EM fault Modelling : the sampling fault Model explained

M. Dumont, M. Lisart, P. Maurine

23 Mai 2019
- State of the Art & the Sampling fault model
- Lessons from EM Induction theory
- Modeling
  - Impact of an EMFI on the power and ground grids
  - Impact of an EMFI on IC operation
- Lessons to design robust ICs
- Lessons to design efficient EMFI platforms
- Conclusion
State of the Art
<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>EM injection disrupts the behavior of embedded memories</td>
<td>‘Eddy current for Magnetic Analysis with Active Sensor’ (Esmart 2002)</td>
</tr>
<tr>
<td>2007</td>
<td>EM injection disrupts the course of a RSA algorithm</td>
<td>‘Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results’ (Austrochip 2007)</td>
</tr>
<tr>
<td>2009</td>
<td>Harmonic EM Injection modifies the propagation delays of logical paths</td>
<td>‘Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection’ (EMC-Zurich 2009)</td>
</tr>
<tr>
<td>2011</td>
<td>Harmonic EM Injection modifies the oscillating Frequency of an internal clock generator</td>
<td>‘Local and Direct EM Injection of Power Into CMOS Integrated Circuits’ (FDTC 2011)</td>
</tr>
<tr>
<td>2012</td>
<td>Harmonic EM Injection modifies the behavior of RO based TRNG (phase locking)</td>
<td>‘Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator’ (COSADE 2012)</td>
</tr>
<tr>
<td>2012</td>
<td>EM pulse Injection produces timing faults during the course of hardware cryptographic modules</td>
<td>‘Injection of transient faults using electromagnetic pulses - Practical results on a cryptographic system’ (ePrint 2012)</td>
</tr>
<tr>
<td>2012</td>
<td>EM pulse Injection produces timing faults during the course of hardware and software ...</td>
<td>‘Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES’ (FDTC2012)</td>
</tr>
<tr>
<td>2014</td>
<td>Evaluation of a countermeasure based on the timing slack monitoring</td>
<td>‘Efficiency of a Glitch Detector against Electromagnetic Fault Injection’ (DATE 2014)</td>
</tr>
<tr>
<td>2014</td>
<td>EM injection does not induce only timing faults</td>
<td>‘Evidence of a Larger EM-Induced Fault Model’ (Cardis 2014)</td>
</tr>
</tbody>
</table>
Sampling Fault Model


i) Deduced from experiments

ii) EMFI disrupts signals at the input of DFFs:
- data D,
- Clock CK,
- Reset R,
- Set,
- Vdd and Gnd

iii) Faults occur within the sampling window of duration \((t_{\text{setup}} + t_{\text{hold}})\) around rising clock edges

iv) EM susceptibility is maximum during sampling windows

---

Diagram:

- **Required EM power**
- **EM Susceptibility**
- **High** \(V_{\text{High}}\)
- **Low** \(V_{\text{Low}}\)
- **Stability window**: \(t_s - t_{\text{setup}}\)
- **Fenêtre de calcul**: \(t_s + t_{\text{hold}}\)
- **Bitsets or bitresets**: \(\text{Bitsets or bitresets}\)
- **Sampling faults**: \(\text{Sampling faults}\)
EM Induction
EM Induction: basics and implications related to EMFI

**EM Induction: basics and implications related to EMFI**

**Interconnect wires**

**Supply and ground networks**

EM induction induces a emf on closed loops!

EMFI induces parasitic currents only in the power and ground networks
Impact of EMFI on the power and ground grids

Modeling @ Physical level
EM Induction on the power & ground grids

Coupling with the Power Grid

\[ M_V = k_V \sqrt{L_{1probe} \times L_{2V}} \]

Coupling with the Ground Grid

\[ M_G = k_G \sqrt{L_{1probe} \times L_{2G}} \]

Asymmetric EM coupling

Supply & Pad

Power & Ground Grids

Supply & Pad
EM Induction on the power & ground grids: Swing

- \( L_{probe} = 1\, \text{nH} \)
- \( L_{2V} = 300\, \text{pH} \)
- \( L_{2G} = 400\, \text{pH} \)
- \( k_V = 0.3 \)
- \( k_G = 0.9 \)
- \( R = 1\, \Omega \)
- \( C_{GV} = 1\, \text{nF} \)

\[
L_1 \cdot \text{probe} = 1\, \text{nH} \\
L_2 \cdot V = 300\, \text{pH} \\
L_2 \cdot G = 400\, \text{pH} \\
\begin{align*}
V_{\text{pulsed}} &= 400\, \text{V} \\
\text{PW} &= 6\, \text{ns}
\end{align*}
\]

Swing is greater than \( V_{dd} \) for few ns

Swing is lower than \( V_{dd} \) for few ns

Propagation and attenuation of the swing drop / bounce toward or from the supply pads
EM Induction on the power & ground grids

If $k_V = k_G$, EMFI has not effect on IC operation

But there is no reason to have symmetric EM couplings and plenty to have asymmetric ones:
- probe position
- probe geometry
- asymmetric geometries of power and ground networks
- ...
Impact of EMFI on IC operation

Modeling @ Logical level
Impact of EMFI on IC operation: simulation testbench

- all elements experience the same perturbation
- $D_{\text{ref}}$ stable (no timing fault possible)
- observation of 1 rising clock edge

$$F = \frac{CK2Q|\text{nom}}{CK2Q|\text{inj}}$$

- $F > 1$ Speed up
- $F = 1$ Normal operation
- $0 < F < 1$ Slowing down: potential timing fault @ the next clock edge (depends on $T_{\text{ck}}$)
- $F = 0$ Sampling fault
Impact of EMFI on IC operation: Amplitude Variation

Sampling fault windows

Independent of clock frequency

$\Delta S = 0V$  
$\Delta S = 1.2V$  
$\Delta S = 1.5V$  
$\Delta S = 1.6V$  
$\Delta S = 1.8V$  
$\Delta S = 2.2V$

$CK_{nom}2E$ (ns)
How EM faults occur?

(1) First edge of \( V_{\text{pulse}} \) reverses the supply voltage

(2) ‘IC is frozen’ (part of it)

(3) Second edge of \( V_{\text{pulse}} \)
   - Supply voltage recovery starts
   - IC remains ‘frozen’, \( S<Vdd-|V_T| \)
   - Even the clock edge is ‘frozen’ and thus delayed

(4) Second edge of \( V_{\text{pulse}} \)
   - IC wakes up, \( S>Vdd-|V_T| \) and according to \( CK_{\text{ref}}2E \)
     a sampling fault occurs or not

(5) IC works again in nominal conditions

Importance of having 2 opposite EM pulses
   - 1st EM pulse reverses the supply voltage
   - 2nd EM pulse controls the wake up phase

Importance of fine timing tuning EMFIs
   - required time resolution \( \sim 100\text{ps} \)
How EM faults occur?

With respect to the normal arrival time of the rising clock edge

1. **Too early EMFIs**
   - IC recovery was sufficiently long to not have a fault

2. **Successful EMFIs**
   - $D < 0.5 \text{Vdd}$
   - $\text{Not}(D) > 0.5 \text{Vdd}$ (normal operation $\text{Not}(D) = 0$)
   - $\Rightarrow$ the DFF samples a wrong value

3. **Too late EMFIs**
   - IC has not enough recovered
   - $D < 0.5 \text{Vdd}$
   - $\text{Not}(D) << 0.5 \text{Vdd}$
   - $\Rightarrow$ the DFF abnormally samples the right value
Experimental evidences

How demonstrate the soundness of the modelling ??
EMFI pollutes measurements at several meters from the DUT ...

Look for indirect evidences
- Vary EMFI settings in simulation and experimentations
- Compare simulated and experimental trends

Testchip 40nm
Hardware AES
Controllable clock
Experimental evidences

Simulations predict periodical sampling fault windows of constant width with period equal to $T_{CK}$.

Experiments confirm this prediction despite the jitter (1.5ns) of the voltage pulse generator (SFW ~5 to 6ns).
Experimental evidences

Model predicts sampling fault width is independent of PW, the width of the pulse applied to the probe.

Experiments confirms this prediction ...
Experimental evidences

Simulations predict:
- a threshold on \( V_{\text{pulse}} \) to induce fault
- an increase of the width sampling fault windows with \( V_{\text{pulse}} \)

Experiments confirms this prediction...
Conclusions

- explanation on how EM faults occur (@least on µC)
  - EMFI locally freezes and wakes up the supply voltage
  - Induction of sampling faults
  - Sampling faults occur during the supply voltage recovery

- Guidelines for the design of more robust ICs

- Perspectives :
  - enhanced EMFI platforms to target SoC
  - modeling EM faults in SoC context with current EMFI platforms