Long-Term Electromagnetic Robustness of Integrated Circuits - Application for the traceability of integrated circuits

Sonia Ben Dhia
LAAS-CNRS
France

March 14th 2013
Summary

- Context: Electromagnetic Robustness
- Experimental results (emission and immunity)
- Degradation mechanisms that affect EMC
- Using IC EMC signature for the traceability
EMC at IC level: two main concepts

Susceptibility to EM waves

- System
- Equipment
- Printed circuit boards
- Components

Emission of EM waves

- Personal entrainment
- Interferences
- Safety systems

ICs play an important role in electronic systems EMC
Electromagnetic Reliability of electronic systems

Impact of IC aging on system EMC?

During lifetime:
- harsh conditions (over voltages, T°, vibration...)
  accelerate aging and degradations

Still functional but...
EMC compliance can be affected!
→ Long term EMC compliance?
How EMC is handled at IC level?

- To comply to EMC level specifications, **ICs** must pass qualification tests defined by IEC standards => **One fresh sample of the component**

A dedicated EMR qualification methodology is mandatory to:
- estimate aging effect on EMC to ensure EMC compliance
- Adapt, optimize or tighten EMC margin

**EMC margins** to compensate variability sources and ensure EMC compliance.
Research project objectives

- Clarify the impact of aging on EMC of ICs
- Evaluate the effect of technology / design on long-term EMC
- Understand mechanisms that affect IC EMC
- Model to predict emission and susceptibility levels drifts
Experimental statements
Experimental methodology

Batch of N “fresh” samples

Accelerated aging (thermal, voltage stress)

Climatic chamber, DC stress, ESD...

Batch of N “aged” samples

EMC characterization (conducted mode preferred)

Statistical characterization of:
- Set-up repeatability
- Component dispersion
- Aging induced drift
EMC characterization: Emission spectrum

- Conducted measurement
- Radiated measurement

**Spectrum analyzer**

**TEM Cell**

**Parasitic emission (dBµV)**

- Frequency (MHz)
- Measured emission
- Below specification: EMC compatible
- Customer Specification

**CORE**

- Analog
- RF

**IC activity noise**

- IEC 61967-4
- IEC 61967-2

**Spectrum analyzer**

**TEM Cell**

**Parasitic emission (dBµV)**

- Frequency (MHz)
- Measured emission
- Below specification: EMC compatible
- Customer Specification
EMC characterization: Immunity spectrum

Oscilloscope

\[ V_{DD} \]
\[ V_{SS} \]
\[ \Delta V \]
\[ \Delta T \]

failure criteria detected

\[ P_{INC} \] (dBm)

Minimal Incident power to produce IC failure

Measured immunity

Above specification: EMC compatible

Customer specification

Conducted or radiated RFI:
- increases incident power
- increases incident frequency

\[ P_{INC} \]
Highlight aging effect on Emission

Various cases study:
- functions
- technologies
- accelerated life tests

Aging stress seems to reduce ICs emission level
• Aging can multiply by 10 the sensitivity to RF disturbances!
• Non negligible effect on failure risk linked to EMC
Aging effect on DC-DC converter (product)

- HTOL stress (150°C, 8 days)
- Conducted Emission of the output
- Regulated output measurement

Emission level of the DC-DC increases
At system level, what is the consequence of simultaneous improvement of IC emission and degradation of external decoupling?

Identification of the degraded devices:

Emission of Aged DC-DC with fresh external C & L decreases!
Degradation mechanisms that affect EMC
Impact of device aging on EMC of ICS

- Long time operation
- Harsh environment condition

Device aging

- Negative Bias Temperature Instability (NBTI)
- Hot Carrier Injection (HCI)
- Time Dependent Dielectric Breakdown (TDDB) ...

Degradation mechanism

- Drain current (Io)
- Transconductance (gm)
- Threshold voltage (Vt)
- Mobility (μ)

Device parameter drift

- Noise margin (Vt)
- Oscillation frequency (gm,Vt)
- Power Supply Rejection Ratio = f(gm, Vt)
- Jitter = f(Vt,gm)...

Circuit performances

Need for Experiments focused on device parameter drifts / circuits performances

CMOS 90nm – thick oxide

EMC failure
Degradation of MOS threshold voltage

- Dedicated test chip (90nm) with simple structures:
  NMOS, PMOS, Inverters, IO drivers, current mirror, …

Electrical stress induces:
- a decrease of mobility and
- an increase of threshold voltage

Evolution of threshold voltage of a 90nm PMOS device exposed to negative gate-source voltage

NBTI mechanism

\[ \Delta V_{th} = 4.91 \times t^{0.1548} \]

\[ \Delta V_{th} = 0.62 \times t^{0.2627} \]
Degradation of current drive (IO 90nm)

Evolution of the transient current produced by I/O switching during DC stress applied on power supply (HCI mechanism).

- Slowing down of driver transition time
- Non symmetric degradation of output current drive

Spreading of current consumption

Digital core (CMOS 90nm Freescale)

- On-chip sensor to monitor:
  - Power supply bounce on VddCore
  - Core Internal switching data
Spreading of current consumption

- Power supply voltage bounce measurements before & after aging using integrated on chip sensors

Power supply monitoring:
- Voltage bounce is reduced by 30%
- Slowing down of current impulse but still the same pseudo-oscillation frequency and damping.

Core Switching data monitoring:
- Increase of the propagation time of a data through the digital core due to internal wear-out mechanisms accelerated by electrical stress.

Origin of PI evolution: spreading of the dynamic current consumption due to internal wear-out mechanisms accelerated by electrical stress.
Summary

- Ensuring the long-term EMC for integrated circuit is essential to guarantee a high safety level of electronic applications.

- The conclusion about effect of IC aging on emission and susceptibility is complex: depending on the technology, the circuit nature, the stress…

- Modeling of IC aging allows a clarification of the origin of emission & susceptibility level changes.

- Important prospect work:
  - including IC emission & immunity drift model at system model level to evaluate the risk of non-compliance after years of use and then adapt EMC margin of components and products.
Application for the traceability of integrated circuits

Alexandre Boyer, Sonia Ben Dhia, He Huang
alexandre.boyer@laas.fr, sonia.ben.dhia@laas.fr

March 2012
Introduction – IC counterfeit

Integrated circuit counterfeit

- Problem of counterfeit devices concerns both discrete devices (passive, diodes, transistors) and integrated circuits (microcontroller, memory, RF transceiver...).
- Real issue to ensure correct performances, reliability and safety.
- In 2010 the loss due to counterfeit was about 10 billions $.

_U.S. Department of Commerce (Bureau of industry and security, Office of technology evaluation), Defense Industrial Base Assessment: Counterfeit Electronics, January 2010_
Introduction – IC counterfeit

Counterfeiting methods

- Re-marking / Re-packaging: old recycled components or use of a cheaper device
- False component: a different component or no component are packaged
- Duplicated component: same internal schematic but designed according to a different technological process

From U.S. Department of Commerce
Introduction – IC counterfeit

Integrated circuit counterfeit – Detection techniques

- Detection methods monitor any sign which highlights a counterfeit. They are based on more or less complex methods, destructive or not:
  - Visual or X-ray inspection of packaging and marking
  - Decapsulation and analysis of component architecture
  - Package material analysis (Scanning Electron Microscopy, X-ray fluorescence, Scanning Acoustic Microscopy…)
  - Pin electrical test (voltage/current, resistance, … ESD test, dependence to temperature…

J. Federico, Detecting Counterfeit Electronic Components, NJ Micro Electronic Testing

N. Petr, A. Milan, S. Petr, Counterfeit Electronic Components Detection Possibilities, Recent Researches in Automatic Control, 185-188
Introduction – IC counterfeit

**Objectives**

- Propose an alternative method for the traceability of integrated devices, based on a contactless measurement of ICs « electromagnetic signature ».

- The « electromagnetic (EM) signature » produced by IC activity depends on technology, placement & routing, package, decoupling, filtering, temperature, aging, presence of defaults…

---


Proposed detection methodology

**Principle of the evaluation**

- Measurement of the EM signature in frequency domain in conducted or radiated mode of a circuit in a nominal configuration.
- Comparison with the EM signature of a reference circuit (« reference signature »).
- Detection of internal difference and diagnosis about the nature of the tested device (counterfeit or not).
Proposed detection methodology

Reference group (N components)

EM measurement

Reference signature

Suspect device

EM measurement

EM signature of suspect device

Envelop extraction, analysis

Meas. Uncertainty
Device dispersion

Diagnosis: Counterfeit?
Proposed detection methodology

*Description of the methodology – statistical analysis*

- Two analysis criteria are proposed from the reference $E_{\text{ref}}$ and DUT $E_{\text{DUT}}$ signature.

- **Criterion 1:** z-score → the difference between DUT and reference signature, given in term of standard deviation of the reference signature

$$z(i) = \frac{E_{\text{DUT}}(i) - E_{\text{ref}}(i)}{\sigma_{\text{ref}}(i)}$$

- **Criterion 2:** Correlation $R$ or determination $R^2$ coefficient between group of harmonics $(i: j)$ → it determines if linear relation exists between both signatures.

$$R(i : j) = \frac{\text{Cov}(E_{\text{ref}}(i: j), E_{\text{DUT}}(i: j))}{\sigma_{\text{ref}}(i : j) \times \sigma_{\text{DUT}}(i : j)}$$
Case study 1 – Digital cores
Case study 2 – Microcontrollers
Case study 3 – EEPROMS
Case study 1 – Digital cores

Description of the case study

- One digital core designed in CMOS 0.25 µm, two different versions:
  - Core 0: Reference core
  - Core 1: Same core
    - + 100 pF distributed on-chip decoupling
    - + substrate isolation

- **Objective:** Can we distinguish “EM signature”
  - ref Core 0 / Core 1 (design options)
  - ref Core 0 / Aged Core 0 (effect of aging)

- 10 samples with Core0 has been submitted to HTOL:
  - 400 hours, 150°C, VDD+10%

- Conducted measurement of transient current (1 Ω method)
Case study 1 – Digital cores

Comparison between core 0 and core 1

- Visible differences in emission spectrum.
- Statistical analysis highlights the differences.
Case study 1 – Digital cores

Comparison between “Fresh” and “Aged” core 0

- Visible differences in emission spectrum.
- Statistical analysis highlights the differences.
Case study 1 – Digital cores

**Result summary**

- Clear distinction between devices with design differences
- Clear distinction between “fresh” and aged components.
- No distinction between identical components
Case study 2 – Aged microcontroller

Description of the case study

- 16 bit microcontroller from Microchip (PIC18F2480).
- same internal software, same test board
- 3 types of electromagnetic measurements:
  - Conducted mode (150 Ω probe)
  - Radiated in TEM cell
  - Near field
- 24 devices spread in 4 groups for different stress

<table>
<thead>
<tr>
<th>Group</th>
<th>Stress type</th>
<th>Component id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fresh</td>
<td>Fresh1 → Fresh12</td>
</tr>
<tr>
<td>2</td>
<td>Stress 1 (168 h, Vdd = 7.5 V, ambient T°c)</td>
<td>Aged1 → Aged4</td>
</tr>
<tr>
<td>3</td>
<td>Stress 2 (200h, Vdd = 7 V, T = 100 °c)</td>
<td>Aged5 → Aged8</td>
</tr>
<tr>
<td>4</td>
<td>Stress 3 (572h, Vdd = 7 V, T = 100 °c)</td>
<td>Aged9 → Aged12</td>
</tr>
</tbody>
</table>
Effect of aging

- Small differences in emission spectrum, the stresses do not induce a significant aging of microcontrollers.
- Statistical analysis highlights a start of emission level drift.

Case study 2 – Aged microcontroller

![Graphs showing emission level and determination coefficient over frequency](chart.png)
Case study 2 – Aged microcontroller

**Result summary**

- Near-field measurement:

- The EM signatures of non-stressed devices have a better correlation with the reference signature than the stressed devices.

- Possible distinction between “fresh” and stress devices, even for a small amount of stress.

- The 3 EM measurement types have given similar results.
Case study 3 – EEPROM memories

Description of the case study

- Comparison of the EM signature of EEPROM from 4 manufacturers.
- Similar characteristic, pin-to-pin compatible, same protocol, identical package (except marking).
- Conducted (current) or radiated (near-field or TEM cell) measurements.
- The same test board is used for all tests.

<table>
<thead>
<tr>
<th>Caractéristique</th>
<th>AT24C04B-PU</th>
<th>24LC04B-I/P</th>
<th>CAT24C04LI-G</th>
<th>M24C04-WBN6P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabricant</td>
<td>ATMEL</td>
<td>MICROCHIP</td>
<td>CATALYST SEMICONDUCTOR</td>
<td>ST-MICROELECTRONICS</td>
</tr>
<tr>
<td>Taille mémoire</td>
<td>4Kbit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration mémoire</td>
<td>512 x 8</td>
<td>2 BLK (256 x 8)</td>
<td>512 x 8</td>
<td>512 x 8</td>
</tr>
<tr>
<td>Fréquence, horloge</td>
<td></td>
<td></td>
<td>400kHz</td>
<td></td>
</tr>
<tr>
<td>Nombre de broches</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type de boîtier</td>
<td>DIP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gamme de tension d'alimentation</td>
<td>1.8V à 5.5V</td>
<td>2.5V à 5.5V</td>
<td>1.7V à 5.5V</td>
<td>2.5V à 5.5V</td>
</tr>
<tr>
<td>Température de fonctionnement</td>
<td></td>
<td></td>
<td>-40 °C à +85 °C</td>
<td></td>
</tr>
<tr>
<td>Prix pour 1 pièce</td>
<td>0.61 €</td>
<td>0.42 €</td>
<td>0.31 €</td>
<td>0.51 €</td>
</tr>
</tbody>
</table>

(FARNELL)
Case study 3 – EEPROM memories

**Comparison of EM signatures**

- Direct comparison of emission spectrum (conducted or radiated) of components from 4 different manufacturers.
- Major differences in term of fundamental frequencies and emission level, linked to technological differences.
- Similar fundamental frequency between Microchip and Catalyst devices, but large difference of amplitude.

![Graph showing conducted emission vs frequency for different manufacturers like ATMEL, Microchip, Catalyst, and ST Microelectronic.](image)
Case study 3 – EEPROM memories

Comparison between Catalyst et Microchip – application of detection methodology

- Catalyst devices are considered as the reference group.
- What is the relation between EM signature of one Microchip device to the reference signature?

The statistical analysis confirms that:
  - Large amplitude difference between EM signatures
  - No linear relation between EM signatures of both groups
Case study 3 – EEPROM memories

Comparison between Catalyst et Microchip – application of detection methodology

- Result summary for 4 devices in each group:
  - Clear distinction between devices from two different manufacturers.
  - No distinction between identical components.
Conclusion

- The EM signature of an IC depends on numerous intrinsic parameters (technology, design, placement & routing, defaults, aging…)

- The EM signature measurements constitutes a side channel for internal differences or aging detection → counterfeit detection.

- The proposed detection method is non destructive, applies on device under nominal operation and can be contactless (radiated coupling).

- The comparison through statistical analysis of EM signature with a reference device group and a suspect device provides a diagnosis about a suspect device.

- More case studies will be necessary to evaluate the robustness of the method.


