Electronic counterfeit detection based on the measurement of electromagnetic fingerprint

He Huang, Alexandre Boyer, Sonia Ben Dhia

Electronic counterfeit detection based on the measurement of electromagnetic fingerprint

H. Huang[a,b], A. Boyer[a,b], S. Ben Dhia[a,b]

[a] *CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France*
[b] *Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France*

Abstract

Counterfeit integrated circuits become a big challenge for the whole electronic industry. The use of electronic counterfeits can cause reduced performance of circuits, or failure of the whole system. New efficient approaches of counterfeit device detection are always required. Since the electromagnetic emission level of integrated devices depends on various circuit parameters like technology, manufacturing and aging, the electromagnetic emission measurement could be an approach to detect the counterfeit. In this article, the principles of the methodology are explained and two case studies are presented, where three ways of analysis of data are discussed.

Corresponding author.
he.huang@laas.fr
Tel: +33 (0)5 61 33 63 94

Electronic counterfeit detection based on the measurement of electromagnetic fingerprint

H. Huang[a,b], A. Boyer[a,b], S. Ben Dhia[a,b]

1. Introduction

An electronic counterfeit is a device whose material, performances, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer [1]. In recent years, there are a growing number of reported incidents related to counterfeit integrated circuits (ICs) [2] with the huge increase of global semiconductor market. The use of electronic counterfeits can cause reduced performance of circuits, such as instability of clock frequency, operating life decrease, a lower storage memory space, or failure of the whole system. The Alliance for Gray Market and Counterfeit Abatement estimates that nearly 10 percent of technological products sold in the global market are counterfeit, which represents about 100 billion dollar loss for the electronics companies every year [3].

Three major techniques exist to produce counterfeit circuits: re-marking components as a higher grade and more expensive chip, re-packaging old devices up to non-qualified components, and duplicating counterfeits through inferior parts or materials [4]. The struggle against this problem relies in a better management of the supply chain and the market [5], the development of advanced authentication methods (e.g. watermarking [6]) and serialization technologies (e.g. 2-D bar code [4]). Besides, industry always looks for non-destructive, rapid and cheap method to detect the electric counterfeit. At present, a large number of detection techniques exist and are already used by industry and detection laboratories: visual inspection of the appearance of component (texture, mold mark, pitch form…) in order to detect raw counterfeit devices, decapsulation to verify the die layout, material analysis methods, like fluorescent X-ray or C-mode scanning acoustic microscope for package analysis, and different levels of electrical testing (V/I characteristics, ESD test, operation life test…) [7].

Although there are lots of methods to detect counterfeit devices, most of them are destructive, and none can cover 100% of counterfeit types. Moreover, the detection methods have to evolve because the counterfeiting techniques may adapt to them. Furthermore, we need a large number of detection techniques to deal with the large number of counterfeiting possibilities.

The electromagnetic emission (EME), also called "electromagnetic fingerprint" (EMF) in this article, is a contactless side channel related to the IC transient activity. It depends on numerous circuit parameters such as technology, placement and routing, embedded code, internal filtering, packaging, temperature, aging [8] [9]... Any modification of one of these parameters may lead to a significant change of the electromagnetic emission. This principle emerges as a new idea to detect counterfeit ICs [10] [11]. However, few demonstrations of the method application have been shown in the literature. This paper aims at presenting a study about the feasibility to distinguish authentic and different devices through EME measurements.

2. Description of the detection methodology

2.1. Principles of the method

The detection test consists in comparing the EM fingerprint measured from a suspect test device and a reference fingerprint obtained from good devices, because a counterfeit component or circuit normally exhibits a different or degraded transient operation compared to the nominal behavior of the original device. The electromagnetic (EM) fingerprint is a parasitic electromagnetic signal produced by the IC internal activity, measured in conducted and/or radiated mode, in given experimental conditions.

The device under test (DUT) could be a small active component, a complicated electronic system or whatever electronic active device which can generate electromagnetic emission. During the measurement, the

devices must be powered and set in a given configuration which induces at least a transient current consumption. If all the measurements are done in similar conditions, any significant difference of the electromagnetic emission will indicate a difference between the devices. However, only one known good device is not enough to extract a reference fingerprint due to measurement errors and process dispersion. It is better that the reference fingerprint could include statistical information about the EM fingerprint of authentic devices. It can be extracted from the measurements of a sufficiently large number of known good devices. Fig. 1 details the different steps of the proposed method.

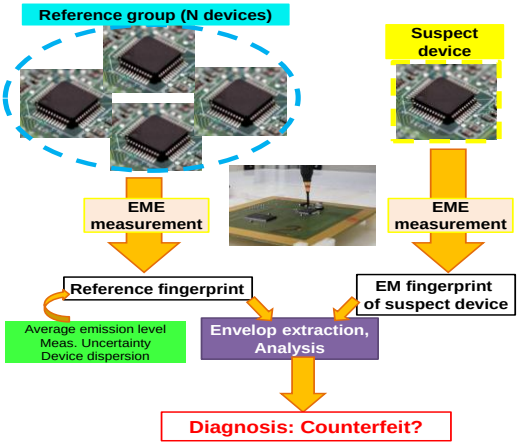


Fig. 1. Description of the detection methodology

2.2. Electromagnetic measurements

The electromagnetic noise produced by the circuit activity can be coupled according to three modes: conducted mode, far-field radiated mode or near-field mode. The two last modes ensure contactless measurement. In addition, the near-field mode allows localization of the source of electromagnetic [12]. Proven methods for characterizing electromagnetic emissions from ICs between 150 KHz to 1 GHz are proposed by IEC 61967 standard [13], which is extensively used by IC manufacturers for electromagnetic compatibility qualification. The concepts, requirements and advices given by this standard can be followed. Besides, all the EME measurements do not damage the device under test, and the type of measurement could be chosen according to the device and the requirement of detecting application. No matter which measurement method is chosen, the same measurement conditions for the different devices should be guaranteed.

The measurement can be done in the time domain with oscilloscopes or frequency domain with narrow band receivers such as spectrum analyzer. Normally the measurement in the frequency domain is more sensitive due to its lower noise floor. Moreover, as transient current induced by circuit activity has an impulse nature, its spectrum covers a large frequency range. In following case studies, more differences can be detected in frequency domain than in time domain.

2.3. Analysis method of measured data

The analysis of the emission spectrum measured in the frequency domain is discussed in this paper. At frequency k the amplitude measured are stored in a vector E(k), the frequency range includes a finite number of frequencies M, so k = [1: M]. If the circuit activity is periodic, the amplitude can be extracted at harmonic frequencies. The reference fingerprint is noted $E_{REF}(k)$ and the fingerprint of the suspect device under test is noted $E_{DUT}(k)$. The reference fingerprint $E_{REF}(k)$ contains the average emission level measured at frequency k over the N reference samples. Only the points whose amplitude is larger than the noise floor are taken into account to minimize measurement errors. According to the work of [14], the distribution of emission level around the average level is supposed to be normal. The dispersion around the average level of $E_{REF}(k)$ in frequency k, which is linked to measurement uncertainties and process differences, is given in term of standard deviation $\sigma_{REF}(k)$. The standard deviation can be obtained from the measurements of N reference samples of certain times (e.g. 5 times per reference sample).

Three statistical criteria are selected in this paper for the analysis of the EM fingerprint between the reference and suspect devices. However, like all the other statistical methodologies, these three criteria that we choose cannot represent all the relationships between the DUT and the reference, but as the preliminary analysis, they are effectual to identify the differences related to counterfeits.

2.3.1. Z-score

The first criterion is called z-score (also called standard score) (1). For the frequency k, this estimator gives the amplitude difference between the suspect device $E_{DUT}(k)$ and reference fingerprints $E_{REF}(k)$, divided by the standard deviation of the reference fingerprint $\sigma_{REF}(k)$. For each frequency, this figure provides an indication about the probability of

differences between the suspect device and reference emission levels, so a z-core in frequency k close to 0 means that the emission levels of the two devices are similar at this frequency.

To simplify the conclusion, a global Z-score is defined as the mean value of all the frequency range (2). According to the three-sigma rule (68–95–99.7 rule), in a normal distribution nearly all values (about 99.73%) lie within three standard deviations of the mean. So in the detecting test, if Z is more than 2, there are only 5% of the probability that the component is not counterfeit, and if Z is more than 3, we can almost conclude that the test chip is a counterfeit.

$$z(k) = \frac{\left| E_{DUT}(k) - E_{REF}(k) \right|}{\sigma_{REF}(k)} \quad (1)$$

$$\overline{Z} = \frac{\sum z(k)}{M}, k \in [1, M] \quad (2)$$

2.3.2. Determination coefficient R²

The second alternative criterion is the determination coefficient R^2 (3). Where, C_{ov} is the covariance of the reference vector and the DUT vector, and σ is the standard deviation of these two vectors respectively. It is computed over a group of frequencies (from frequency i to frequency j).

$$R^2(i:j) = \left[\frac{Cov\left(E_{REF}(i:j), E_{DUT}(i:j)\right)}{\sigma_{E_{REF}(i:j)} \cdot \sigma_{E_{REF}(i:j)}} \right]^2 \quad (3)$$

This coefficient determines whether a linear relation exists between a suspect device and reference device fingerprints, it relates to goodness of fit. The interval of the value of R^2 is [0, 1], a determination coefficient close to 1 indicates a strong linear relation between suspect device and reference fingerprints, and vice versa. Unlike the Z-score, the determination coefficient provides an insight of the global trend but not each single frequency.

2.3.3. Feature selective validation FSV

The Feature Selective Validation (FSV) method is the method chosen in a recent IEEE standard for validation of simulation results (IEEE standard 1597.1) [15]. The FSV theory was proposed to describe the quality of electromagnetic simulation results compared to measurement results. However, the basic concept of this method is the comparison of goodness of the fit between two sets of data.

FSV proposes three measures: Amplitude Difference Measure (ADM), which compares the amplitudes and trends information of the two data sets; Feature Difference Measure (FDM), which compares the rapidly changing features; and Global Difference Measure (GDM) which is a combination of ADM and FDM. One original point of this method is that the difference measure values (ADM, FDM and GDM) are divided into six categories as presented in Table 1. These natural language descriptions of fitting level make the results more intelligible. More details of the algorithm for these measures could be found in the standard and the website of the FSV project [15]. A free copy of the FSV to calculate difference measure values can also be downloaded from this site.

Table 1
FSV interpretation scale

FSV value (quantitative)	**FSV interpretation (qualitative)**
Less than 0.1	Excellent
Between 0.1 and 0.2	Very good
Between 0.2 and 0.4	Good
Between 0.4 and 0.8	Fair
Between 0.8 and 1.6	Poor
Greater than 1.6	Very poor

3. Case study I: Distinction between components with technological differences

As buying certified counterfeit circuits is uncertain, the proposed study is done on "simulated counterfeit devices", i.e. with known small technological differences or stressed devices representing two major types of counterfeits in the electronic product market.

The DUT is a mixed signal test chip which has been designed in CMOS 0.25 µm process. The test chip includes two digital cores: Core0 and Core1. These two digital cores have the same construction except for Core1 an additional on-chip distributed capacitor of 100 pF which have almost no influence to normal operation.

Core0 is selected as the reference. The reference electromagnetic fingerprint is obtained from a group of 7 authentic circuits (from Core0_1 to Core0_7). Nine other components are set to be the suspect components under test: one component called Auth0 which is designed with the same technology of Core0 and eight components Core1 (from Core1-1 to Core1-8) which have small technological differences with references.

Conducted emission tests have been chosen because more differences could be observed than the

radiated measurements in this case study. The transient current that returns to the ground is measured by the use of a 1 Ω resistor probe detailed in the standard 61967-4 [9]. The fundamental frequency seen in the emission spectrum is 4 MHz, so an envelope could be obtained with this frequency and the harmonic frequencies. As shown in the Fig. 2, the reference fingerprint with the EM emission of one Core1 and Auth0 devices are compared. The general shapes of the three spectra are similar and, in spite of small differences between these different devices, it is difficult to conclude about the differences between the three samples. Statistical analysis can provide a more precise conclusion by revealing differences or correlations between EM fingerprints.

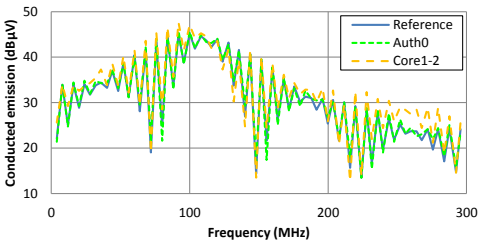


Fig. 2. EMR of reference Core0, Auth0 and Core1-2

3.1. Z-score analysis

Fig. 3 compares the z-score of Core1-2 and Auth0. The result reveals that a huge difference exists between the fingerprint of Core1-2 and reference over all the considered frequency range. The highest z-score reaches more than 10 times the standard deviation of the reference fingerprint SREF, and the average difference is about 4 times SREF, so the probability for this Core1 device to have a similar EM fingerprint as the reference devices is very small. In contrast, the average difference between Auth0 fingerprint and the reference fingerprint is about one standard deviation. It is unlikely that Auth0 and reference devices have different EM fingerprints.

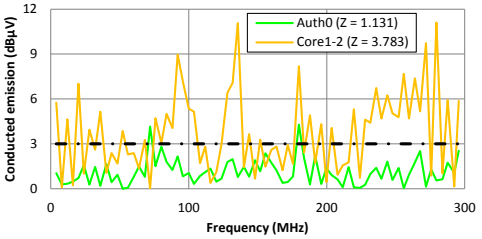


Fig. 3. Z-score of Auth0 and Core1-2

Analyses on the other devices provide similar results, as shown in Fig. 4. Since the average z-scores measured with each Core1 device are all greater than 3, a conclusion about their authenticity could be derived.

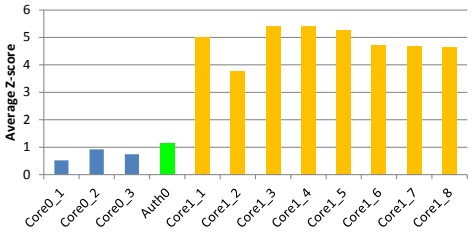


Fig. 4. Average Z-score of reference Core0, Auth0 and Core1

3.2. Determination coefficient R² analysis

Fig. 5 presents a scatter plot between the emission levels of the reference and two tested devices (Auth0 and Core1-5). A clear linear relation exists between Auth0 and reference group emission levels, and this is underlined by a determination coefficient very close to 1. The small differences are due to measurement errors and process dispersion. In contrast, the linear relation between Core1 and reference is not so obvious, as demonstrated by the lower value of R² (Fig. 6).

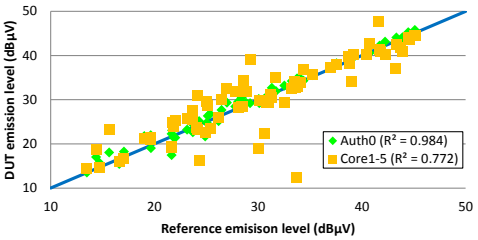


Fig. 5. Scatterplot of Auth0 and Core1-5 emission levels vs. reference emission level

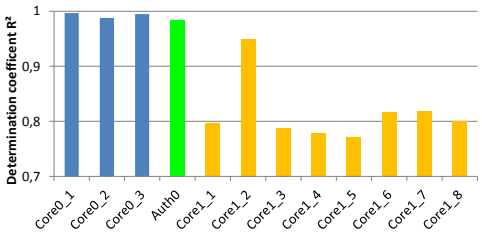
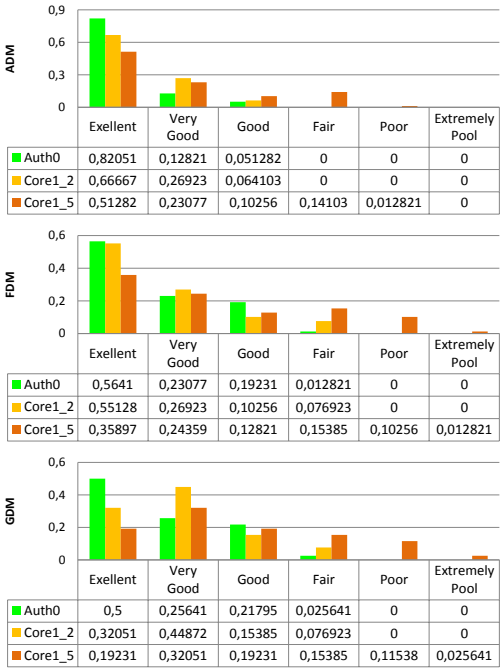


Fig. 6. Determination coefficient of reference Core0, Auth0 and Core1 devices

3.3. FSV analysis

The FSV analysis is based on the FSV tool download form the site of the FSV project [16]. Three major measures (ADM, FDM and GDM) are applied by FSV. The results of three DUTs (Auth0, Core1-2 and Core1-5) are depicted in Fig. 7. The graph using

probability density function histograms of the six "Levels" gives a better understanding of how close the EMFs of the tested DUT and reference device is. In all the results, Auth0 shows a better agreement level than the two other devices in the level 'Excellent'. The ADM graph shows us a bigger difference between the authentic device and the devices with small technology differences, which means that in this case study the comparison based on the amplitude analysis could show us more details related to technological differences. The FSV analysis method is also hard to set an exact value to judge directly whether the test device is a counterfeit or not, as the same problem as the determination coefficient method has.



	Exellent	Very Good	Good	Fair	Poor	Extremely Pool
Auth0	0,82051	0,12821	0,051282	0	0	0
Core1_2	0,66667	0,26923	0,064103	0	0	0
Core1_5	0,51282	0,23077	0,10256	0,14103	0,012821	0

	Exellent	Very Good	Good	Fair	Poor	Extremely Pool
Auth0	0,5641	0,23077	0,19231	0,012821	0	0
Core1_2	0,55128	0,26923	0,10256	0,076923	0	0
Core1_5	0,35897	0,24359	0,12821	0,15385	0,10256	0,012821

	Exellent	Very Good	Good	Fair	Poor	Extremely Pool
Auth0	0,5	0,25641	0,21795	0,025641	0	0
Core1_2	0,32051	0,44872	0,15385	0,076923	0	0
Core1_5	0,19231	0,32051	0,19231	0,15385	0,11538	0,025641

Fig. 7. ADM, FDM and GDM of test samples

4. Case study II: Distinction between authentic and stressed components

One principle source of counterfeit devices is related to the reuse of non-qualified and recycled old devices. This part aims at demonstrating the comparison of the EM fingerprints of a group of reference components with a same but aged reference.

In this case study, new Core2 components are used (7 DUTs: Core2-1 to Core2-7), they have been submitted to stress conditions according to High Temperature Operating Life (HTOL) test [17]. During 408 hours, the samples have been powered under high temperature conditions (150°c). Before and after the accelerated-life test, same conducted electromagnetic emission test of the previous case study is employed. The reference group is constituted by 7 fresh components. After aging the components are still functional and a little variation of the emission level is observed, as shown in Fig. 8.

The result of this study reveals that the aging of circuit can induce detectable changes in the EM fingerprint.

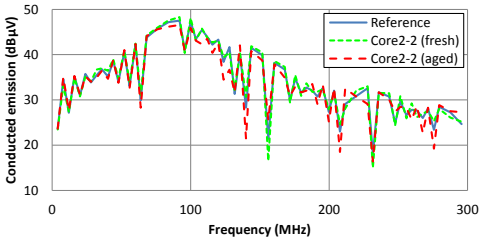


Fig. 8. Comparison between reference (Core2), Core2-2 (fresh) and Core2-2 (aged) fingerprints

The average z-score in Fig. 9 shows that the average emission level differences between aged components and reference group are at least twice larger than the fresh samples, so the likeness of these aged components with reference devices are highly doubtful, especially several components whose average z-score larger than 3 after aging (#2 and #5) which may be identified as counterfeit.

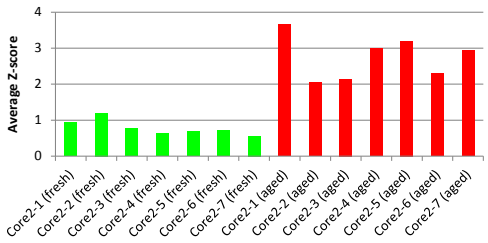


Fig. 9. Average Z-score of fresh and aged Core2 devices

Moreover, the linearity of the relation between the DUT fingerprint and reference tends to degrade after the accelerated aging, as shown by the results of R^2 in Fig. 10.

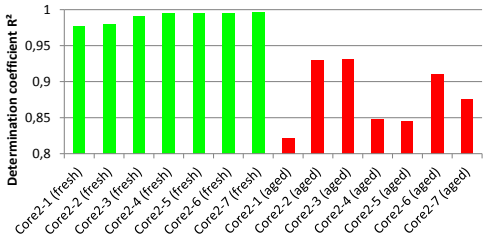


Fig. 10. Determination coefficient of fresh and aged Core2 devices

Besides, the fresh components show a much better fitting level than the aged devices by the FSV analysis in Fig. 11. The result of this study reveals that the aging of circuit can induce detectable changes in the EM fingerprint.

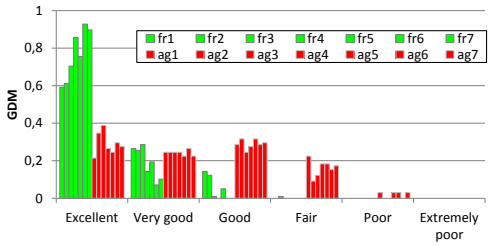


Fig. 11. ADM of FSV fresh and aged Core2 devices

As discussed in the previous case study, only the z-score method could propose a clear demarcation line for the counterfeit detection. Though the other two methods are also very efficient to reveal the difference related to the source of counterfeit, the distinction between original and modified components is less clear than with the z-score measure.

5. Conclusion

This paper has proposed a preliminary demonstration of an alternative method dedicated to the analysis of traceability of integrated devices, based on a measurement of the « electromagnetic fingerprint » of a circuit. Three statistical methods have been tested and compared (z-score, determination coefficient and FSV). The presented results have shown that significant changes in the electromagnetic fingerprint of a circuit can be measured when some modifications of the original design are provided or when it is submitted to an accelerated-aging test. These two case studies represent two typical kinds of counterfeit: re-marking components and re-packaging old devices. Conducted measurements have been led to extract the electromagnetic fingerprint in the case studies of this paper, and several parallel tests applied in other circuits with radiated or near-field measurement methods have also provided positive results.

As an alternative method, we cannot assure that it works for all counterfeit possibilities. Besides, with this method it's hard to single out the counterfeit source in a system, and this method cannot be used to identify the counterfeit type, that means even a significant difference is observed between the reference and the DUT, it's hard to define this difference is related to the aging or a different design. However, the objective of this study is to demonstrate that the EME differences related to counterfeit possibilities are significant and measurable, so EME measurement could be an alternative to detect counterfeit devices.

In future studies, more works are required to evaluate the robustness of the method, including the approaches for EME data analysis. Besides, the precision and limitation of the method, and also the comparison of the advantages and drawbacks with other detection techniques should be discussed. Also, improvements have to be brought to increase the speed of measurements (parallel tests, rapid analyzor, compromise between measurement accuracy, noise floor and measurement time).

References

[1] H. Livingston, "Avoiding Counterfeit Electronic Components", IEEE Transactions on Components and Packaging Technologies, Vol. 30, No. 1, pp. 187-189, March 2007.

[2] U.S. Department of Commerce (Bureau of industry and security, Office of technology evaluation), "Defense Industrial Base Assessment: Counterfeit Electronics", January 2010.

[3] M. Pecht, S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising of counterfeit electronics", IEEE Spectrum, Vol.34, No. 5, pp. 37-46, May 2006.

[4] S. Bastia, "Next Generation Technologies to Combat Counterfeiting of electronic components", IEEE Transactions on Components and Packaging Technologies, Vol. 25, No. 1, pp. 175-176, Mar 2002

[5] F.E. McFadden, R. D. Arnold, "Supply Chain Risk Mitigation for IT Electronics", IEEE International Conference on Technologies for Homeland Security, 2010.

[6] F. Koushanfar and al., "Can EDA combat the rise of electronic counterfeiting?", 49th Design Automation Conference, June 3-7 2012.

[7] H. W. Hewett, "Methods used in the detection of counterfeit electronic components", SMTA International Conference, October 2010.

[8] J.P. Muccioli et al., "Characterization of the RF Emissions from a Family of Microprocessors Using a 1 GHz TEM Cell", IEEE Symposium on EMC, 1998.

[9] S. Ben Dhia, A. Boyer, B. Li, A. C. Noye, "Characterization of the Electromagnetic Modelling drifts of a nanoscale IC after Accelerated Life Tests", Electronic Letters, Vol. 46, No. 4, pp. 278-279, 18th February 2010.

[10] K. Gross, R.C. Dhankula, A.J. Lewis, "Detecting counterfeit electronic components using EMI telemetric fingerprints", US Patent Application US 2009/009830 A1, 2009.

[11] W.J. Keller, S.D. Freeman, "System and method for physically detecting counterfeit electronics", US Patent Application, 20120226463, September 2012.

[12] K. Slattery, W. Cui, "Measuring the electric and magnetic near fields in VLSI devices", IEEE Symposium on EMC, August 1999.

[13] IEC 61967, "Integrated circuits - Measurement of electromagnetic emissions, 150 kHz to 1 GHz", IEC, Geneva, Switzerland, 2006.

[14] B. Li, Study of aging effects on electromagnetic compatibility of integrated circuits. Thesis, University of Toulouse, 2011.

[15] IEEE, "Standard for validation of computational electromagnetics computer modeling and simulation," IEEE Std 1597.1, Piscataway, NJ, 2009.

[16] http://www.cse.dmu.ac.uk/~apd/FSV%20web/index.html#_This_website, The Feature Selective Validation (FSV) Project

[17] AEC-Q100-Rev-FAutomotive Electronics Council, Component Technical Committee, Stress test qualification for integrated circuits, 2003.