Non Intrusive Fault Detection Through Electromagnetism Analysis

Sébastien Thomas¹², Didier Regis², David Faura², Marc Gatti², Guillaume Duc¹, Jean-Luc Danger¹
¹ Institut TELECOM / TELECOM ParisTech, 46 rue Barrault, 75634 Paris Cedex, France
{bthomas,danger,duc}@telecom-paristech.fr
² THALES Avionics, 18 avenue du Marechal Juin, 92 366 Meudon-La-Foret Cedex, France
{sebastien.thomas,didier.regis,david.faura,marc-j.gatti}@fr.thalesgroup.com

Abstract

In this paper we introduce a fully non intrusive test method which is based on the Differential Electro-
Magnetic Analysis (EMA). Our objective is to demonstrate the capability of this new method to detect
stuck-at-0 faults voluntary injected in a full-custom circuit. This detection is carried out by comparing a
reference trace, called Reference Signature, with a differential trace representing the observed electro-
magnetic activity. The results show the efficiency of the proposed method. We will then introduce the possibility
offered by EM measurement to be used to detect degradation of physical parameters on equipments
where no intrusions are allowed.

1. Introduction

In the past few years, Deep Sub-Micron (DSM) technologies appeared, these technologies offered many
advantages in terms of increased performance, reduced energy consumption and cost. Unfortunately these
improvements are reached at the cost of a loss of reliability and operational lifetime [1]. Nowadays for
most of products using DSM technologies, these inconveniences are not an issue, reliability requirements
are still achieved: only 1 to 5 years operational lifetime target and up to a failure rate of 1000 FITs (Failure In
Time). But in avionic domain, reliability is a major issue because lifetime requirements are much higher (over 20
years lifetime target and a maximum failure rate of 100 FITs), in harsh operational conditions.

The impact of the failure mechanisms on the component lifetime evolves according to the techno-
logies and the DSM does not make an exception [2]. It becomes then necessary to define new monitoring
methods able to anticipate the degradation failures. As an avionic typical issue is the fly-certification, the
adequate method would be non intrusive, i.e. it would not disturb the execution of the surveyed target.

This article is organized as follows. In Section 2 we have made a state of the art regarding reliability
monitoring. Section 3 presents our methodology, then in Section 4, its implementation. Section 5 will show
experimental results and conclusion and perspectives are discussed in Section 6.

2. State of the art in reliability monitoring

Faces to this issue, some solutions were studied. In 2002, Satchidananda Mishra and al. presented the “In-
situ Sensors for Product Reliability Monitoring” [3]. The Figure 1 presents how it could be applied.

![Figure 1. “In-situ sensors for product reliability monitoring”](image)

This method allows the anticipation of the failure of a complete circuit by comparison with duplicated cells
whose lifetime has voluntary been degraded, used as “prognostic monitors”. To degrade a cell to divide its
lifetime expectancy by a factor precise enough is not easy. Moreover, the Constant Failure Rate (CFR) of the
main cell is much lower than which ones were degraded, a breakdown during their optimal periods is not
impossible and would completely falsify a statistic-based diagnosis. Finally, the use of several cells instead of the
only one can turned out problematic at the level of consumption, costs, square or interferences.

In 2007, Mridul Agarwal and al. [4] developed a programmable analogical sensor allowing the estimation
of the degradation state of 65nm circuit. In 2010, J.C. Vazquez and al. [5] took back this study and refined it to
make them less vulnerable in variations of temperature and tension. The phenomena due to the aging increase
the transition delays. By following this parameter, it is possible to estimate the aging state of the circuit. Actually, the proposed method applies a filter to the critical path of the internal logic of the circuit (Figure 2). When a transition is detected during a short predetermined temporal window, it is possible to conclude that the circuit becomes too old to continue to perform its role a long time.

![Figure 2. Aging sensor system](image)

To make this method efficient, it is necessary to be able to determine very precisely where to place this temporal window. Moreover, developing an in-situ sensor with the same technology and in the same place than the design under test would expose it to the same aging phenomena and would bias the result. Another point to be underlined is the fact that the integration of one or several sensors (to have a better follow-up, with various degrees of alert) requires a modification of the design. Finally, using this method with an already fly-certified design would involve an unacceptable increase of cost.

As current methods are not adapted for in-flight degradation detection, because they are too much expensive in term of square, consumption or cost, we proposed a new method allowing the monitoring of an embedded system without duplicating the circuit or being intrusive.

Test and cryptography have common features: they try to extract information from a device by observing it (information acquisition phase). Hence, links appears between these two domains. For instance, the power consumption is observed in Differential Power Analysis (DPA) [6] in cryptographic domain, as Direct Drain Quiescent Current (IDDQ) [7] uses it in test. Timing analysis brings enough information to be used in both domains [8]. Another way to access information is the ElectroMagnetic Analysis (EMA) [9-10]. Such analysis is potentially very interesting to test a chip as it is contactless, fully non-intrusive and can be applied when a program is running on it.

3. Proposed method

The principle of our methodology relies on the differential electromagnetic analysis of the circuit activity. The signature of every signal is represented by a specific function extracted from a database of acquired electromagnetic traces. The fault detection consists in comparing this signature, used as a reference, with the electromagnetic activity of the controlled signals observed during the life of the circuit.

As presented in Figure 3, the method is composed of two stages: A profiling and a control stage.

![Figure 3. Overview of the method](image)

3.1. Profiling stage

This stage aims at providing the reference signature of every signal which are extracted from a pool of electromagnetic traces. This stage which is performed once, offline, at the beginning of the life of the component (to be sure that the component is working properly). The first one is an acquisition phase to build a reference trace database, then a process of partitioning to classify the traces according to the activity of each signal, and finally a process of distinguishing to compare the partitions in order to create a reference signature.

3.1.1. Acquisition

The traces are acquired using an RF probe placed above the circuit. During the grabbing of the activity, a test function is run in the circuit in such a way the signals to control are active (i.e. they do not keep the same values). A perfect knowledge of the implementation and of the current state is mandatory to know whether the signals are active or not at a particular clock period. The profiling database can be common to all the signals if the function run during the acquisition involve them all.
3.1.2. Partitioning

This phase aims at partitioning the acquired traces according to a model of the activity of a targeted signal. A basic yet efficient activity model is the Hamming distance (HD) \([11]\) of two consecutive states of the signal to test. Indeed this corresponds to the main activity of a CMOS gate, as one of the transistor from the pair is saturated, thus capacitors are charged/discharged, and a short-circuit current occurs. Other more realistic models can be considered. For instance, the rising and falling transitions could be differentiated.

With the HD model, the EM traces can be partitioned into two sets: set \(T_0\) contains the traces where the signal is active (a commutation has occurred) and set \(T_E\) contains the traces where the signal is inactive (no transition has occurred). As a great majority of designs are synchronous with a common clock signal, the length of the traces is merely the clock cycle. Hence the first partition contains the cycles with an activity of the tested signal, and the second partition those without any activity. More complex partitioning could be considered. For instance, the control can be carried out on an \(n\)-bit bus. In this case, \(n+1\) partitions with the HD model are used: from 0 transitions to \(n\) transitions.

3.1.3. Distinguishing

Once the partitions are created, a function, called differentiator, is executed to efficiently discriminate the partitions. The result is a signature which expresses the signal behaviour according to the activity model. If we consider two partitions using the HD model, a simple distinguisher is the difference of mean:

\[
D = E(T_E) - E(T_0)
\]  (eq. 1)

\(D\) is the differential signature of the activity of the signal. It is obtained by computing the mean trace of each set \((E(T_E))\) is a trace obtained by averaging all the traces in set \(T_E\) and by subtracting the two mean traces. If all other signals are uncorrelated with the signal of interest, this difference of mean will mathematically remove the acquisition noise and the activity of the other signals. Hence this differential signature is itself a trace which carries information of the signal at every sample.

More complex signatures could be used. For instance a common distinguisher is the Pearson Coefficient when a group of \(n\) signals is considered:

\[
\rho = \frac{\text{Cov}(T,M)}{\sigma_T \sigma_M}
\]  (eq. 2)

Where \(M\) is is the HD model which can take \(n+1\) values, \(T\) is the observed value of the trace, \(\sigma_T\) and \(\sigma_M\) are the standard deviation of \(T\) and \(M\). The \(\rho\) coefficient expresses a correlation between 0 and 100%. Thus the signature is a trace where every time sample is a correlation of the observation with a predicted activity.

3.1.4. Control stage

This control stage is very similar to the profiling stages as the three processes of acquisition, partitioning and distinguishing are the same, except that this stage is performed during the life of the component (when we want to test whether it is working properly), and that the output is a control signature which has to be compared with the reference signature obtained during the profiling phase.

When a fault occurs on a signal, its control signature is necessarily different from the reference signature. For instance in case of stuck-at fault, the difference-of-mean distinguisher (eq.1) should reveal no differences between the two set of traces. The reliability of the comparison depends on the Signal to Noise Ratio of the acquisition and thus the number of traces. Thus the method requires a minimum number of traces and a threshold to decide whether or not a fault exists from the comparison between the control trace and the reference trace.

4. Implementation

The implementation required a FPGA in which the design under test is loaded, an EM probe, an Oscilloscope and a Computer to manage the acquisition and to analyse the results. The Figure 4 presents a schematic setup of the complete implementation.

![Figure 4. Schematic setup of the complete implementation](image)

4.1. EveSoc platform

A good knowledge of the implementation and of the current state of the targeted unit is mandatory to be able to predict if the chosen signal is supposed to be active or not at a particular clock period.

To apply the method on a FPGA, a test circuit has been specifically designed. This circuit is included in a SoC called “EveSoc” \([12]\) which allows a designer to easily plug-in a Custom Circuit and make easy the interaction between this one and the external world through a UART module. Figure 5 shows the internal description of the Soc. The CPU is a 6502 microprocessor. It is the master on the VCI bus and can drive every module. The ROM is a 2Kbytes ROM containing the boot code of the CPU. The program stored in the ROM makes the computer wait for commands on the UART and execute them. The RAM is a 32Kbytes memory used by the CPU to store any kind of data. The UART is a standard UART processing EveSoc I/O signals. Every data received by the UART is
directly sent to the CPU, as well as data received from
the CPU are directly transmitted over the serial line. The
IRQ Ctl is the interrupt controller. It centralizes every
interrupt signals sent by other modules then send a
unique interruption to the CPU, which can then process
the incoming modules interruptions. The Bus Ctl is this
module manages communications between the CPU and
other modules. It connects the appropriate module to the
VCI bus according to the address specified by the
microprocessor. The Custom Test Circuit is our
Module Under Test. Figure 6 helps to understand how it
has been developed. The other modules FIX and DES
are not used for this study and are disabled.

![EveSoC intern description](image)

**Figure 5. EveSoC intern description**

The Custom Test Circuit is mainly composed of two
independent modules:

- The first one is a standard 8-bit Ramp. The goal of
  this module is to provide signals which have
different activity levels in order to check the method
on different signals. The output of the “Ramp
Module” takes successively the values shown in
Figure 7.

- The second one is based on 3 standard LFSR
  (Linear Feedback Shift Registers) elements. The
  goal of the LFSR is to emulate the algorithmic
  computation external to the tested module. Each
  LFSR has a different size (8-9 and 10 bits) and a
different polynomial generator. The output of the
  “LFSR Module” is the result of the XOR-operation
  between the 8 last bits of each element. In order to
  obtain independent values at each execution cycle,
  these LFSRs are respectively shifted 5, 6 and 7
times during only one execution period.

![Custom Test Circuit](image)

**Figure 6. Custom Test Circuit used to apply the fault detection system**

The outputs of these two modules are XOR-ed to
obtain the global output of the test circuit called
“Result”. The implementation is perfectly known,
therefore the successive values on all the inside nodes
and on the external output are predictable at every clock
debug.

The last part of the circuit is the stuck-at faults
simulation system. Two registers (“Stuck0” and
“Stuck1”) are used to simulate a fault. As shown in
Figure 1, with this two registers and only three simple
gates, it is possible to mask the output of the ramp with a
specific value on a bit, exactly as it would happen in case
of a stuck-at fault.

![Ramp Module](image)

**Figure 7. Values on the output of the Ramp Module**
4.2. Acquisition
First step of the method is the creation of the traces database. A large number of traces is acquired using an antenna placed near the circuit under analysis. The acquisition block schema is presented in Figure 8.

**Figure 8. Acquisition block schema**

The Custom Test Circuit presented in Section 4.1 has two initialization fields:
- \( \alpha \) is the initialization of the Stuck0 and Stuck1 registers for the fault simulation. Its value is the concatenation of one byte for stuck-at-one faults and one byte for stuck-at-zero i.e. for no fault injection \( \alpha_0 = \text{0x0000} \) or for a stuck-at-zero fault on the bit 0, \( \alpha_1 = \text{0x0001} \). This initialization is fixed during an acquisition meant to fill a dedicated database.
- \( \beta \) is the initialization of the LFSR Module. This parameter is randomized before every record in order to obtain a random activity.

With this method, the way to build the reference traces or control traces databases is the same. The only changing parameter is the \( \alpha \) one: \( \alpha_0 \) for the reference traces database, an other \( \alpha \) for the control traces database, depending on the wanted fault, as explained just before.

4.3. Signature elaboration
The principle of our methodology is very close to the one developed for EMA. Recorded traces are partitioned in two groups depending on the supposed activity of the signal under test at a given cycle. As for the acquisition, and as it was presented in Figure 3, the reference signature elaboration and the control signature elaboration are performed by using the same method.

Figure 9 presents the analysis block schema for a one-bit analysis.

**Figure 9. One-bit analysis block schema**

As described in Section 3, we divide the recorded traces into two partitions:
- The first one is filled with the traces where the chosen bit is supposed to have switched at the chosen cycle (raising up or falling down).
- The second one represents the last traces, where the value of bit is supposed to stay invariant ("1 to 1" or "0 to 0").

Statistically, the two groups obtained are composed of half the number of traces recorded as the activity is uniform (1/2, 1/2). By subtracting the average of the second group by the average of the first one, we obtained a differential trace which represents the electromagnetic activity due to the chosen signal during the targeted cycle of the execution. As a matter of fact, this method highlights the relevant activity and decreases the noise (trigger perturbations, configuration period activity and other possible record perturbations).

5. Experimentation and results

5.1. Circuit configuration and first traces recording
The circuit is loaded in an ALTERA Stratix II FPGA on a SASEBO-B Board. The electromagnetic probe [13] is placed on the backside of the FPGA, close to a decoupling capacitor (Figure 10). This allows the following of the instantly consumption of a particular area. The circuit is running at a frequency of 24 MHz and the scope frequency is 5G samples per second.

The circuit is configured with random values for the initialization of the LFSR and with no stuck-at fault between the output of the ramp and the XOR with the output of the LFSR module, thus traces of the activity of the right behaviour could be recorded. Figure 8 shows the result of a single record obtained by applying the described protocol.
A start signal is raised when configuration part is over, 6 periods after the beginning of the record called trigger. The working cycle numbers are counted from 0, right after the start signal, to 17, at the end of the ramp execution. The Electromagnetic activity is disrupted by the trigger during the first cycle of recording. In the next cycles, we can see that the activity recorded is oscillating between +20mV and -20mV at a period equal to twice the clock period. The electromagnetic sensing allows the detection of the sign of the current. Hence the clock edges are clearly discriminated.

Figure 11. Global electromagnetic activity of the circuit

In this part, we present how the analysis is made following the principle presented in Section 2. Finally we check the results by applying the method on a healthy circuit.

We aim to highlight the electromagnetic activity due to only one signal at a particular clock period. We choose the bit 0 of the XOR-operation between the Ramp part and the LFSR part (cf. Figure 6). We decide to look at the second cycle of the execution, which corresponds to the activity of the bit 0 when the ramp rises up for the first time (cf. Figure 7).

In Figure 12, we can notice that the greatest activity is located at cycle 2. The signal under test has a very small footprint in the circuit. The order of magnitude is three hundred times smaller than the global electromagnetic activity records (Figure 11).

Figure 12. Electromagnetic activity of the bit 0 of “Result” at the cycle 2

We know the implementation of the circuit and the fact that the bit 0 of the rump module has a repetitive activity during 16 cycles. We could exploit this. Actually, we could repeat the analysis 16 times on the 16 successive cycles of the execution. By resynchronizing the obtained waves by left-shifting them and by adding them on the first one, we obtain a better and faster result. Figure 13 presents the result obtained on a shorter temporal window with a database of one thousand traces. It shows not only one activity peak. This is explained by the design itself. Actually, it contains 3 successive synchronous stages: a register after the XOR, the ALTERA embedded RAM, driven by the falling edge of the clock and another register after.
5.2. Uniqueness of the EM signature

To be sure that the obtained trace would really represent the electromagnetic signature of the wanted bit, the same protocol is repeated a second time with one thousands new traces without fault injection i.e. the control traces database with an acquisition using an initialization $\alpha_0=0x0000$.

The difference between the two EM signatures is illustrated in Figure 14. As we can see, this trace shows only some noise, as expected. Indeed, there should not be any relevant difference between the reference signature and the control signature of a healthy signal.

Figure 14. Differential trace between two EM signatures without fault injected

5.3. One-bit analysis

A stuck-at-0 fault is simulated by modifying the value of the “Stuck0” register initialization (cf. Section 4.2) i.e. $\alpha_1=0x0001$. The only signal directly affected is the bit 0 of the “Ramp Module” output. The XOR-operation before the Ramp and the signal “Result” propagate the fault and an analysis on this one is relevant. A new acquisition campaign is launched and the analysis is operated to get the control signature of the bit 0.

Figure 15. Control signature of the bit 0 of the signal “Result” with a stuck-at-zero fault simulated

The resulting differential trace displayed in Figure 15 is different from the correct electromagnetic signature presented in Figure 13.

Figure 16. Differential trace between the reference and the signature with a stuck-at-0 fault injected on the bit 0

As for the second correct records campaign, the difference between the reference and the faulted signal signature is shown in Figure 16. The maximum peak is 10 times greater than the noise. This clearly indicates a difference between the electromagnetic signature of a faulted signal and the correct one. Thus, the fault is detected.

5.4. Eight-bit analysis

As the method allows the following of a particular bit, it is interesting to enlarge it by applying it on the 8 bits of the same signal Result. The distinguisher used here is the Pearson Coefficient presented in Section 3.1.3 (eq. 2).

The Reference Signature obtained by the Profiling Phase is shown in Figure 17.

Figure 17. Eight-bit Reference Signature of the signal Result

As for the one-bit analysis, a Control Phase without fault injection ($\alpha_0=0x0000$) gives the same result than the Profiling phase. The Differential analysis between
this Control Signature and the Reference Signature is nothing more than some noise. The DUT is healthy.

With the same database used for the one-bit analysis when a fault was injected on the bit 0 (α_i=0x0001), the obtained Control Signature is different from the Reference signature. Figure 18 shows the result of the differential analysis. A fault on the signal is detected.

![Differential trace between the reference signature and the control signature with a stuck-at-0 fault on the bit 0.](image)

Figure 18. Differential trace between the reference signature and the control signature with a stuck-at-0 fault on the bit 0.

6. Conclusion and perspectives

In this article, we have presented a new approach to test a running circuit using its electromagnetic activity. We have demonstrated that a stuck-at-0 fault could be detected only by their impact on the electromagnetic field.

This experiment was carried out on eight bits, but could be extended to test a complete circuit using a more complex partitioning and analyzing. In this case, the number of needed traces could be increased in order to reduce the parasitic noise.

We have demonstrated that our method is able to detect a stuck-at fault. The next step would be to optimize our methodology and system measurement in order to detect degradation of physical parameters due to intrinsic failure mechanisms, for instance to evaluate aging effects. Actually, we know that these degradations impact on component parameters, like delays and consumptions [14]. Electromagnetic activity is directly linked to these parameters, thus the degradations should be detectable before the complete failure.

References