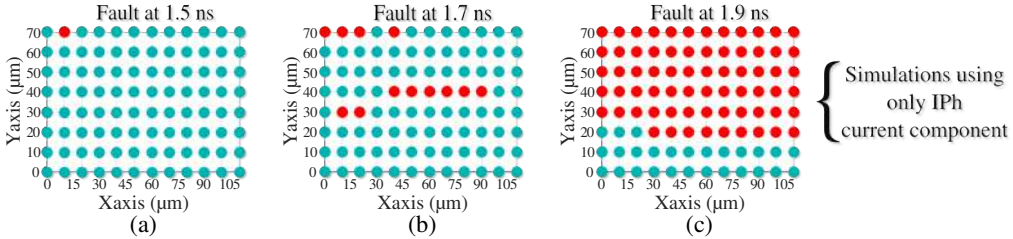


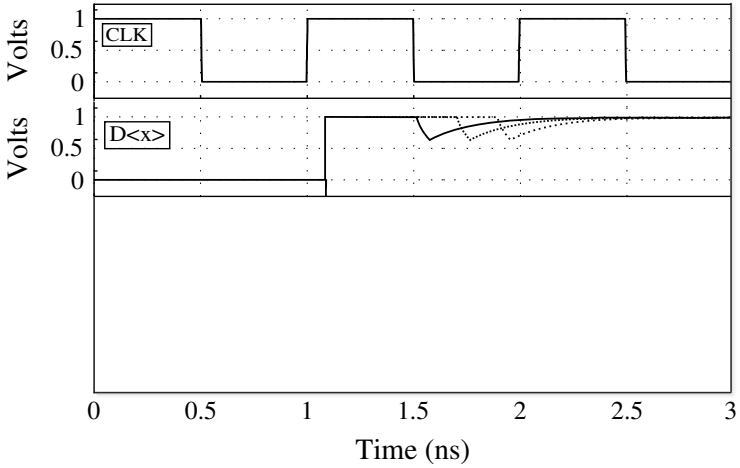


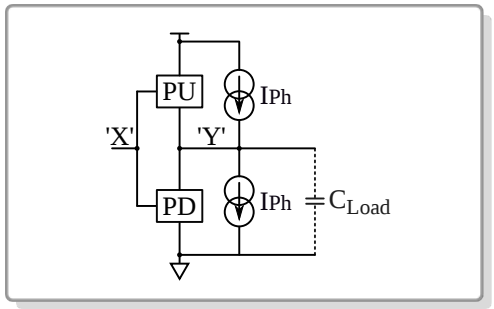


5.2 - Simulated Scenarios and Fault Injection Maps

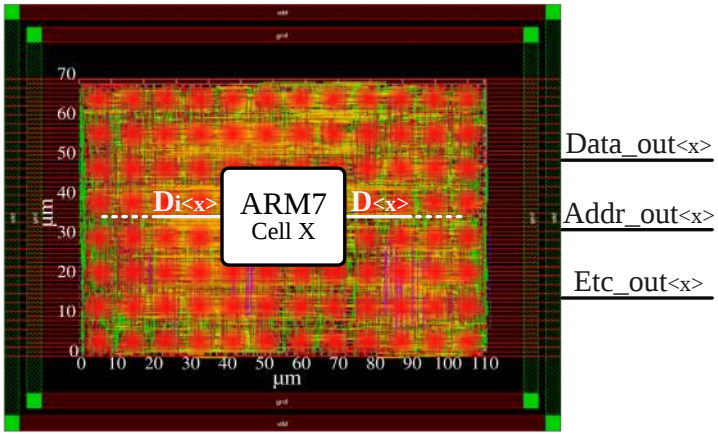


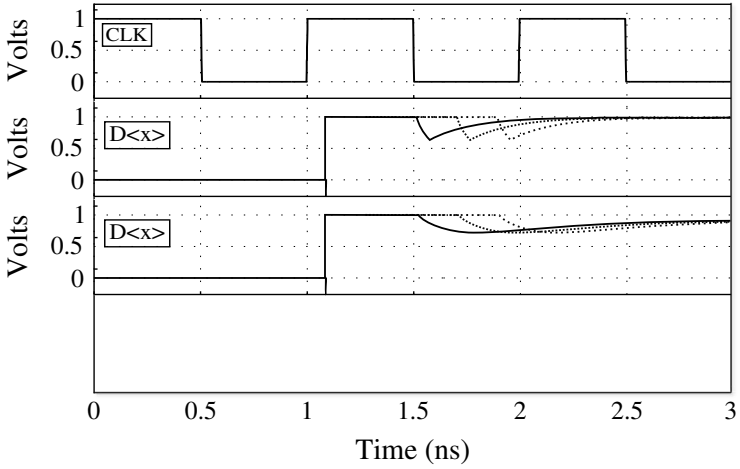


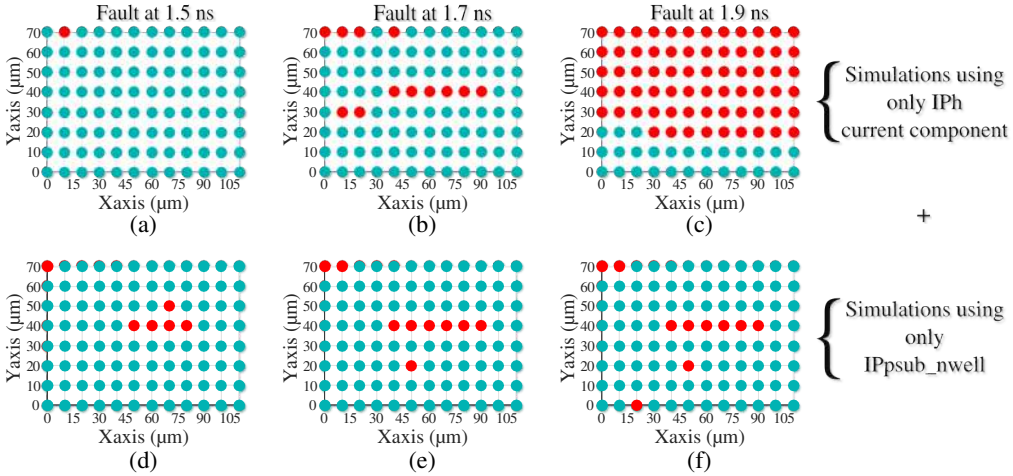


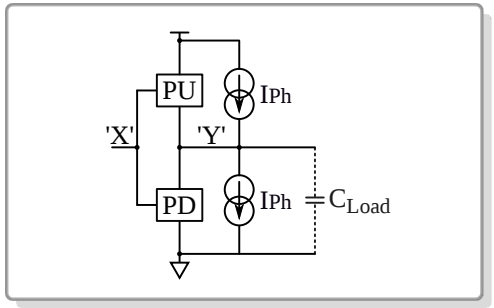


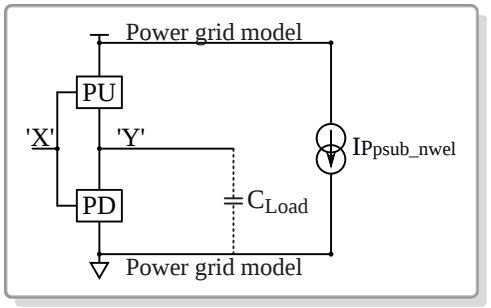
5.2 - Simulated Scenarios and Fault Injection Maps



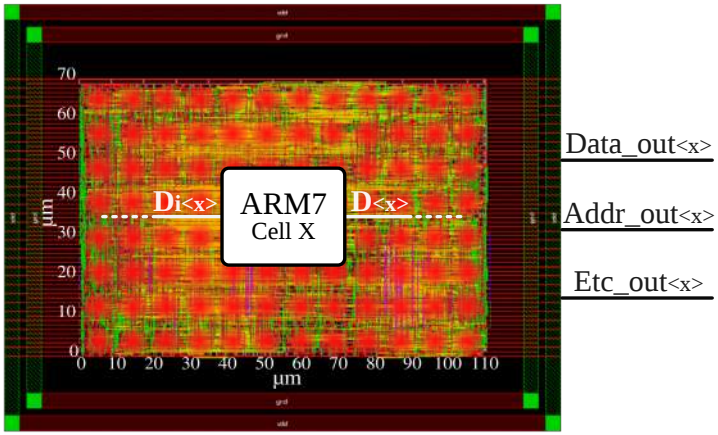


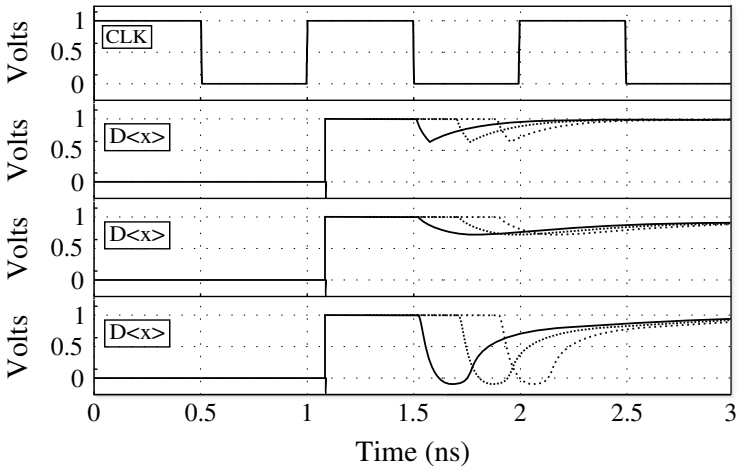


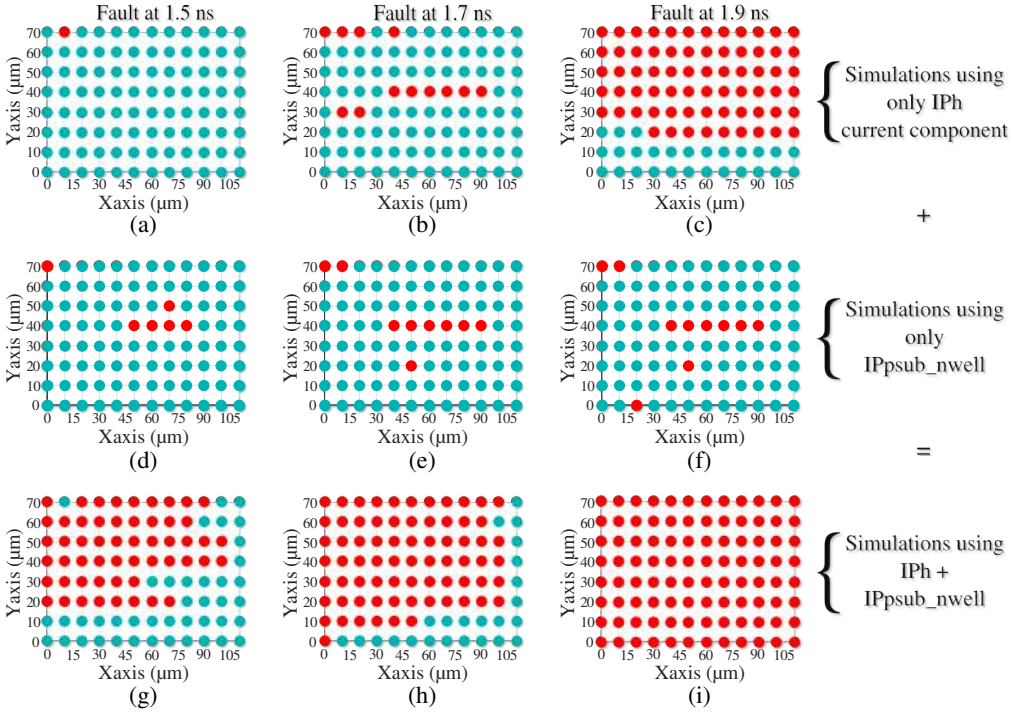


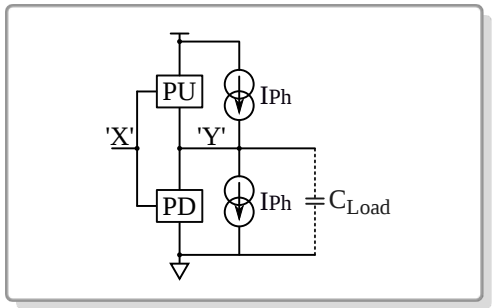


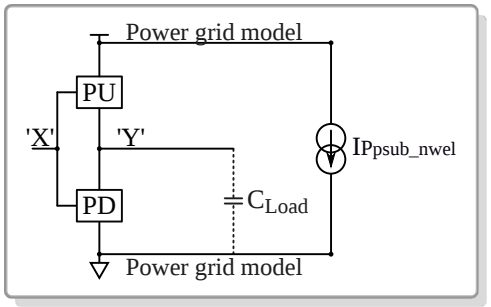
5.2 - Simulated Scenarios and Fault Injection Maps

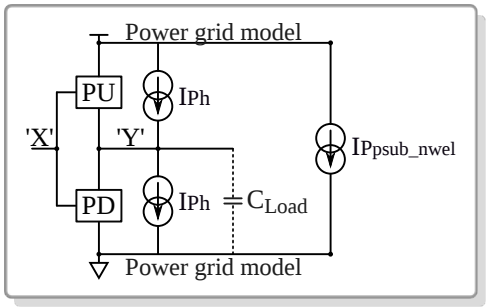




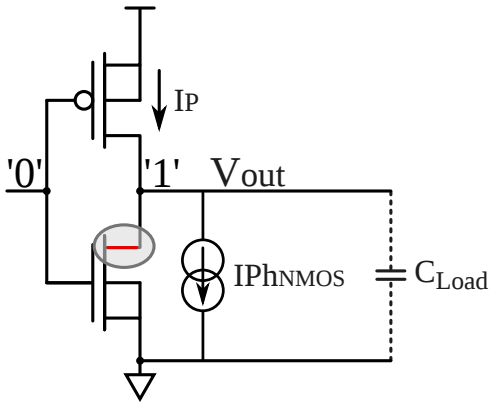


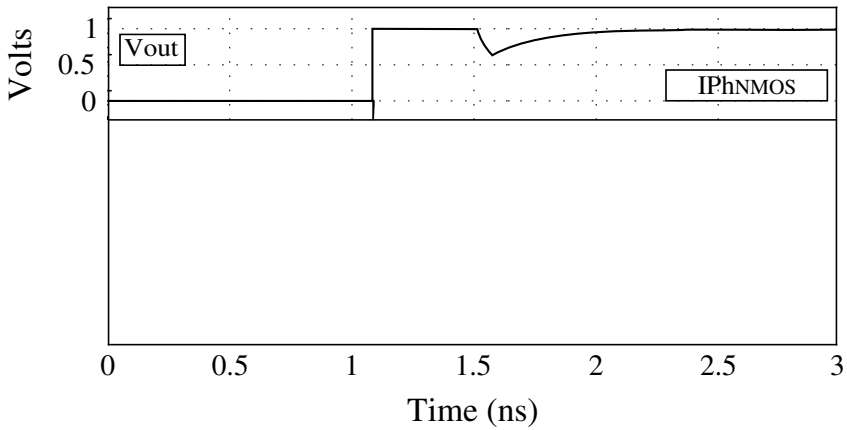


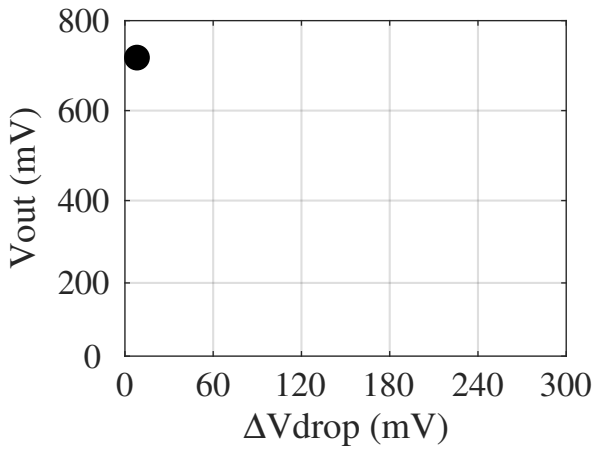




5.3 - IR drop contribution to the fault injection mechanism

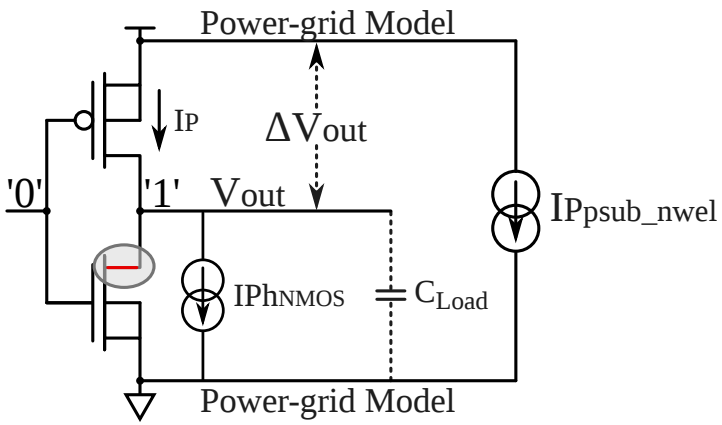


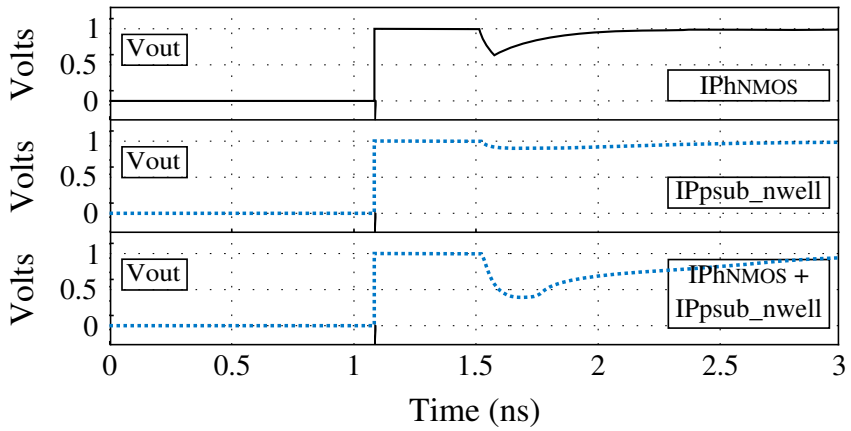


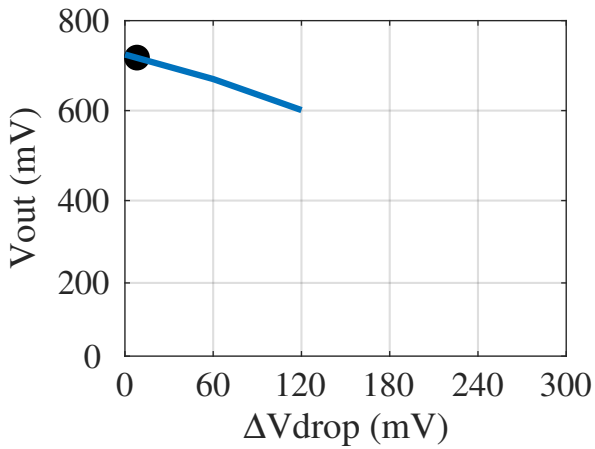


$$\Delta V_{out}(without IR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism



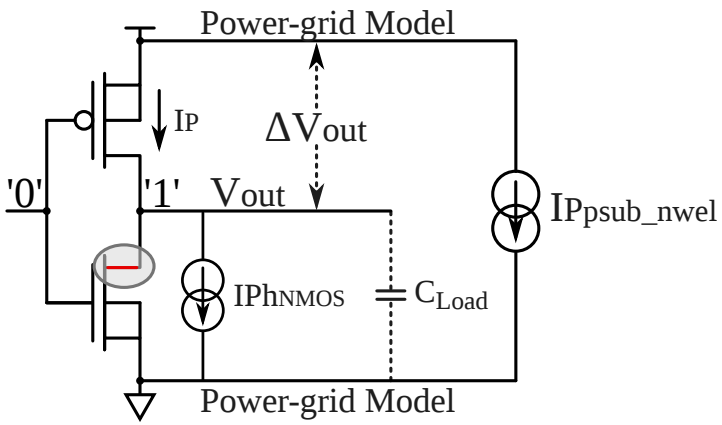


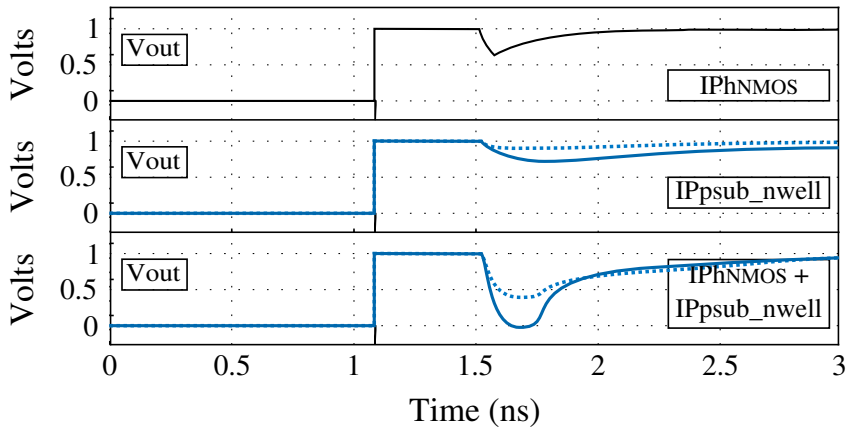


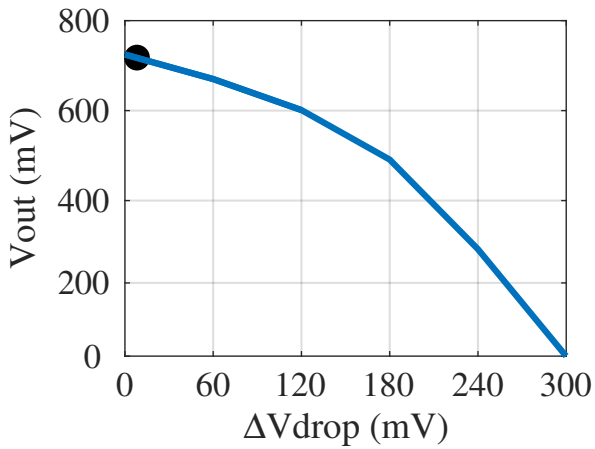
$$\Delta V_{out}(without IR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

$$\Delta V_{out}(with IR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism



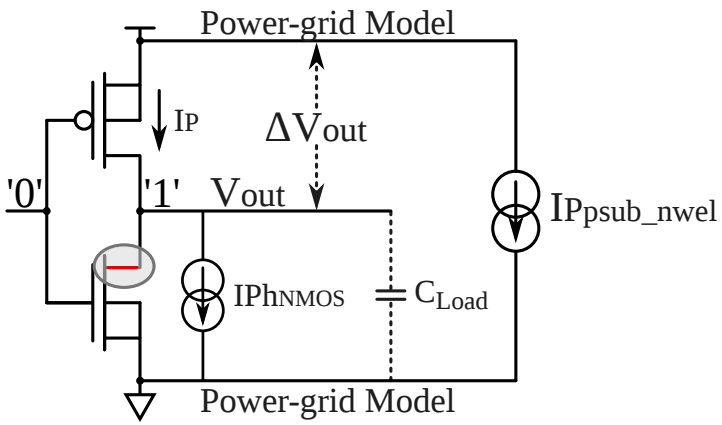


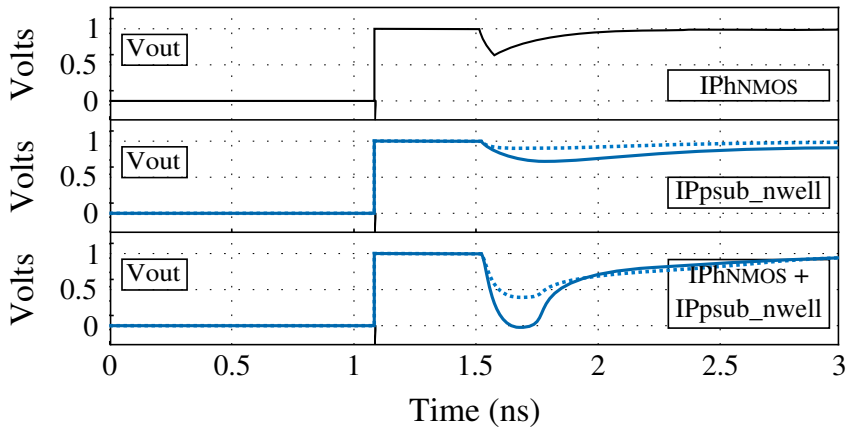


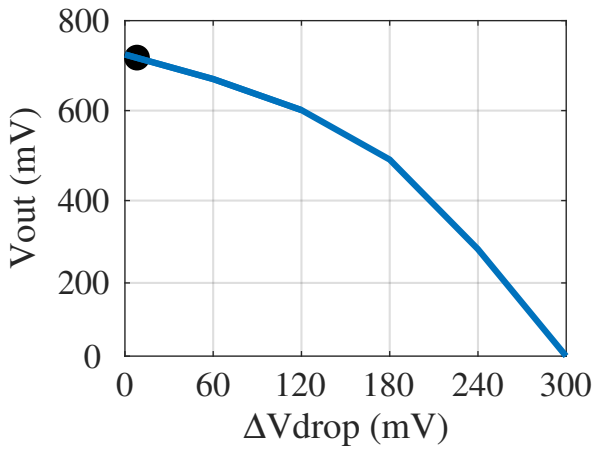
$$\Delta V_{out}(without IR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

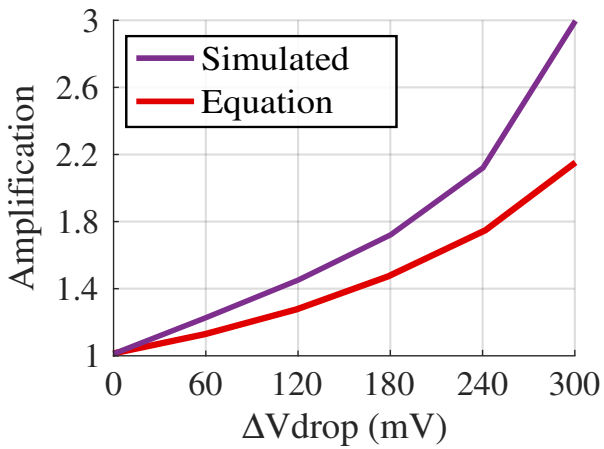
$$\Delta V_{out}(with IR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism









$$\Delta V_{out}(withoutIR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

$$\Delta V_{out}(withIR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

$$\frac{\Delta V_{out}(withIR)}{\Delta V_{out}(withoutIR)} = \frac{1}{1 - \frac{V_{drop}}{V_{DD} - V_T}}$$

Outline

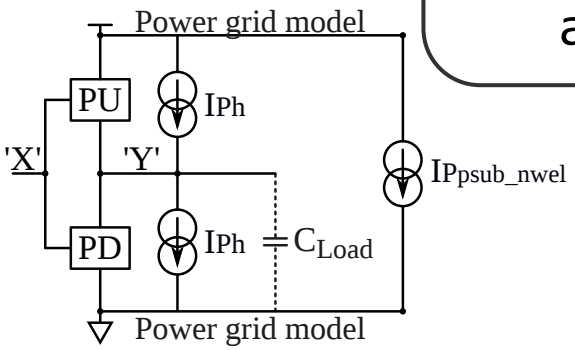
Outline

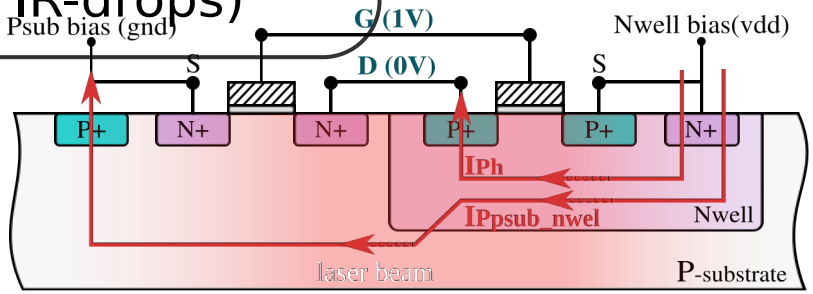
Conclusions

I_{Ppsub_nwell} current component is always present (causing IR-drops)

Conclusions

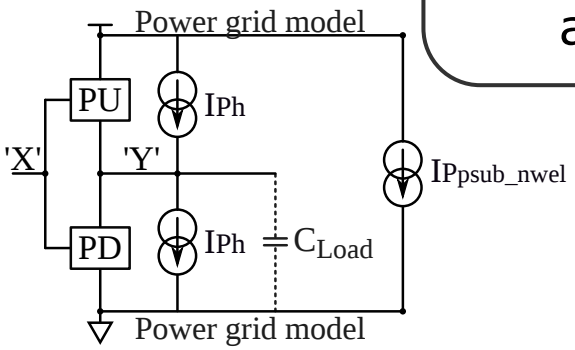
I_{Ppsub_nwell} current component is always present (causing IR-drops)

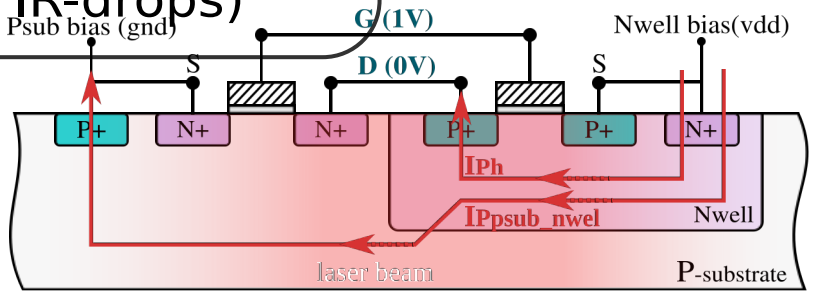




Conclusions

I_{Ppsub_nwell} current component is always present (causing IR-drops)

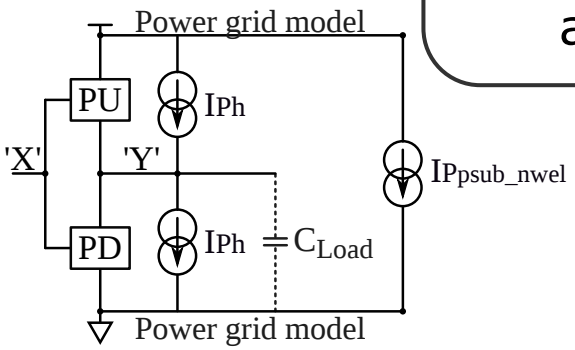


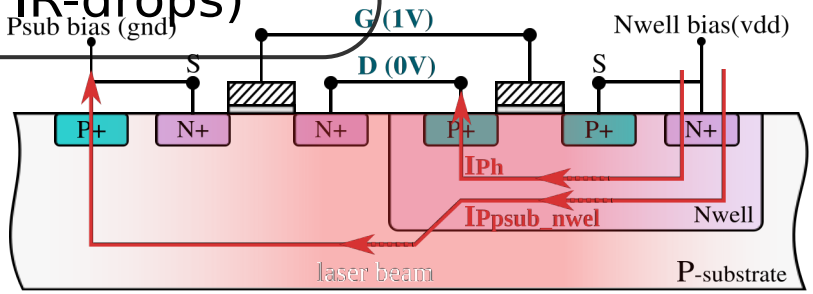


Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection

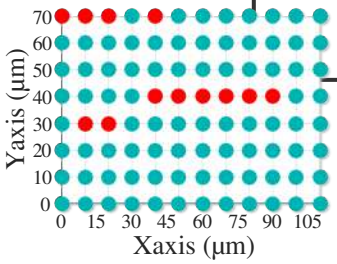
Conclusions

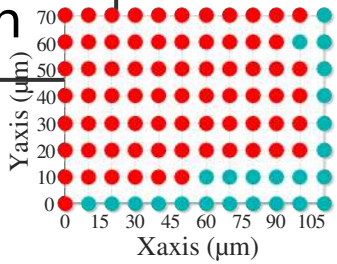
I_{Ppsub_nwell} current component is always present (causing IR-drops)





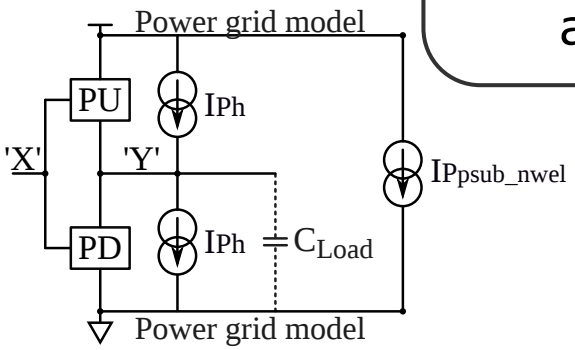
Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection

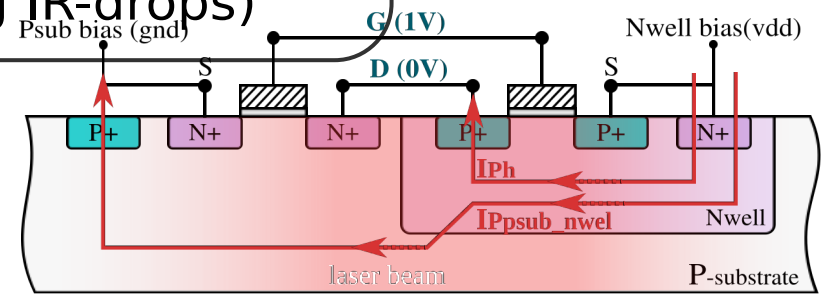




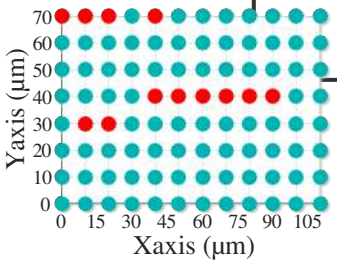
Conclusions

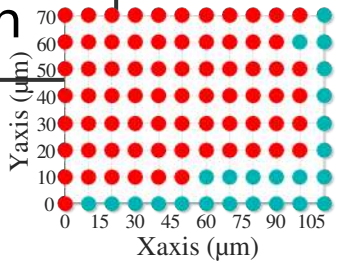
IPpsub_nwell current component is always present (causing IR-drops)



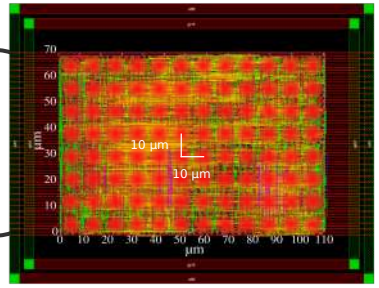


Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection





Methodology to simulate the effects of laser shots on ICs based on standard CAD tools



SMACD'17
June 15, 2017

Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos

LIRMM

tima

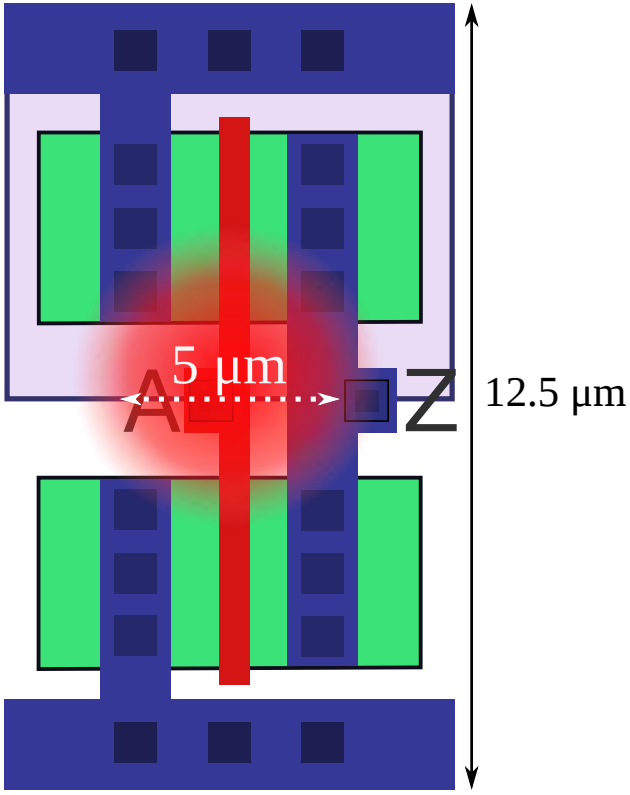
MINES Saint-Étienne
Une école de l'IMT

Appendix

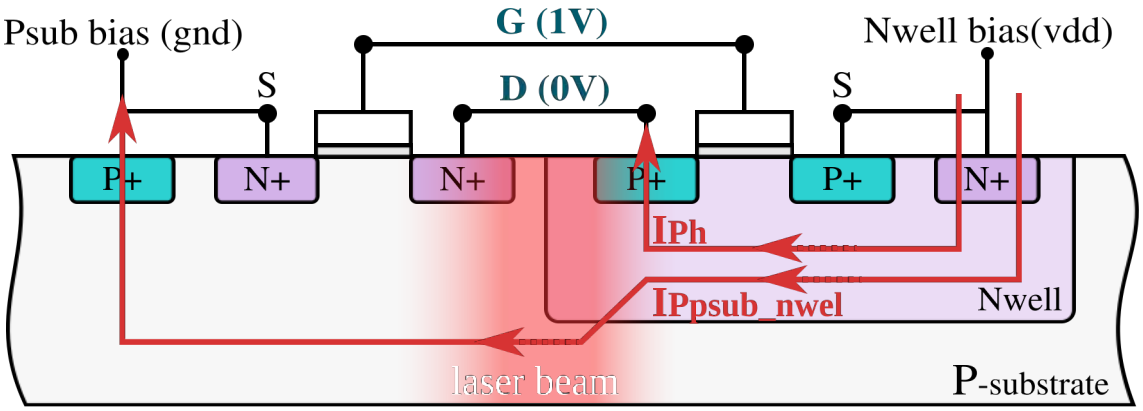
2.2 - Limits of the classical transient fault model

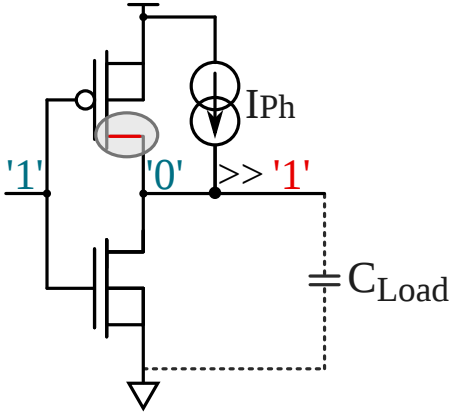
Case 4:

Both NMOS and PMOS transistors are illuminated by the laser beam



tech: 250 nm



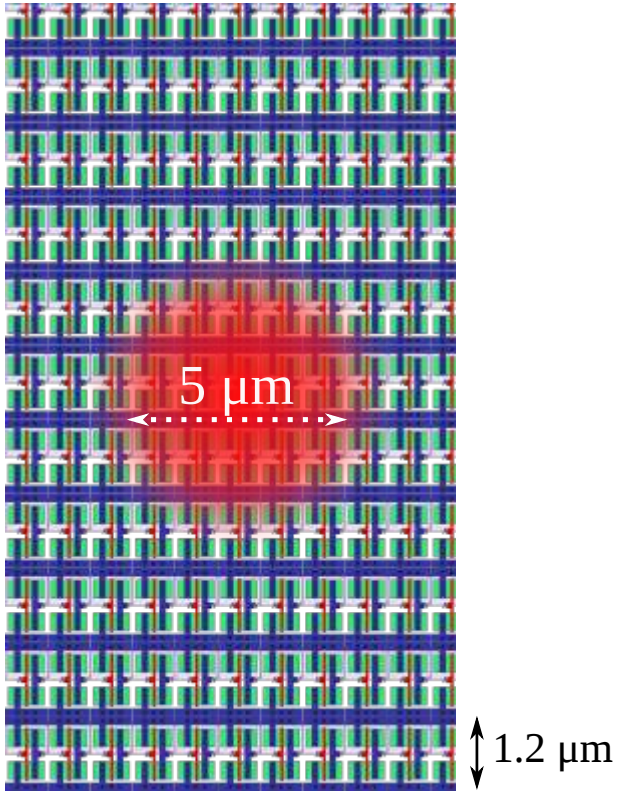


Laser-induced currents
in the Nwell-Psub junction
(classical model is **incomplete**)

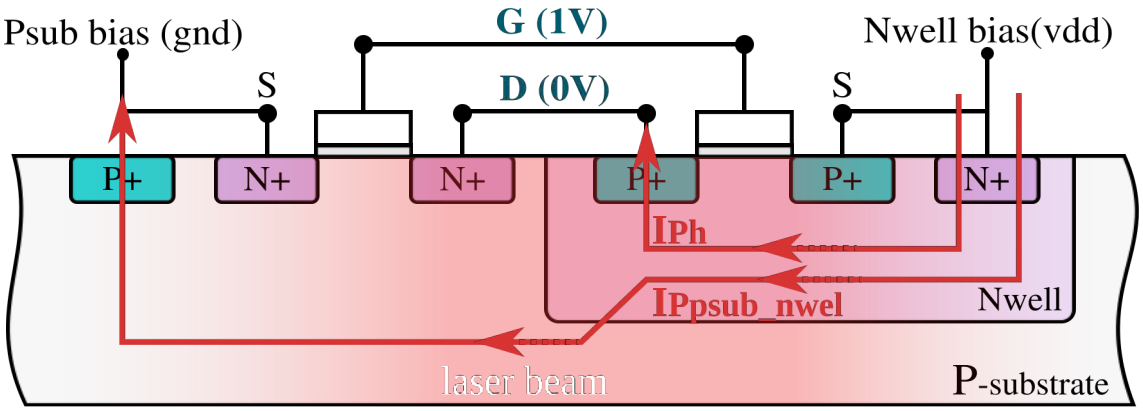
2.2 - Limits of the classical transient fault model

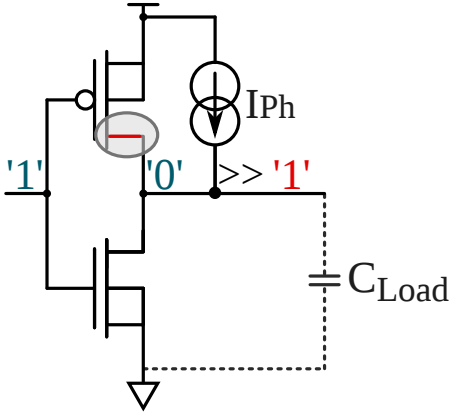
Case 6:

NMOS and PMOS transistors are **always** illuminated by the laser beam



tech: 28 nm

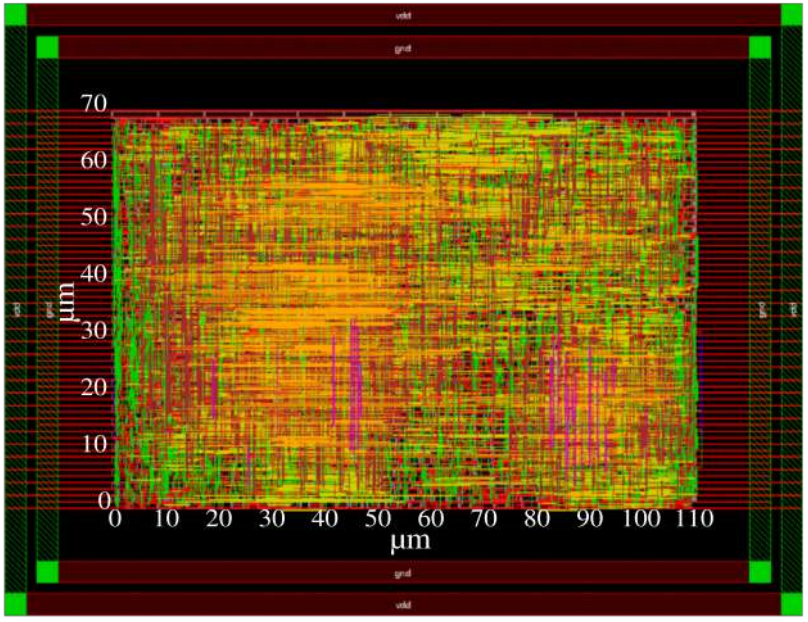




Laser-induced currents
in the Nwell-Psub junction
(classical model is **incomplete**)

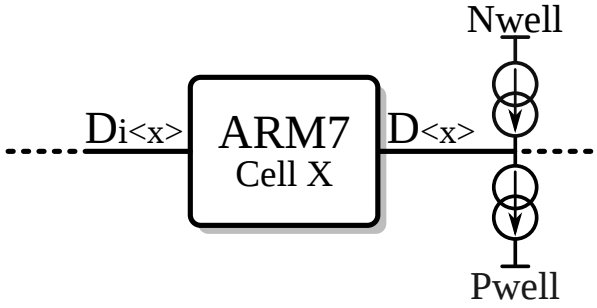
4.2 - 1st step

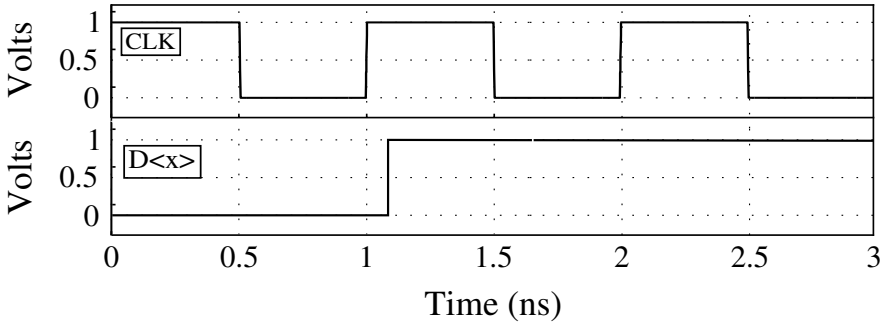
Run a fault free electrical simulation



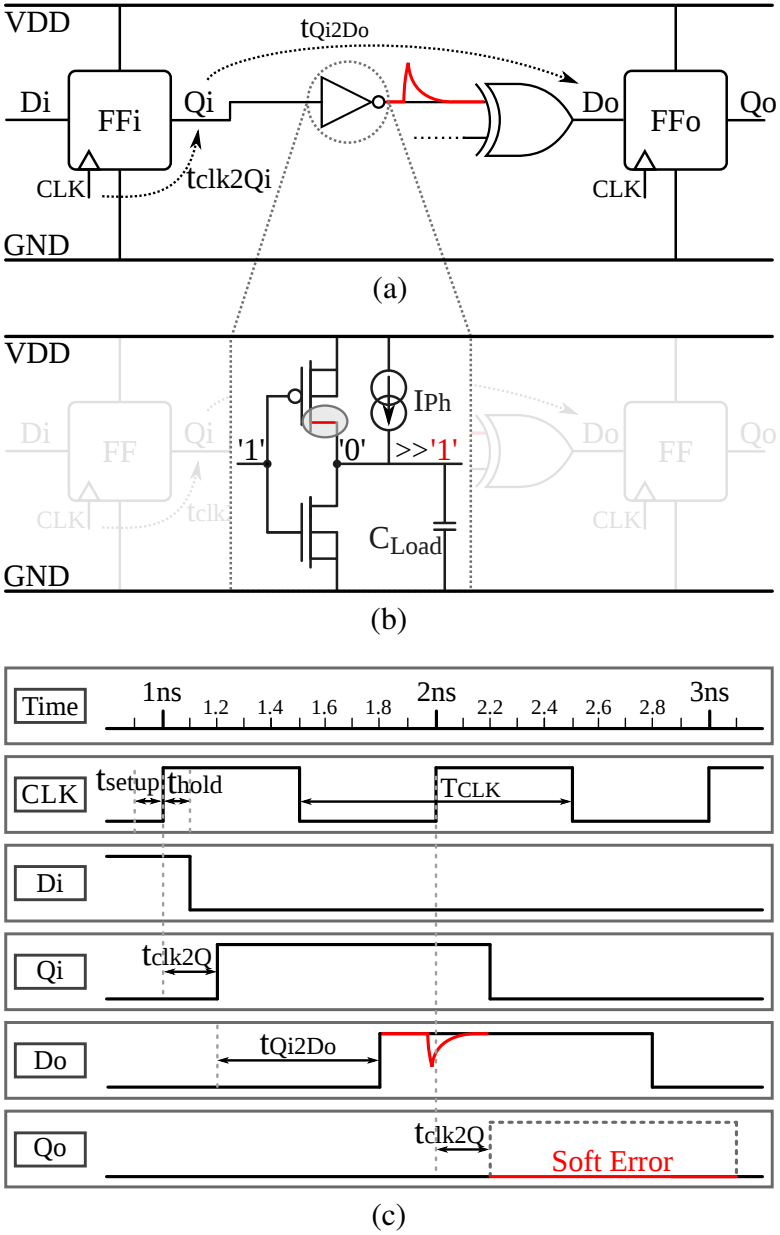
Upgraded model still not in use

Save a golden table with all inputs and outputs of each cell as a function of time

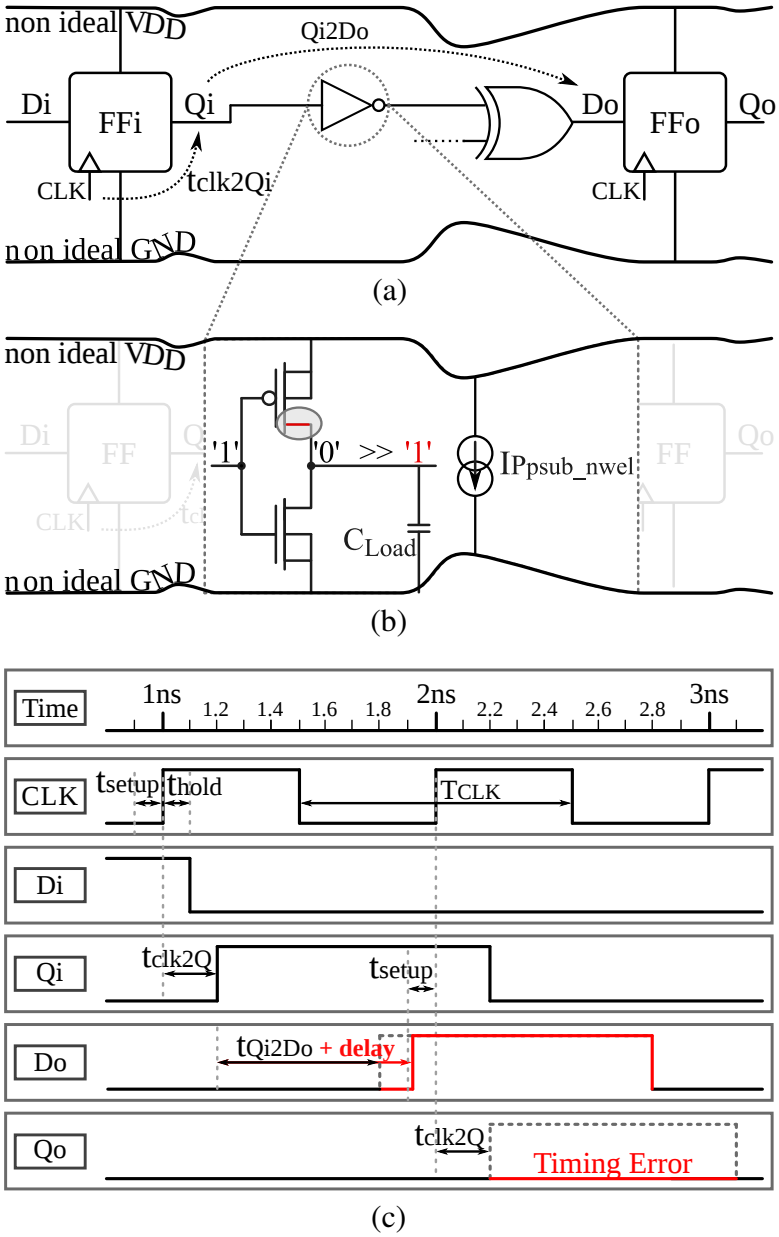




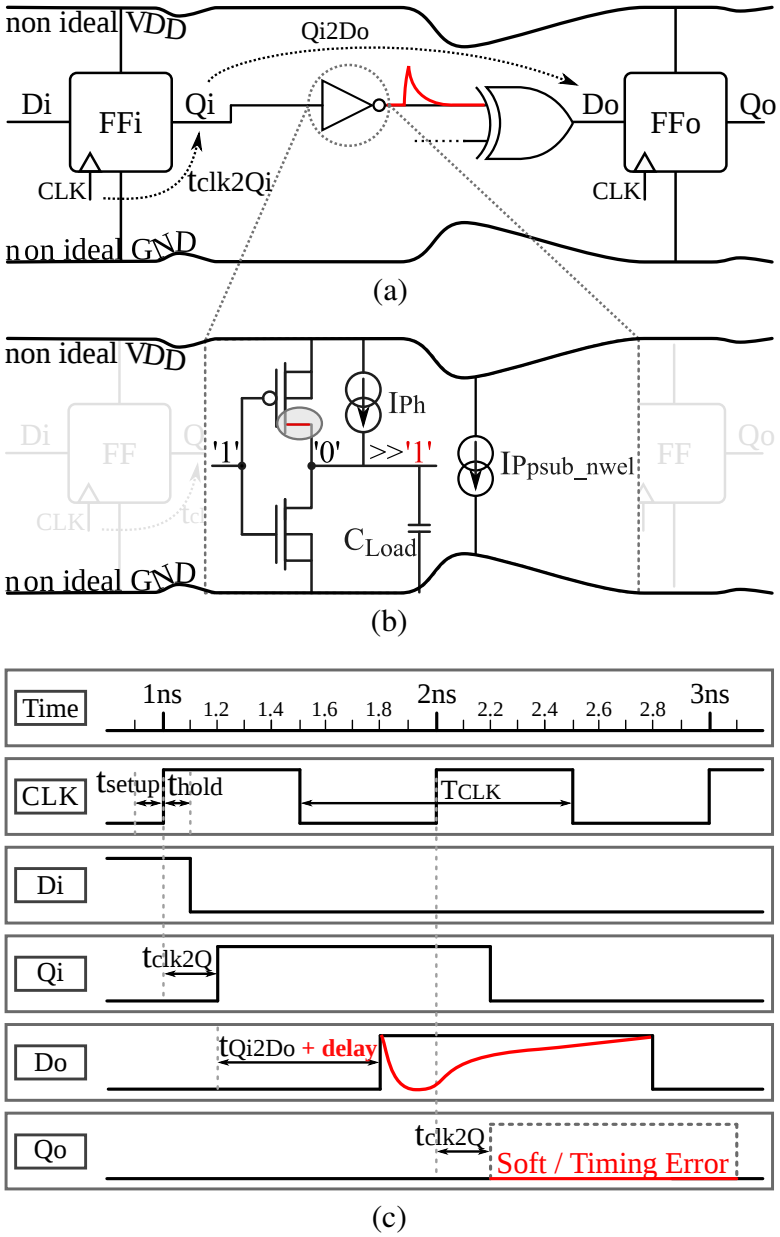
3.2 - Influence of the IPh current component



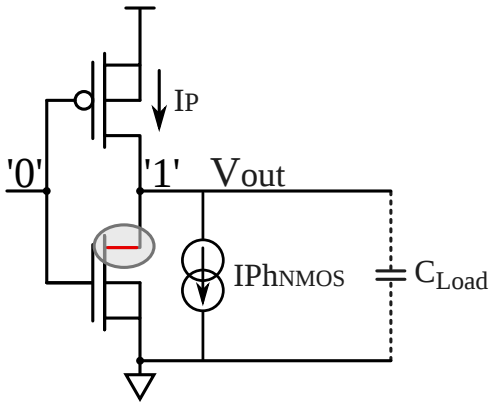
3.3 - Influence of the IPpsub_nwell current component

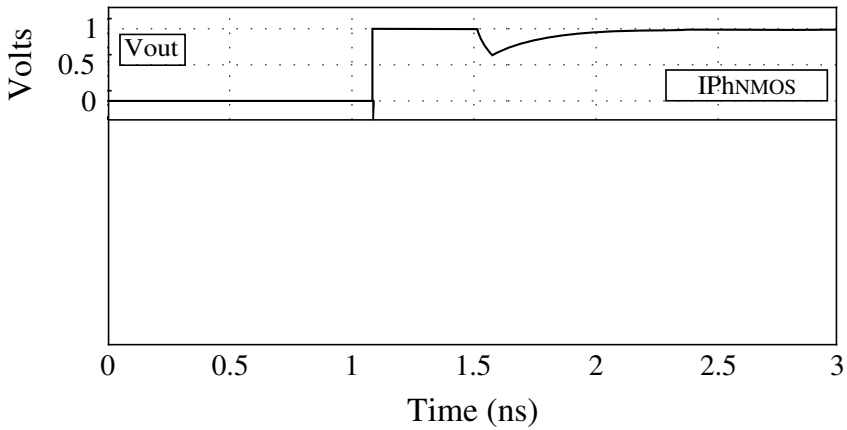


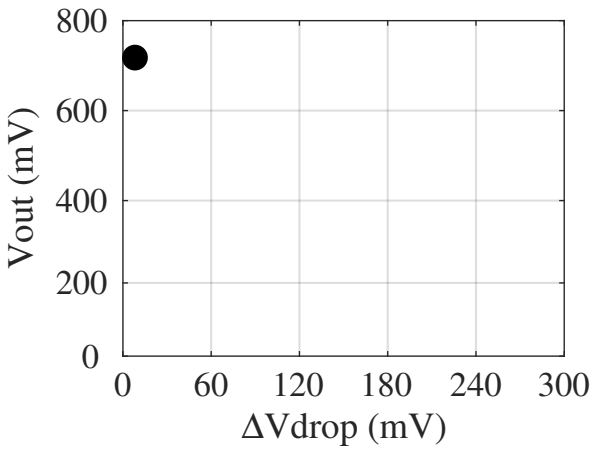
3.4 - Influence of IPh and IPpsub_nwel current components



5.3 - IR drop contribution to the fault injection mechanism

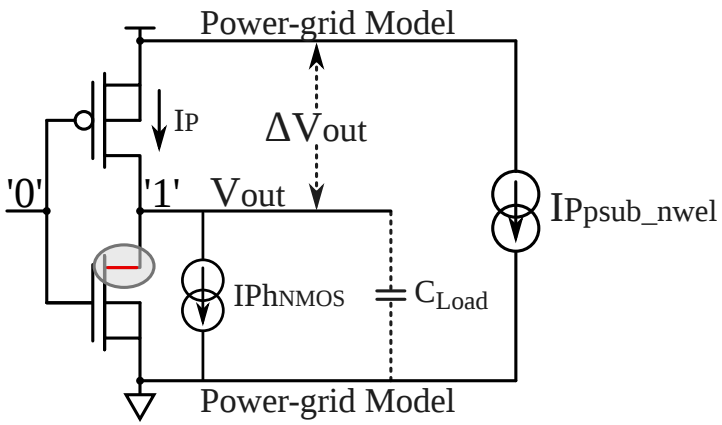


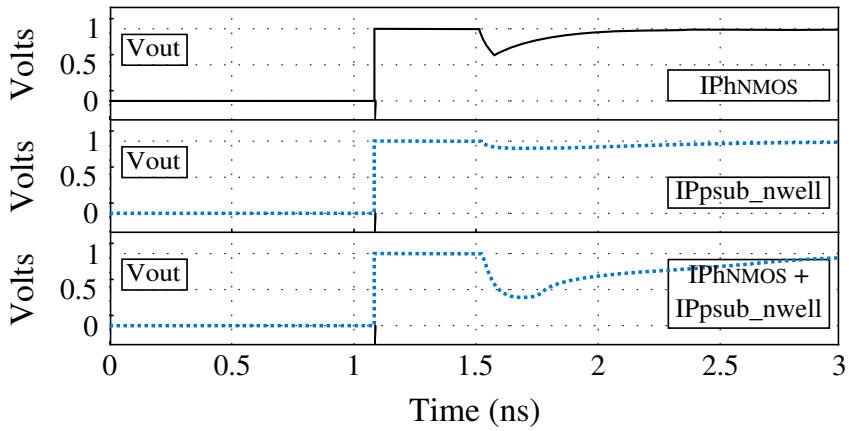


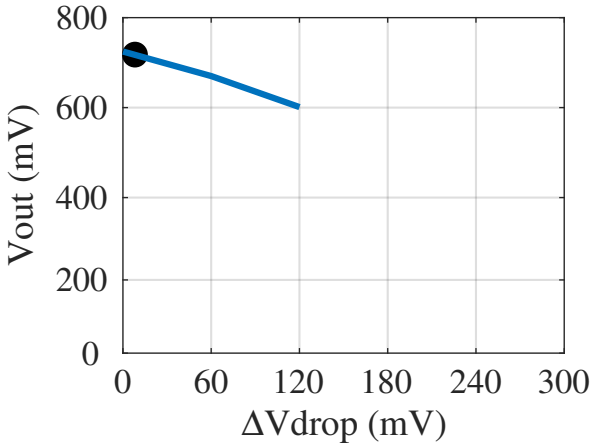


$$\Delta V_{out}(withoutIR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism



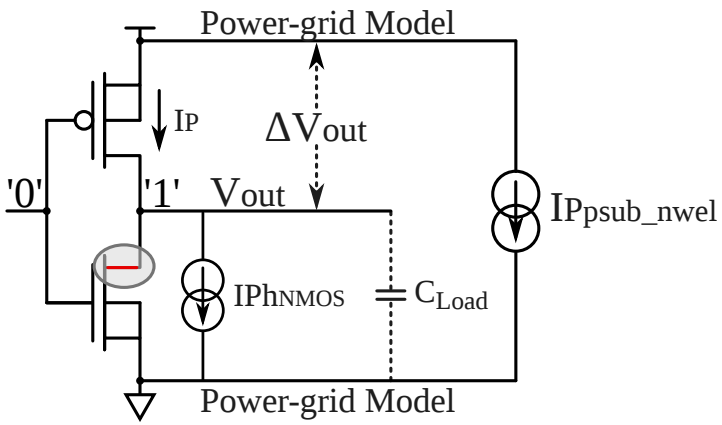


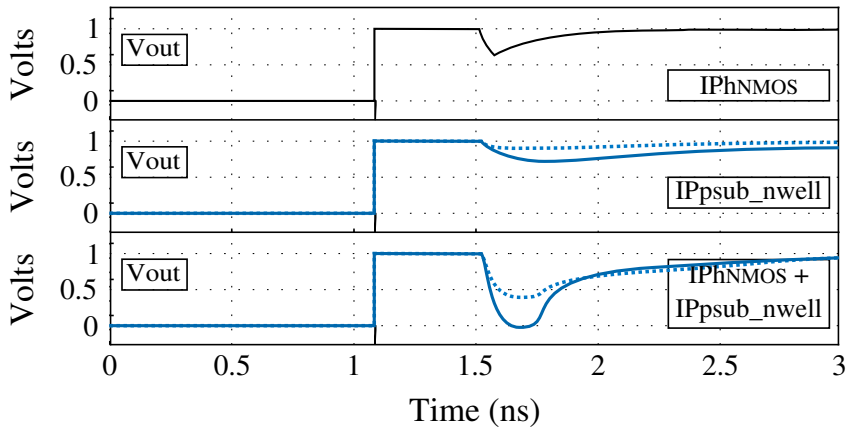


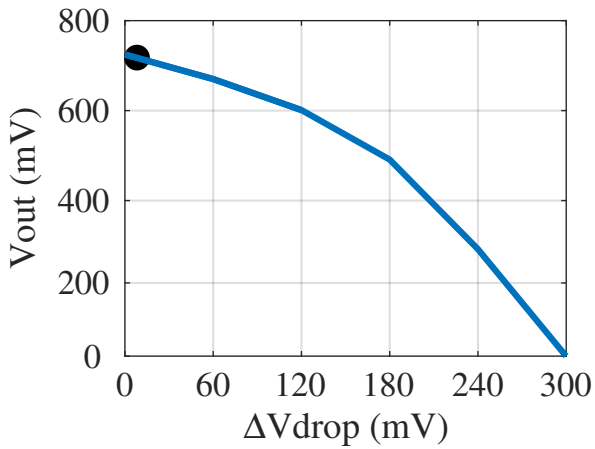
$$\Delta V_{out}(without IR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

$$\Delta V_{out}(with IR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism



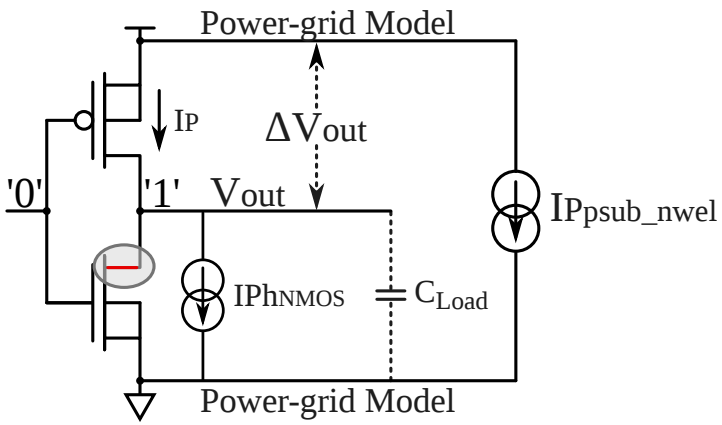


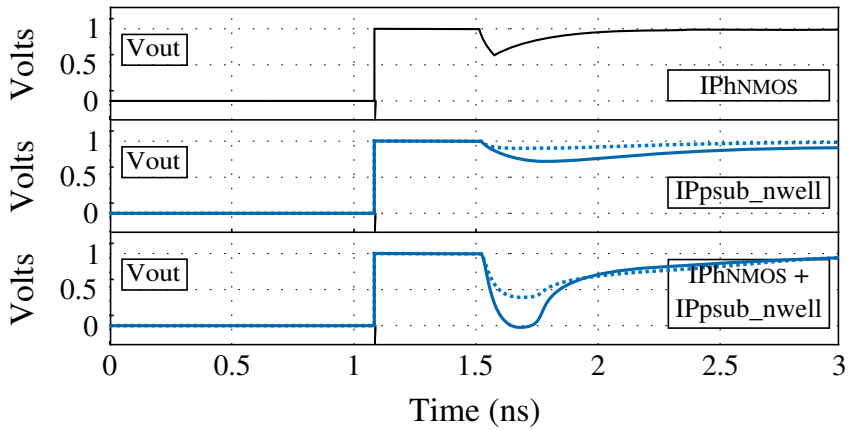


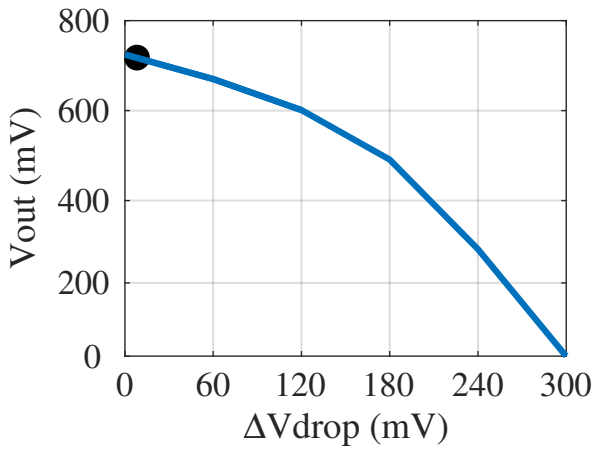
$$\Delta V_{out}(without IR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

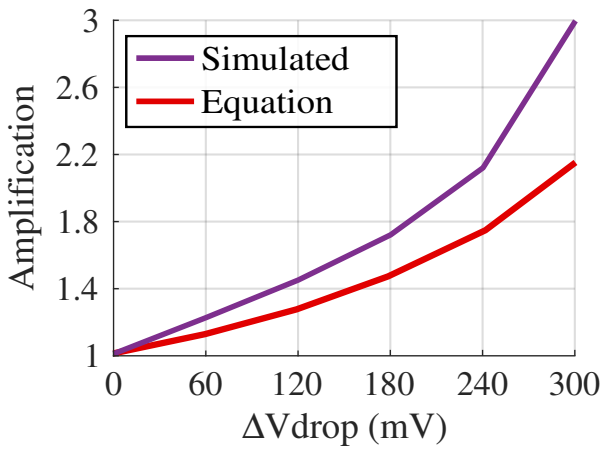
$$\Delta V_{out}(with IR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

5.3 - IR drop contribution to the fault injection mechanism







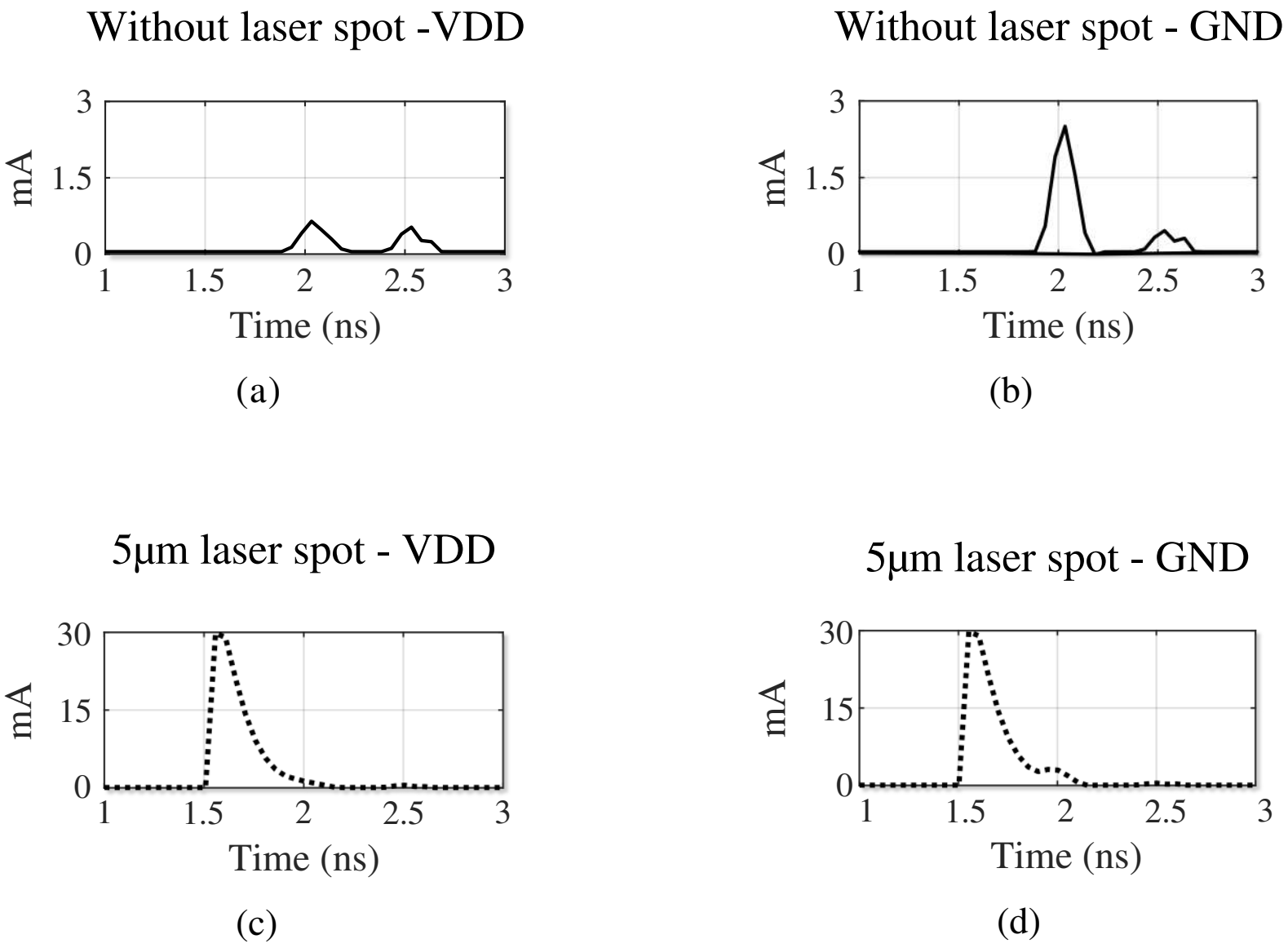


$$\Delta V_{out}(withoutIR) = -\frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}$$

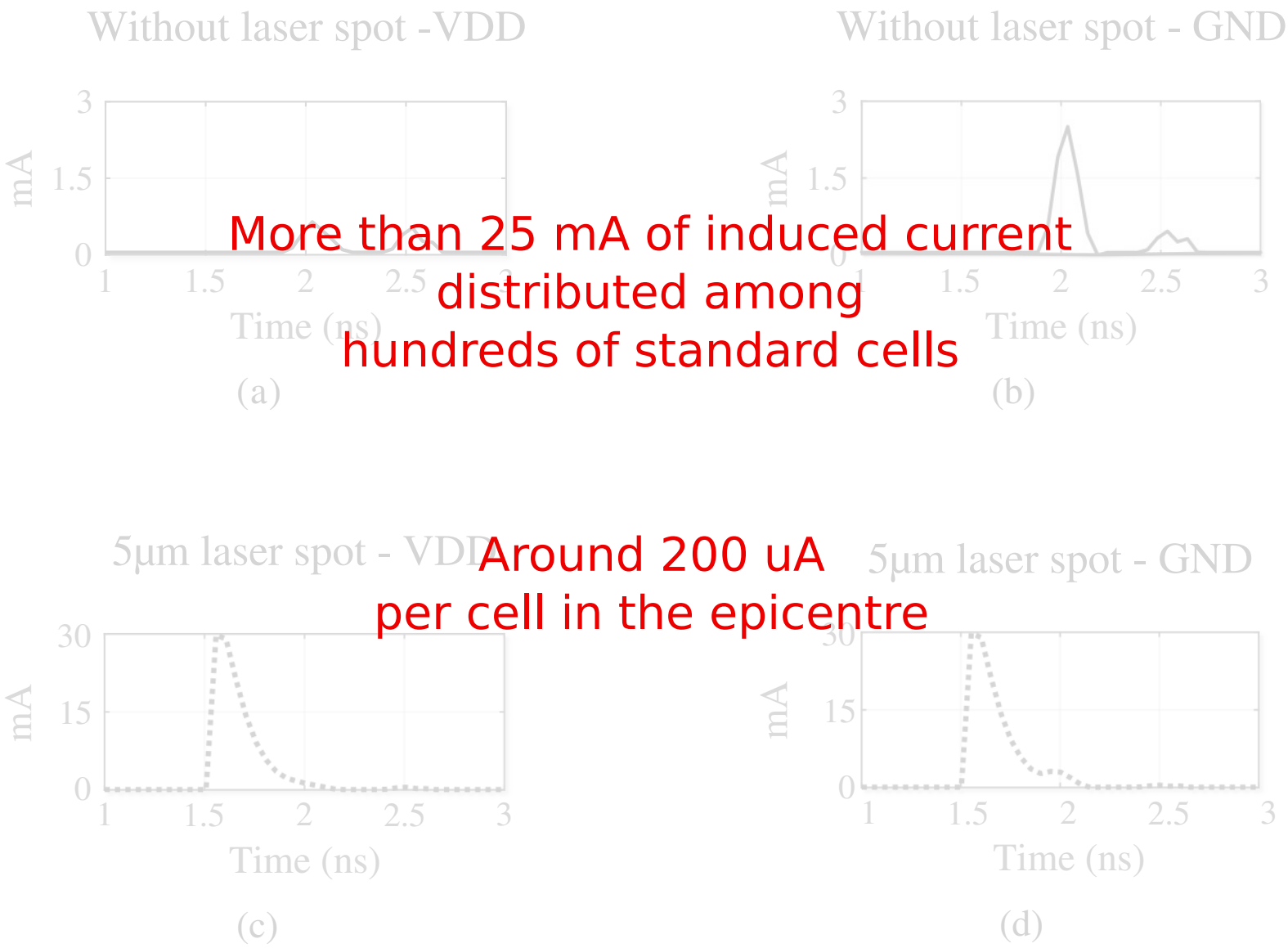
$$\Delta V_{out}(withIR) = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}$$

$$\frac{\Delta V_{out}(withIR)}{\Delta V_{out}(withoutIR)} = \frac{1}{1 - \frac{V_{drop}}{V_{DD} - V_T}}$$

5.5 - Total dynamic current flowing in the circuit



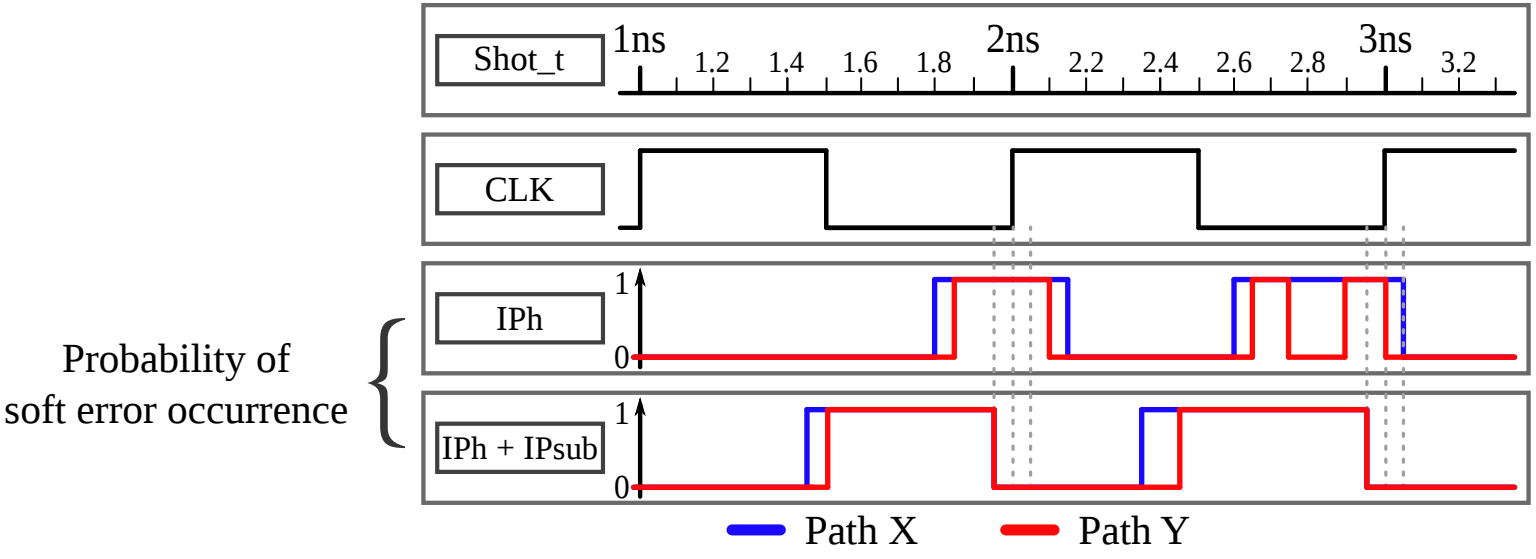
5.5 - Total dynamic current flowing in the circuit



More than 25 mA of induced current distributed among hundreds of standard cells

Around 200 uA per cell in the epicentre

5.4 - Probability of soft error occurence



Shot_t: Laser shot time

IPh: IPh contribution only

IPh + IPsub: IPh + IPsub_nwell contribution