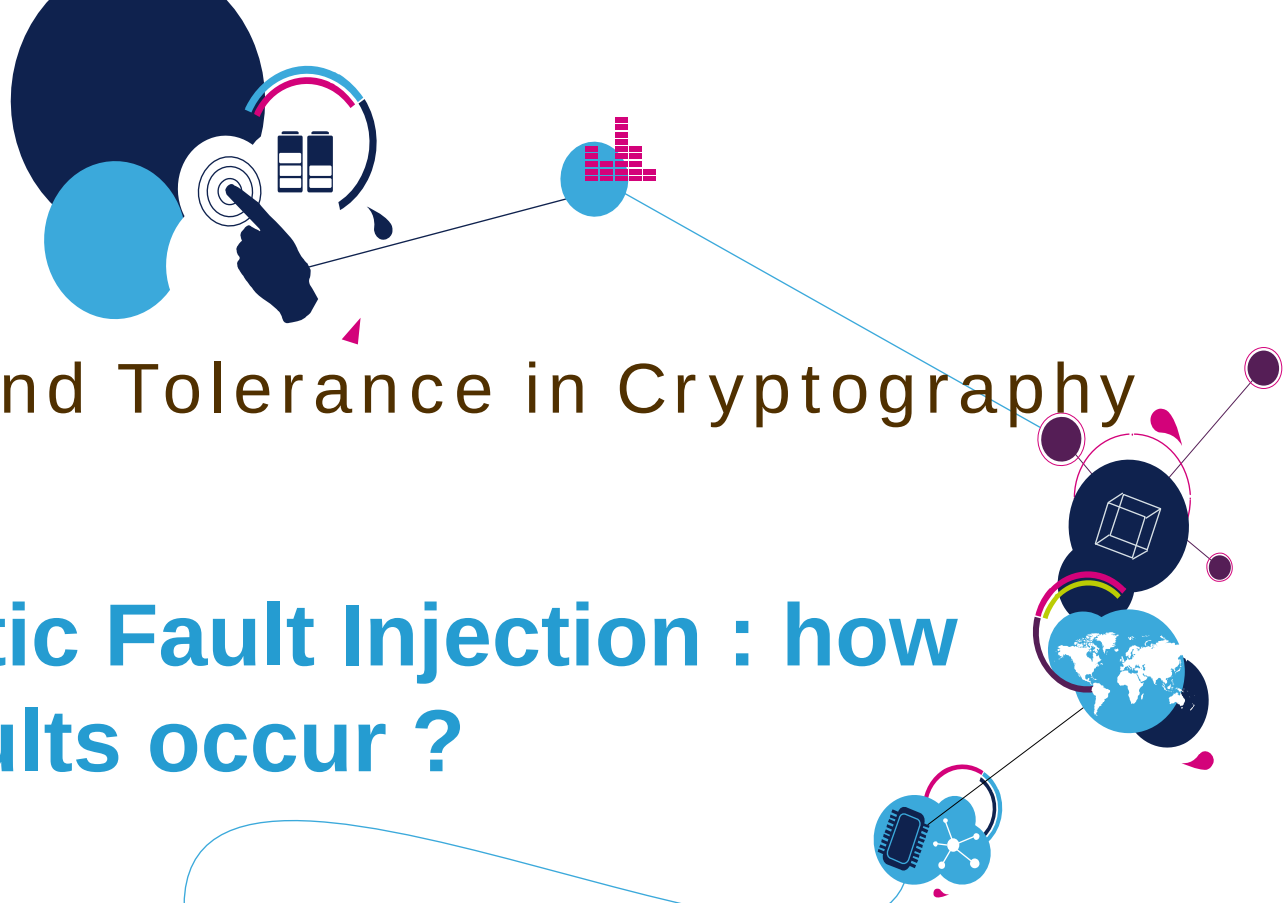
Electromagnetic Fault Injection : How Faults Occur

Mathieu Dumont, Mathieu Lisart, Philippe Maurine

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography



Fault Diagnosis and Tolerance in Cryptography 2019

Electromagnetic Fault Injection : how faults occur ?

Authors : **Mathieu DUMONT** [1,2] , Philippe MAURINE [2], Mathieu LISART [1]

[1] STMicroelectronics, Rousset, France
[2] LIRMM, University of Montpellier, Montpellier, France

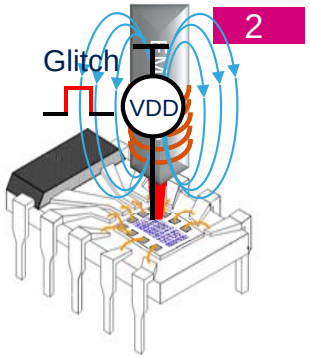
LIRMM

24/08/19

life.augmented

Introduction

- Context :
  - Attack by Fault injection : Glitch attack, Laser attack, **Electromagnetic Fault injection (EMFI).**
  - EMFI Fault model : Timing Fault (2012) by A.Dehbaoui ; **Sampling fault** (2016) S.Ordas.

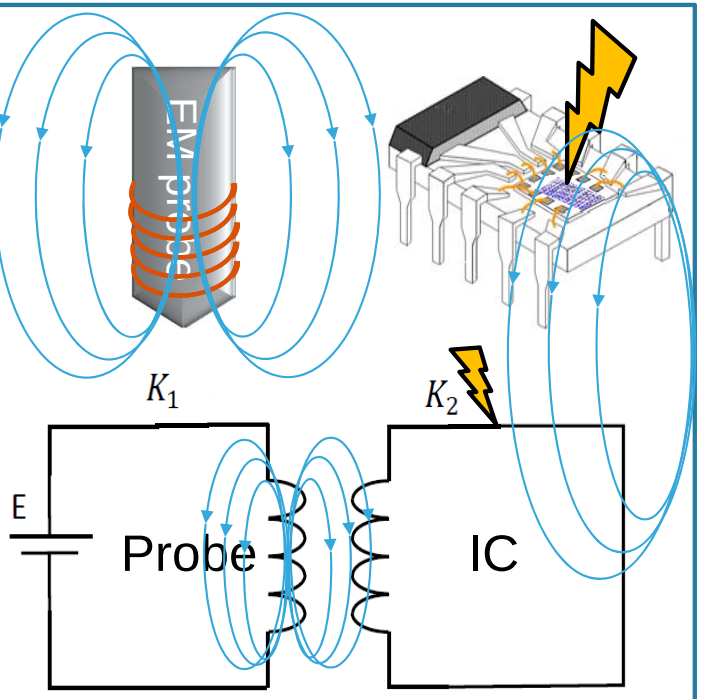


- Objectives :
  - Modelling : impact of an EMFI on IC supply voltage
  - SPICE simulation : impact of an EMFI on IC operation
  - Experimental validation

- Modelling: Impact of an EMFI on IC supply voltage
- Spice Simulation : impact of EMFI on IC operation
- Experimental Validation

Modelling: Impact of an EMFI on IC

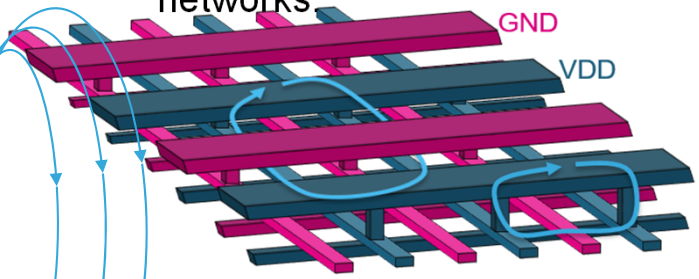
- EM Induction: hypothesis ?



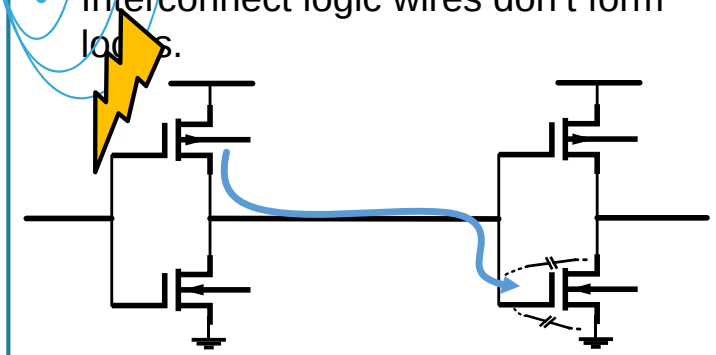
- EM induction induces currents variation on closed loops.

- Metal wires from the power/ground networks form many loops !

EMFI induces parasitic currents mostly in the power and ground networks.

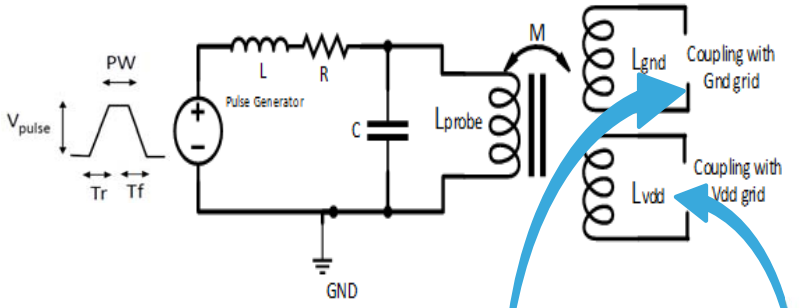


- Interconnect logic wires don't form loops.

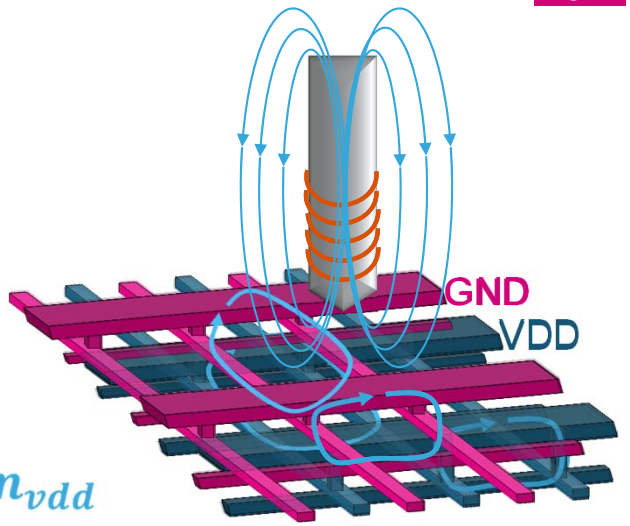


Modelling: Impact of an EMFI on IC

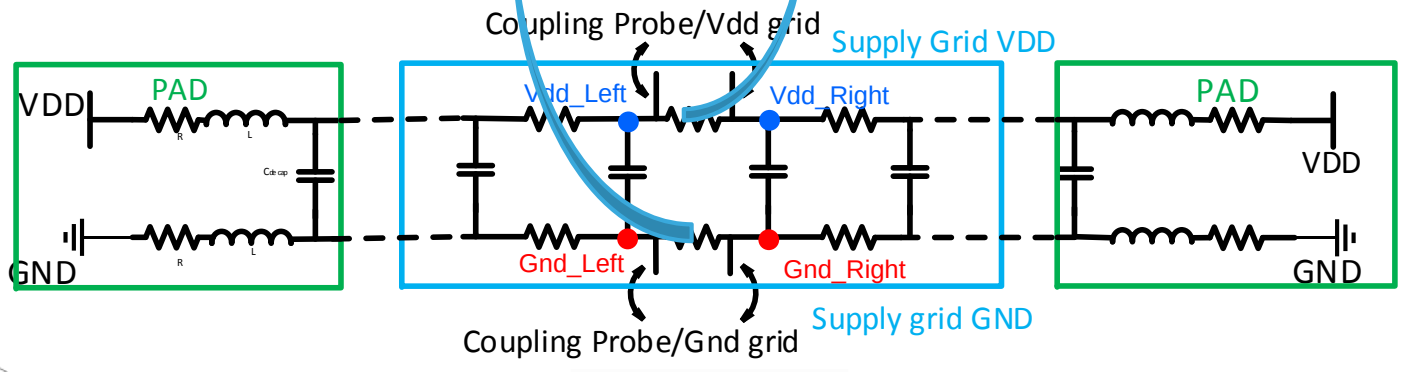
- Impact of EMFI on supply voltage.



$$m_{gnd} = k_{gnd}\sqrt{L_{probe} \times L_{gnd}}$$
$$m_{vdd} = k_{vdd}\sqrt{L_{probe} \times L_{vdd}}$$

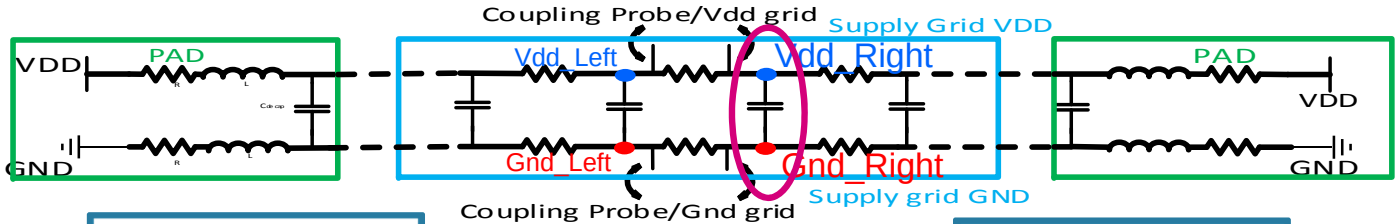


m_{gnd} m_{vdd}



Modelling: Impact of an EMFI on IC

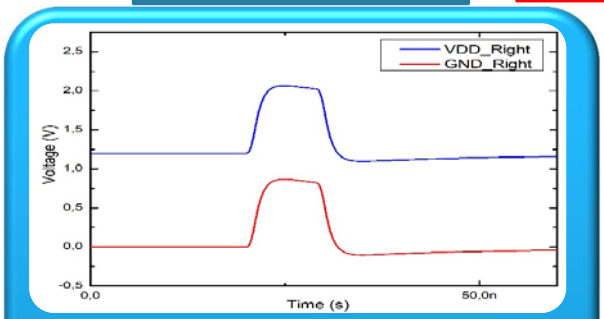
- Impact of EMFI on supply voltage.

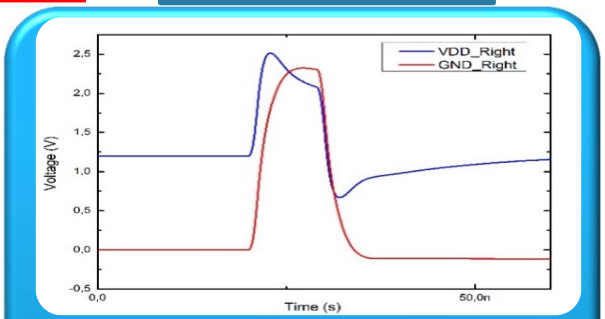


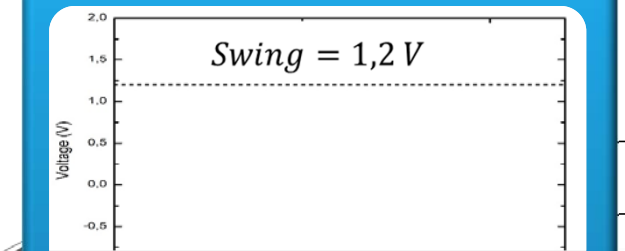
$m_{vdd} = m_{gnd}$

$\boldsymbol{Swing = Vdd - Gnd}$

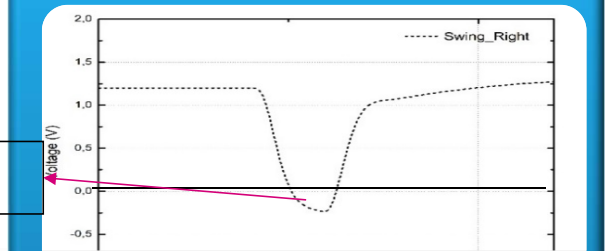
$m_{vdd} \neq m_{gnd}$



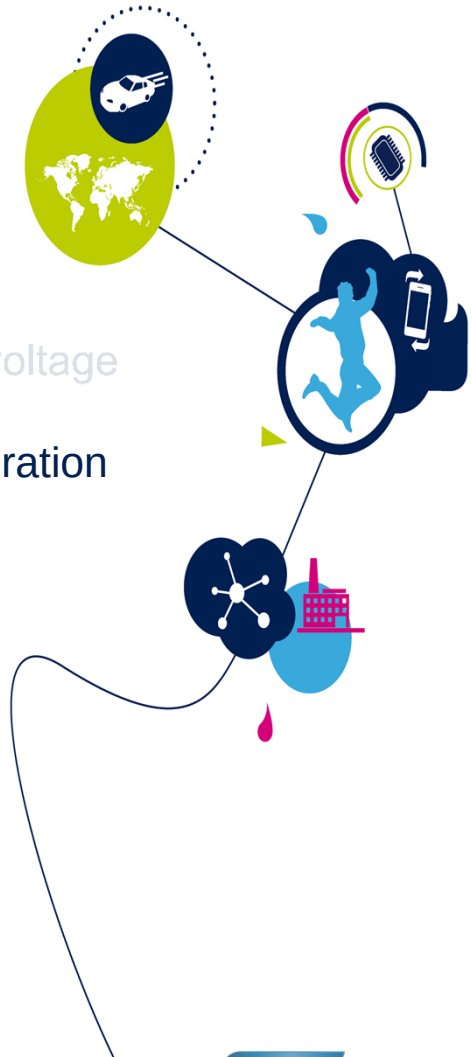




Swing is negative for few ns !

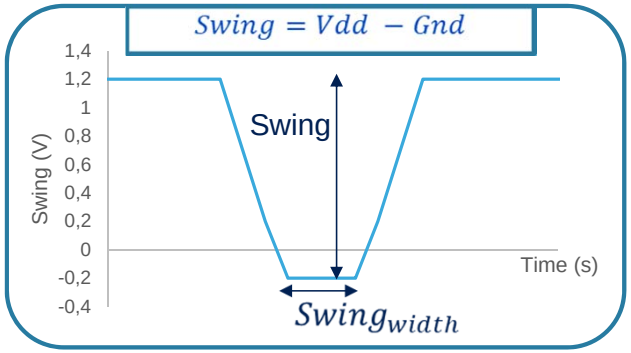


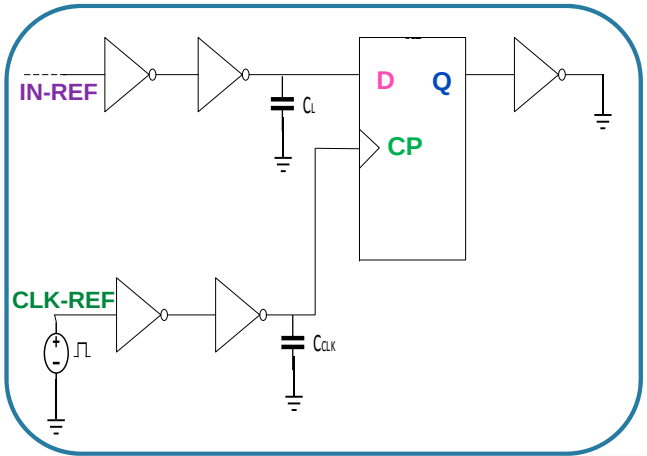
- Modelling: Impact of an EMFI on IC supply voltage
- Spice Simulation : impact of EMFI on IC operation
- Experimental Validation

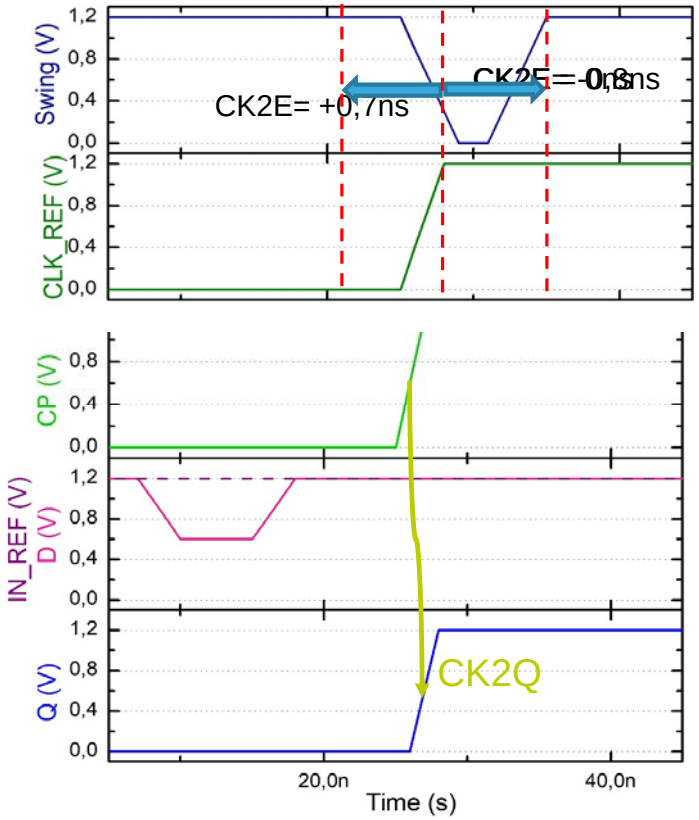


Modelling: Impact of an EMFI on IC

- Testbench Simulation







Modelling: Impact of an EMFI on IC

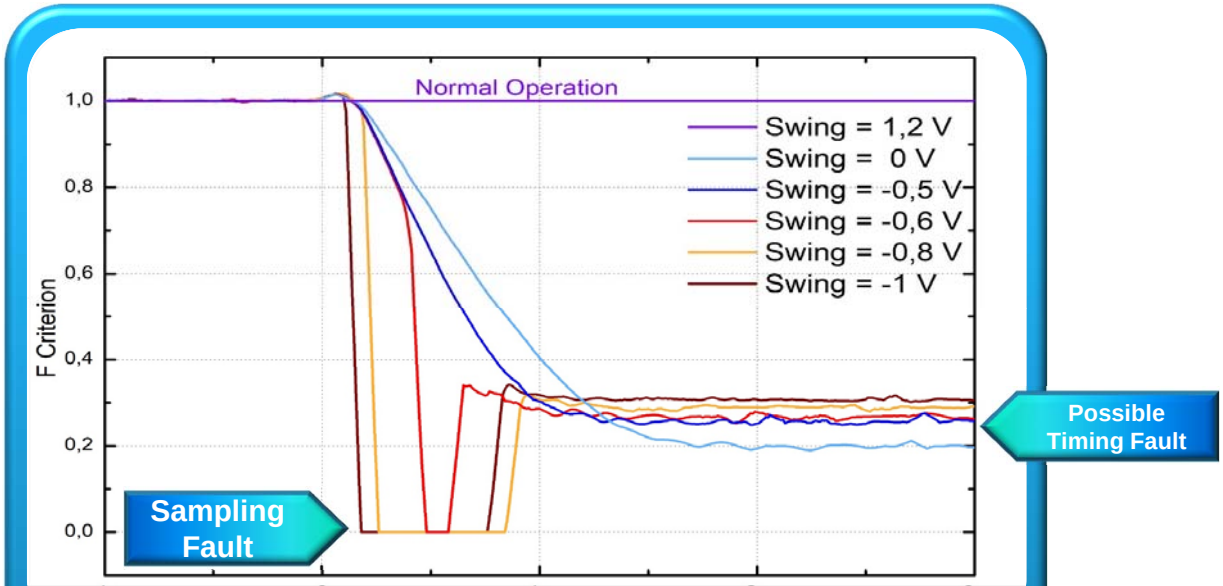
- Logic simulation: Swing amplitude impact on IC operation

Fault criterion F :

$$F = \frac{(CK2Q)_{ref}}{(CK2Q)_{inj}}$$

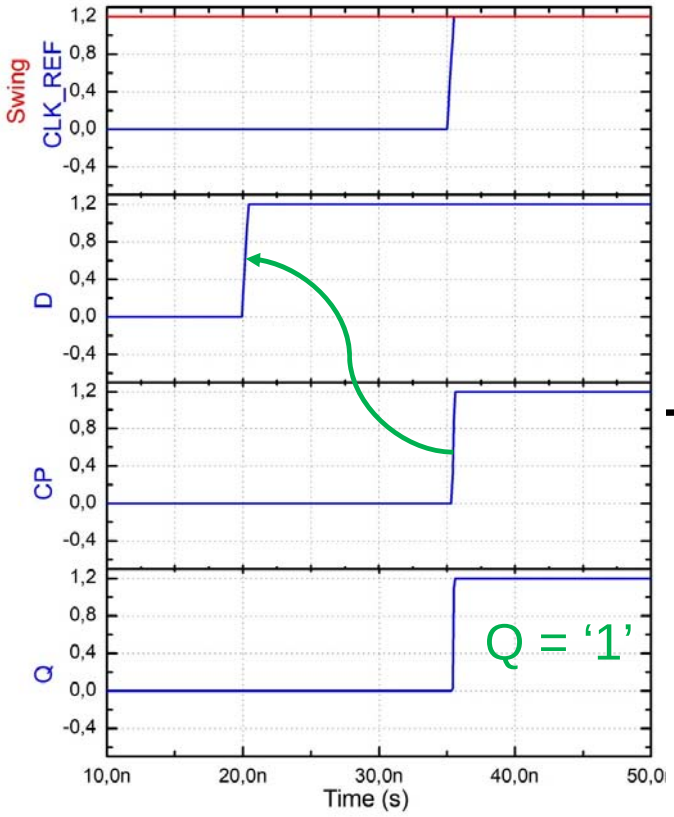
- $F = 1$ Normal Operation
- $0 < F < 1$ Delay
- $F = 0$ **Sampling Fault**

$(CK2Q)_{inj} \geq (CK2Q)_{ref}$



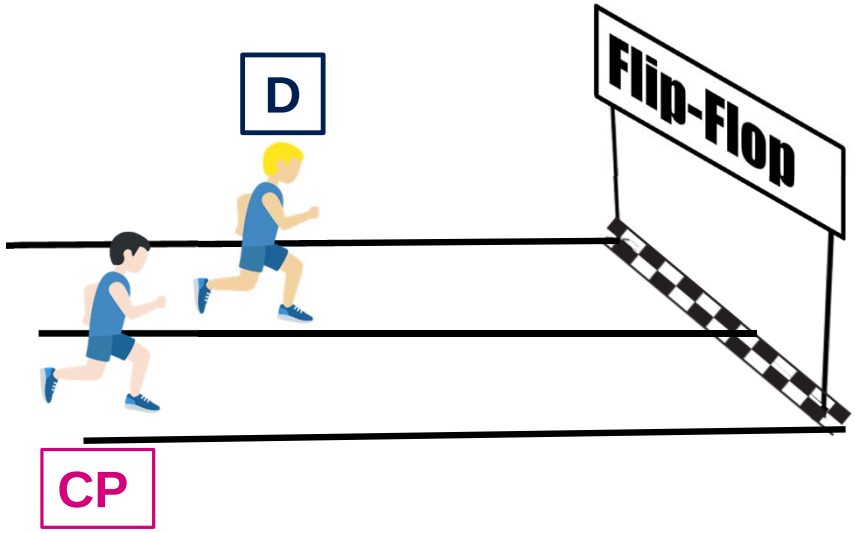
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation



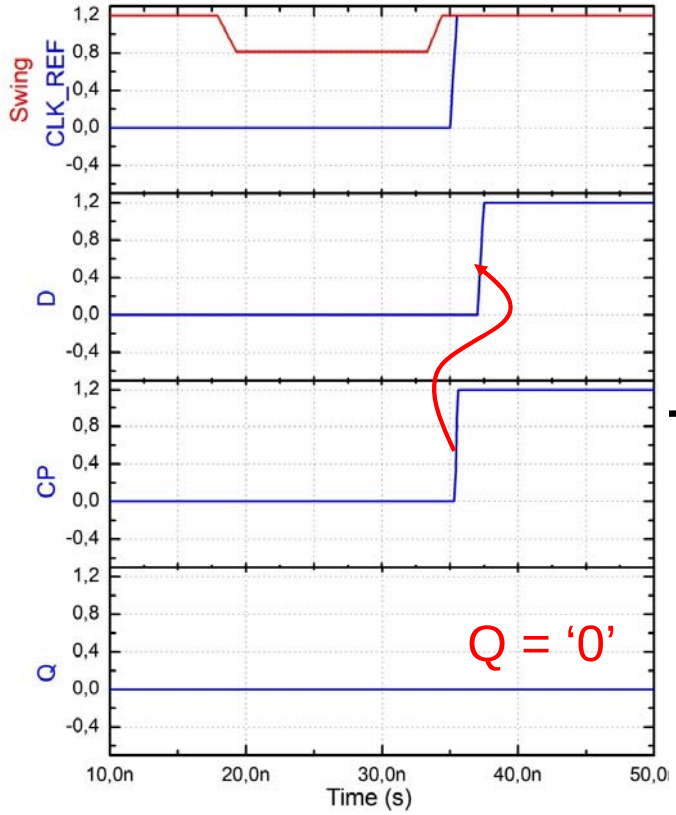
Normal Operation

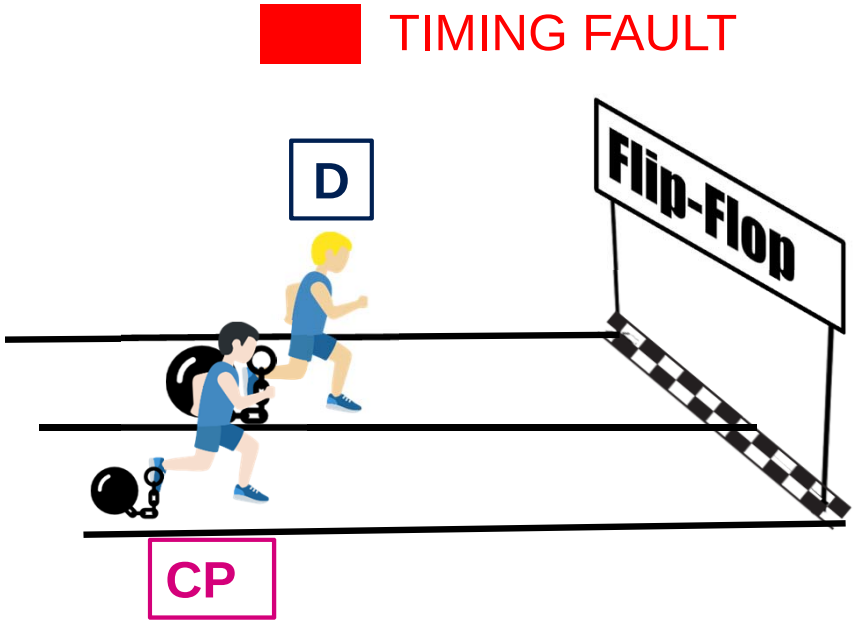
NO FAULT



Modelling: Impact of an EMFI on IC

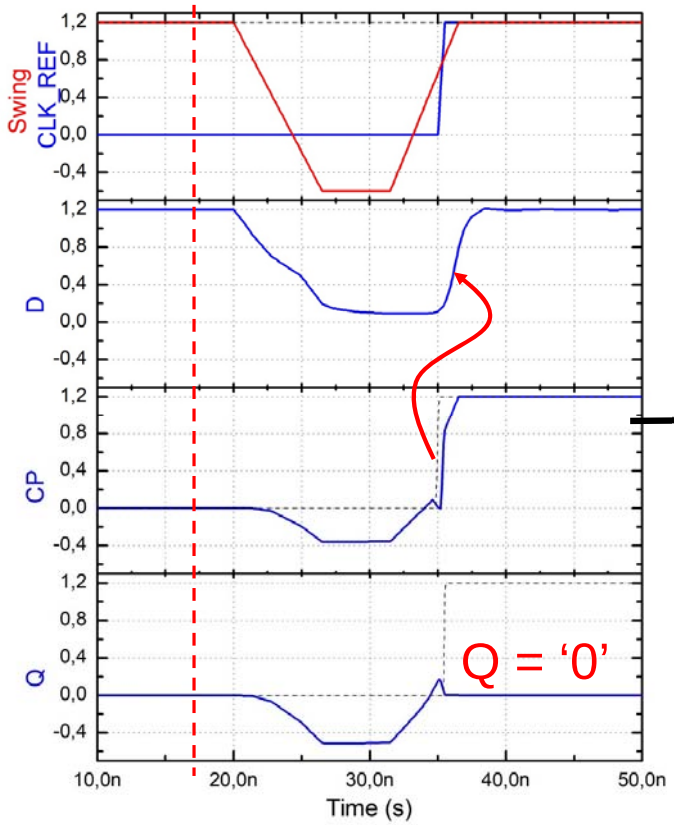
- Sampling Fault explanation

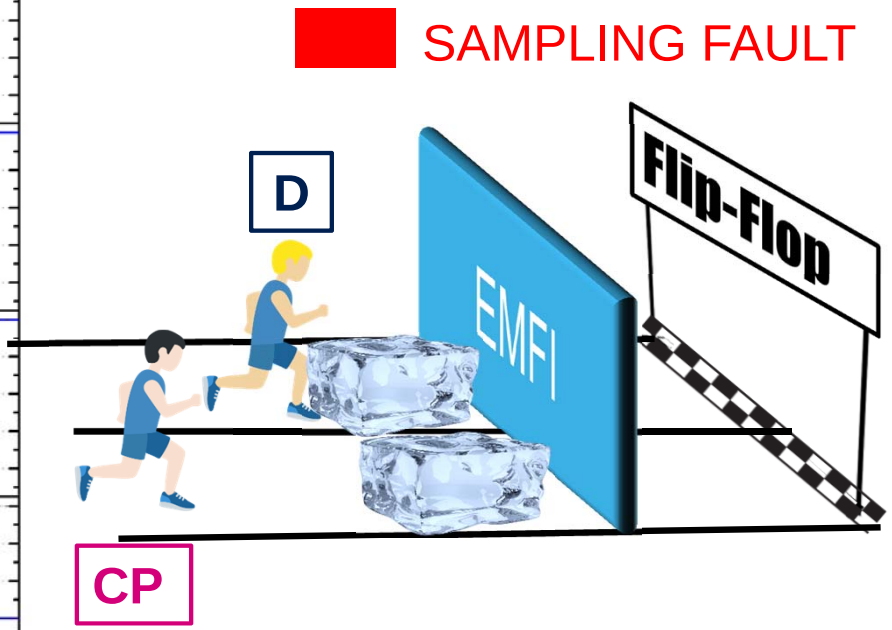




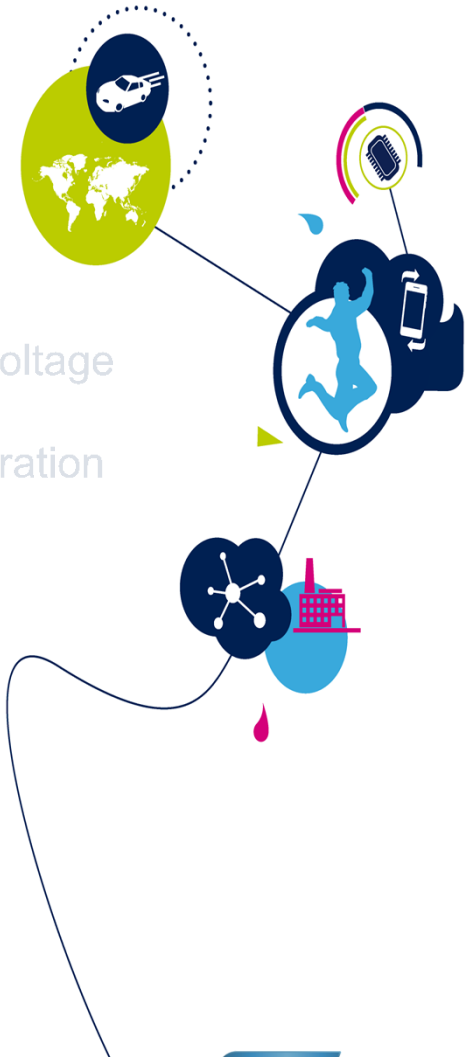
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation





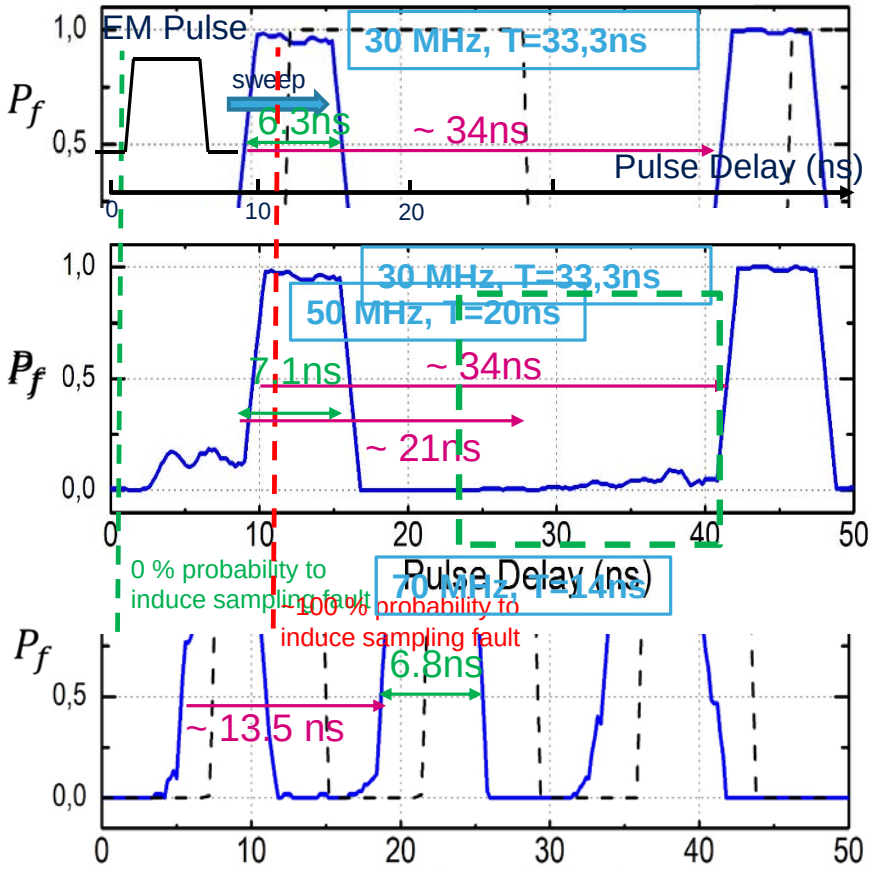
- Modelling: Impact of an EMFI on IC supply voltage
- Spice Simulation : impact of EMFI on IC operation
- Experimental Validation



EMFI experimental validation

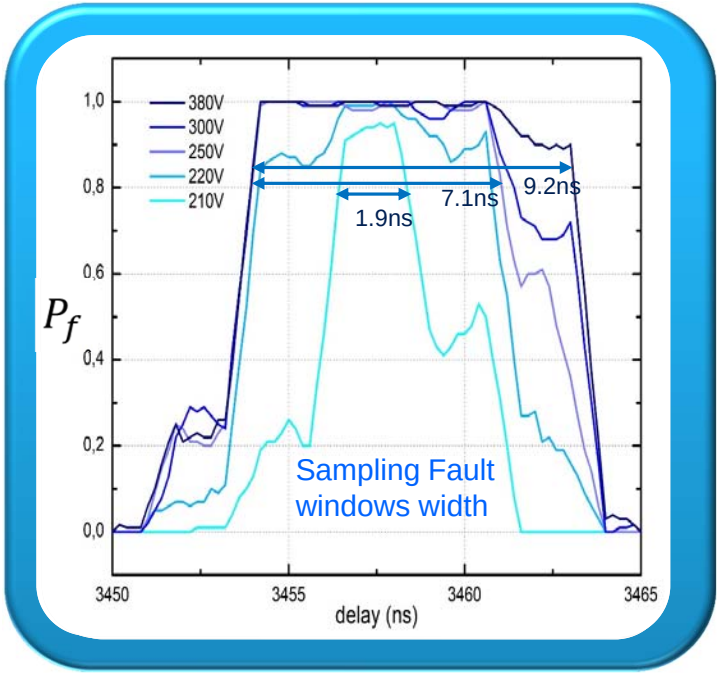
Effect of F_{CLK} variations

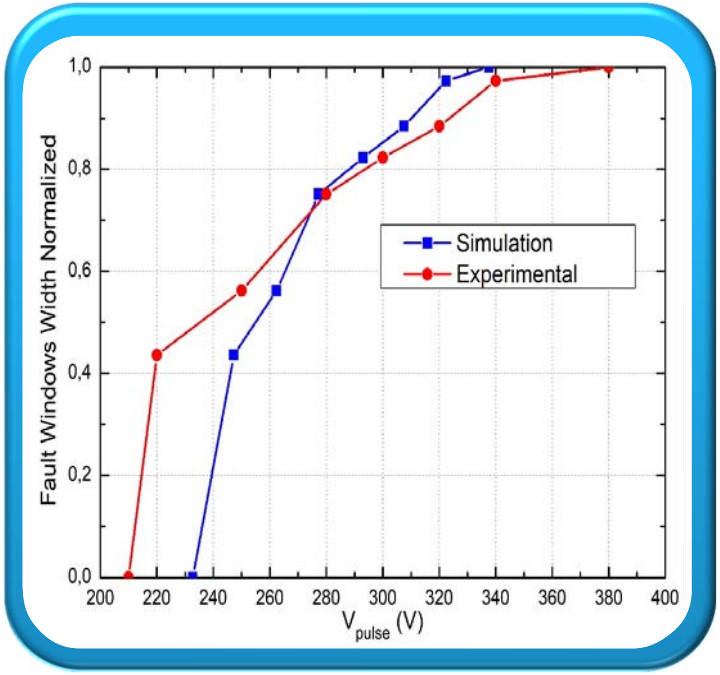
- Target : AES 128bits.
- EM pulse sweeps, for few periods, with a pulse delay step of 100ps.
- 50 EMFI shots are performed at each sweep to determine **fault probability** P_f $(0 < P_f < 1)$.
- As expected **Sampling Fault Windows** appear with a period equal to that of the IC.
- Their width are independent of the frequency.



EMFI experimental validation

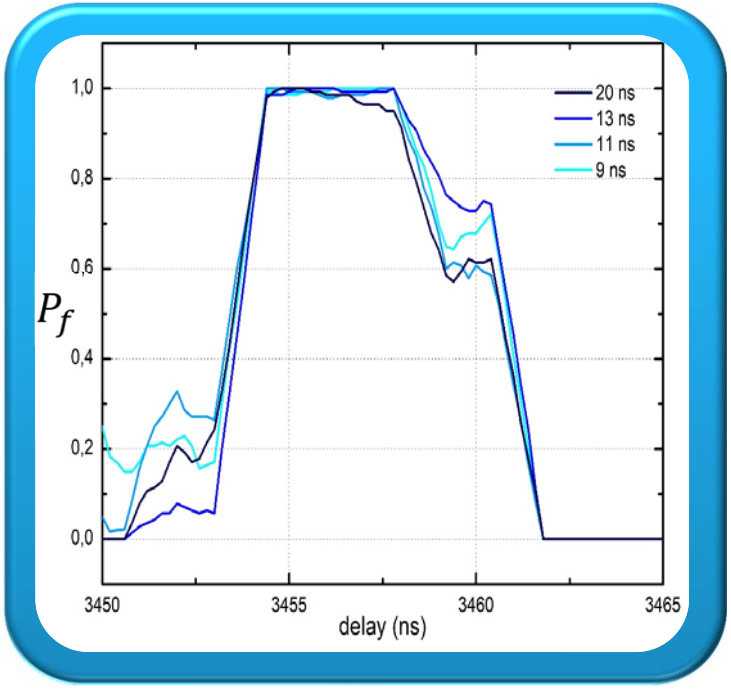
- **Effect of V_{pulse} variations**
  - Determine the evolution of the Sampling Fault Window width in function of V_{pulse} variations.
  - The width of Sampling Fault Windows increases with V_{pulse}.

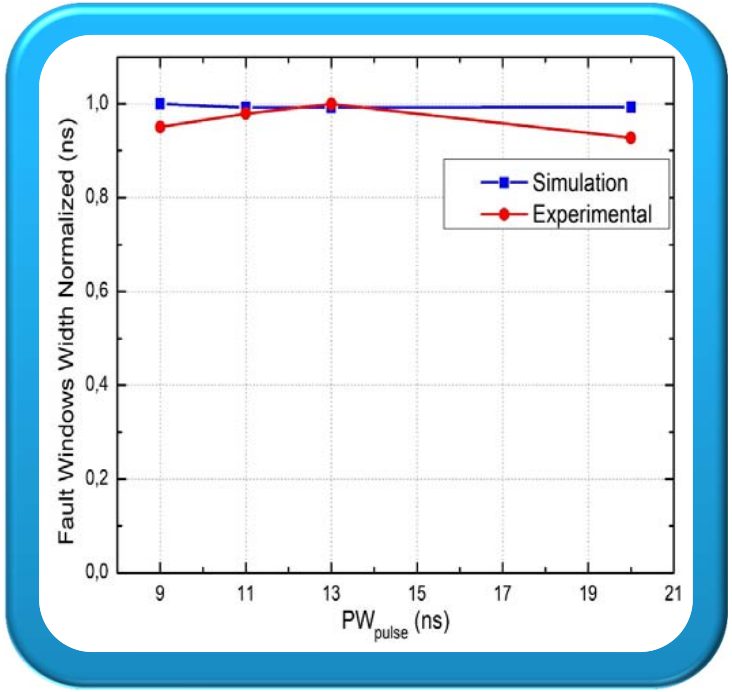




EMFI experimental validation

- Effect of PW variations
  - Determine the evolution of the Sampling Fault Window width in function of PW variations.
  - The Pulse Width does not affect much the sampling fault window.





Conclusion

- ## Conclusion
  - Modelling simulations show that EMFI induces a voltage **bounces or drops** on **power networks Vdd and GND.** That could induce a **Swing drop.**
  - Sampling Fault occurs when **EM Field** is applied during IC operation around rising CLK edge. In **simulation** and **experimentally**.

- ## Perspective
  - More accurate **coupling model.**
  - Experimental validation and parallel on **one register** only.

Thank you

Electromagnetic Fault Injection : how faults occur ?

Authors : **Mathieu DUMONT** [1,2] , Philippe MAURINE [2], Mathieu LISART [1]

[1] STMicroelectronics, Rousset, France
[2] LIRMM, University of Montpellier, Montpellier, France

FDTC 2019

Modelling: Impact of an EMFI on IC

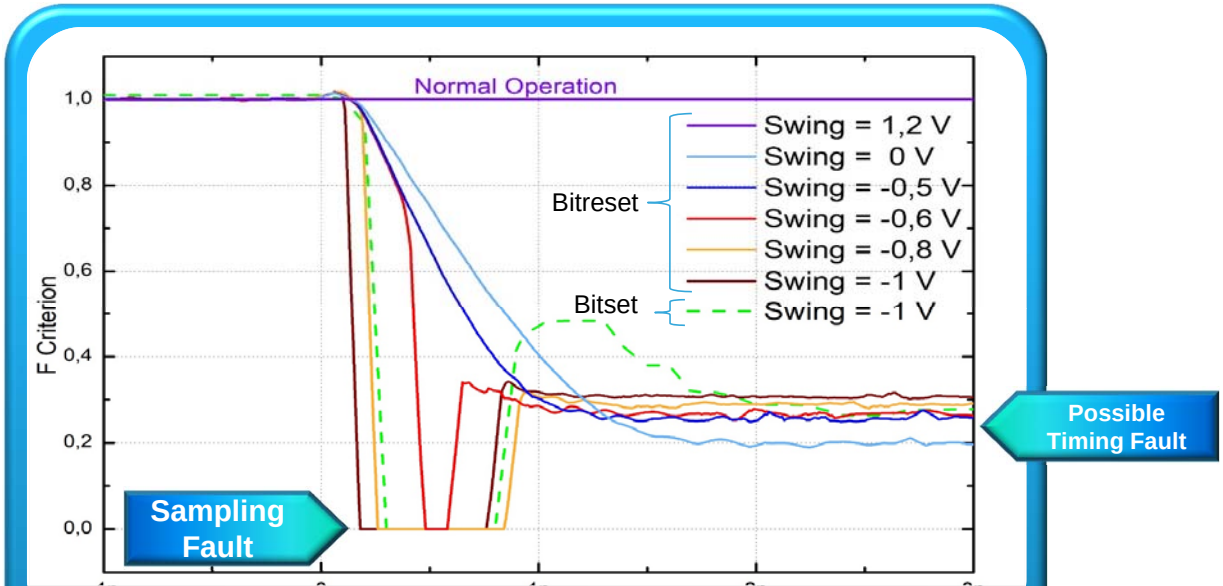
- Logic simulation: Swing amplitude impact on IC operation

Fault criterion F :

$$F = \frac{(CK2Q)_{ref}}{(CK2Q)_{inj}}$$

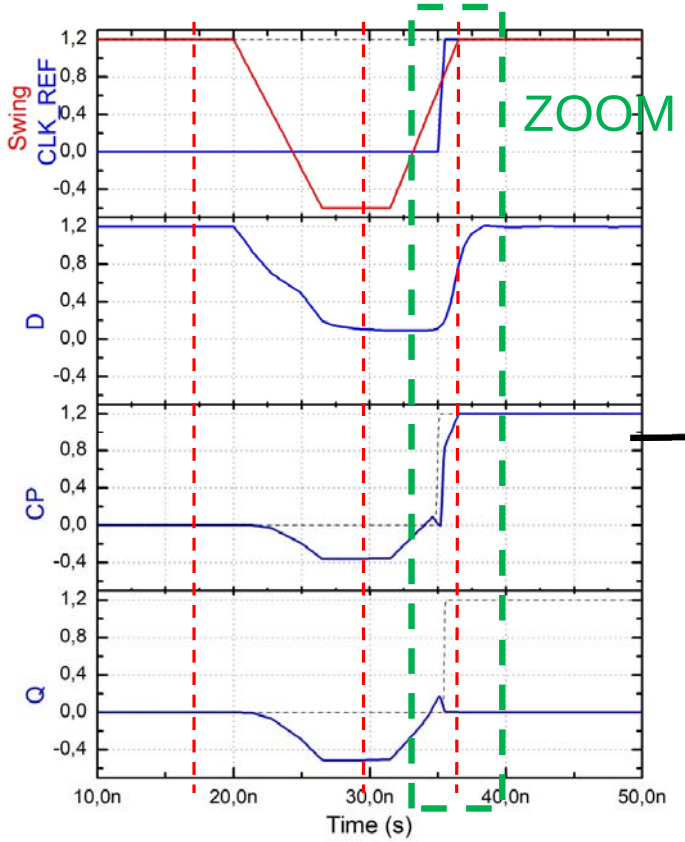
- $F = 1$ Normal Operation
- $0 < F < 1$ Delay
- $F = 0$ **Sampling Fault**

$(CK2Q)_{inj} \geq (CK2Q)_{ref}$



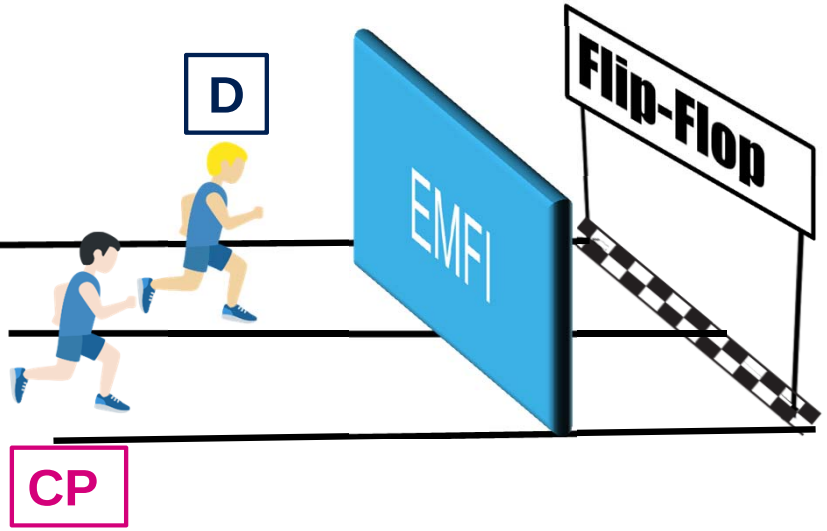
Modelling : Impact of an EMFI on IC

- Sampling Fault explanation



ZOOM

SAMPLING FAULT



Modelling : Impact of an EMFI on IC

- Sampling Fault explanation