Avoiding Counterfeit Electronic Components

Counterfeit EEE Parts Panel
Henry Livingston, BAE Systems
Definitions

• Counterfeit Electronic Component
  • Equipment Manufacturing Industry
  • Semiconductor Manufacturing Industry
  • Independent Distributor Industry
  • U. S. Government

• An Aerospace and Defense Equipment Manufacturer’s View
  • What is a counterfeit electronic component?
  • What is not?
Electronics Manufacturing Industry Definition

The following definition* was developed by the Electronics Manufacturing Productivity Facility (EMPF) of the American Competitiveness Institute (ACI)

- Counterfeit electronic components and boards are defined as:
  - Substitutes or unauthorized copies of a product
  - A product in which the materials used or the performance of the product has changed without notice
  - A substandard component misrepresented by the supplier

- Per recent correspondence with the ACI/EMPF, the second item applies to changes in materials or performance made by the original part or material manufacturer without notifying the user before offering the part.

B. Partee, “Empfasis article - Counterfeit Components (December 2003)”, bpartee@aciusa.org,
e-mail received 1 November 2006
Semiconductor Manufacturing Industry Definition

- The following definition was provided by Anti-Counterfeiting Task Force (ACTF) of the Semiconductor Industries Association (SIA) * … (derived from the ACI/EMPF definition)

- Counterfeit electronic components are defined as:
  - Substitutes or unauthorized copies of a product
  - A product as defined by the manufacturers part number ID, date code and Manufacturers ID in which the materials used or the performance of the product has changed without notice by someone other than the original manufacturer of the product.
  - A substandard component misrepresented by the supplier

* J. Stradley (chairman), "Anti-Counterfeiting Task Force", December 05, 2006
Independent Distributor Industry Definition

• The following definitions* were developed by the Independent Distributors of Electronics Association (IDEA) …
  • Counterfeit Product:
    • Items that are produced or distributed in violation of intellectual property rights, copyrights, or trademark laws.
  • Fraudulent Product/Transaction:
    • Items that are deliberately altered in such a way as to misrepresent the actual quality of the item with intent to defraud or deceive the purchaser. Any information omitted or means taken to mislead the purchaser to believe that such items are authentic or lawful.

• Using the Term "Counterfeit"

  “Quality independent distributors do not typically use the term "counterfeit" unless the manufacturer of the product states that they have determined the product is counterfeit in writing. Instead independent distributors typically condition the term "counterfeit" with the word "suspect", meaning that based on the expertise that resides within that independent distributor's business that they suspect that the part may indeed be counterfeit.”

• Additional definitions developed for …
  • Refurbished, used and unused parts
  • Franchised Distributor, Independent Distributor, Broker

* IDEA-STD-1010-A, Acceptability of Electronic Components Distributed in the Open Market.
Copyright © Independent Distributors of Electronics Association (IDEA) 2006 (http://www.idofea.org/)
U. S. Government Definition

The following definition* was developed by the U.S. Department of Energy, Office of Environment, Safety and Health (Office of Corporate Performance Assessment)

- A counterfeit item is a suspect item that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer.

- A suspect item is one in which there is an indication by visual inspection, testing, or other information that it may not conform to established Government- or industry-accepted specifications or national consensus standards.
  - Suspect items must be further investigated to determine whether they are counterfeit. When an item contains indications, but insufficient evidence, of irregularities such as noncompliance with agreed-upon specifications in the manufacturing process, it may be declared suspect.

* DOE HS-32 Suspect/Counterfeit-Defective Items website (http://www.eh.doe.gov/sci) ...
S/CI Awareness Training Manual (October 2006)
Counterfeit Electronic Components …
An Aerospace and Defense Equipment Manufacturer’s View

• A counterfeit item is one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer. (From a definition developed by the U.S. Department of Energy)

• Counterfeiting often involves cases where parts are offered that present a product substitution risk to the Government Equipment Manufacturer and to the Government user. Examples include …
  • Parts remarked to disguise parts differing from those offered by the original part manufacturer (e.g. original manufacturer, country of origin, specified performance)
  • Defective parts scrapped by the original part manufacture
  • Previously used parts salvaged from scrapped assemblies

… These are incidents that jeopardize the performance and reliability of electronics and are the subject of ongoing criminal investigations by the US Government
What is not a Counterfeit Electronic Component? …
An Aerospace and Defense Equipment Manufacturer’s View

• The following methods are not associated with counterfeiting …
  • “Refinishing” parts to support assembly producibility and ensure equipment reliability
  • “Upscreening” parts to satisfy customer requirements
  • “Uprating” parts to assess their capability to meet the performance requirements of the application in which the part is used outside the manufacturer’s specification range

… These are methods applied by Electronics Manufacturers and Government users to assure parts will fulfill equipment performance and reliability requirements
What is not a Counterfeit Electronic Component? …
An Aerospace and Defense Equipment Manufacturer’s View

• “Refinished” parts …
  • Pure tin has been used by commercial industry for many years and has now become a popular “Lead Free” solution for part manufacturers who discontinued the use of a Tin-Lead (SnPb) terminal finish.
    • As a result of the reliability issues presented by the use of pure tin and other lead-free components in high performance assemblies and systems, many manufacturers are looking for component level mitigation techniques to retain or increase the reliability of their products.
    • One such method, known as solder dipping, involves replacing the unwanted finish of a component with a more desirable type.
      • See GEIA-STD-0006 (draft), “Requirements for Using Solder Dip to Replace the Finish on Electronic Components”
What is **not** a Counterfeit Electronic Component? …
An Aerospace and Defense Equipment Manufacturer’s View

• “Upscreened” parts …
  • Many Government customer requirements demand additional testing to ensure parts will meet equipment reliability demands. Examples include …
    • Particle Impact Noise Detection (PIND) testing to screen out parts containing free particles within the cavity of the package
    • Sequential environment testing of plastic packaged parts that are not available as hermetic, military grade product offerings
    • Radiation Hardness Assurance testing to meet space application requirements
What is not a Counterfeit Electronic Component? …
An Aerospace and Defense Equipment Manufacturer’s View

• “Uprated” parts …
  • “Uprating” is a process to assess the capability of a device to meet the performance requirements of the application in which the device is used outside the manufacturer’s specification range.
    • Many device manufacturers have exited the military market in recent years, resulting in decreased availability of devices specified to operate over wide temperature ranges.
    • If there are no reasonable or practical alternatives, then a potential response is for equipment manufacturers to use devices in temperature ranges that are wider than those specified by the device manufacturer.
      • See EIA-4900, “Use of Semiconductor Devices Outside Manufacturers’ Specified Temperature Ranges”
Strategic & Proactive Approaches to Avoiding Counterfeit Electronic Components

• Distributor selection
  • Franchised / Authorized Distributors
  • Independent Distributors

• Risk Mitigation Methods to Avoid Counterfeit Electronic Components

• Outsourcing Electronic Component Procurement

• Aftermarket Supply Issues

• Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management
Franchised and Authorized Distributors

- The most effective approach to avoiding counterfeit electronic components is to purchase product …
  - Directly from the original manufacturer, or
  - From a distributor, reseller or aftermarket supplier who is franchised or authorized by the original manufacturer
    - Contractual bond between the original manufacturer and the distributor …
      - Original manufacturer warrantee
      - Product integrity via proper handling, storage and shipping procedures
      - Failure analysis and corrective action support
      - Traceability via certificates of conformance and acquisition traceability
  - Franchised distributors include large and small businesses, including Small Disadvantaged Businesses (SDB)
    - Consult the original manufacturer for distributors, resellers or aftermarket suppliers who are franchised or authorized by the original manufacturer

- A substantial number of products, however, are no longer available through these channels.
  - Independent distributors will continue fill this gap.
Independent Distributors

• Independent distributors purchase new excess inventories from end users with the intention to sell and redistribute back into the market.

• Independent distributors subsequently sell (re-distribute) the new parts from these excess inventories to fulfill inventory shortages with hard-to-find, obsolete, and competitively priced parts.

• End users are typically original equipment manufacturers (OEMs) and contract manufacturers (CMs) at locations all over the world.

• Independent distributors do not typically have limiting contractual agreements or obligations to the components manufacturers.

From …
IDEA-STD-1010-A, Acceptability of Electronic Components Distributed in the Open Market.
Copyright © Independent Distributors of Electronics Association (IDEA) 2006 (http://www.idofea.org/)
A Case Study

- **GIDEP Alert J5-A-07-01 (12/5/2006)**
  - BAE Systems expected to receive 5962-8768401QA with the QP Semiconductor manufacturer identification mark.
  - BAE Systems received parts marked with Part Identifying Number (PIN) 5962-8768401QA, the Philips Semiconductor manufacturer identification and date code 0336.
    - Philips Semiconductor discontinued producing all military grade products in 1997.
  - Part marking did not include a country of origin mark required by MIL-PRF-38535.
  - Parts contained die manufactured by Intel marked 1980.

- **BAE Systems purchased these parts from …**
  - Port Electronics Corp … who purchased them from …
    - Aapex International Inc … who purchased them from …
      - Newkoda (H.K.) Electronics Co … who purchased them from …
        - Chao Yang Hualian Electronic Co … who purchased them from …
          … ? …
Risk Mitigation Methods to Avoid Counterfeit Electronic Components

• The following mitigation methods can be applied to reduce the risk of receiving counterfeit parts when acquired through an independent distributor (e.g. “broker”) …
  • Traceability Documentation
    • Without certificates of conformance and acquisition traceability, the purchaser takes on unknown risks.
    • The independent distributor’s own acquisition certification should be in addition to the certificates of conformance and acquisition traceability provided by the manufacturer and previous distributors.
  • Compliance Verification (authenticity analysis)
    • Visual Inspection
    • Testing
    • Physical Analysis
    … particularly when the independent distributor cannot produce certificates of conformance and acquisition traceability through their supply chain
Counterfeit Detection

• GIDEP documents reporting suspect counterfeit cases provide further insight into detection techniques

• The Independent Distributors of Electronics Association (IDEA) published a standard which includes inspection techniques for counterfeit detection …

• Recent industry symposia include information on counterfeit detection techniques…
Caution …

- These risk mitigation methods may not definitively distinguish authentic parts from counterfeits without
  - Comparison to known authentic examples
  - Assistance from the original manufacturer

- Without knowledge and verification of the handling, storage and shipping procedures applied throughout the supply chain, the purchaser takes on the risk of acquiring damaged parts

- Cases have been reported where samples from parts offered by a broker were examined to verify authenticity prior to shipment, but the parts subsequently shipped by this broker were counterfeit
  - See GIDEP Alerts PD-A-06-01 and PD-A-06-02
Counterfeit Detection Support from Original Component Manufacturers

• Some original component manufacturers (OCMs) will provide support to users who believe they may have received counterfeit parts
  • Example: Maxim Worldwide Security
    http://www.maxim-ic.com/sales/counterfeit_parts.cfm

• Obtaining support from OCMs can be a significant challenge
  • OCMs have no obligation to provide support for products that are not acquired through their franchised or authorized distributors, resellers or aftermarket suppliers
  • OCMs discourage users from purchasing their products from Independent Distributors
Independent Distributor Selection

• Source selection should include an assessment of the independent distributor’s ability to verify the authenticity of the products they offer.
  • Certificates of conformance and acquisition traceability
  • Compliance verification via visual inspection, testing and physical analysis
  • Purchasing and acceptance practices
    • Subscribe to self-policing organizations
    • Use of escrow services to hold the money until the independent distributor verifies the authenticity of products offered
    • Use of net one or net two-day payment where the seller ships the parts and the distributor has one or two days to inspect and accept them before the distributor wires payment

• Examples of industry standards that can be used for evaluating the suitability of an independent distributor
  • JESD31, General Requirements for Distributors of Commercial and Military Semiconductor Devices. (JEDEC [http://www.jedec.org/download/])

• Vet the independent distributor in advance of procurement activity to ensure …
  • Suspect counterfeiting incidents have not occurred previously with this distributor
  • The independent distributor has the financial means to support any contractual guarantees expected
Outsourcing Electronic Component Procurement

- Some users outsource procurement to another entity
  - Electronics Manufacturing Service (EMS) provider
  - Contract Manufacture

- The selection of an EMS provider or Contract Manufacturer should include audits of their methods and purchasing records to ensure their procurement practices mitigate the risk of acquiring counterfeit parts.
  - Refer to “Independent Distributor Selection”
Aftermarket Supply Issues

- Some aftermarket sources produce finished products from a die bank
  - Residual inventory of die no longer in production

- These aftermarket sources do not always issue End-of-Life notices or notify their industry and Government customers when die inventory is exhausted
  - In one case, DSCC (not the aftermarket manufacturer) issued a notice when notified that die inventory had been exhausted
  - A review of the GIDEP database showed no DMS notices issued by this manufacturer
  - End-of-Life notices were not published on the manufacturer’s website

- Users are encouraged to periodically contact aftermarket sources concerning their continued ability to supply products
Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management

- A significant driver for the use of independent distributors is the continued need for parts that are no longer produced by the original manufacturer.

- In order to reduce the likelihood of having to purchase parts through an independent distributor, Electronic Equipment Manufacturers should proactively manage the life cycle of their products versus the life cycles of the parts used within them.
  - GEIA Handbook GEB1 includes key practices used during system development and support to mitigate the effects of future obsolescence.
  - GEIA GEB1, Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Practices.
### GEIA GEB1, Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Practices

#### Phase 0 to Phase III:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Concept Exploration</th>
<th>Program Definition and Risk Reduction</th>
<th>EMD / LRIP</th>
<th>Production, Fielding / Deployment, &amp; Operational Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 0</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Phase I</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Phase II</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Phase III</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

#### Proactive DMSMS Mitigation Approaches (4.1):
- **Technology Road Mapping**: X
- **Planned System Upgrade**: X
- **Technology Insertion**: X
- **Technology Transparency**: X
- **Life Cycle Analysis / DMSMS Monitoring**: X

#### Response to DMSMS Events (4.2):
- **Alternate Source**: X
- **Substitution**: X
- **Emulation**: X
- **Life of Type Buy**: X
- **Redesign / Design Modification**: X
- **Reverse Engineering**: X
- **Reclamation**: X

---

**Planning for system upgrades in Phase I & II based upon Technology Insertion Solution**

**Bridge buy to support production until redesign available**

**Reclamation typically a last resort**

---

*Approved for public release; distribution is unlimited.*
GIDEP Reporting for Counterfeit Parts

- Many suspect counterfeit component cases are reported via GIDEP using Failure Experience documents (AL, PA, AN, LL)
  - These document types were designed for reporting quality or reliability deficiencies associated with parts, materials, etc. produced by a given manufacturer
  - Failure Experience documents not well suited for reporting suspect counterfeit cases;
    Conventions used by participants are not consistent
    - “Manufacturer” (Block 4) and “CAGE” (Block 12) sometimes used to identify the supplier of the counterfeit …
      in other cases the manufacturer whose part was counterfeited is reported here
    - Limited data fields to report additional suppliers involved a particular counterfeit case
GIDEP Reporting for Counterfeit Parts (continued)

• GIDEP planning to establish a new document type for reporting suspect counterfeits

• GIDEP issued interim guidance to GIDEP representatives for reporting suspect counterfeits using existing Failure Experience reporting vehicles
  • See “Weekly News - 22 January 2007”…
  “Guidelines for Reporting Suspect Counterfeit Products”

• GIDEP point of contact …
  Ms. Jinhee Graebe, Failure Experience Data Manager
  jgraebe@gidep.org
  951-898-3245
GEIA G-12 Solid State Devices Committee
Counterfeit Parts Task Group

- The GEIA G-12 Solid State Devices Committee develops solutions to technical problems in the application, standardization, and reliability of solid state devices.
  - The G-12 Committee evaluates and prepares recommendations for specifications, standards, and other documents, both government and industry, to assure that solid state devices are suitable for their intended purposes.

- G-12 Counterfeit Parts Task Group
  - Charter: To develop a set of guidelines that include mitigating strategies that can be used within the industry to mitigate the risk of receiving counterfeit parts from various supply chains.
    - Operating Guidelines and Security Measures
    - Mitigation of Part Damage
    - Mitigating Strategies for future procurement of parts, materials, and processes
    - GIDEP Reporting
    - ... etc ...

http://www.geia.org/
Summary

- In today’s supply chain environment, electronic equipment manufacturers and Government users must be vigilant in order to avoid counterfeit electronic components.
  - The vast majority of counterfeit cases reported are associated with purchases through independent distributors.

- The most effective approach to avoiding counterfeit electronic components is to purchase product directly from the original manufacturer, or from a distributor, reseller or aftermarket supplier who is franchised or authorized by the original manufacturer.
  - A substantial number of products, however, are no longer available through franchised or authorized suppliers.

- While they provide a necessary function within the electronic component supply chain, independent distributors are not all created equal.
  - Electronic equipment manufacturers and Government users need to understand the independent distributor’s operations and business processes.
  - When considering purchases through independent distributors, electronic equipment manufacturers and Government users should use mitigation methods and strategic approaches to reduce the potential for acquiring counterfeit parts.