Methodology Development for Counterfeit Component Mitigation

Martin Huehne¹, Jeffrey ChangBing Lee², Harrison Miles³, Mark Schaffer⁴

¹ Celestica, Thailand
² IST – Integrated Service Technology Inc., Hsinchu, Taiwan, China
³ Corelis, USA
⁴ iNEMI, Virginia, USA

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 to its ability to recognize supply constraints and quickly respond, effectively taking advantage of a complex and vulnerable supply chain. Events like 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, aerospace, and defense. At the manufacturing level, the use of undetected counterfeits leads 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. For some time the weak link in the supply chain has been identified at the level of independent distributors. 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-Assessment project group takes a more 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 matrix that can be used to reduce the risks for manufacturers.

Keywords: Counterfeit component; Supply chain; Risk assessment matrix; Counterfeit detection

INTRODUCTION
The concept 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
- Options or upgrades

The Semiconductor Industries Association Anti Counterfeiting Task Force 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


“… 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. The scrap would subsequently be sold into the supply chain.

**Devices used as qualification samples**
OCMs and OEMs use 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.

**Reclamation and reuse of components**
Large quantities of electronic equipment containing working devices is scrapped. These products are usually dumped in landfill sites or crushed at refuse locations. 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 these devices 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 do not pass the more stringent testing 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 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.

SITUATION ANALYSIS

iNEMI segregates the electronics industry into the following product sectors:

- Aerospace and Defense
- Automotive
- Medical
- Netcom (Network, Data communications & Telecommunications)
- Office and Large Business Systems
- Consumer and Portable

Table 1: Industry Sector Desired Product Life-Cycles

<table>
<thead>
<tr>
<th>Industry</th>
<th>Sector</th>
<th>Desired Product Life-cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerospace &amp; Defense</td>
<td>Avionics (Civil)</td>
<td>10 to 20 years</td>
</tr>
<tr>
<td></td>
<td>Avionics (Military)</td>
<td>10 to 30 years</td>
</tr>
<tr>
<td>Automotive</td>
<td>Cars and Trucks</td>
<td>10 to 15 years (warranty)</td>
</tr>
<tr>
<td>Medical</td>
<td>External Equipment</td>
<td>5 to 10 years</td>
</tr>
<tr>
<td></td>
<td>Internal Equipment</td>
<td>7 years</td>
</tr>
<tr>
<td>Netcom (Telecom &amp; Data)</td>
<td>Infrastructure</td>
<td>10 to 30 years</td>
</tr>
<tr>
<td></td>
<td>Data Center</td>
<td>7 to 10 years</td>
</tr>
<tr>
<td>Office &amp; Large Business Systems</td>
<td>Industrial Controls</td>
<td>7 to 15 years</td>
</tr>
<tr>
<td>Consumer &amp; Portable</td>
<td>Appliances</td>
<td>7 to 15 years</td>
</tr>
<tr>
<td></td>
<td>Cell Phones</td>
<td>18 to 36 months</td>
</tr>
<tr>
<td></td>
<td>Laptop Computers</td>
<td>24 to 36 months</td>
</tr>
<tr>
<td></td>
<td>Desktop Computers</td>
<td>24 to 60 months</td>
</tr>
</tbody>
</table>

None of these product sectors is safe from the 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.

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 initial phase (Phase 1) of the project is broken into several high level tasks. The first three tasks that this paper is based on 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 Statement of Work, the project is focused on those attributes which are of most value to the supply chain and the participating project members and are applicable to multiple spaces across the supply chain. The primary effort was directed toward identification and development of metrics to assess the overall extent of the counterfeit problem in the electronics industry. The results 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 to understand the total cost of ownership associated with those risks. The methodologies and strategies developed will 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 pass these components to the end-user. Metrics to assess the overall extent of the problem and the prevalence and success level of anti-counterfeiting efforts will be identified for all phases. The remaining set of tasks are outlined in the Next Steps section.

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

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 to identify the key players in each manufacturing sector (Figure 2).
The Board Manufacturer Cluster diagram (Figure 2) highlights two principle 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 the supply chain and evading traceability of the pedigree of the electronic components. Condition favoring the counterfeit pathways will most commonly exist during extreme supply disruptions (e.g., specific component shortages) or as a result of new entrants into the workflow or substantial growth in a major flow block role play. A good example is the increasing role that recycling and disposal is playing in the global movement towards green manufacturing.

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.

**CALCULATING RISK OF COUNTERFEIT USE**

*Note: Figure 3 is an example of the 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 know history of counterfeit supply.

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 determining 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 highest when the sales channel is unknown; there is no control or traceability on excess inventory, prototypes, reworks or scrap; and the end customer is unknown. In contrast, where the end customer is well known; the sales channel is well defined; and the excess inventory, prototypes, reworks and scrap are well controlled, the outputs risk is lowest.

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. Standard AS5553A 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 3rd party certification body and is compliant with:

a) AS6081 (Counterfeit Electronics Parts; Avoidance Protocol, Distributors) [3],
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 you require from the distributor you select can be balanced in terms of the cost vs. risk avoidance benefit for your business needs.

For those 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. This 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: [4,5]
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 for details of the detection methods.

### Table 2: Counterfeit Detection Methods

<table>
<thead>
<tr>
<th>Minimum Inspections for receiving parts</th>
<th>Detailed Inspection</th>
<th>Analytical Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-destructive analysis Techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optical inspection with stereo microscope</td>
<td>Scanning acoustic microscopy</td>
<td></td>
</tr>
<tr>
<td>X-Ray Inspection</td>
<td>XRF analysis</td>
<td></td>
</tr>
<tr>
<td>Electrical Test</td>
<td>Functional Test</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gene Test</td>
<td></td>
</tr>
<tr>
<td>Destructive Analysis Techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solvent test</td>
<td>Cross sectional and microscopic inspection</td>
<td></td>
</tr>
<tr>
<td>Decapsulation Test</td>
<td>SEM-EDX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICP/OES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GC/MS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UV/vis spectroscopy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTIR spectroscopy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ion chromatography (IC)</td>
<td></td>
</tr>
</tbody>
</table>

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.

REFERENCE

APPENDIX:
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.

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.

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.
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 6: Marking confirmation with acetone.

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.

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.
Figure 9: Analytical Detection Methodologies