Electromagnetic Fault Injection: How Faults Occur
Mathieu Dumont, Mathieu Lisart, Philippe Maurine

To cite this version:

HAL Id: lirmm-02328109
https://hal-lirmm.ccsd.cnrs.fr/lirmm-02328109
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.
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 :

• 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.

- Interconnect logic wires don’t form loops.

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

- **Probe IC**

- **EM probe**
Modelling: Impact of an EMFI on IC

- Impact of EMFI on supply voltage.
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

\[ \text{Swing} = V_{dd} - Gnd \]

\[ \text{Swing}_{width} \]

\[ \text{CLK-REF} \]

\[ \text{CLK} \]

\[ \text{CP} \]

\[ \text{D} \]

\[ \text{Q} \]

\[ \text{IN-REF} \]

\[ \text{OUT} \]

\[ \text{CK2Q} \]

\[ \text{CK2E} = +0.7\text{ns} \]

\[ \text{CK2E} = -0.8\text{ns} \]
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
Modelling: Impact of an EMFI on IC

• Sampling Fault explanation

Normal Operation

Q = ‘1’
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation

Q = '0'

TIMING FAULT
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation

Q = ‘0’
- 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 128 bits.
  - EM pulse sweeps, for few periods, with a pulse delay step of 100 ps.
  - 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 is independent of the frequency.
EMFI experimental validation

**Effect of $V_{\text{pulse}}$ variations**

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

![Graph 1: Sampling Fault windows width](image1)

![Graph 2: Fault Windows Width Normalized](image2)
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.
Electromagnetic Fault Injection: how faults occur?

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

[^1]: STMicroelectronics, Roussset, 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

![Graph showing the impact of swing amplitude on IC operation]
Modelling: Impact of an EMFI on IC

• Sampling Fault explanation
Modelling: Impact of an EMFI on IC

- Sampling Fault explanation

- **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.