A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment

Ujjwal Guin · Daniel DiMase ·
Mohammad Tehranipoor

Received: 22 July 2013 / Accepted: 28 November 2013

Abstract The increasing threat of counterfeit electronic components has created specialized service of testing, detection, and avoidance of such components. However, various types of counterfeit components – recycled, remarked, overproduced, defective, cloned, forged documentation, and tampered – pose serious threats to supply chain. Over the past few years, standards and programs have been put in place throughout the supply chain that outline testing, documenting, and reporting procedures. However, there is little uniformity in the test results among the various entities. Currently, there are no metrics for evaluating these counterfeit detection methods. In this paper, we have developed a detailed taxonomy of defects present in counterfeit components. Based on this taxonomy, a comprehensive framework has been developed to find an optimum set of detection methods considering test time, test cost, and application risks. We have also performed an assessment of all the detection methods based on the newly introduced metrics – counterfeit defect coverage, under-covered defects, and not-covered defects.

Keywords Counterfeit IC · Detection methods · Assessment · Defect coverage

Responsible Editor: T. Xia

U. Guin (✉) · M. Tehranipoor
Department of ECE, University of Connecticut, Storrs, CT, USA
e-mail: ujjwal.guin@uconn.edu

M. Tehranipoor
e-mail: tehrani@engr.uconn.edu

D. DiMase
Honeywell Inc., Morristown, NJ, USA
e-mail: Daniel.DiMase@Honeywell.com

1 Introduction

Counterfeiting of integrated circuits (ICs) has become a major challenge due mainly to deficiencies in the existing test solutions. Over the past few years, numerous reports [44] have pointed to the counterfeiting issues in the electronics component supply chain. The most recent data provided by Information Handling Services Inc. (IHS) shows that reports of counterfeit ICs have quadrupled since 2009 [6]. The Senate Armed Services public hearing on this issue and the subsequent report clearly identified counterfeit detection as a major issue to address [48, 49]. Counterfeit components are of great concern to the government and industry because of – (*i*) their reliability issues, and (*ii*) potential system failures or malfunctions that can cause mission failures [45].

Counterfeit ICs enter the component supply chain mostly through recycling and remarking [21]. The components are taken off of the scrapped boards, cleaned, remarked, and then sold on the open market as new. In the United States only 25 % of electronic waste was properly recycled in 2009 [47]. That percentage is even lower in other countries. This huge resource of e-waste provides counterfeiters with the necessary fuel to build up an extremely large supply of raw materials for counterfeiting. Moreover, due to the globalization of the semiconductor industry and the prohibitively high cost required to create foundries [30], the design houses no longer fabricate, package and test their designs. They give the contract to the foundries for the fabrication of wafers/dies and assembly companies for IC packaging and testing. The foundry/assembly, however, can ship defective, out-of-spec, or even over-produced chips to the black market without the design house's knowledge. Along with this, the counterfeiters can clone the ICs (sometimes it might be substandard if not tested properly) by

Published online: 15 January 2014

using illegally obtained IPs or through reverse engineering which eventually make the design house suffer by losing its revenue and reputation [43].

We believe that research in detecting counterfeit electronic components is still in its infancy. Currently, there is a minuscule research exists in this field. There are only few standards in place to provide the guidance for the detection of counterfeit components [9, 19, 34]. These standards apply to those electronic components that are already circulating in the supply chain (mainly obsolete and active components). The obsolete components are no longer being manufactured and active components are being fabricated based on the previous design and developed masks. On the other hand, design for counterfeit prevention mechanisms can be implemented on new components by – (i) adding the anti-counterfeiting mechanism using on-chip sensors for measuring chip usage [50, 52–54], (ii) creating physically unclonable functions by generating a unique ID for each chip [4, 24, 25, 32, 40], (iii) creating a set of security protocols (hardware metering) that enable the design house to achieve the post-fabrication control of the produced ICs [22, 23], and (iv) applying a coating of plant DNA on the package [29]. However, we cannot implement these anti-counterfeit measures in these obsolete and active components as we cannot change the designs (e.g., masks).

In this paper, our focus is on the assessment of all counterfeit detection methods which mostly address the detection of the majority of components circulating in the supply chain. Today's counterfeit detection methods pose a distinct challenge to original component manufacturers (OCM), original equipment manufacturers (OEM), and test labs, and an urgent assessment of these methods is extremely necessary. First, most of the counterfeit detection methods are destructive. Sample preparation is extremely important as it directly relates to test confidence. If a few counterfeit components are mixed with a large batch, the probability of selecting the counterfeit one is extremely small. Second, the test time and cost are the major limiting factors. Third, the equipment used for the physical inspection of such parts (e.g., scanning electron and acoustic microscopy (SEM or SAM)) is not custom designed to detecting counterfeit parts, resulting in large timing overheads. Fourth, the tests are done in an ad-hoc fashion with no metrics for quantifying against a set of counterfeit types, anomalies, and defects. Most of the tests are carried out without automation. The test results mostly depend on subject matter experts (SMEs). The decision-making process is entirely dependent on these operators (or SMEs), which is, indeed, error prone. A chip that might be considered counterfeit in one lab could be marked authentic in another. This was proven by a test run by SAE G-19A, Test Laboratory Standards Development Subcommittee [35], which found that some labs reported the chip as counterfeit and other labs as authentic [7].

To address the above issues, in this paper, we have developed a comprehensive framework to help assess the effectiveness of existing counterfeit detection methods. Our contributions include:

(i) *Development of taxonomies*: We develop a detailed taxonomy of the defects present in counterfeit ICs. To the best of our knowledge, this is the first approach to analyzing counterfeit components considering the vulnerabilities in the electronic component supply chain. We develop a taxonomy for counterfeit types to analyze supply chain vulnerabilities. Our counterfeit method taxonomy describes all the test methods currently available for counterfeit detection. This paper mainly focuses on test technologies targeted at counterfeit parts already on the market (known as obsolete and active parts).

(ii) *Development of metrics for evaluating counterfeit detection methods*: We introduce counterfeit defect coverage (CDC) as an assessment metric for counterfeit detection methods. We also develop under-covered defects (*UCDs*) and not-covered defects (*NCDs*) as part of the assessment metric.

(iii) *Development of a method selection algorithm*: We propose a model to recommend a set of tests for maximizing the test coverage (*CDC*). This model is built on the confidence level matrix, which represents the effectiveness of a method to detect a particular defect. This is the first attempt to cumulatively address the assessment of all test methods in a data-driven manner. This model also takes feedback from the subject matter experts.

(iv) *Assessment of detection methods*: We contribute to the assessment of existing counterfeit detection methods using our proposed *CDC* model and the newly developed metrics mentioned above.

The rest of the paper is organized as follows. In Section 2 we describe different types of counterfeits polluting the supply chain. A taxonomy of counterfeit detection methods is presented here as well. Section 3 introduces a detailed taxonomy for the defects and anomalies that are typical of counterfeit components. We then assess the detection methods in Section 4. We present our proposed algorithm to find the optimum set of tests required to maximize test coverage. The experimental results are shown in Section 5. Section 6 concludes the paper.

2 Taxonomies: Counterfeit Components and Detection Methods

Today, various types of counterfeit components enter the electronic component supply chain that must be segregated from the genuine components through inspections and tests. In this section we will first catalog all types of counterfeit components and then present the currently available methods for counterfeit detection.

2.1 Taxonomy of Counterfeit Components

A counterfeit electronic component - (i) is an unauthorized copy; (ii) does not conform to the original OCM design, model, and/or performance standards; (iii) is not produced by the OCM or is produced by an unauthorized contractors; (iv) is an off-specification, defective, or used OCM product sold as new or working; or (v) has incorrect or false markings and/or documentation [46]. Based on the definition above and analyzing supply chain vulnerabilities, we classify counterfeit types into seven distinct categories [16–18] which is shown in Fig. 1.

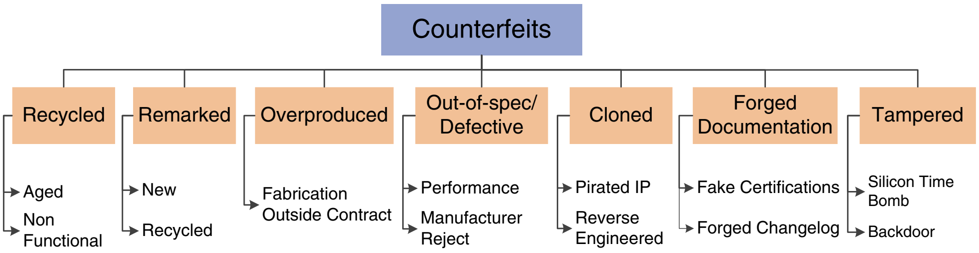
The most widely discussed counterfeits are the *recycled* and *remarked* types. It is reported that in today's supply chain, more than 80 % of counterfeit components are *recycled* and *remarked* [21]. The recycled components may be have significant performance degradation or be completely nonfunctional due to aging or mishandling. The remarked components are also of two types – parts taken from a scrapped printed circuit board (PCB) or new parts are remarked to upgrade the component, for example, from commercial grade to industrial or defense grade. In *overproduction*, any untrusted foundry/assembly that has access to a designer's IP now also has the ability to fabricate ICs outside of contract. They can easily sell excess ICs on the open market. These parts may not be tested under the conditions set by the designer before being shipped to the market. The other variation of an untrusted foundry sourcing counterfeit parts is an *out-of-specification (spec)* or a rejected (here called *defective*) part being sold instead of destroyed. A *cloned* component is an unauthorized production without a legal IP. Cloning can be done in two ways – by reverse engineering and by obtaining IPs illegally. *Forged documentation* may include certifications of compliance for some standards or programs, or a revision history or change-log of a component. The final category of counterfeit is the *tampered* type. Tampering can be done during any phase of the life cycle of a component. It can either be in the die level ("hardware Trojan") or package level. The tampering can be done during design and fabrication. Tampered components can potentially leak valuable and sensitive on-chip stored information to the counterfeiter or act as a silicon time bomb in the field [20, 42, 43]. In this paper, we will not focus on the last two types of counterfeit components, as they pose a different set of challenges for their detection.

2.2 Taxonomy of Detection Methods

The components must go through a detailed acceptance test before being used in the system to ensure that they meet the quality and reliability requirements and that they are authentic, especially when they are used in critical applications. In this section, we will discuss all methods currently available for the detection of counterfeit components. They are broadly classified into two types – physical and electrical methods. Figure 2 represents the taxonomy of detection methods, $M1$ through $M21$. Mi–j represent sub-category j in method Mi.

Physical methods are mostly performed to verify the physical and chemical/material properties of the component to detect the physical counterfeit defects (in Section 3) during the authentication of a component. These methods are classified into four major categories: (i) *Incoming Inspection*: All the components are strictly inspected and documented by incoming inspection. All the easy-to-detect defects and anomalies related to the component are inspected carefully. The exterior part of the component is examined by low power visual inspection (generally less than 10X magnification) while the interior part is analyzed by X-Ray imaging. (ii) *Exterior Tests*: The exterior part of the package and leads are analyzed by exterior tests. These tests are used to detect the defects related to the exterior parts of the components. In blacktop testing, acetone or dynasolve is applied to test part's marking permanency. In microblasting, various blasting agents with proper grain sizes are bombarded on the surface (package) of the component and the materials are collected for analysis. Hermiticity Testing is a special type of package analysis specific to hermetically sealed parts that tests the hermetic seal. Scanning acoustic microscopy (SAM) is one of the most efficient, though expensive, ways of studying the external and internal structure of a component. For example, if the component is damaged during the counterfeiting process, the cracks

Fig. 1 A taxonomy of counterfeit component types



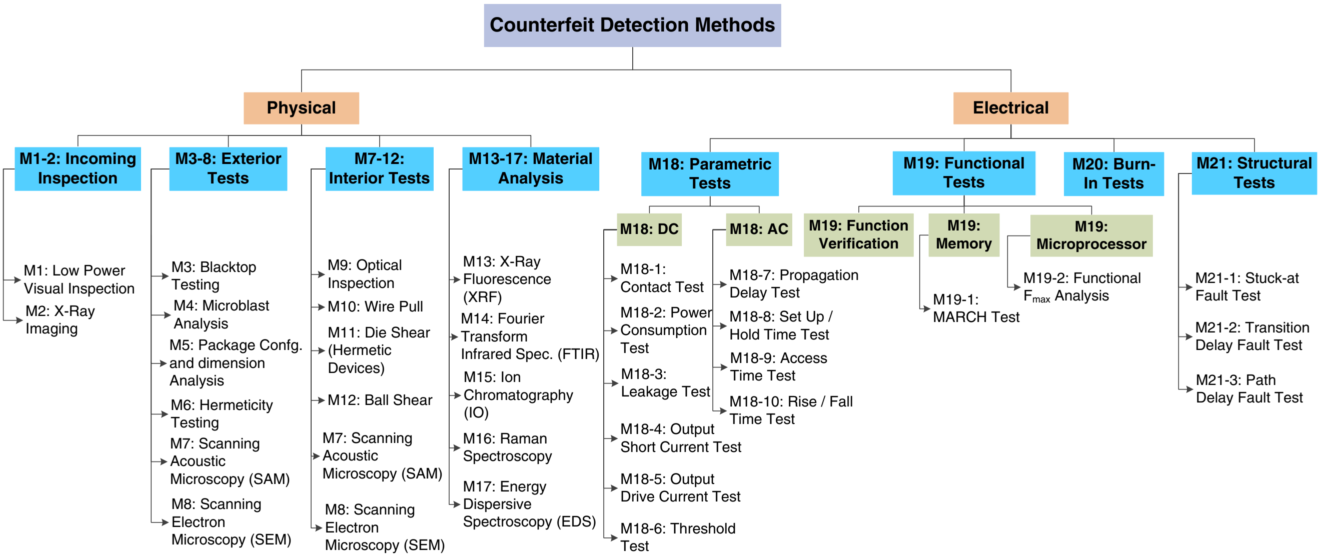

Counterfeit Detection Methods
Physical
Electrical
M1-2: Incoming Inspection
M3-8: Exterior Tests
M7-12: Interior Tests
M13-17: Material Analysis
M18: Parametric Tests
M19: Functional Tests
M20: Burn-In Tests
M21: Structural Tests
M1: Low Power Visual Inspection
M2: X-Ray Imaging
M3: Blacktop Testing
M4: Microblast Analysis
M5: Package Confg. and dimension Analysis
M6: Hermeticity Testing
M7: Scanning Acoustic Microscopy (SAM)
M8: Scanning Electron Microscopy (SEM)
M9: Optical Inspection
M10: Wire Pull
M11: Die Shear (Hermetic Devices)
M12: Ball Shear
M7: Scanning Acoustic Microscopy (SAM)
M8: Scanning Electron Microscopy (SEM)
M13: X-Ray Fluorescence (XRF)
M14: Fourier Transform Infrared Spec. (FTIR)
M15: Ion Chromatography (IO)
M16: Raman Spectroscopy
M17: Energy Dispersive Spectroscopy (EDS)
M18: DC
M18: AC
M18-1: Contact Test
M18-2: Power Consumption Test
M18-3: Leakage Test
M18-4: Output Short Current Test
M18-5: Output Drive Current Test
M18-6: Threshold Test
M18-7: Propagation Delay Test
M18-8: Set Up / Hold Time Test
M18-9: Access Time Test
M18-10: Rise / Fall Time Test
M19: Function Verification
M19: Memory
M19: Microprocessor
M19-1: MARCH Test
M19-2: Functional F$_{max}$ Analysis
M21-1: Stuck-at Fault Test
M21-2: Transition Delay Fault Test
M21-3: Path Delay Fault Test

Fig. 2 A taxonomy of counterfeit detection methods

and other anomalies will be detected by this method. (iii) *Interior Tests*: The interior tests are used to detect the internal defects and anomalies related to die and bond wires. For interior tests, one needs to decapsulate/delid the chip first. The inspection of the internal structure, top surface of a die, bond wires, or metallization traces etc., of an electronic component are performed. The integrity of the bonds with the die is tested using the wire pull test. Die attach integrity is verified by using a die shear test. A ball shear test is applied to verify the ball bond integrity at the die. In scanning electron microscopy (SEM), the images of die, package, or leads are taken by scanning it with a focused beam of electrons. If there is an anomaly present in it, it can easily be detected by SEM. (iv) *Material Analysis*: The chemical composition of the component are verified using material analysis. The defects related to the materials of the package and leads are tested by using these methods. This category includes X-Ray fluorescence (XRF), energy dispersive x-ray spectroscopy (EDS), Fourier transform infrared spectroscopy (FTIR), etc.

Electrical test methods are mostly applied to verify the correct functionality and performance of a component. Common electrical tests include: (i) *Parametric Tests*: These tests are performed to measure the electrical parameters of a chip [5, 31, 38]. During the counterfeiting process (recycling, remarking, etc.) the DC and AC parameters of the component may shift from its specified value (mentioned on the datasheet). After observing test results from a parametric test, a decision can be made as to whether or not a component is counterfeit. Detailed descriptions of each test can be found in [5]. (ii) *Functional Tests*: Functional tests are the most efficient way of verifying the functionality of a component. MARCH tests [5, 27, 41] can be applied for counterfeit detection. Functional f_{max} analysis can be implemented to detect counterfeit microprocessors. (iii) *Burn-In Tests*: The device is operated at an elevated temperature to simulate a stress condition to find infant mortality failures and unexpected failures to assure reliability [10, 11], and (iv) *Structural Tests*: Structural tests are designed to detect the manufacturing defects efficiently using scan structure [12, 13, 37]. It can be useful to detect the defects present in out-of-spec/defective counterfeit components if the access to scan chains in digital ICs is provided and the netlist for the circuit is given.

3 Counterfeit Defects

The detection of a counterfeit component is a complex problem that requires a comprehensive assessment of all currently available detection methods. To achieve this, in this section, we present a detailed taxonomy of the defects and anomalies present in the counterfeit parts (described in Section 2). The objective of developing this taxonomy is to evaluate each test method presented in Section 2.2 based upon their capability of detecting defects. Figure 3 presents the classification of these defects identified in all different counterfeit types. The defects are broadly classified into two categories, physical and electrical.

3.1 Physical Defects

Physical defects are directly related to the physical properties of the components. They can be classified as exterior and interior defects depending on the location of the defect related to the packaging. They are classified as follows.

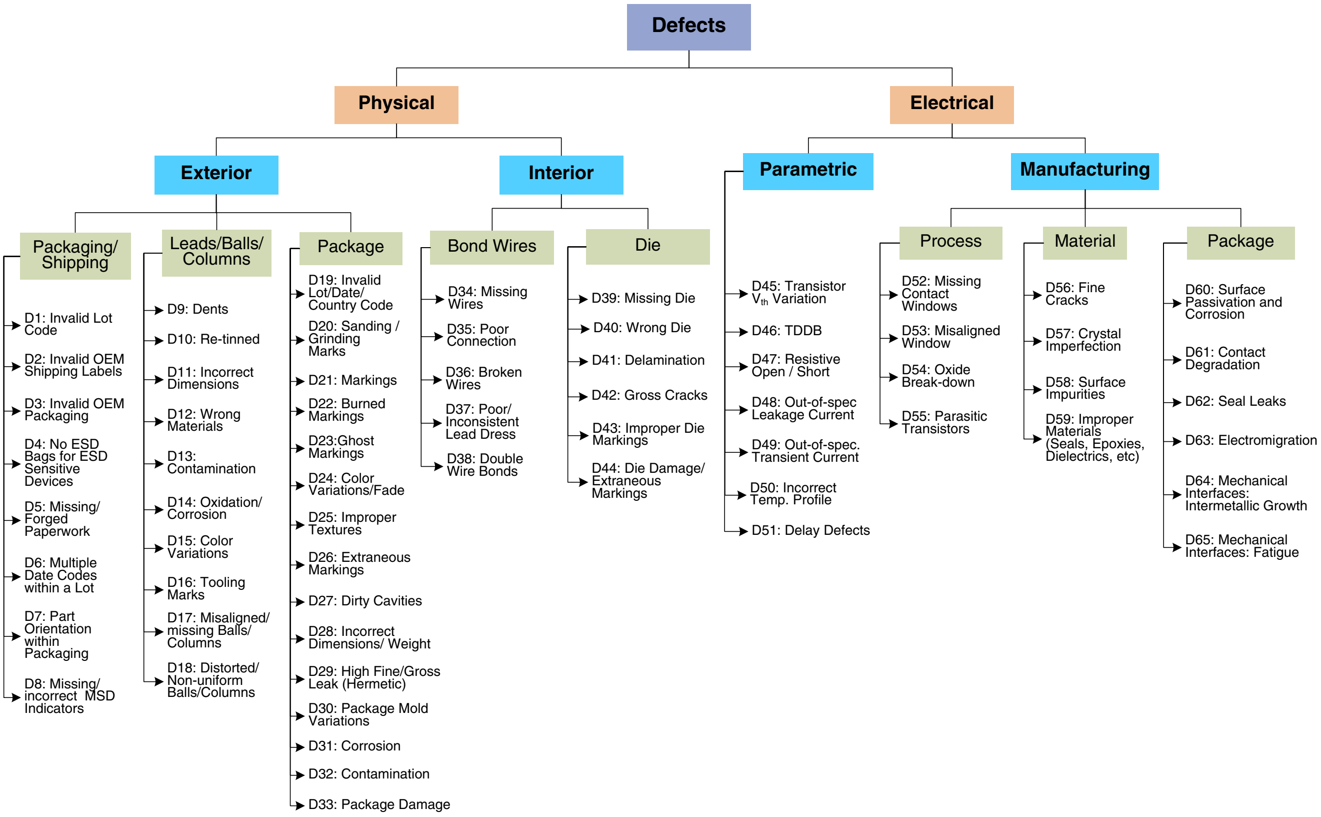

Defects
Physical
Electrical
Exterior
Interior
Parametric
Manufacturing
Packaging/ Shipping
Leads/Balls/ Columns
Package
Bond Wires
Die
Process
Material
Package
D1: Invalid Lot Code
D2: Invalid OEM Shipping Labels
D3: Invalid OEM Packaging
D4: No ESD Bags for ESD Sensitive Devices
D5: Missing/ Forged Paperwork
D6: Multiple Date Codes within a Lot
D7: Part Orientation within Packaging
D8: Missing/ incorrect MSD Indicators
D9: Dents
D10: Re-tinned
D11: Incorrect Dimensions
D12: Wrong Materials
D13: Contamination
D14: Oxidation/ Corrosion
D15: Color Variations
D16: Tooling Marks
D17: Misaligned/ missing Balls/ Columns
D18: Distorted/ Non-uniform Balls/Columns
D19: Invalid Lot/Date/ Country Code
D20: Sanding / Grinding Marks
D21: Markings
D22: Burned Markings
D23:Ghost Markings
D24: Color Variations/Fade
D25: Improper Textures
D26: Extraneous Markings
D27: Dirty Cavities
D28: Incorrect Dimensions/ Weight
D29: High Fine/Gross Leak (Hermetic)
D30: Package Mold Variations
D31: Corrosion
D32: Contamination
D33: Package Damage
D34: Missing Wires
D35: Poor Connection
D36: Broken Wires
D37: Poor/ Inconsistent Lead Dress
D38: Double Wire Bonds
D39: Missing Die
D40: Wrong Die
D41: Delamination
D42: Gross Cracks
D43: Improper Die Markings
D44: Die Damage/ Extraneous Markings
D45: Transistor V_{th} Variation
D46: TDDB
D47: Resistive Open / Short
D48: Out-of-spec Leakage Current
D49: Out-of-spec. Transient Current
D50: Incorrect Temp. Profile
D51: Delay Defects
D52: Missing Contact Windows
D53: Misaligned Window
D54: Oxide Break-down
D55: Parasitic Transistors
D56: Fine Cracks
D57: Crystal Imperfection
D58: Surface Impurities
D59: Improper Materials (Seals, Epoxies, Dielectrics, etc)
D60: Surface Passivation and Corrosion
D61: Contact Degradation
D62: Seal Leaks
D63: Electromigration
D64: Mechanical Interfaces: Intermetallic Growth
D65: Mechanical Interfaces: Fatigue

Fig. 3 A taxonomy of defects and anomalies present in counterfeit electronic components

1) **Exterior Defects**: Exterior defects are classified into three major categories:

   (i) *Packaging/Shipping*: The most obvious defects will be ones that are associated with the packaging or shipping. An invalid lot code should be a red flag that the part is a counterfeit. This code should be checked with the OCM or OEM to ensure that it is authentic. OEMs and OCMs both have their own shipping labels and packaging with company logos and other relevant information. If any of this is invalid or missing then the component is likely forged. If an electrostatic discharge (ESD) sensitive device ships without any ESD protection then it is a sign that the distributor does not do much quality control, and it is also likely that the counterfeit part can come from them. Similarly, if a moisture sensitive device (MSD) is shipped without any MSD indicators, it may be a clear indication that it is a suspect part. Multiple date codes within a lot may also lead an entire lot to be counterfeited. Large orders of parts will either ship with test results or have them available for review from the OCM. If these are missing or appear forged, the parts should be flagged for further review.

   (ii) *Leads/Balls/Columns*: The leads can provide much information about the IC, e.g., whether it was previously used, cloned, etc. Physically, leads should adhere to datasheet specifications, including straightness, pitch, separation, etc. The final coating on the leads should be consistent throughout the entire lot as well. Leads should also have a consistent elemental construction. Defects due to wrong materials would be use of the incorrect material. For example, if a part plating was supposed to be nickel and it is actually tin, then the wrong material was used. If there is contamination, then the plating may be correct, but it has organics all over it. The color variations of the lead may also be a sign of counterfeiting. If some leads appear to have a darker or duller finish, it could be a sign that they have been soldered or removed from a previous printed circuit board. There may be oxidation/corrosion on the lead due to the harsh recycling process. Missing tool marks on the lead may be an indication of a used component as the replating covers those tool marks during recycling. Finally, distorted/misaligned/non-uniform balls and columns indicate a counterfeit part.

(iii) *Package*: The package of an IC can reveal significant information about the authenticity of a chip. As this is the location where all model numbers, country of origin, date codes, and other information are etched, counterfeiters will try to be especially careful not to damage anything and keep the package looking as authentic as possible. Any invalid date/lot/country codes are an indicator that the part is counterfeit. If the package exhibits any external sanding or grinding marks, it has likely been remarked. The labels that are on the package should be permanent and clean. The markings on a counterfeit part may be crooked, uneven, or sloppy. The imprecise laser may also hover over spots too long and cause burn marks on the package. There are even cases of misprinted company logos being printed on parts. Ghost markings, color variations, improper textures, and extraneous marking on the package all give a clear indication of a reused or remarked component.

Cavities in the package are a part of the manufacturing process. Components that have the same lot codes should all have cavities located in the same positions. These cavities should not have any markings or laser-etched lettering in them. The edges around the cavity should be sharp and precise. If the edges seem to be rounded down, it may be an indication that the package was sanded down for remarking. Also along those lines, the package itself should be compared against the datasheet for dimensions, including weight. A more complicated defect deals with components that are hermetically sealed. The seal on such component ensures the it's correct operation in the environment that it was designed to operate in. A break in this seal lead to the failure of the component. The seal of a hermetic part can be broken by excessive force or heat, both typical of a crude recycling process. The final exterior defect includes corrosion and contamination on the package.

2) **Interior Defects**: Interior defects can be mainly divided into two types: bond wire or die-related defects. These defects are located inside the package.

(i) *Bond Wires*: The inside of an integrated circuit contains a die and bond wires in case of wire-bond packaging. If a bond wire is missing or broken, the circuit will fail during functional operation. In defense grade chips, multiple wires are normally used for a single connection. A missing wire could result in reduced reliability. Poor connection is a type of latent defect, where the component may work normally for a while before the user experiences any kind of degradation in performance. If under enough environmental stress or if exposed to a large shock (ESD, for example) the wire itself may be completely burnt-out. Components that have gone through the recycling process may have been so mishandled that the connection from the bond wire to the die is broken. When die recovery occurs and the die is lifted from one package and repackaged, the counterfeiters re-ball leaving double ball bonds. Double ball bonds are allowed up to certain amounts for rework, but when all are double bonded the part is likely counterfeited by die recovery.

(ii) *Die*: The missing die defect represents the absence of a die inside the package of a component. Wrong die occurs when the die is different than what it is expected to be. Due to imperfections of fabrication, a die may contain trace amounts of air between layers of the die. When heated, these pockets will expand. If there is enough air present, the die pocket will expand to the point of delaminating and adjacent connected layers will separate. This is known as "popcorning" due to the resemblance. This defect is referred to as delamination. A component that has gone through a crude recycling process is subject to extreme changes in temperature and harsh environments that it was not designed to withstand. If gross cracks exist in the die, then the defects come under gross crack category. There are markings on the die that can help in proving authenticity when compared to the package markings. If an inconsistency is present, the defect belongs to improper die markings. The die can also be damaged during the recycling process.

3.2 Electrical Defects

A defect in an electronic system is the difference between the implemented hardware and its intended design and specification [5]. Typical electrical defects in a counterfeit IC can be classified into two distinct categories. They are parametric defects and manufacturing defects.

1) **Parametric Defects**: Parametric defects are the manifestation of a shift in component parameters due to prior usage or temperature. A shift in circuit parameters due to aging will occur when a chip is used in the field for some time. The aging of a chip used in the field

can be attributed to four distinct phenomenon which are becoming more prevalent as feature size shrinks. The most dominant phenomena are negative bias temperature instability (NBTI) [1, 2, 33, 36, 51] and hot carrier injection (HCI) [8, 26, 28, 51] which are prominent in PMOS and NMOS devices, respectively. NBTI occurs in p-channel MOS devices stressed with negative gate voltages and elevated temperatures due to the generation of interface traps at the Si/SiO_2 interface. Removal of the stress can anneal some of the interface traps, but not completely. As a result, it manifests as the increase of threshold voltage (V_{th}) and absolute off current (I_{off}) and the decrease of absolute drain current (I_{DSat}) and transconductance (g_m). HCI occurs in NMOS devices caused by the trapped interface charge at Si/SiO_2 surface near the drain end during switching. It results in nonrecoverable V_{th} degradation. These effects also lead to out-of-spec leakage current and out-of-spec transient current. Delay defects are also the direct effect all the parametric variations mentioned above.

Time-dependent dielectric breakdown (TDDB) [15, 39] is an another effect of aging which irreparably damages the MOS devices. The MOS devices with very thin oxide layers are generally subjected to a very high electric field. The carrier injection with this high electric field leads to a gradual degradation of the oxide properties, which eventually results in the sudden destruction of the dielectric layer. Finally, electromigration [3], mass transport of metal film conductors stressed at high current densities, may cause a device to fail over time. If the two interconnects are close enough, the atoms migrate and that leads to bridging between these interconnects. This may also lead to an open interconnect due to the apparent loss of conductor metal.

2) **Manufacturing Defects**: The defects under this category come from the manufacturing process. These defects are classified into three categories - process, material, and package.

   (i) *Process*: The defects under this category come from the photolithography and etching processes during fabrication. The misalignment of photomasks and over or under etching results in process defects. Missing metal-to-polysilicon windows causes the transistor gate to float. The misaligned windows also affect the current carrying capability. Due to the over-etched and misaligned contact windows, parasitic transistor action may occur between adjacent devices. Electric charge buildup takes place between the two adjacent diffusions under a sufficient electric field to revert the layer to a conducting channel and the device fails.

   (ii) *Material*: These are the defects that arise from impurities within the silicon or oxide layers. Crystalline defects in silicon changes the generation-recombination of carriers and eventually results in the failure of the device. Crystal imperfections, surface impurities, and improper materials come under this category. Fine cracks in the material are also added to this category.

   (iii) *Package*: The passivation layer provides some form of protection for the die. Failure occurs when corrosion causes cracks or pin holes in the passivation layer. The aluminum layer can easily be contaminated with the presence of sodium and chloride and results in an open circuit. The defects in metallization often result from electromigration. Intermetallic growth and fatigue in the bond and other mechanical interfaces are also results from the metal impurities and temperature, and they cause the device to fail. Finally, seal leaks are added to this category.

4 Assessment and Selection of Counterfeit Detection Methods

The detection of counterfeit electronic components is still in its infancy, and there are major challenges that must be overcome in order to deploy 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 by increasing confidence level in detecting counterfeit components. To achieve this, current test technologies must be comprehensively assessed and their effectiveness must be carefully evaluated. One set of tests may be effective at detecting counterfeit defects in a specific type of component (e.g., microprocessors, memories, etc.) but this same set of tests may not extend to other component types or components. In this section, we will assess the available methods for detecting different counterfeit components and types.

The physical methods can be applied to all component types. However, some of the methods (e.g., interior methods, $M8 - 12$) are destructive and take hours to run. As a result, such tests are done on a sample of components. On the other hand, electrical methods are nondestructive and time efficient compared to physical tests. No sampling is required and all the parts can be tested. However, electrical tests do not target all types of components uniformly, e.g., the test sets for functional verification of an analog chip is completely different than its digital counterpart.

Table 1 Assessment of counterfeit detection methods

Test Methods	Counterfeits			
	Recycled/Remarked[1]	Overproduced[2]	Out-of-spec/Defective	Cloned[2]
M1: Low Power Visual Inspection (LPVI)	D1-10, D15 -16, D19 -27, D30, D33	D1-8	D1-9	D1-8
M2: X-Ray Imaging	D17-18, D33-44	NA	D17-18, D35 -37, D41-44	D40-44
M3: Blacktop Testing	D20-26	NA	NA	NA
M4: Microblast Analysis [3]	D20-26	NA	NA	NA
M5: Package Configuration and Dimension Analysis	D11, D28	NA	D11, D28	NA
M6: Hermeticity Testing	D29, D62	D29, D62	D29, D62	D29, D62
M7: Scanning Acoustic Microscopy (SAM)	D9, D17-18, D33-44	NA	D17-18, D33 -37, D41-44	D40-44
M9: Optical Inspection	D33-40, D42 -44, D64	D35, D64	D33-40, D42 -44, D64	D40, D42-44
M10: Wire Pull	D35, D65	D35, D65	D35, D65	D35, D65
M11: Die Shear	D41	D41	D41	D41
M12: Ball Shear	D17-18	NA	D17-18	NA
M8: Scanning Electron Microscopy (SEM)	D19-27, D30 -31, D39-40, D42-44	NA	D42-44	D40, D42-44
M13: X-Ray Fluorescence (XRF)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M14: Fourier Transform Infrared Spectroscopy (FTIR)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M15: Ion Chromatography (IO)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M16: Raman Spectroscopy	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M17: Energy Dispersive X-Ray Spectroscopy (EDS)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M18: Parametric Tests	D33-36, D38 -40, D42, D45 -50, D56	D45-50	D33-36, D38 -40, D42, D45 -50, D56	D40, D42, D45-50, D56
M19: Functional Tests	D33-36, D38 -40, D42, D51 -56, D61, D63 -65	D51-56,D61, D63-65	D33-36, D38 -40, D42, D51 -56, D61, D63 -65	D42, D51 -56, D61, D63-65
M20: Burn-In Tests	D34-42, D50 -51, D53-54, D56, D61, D63-65	D50-51, D53-54, D56, D61, D63-65	D34-42, D50 -51, D53-54, D56, D61, D63-65	D40-42, D50 -51, D53-54,D56, D61, D63-65
M21: Structural Tests	D34-42, D47, D51-56	D47, D51-56	D34-42, D47, D51-56	D40-42, D47, D51-56

[1] The recycled and remarked parts are highly correlated. Remarking is a part of recycling. Thus, remarked parts can be recycled. Also, remarking for new parts to change the specifications involves recycling

[2] We can only detect overproduced, and cloned counterfeit types if there are counterfeit defects present in them

[3] After microblasting, the materials are collected and send to material analysis

Table 1 shows our comprehensive assessment of all test methods. Column 1 presents the test methods (from Fig. 2). Columns 2 to 6 present counterfeit types (from Fig. 1). The entries in Columns 2 to 6 list all the possible defects (discussed in Section 3) that the methods can detect. Here we use the defect numbers $Di - j$ instead of mentioning their complete names. For example, low-power visual inspection (LPVI) can detect all packaging/shipping defects ($D1 - 8$). In addition, the majority of defects from leads/balls/columns and package ($D9 - 10$, $D15 - 16$, $D19 - 27$, $D30$, and $D33$) can be detected by this test method. These defects are present mostly in the recycled, and remarked counterfeit types. Defects $D1 - 8$ are present in other counterfeit types (overproduced, out-of-spec/defective, and cloned). The package configuration and dimension analysis method can detect all the dimension-related defects of leads/balls/columns and package ($D11$ and $D28$). These defects are probably not present in the overproduced and cloned counterfeit types. That is the reason we put NA in the corresponding fields. We can proceed with the same description for rest of the test methods. This table has been reviewed by industry experts and the members of G19-A committee. Based on this assessment, we will construct a confidence level matrix in the following, which is the building block of our method selection algorithm.

4.1 Method Selection Algorithm

The detection of counterfeit components is a multifaceted problem, and it requires a set of detection methods to certify a component as genuine with a desired level of confidence. We will introduce counterfeit defect coverage (*CDC*) to represent the level of confidence for detecting a counterfeit component after performing a set of tests. In this section, we will develop a algorithm to find the optimum set of detection methods that will maximize *CDC* while considering the constraints on test time, cost, and application risks.

Table 2 presents the terminologies and their matrix notation. Matrix M denotes the complete set of test methods currently available for counterfeit detection. m and n represent the number of test methods and defects, respectively. The vector C and T represent the normalized value of test cost and time, where $\sum_{i=1}^{m} c_i = 100$ and $\sum_{i=1}^{m} t_i = 100$. The vector *AR* stands for application risk. We have considered application risk in five distinct types – critical, high, medium, low, and very low from SAE G19-A. We have assigned a value (0 to 100: *AR*=[0.95 0.85 0.75 0.65 0.55], critical=0.95,..., very low=0.55) to each application risk, where a higher value stands for a higher application risk.

Percent counterfeit component (*PCC*) represents the reported percent of counterfeit components present in the supply chain. This data will be available through the Government Industry Data Exchange Program (GIDEP) since the Government requires all test labs, OCMs, and OEMs to report all counterfeit incidents [14, 45]. A current report shows that around 80 % of components belong to recycled and remarked counterfeit types [21]. The counterfeit defect matrix (*CD*) represents the defects associated with each counterfeit type. The rows and columns of *CD* are the defects and counterfeit types, respectively. Each entry d_{ij} would be 1 if a defect for a counterfeit type is present, otherwise this entry would be 0. Defect frequency (*DF*) is defined as how frequently the defect is visible in the supply chain. Defect frequency is one of the key parameters for evaluating counterfeit defect coverage, as the detection of high frequency defects impacts CDC significantly.

Table 2 Terminologies used in our proposed method selection algorithm

Terminology	Matrix Notation[a]
Test Methods	$M = [M_1\ M_2\ \dots\ M_m]^T$ $M_i \in \{0, 1\} = \{\text{Not Selected, Selected}\}$
Test Cost	$C = [c_1\ c_2\ \dots\ c_m]^T$, where $\sum_{i=1}^{m} c_i = 100$
Test Time	$T = [t_1\ t_2\ \dots\ t_m]^T$, where $\sum_{i=1}^{m} t_i = 100$
Counterfeit Defects	$D = [D_1\ D_2\ \dots\ D_n]^T$
Application Risks	$AR = [AR_1\ AR_2\ \dots\ AR_5]^T$, AR_1: Critical, AR_2: High, AR_3: Medium AR_4: Low, AR_5: Very Low
Percent Counterfeit Component	$PCC = [p_1\ p_2\ \dots\ p_7]^T$ p_1: Recycled, p_2: Remarked, ..., p_7: Tampered
Counterfeit Defect Matrix	$CD = \begin{bmatrix} d_{11} & d_{12} & \dots & d_{17} \\ d_{21} & d_{22} & \dots & d_{27} \\ \vdots & \vdots & \vdots & \vdots \\ d_{n1} & d_{n2} & \dots & d_{n7} \end{bmatrix}$, where $d_{ij} \in \{0, 1\}$ ={Not Present, Present} And rows and columns represent defects and counterfeit types respectively.
Defect Frequency	$DF = CD * PCC^T$
Target Defect Confidence Level	$DC = [DC_1\ DC_2\ \dots\ DC_n]^T = AR[i] * DF$

[a] $[.]^T$ represents the transpose of a matrix [.]

Defect frequency depends on the counterfeit types and is the matrix multiplication of the counterfeit defect matrix (*CD*) and the percent counterfeit component (*PCC*). The calculation of defect frequency is a one-time task. Once the system is in place, the test results, depending on the type of defects present in the counterfeit component, will update *DF*. The application risk has been incorporated into our technique by introducing a target defect confidence level (*DC*) for each defect. This is basically the multiplication of the application risk and the defect frequency for each defect. For high-risk applications, the value of *DC* for a counterfeit defect will be higher compared to low-risk applications at a fixed *DF*. Based on *DC*, we will develop under-covered defects (*UCDs*), one of our proposed assessment metrics.

One of the important pieces of data used in our test selection technique is the defect confidence level matrix (X), which is defined as:

$$X = \begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ m \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \dots & n \end{array} \\ \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix} \end{array}$$

where the rows $(1, 2, .., m)$ and columns $(1, 2, .., n)$ are denoted as the methods and defects, respectively. Each entry of the matrix X represents the defect detection capability of a method, i.e., the confidence level of detecting a defect by a test method. This matrix is generated with the help of G-19A group members. Once this model is implemented, each entry of the X matrix will be updated with the test results.

If two or more methods detect the same defect then the resultant confidence level will be increased and is given by the following equation,

$$x_{Rj} = 1 - \prod_{i=1}^{m_s} \left(1 - x_{ij}\right) \quad \text{for defect } j \tag{1}$$

where m_s represents the number of tests in the recommended test set.

To evaluate the effectiveness of these test methods, it is of utmost importance to develop a test metric that represents coverage for detecting counterfeit defects. They are described as follows:

(i) *Counterfeit Defect Coverage*: Counterfeit defect coverage (CDC) is defined as the resultant confidence level of detecting a component as counterfeit after performing a set of tests, and it is presented by the following equation:

$$CDC = \frac{\sum_{j=1}^{n} (x_{Rj} \times DF_j)}{\sum_{j=1}^{n} DF_j} \times 100\ \% \tag{2}$$

The counterfeit defect coverage cannot assess total risks alone. We have introduced two types of defects – not-covered defects (*NCD*) and under-covered defects (*UCD*) – for better assessment of the test methods.

(ii) *Not-Covered Defects*: Defects are called *NCD*s when a set of recommended tests cannot detect them. A counterfeit defect *j* will be a *NCD* if $x_{Rj} = 0$ after performing a set of tests.

(iii) *Under-Covered Defects*: Defects are called *UCD*s when a set of recommended tests cannot provide the desired confidence level. The defects belong to this category when the resultant confidence level is less than the target defect confidence level. Thus the required condition for a defect *j* to be a *UCD* when,

$$x_{Rj} < DC_j \tag{3}$$

The objective of method selection algorithm is to find an optimum set of methods to maximize counterfeit defect coverage while considering the constraints of test time, cost, and application risk. A counterfeit defect can be detected by multiple methods with different levels of confidence. Thus, the problem becomes the selection of most suitable methods to achieve the highest CDC considering these constraints. The problem can be formulated as:

Select a set of methods $M^S \subset M$ to Maximize CDC
Subjected to:

$$x_{Rj} \geq DC_j,\ \forall\, j \in \{1:n\} \text{ for critical applications}$$

or

$$\begin{cases} M_1c_1 + M_2c_2 + \ldots + M_mc_m \leq c_{user} & \text{for non-critical} \\ M_1t_1 + M_2t_2 + \ldots + M_mt_m \leq t_{user} & \text{applications} \end{cases}$$

Algorithm 1 describes the proposed method selection. It starts with initializing the recommended test set to null. It then calculates the defect frequency (*DF*) and the target defect confidence level (*DC*). It then prioritizes the defects by sorting according to *DF*, as we want to capture high-frequency defects first to achieve a higher *CDC* and reduce the total test cost and time.

Algorithm 1 Proposed method selection

```
Initialize selected methods, $M^S \leftarrow \{\phi\}$
Specify cost limit set by the user $c_{user}$ except for critical risk applications
Specify test time limit set by the user $t_{user}$ except for critical risk applications
Specify application risk, $AR_k \leftarrow$ user application risk
Calculate defect frequency, $DF \leftarrow$ CALCULATE($DC$, $PCC$)
Calculate defect confidence level, $DC \leftarrow AR_k * DF$
Sort defects according to defect frequency, $D \leftarrow$ SORT ($DF$)
if (application risk = critical) then
    for (all defect index $j$ from 0 to $n$ in $DC$) do
        Sort methods according to $x_{ij}$, $M' \leftarrow$ SORT ($M$, $X$)
        Calculate $x_{Rj}$, $x_{Rj} \leftarrow$ CALCULATE ($X$, $M'$)
        for (all method index $i$ from 0 to $m$ in $M'$)) do
            SELECTMETHODS ($X$, $M'$, $x_{Rj}$, $DC_j$)
        end for
    end for
else
    for (all defect index $j$ from 0 to $n$ in $DC$) do
        Sort methods according to test time and cost, $M' \leftarrow$ SORT ($M$, $T$, $C$)
        Calculate $x_{Rj}$, $x_{Rj} \leftarrow$ CALCULATE ($X$, $M'$)
        for (all method index $i$ from 0 to $m$ in $M'$)) do
            SELECTMETHODS ($X$, $M'$, $x_{Rj}$, $DC_j$, $t_{user}$, $c_{user}$)
        end for
    end for
end if
Report $M^S$ and $CDC$, $NCD$s and $UCD$s
```

For critical risk applications, our primary objective is to obtain the maximum *CDC* irrespective of test cost and time.

On the other hand, for low and very low risk applications, test time and cost are more important than getting the maximum *CDC*. For medium- and high-risk applications, we can get a higher confidence level by setting a higher test time and cost limit. For critical applications, SORT() function (line 10) takes *M* and *X* as arguments and sorts them according to x_{ij} and discards the method *i* when $x_{ij} = 0$. Equation 1 has been implemented by CALCULATE() function (line 11). The SELECTMETHODS() function (line 13) takes x_{Rj} and DC_j as argument and selects methods until the condition $x_{Rj} > DC_j$ is met. If this condition is not met after iterating all the methods, then the defects belong to the *UCDs* and *NCDs*. For other applications, the SORT() function (line 18) takes *M*, *T*, and *C* as arguments and sorts according to linear combinations of t_i and c_i ($0.5t_i$+$0.5c_i$) and discards the method *i* when $x_{ij} = 0$. The resultant confidence level has been calculated by CALCULATE() function (line 19) by implementing (1). The SELECTMETHODS() function (line 21) takes x_{Rj}, DC_j, t_{user}, and c_{user} as argument and selects the methods that require the minimum test time and cost to achieve $x_{Rj} > DC_j$.

5 Results

The simulation results focus on the assessment of test methods based on the current level of expertise existing in the field of counterfeit detection. The proposed method selection algorithm is implemented in a C/C++ environment. We have accumulated the data for the confidence level matrix (*X*), test cost (*C*), and test time (*T*) from various test labs and subject matter experts in collaboration with G-19A. We have assumed that the test cost and time are constant for all the applications from critical to very low for a counterfeit detection method. In this section we will present the simulation results that correspond to this information received from two test labs for the comparison study. Because of the confidentiality agreement we will only present the normalized value of the above test cost, time and confidence level information.

Figure 4 shows the change of *CDC* with the increase in the number of methods. In this experiment, we have considered critical risk applications as it provides the maximum *CDC* irrespective of test time and cost. The x-axis represents the number of methods in the recommended test set. The first few methods detect a majority of defects, and the coverage increases rapidly. We can achieve a coverage (*CDC*) of around 73 % from the first four methods. As the number of methods increases, the rate of increase goes down and eventually reaches to 93.5 % for *Test Lab1* and 95 % for *Test Lab1*. From the graph, it is clear that the capabilities of the two labs are similar. However, *Test Lab2* provides a slightly higher *CDC* compared to *Test Lab1*.

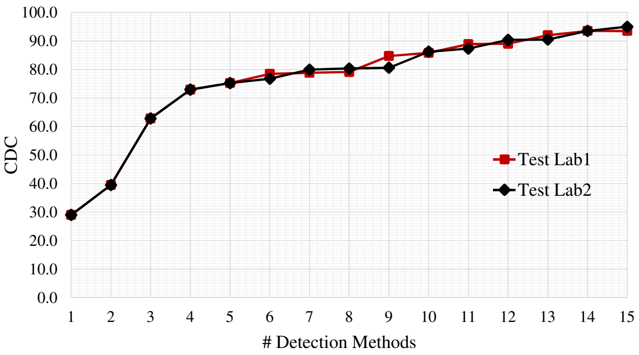


Fig. 4 Counterfeit defect coverage vs. number of counterfeit detection methods (see the sequence in Table 3)

Table 3 shows the recommended test set for critical applications. We will first describe ten methods for comparing the capabilities of *Test Lab1* and *Test Lab2*. The first method is low-power visual inspection (LPVI) as it detects a majority of the exterior physical defects that is common to both labs. The second recommended method is scanning electron microscopy (SEM), which mostly detects interior physical defects. The third and fourth methods are functional and parametric tests. A majority of electrical defects can be detected by these two methods. The recommended test set for *Test Lab1* and *Test Lab2* is similar except for the structural tests which result in the increased *CDC* for *Test Lab2*. To achieve a higher test confidence, we need to focus on developing new test methods with better defect detection capability. It is also important to balance the tests in the physical and electrical categories uniformly to cover most (all if possible) of the defects.

Figure 5 shows the recommended set of tests for low and high risk applications. We have arbitrarily selected *Test Lab2* to find the recommended test set. For low risk application, we consider test time and cost of 15 units each. The incoming components under tests first go through *low power visual inspection*, then *functional tests*, *parametric tests*, *X-Ray imaging*, *X-Ray fluorescence*, and finally *package configuration and dimension analysis*. For high risk application, we relax the test cost and time constraint to 50 units each. It is clear from the Fig. 5 that there are few tests, (e.g., *scanning electron microscopy*, *structural tests*, etc.) added to the recommended list. The test results i.e., *CDC*, *NCDs* and *UCDs* are shown in the successive figures.

Figure 6 shows the counterfeit defect coverage versus user specified test time and cost for high risk application. The test time and cost axis represent the normalized value of user specified test time and cost, not the actual hour and dollar value. We have considered equal test time and cost in the x-axis for this simulation. It is clear from the figure that the test coverage rises rapidly with test cost and time, as the first few low-cost tests detect a majority of defects from the

Table 3 Recommended set of tests

Test Sequence	Test Lab1	Test Lab2
1	M1: Low Power Visual Inspection (LPVI)	M1: Low Power Visual I nspection (LPVI)
2	M8: Scanning Electron Microscopy (SEM)	M8: Scanning Electron Microscopy (SEM)
3	M19: Functional Tests	M19: Functional Tests
4	M18: Parametric Tests	M18: Parametric Tests
5	M20: Burn-In Tests	M20: Burn-In Tests
6	M2: X-Ray Imaging	M21: Structural Tests
7	M9: Optical Inspection	M2: X-Ray Imaging
8	M3: Blacktop Testing	M9: Optical Inspection
9	M17: Energy Dispersive X-ray Spectroscopy (EDS)	M3: Blacktop Testing
10	M13: X-Ray Fluorescence (XRF)	M17: Energy Dispersive X-ray Spectroscopy (EDS)
⋮	⋮	⋮

defect taxonomy (described in Fig. 4). However, the performance of *Test Lab2* is better than *Test Lab1* in a lower time and cost range as the *CDC* reaches to around 70 % at a cost and time of 2.5 unit each, whereas the *CDC* for *Test Lab1* reaches that limit at a cost and time of 11.5 unit each. After that the performance of both labs becomes similar. We cannot achieve a *CDC* of more than 95 % for *Test Lab2* and 93.5 % for *Test Lab1*, even with infinite time and money, as it reaches an upper bound.

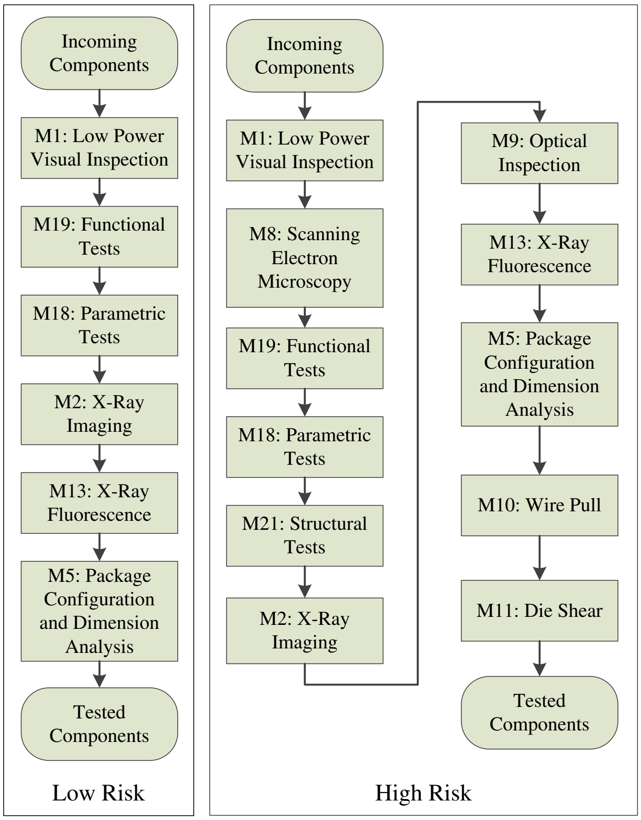


Fig. 5 Test sequence for low and high risk application

Figure 7 shows how *CDC* varies with the test cost and time while considering application risks. The time and cost values are arranged in increasing fashion, such as, $C1 < C2 < C3 < C4$ and $T1 < T2 < T3 < T4$. The pair $\{Ci, Ti\}$ is used as the user specified cost and time when running the algorithm. The $\{Ci, Ti\}$ value pair is constant for all application types during this simulation. In this simulation, We have considered C = [15(C1) 30(C2) 50(C3) 70(C4)] and T = [15(T1) 30(T2) 50(T3) 70(T4)]. The labels on the graph represent [K H M L V] = [Critical High Medium Low Very Low] as five different application risks. The *CDC*s for both labs are constant for critical risk applications as the algorithm does not consider user specified cost and time. From the graph, it is clear that the *CDC* does not vary significantly for other risk applications as we consider the same test cost and time for all the applications for a detection method. However, it increases as we relax the test cost and time constraints (allow more time and expense).

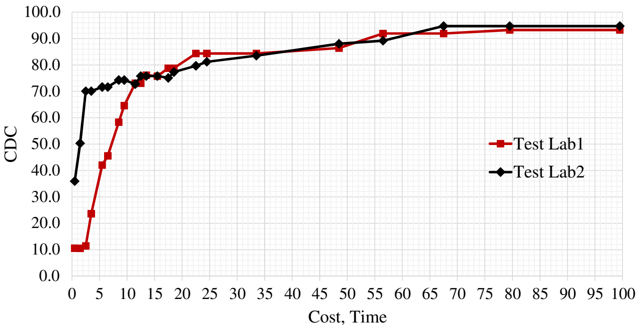
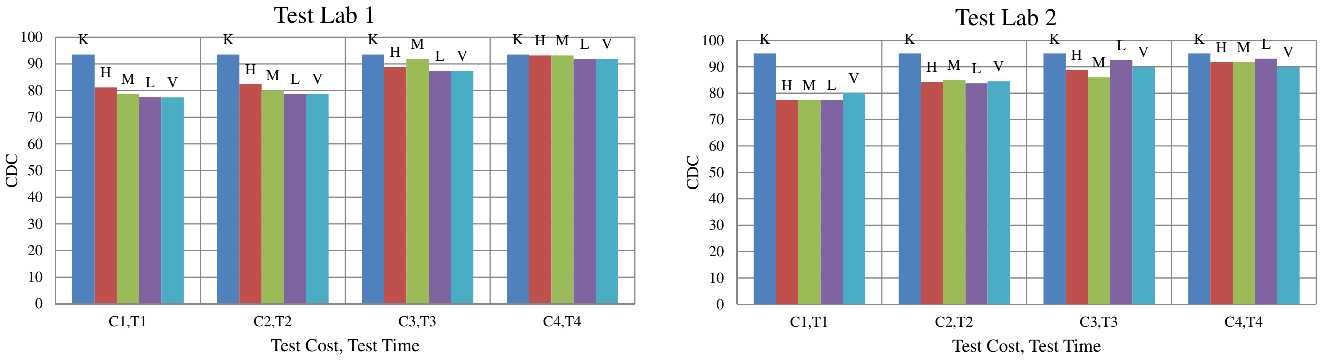


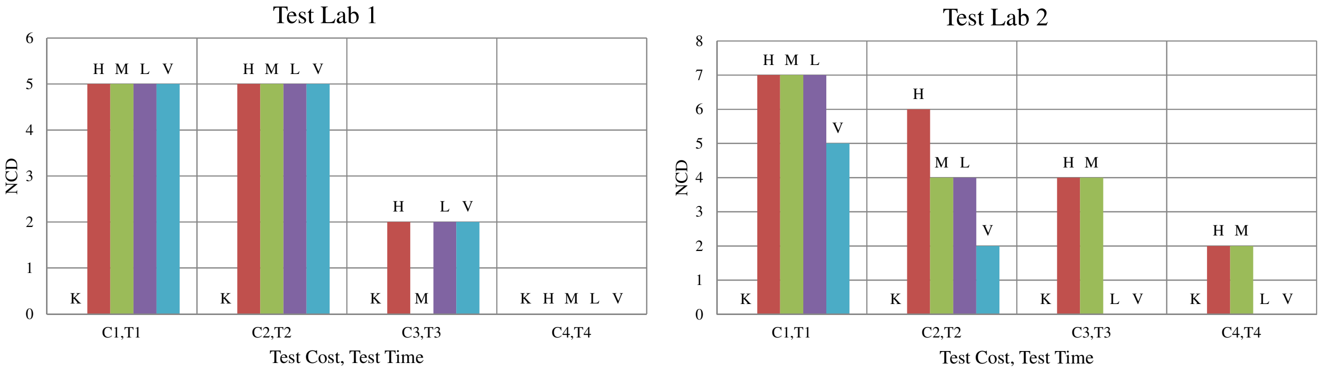
Fig. 6 Counterfeit defect coverage vs. user specified test time and cost (normalized)



(a) CDC for Test Lab1.

(b) CDC for Test Lab2.

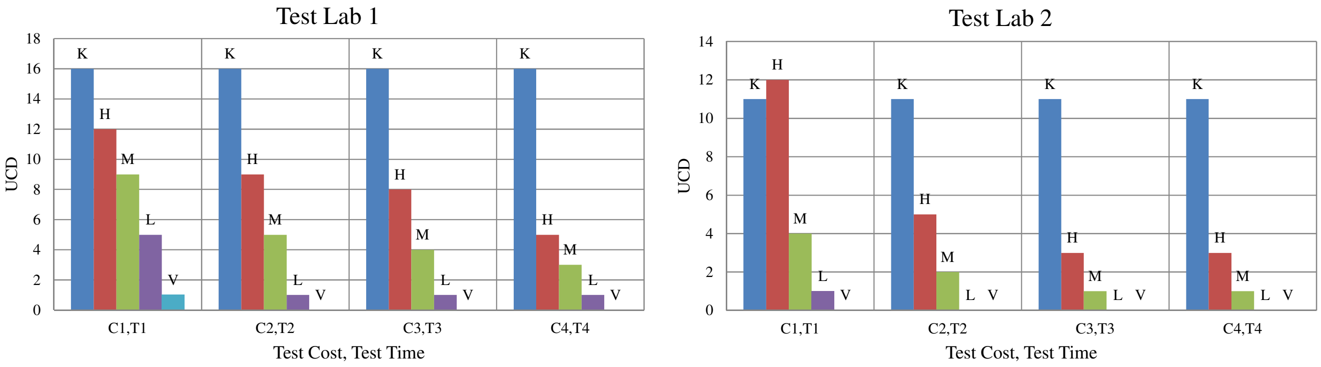
Fig. 7 CDC vs. test cost and time for different application risks



(a) NCDs for Test Lab1.

(b) NCDs for Test Lab2.

Fig. 8 Not-covered defects (*NCD*) vs. test cost and time for different application risks



(a) UCDs for Test Lab1.

(b) UCDs for Test Lab2.

Fig. 9 Under-covered defects (*UCD*) vs. test cost and time for different application risks

Figure 8 shows the variation of *NCDs* with the test cost and time while considering application risks. The *NCDs* for both labs are zero for critical applications as the algorithm targets all defects (no test cost and time constraints). For other application risks, this number goes down with increased test cost and time as more methods are added in the recommended test set. The number of *NCDs* does not vary significantly among different application risks with a particular test cost and time.

Figure 9 shows the variation of *UCDs* with the application risks. The *UCDs* are constant for both labs for critical applications as there are no test cost and time constraints for selecting the methods. The *UCDs* are higher for critical applications as it has to satisfy more stringent constraints (3) compared to other applications. For other risks, this number goes down with increased test cost and time as more methods are added in the recommended test set. The number of *UCDs* declined significantly from high risk to very low risk applications with a particular test cost and time as they satisfy (3).

6 Conclusion

In this paper we have developed a detailed taxonomy of the defects present in all counterfeit types to assess the currently available counterfeit detection methods. We have carried out the assessment by describing these detection methods' ability to identify counterfeit defects. We have also introduced the CDC, NCD, and UCD as the metrics for the assessment of a set of detection methods. We have proposed a method selection technique considering application risks, test time, and cost.

Acknowledgments The authors would like to thank Steve Walters of Honeywell, and the G19-A group members for providing valuable feedback on the defect taxonomy. The authors would also like to thank Huynh Yvonne of Boeing and Sultan Lilani of Integra Tech. for their feedback on developing the model.

References

1. Alam M, Mahapatra S (2005) A comprehensive model of pmos nbti degradation. Microelectron Reliab 45(1):71–81
2. Bhardwaj S, Wang W, Vattikonda R, Cao Y, Vrudhula S (2006) Predictive modeling of the nbti effect for reliable design. In: Proceeding of IEEE on custom integrated circuits conference, pp 189–192
3. Black J (1969) Electromigration - a brief survey and some recent results. IEEE Trans Electron Devices 16(4):338–347
4. Bolotnyy L, Robins G (2007) Physically unclonable function-based security and privacy in rfid systems. In: Proceeding of IEEE International conference on pervasive computing and communications, pp 211–220
5. Bushnell M, Agrawal V (2000) Essentials of electronic testing for digital, memory, and mixed-signal VLSI circuits. Springer
6. Cassell J (2012) Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security
7. CHASE (2013). http://www.chase.uconn.edu/arochase-special-workshop-on-counterfeit-electron ics.php
8. Chen K-L, Saller S, Groves I, Scott D (1985) Reliability effects on mos transistors due to hot-carrier injection. IEEE Trans Electron Devices 32(2):386–393
9. CTI (2011) Certification for coutnerfeit components avoidance program. http://www.cti-us.com/pdf/CCAP101Certification.pdf
10. Department of Defense (2010) Test method standard: microcircuits. [Online]. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-883/std883.pdf
11. Department of Defense (2012) Test method standard: test methods for semiconductor devices. [Online]. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-750/std750.pdf
12. Eldred RD (1959) Test routines based on symbolic logical statements. J ACM 6(1):33–37
13. Galey JM, Norby RE, Roth JP (1961) Techniques for the diagnosis of switching circuit failures. In: Proceedings of the Second annual symposium on switching circuit theory and logical design, pp 152–160
14. GIDEP, Government-Industry Data Exchange Program (GIDEP). http://www.gidep.org/
15. Groeseneken G, Degraeve R, Nigam T, Van den Bosch G, Maes HE (1999) Hot carrier degradation and time-dependent dielectric breakdown in oxides. Microelectron Eng 49(1–2):27–40
16. Guin U, Tehranipoor M (2013) Counterfeit detection technology assessment. In: GOMACTech
17. Guin U, Tehranipoor M (2013) On selection of counterfeit IC detection methods. In: IEEE North Atlantic test workshop (NATW)
18. Guin U, Tehranipoor M, DiMase D, Megrdician M (2013) Counterfeit IC detection and challenges ahead. In: ACM SIGDA
19. IDEA, Acceptability of electronic components distributed in the open market. http://www.idofea.org/products/118-idea-std-1010b
20. Karri R, Rajendran J, Rosenfeld K, Tehranipoor M (2010) Trustworthy hardware: identifying and classifying hardware trojans. Computer 43(10):39–46
21. Kessler LW, Sharpe T (2010) Faked parts detection, circuits assembly, the journal for surface mount and electronics assembly
22. Koushanfar F, Qu G (2001) Hardware metering. In: DAC, pp 490–493
23. Koushanfar F, Qu G, Potkonjak M (2001) Intellectual property metering. In: Inform. Hiding. Springer-Verlag, pp 81–95
24. Kumar S, Guajardo J, Maes R, Schrijen G-J, Tuyls P (2008) Extended abstract: the butterfly puf protecting ip on every fpga. In: Proceedings of IEEE International workshop on hardware-oriented security and trust, pp 67–70
25. Kursawe K, Sadeghi A-R, Schellekens D, Skoric B, Tuyls P (2009) Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage. In: Proceeding of IEEE International workshop on hardware-oriented security and trust, pp 22–29
26. Mahapatra S, Saha D, Varghese D, Kumar P (2006) On the generation and recovery of interface traps in mosfets subjected to nbti, fn, and hci stress. IEEE Trans Electron Devices 53(7):1583–1592

27. Mazumder P, Chakraborty K (1996) Testing and testable design of high-density random-access memories. Springer
28. McPherson J (2006) Reliability challenges for 45nm and beyond. In: Proceeding of ACM/IEEE on Design automation conference, pp 176–181
29. Miller M, Meraglia J, Hayward J (2012) Traceability in the age of globalization: a proposal for a marking protocol to assure authenticity of electronic parts. In: SAE aerospace electronics and avionics systems conference
30. Mouli C, Carriker W (2007) Future Fab: how software is helping Intel go nano–and beyond. IEEE Spectr 44(3):38–43
31. Nelson GF, Boggs WF (1975) Parametric tests meet the challenge of high-density ICs. Electronics 48(5):108–111
32. Pappu R (2001) Physical one-way functions. PhD dissertation, Massachusetts Institute of Technology
33. Reddy V, Krishnan A, Marshall A, Rodriguez J, Natarajan S, Rost T, Krishnan S (2002) Impact of negative bias temperature instability on digital circuit reliability. In: Proceeding on reliability physics, pp 248–254
34. SAE (2009) Counterfeit electronic parts; avoidance, detection, mitigation, and disposition. http://standards.sae.org/as5553/
35. SAE, http://www.sae.org/works/committeeHome.do?comtID=TEAG19
36. Schroder DK, Babcock JA (2003) Negative bias temperature instability: road to cross in deep submicron silicon semiconductor manufacturing. Appl Phys 94(1):1–18
37. Seshu S, Freeman DN (1962) The diagnosis of asynchronous sequential switching systems, vol EC-11
38. Soma M (1993) Fault coverage of dc parametric tests for embedded analog amplifiers. In: Proceedings on International test conference, pp 566–573
39. Stathis J (2001) Physical and predictive models of ultrathin oxide reliability in cmos devices and circuits. IEEE Trans Device Mater Reliab 1(1):43–59
40. Suh G, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: Proceedings of ACM/IEEE on Design automation conference, pp 9–14
41. Suk D, Reddy S (1981) A march test for functional faults in semiconductor random access memories. IEEE Trans Comput C30(12):982–985
42. Tehranipoor M, Koushanfar F (2010) A survey of hardware trojan taxonomy and detection. IEEE Des Test 27(1):10–25
43. Tehranipoor M, Wang C (2012) Introduction to hardware security and trust. Springer
44. trust-HUB, http://trust-hub.org/home
45. US Congress, National Defense Authorization Act for Fiscal Year 2012. [Online]. Available: http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf
46. U.S. Department Of Commerce (2010) Defense industrial base assessment: counterfeit electronics
47. U.S. Environmental Protection Agency (2011) Electronic waste management in the united states through 2009
48. U.S. Senate Committee on Armed Services (2012) Inquiry into counterfeit electronic parts in the department of defence supply chain
49. U.S. Senate Committee on Armed Services (2012) Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms. [Online]. Available: http://www.gao.gov/assets/590/588736.pdf
50. Villasenor J, Tehranipoor M (2012) Are you sure its new? the hidden dangers of recycled electronics components. In: IEEE spectrum
51. Wang W, Reddy V, Krishnan A, Vattikonda R, Krishnan S, Cao Y (2007) Compact modeling and simulation of circuit reliability for 65-nm cmos technology. IEEE Trans Device Mater Reliab 7(4):509–517
52. Zhang X, Tehranipoor M (2013) Design of on-chip lightweight sensors for effective detection of recycled ICs. In: TVLSI
53. Zhang X, Tuzzio N, Tehranipoor M (2012) Identification of recovered ics using fingerprints from a light-weight on-chip sensor. In: DAC, pp 703–708
54. Zhang X, Xiao K, Tehranipoor M (2012) Path-delay fingerprinting for identification of recovered ICs. In: DFT

Ujjwal Guin is a doctoral student at the Electrical and Computer Engineering Department, University of Connecticut. He received his B.E. degree from Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, India and M.Sc. degree from Department of Electrical and Computer Engineering, Temple University in 2004 and 2010, respectively.

He was the recipient of the Best Student Paper Award, NATW 2013. His current research interests include counterfeit detection and avoidance, hardware security, VLSI testing, and reliability.

Dan DiMase is the Director of Compliance and Quality at Honeywell International Inc, working in the counterfeit parts prevention team for the Aerospace Quality organization. He is involved in implementing policies and procedures to mitigate the counterfeit risk, and oversees customer and regulatory concerns. He participates in standards development activities to deploy industry best practices and procedures, and to create testing solutions for detection of suspect counterfeit electronic parts, He also contributes in site and supplier audits for Honeywell. He has worked on the NASA Contact Assurance Services team assisting NASA centers become compliant to NASA policy and the AS5553 standard for mitigating counterfeit electronic parts.

Mr. DiMase is an active participant in SAE International's G-19 Counterfeit Electronic Parts Document Development group. He is chairman of the Test Laboratory Standard Development committee, co-chairman of the Distributor Process Rating committee, and actively participates on the Counterfeit Electronic Parts standard development committee for distributors. Among other committees, has been active in the executive committee of the Aerospace Industry Association's Counterfeit Parts Integrated Project Team. He is on the Development of Homeland Security's Customs and Border Protection Advisory Committee on Commercial Operations of CBP in the Intellectual Property Rights subcommittee. He received a special recognition award at the DMSMS and Standardization 2011 Conference for his leadership role in mitigating counterfeit parts.

Dan DiMase has over 20 years of industry experience, previously serving in leadership position as president of SemiXchange, Inc. and ERAI. He is a results-oriented leader proficient in supply-chain, operations and finance, with cross functional expertise in numerous areas, including international logistics, global sourcing, risk management, and strategic planning. He has a Six-Sigma Green Certificate from Bryant University. He received his Bachelor of Science degree in Electrical Engineering from The University of Rhode Island. He has an Executive MBA from Northeastern University.

Mohammad Tehranipoor is currently the F.L. Castleman Associate Professor in Engineering Innovation at the University of Connecticut. His current research projects include: computer-aided design and test for CMOS VLSI designs, reliable systems design at nanoscale, counterfeit electronics detection and prevention, supply chain risk management, and hardware security and trust. Dr. Tehranipoor has published over 200 journal articles and refereed conference papers and has given more than 110 invited talks and keynote addresses since 2006. He has published four books and ten book chapters. He is a recipient of several best paper awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, the 2009 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award.

He serves on the program committee of more than a dozen of leading conferences and workshops. He served as Program Chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T-2009 and DFTS-2009, and Vice-general Chair for NATW-2011. He co-founded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair and Chair of Steering Committee. He is currently serving as an Associate EIC for IEEE Design & Test, an Associate Editor for JETTA, an Associate Editor for Journal of Low Power Electronics (JOLPE), an IEEE Distinguished Speaker, and an ACM Distinguished Speaker. Dr. Tehranipoor is a Senior Member of the IEEE and Member of ACM and ACM SIGDA. He is currently serving as the director of CHASE center.