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

- Metal wires from the power/ground networks form many loops.
- Interconnect logic wires don’t form loops.

Modelling: Impact of an EMFI on IC

- EM Induction: hypothesis?
- EM induction induces currents variation on closed loops.

- EMFI induces parasitic currents mostly in the power and ground networks.
Modelling: Impact of an EMFI on IC

• Impact of EMFI on supply voltage.

\[ m_{gnd} = k_{gnd} \sqrt{L_{probe} \times L_{gnd}} \]
\[ m_{vdd} = k_{vdd} \sqrt{L_{probe} \times L_{vdd}} \]
Modelling: Impact of an EMFI on IC

• Impact of EMFI on supply voltage.

\[ m_{vdd} = m_{gnd} \]

\[ Swing = Vdd - Gnd \]

\[ Swing = 1.2 \, V \]

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

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

\[ Swing_{width} \]

\[ \text{Time (s)} \]

\[ \text{Clk-Ref (V)} \]

\[ \text{Clk (V)} \]

\[ \text{D (V)} \]

\[ \text{Q (V)} \]

\[ \text{Out (V)} \]

\[ \text{Swing} \]

\[ \text{In-Ref (V)} \]

\[ \text{Clk-Ref (V)} \]

\[ \text{D (V)} \]

\[ \text{Q (V)} \]

\[ \text{Clk (V)} \]

\[ \text{Out (V)} \]

\[ \text{In-Ref (V)} \]

\[ \text{Clk-Ref (V)} \]
Modelling: Impact of an EMFI on IC

- Logic simulation: Swing amplitude impact on IC operation

Fault criterion $F$:

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

- $F = 1$ 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 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 $V_{\text{pulse}}$ 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 showing the effect of $V_{\text{pulse}}$ on Sampling Fault Window width](image)
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\textsuperscript{[1,2]}, Philippe MAURINE\textsuperscript{[2]}, Mathieu LISART\textsuperscript{[1]}

\textsuperscript{[1]} STMicroelectronics, Rousset, France
\textsuperscript{[2]} LIRMM, University of Montpellier, Montpellier, France
Modelling: Impact of an EMFI on IC

Logic simulation: Swing amplitude impact on IC operation

Fault criterion $F$:

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

- $F = 1$ Normal Operation
- $0 < F < 1$ Delay
- $F = 0$ Sampling Fault
Modelling: Impact of an EMFI on IC

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

Sampling Fault explanation

- **CLK = 0**
  - **Master**
  - **Slave**
  - 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.