AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Detection and Avoidance Measures of IC Counterfeits: A Survey

[1]Anju Boby, [2]Dr.G. Mohanbabu and [3]S.Gopalakrishnan

[1]PG Scholar, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul - 624619, India.
[2]Assistant Professor, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul - 624619, India.
[3]Assistant Professor, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul - 624619, India.

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 September 2014
Available online 12 November 2014

Keywords:
IC counterfeiting, recycled integrated circuits(IC), electronic component supply chain, anti-counterfeit measures.

ABSTRACT

The emerging threat of counterfeit electronic components has become a major challenge in the 21st century. Due to globalization of the semiconductor design and fabrication process, integrated circuits (ICs) are becoming increasingly vulnerable to malicious activities. To address this growing threat, specialized techniques for detection of such parts has been created. These techniques are difficult to implement due to its large test time and cost for implementation. As counterfeiters introduce newer techniques, their detection becomes more challenging for component manufacturers and distributors. In this paper, we discussed various types of IC counterfeits and anti-counterfeit measures which help to prevent counterfeit components from ever entering into the secured electronic components and to provide capabilities for easy detection.

To Cite This Article: Anju Boby, Dr.G. Mohanbabu and S.Gopalakrishnan., Detection and Avoidance Measures of IC Counterfeits: A Survey. ***Aust. J. Basic & Appl. Sci.,*** *8(18): 37-42, 2014*

INTRODUCTION

An integrated circuit (IC) is an electronic circuit on one small plate ("chip") of semi-conductor material. Several million transistors or components could be integrated into one chip, which is widely used in all electronic equipment, such as laptops, mobile phones, digital home appliances etc. Counterfeiting of such integrated circuits has become a major issue that impacts the security of a wide variety of electronic systems.

Counterfeit component is an electronic part that is not genuine as it is an unauthorized copy and is not produced by the original component manufacturers (OCM) or is produced by unauthorized contractors. It is an electronic component that is defective or with false specification that are resold as new in the market (Bureau of Industry and Security, 2010). The consequences of using counterfeit electronic components can obviously be dramatic when critical systems begin to fail due to the use of counterfeit or low quality components. Counterfeiting affects a diverse array of products, ranging from bolts to clothing to sophisticated semiconductors. Counterfeit ICs pose a significant threat to the global electronics component supply chain and detection of such components become more challenging as counterfeiters increasing their level of sophistication. Counterfeiters are improving their techniques to an extent so that they can successfully duplicate a company itself. Counterfeiting of integrated circuits has become a major issue in the semiconductor industry due to the deficiencies in the existing test solutions and lack of effective avoidance mechanisms. Over the past few years, numerous reports (Bureau of Industry and Security, 2010) have pointed to the counterfeiting issues in the electronics component supply chain. A study conducted by U.S Department of Commerce from 2005 to 2008 reveals that 50% of original component manufacturers (OCM) and 55% of distributors (authorized and unauthorized) have encountered counterfeit parts. From the given figure (1) we can say that reports of counterfeit parts have quadrupled since 2009. In addition the trends shown in figure suggest that this number is only going to increase over time.

Counterfeit Types:

A counterfeit electronic part is (a) an unauthorized copy (b) doesn't belong to original component manufacturer (OCM) design/model (c) defective / false specification parts (d) products that are resold as new (e) has false markings or documentation (Bureau of Industry and Security, 2010). Based on the above description, we classify counterfeit parts into seven different categories- remarked, recycled, out of specification,

Corresponding Author: Anju Boby, PG Scholar, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul -624619, India.

overproduced, cloned, tampered and forged documentation (Guin, U., M. Tehranipoor, 2013; Guin, U., *et al* 2013). In recent years it is reported that in electronic supply chain more than 80% of the counterfeit components are recycled and remarked.

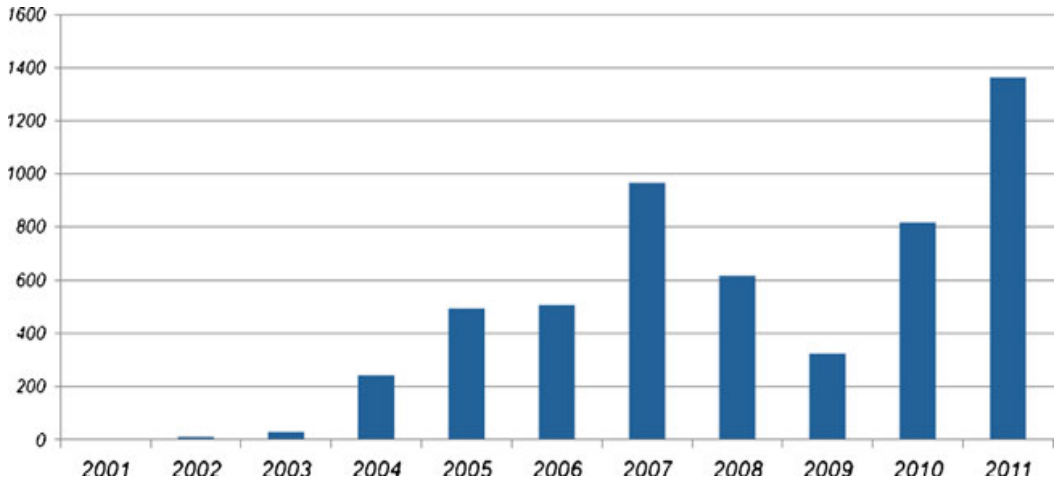

Fig. 1: Counterfeits incidents reported for microcircuits from 2001 to 2011.

1) Recycled:

One of the most widely discussed counterfeit types is recycled. More than 80% of the counterfeit components in today's electronic supply chain are recycled (Kessler, L.W. and T. Sharpe, 2010). Recycling is a process by which the used components are removed from scrapped printed circuit boards (PCBs) and their package is repainted. These components are then resold as new in the electronic market. The recycled parts may either be non-functioning, not performing to manufacturer's specification and early usage has done significant damage to the parts life cycle and introduces reliability concerns.

2) Remarked:

In remarking process, the counterfeiters remove the old markings (part number, date code, country of origin, etc.) on the package and mark them again with false information. The remarked parts are of two types- equivalent parts type from a cheaper brand or new parts remarked to higher grades i.e., upgrading a component from commercial grade to military/industrial grade, mainly to increase profit. Remarked components may not perform in accordance with expected specifications and may also have significant reliability concerns.

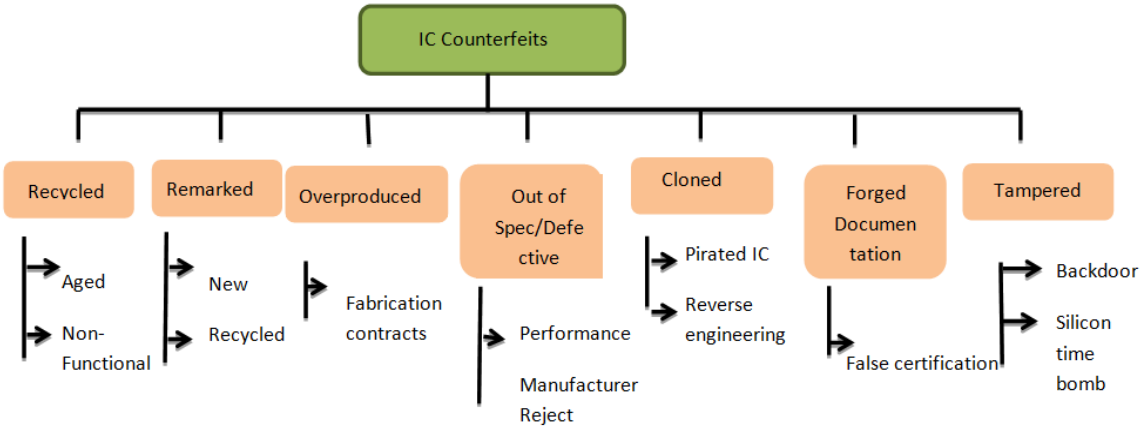

Fig. 2: Counterfeit component types.

3) Overproduced:

Due to the increasing cost and the complexity of the foundries and their process, the semiconductor business has largely shifted to a contract foundry business model over the past two decades. It is also true for the assembly where the ICs are packaged, tested and shipped to the market. Any untrusted foundry/assembly that has access to the designer's intellectual property (IP) can be able to fabricate, assemble and then sells parts in the open market outside the contract without designer's knowledge.

4) Out of specification/Defective:

A component is considered defective during the manufacturing tests if it produces incorrect response to even one test vector. But sometimes the probability of activating a components defective node extremely small. If these components enter into the supply chain, detection will be extremely difficult as they produce correct responses in most of the test cases. These components can be a serious threat to the reliability and quality of a system.

5) Cloned:

Cloning is another type of IC counterfeits done by most of the counterfeiters. In cloning counterfeiters copied a design instead of designing in order to reduce the large cost of development. A cloned part is a fake part, that having the no legal rights for the production of the device. Cloning can be done in two ways (1) by reverse engineering and (2) by obtaining IPs illegally. In reverse engineering, counterfeiters copy designs and then fabricate parts which are the exact copy of their original counterpart.

6) Forged documentation:

The forged documentation is the easiest way to fake a chip where specifications of the IC on datasheets can be changed by the counterfeiters. Specification testing is one way for detecting those chips. But testing in the absence of the original component manufacturer's test vectors/programs becomes impossible and also expensive.

7) Tampered:

Tampering can be done during any phase of the component's life cycle; it can be either die level or package level. Tampered components can leak valuable and secret on-chip information to the attacker (backdoor attack) or can either act as a silicon time bomb (Military Times, 2011) where the chances of bursting the device is more when they are used again in the field.

Counterfeit Detection Methods:

Counterfeiting of integrated circuits is a multidimensional problem due to the limitations in the existing techniques and unavailability of effective avoidance mechanisms. Counterfeit components have similar external appearance, functions and specifications as the devices they are meant to mimic, but they are used earlier before they are resold. Hence excellent visual inspection techniques will have difficulty in identifying those ICs. It is important to develop new techniques to reach a definite conclusion whether a part is counterfeit or not. In this section we will describe various existing anti-counterfeit measures.

1) Physical tests:

Physical tests (Guin, U., M. Tehranipoor, 2013) are performed to analyse physical and chemical /material properties of the ICs, such as package, leads, dies and their chemical and material composition. They are classified into four classes.

1) ***External visual inspection (EVI):***

External visual inspection is used for analysing electronic components to determine if a device has been changed from its known/actual state. It is a process of analysing the features such as components condition, markings, and presence of a secondary coating, lead conditions, geometry, dimensions and surface quality. As this process is non-destructive, the device that undergone EVI verification can be used afterwards.

2) ***Package Analysis:***

During the package analysis, physical dimensions of the circuit under tests (CUT) are measured either by hand-held or automated test equipment. Any abnormal deviation of measurement from the specification sheet indicates that the CUT may be counterfeit.

3) ***Internal Verification:***

It is a test method used to verify the internal structure of an IC. This will help to determine whether the part appears defective or not. The internal structure of the CUT can be analysed using x-ray imaging. One can compare the images taken from the CUT with a known good component to determine whether the part appears authentic or not.

4) ***Material Analysis:***

Internal chemical composition of the IC is analysed using material analysis. This is the only tests that can identify defects and abnormalities related to materials. There are many tests available that can perform material

analysis such as X-ray fluorescence (XRF), Fourier Transform Infrared Spectroscopy (FTIR), RAMAN Spectroscopy etc.

2) Electrical tests:

These methods are mostly used to verify the correct functionality and performance of ICs.

Parametric Tests:

Parametric tests (Nelson, G.F., W.F. Boggs, 1975; Soma, M., 1993) are performed to measure the AC/DC parameters of the chip. These parameters may shift from their expected values (in the datasheet) if the chip has been used for before. In DC parametric test (Bushnell, M., V. Agrawal, 2000) we measure the electrical parameters using ohm's law. These tests include contact test, power consumption test, output short current/drive current test and threshold test. In AC parametric tests, AC parameters can be measured by using AC voltages with a set of frequencies. It includes rise/fall time tests, set up, hold and release time tests and propagation delay tests.

1) Functional tests:

In functional verification component's functionality is verified and most of the defects can be detected by these tests. It is one of the most efficient and expensive way of detecting IC counterfeits. For a memory device, read/write operations can be performed to verify its functionality e.g. MARCH test (Bushnell, M., V. Agrawal, 2000).

2) Burn-In Test:

Burn-In test (Jensen, F., N.E. Petersen, 1982) is an accepted practice for detecting early failures in a population of semiconductor devices. The device is operated at an elevated temperature to determine infant mortality failures and unexpected failures in order to ensure reliability. This process may also be called heat soaking. Components may be under continuous test or simply tested at the end of the burn-in period. By applying a burn-in, early in-use system failures can be avoided at the expense (trade-off) of a reduced yield caused by the burn-in process.

3) Structural Tests:

Structural testing (Poage, J.F., 1963) is the testing of the structure of the system or component. In contrast to functional tests structural tests are based on code structure. It is often referred to as white-box or glass-box or clear box testing because in structural testing we are concerned about what is happening inside the system/component. Structural tests are automated and much more fine grained than functional tests.

Counterfeit Avoidance Measures:

There are several techniques existing to prevent counterfeit components from entering into secured electronic devices. In this section we are describing some of those techniques.

1) Physical Unclonable Functions:

Physical Unclonable Functions is one of the physical tamper proofing technique that has emerged as an essential element in secure system design. In E.Ozturk, G Hammouri, and B.Sunar (2008), proposed PUF to build tamper proof hardware and thereby create secure data storages. A PUF is a physical pseudo-random function which may be implemented by exploiting the small variances of the wire and gate delays that are unique for each integrated circuit (IC), even if they are logically identical. These variances depend on highly unpredictable factors, which are mainly caused by the inter-chip manufacturing variations (Suh, G. and S. Devadas, 2007). Hence, given the same input, the PUF circuit will return a different output on different chipsets. These variations can help to generate a unique signature for each IC in a challenge-response form, which allows later identification of genuine ICs. This technique is highly unique which can be used for identifying remarked/ overproduced /cloned digital ICs.

2) Hardware Metering:

In F. Koushanfar (2011) conducted a survey on hardware metering. Hardware metering is a set of security protocols that enables the design house to gain post fabrication control of the produced IC. It can be either active or passive metering. In passive metering (Kumar, S., 2008; Lofstrom, K., 2000) each ICs are uniquely identified and registered them in challenge-response pairs. Whenever an IC is suspected then it will be taken out and check for proper registration. In active metering (Alkabani, Y., 2007; Baumgarten, A., 2010; Chakraborty, R., S. Bhunia, 2008), each IC is locked until it is unlocked by the IP holder. Locking can be done in variety of ways such as 1) initializing ICs to a locked state on power-up 2) combinational locking by, for instance, scattering

XOR gates randomly throughout the design, and 3) adding a finite-state machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs.

3) Combating Die Recovery Sensors (CDR):

In X. Zhang and M. Tehranipoor (2012) discussed about combating Die Recovery sensors for recycled IC detection. CDR is a novel fingerprinting technique based on ring oscillators to distinguish the used ICs from the unused ones. The technique inserts a light weight sensor in the chip to capture the usage of the chip in the field and provides an easy detection capability. This type of sensor relies on the aging effect of MOSFETs, as the chip used in the field for a certain period experiences aging because of the wear out mechanisms such as NBTI and HCI.CDR sensor composed of a reference ring oscillator and stressed ring oscillator, the stressed RO is designed to age at very high rate using HVT gates while the reference RO is gated off during chip operation. The frequency difference between the two ROs denotes the circuit usage time.

4) Anti-Fuse Memory based sensor:

In Xuehui Zhang and Mohammad Tehranipoor (2014) proposed an on-chip light weight sensors for effective detection of recycled ICs. It is composed of counters and anti-fuse memory block, the counters are used to measure the circuit usage time and the value is simultaneously stored into the AF memory block. Since the anti-fuse memory is one time programmable, counterfeiters cannot erase the contents once stored into the memory during recycling process.

Conclusion:

In this survey, it has been concluded that electronic components undergone several counterfeit attacks which are serious threat to our secured electronic devices. Several IC testing (both physical and electrical) techniques were introduced to efficiently detect counterfeit ICs and thereby preventing them from entering into secured electronic devices. Different counterfeit avoidance measures were introduced, but cost of implementation is seemed to high. New low power, low cost anti counterfeit measures must be developed in-order to overcome this global counterfeiting problem.

REFERENCES

Alkabani, Y., F. Koushanfar, M. Potkonjak, 2007. Remote activation of ICs for piracy prevention and digital right management in Proceedings of IEEE/ACM international conference on computer aided design, pp: 674-677.

Baumgarten, A., A. Tyagi, J. Zambreno, 2010. "Preventing IC piracy using reconfigurable logic barriers". IEEE Test of Computer aided design, 27(1): 66-75.

Bureau of Industry and Security, U.S. Department of Commence. *Defence Industrial Base Assessment: Counterfeit Electronics (2010)* [Online].

Bushnell, M., V. Agrawal, 2000. "Essentials of electronic testing for digital, memory, and mixed-signal VLSI circuits", Springer.

Chakraborty, R., S. Bhunia, 2008. "Hardware protection and authentication through netlist level obfuscation". In: Proceedings of IEEE/ACM international conference on computer-aided design, pp: 674-677.

Guin, U., M. Tehranipoor, 2013. "On selection of counterfeit IC detection methods" in IEEE North Atlantic test workshop (NATW).

Guin, U., M. Tehranipoor, D. DiMase, M. Megrdician, 2013. "Counterfeit IC detection and challenges ahead" in ACM SIGDA.

Jensen, F., N.E. Petersen, 1982. "Burn-in: an engineering approach to the design and analysis of burn-in procedures". Wiley.

Kessler, L.W. and T. Sharpe, 2010. "*Faked Parts Detection"* [Online].

Koushanfar, F., 2011. "*Hardware Metering: A Survey" (2011) [*Online].

Kumar, S., J. Guajardo, R. Maes, G.J. Schrijen, P. Tuyls, 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.

Lofstrom, K., W. Daasch, D. Taylor, 2000. "IC identification circuit using device mismatch" in Proceedings of IEEE international solid-state circuits conference, pp: 372-373.

Military Times, 2011. *Officials: "Fake Electronics Ticking Time Bombs"*, San Diego, CA, USA [Online].

Nelson, G.F., W.F. Boggs, 1975. "Parametric tests meet the challenge of high-density ICs". Electronics 48(5): 108-111.

Ozturk, E., G. Hammouri and B. Sunar, 2008. "Physical unclonable function with tristate buffers," in *Proc. IEEE International Symposium on Circuits Systems*, pp: 3194-3197.

Poage, J.F., 1963. "Derivation of optimal tests to detect faults in combinational circuits". in Proceedings of the symposium on mathematical theory of automata, pp: 483-528.

Soma, M., 1993. "Fault coverage of dc parametric tests for embedded analog amplifiers". In: Proceedings on international test conference, pp: 566-573.

Suh, G. and S. Devadas, 2007. "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of 44th ACM/IEEE Design Automation Conference*, pp: 9-14.

Zhang, X. and M. Tehranipoor, 2012. "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proceedings of Design Automation Conference*, pp: 703-708.

Zhang, X., M. Tehranipoor, 2013. "Design of on-chip light-weight sensors for effective detection of recycled ICs", in IEEE transactions on VLSI.