Qualification and Testing Process to Implement Anti-Counterfeiting Technologies into IC Packages

Nathalie Kae-Nune / Stephanie Pesseguier
STMicroelectronics, Corporate Security Department

Abstract— **Counterfeiting is no longer limited to just fashion or luxury goods, the phenomenon has now reached electronics components which failure represents a high risk to the safety and security of human communities. One way for the semiconductor (SC) industry to fight against counterfeiting of electronic parts is to add technological innovation at the component level itself. The target is to enable the product authentication in a fast and reliable way. Because semiconductor manufacturing is a complex and delicate operation producing highly complex products which are sensitive to many environmental factors, any introduction of changes in its production – which the implementation of anti-counterfeiting (A/C) technologies must also comply to – must undergo thorough testing and qualification steps. This is mandatory to control the compliancy to the strict delivery requirements, quality and reliability level the industry has established, in line with the product performance specifications. This paper aims to explain the comprehensive requirements specification developed by members of semiconductor and related industries in Europe, to add authentication technologies solutions into IC packages. It also describes the qualification processes and testing plans to implement the most adequate and effective anti-counterfeiting technology (A/T). One of the main challenges in this A/C task is to make sure that the added A/C feature in electronic components does not create any additional reliability or failure issue, nor introduce additional risks that will benefit counterfeiters.**

Keywords— Anti-counterfeiting technologies, authentication, remarking, re-packaging, component counterfeiting, failure analysis, failure prevention, reliability testing

I. INTRODUCTION

Counterfeiting and product piracy have become societal problems of increasingly high importance. Selling counterfeit products as originals provides colossal profits to unscrupulous vendors. Legitimate manufacturers are suffering from a negative financial and business impact (lost revenue, cost related to customer returns and legal issues, damaged reputations and compromised credibility).

For the SC industry, around 1% of the SC sales is estimated to be counterfeited units, translating into a business volume in the order of 3 billion US$ (2011 S/C revenue worldwide), as per the Anti-counterfeiting Taskforce (ACTF) of the European Semiconductor Industry Association (ESIA).

Not only do counterfeit components impose tremendous loss of sales to SC manufacturers, distributors, electronics equipment manufacturers and end users, their poor performance and reliability is directly threatening the public health and safety, as well as the national security when it comes to risks posed to military systems. The US government is prompted to take a closer look into the military supply chain as more and more counterfeit parts are making their way into the US defense supply chain [1]. This results into the requirement given to the US Department of Defense (DOD) to address the detection and avoidance of counterfeit electronic parts, as specified in the National Defense Authorization Act for Fiscal 2012 (NDAA), Section 818.

The market research firm IHS predicts counterfeiting of semiconductors to become a more prevalent problem in the future especially when the SC industry enters a phase of accelerating growth. On the other hand, counterfeiters have gotten more sophisticated. They watch the market and adapt themselves to profit and shift the weaknesses in their favor. Over the past years, it became harder to distinguish the original product from its counterfeit. Counterfeiters are now more ingenious to copy and replicate electronic components, with more correctly marked codes. They are more skilled to rework electronic components, increasing remarking cases. This requires more physical decapsulation or lab assisted analysis to detect counterfeit electronic parts that entered the market.

In response to this growing trend of hardly detectable counterfeit electronic parts, there is a need for industry members, industry associations, government agencies and all tiers of the supply chain to work together in order to establish a wide range of measures to support the identification and seizure of counterfeits.

Combating counterfeit chips starts by controlling the purchasing and supply chain with trusted suppliers, and by tightening the procurement procedures, as envisioned by the US NDAA. Then, inserting A/T at the component level to allow a faster and more reliable product authentication can be an additional tool to combat counterfeit. However, implementing authentication technology itself will not aid in stopping counterfeits from entering the SC supply chain.

Moreover, adding authentication technologies into the production of components can be extremely costly and also risky as it can create additional reliability or failure issue, as well as generate new weaknesses and vulnerabilities that counterfeiters can profit and turn to their advantages. Proceeding without rigorous qualification testing will actually do more harm than good.

The SC industry cannot blindly accept changes in its production without a thorough verification process to check that putting authentication technologies in ICs will not affect the product functionality, quality and reliability, and that it can

978-3-9815370-0-0/DATE13/©2013 EDAA

be applicable to the SC industrial and safety environment, without losing control on the existing production. Furthermore, the technology must demonstrate its efficiency, robustness and resistance against attacks, all in full compliancy with the performance criteria and requirements stated in the international ISO standard [2].

Below chapters describe the complete qualification and testing methodology built and launched by members of SC and related industries in Europe to assess and evaluate the implementation onto IC packages of short listed numbers of A/C technologies from a prospected range of some twenty technologies analyzed and mapped as possibly satisfactory for the SC industry. The content of the qualification and testing plan was elaborated to map the below described A/C requirements specifications, geared to the semiconductor constraints. The whole plan has been deployed and is running now for more than two years, providing valuable results to the SC industry.

II. PERFORMANCE REQUIREMENTS FOR AUTHENTICATION TECHNOLOGIES IN THE FIELD OF ELECTRONIC COMPONENTS

In the field of electronic components, the top priority of implementing authentication technology is set at the **Semiconductor Packaging level**. Such decision is supported by the following reasons:

- Today electronic chips counterfeiting is often related to tampering with the packaging. Common practices of counterfeiters are re-marking of low-value legitimate chip into a higher grade and therefore more expensive chip, refurbishment of obsolete parts, or re-packaging of used products. There is a need to detect such infringement;
- In the standard practice of chip counterfeit (fake chip in a non legitimate packaging), there is a need to distinguish the original packaging from its counterfeit;
- Higher systems integration technologies using multi-chip packaging, through-silicon via technologies or package-stacking approaches are growing in importance. This leads to higher value, sophisticated and highly advanced packaged device, playing a more critical operational role within the safety/security related application.

As a matter of fact, the authentication technologies used to determine the electronic component authenticity must cover the detection of the following counterfeiting scenarios:

- Unauthorized modifications to the packaging surfaces
- Completely counterfeited packaging

A. Objectives

This chapter aims to provide a comprehensive specification of requirements on the performance criteria against which any authentication solution will be measured and assessed.

Authentication solution should not affect the functionality and the integrity of the product. At the same time, it must demonstrate the potential to integrate in existing manufacturing processes and maintain high-quality volume production, respecting the semiconductor cost, safety and environmental constraints.

Prior to deployment, any A/T must be tested and qualified to SC industry-identified criteria for both effectiveness and efficiency.

The criteria are broken down into the six areas described in the following chapters.

B. Effectiveness – Related to Component Specifications

These requirements are related to device specifications and its intended application.

The technology must:

- Not alter device performance
- Work according to specifications under all device operating conditions
- Pass all already existing device reliability tests; and,
- Resist environmental/physical/chemical treatments common in electronics manufacturing and in the application of electronic equipment in its intended operational environment (automotive, industrial, medical, security, military, etc.)

C. Effectiveness – Related to IC Industrialization

The technology must demonstrate the potential for integration in a production line and for fast automatic reading.

These criteria will ensure that the authentication element can be integrated into the IC packaging process and meet the production and supply requirements:

- Impact on Process: the technology must be attachable and measureable from an automatic reading unit within the assembly production line.
- Impact on Process Yield: limited yield loss linked to the operation including ESD damages (both attach and read failures)
- Impact on Process Time: fully industrialized

D. Effectiveness – Related to Environment

These requirements specify conditions dictated by the many varieties among semiconductor products and the semiconductor production environments.

It covers:

- Appearance of the component after tagging
- Area/volume available for tagging
- Types of semiconductor packages to be covert
- Requirements with respect to safety and the production environment.

E. Efficiency – Authentication Principles

These requirements specify conditions of counterfeit identification as well as time to authenticate. This includes measuring the detection time, false positives or negatives, and operating lifetime including maintaining functionality under a wide range of product operating conditions.

It covers:

- Detection of given counterfeit scenarios
- Detection principle of authentication element
- Time to integrate and authenticate the authentication element
- Detection certainty and reliability (6-sigma concept)
- Operating lifetime of the authentication element
- Code diversification capability

F. *Efficiency –Reading & Detection*

These requirements specify the reading pass/fail information output. This applies to the required properties of the reader, including the need for automated reading, for example, in the production line, as well as manual reading, for example, in government supply depots.

It includes:

- Availability of a handheld reader
- Potential for integration into the device manufacturing line for automatic reading
- Reading reliability for both manual and automatic reading
- Reading equipment specifications (interface, power, safety)

G. *Efficiency – Resistance against attacks*

These requirements specify the technology's resistance to attacks. This includes the technology itself, the process to apply it to the semiconductor, as well as the tools and procedures to read the technology.

The authentication technology must withstand the following attacks defined in [2]:

- Reverse engineering, copy and imitation
- Tampering
- Alteration
- Side channel resistance

III. FAILURE ANALYSIS AND PREVENTION TESTS

The A/T insertion shall not impact the electronic component's functionality and performance, nor change its aspect, nor its marking readability.

First feasibility tests must be performed in order to demonstrate the possible adaptation of the technology into the existing SC production process.

Then, to avoid potential failure of components and to ensure that components remain in line with their initial specifications, failure analysis and prevention tests have to be conducted.

A. *Insertion Step Trials*

The A/T can be inserted at different assembly process steps (e.g. during the molding, before the curing, after the curing, after tinning, after laser marking).

Analysis was conducted to list the most relevant insertion steps, based on the authentication technology and its specific characteristics but also on the production assembly line constraints.

Various insertion points were tested in order to find the most appropriate ones taking into account the following parameters:

- Final visual acceptance
- Evolution of A/T signal all along the assembly process
- Potential functional and performance issues induced by the technology insertion

Fig. 1 shows an example of tagged components (3 different A/Ts and 3 insertion points) which have undergone the complete assembly process, mapped with their corresponding signal measurements, which analysis led to the selection of the best combinations in terms of aspect and signal intensity.

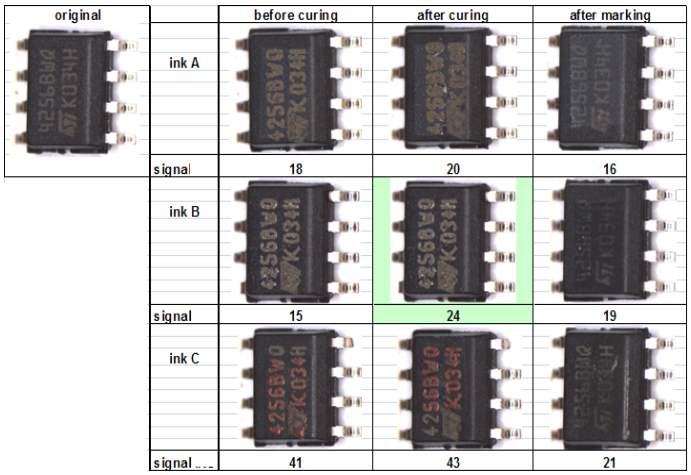

Fig. 1 Matrix of tagged samples: 3 assembly steps and 3 A/Ts

B. *Adherence*

Different deposition methods (pad printing, screen printing, roll printing, tampon, plasma torch, laser tagging …) were tested in order to determine the one providing the best adherence of the A/T together with the most acceptable visual aspect.

Usual A/T adherence testing methods are: Knife test, Tape test, Pull-Off tests, Scrape tests, ...

C. *Diffusion and A/T Deposition Thickness Measurement*

It is useful to characterize the diffusion directions and measure the diffusion depth an A/T can have within the package compound, as well as to measure the deposition thickness the A/T can reach, in order to assess how the packaging tampering can be detected with respect to the SC industry marking standard.

It is also interesting to know how the A/T signal evolves in case of partial delayering.

D. *Functional Electrical Parametric Tests*

Functional and electrical tests are needed to check if products still comply with their initial specifications and to

detect any impact raised by the A/T insertion.

The content of these tests depend on the considered products. For instance:

- Functional and parametric tests of peripherals and embedded macro-cells for microcontrollers
- Electrical tests for diodes through measurements of specific signals (Forward Voltage, High Forward Voltage, Reverse Voltage and Reverse Leakage Current)

These tests shall be performed before and after each step cycle of the reliability tests (refer to section IV).

E. Visual Acceptance

The insertion of A/T shall not impact the visual appearance of the final product. Any technology shall not compromise the correct reading of the original component marking.

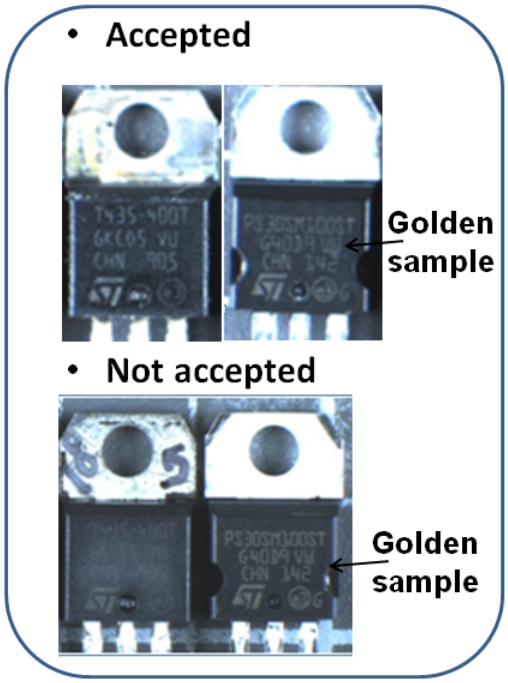

Fig. 2 Visual aspect of tagged components

F. Reading Stability

The authentication tool (reader) has to be reliable and the reading results must be repeatable. Objective is to get a reliable result during an authentication process upon one reading trial.

In order to assess the reader capability, a sufficient quantity of tagged parts must be measured with the corresponding authentication tool at least 100 times. If the reading process is stable, a normal Gaussian distribution is obtained as shown in Fig. 3.

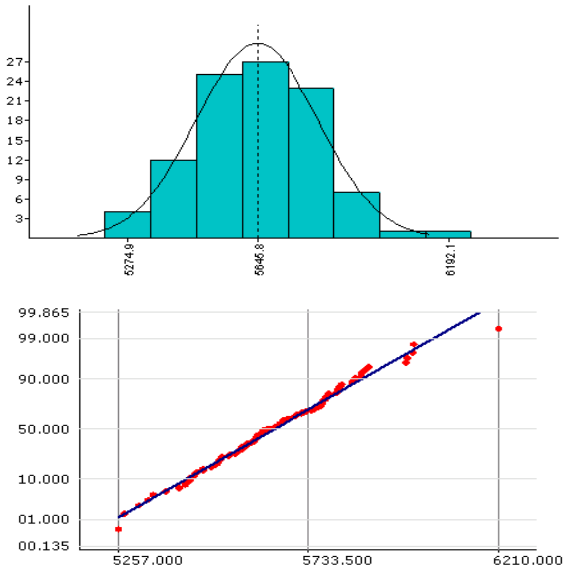

Fig. 3 Reading trials distribution

IV. RELIABILITY TESTS

The inserted authentication element shall have a lifetime close to the electronic component under its operating conditions, around 10 years in the semiconductor domain.

In order to simulate the thermo-mechanical stress that the technology will face during the component lifetime and also to assess the A/T lifetime itself, aggressive 1st-level and 2nd-level reliability tests have to be performed.

JEDEC gives global standards for the microelectronics industry and JC-14 committee is responsible for standardizing quality and reliability methodologies for solid state products used in commercial applications such as computers, automobiles, telecommunications equipment, etc. It also develops standards for board-level reliability of solid state products used in commercial equipment.

Some reliability tests, described below, issued from the JEDEC standards were performed.

A. 1st Level Reliability Tests

Reliability is defined as the ability of a device to conform to its electrical and visual/mechanical specifications over a specified period of time under specified conditions at a specified confidence level.

1st level reliability testing also called Package-level reliability testing refers to the assessment of the over-all reliability of the device in packaged form without considering its solder interconnect reliability when it is board mounted. This consists of subjecting packaged samples to reliability tests that expose the various sample sets to different stress conditions (temperature, humidity, pressure,…), after which the samples are tested for any degradation in quality after the stress. Since reliability stresses are often destructive, only a sample population is used for reliability testing. As such, the assessment of the reliability of the rest of the population is essentially statistical and probabilistic in nature.

In below engaged 1st level reliability tests, cycle steps up to 1000 cycles were performed, with a checking of the visual aspect and of A/C signal evolution at each step.

1) TCT - Temperature Cycling Test [3]

This standard provides a method for determining solid state devices capability to withstand extreme temperature cycling (-55°C to +150°C). This allows to investigate failure modes related to the thermomechanical stress induced by the different thermal expansion of the materials interacting in the die package system. Typical failure modes are linked to metal displacement, dielectric cracking, molding compound delamination, wire-bonds failure, die attach layer degradation.

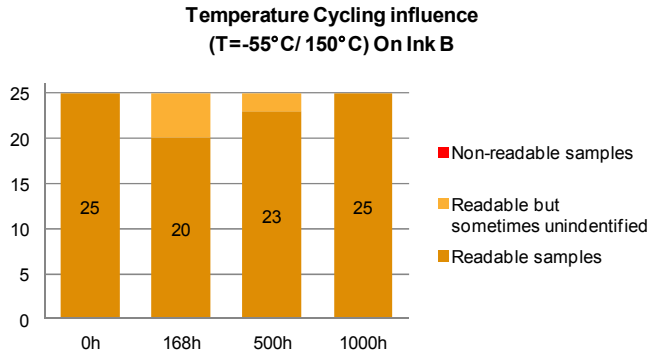

Fig. 4 TCT Results (example)

2) THBT - Temperature Humidity Bias Test [4]

This standard establishes a defined method and conditions for performing a temperature humidity life test with bias applied. The test is used to evaluate the reliability of non-hermetic packaged solid state devices in humid environments. It employs high temperature and humidity conditions to accelerate the penetration of moisture through external protective material or along interfaces between the external protective coating and conductors or other features which pass through it (conditions: 85°C, 80% humidity, 80V).

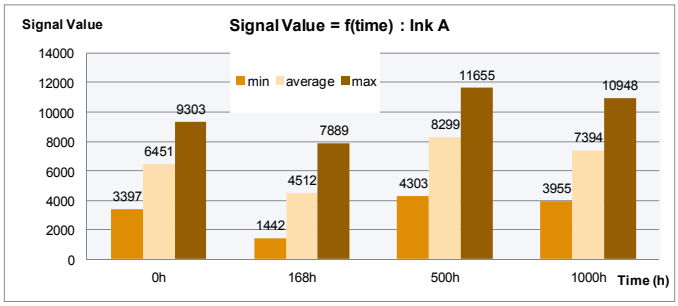

Fig. 5 Evolution of A/C signal during THBT

3) HTST - High Temperature Storage Test [5]

HTST is typically used to determine the effects of time and temperature, under storage conditions, for thermally activated failure mechanisms and time-to-failure distributions of solid state electronic devices, including nonvolatile memory devices (data retention failure mechanisms). Thermally activated failure mechanisms are modeled using the Arrhenius Equation for acceleration. During the test, accelerated stress temperatures are used without electrical conditions applied. This test ("accelerated aging") may be destructive, depending on time, temperature (+150°C advised for electronic components) and packaging.

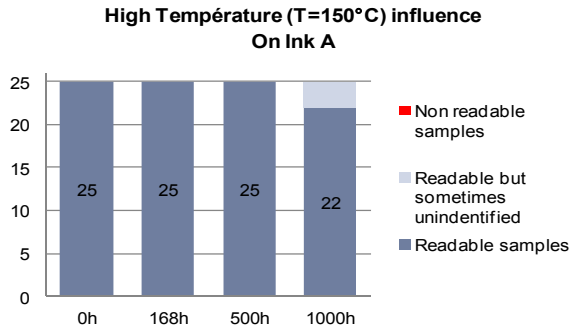

Fig. 6. HTST results (example)

4) ACT - Autoclave Test [6]

This test allows the user to evaluate the moisture resistance of non-hermetic packaged solid state devices. The Unbiased Autoclave Test is performed to evaluate the moisture resistance integrity of non-hermetic packaged solid state devices using moisture condensing or moisture saturated steam environments. It is a highly accelerated test which employs conditions of pressure, humidity and temperature (2 bars pressure, 100% humidity, 121°C) under condensing conditions to accelerate moisture penetration through the external protective material or along the interface between the external protective material and the metallic conductors passing through it. This test is used to identify failure mechanisms internal to the package and is destructive.

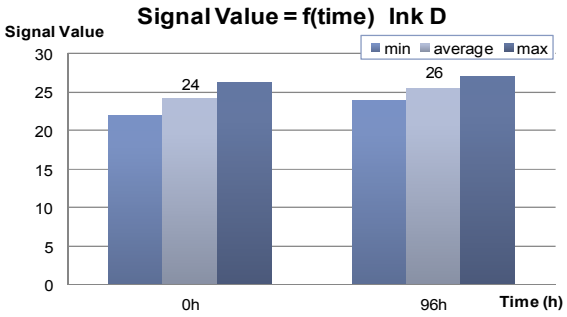

Fig. 7 Evolution of A/C signal during ACT

5) SAT - Salt Atmosphere Test [7]

This Salt Atmosphere Test is conducted to determine the resistance of solid state devices to corrosion. It is an accelerated test that simulates the effects of severe seacoast atmosphere on all exposed surfaces. SAT is considered destructive. It is intended for lot acceptance, process monitoring, and qualification testing. Typical conditions are 35°C, 5% NaCl solution.

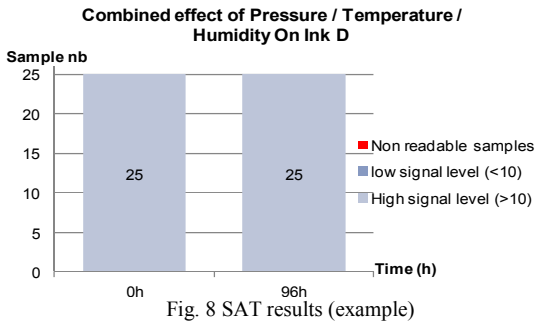

Fig. 8 SAT results (example)

6) SRT - Solder Reflow Test [8]

This standard identifies the classification level of non-hermetic solid-state surface mount devices (SMDs) that are sensitive to moisture-induced stress. It is used to determine what classification level should be used for initial reliability qualification. Once identified, the SMDs can be properly packaged, stored and handled to avoid subsequent thermal and mechanical damage during the assembly solder reflow attachment and/or repair operation. Typical conditions are to apply a soldering temperature curve profile up to 260°C several times.

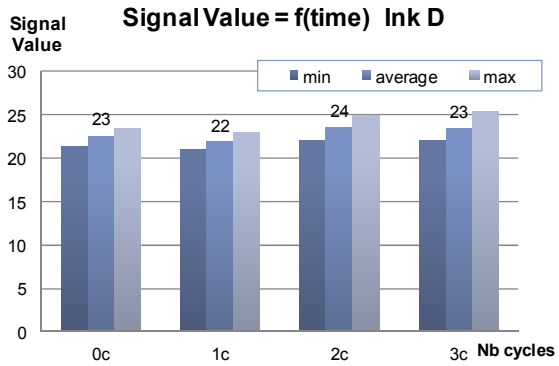

Fig. 9 Evolution of A/C signal during SRT

B. 2nd Level Reliability Tests

In the 2nd level reliability tests, also called Board level tests, stresses having the ability to lead to premature failure are concentrated on the solder joint interconnect performance of the surface mount package when it is board mounted. These tests consist of different mechanical and thermal shocks/stresses that simulate and/or accelerate the scenario experienced by the device during field applications. This assures that early failures are not infant-mortalities due to defective solder joints.

Typical examples for 2nd level reliability tests are Board Level Temperature Cycle Test (BLTCT, [9]), Board Level Drop Test (BLDT, [10] [11]), Board Level Bend Test (BLBT, [12]), and Board Level Vibration Test (BLVT, [13]). The "Board Level" term is used to emphasize that samples are board mounted while being tested. These specific tests concern reliability of the soldering between the components and a board.

Details of engaged 2nd level reliability tests will be provided in another publication.

V. CONCLUSION

Semiconductor manufacturers are severely affected by the growing rate of chips counterfeits. Not only do they lose direct sales, their credibility and brand image are also strongly compromised.

To gain back control over their brands and support the combat against counterfeiting, members of semiconductor and related industries in Europe joined an R&D program to assess the effort needed to implement authentication technology solutions into IC packages. The aim of the SC industry experts is to determine the best route to integrate appropriate authentication technologies into their products, without compromising the existing SC operations and with a cost control approach.

The SC manufacturers will therefore benefit from a cost and a response time reduction in the authentication process following device failure or seizure.

The described test procedure is helping to adapt the counterfeit-proof technologies and tools to achieve the highest level of effectiveness and efficiency to combat counterfeiting in the SC domain. This effort will help to stay one step ahead of the counterfeiters. However, it cannot be emphasized enough that simply adding authentication means will deter counterfeiting and copying of ICs but it will not stop unreliable products to enter the market.

This paper focused mainly on the qualification and test plan related to failure analysis, failure prevention and the reliability of the product. Another paper will describe the test plan elaborated to check the resistance against attack. Guidelines will be provided to the SC industry about how to incorporate the authentication technology into its mass production environment.

REFERENCES

[1] SACS (The Senate Armed Services Committee) report - Inquiry into counterfeit electronic parts in the department of defense supply chain, by of the committee of armed services, united states services, MAY 21, 2012

[2] Performance criteria for authentication solutions used to combat counterfeiting of material goods, ISO12931

[3] JEDEC standard JESD22-A104D

[4] JEDEC standard JESD22-A101C

[5] JEDEC standard JESD22-A103D

[6] JEDEC standard JESD22-A102D

[7] JEDEC standard JESD22-A107B

[8] JEDEC standard J-STD-020D.1

[9] IPC standard IPC-9701

[10] JEDEC standard JESD22-B111

[11] Mechanical modeling and analysis of board level drop test of electronic package (IEEE, Junfeng Zhao, Assembly Technol. Dev., Intel Technol. Dev. Ltd., Shanghai Garner, L.J).

[12] JEDEC standard JESD22-B113A

[13] JEDEC standard J-STD-B103