On Selection of Counterfeit IC Detection Methods

Ujjwal Guin and Mohammad Tehranipoor

ECE Dept., University of Connecticut
{ujjwal, tehrani}@engr.uconn.edu

***Abstract*—Counterfeiting of electronic components pose a major threat to the global electronic supply chain. To counteract this increasing threat, a specialized service of testing, detection, and avoidance of counterfeit parts has been created. In this paper, we present an innovative technique to identify the optimum set of tests for counterfeit detection considering test time, cost and application risks.**

I. Introduction

Counterfeit electronic components are a great threat to the global supply chain. The most recent data provided by Information Handling Services Inc. (IHS) shows that reports of counterfeit parts have quadrupled since 2009 [1]. The counterfeit components are penetrating supply chain mostly through recycling [2]. In United States, only 25% of electronic waste has been properly recycled in 2009 [3]. That percent is even lower for other countries. This huge resource of e-waste provides the counterfeiters the necessary fuel to build up an extremely large supply of counterfeit components.

There are standards in place that include guidance or requirements for detection of the counterfeit parts [4] [5] [6]. 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. The 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 [7] or physically unclonable functions by generating unique ID for each chip [8] [9], to name a couple. Some of these preventive techniques address threats from different counterfeit types beyond recycled and remarked devices.

In this paper, we have developed a detailed taxonomy for the defects present in the counterfeit parts. We have developed a technique to find a set of test methods that will give the maximum counterfeit defect coverage (CDC). The technique is not only driven by the data but also takes the feedback from the subject matter experts. To the best of our knowledge, this is the first attempt to present classifications of counterfeit components and defects and assess the existing counterfeit detection methods based on newly developed metrics.

The paper is organized as follows: in Section II we present different types of counterfeits and defects present in the electronic supply chain. We then present our test selection technique in Section III. The experimental results are shown in Section IV. Section V concludes the paper.

II. Background

A counterfeit electronic component - (i) is an unauthorized copy; (ii) does not conform to original 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 working; or (v) has incorrect or false markings and/or documentation [10]. In addition to the above, we also consider overproduced, cloned and tampered parts as counterfeit electronic parts. Figure 1 shows our classification of all different types of counterfeit electronic components.

The most widely discussed types of counterfeits are the recycled and remarked type. It is reported that in today's supply chain, more than 80% of the counterfeit components are recycled and remarked [2]. The recycled parts may either be non-functioning or the prior usage has done significant damage to the part's life cycle. The remarked parts are also of two types - used parts taken from a PCB or new parts are remarked to a higher grade, such as upgrade a component to defense or industrial grade from commercial grade, mainly to increase the profit. The components become overproduced when an untrusted foundry/assembly has the access to a designer's IP and thus it has control on how many chips to fabricate, assemble, and sell in the open market without the knowledge of design house. These parts may not be tested under the conditions set by the design house before being shipped to the market. The other variation of an untrusted foundry sourcing counterfeit parts is an out-of-specification (spec) or a defective part being sold instead of destroyed. A cloned part is an unauthorized production of a part without having the legal IP. Cloning can also be done with reverse engineering of the original design. The forged documentation category is probably the easiest to fake. However, its detection is not probably the easy one. 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 stored information to the counterfeiter or act as a silicon time bomb in the field [11].

A. Counterfeit Defect Taxonomy

Figure 2 presents the classification of the defects present in the counterfeit components.

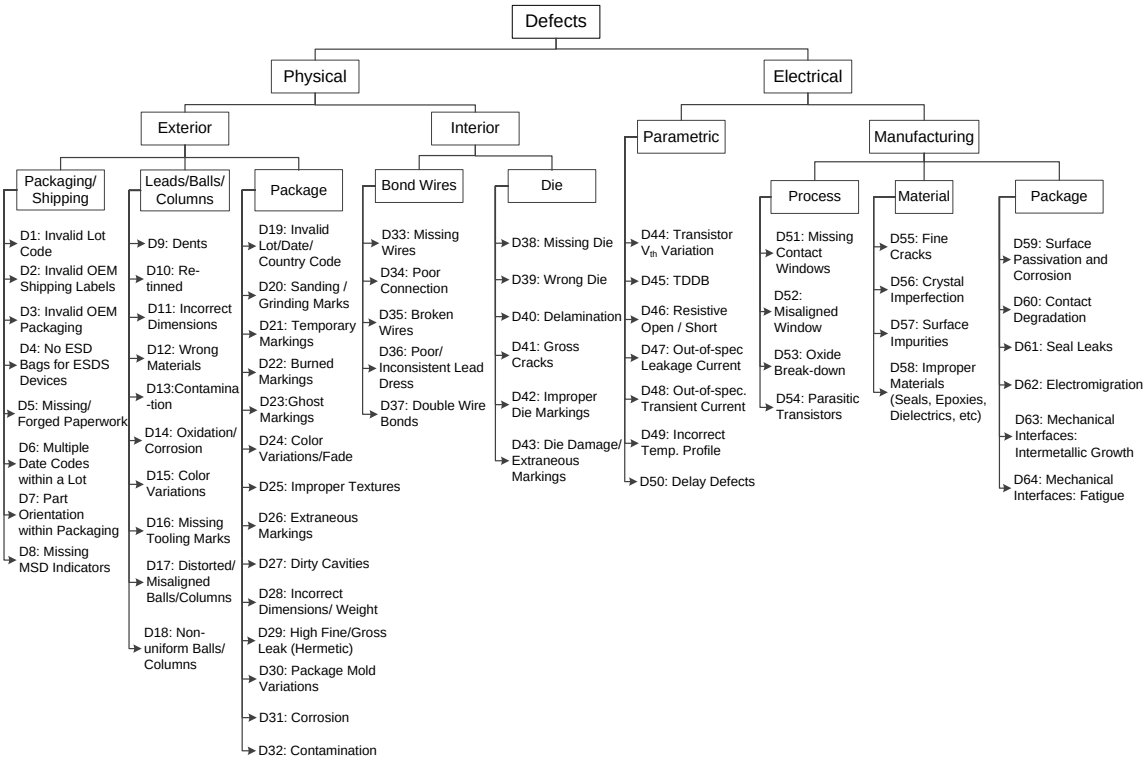

Figure 2. Taxonomy of defects in counterfeit components.

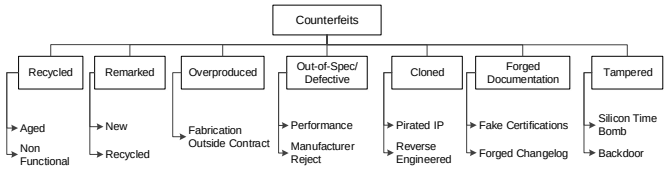

Figure 1. Taxonomy of counterfeit types.

1) Physical Defects: Physical defects are directly related to the physical property of the components. It can be classified as exterior and interior defects depending on the location of the defect related to the packaging. Exterior defects are (i) $Packaging/Shipping$: The most obvious defects will be ones that are associated with the packaging or shipping the parts arrived in. (ii) $Leads/Balls/Columns$: Leads/balls/columns of an IC can show how the part has been handled if it was previously used. Physically, they should adhere to datasheet specifications, including size and shape. The final coating on the leads should conform to specification sheet. (iii) $Package$: The package of an IC can reveal significant information about the chip. As this is the location that all model numbers, country of origin, date codes, and other information are etched, it makes the most sense that counterfeiters need to be especially careful to not damage anything while keeping the package looking as authentic as possible. Interior defects are mainly divided into two types. Either it can be bond wire or die related defects. These defects are located inside the package. (i) $Bond\ Wires$: There are some common defects related to bond wires are missing bond wires inside the package, poor connection between the die and bond wire, etc. (ii) Die: Die reveals a significant amount of relevant information regarding the component. The defects present in the die are from die markings, cracks, etc.

2) Electrical Defects: Typical electrical defects can be classified into two distinct categories, namely parametric defects and manufacturing defects. The main reason for adding manufacturing defects under electrical category is that we can almost completely detect these defects by manufacturing tests (a.k.a, electrical tests). (i) $Parametric\ Defects$: Parametric defects are the manifestation of the shift of 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. (ii) $Manufacturing\ Defects$: The defects under this category come from the manufacturing process. These defects are classified into three categories – process, material and package.

B. Counterfeit Detection Taxonomy

Figure 3 shows a taxonomy of counterfeit detection methods. The test methods are classified into two distinct categories – physical tests and electrical tests. Physical tests are mostly performed to verify the physical and chemical/material properties of the component. These tests are classified into four major categories: (i) $Incoming\ Inspection$: When an order is first received, it first goes through the incoming inspection. All parts should be strictly documented and inspected during

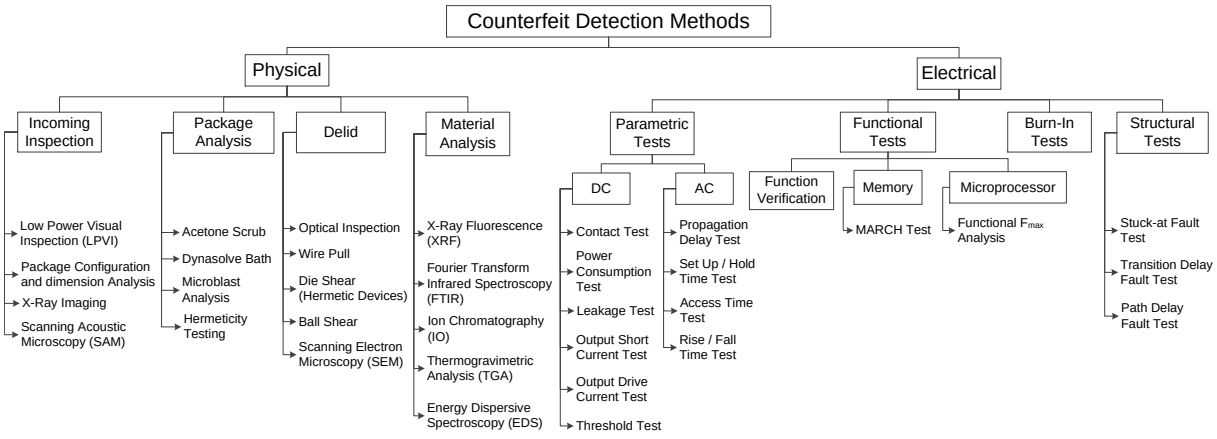

Figure 3. Taxonomy of counterfeit detection methods.

incoming inspection. (ii) $Package\ Analysis$: Acetone scrub or dynasolve bath is the procedure of testing a 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 the analysis. (iii) $Delid$: Delid is a process by which the inspection of the internal structure, top surface of a die, bond wires or metallization traces etc., of an electronic component can be performed. (iv) $Material\ Analysis$: The chemical composition of the component are verified using material analysis. This category includes X-Ray fluorescence (XRF), energy dispersive spectroscopy (EDS), etc.

Electrical test methods are mostly applied to verify the correct functionality and performance of a component. The common electrical tests include: (i) $Parametric\ Tests$: These tests are performed to measure the parameters of a chip (ii) $Functional\ Tests$: Functional tests are the most efficient way of verifying the functionality of a component and perhaps the most expensive one. (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, and (iv) $Structural\ Tests$: Structural tests are very effective to detect the manufacturing defects for out-of-spec/defective counterfeit types.

III. Proposed Test Selection Technique

In this section, we will develop a technique to find an optimum set of detection methods that will maximize counterfeit defect coverage (CDC) considering test time and cost. We will introduce CDC as to represent the confidence level of detecting a component as counterfeit after performing a set of tests. Let us first introduce the terminologies which will help us calculate CDC.

Table I represents the terminologies and their matrix notation. Matrix M denotes the complete set of test methods. m and n represents the number of test methods and defects respectively. The matrix AR stands for application risk. We have considered application risk in five distinct types – critical, high, medium, low and very low from SAE G-19A, Test Laboratory Standards Development Subcommittee. We have assigned a value (0 to 100) to each application risk. Higher value stands for higher application risk. Percent counterfeit component (PCC) represents the percent of counterfeit components present in the electronic supply chain. This data will be available through Government-Industry Data Exchange Program (GIDEP)since there is a reporting requirement of counterfeit incidents to all test labs by Department of Defense [12] [13]. Currently, around 80% of components belongs to recycled and remarked counterfeit types [2]. The defect matrix (D) represents the defects associated with a particular counterfeit type. The rows and columns of D 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 frequent the defect is visible into the supply chain. It is the multiplication of the defect matrix (D) and percent counterfeit component (PCC). The calculation of defect frequency is 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 in our technique by introducing target defect confidence level (DC) for each defect. It is basically the multiplication of application risk and defect frequency for each defect.

One of the important data used in our test selection technique is the defect confidence level matrix X and 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

Table I
TERMINOLOGIES

Terminology	**Matrix Notation** *
Test Methods	$M = [m_1\ m_2\ \ldots\ m_m]^T$ $m_i \in \{0,1\} = \{\text{Not Selected, Selected}\}$
Test Cost	$C = [c_1\ c_2\ \ldots\ c_m]^T$
Test Time	$T = [t_1\ t_2\ \ldots\ t_m]^T$
Application Risks	$AR = [AR_1\ AR_2\ \ldots\ AR_5]^T$, AR_1: Critical, AR_2: High, AR_3: Medium AR_4: Low, AR_5: Very Low
Percent Counterfeit Component	$PCC = [p_1\ p_2\ \ldots\ p_7]^T$ p_1: Recycled, p_2: Remarked, …, p_7: Tampered
Defects	D= $\begin{bmatrix} d_{11} & d_{12} & \ldots & d_{17} \\ d_{21} & d_{22} & \ldots & d_{27} \\ \vdots & \vdots & \vdots & \vdots \\ d_{n1} & d_{n2} & \ldots & d_{n7} \end{bmatrix}$, where $d_{ij} \in \{0,1\}$ ={Not Present, Present} And rows and columns represent defects and counterfeit types respectively.
Defect Frequency	$DF = D * PCC^T$
Target Defect Confidence Level	$DC = [DC_1\ DC_2\ \ldots\ DC_n]^T$ $= AR[i] * DF$

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

test method.

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

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

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

A. Assessment Metric

To evaluate the effectiveness of test methods, it is of utmost importance to develop a test metric that represents coverage for targeting 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 is presented by the following equation:

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

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) $Not-covered\ defects$: The defects are called NCDs when a set of recommended tests cannot detect them.
(iii) $Under-covered\ defects$: The defects are called UCDs when a set of recommended tests cannot provide the desired confidence level. The defects belongs to this category when x_{Rj} is less than DC.

B. Proposed Algorithm

In this research our objective is to find an optimum set of tests to maximize the counterfeit defect coverage considering test time, test cost and application risk. The problem can be formulated as:

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

$$x_{Rj} \geq DC_j \quad \textit{for critical applications}$$

or

$$\begin{aligned} m_1c_1 + m_2c_2 + \ldots + m_mc_m \leq c_{user} \quad & \textit{for non-critical} \\ m_1t_1 + m_2t_2 + \ldots + m_mt_m \leq t_{user} \quad & \textit{applications} \end{aligned}$$

For critical applications, our prime objective is to get the maximum test coverage irrespective of the test cost and time. On the other hand, for low and very low risk applications test time and cost are more important than getting maximum coverage. For medium and high risk application we can get higher confidence level by setting higher test time and cost limit.

IV. RESULTS

The simulation results mainly focus on the assessment of test methods based on the current level of expertise exist in the field of counterfeit detection. The CDC engine is implemented in 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. The simulation results are presented in three segments – (i) the change in CDC with the increase in number of tests, (ii) the increase in CDC with test time and cost, and (iii) application criticality affect on the detected defects.

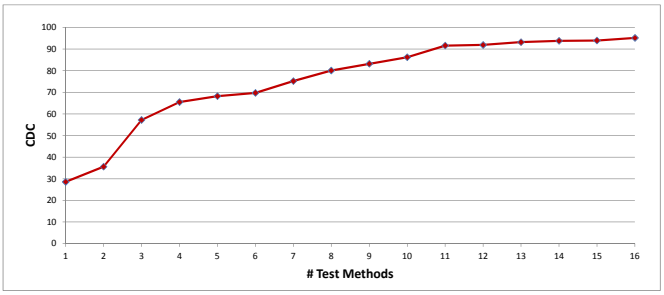

Figure 4. Counterfeit defect coverage vs. number of tests.

Figure 4 shows the change of CDC with the increase in number of tests. The x-axis represents the number of tests in the recommended test set. First few tests detect majority of defects and the coverage increases rapidly. As the number of tests increase, the rate of increase goes down and eventually reaches to 95%. Our current test technology can provide 95% as maximum achievable test confidence. In the algorithm, the test methods are ranked in such a way that we can get the maximum benefit in terms of test time and cost.

Table II
RECOMMENDED SET OF TESTS

Test Sequence	Tests
1	Low Power Visual Inspection (LPVI)
2	X-Ray fluorescence (XRF)
3	Parametric Tests
4	X-Ray Imaging
⋮	⋮

Table II shows the recommended test set. We will mention first few tests as this recommended set depends on the type of component under test (CUT). The first test is low power visual inspection (LPVI) as it detects majority of exterior physical defects. The second recommended test is X-Ray fluorescence which mostly detects related to chemical composition. The third and fourth tests are parametric tests and X-Ray imaging respectively. Majority of electrical defects can be detected by low cost parametric tests. The rest of the tests depends on CUT. To achieve a higher test confidence, we need to focus on developing new test methods with better detection capability of defects. It is also important to balance the tests in physical and electrical categories uniformly to cover most (all if possible) of the defects.

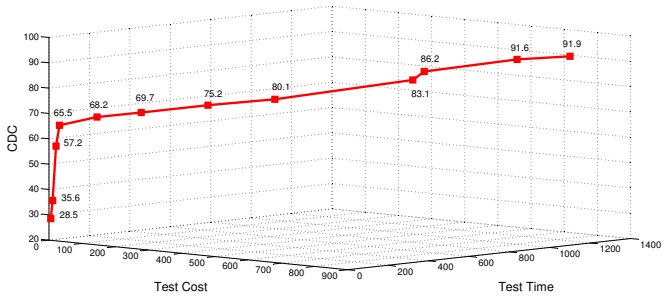

Figure 5. Counterfeit defect coverage vs. test time and cost.

Figure 5 shows the counterfeit defect coverage vs. test time and cost. The test time and cost axis do not represent the actual time and dollar value. The test coverage rises rapidly with test cost and time as the fact that the first few low cost tests detect majority of the defects as described in Figure 4. To achieve higher confidence level (more than around 65.5%), one needs to invest more on detection methods. We cannot achieve more than 95% coverage even one put infinite time and money as it reaches the upper bound.

Figure 6 represents the variation of undetected defects ($NCDs$ and $UCDs$) vs application risks. We did not consider critical risk application in the graph as there are no test time and cost constraint. Form the figure it is obvious that the number of $UCDs$ increase from very low to high risk application considering a specified test time and cost. The number of $NCDs$ are constant as from the fact that for a specified test time and cost the number of tests are constant for all type of applications. If we increase the test time and cost, the number of $UCDs$ and $NCDs$ decrease as more and more tests are added in the recommended test set. We also

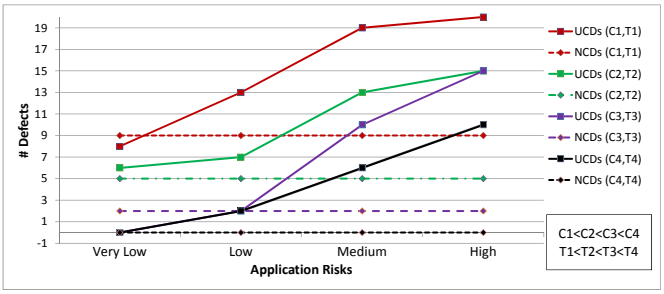

Figure 6. Undetected defects vs. application risks.

observe the similar trend for $UCDs$ at different test time and cost.

V. CONCLUSION

In this paper we have developed counterfeit and defect taxonomies to assess all the currently available test methods. We have carried out the assessment by describing the detection capability of counterfeit defects by the test methods. We have introduced the test confidence after performing a set of recommended tests to evaluate their detection capability.

REFERENCES

[1] IHS , "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security," Apr. 2012, http://www.ihs.com/images/IHS-iSuppli-Reports-Counterfeit-Parts-Quadruple-Since-2009.pdf.

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

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

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

[5] CTI , "Certification for coutnerfeit components avoidance program," Sept. 2011, http://www.cti-us.com/pdf/CCAP101Certification.pdf.

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

[7] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proc. of IEEE on Design Automation Conference*, June 2012, pp. 703 –708.

[8] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[9] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. of ACM/IEEE on Design Automation Conference*, June 2007, pp. 9 –14.

[10] U.S. Department Of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," Jan. 2010.

[11] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test*, vol. 27, no. 1, pp. 10–25, 2010.

[12] US Congress, "National Defense Authorization Act for Fiscal Year 2012." [Online]. Available: http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf

[13] GIDEP, "Government-Industry Data Exchange Program (GIDEP)," http://www.gidep.org/.