# Counterfeit IC Detection and Challenges Ahead

Ujjwal Guin, University of Connecticut
Mohammad Tehranipoor, University of Connecticut
Dan DiMase, Chairman - SAE G-19A, Test Laboratory Standards Development Committee
Mike Megrdichian, SAE G-19A, Test Laboratory Standards Development Committee

Counterfeit integrated circuits (ICs), commonly known as microcircuits, pose a significant threat to the global electronics component supply chain and are becoming more difficult to detect as the counterfeiters increase their level of sophistication. They are of great concern to industry and government [1] because a system malfunction can present situations that cause mission failures, health and safety concerns, and could jeopardize national security; they can have a negative impact on brand reputation, and research and development efforts; counterfeits pose a reduction in reliability; and they channel substantial resources to criminal networks, organized crime and the illicit marketplace. It was estimated that the cost of counterfeiting and piracy for G20 nations was $450 to $650 billion in 2008 and will grow to $1.2 to1.7 trillion in 2015 [17]. In the past couple of years, numerous reports (to be found in [11]) have uncovered the counterfeit issues in the United States electronics component supply chain. US Senate's Armed Services Committee clearly identified counterfeit ICs as a major issue to address because of its significant implications on taxpayer money as well as the threat to the warfighter that can be associated with deploying counterfeit parts in DOD critical applications [12-13].

There are standards in place that include guidance or requirements for detection of the counterfeit parts [3][4][5]. However, at present these standards are reactive to the parts that are already circulating in the market. Also, these standards mainly deal with two types of counterfeits, namely, recycled and remarked (i.e. used parts sold as new) and out-of-specification overproduced devices. However, overproduced devices that meet specification cannot be detected using these standards. The standards test methods may not detect some other counterfeit types (e.g. cloned, overproduced, and tampered devices) and are reactive versus proactive. In a proactive approach, design for counterfeit prevention takes on the anti counterfeiting mechanism for parts that are currently (will be) fabricated using on-chip sensors for measuring chip usage [16] or physically unclonable functions by generating unique ID for each chip [14-15], to name a couple. Some of these preventative techniques address threats from different counterfeit types beyond recycled and remarked devices.

**Counterfeit Types**

A counterfeit electronic component/part- (i) is an unauthorized copy; (ii) does not conform to original component manufacturer (OCM) design, model, and/or performance standards; (iii) is not produced by the OCM or is produced by unauthorized contractors; (iv) is an off-specification, defective, or used OCM product sold as new; or (v) has incorrect or false markings and/or documentation [6]. Based on the above, we classify the counterfeit types in seven distinct categories namely recycled, remarked, defective/out-of-spec, forged documentation, overproduced, cloned, and tampered.

Counterfeit electronic components are penetrating supply chain mostly through the gray market and due to the complexities of the global supply chain network. It is reported that in today's supply chain, more than 80% of the counterfeit components are recycled and remarked [7]. Only 25% of electronic waste has been properly recycled in 2009 in the United States [2]. That percent is even lower for other countries. Even if recycling is properly handled in the United States, countries that have been taking advantage of this large electronic waste as their

resource for counterfeits have enough of their own electronic waste to have an indefinite supply of raw material for counterfeiting purposes.

Recycling and remarking is a process by which the used components are removed from scrapped printed circuit boards (PCBs) and their package is repainted or “blacktopped”, and/or remarked, or in some cases the die is removed from the packaging and is repackaged and remarked. These components are then sold as new in the open market. In some cases, the recycled parts may either be nonfunctioning, not performing to manufacturer specifications, or the prior usage has done significant damage to the part's life cycle and introduces major reliability concerns. In some cases, new parts have also been remarked by counterfeiters. The remarked parts in this category consist of two types – equivalent part types from a cheaper brand or new parts are remarked to a higher grade, i.e. upgrading a component to industrial or military grade from commercial grade, mainly to increase profit. Some of the parametric values of these types of counterfeits may not perform in accordance with expected specifications and may also have significant reliability concerns.

Overproduced components are when an untrusted foundry/assembly has access to a designer’s intellectual property (IP) block and fabricates, assembles, and then sells parts in the open market outside the contract without design houses’ knowledge. These parts may not be tested under the conditions set by the design house before being shipped to the market and therefore introduce reliability concerns. Another variation of an untrusted foundry producing counterfeit parts is an out-of-specification (spec) or a defective part being sold instead of being destroyed. A cloned part is an unauthorized production of a part without having the legal IP rights to produce the device. Cloning can also be done by reverse engineering the original design or pirating the IP. The forged documentation category is probably the easiest to fake where counterfeiters change the specification of the chip on documents; in some cases, these chips can be detected by specification testing. However, testing could be extremely expensive and virtually impossible in the absence of the original component manufacturer’s test fixtures and test programs. The final category of counterfeit is the tampered type. Here, we represent tampered as those ICs possibly including “hardware Trojans”. Tampered components can potentially leak valuable and sensitive on-chip information to the counterfeiter or act as a silicon time bomb in the field [8].

**Counterfeit Detection Methods**

Counterfeiting is a multidimensional problem due to the different counterfeit types, different defect taxonomies, and evolving nature of the counterfeiters. As industry comes up with new detection methods, the counterfeiters come up with new ways to evade detection. One cannot reach a definite conclusion whether a part is counterfeit or not by performing a simple test. A set of test methods is necessary for detection of counterfeit parts, and to achieve a desired confidence level that the part is not counterfeit based on what we know about counterfeiting today. The test methods can be classified into three distinct categories, namely, physical tests, environmental tests, and electrical tests.

Physical tests are mostly performed to verify the physical and chemical/material properties of the component, such as, package, leads, dies, etc and their chemical and material composition. These tests are classified into four major categories: *(i) External Visual Inspection (EVI):* All parts should be strictly inspected and documented during this phase. *(ii) Package Analysis:* Parts should be selected for package analysis by sampling a lot under test. The samples can be used for multiple tests, such as delid and material analysis. If any anomalies were found from previous inspection, they should be included in the sample lot. The package analysis should include inspection for remarking or resurfacing for evidence of blacktopping, microblasting, or

flatlapping. Blacktopping is a counterfeit technique where the counterfeiter may sand plastic encapsulated devices and mix the shavings with an epoxy substance that is later coated on the part to disguise surface alteration. Microblasting is when a counterfeiter uses a superfine blasting process with various media types to “sandblast” part markings off a device. Flatlapping is when a counterfeiter uses an abrasive, rotating lap utilizing loose slurry under low speed and low pressure, typically performed in a figure-eight pattern to avoid evidence of sanding marks. Microblasted and flatlapped parts may or may not be blacktopped to further conceal alteration to the packaging. Some package types (e.g. ceramics) may be painted to conceal alteration of the parts. The inspection for remarking or resurfacing may include aggressive solvents testing to remove blacktopped material and reveal the altered surface of the package. The aggressive solvents test is considered a destructive test and is therefore done on a sample of the lot. *(iii) Delid/Internal Verification: Delid/decapsulation physical analysis is* a test method employed to remove a part of the outer protective coating of a package or encapsulation of a part to examine the internal structure to determine if the part appears authentic. Other internal verification includes Radiological (X-Ray) analysis. *(iv) Material Analysis:* The chemical composition of the component is verified using material analysis. There are several tests that can perform material analysis including X-ray fluorescence (XRF), Fourier transform infrared (FTIR), RAMAN, Energy Dispersive Spectroscopy (EDS), etc. Both FTIR and RAMAN are used to obtain infrared spectra of materials for identification and verification.

An existing problem in counterfeit detection is how to inspect for the case of used parts being sold as new. This also includes commercial parts being misrepresented as MIL or High Rel grade, or devices that have been stored in hostile environments or have been mishandled. The technical solution to detecting used parts sold as new, has to include Environmental Testing. These tests will detect both counterfeit parts and also reliability/quality issues. The technique involves stressing the devices and then inspecting them for changes in both Physical and Electrical Characteristics. The Environmental Tests involve lot sample tests of Temperature Cycling for Active Devices (MCs & SDs) followed by post electrical, Thermal Shock with pre and post electrical for Passive Devices, and Seal Tests for Hermetic Devices. The challenge for the Test Laboratory and User/Requester personnel is in the Interpretation of Test Results of whether the failure is a Counterfeit or a Quality/Reliability issue.

Electrical test methods are mostly applied to verify the correct functionality and performance of a component. These tests may be different for different types of components, namely, analog, microprocessors, programmable logic arrays, memories, etc. Automatic test equipment (ATE) [9] may be required for some high-end digital and analog integrated circuits. The electrical tests are categorized as follows: *(i) Parametric Tests:* Parametric tests are performed to measure DC and AC parameters of a chip. They include contact test, power consumption test, output short current test, output drive current test, threshold test, rise and fall time tests, set-up, hold and release time tests, propagation delay tests, etc. *(ii) Functional Tests:* Functional tests are the most efficient way of verifying the functionality of a component and perhaps the most expensive way. For a memory device, read/write operations can be performed to verify its functionality. For example, MARCH tests can be applied for detecting a counterfeit memory. As another example, functional $f_{max}$ analysis could be applied to detect counterfeit microprocessors as their speed change because of prior usage in the field. *(iii) Burn-In Tests:* The device is operated at an elevated temperature to find infant mortality failures and unexpected failures to assure reliability. *(iv) Structural Tests:* These tests are very effective in detecting manufacturing defects for out-of-spec/defective counterfeit types. However, their effectiveness for detection of counterfeit parts may be challenged by the following concerns: (a) these tests may require access to internal scan chains of an IC. Design houses usually do not provide permission to access their design

by disabling the internal scan chains with a fuse, and (b) obsolete parts may not have design for testability (DFT) structures implemented in them.

**Challenges Ahead**

The detection of counterfeit electronic components is still in its infancy, and there are major challenges which must be overcome for the deployment of effective counterfeit detection methods. We must also make every attempt to stay ahead of the counterfeiters to prevent a widespread infiltration of such parts into our critical infrastructures. The US Congress enacted National Defense Authorization Act (NDAA) of 2012 [10] on December 2011. Section 818 of NDAA 2012 contains new requirements for the Department of Defense (DOD) to detect and avoid counterfeit electronic parts and to implement a risk-based approach to minimize the impact of counterfeit or suspect counterfeit electronic parts.

There are several standards (such as SAE AS6171, CTI CCAP-101 and IDEA STD-1010) in place or in development to guide the user for counterfeit detection and avoidance. However, all these standards mainly focus only on two types of counterfeits – recycled and remarked and out-of-specification overproduced parts while neglecting other counterfeit types. The tests are performed in an ad-hoc fashion with no metrics based on real data from the test results to quantify effectiveness. Most of the tests are carried out without automation. The test results mostly depend on the subject matter experts (SMEs) and their subjective analysis. In turn, the decision making process becomes dependent on the SMEs, which can subject to interpretation. A chip can be considered counterfeit in one lab while it could very well be marked as authentic in another lab. Such inconsistency in detection of counterfeit parts can have catastrophic effects. Further, it is difficult to verify components as genuine for certain counterfeit types, such as overproduced, cloned, and tampered ICs. One cannot detect Trojans almost certainly by any test methods developed so far. Test time and cost are major limiting factors for uniform implementation of detection methods. Some of the physical tests done today are destructive -- sample preparation and random sample practices are extremely important to achieve the desired statistical test confidence. Finally, low-cost design for counterfeit prevention (DfCP) approaches are needed to help prevent counterfeiters from shipping the counterfeited parts to the supply chain. If they do, however, OCMs, OEMs, and test labs could easily detect counterfeited parts much easier with DfCP approaches deployed.

# References:


[1] http://www.chase.uconn.edu/arochase-special-workshop-on-counterfeit-electronics.php

[2] U.S. Environmental Protection Agency, “Electronic waste management in the united states through 2009,” May 2011.

[3] SAE, “Counterfeit electronic parts; avoidance, detection, mitigation, and disposition,” 2009, http://standards.sae.org/as5553/

[4] CTI, “Certification for counterfeit components avoidance program,” September 2011, [Online]. Available: http://www.ctius.com/pdf/CCAP101Certification.pdf

[5] IDEA, “Acceptability of electronic components distributed in the open market,” http://www.idofea.org/products/118-idea-std-1010b

[6] U.S. Department Of Commerce, “Defense Industrial Base Assessment: Counterfeit Electronics,” January 2010

[7] L. W. Kessler and T. Sharpe, “Faked Parts Detection,” 2010, [Online]. Available: http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt

[8] M. Tehranipoor and C. Wang, “Introduction to Hardware Security and Trust”. Springer, 2012

[9] A. Grochowski, D. Bhattacharya, T. Viswanathan, and K. Laker, “Integrated circuit testing for quality assurance in manufacturing: history, current status, and future trends,” Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on, vol. 44,no. 8, pp. 610 –633, aug 1997
[10] US Congress, “National Defense Authorization Act for Fiscal Year 2012.” [Online]. Available: http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf
[11] TRUST-HUB, http://trust-hub.org/home
[12] U.S. Senate Committee on Armed Services, "Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms", 2012, [Online]. Available: http://www.gao.gov/assets/590/588736.pdf
[13] U.S. Senate Committee on Armed Services, “INQUIRY INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN”, 2012, [Online]. Available: http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf
[14] R. Pappu, “Physical one-way functions,” Ph.D. dissertation, Massachusetts Institute of Technology, 2001.
[15] G. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. of IEEE/ACM on Design Automation Conference (DAC), 2007.
[16] X. Zhang, N. Tuzzio, and M. Tehranipoor, “Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor,” in Proc. of IEEE/ACM on Design Automation Conference (DAC), 2012.
[17] International Chamber of Commerce, “Estimating the global economic and social impacts of counterfeiting and piracy”, February 2011.