International Electronics Manufacturing Initiative
Advancing manufacturing technology
United States • China • Ireland • Japan

2214 Rock Hill Road, Suite 110 • Herndon, VA 20170-4214
Tel: +1 703-834-0330 • Fax: +1 703-834-2735
www.inemi.org • info@inemi.org

Development of a Methodology to Determine Risk of Counterfeit Use

iNEMI Counterfeit Components Project Team
Mark Schaffer, iNEMI, marks@inemi.org

ABSTRACT

Counterfeit components have become a multi-million dollar, yet undesirable, part of the electronics industry. The profitability of the counterfeit industry rests in large part on its ability to recognize supply constraints and quickly respond, effectively taking advantage of a complex and vulnerable supply chain. Factors such as product obsolescence, long life cycles, economic downturn and recovery, local disruptions in manufacturing due to natural disasters, and lack of proper IP legislation all represent opportunities for the counterfeit component industry to flourish. Electronic counterfeits affect every segment of the market, including consumer goods, networking and communications, medical, automotive, and aerospace and defense. In manufacturing, the use of undetected counterfeits can lead to increased scrap rates, early field failures, and increased rework rates; while this presents a major problem impacting profitability, the use of counterfeit components in high reliability applications can have far more serious consequences with severe or lethal outcomes.

The independent distributor level has typically been seen as the weak link in the supply chain where counterfeits are most likely to be introduced. With the emergence of new legislation and through the efforts of different industry entities, new standards and guidelines are now available for suppliers to establish and maintain product traceability and to establish receiving inspection and detection protocols. There is no substitute for a healthy supply chain, and distributors play an essential role in the dynamics of the system. At the same time, there is an increased awareness of the need for proper management of electronic waste. Regardless of the nature of the counterfeits, whether cloned, skimmed, or re-branded, counterfeits are dangerous and too expensive to be ignored.

The work presented here by the iNEMI Counterfeit Components Project takes a comprehensive view of the problem by surveying the possible points of entry in the supply chain and assessing the impact of counterfeit components on the industry at various points of use. We then propose a risk assessment calculator that can be used to quantify the risks of procuring counterfeit parts. This calculator is aimed at all segments of the supply chain and will be of interest to component manufacturers, product designers, distributors, loss estimators, industry groups and end users.

INTRODUCTION

The existence of counterfeit electronic components, materials and assemblies (hereafter referred to simply as counterfeit components) is not a new phenomenon[1] [2]. However, global trade of counterfeit components has recently increased markedly. There are four distinct categories of electronic products in which counterfeit components are most frequently found:

- Manufacturing shortfall and product shortages
- High value products
- Obsolete, discontinued, and legacy devices
- Field installable options or upgrades

---

1 Bill Crowley, “Automated Counterfeit Electronic Component Warning System and Counterfeit Examples”, SMTA/CALCE Counterfeit Symposium, June 2012

2 Philip DiVita et al, “Avoiding Counterfeit Parts When Addressing Component Obsolescence”,SMTA/CALCE Counterfeit Symposium, June 2012

The Semiconductor Industries Association Anti-Counterfeiting Task Force[3] has defined counterfeiting as:

- Substitution or the use of unauthorized copies of a device or product
- The use of inferior materials or a modification of performance without notice
- The sale of a substandard component or product in place of an original OCM device or OEM product

The following definition was adopted from "Defense Industrial Base Assessment: Counterfeit Electronics"; US Dept of Commerce – Office of Technology Evaluation; January 2010.[4]

… a counterfeit is an electronic part that is not genuine because it:

- Is an unauthorized copy
- Does not conform to original manufacturer's design, model, and/or performance standards
- Is not produced by the original manufacturer or is produced by unauthorized contractors
- Is an off-specification, defective, or used product sold as "new" or working
- Has incorrect or false markings and/or documentation

COUNTERFEIT DEVICE CATEGORIES

Counterfeit components can be produced, sourced, and distributed in many different ways. The identity of these non-standard parts is usually very well concealed in the present supply chain. Types of counterfeit components can be divided into the following categories.

Cloning
The complete manufacture of a reverse engineered device to have the same form, fit, and function as the original. Devices are produced on low end equipment and will not meet the original reliability requirements. Devices are branded and sold as Original Component Manufacturer (OCM) parts.

Product "skimming", subcontractors, or second source suppliers
Manufacturers may over-produce or claim a lower production yield. These extra devices can then be introduced into the market through the broker chains.

Disposal of scrap and rejects
Devices rejected during manufacturing are sent to recyclers to salvage precious metals. Recyclers may certify destruction without scrapping devices and subsequently sell it back into the supply chain.

Devices used as qualification samples
OCMs and OEMs used large quantities of devices to qualify/certify form, fit and function of devices. Accelerated life testing is used to evaluate the functionality and reliability at end of life. Pilfered devices stored for future evaluations can be sold into the supply chain as virgin product. When scrapped, many units may still function making this material a prime target for diversion frauds.

Reclamation and reuse of components
Large quantities of electronic equipment containing working devices are scrapped. Valuable components can be recovered for reuse; however, uncontrolled removal can damage and/or compromise the original electrical performance, reliability and operational life. These compromised parts can then be sold into the supply chain.

Re-branding
Some products have high performance requirements and must undergo more extensive testing during manufacture (for example, devices that must operate at extreme temperature ranges, such as automotive, aerospace and military applications, or high speed versions of memory modules and processors). Devices with lower specifications that were never tested to the more stringent specifications are acquired at a lower cost, re-marked, and resold at the higher price.

False claims of conformity to industry certifications (e.g. RoHS)
Paperwork is provided stating devices are compliant and old (non-compliant) devices are substituted.

Devices containing embedded malicious malware
Programmable devices are reprogrammed to cause latent damage to products. This problem is most critical in the aerospace, defense, and medical sectors in which counterfeits could render systems inoperative, compromising the safety and security of users. The Office and Large Business Systems sector, in particular, the FSI (financial services institutions) and pharmaceuticals own a lot of embedded servers supporting mission critical activities that could pose serious economic and health risks. The latter may have greater implications and impact on a global crisis via malware.

[3] http://www.semiconductors.org

[4] http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

SITUATION ANALYSIS

iNEMI segregates the electronics industry into the following product sectors:

- Aerospace and Defense
- Automotive
- Medical
- High-End Systems (including data communication, networking, voice communication and large business systems)
- Office Systems
- Consumer and Portable

Table 1: Industry Sector Product Service Time

Industry	Sectors	Product Service Time
Aerospace & Defense	Avionics (Civil)	10 to 20 years
	Avionics (Military)	10 to 30 years
Automotive	Cars and Trucks	10 to 15 years (warranty)
Medical	External Equipment	5 to 10 years
	Internal Equipment	7 years
High-End Systems	Infrastructure Equipment	10 to 30 years
	Data Center Equipment	7 to 10 years
	High End Servers	7 to 10 years
	Industrial Controls	7 to 15 years
Office Systems	Desktop Computers	24 to 60 months
Consumer & Portable	Appliances	7 to 15 years
	Cell Phones	18 to 36 months
	Laptop Computers	24 to 36 months

All of these product sectors are at risk to introduction of counterfeit components; however, each has its own set of requirements for commonly used components. It is not clear that there is a "one size fits all" solution to the counterfeit components problem due to the variations in requirements among sectors.

Aerospace and Defense

These products require flawless performance on demand, in a multitude of rugged environments, and must sustain this performance over long periods of continuous service. Due to the long service life, systems rely on legacy devices to maintain and expand existing systems. Defense and aerospace systems require extensive testing to meet performance requirements and designs are modified (ruggedized) to meet the thermal, vibration, humidity, salt, fog, and other environmental and reliability requirements associated with DoD platforms. Both need to have a proven supply chain to ensure devices meet security requirements.

Automotive Electronics

These applications involve temperature extremes that require improved process controls on the devices. Controllers communicate with sensors and drive relays, injectors, motors, lamps and solenoids. The engine controller is currently the most complex product for harsh-environment automotive electronics. There is also the need for large traces required by high current and power circuitry. Long life, high reliability devices are needed as product warranties extend to as long as 10 years.

Medical Products

These include large infrastructure equipment, small stationary equipment, and implantable devices. High reliability is required for life critical applications such as electronic implants, medical imaging systems, and resuscitation systems. Many of the large systems use legacy devices and need a reliable supply of replacement parts.

High-End Systems

These include three major categories: high-performance computing, data centers and communications. The networking and computing hardware has been gaining more common components as the communications becomes an integral part of enterprise computing and as technology advancements enable tighter integration of the communication and computing technologies in commercial business systems. The products represented include mainframe and high-performance computers, the data centers and server farms that house the computers, and communications equipment such as switches and routers and enterprise service provider equipment.

Office Systems

These include desktop PCs, and other general office equipment (printers, copiers). This sector is cost sensitive and requires the latest cost effective technologies. The main vulnerabilities relative to counterfeit components are cloning, product "skimming," reclamation, and rebranding.

Consumer and Portable

These products are increasing in complexity; however the main drivers are the reduction in cost and increase in functionality while looking at ways of continuously shrinking the system footprint. The sector has the shortest product life, and the main vulnerabilities are similar to the office and large business systems, i.e., cloning, product "skimming", reclamation, and rebranding.

POSSIBLE STRATEGIES

Dealing with the different counterfeit device categories will require the use of a variety of strategies. There are different strategies for each category that are most likely to be successful:

Cloning

Legacy and high value components are suspected to be the most dominant. Device serialization may prove to have a beneficial impact on this category of counterfeits.

Product “skimming”, subcontractors, or second source suppliers

Place better controls on the documentation with violators identified and prevented from conducting further business.

Disposal of scrap and rejects

Establish better controls on scrap processing and handling. Systems designed to more effectively monitor and audit the waste stream may be needed.

Devices used as qualification samples

This form of counterfeit may not be prevalent enough to warrant developing solutions; however this needs to be verified by an investigation into the extent of this source of counterfeit components.

Reclamation and reuse of components

Some OCMs and OEMs have legitimate operations to reclaim and reuse components using strict procedures to ensure that quality and reliability have not been compromised. Verification procedures for legitimate devices need to be established.

Re-branding

Inspection, inspection, inspection (mechanical, electrical, etc.) as well as lot testing.

False claims of conformity to industry certifications (e.g. RoHS)

Incoming inspection should be required, since counterfeiters are providing false documentation. Traceability and serialization may help to reduce this category of counterfeit devices.

Devices containing embedded malicious malware

This problem is most critical in the aerospace and defense and medical sectors in which counterfeits could render systems inoperative, compromising the safety and security of users. The use of all possible approaches to counterfeit reduction is warranted for this sector.

INITIAL WORK

The first phase of iNEMI’s Counterfeit Components Project is broken into several high-level tasks. The first three tasks (on which this paper is based) were:

Task 1: Identify and summarize any related research or development within the industry and academic communities.

Task 2: Review and tabulate successes that have worked in the past (Best Known Methods/Best Known Practices).

Task 3: Develop a methodology to evaluate or assess the risk of counterfeit use.

In addition to the tasks specifically identified in the Project Statement of Work, the team also:

- Focused on those attributes that are of most value to the supply chain and participating project members, and that are applicable to multiple spaces across the supply chain.
- Identified and developed methodologies with associated metrics to assess the overall extent of the counterfeit problem in the electronics industry. The outputs will enable iNEMI members to assess the risk of counterfeit use in their respective industries, the risk of untrusted sources of supply in that industry and understand the total cost of ownership associated with those risks.
    - The methodologies and strategies apply to all phases of the manufacturing cycle and supply chain. Not only do counterfeit components have a serious impact on the OCM, but impact all downstream users from the legitimate component brokers to the OEMs that integrate these components to the end-user.
    - Metrics to assess the overall extent of the problem and anti-counterfeiting will be identified for all phases.

The team began by identifying the key sectors of the electronics supply chain (Figure 1).

- Wafer Manufacturers
- Chip Manufacturers
- Board Manufacturers
- System Manufacturers
- After Market Sales and Refurb Support
- Disposal/Recycle

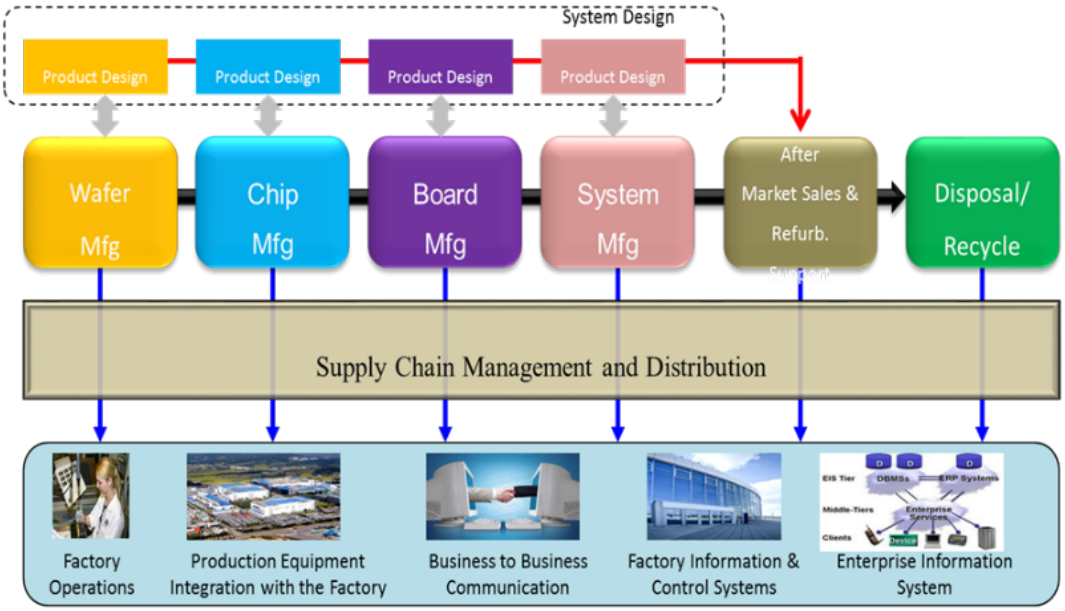

Figure 1: Electronic Manufacturing Workflow Diagram[5]

[5] 2010 iNEMI Roadmap

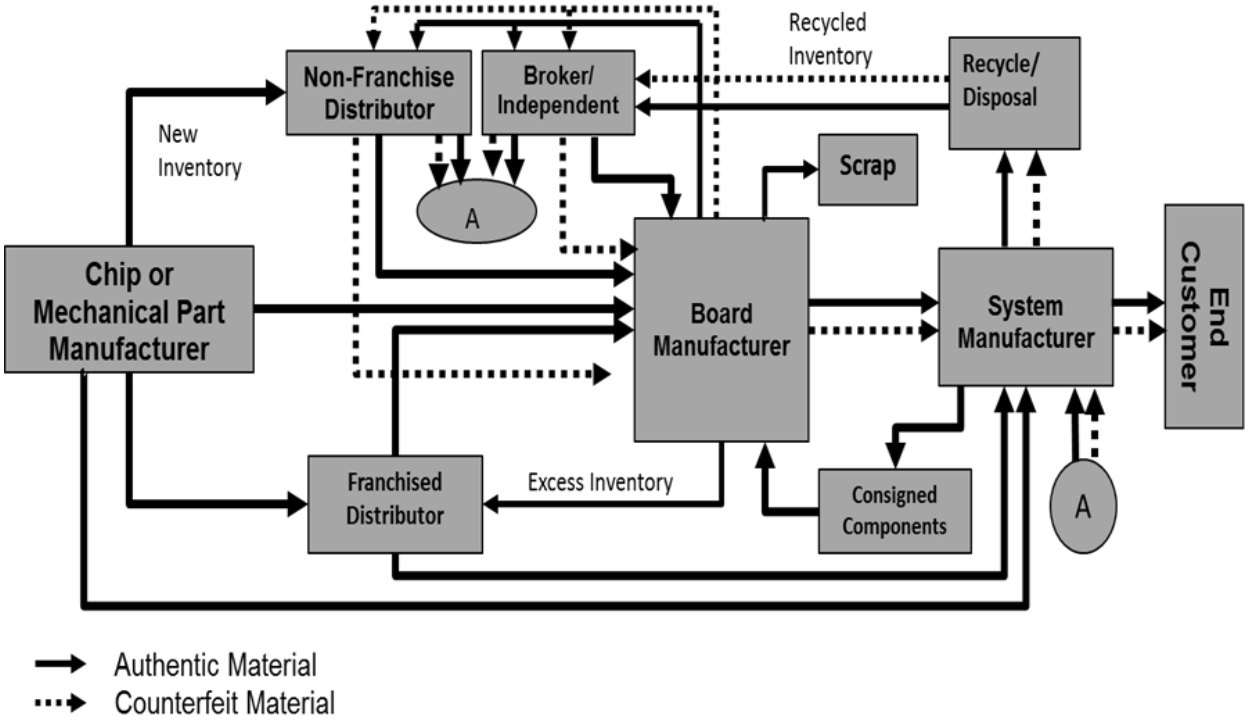

Figure 2: Board Manufacturer Cluster

The electronics supply chain was then broken into a series of manufacturing "cluster maps" to help visualize how materials, parts, assemblies, and waste move, and identify the key players in each manufacturing sector (Figure 2).

The Board Manufacturer Cluster diagram (Figure 2) highlights two principal flows between the major Electronic Manufacturing Workflow blocks: the "*authentic*" and "*counterfeit*" material flow paths. The authentic material flow pathways indicate peer-to-peer connections where the board manufacturer has established strong agreements and has policies in place to prevent corruption of their supply stream. These measures generally provide a high confidence in the supply chain and feature traceability of the pedigree of electronic components.

The counterfeit material flow pathways highlight potential opportunities for breaching into the supply chain and corrupting traceability and pedigree of the electronic components. The risk of infiltration using one of these pathways increases when product shortages occur. Risks can also increase as new participants enter the networks to service growing demand. For example, as green manufacturing increases demand for recycling, new players rushing to capture market share may overlook security protocols. Also consider how criminals are well versed at pretending to be new participants.

With the completion of the cluster maps for the electronics supply chain, the team was able to begin work on the task of developing a methodology for assessing the risk of counterfeit use.

DEVELOPING A RISK ASSESSMENT CALCULATOR

1. Premise of the Spreadsheet / Assumptions

Examining the cluster maps for the different segments of the electronics supply chain, the team decided that the risk of counterfeit use was based on four key elements:

- The profile of the product in question
- The inputs or characteristics of the supplier and supply line
- The processes used on the product to deter counterfeit use
- The outputs or channel characteristics

The team's goal was to provide a quantitative methodology on risk assessment built on these four key elements that any company could use to rate their product.

2. Structure of the Spreadsheet / Rating Scale

2.1) Product Profile

The profile of the product in terms of demand for that product and where it is on the life cycle are key determinants in the risk of counterfeit use. The higher the demand for a product, the more attractive it becomes for counterfeiting. If a product is in high demand and also the original supply is near end of life, then the product profile risk of counterfeit is highest.

2.2) Inputs

The profile of the supplier and the history of that supplier in terms of counterfeit incidents, the clarity of the supply line, and the anti-counterfeit controls used by the supplier are key factors in determining the risk of counterfeit use. For example the inputs risk is highest where the supplier is a broker with no controls who has previously supplied confirmed counterfeit product and cannot confirm the origin of the product in question. Conversely, the inputs risk is lowest when the product is coming directly from the OCM, there are strong counterfeit mitigation procedures in place, and there is no known history of counterfeit supply.

Methodology to Evaluate or Assess the Risk of Counterfeit use — **Example Only**

Product	Profile	Inputs					Process				Outputs						Total Rating
	Demand / EOL	Supplier	Supply Line	Mitigation & Controls	Supplier History	Score	Ease of Counterfeit	Ease of Detection	Counterfeit Controls	Score	Sales Channel	Excess Inventory & Prototype	Customer	Rework	Disposal	Score	
ASIC	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
FPGA	3	3	3	3	1	27	3	3	3	27	3	3	3	3	3	729	1454
FLASH	5	5	5	5	5	625	5	3	5	75	5	5	5	5	5	15625	48594
Hard Drive	3	1	1	1	1	1	5	3	2	30	4	4	5	3	5	6000	10892

Please select the rating from the table below that best corresponds to the description for that rating.

Rating = 1	Product has Low demand and/or is not EOL	OCM	Direct from OCM	Supplier has Strong Mitigation & Controls	No known Counterfeit Incidents	Very difficult to counterfeit; requires factory access or capital investment >$1M	Easy to detect, e.g. by check of packaging, documents, labels, history	Uses Unique Overt and Covert Controls & Identifiers that are easy to validate	Direct- OCMs/ Manufacturers /Suppliers	Minimal Excess inventory. Very limited prototyping/tight OCM security and traceabke records that are digitally signed/encrypted and/or independently audited.	Direct to OEM	In-house only under tight controls in certain designated areas, tight security and traceable records (signed/encrypted and/or independently audited)	In house only, on site physical destruction, traceable records (signed/encrypted and/or independently audited)
Rating = 2	No 2 rating	No 2 rating	No 2 rating	No 2 rating	No 2 rating	Requires major equipment / facilities such as wire bonders and laser markers, >$100k capital	Possible by optical inspection	Unique Overt or Covert Controls / Identifiers that are easy to validate	Known channel: Franchised/ Authorized Distributors	Excess and prototype inventory under tight controls and security	Trusted Sales Rep and Franchised Distributor to OEMs	In-house + vendor, under tight controls and security	In house + vendor physical destruction, traceable records, third party certification*
Rating = 3	Product has Low demand and is EOL or high demand and not EOL	Authorised Distributor	Multiple known suppliers	Some evidence of mitigation / controls	Counterfeit supply suspected	Requires moderate equipment and capital ($10k-100k)	Possible by routinely applied 2D X-ray inspection, decapsulation	Overt and Covert Controls / identifiers but validation not easy	Limited - OEMs/ CMs and some use of Brokers	Significant inventory but under tight controls and security	Trusted Sales Rep and Unfrachished distributor to CMs	Primarily offsite vendor based, with controls and security.	Offsite vendor, with controls and records for pyhsical destruction
Rating = 4	No 4 rating	No 4 rating	No 4 rating	No 4 rating	No 4 rating	Needs simple equipment such as sand blasters and ink printers (<$10k capital)	Requires advanced analytical tactics, i.e. XRD, CSAM, 3D X-ray	Some overt controls / identifiers but validation not easy	Very Limited - Primarily Reputable Independent Distributors/Brokers	Some controls in place. No traceable records. No security	Independent Distributors, dependent on end user oversite.	Offsite some controls in place. No traceable records. No security	Offsite vendor, some controls and records. No proof of physical destruction
Rating = 5	Product has High demand & is EOL	Boker or Ind. Distributor	Supply line not defined / clear	No evidence of mitigation / controls	Counterfeit supply confirmed	Easy - little / no investment required (<$100)	Difficult to detect; nearly indistinguisible from authentic	No special controls in place	No control / Unknown-Unknown Independent Distributors/Brokers /Unknown Sources	Excess and prototype inventory not controlled	Customer not defined, open market.	Offsite Vendor, no controls and no traceability	Offsite Vendor, no controls and no traceability

Figure 3: Methodology to Evaluate Risk of Counterfeit Use (*Note:* Figure 3 and Appendix 1 are examples of the same risk.)

2.3) Process

The processes required to produce the product, the ease of counterfeit detection of that product and the counterfeit controls used in the original product are also key factors in determining the risk of counterfeit use. Where a product requires a large capital investment, is easy to authenticate and uses a high level of counterfeit controls, the process risk of counterfeit use is low. On the other hand, where there is little or no investment required to make the product, validation is difficult, and there are no special counterfeit controls in place, the process risk of counterfeit use is highest.

2.4) Outputs

The key factors in the case of the Outputs risk are the sales channel used, the handling of excess inventory, prototypes, reworks and scrap and the customer profile. The Outputs risk is at its highest when the sales channel is unknown; when there is no control or traceability on excess inventory, prototypes, reworks or scrap; and where the end customer is unknown. In contrast, where the end customer is well known, the sales channel is well defined and the excess / prototypes / reworks and scrap are well controlled, the Outputs risk is lowest.

3) Examples of Calculation

Rating each of the four key risk elements above, the methodology gives an overall score for the product in question. FLASH is a well-known target for counterfeiters, making it a good test of the methods developed here. Based on the values used by the team for each of the factors, the overall rating is very high indicating that our methodology gives the risk of counterfeit use as very high. In contrast the rating for a typical ASIC device is very low, i.e., the risk of counterfeit use is low. These results serve to validate this method or risk assessment.

At this stage, the methodology is useful for comparative purposes only. The team would like to encourage iNEMI members to test the methodology and provide feedback to the team. The wide range of data collected would enable the team to provide guidelines in the form of levels of risk of counterfeit use. For example, an overall rating of 1 ~ 500 means the risk of counterfeit use is very low and no additional actions are recommended. A rating of 5000 ~ 10,000 means the risk is very high and immediate action needs to be taken in the high risk areas.

When materials are purchased through the distribution channel, there are ways to minimize exposure to suspect, fraudulent, or counterfeit parts passing undetected through the distributor to you. SAE International Standard AS5553A[6] identifies a series of controls and certifications to ensure detection and prevention of counterfeit components. You can select a distributor that has been audited by a third party certification body and is compliant with:

a) AS6081 (Counterfeit Electronics Parts; Avoidance Protocol, Distributors)[7],

[6] http://standards.sae.org/as5553/

[7] Anne Poncheri, "AS6081-Fraudulent/Counterfeit Electonic Parts; Avoidance,Detection.Mitigation and Disposition-Distributor", SMTA/CALCE Counterfeit Symposium, June 2012

b) AS6301 (AS6081 Verification Criteria) and

c) ISO / IEC 17025 certified for counterfeit testing

For distributors to be compliant with these standards, all materials must be inspected, tested, and certified as non-counterfeit materials before they can resell the parts. This level of testing will add additional cost to the materials, but the risk will be significantly mitigated. The level of testing and controls required from the Distributor selected can be balanced in terms of the cost vs. risk avoidance benefit for your business needs.

For suppliers outside the authorized distribution channel, there are qualitative means to better assure end customers that your organization is providing genuine materials. Chief among these is to always know your source of supply which can be achieved by tracking and recording problems to provide a historical record of past transactions. This is particularly important for high-volume suppliers.

In addition, understanding parts and associated package types is a must. This affords the purchaser the ability to recognize the most blatant attempts at counterfeiting. This may lead to a limiting of drop shipping parts from their original source to an end customer with no handling by the intermediary party. There is an associated cost impact to inspect parts; however, it may be a necessary cost of doing business, in particular when there are unknown providers in the chain.

COUNTERFEIT DETECTION METHODS

Incoming inspection for counterfeit parts can be broken down into two basic categories[8] [9]:

1) Procedures that anyone can execute to provide the minimum level of protection

2) Procedures that require more analytical techniques utilizing specialized equipment and expertise

The following table provides a list of some different types of analytical and inspection techniques. See Appendix 2 for details of the detection methods.

Table 2: Counterfeit Detection Methods

	Minimum Inspections for Receiving Parts	**Detailed Analytical Inspection**
Non-destructive analysis Techniques	Optical inspection with stereo microscope	Scanning acoustic microscopy
	X-ray inspection	XRF analysis
	Electrical test	Functional Test
		Gene Test
Destructive Analysis Techniques	Solvent test	Cross sectioning and microscopic inspection
	Decapsulation test	SEM-EDX
		ICP/OES
		GC/MS
		UV-vis spectroscopy
		FTIR spectroscopy
		Ion chromatography (IC)

[8] Donald Davidson ,"An Assessment of Counterfeit Detection and Confirmation", SMTA/CALCE Counterfeit Symposium, June 2012

[9] Gary M. Beckstedt, Jr. ,"Supply Chain Management and Internal Inspection Techniques to Mitigate Counterfeit Component Impact", SMTA/CALCE Counterfeit Symposium, June 2011

NEXT STEPS

There are several identified tasks underway that will build on the Risk of Counterfeit Use calculator and the supply chain cluster maps. These future tasks include:

Task 4: Development of a methodology to evaluate or assess the aggregated risk of untrusted sources of supply, including how to identify potential risk of untrusted sources. In order of priority, some key factors that encourage untrusted sources include:

- Demand and product life - market potential for these products
- Ease of counterfeiting
- Sales channel
- Rework / disposal
- Ease of detection / consequences of detection
- Counterfeit controls on authentic product

Task 5: Development of an assessment / mitigation strategy which includes a methodology to estimate long term cost of ownership. Key factors on how to identify long term cost of ownership being considered are:

- Immediate revenue impact
- Warranty and service costs
- Brand damage
- Supply chain risk management (people, time and money)

Task 6: Definition and development of a metric that can be used to assess the magnitude of the problem.

FUTURE ACTIVITIES

The project team will consider additional activities that would constitute follow-on work (Phase 2 activities) and will develop an extension of this effort into a separate project. The development of protocol(s) to assist in identifying the pedigree of parts in the supply chain would fall outside the scope of this initial project and would be one possibility for Phase 2. This would involve definition of protocols for tracking the life of components such that a pedigree is developed for each part that identifies when, where, and under what conditions it was manufactured and what paths it has taken within the supply chain.

Methodology to Evaluate or Assess the Risk of Counterfeit use

Example Only

Product	Profile	Inputs					Process				Outputs						Total Rating
	Demand / EOL	Supplier	Supply Line	Mitigation & Controls	Supplier History	Score	Ease of Counterfeit	Ease of Detection	Counterfeit Controls	Score	Sales Channel	Excess Inventory & Prototype	Customer	Rework	Disposal	Score	
ASIC	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
FPGA	3	3	3	3	1	27	3	3	3	27	3	3	3	3	3	729	1454
FLASH	5	5	5	5	5	625	5	3	5	75	5	5	5	5	5	15625	49594
Hard Drive	3	1	1	1	1	1	5	3	2	30	4	4	5	3	5	6000	10892

Please select the rating from the table below that best corresponds to the description for that rating.

Rating = 1	Product has Low demand and/or is not EOL	OCM	Direct from OCM	Supplier has Strong Mitigation & Controls	No known Counterfeit Incidents	Very difficult to counterfeit; requires factory access or capital investment >$1M	Easy to detect, e.g. by check of packaging, documents, labels, history	Uses Unique Overt and Covert Controls & Identifiers that are easy to validate	Direct- OCMs/ Manufacturers /Suppliers	Minimal Excess inventory. Very limited prototyping/tight OCM security and traceabke records that are digitally signed/encrypted and/or indepedently audited.	Direct to OEM	In-house only under tight controls in certain designated areas, tight security and traceable records (signed/encrypted and/or independently audited)	In house only, on site physical destruction, traceable records (signed/encrypted and/or independently audited)
Rating = 2	No 2 rating	No 2 rating	No 2 rating	No 2 rating	No 2 rating	Requires major equipment / facilities such as wire bonders and laser markers, >$100k capital	Possible by optical inspection	Unique Overt or Covert Controls / Identifiers that are easy to validate	Known channel: Franchised/ Authorized Distributors	Excess and prototype inventory under tight controls and security	Trusted Sales Rep and Franchised Distributor to OEMs	In-house + vendor, under tight controls and security	In house + vendor physical destruction, traceable records, third party certification*
Rating = 3	Product has Low demand and is EOL or high demand and not EOL	Authorised Distributor	Multiple known suppliers	Some evidence of mitigation / controls	Counterfeit supply suspected	Requires moderate equipment and capital ($10k-100k)	Possible by routinely applied 2D X-ray inspection, decapsulation	Overt and Covert Controls / identifiers but validation not easy	Limited - OEMs/ CMs and some use of Brokers	Significant inventory but under tight controls and security	Trusted Sales Rep and Unfrachished distributor to CMs	Primarily offsite vendor based, with controls and security.	Offsite vendor, with controls and records for pyhsical destruction
Rating = 4	No 4 rating	No 4 rating	No 4 rating	No 4 rating	No 4 rating	Needs simple equipment such as sand blasters and ink printers (<$10k capital)	Requires advanced analytical tactics, i.e. XRD, CSAM, 3D X-ray	Some overt controls / identifiers but validation not easy	Very Limited - Primarily Reputable Independent Distributors/Brokers	Some controls in place. No traceable records. No security	Independent Distributors, dependent on end user oversite.	Offsite some controls in place. No traceable records. No security	Offsite vendor, some controls and records. No proof of physical destruction
Rating = 5	Product has High demand & is EOL	Boker or Ind. Distributor	Supply line not defined / clear	No evidence of mitigation / controls	Counterfeit supply confirmed	Easy - little / no investment required (<$1000)	Difficult to detect; nearly indistinguisible from authentic	No special controls in place	No control / Unknown-Unknown Independent Distributors/Brokers /Unknown Sources	Excess and prototype inventory not controlled	Customer not defined, open market.	Offsite Vendor, no controls and no traceability	Offsite Vendor, no controls and no traceability

APPENDIX 2:

INSPECTION AND ANALYTICAL METHODS FOR COUNTERFEIT DETECTION

Inspection for counterfeit parts at incoming inspection can be broken down into two basic categories; first one that almost anyone can execute for minimum level of testing and second those that require more analytical techniques utilizing specialized equipment and expertise.

First category for inspection – minimum inspections for receiving parts

1.1 Non-destructive analysis

a. Optical Inspection under a stereo microscope (2D or 3D OM).

Key items to look at include: package markings (part number, date code, lot number, logo and if it is made with laser or ink). Often times, font style ink quality and misspellings can give indicators of whether the marking is original or modified. The surface of the component body is inspected for any indicators of modification like scratches, evidence of contrasting gloss levels on the coating, residues. The pin 1 dimple is inspected for signs of grinding and possible residue from false coat. The leads are inspected for coated cuts and stress marks and for flux residue. Dimensions are validated with actual part measurements, especially in case of discrete passive components. Some types of taggants added by the OCM for authentication can be inspected.

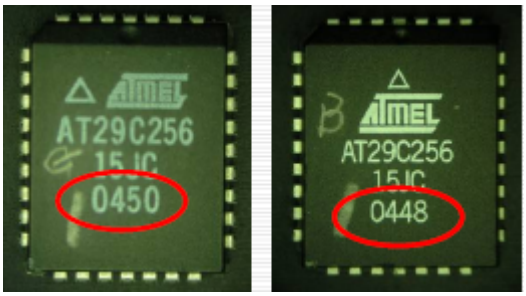

Figure 1: Comparison of package markings on IC.

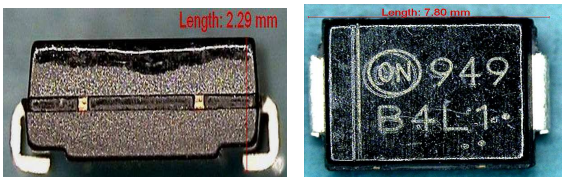

Figure 2: Examples of package modification indicators

b. X-ray inspection

Items to look for during x-ray inspection include the basic internal structure, die size, wire bond locations, missing wire bonds, excessive voids in silver epoxy, poor die attach, polarity of tantalum capacitors. If it is possible to save images from the X-ray imaging system, it could be useful to build a catalog of images for future reference.

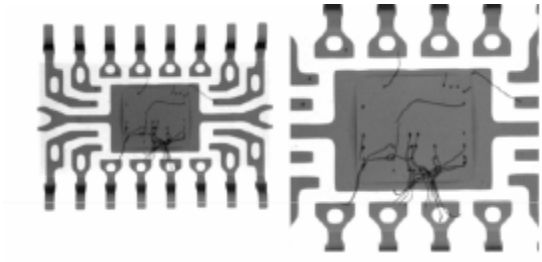

Figure 3: Abnormal wire bonding is found by X-Ray

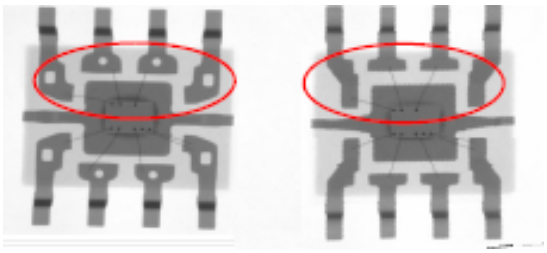

Figure 4: Bonding pad comparison by X-ray

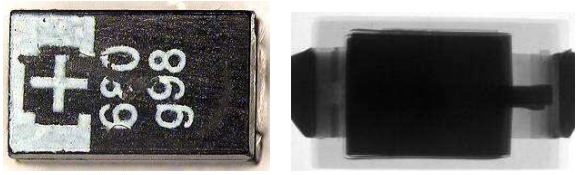

Figure 5: One can see the ink mark on the outside of the package but X-ray imaging reveals reverse polarity.

c. Electrical test, also called static test

Electrical parameters of passives are validated against specifications with an LCR meter. A curve tracer is used to show characteristics and polarity of discrete semiconductors and to compare with specifications such as threshold voltage or leakage current.

1.2. Destructive analysis

a. Solvent test

Various solvents can be applied for a marking permanency test or to test for false top coat.

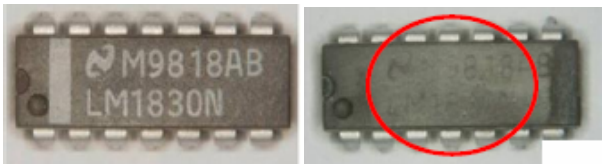

Figure 6: Marking confirmation with acetone.

b. De-capsulation test

Removal of the molding compound using chemical means to reveal the inner die surface permits inspection of the OEM die markings, device name, part number, design marks, the manufacturer's logo and review of the die edges for chipping.

Figure 7. Device name can be checked after decapsulation.

Second more complicated Inspections

These inspections listed below require some specialized equipment. Leverage of a qualified outside lab may be in the best interest if the minimum tests from above indicate some suspect characteristics that require more in-depth analysis.

2.1 Non-destructive analysis

a. Scanning Acoustic microscopy (C-SAM or TSAM)

This technique is not commonly used unless there is a special need. The method uses ultrasound to investigate the internal interfaces. Analysis using this technique is non-destructive. Operation of this type of equipment does require some level of expertise and training to be able to get and interpret the results. Items like delamination from the die, lead frame, or substrate and internal cracks due to stress may be investigated with this technique.

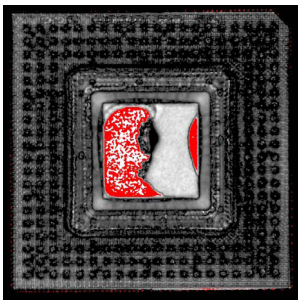

Figure 8: C-scan of BGA with severe delamination

b. XRF Analysis (EDXRF)

XRF is non-destructive provided the part does not need cutting to remove material which absorbs the fluorescence radiation from areas of interest. This technique can verify whether the elemental composition or the plating type and thickness are meeting the expected values. It can quantify materials that may be of interest like elements banned by RoHS, rare earth elements, or others intentionally added to facilitate authentication of the part.

c. Functional test

For integrated circuits, functional test usually requires automated test equipment, which is typically only accessible via the OCM or an external test service lab.

d. Gene test

A gene test is used to identify modified DNA added as a taggant.

2.2. Destructive analysis

a. Cross sectioning and microscopic inspection

After cross sectioning, one can inspect the internal structure of passive components, count the number of layers in ceramic capacitors, and look for stress cracks, delamination, and excessive voiding.

b. SEM-EDX.

The SEM can be used to analyze the surface morphology, e.g. to check for indications of sand blasting. SEM-EDX can be used to identify and quantify foreign elements and to confirm metallic plating.

c. ICP/OES

This technique is used to identify bulk composition and elemental levels with parts per million (ppm) accuracy. It is required for some RoHS tests.

d. GC/MS

GC/MS is used to identify or quantify compounds, e.g. the brominated compounds banned by RoHS.

e. UVvis spectroscopy

This technique is used e.g. to quantify the hexavalent chromium banned by RoHS.

f. FTIR spectroscopy

This technique is used to classify or identify compounds.

g. Ion chromatography (IC)

This technique is used to quantify the amount of various ions of interest on the surface of a sample.



EDXRF FTIR ICP-OES



UVvis IC GC/MS

SEM/EDX

Figure 9: Analytical Detection Methodologies