



HAL
open science

Electromagnetic Fault Injection : How Faults Occur

Mathieu Dumont, Mathieu Lisart, Philippe Maurine

► **To cite this version:**

Mathieu Dumont, Mathieu Lisart, Philippe Maurine. Electromagnetic Fault Injection : How Faults Occur. FDTC 2019 - Workshop on Fault Diagnosis and Tolerance in Cryptography, Aug 2019, Atlanta, GA, United States. pp.9-16, 10.1109/FDTC.2019.00010 . lirmm-02328109

HAL Id: lirmm-02328109

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-02328109v1>

Submitted on 31 Mar 2022

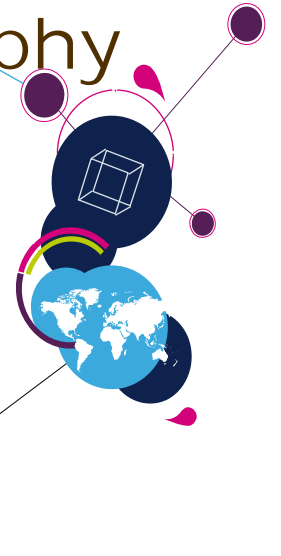
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



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

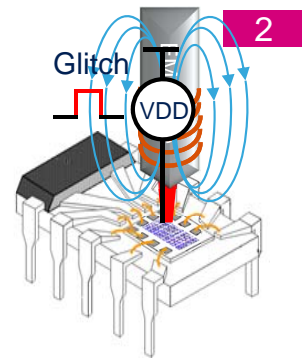
Introduction

- Context :

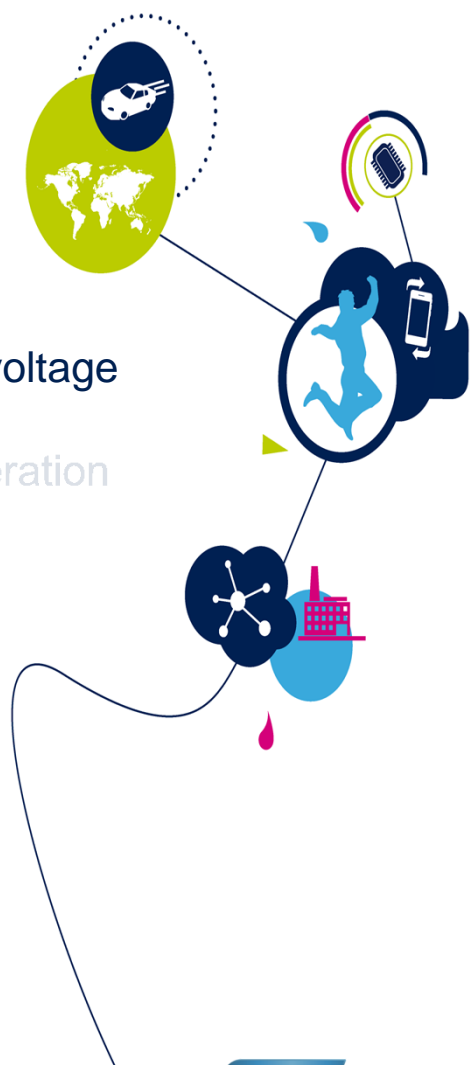
- Attack by Fault injection : Glitch attack, Laser attack, **Electromagnetic Fault injection (EMFI)**.
- EMFI Fault model : Timing Fault (2012) by A.Dehibaoui ; **Sampling fault** (2016) S.Ordas.

- Objectives :

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

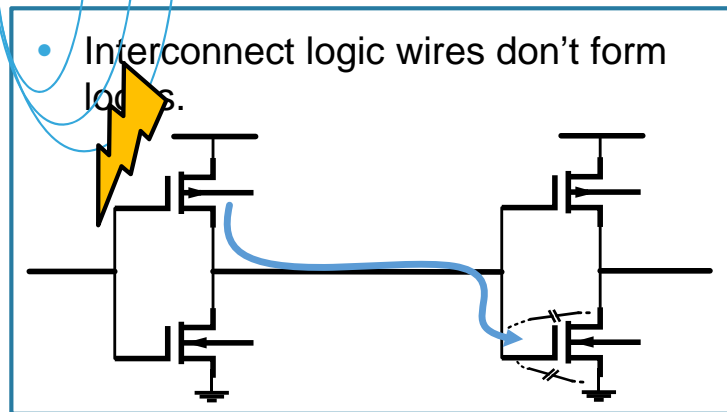
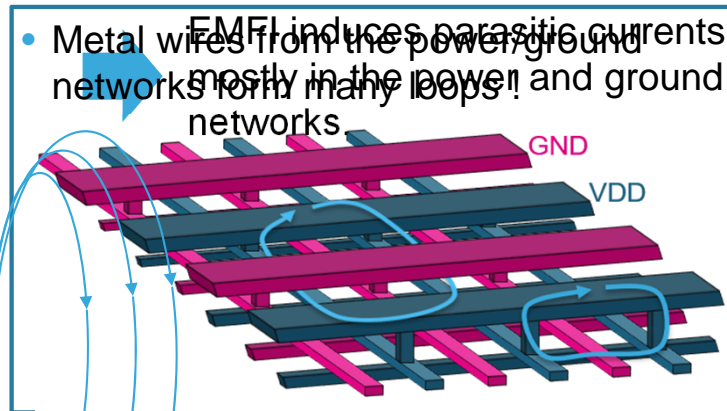
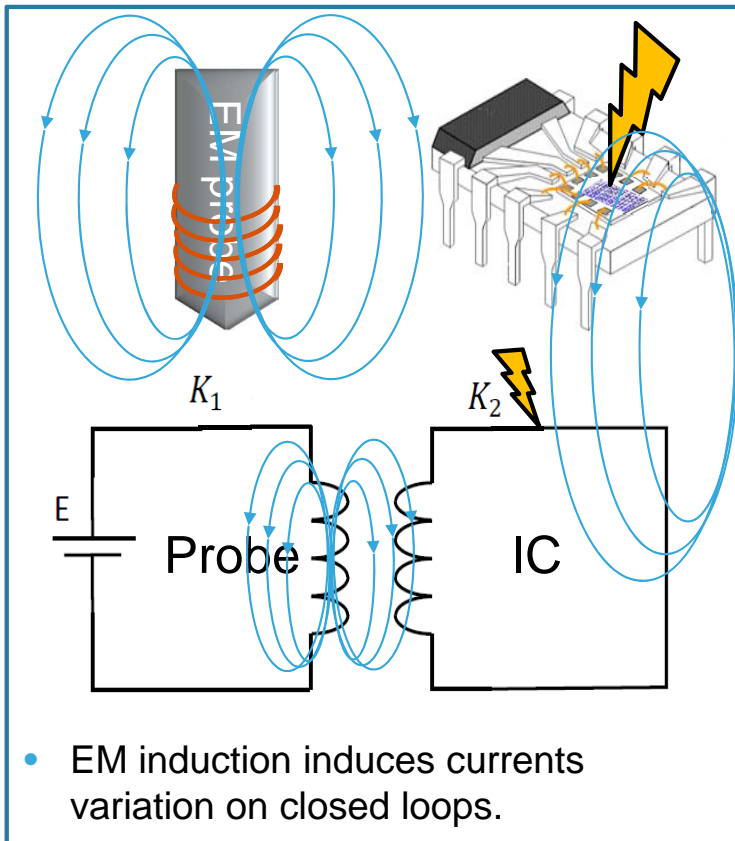


- Modelling: Impact of an EMFI on IC supply voltage
- Spice Simulation : impact of EMFI on IC operation
- Experimental Validation



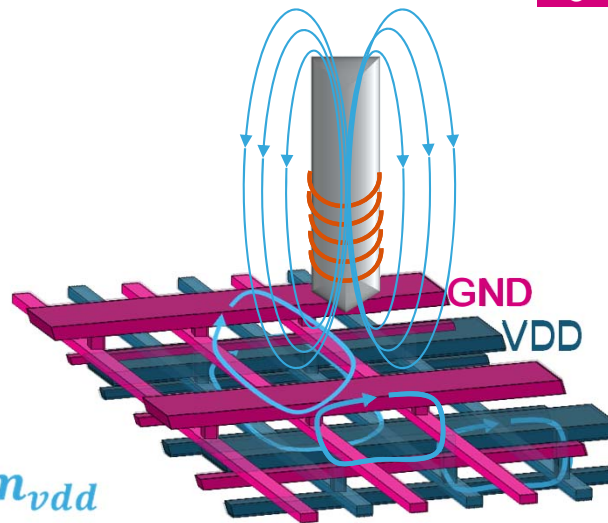
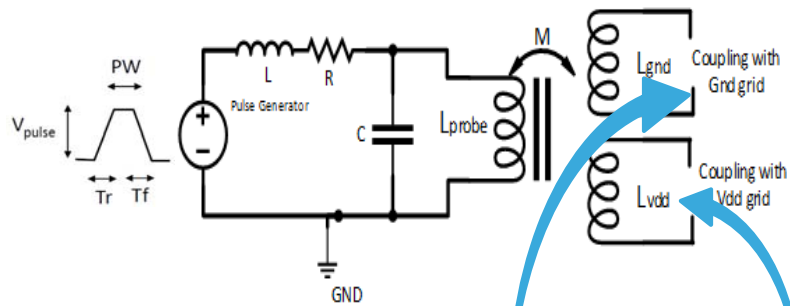
Modelling: Impact of an EMFI on IC

- EM Induction: hypothesis ?



Modelling: Impact of an EMFI on IC

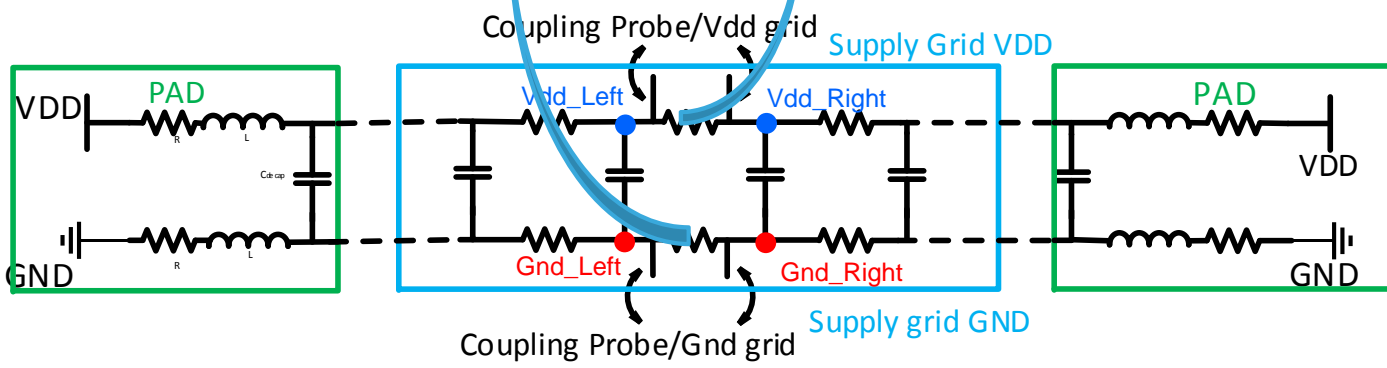
- Impact of EMFI on supply voltage.



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

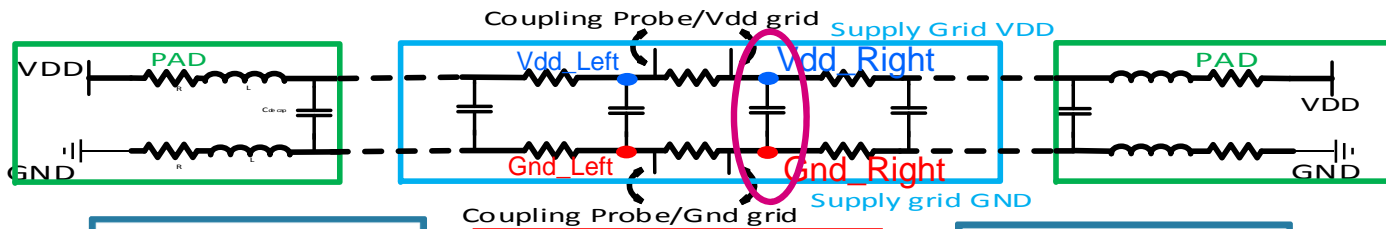
$$m_{vdd} = k_{vdd} \sqrt{L_{probe} \times L_{vdd}}$$

m_{gnd} m_{vdd}



Modelling: Impact of an EMFI on IC

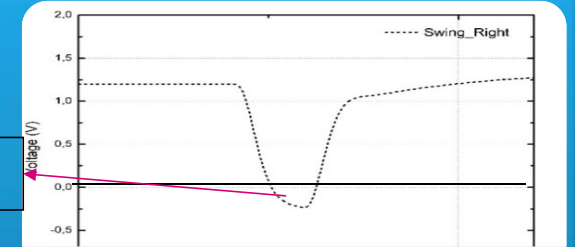
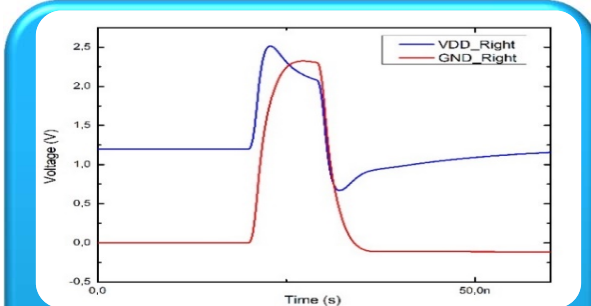
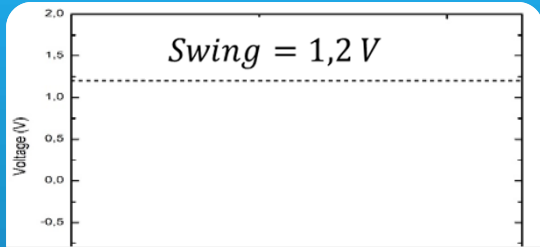
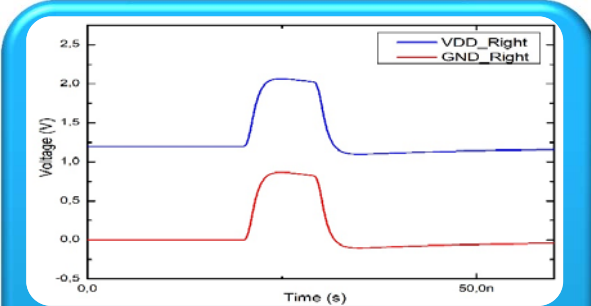
- Impact of EMFI on supply voltage.



$$m_{vdd} = m_{gnd}$$

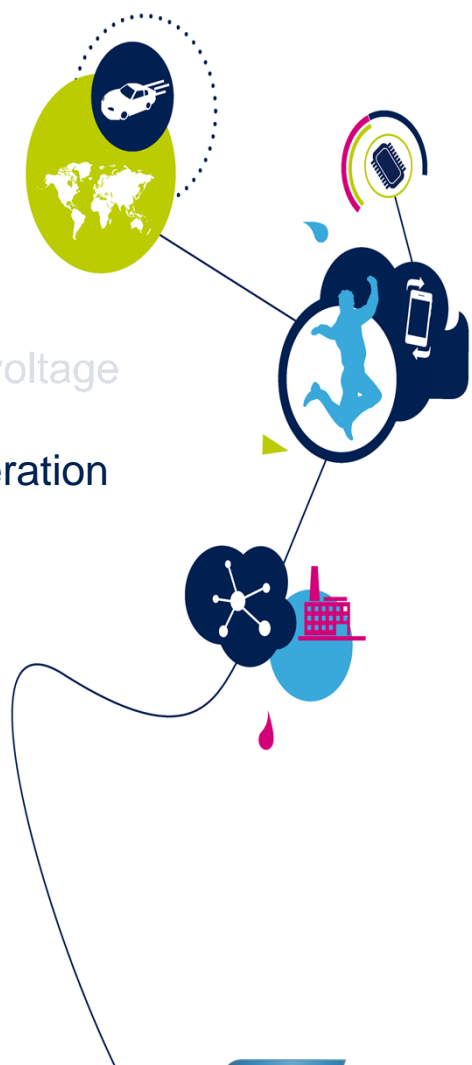
$$\text{Swing} = Vdd - Gnd$$

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



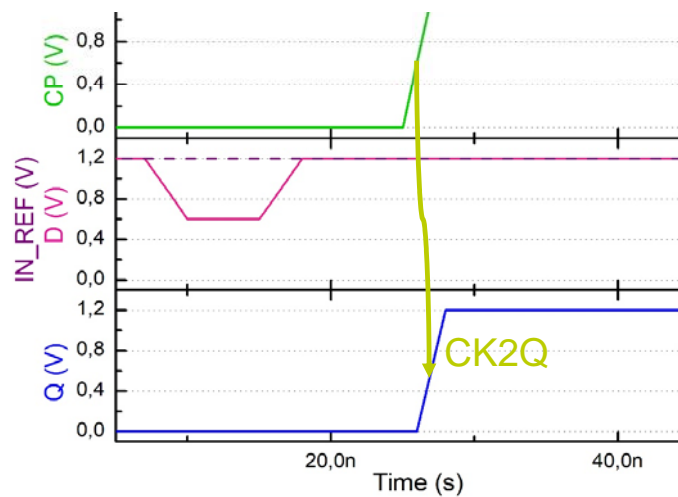
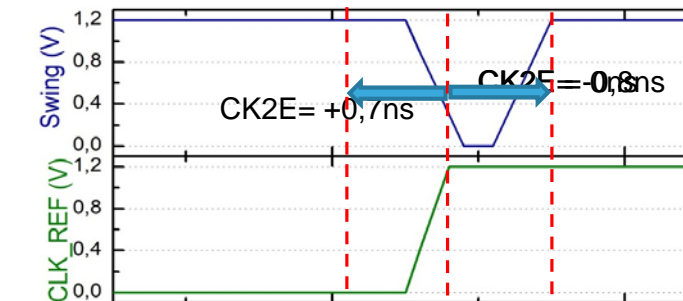
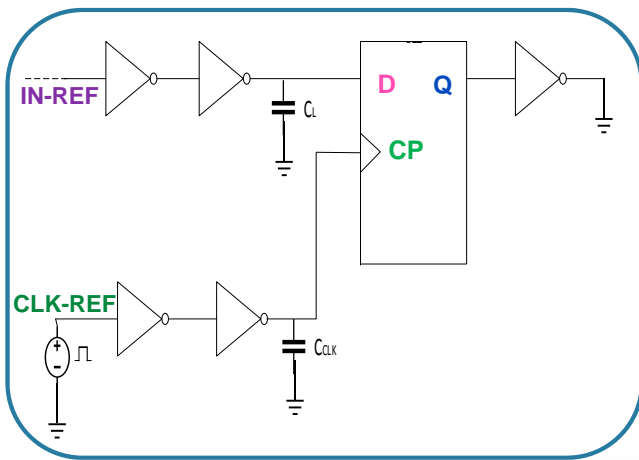
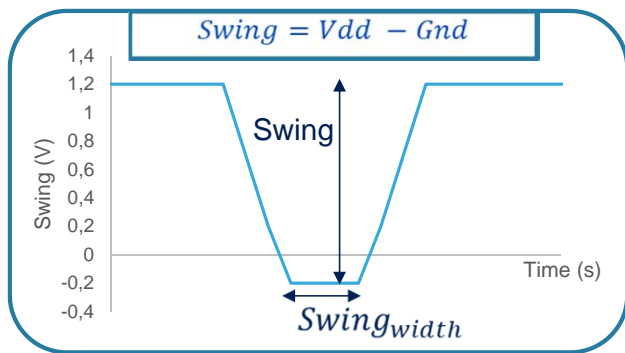
Swing is negative for few ns !

- 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 :

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

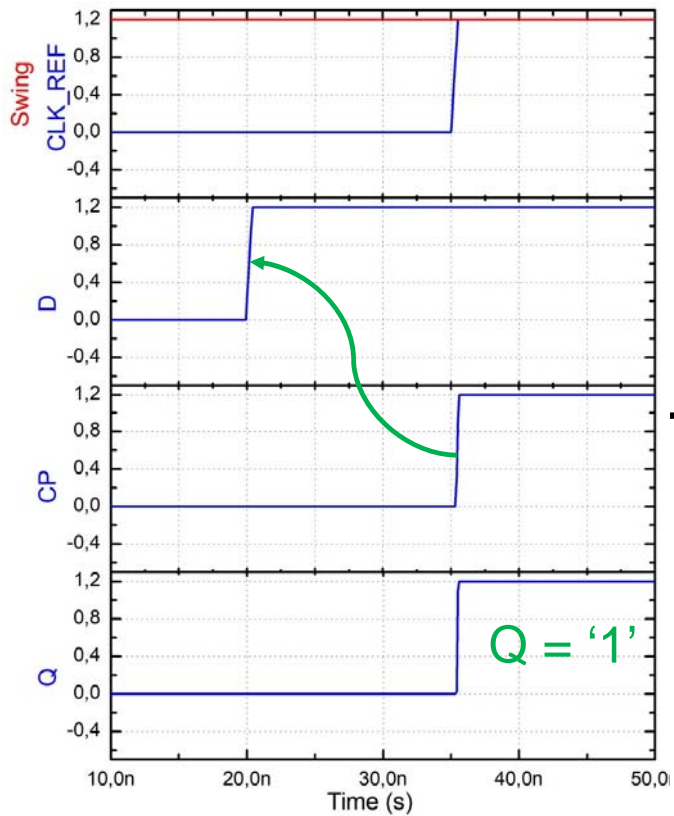
- $F = 1$ Normal Operation
- $0 < F < 1$ Delay
- $F = 0$ Sampling Fault

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



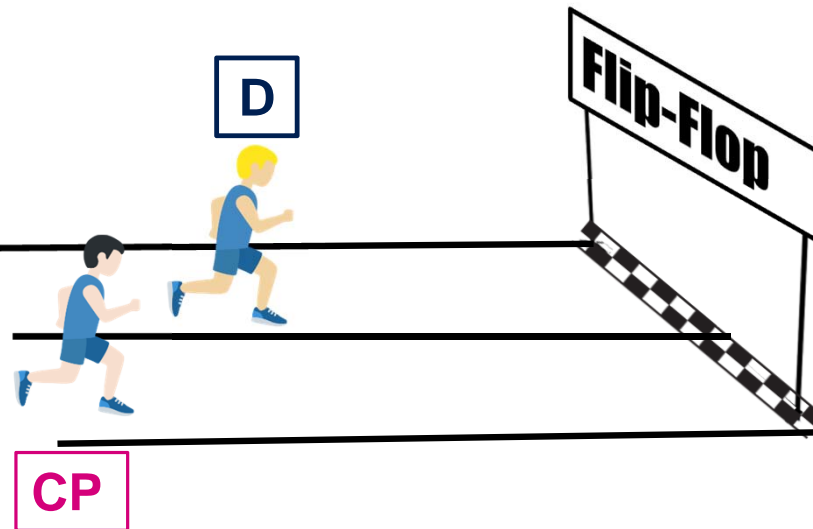
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation



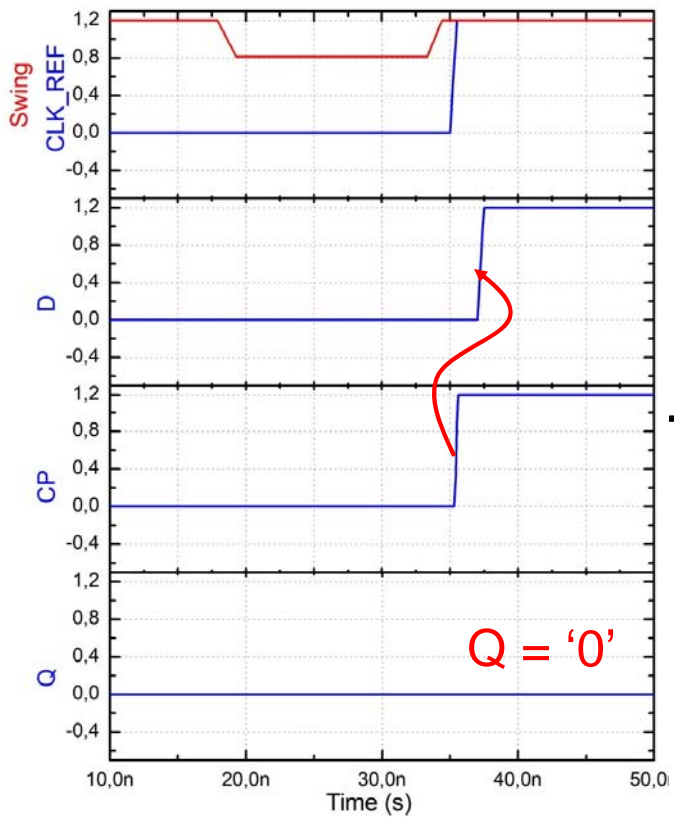
Normal Operation

NO FAULT

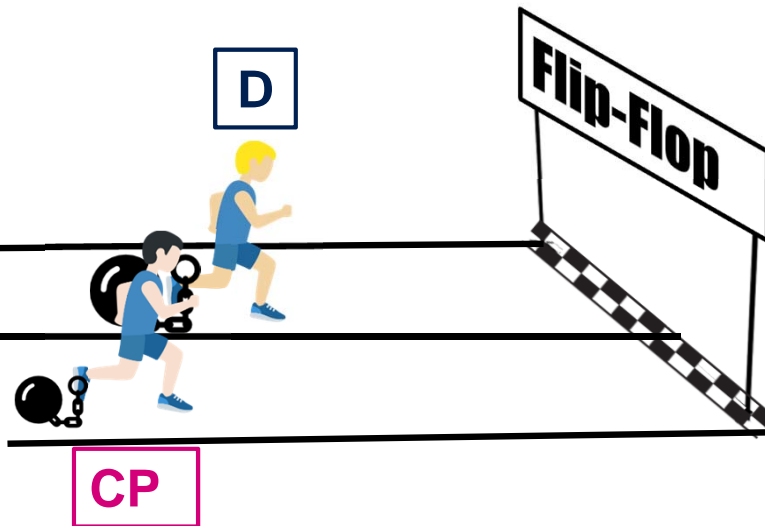


Modelling: Impact of an EMFI on IC

- Sampling Fault explanation

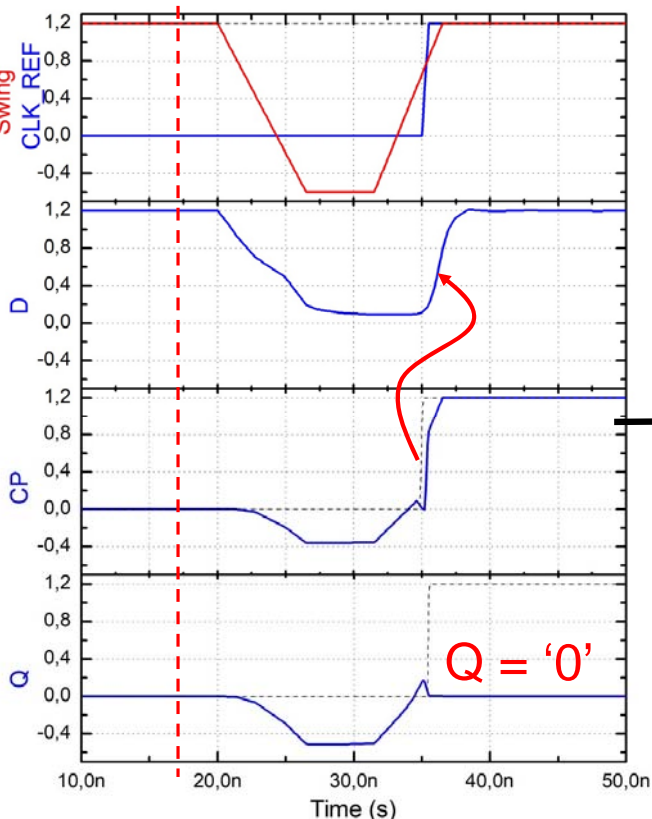


TIMING FAULT

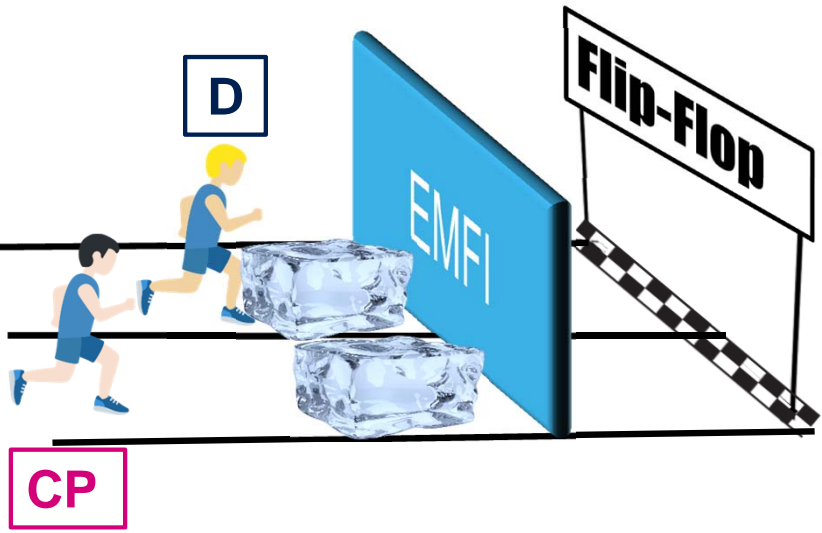


Modelling: Impact of an EMFI on IC

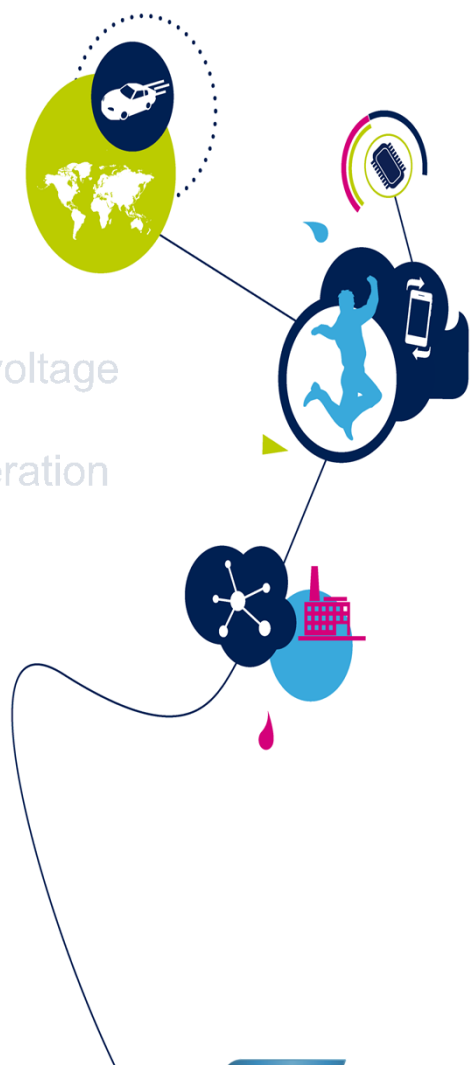
- Sampling Fault explanation



SAMPLING FAULT



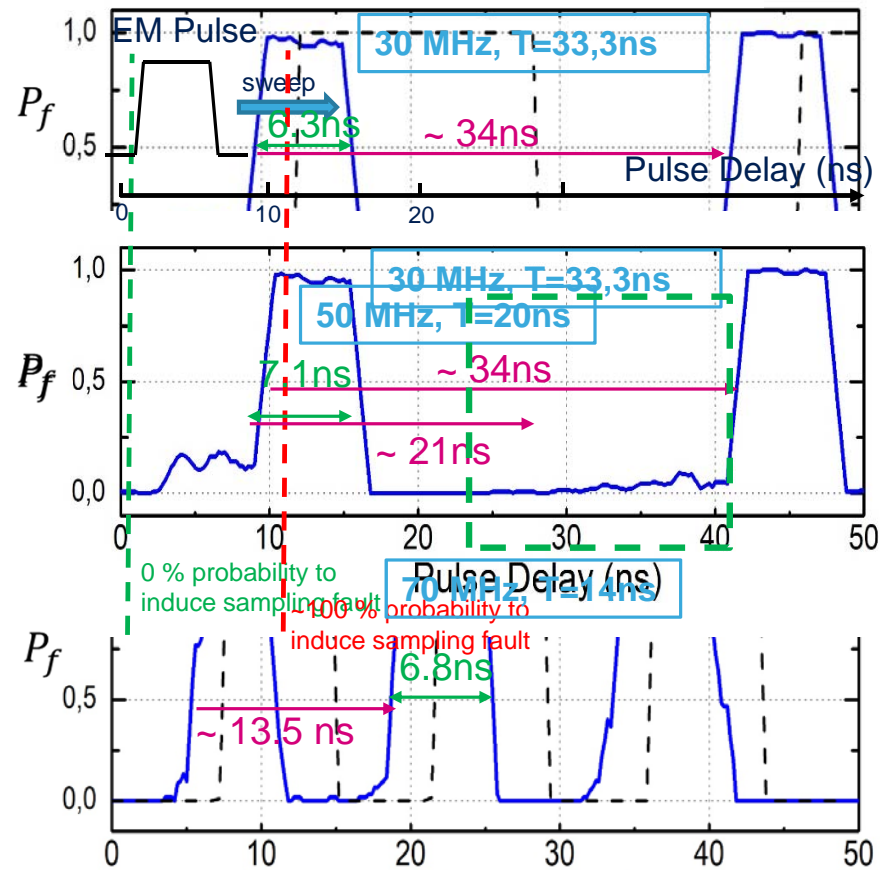
- Modelling: Impact of an EMFI on IC supply voltage
- Spice Simulation : impact of EMFI on IC operation
- Experimental Validation



EMFI experimental validation

Effect of F_{CLK} variations

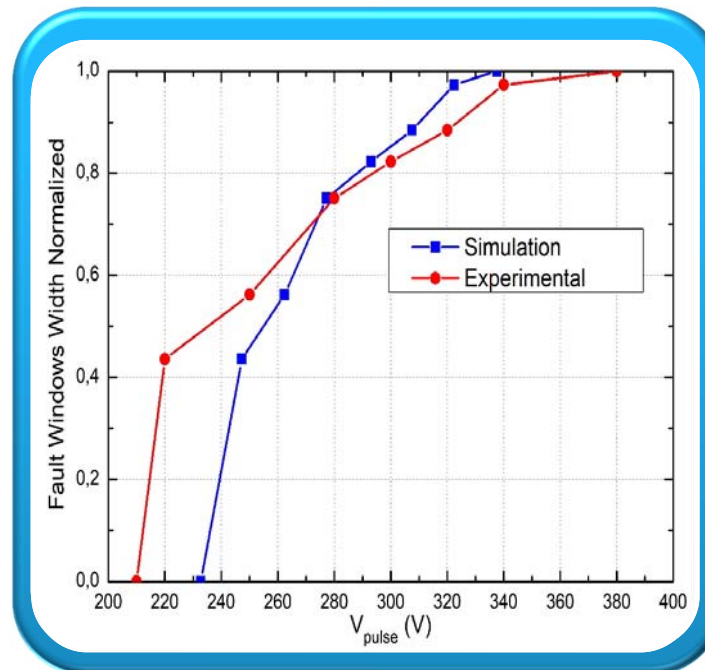
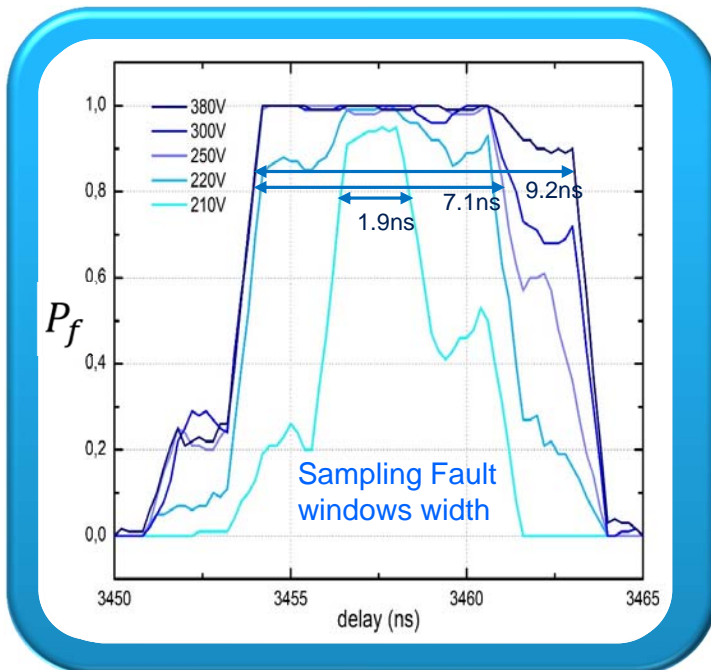
- Target : AES 128bits.
- EM pulse sweeps, for few periods, with a pulse delay step of 100ps.
- 50 EMFI shots are performed at each sweep to determine fault probability P_f ($0 < P_f < 1$).
- As expected Sampling Fault Windows appear with a period equal to that of the IC.
- Their width are independent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

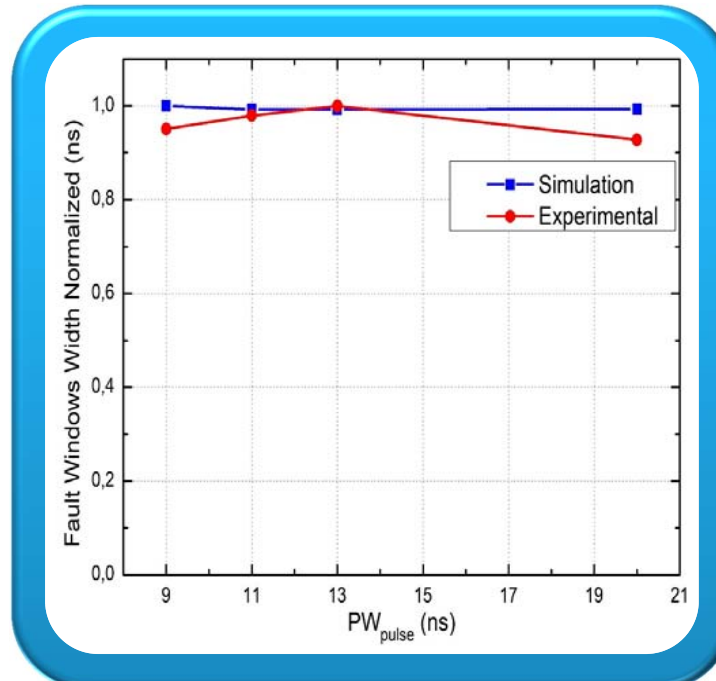
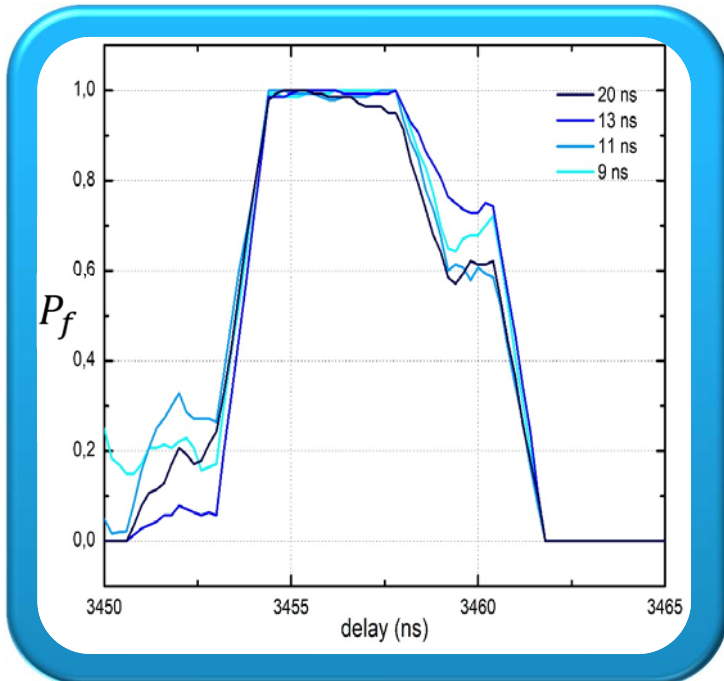


EMFI experimental validation

16

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

17

- 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**.

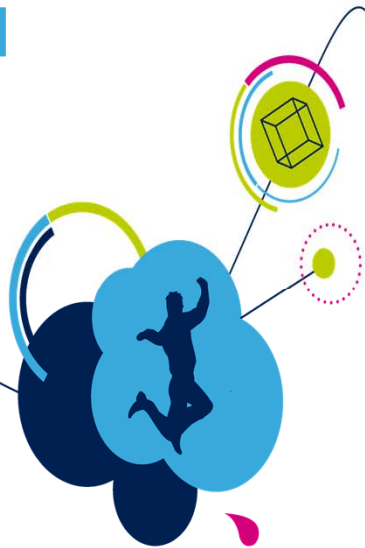


- Perspective

- 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



Modelling: Impact of an EMFI on IC

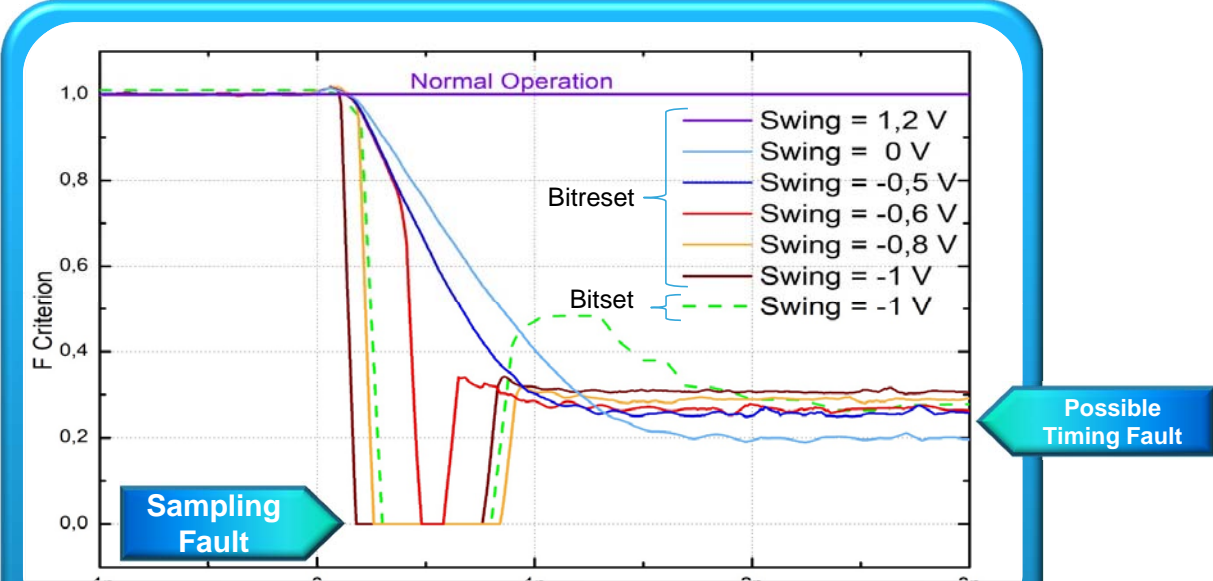
- Logic simulation: Swing amplitude impact on IC operation

Fault criterion F :

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

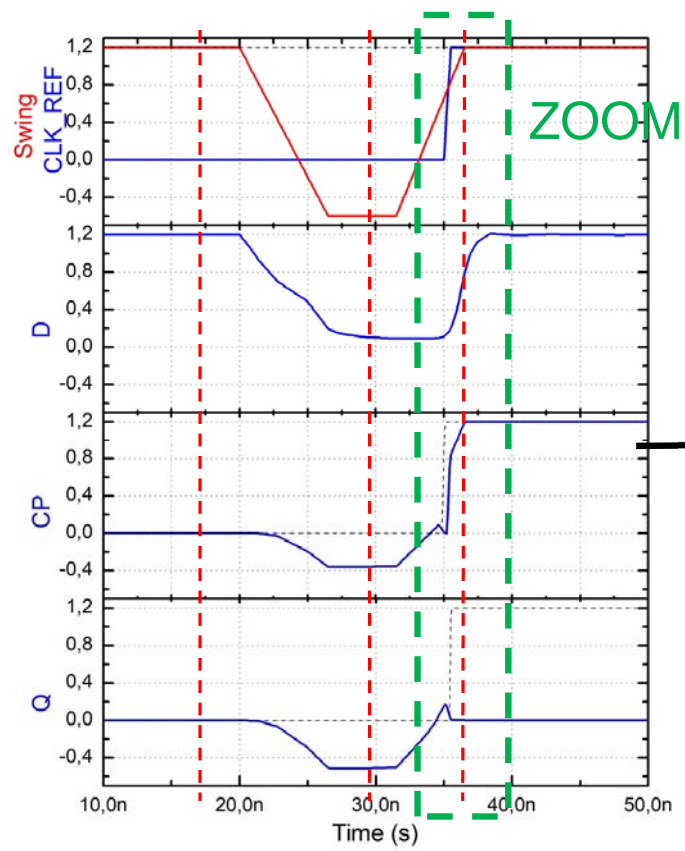
- $F = 1$ Normal Operation
- $0 < F < 1$ Delay
- $F = 0$ Sampling Fault

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

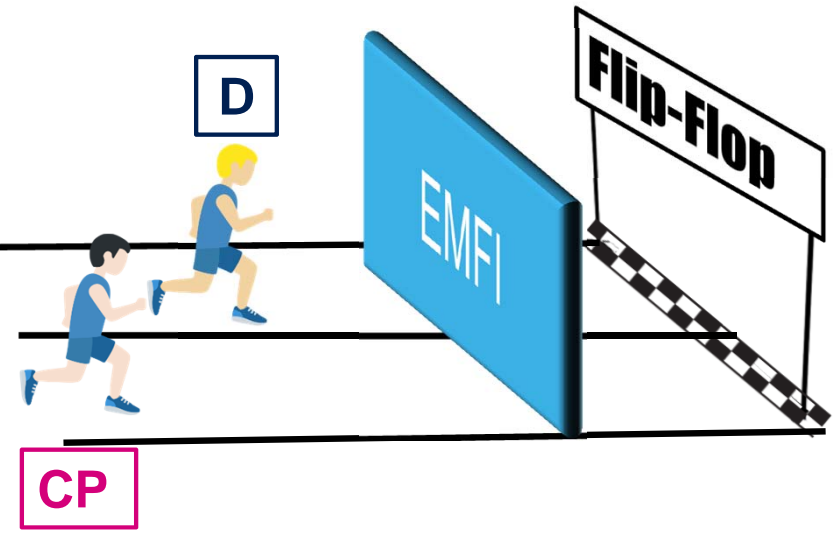


Modelling : Impact of an EMFI on IC

- Sampling Fault explanation



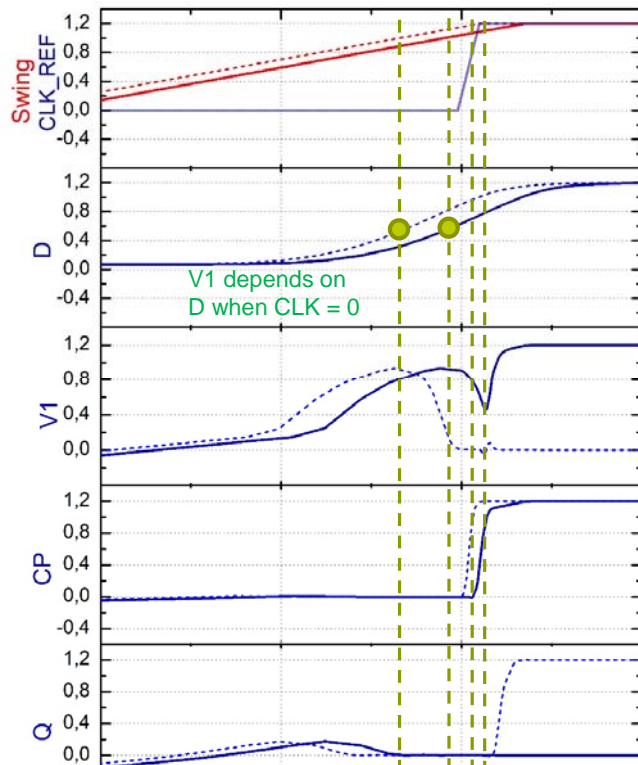
 SAMPLING FAULT



Modelling : Impact of an EMFI on IC

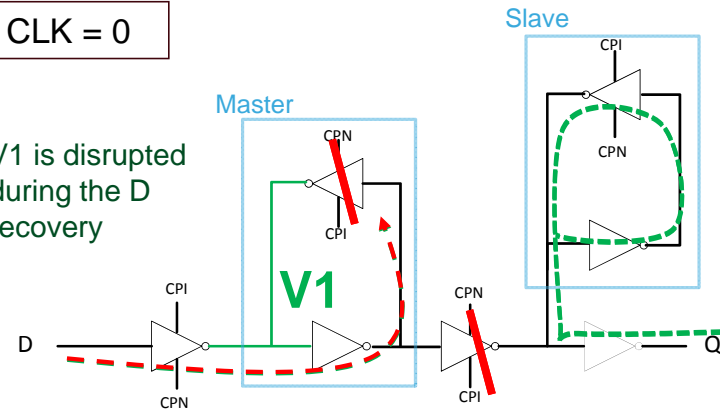
Sampling Fault explanation

..... : CK2Swing = 0 ns ; No Fault
 — : CK2Swing = 0,3 ns ; Sampling Fault



CLK = 0

V1 is disrupted during the D recovery



CLK = 1

If CLK edge occurs during V1 alteration : wrong value is sampled and stored in Master loop.

