Risk Management for Counterfeit Materials: The Role of the COTS Board Manufacturer

"One of the worst trends to emerge in military systems design involves counterfeit electronic parts – those that appear genuine, but are actually substandard, altogether different, or in the worst cases, simply empty packages." – Military & Aerospace Electronics, John Keller editorial, July 2007.

"The garbage-strewn streets of Guiyu [China] reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards [which are] cleaned in the nearby Lianjiang River […]. A sign […] advertises […] 'military' circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But [the] proprietor admits that his wares are counterfeit. His employees sand off markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says […]" - BusinessWeek.com, Dangerous Fakes by Brian Grow et al, October 2, 2008.

Introduction

Numerous media reports and investigations, coupled with public statements by government and industry players, provide ample evidence to suggest that the proliferation of counterfeit parts and materials in the electronics industry is becoming increasingly widespread. Factors such as technology and globalization are helping to increase the sophistication and availability of counterfeit components, making the supply chain more vulnerable to infection.

This situation is forcing the industry to develop strategies to maintain the integrity and reliability of its products. As vigilance increases, the number of confirmed cases will most likely continue to grow.

Definitions

The definitions of counterfeit material and the more conditional term "suspect" can slightly vary within industry groups or government bodies. In general, "counterfeit" typically denotes a violation of intellectual property rights or trademarks, substitution, unauthorized copying, changing of materials without notice, remarking defective or used parts, and other fraudulent, related acts. Suspect materials are those thought to be counterfeit, based on preliminary inspection or testing, but require further investigation before being declared counterfeit.

Counterfeiting Methods

Counterfeit parts can be produced in a variety of ways:

- Relabeling – original labeling may be physically removed, or simply covered and remarked with the required markings. These may be parts of similar functionality to the authentic ones or they could be completely different.
- Reclaiming – authentic parts may be salvaged from discarded circuit card assemblies. Verification of functionality within specifications will not exist.
- Unauthorized manufacture – manufactured and marked to duplicate authentic parts. Technology has increased the effectiveness of this approach, but parts are unlikely to have verification of functionality within specifications.
- Production escapes – test fallout from authorized manufacturing facilities packaged and sold as authentic parts.

Counterfeiting is not limited to actual components. A thorough effort could include fake packaging and supporting documentation.

The Vulnerability of the Defense Industry

The military and aerospace electronics market demands safety and reliability. Electronic systems – and the individuals who rely on them – often operate in demanding, harsh, perilous environments. Therefore, industry players must be extra vigilant in mitigating the risks posed by counterfeit electronic components. There are a number of factors in this market that increase its susceptibility:

- Enhanced temperature and reliability specification requirements.
- Long program/platform lifecycle requirements.
- Diminishing source of supply base.

The responsibility to mitigate the risks posed by counterfeit materials lies throughout the entire supply chain. The commercial-off-the-shelf (COTS) board manufacturer is in a unique position to act as a gatekeeper for its direct and indirect customers further along the chain. Being the last to handle individual components prior to their becoming part of a board level product, a COTS hardware manufacturer must have established processes to reduce the risk of introducing counterfeit parts to its products.

Obsolescence Management

In the military and aerospace market, having to source obsolete components increases the risk of procuring counterfeit parts. This issue stems from unique factors that prevail in this industry:

- Diminishing market weight of the defense segment in the electronics industry.
- Design, production and support cycles that often extend much longer than for most commercial applications.
- A small supply base to support ruggedized component requirements.

Recognizing the realities of these market forces, Curtiss-Wright Controls Embedded Computing, a designer and manufacturer of COTS VME, VPX and CompactPCI products for the aerospace and defense market, has developed processes to mitigate the risks introduced by component obsolescence:

- Product development process includes analysis of forecasted lifecycles and commercial availability of components & technologies, in order to support product lifecycles.
- Resources are allocated to monitor lifecycles and address issues as they occur.
- Internal expertise is augmented with industry monitoring and forecasting services.

The reality of today's COTS market is that component life spans are becoming more abbreviated. Component

manufacturers must keep pace with their customers' demanding product release schedules, as their newest commercial electronic devices are rushed to market. Curtiss-Wright addresses this reality by offering its military and aerospace customers Continuum Lifecycle Services throughout the life of their programs, such as:

- Locking/controlling product configurations.
- Forecasting component obsolescence impacts.
- Supporting longevity of supply and repair beyond the normal product end-of-life period.

In the event of component obsolescence, possible courses of action include:

- Component substitution by an equivalent or better component.
- Customer-funded, component lifetime buy.
- Redesign to replace the affected part.
- Eliminate the function associated with affected part.

The level of risk and appropriate action to address that risk will vary, depending on the customer, the application, production volumes and production lifecycle requirements.

Supply Chain Management

A COTS board designer that operates its own manufacturing facilities has an obvious advantage regarding visibility and control over the materials used in the fabrication of its products. The capabilities and processes that are required to run such an operation allow a company to dynamically react to market conditions that often influence the need to seek alternative supply solutions. Safety stock levels can be set in the material/enterprise resource planning (MRP/ERP) system. In addition, the MRP data can be shared with key suppliers to establish future supply requirements.

Avoidance of counterfeit parts is best accomplished by sourcing materials directly from the component manufacturer, from authorized after-market support or from franchised distributors. Components from these supply sources will have supporting documentation which provides an auditable pedigree.

Counterfeit components most commonly enter the supply chain through independent distributors, also known as brokers. These suppliers are typically used when the manufacturer-authorized sales channels cannot support required deliveries. Independent distributors may source materials from authorized channels, acquire surplus inventory from equipment manufacturers or buy from other brokers. The further from the original source the supply chain extends, the greater the risk of introducing counterfeit components.

The Independent Distributors of Electronics Association (IDEA) has acknowledged its members' susceptibility to counterfeit components. To address concerns, in 2006 the Association published IDEA-STD-1010-A – Acceptability of Electronic Components Distributed in the Open Market. As indicated on the IDEA web site (idofea.org), this publication is "the first inspection standard addressing the needs for the inspection of electronic components traded in the open market. This standard is a must for all quality assurance and inspection departments."

Figure 1: IDEA-STD-1010-A Standard - Acceptability of Electronic Components Distributed in the Open Market

A Real World Example of Supply Chain and Quality Management

Curtiss-Wright manages its supply chain by maintaining an Approved Vendors List (AVL). In order to qualify as an approved vendor, all suppliers are subject to audits and must be able to comply with Quality Clauses assigned to every purchase order.

Moreover, all independent distributors who wish to become a Curtiss-Wright supplier must be certified based on the following criteria:

- Successful audit by Curtiss-Wright.
- IDEA member with IDEA certified inspectors or ERAI member (Electronic Resellers Association International).
- ISO or AS9100 certified (or currently compliant with a plan to be certified).
- Formally documented anti-counterfeit plan/program.

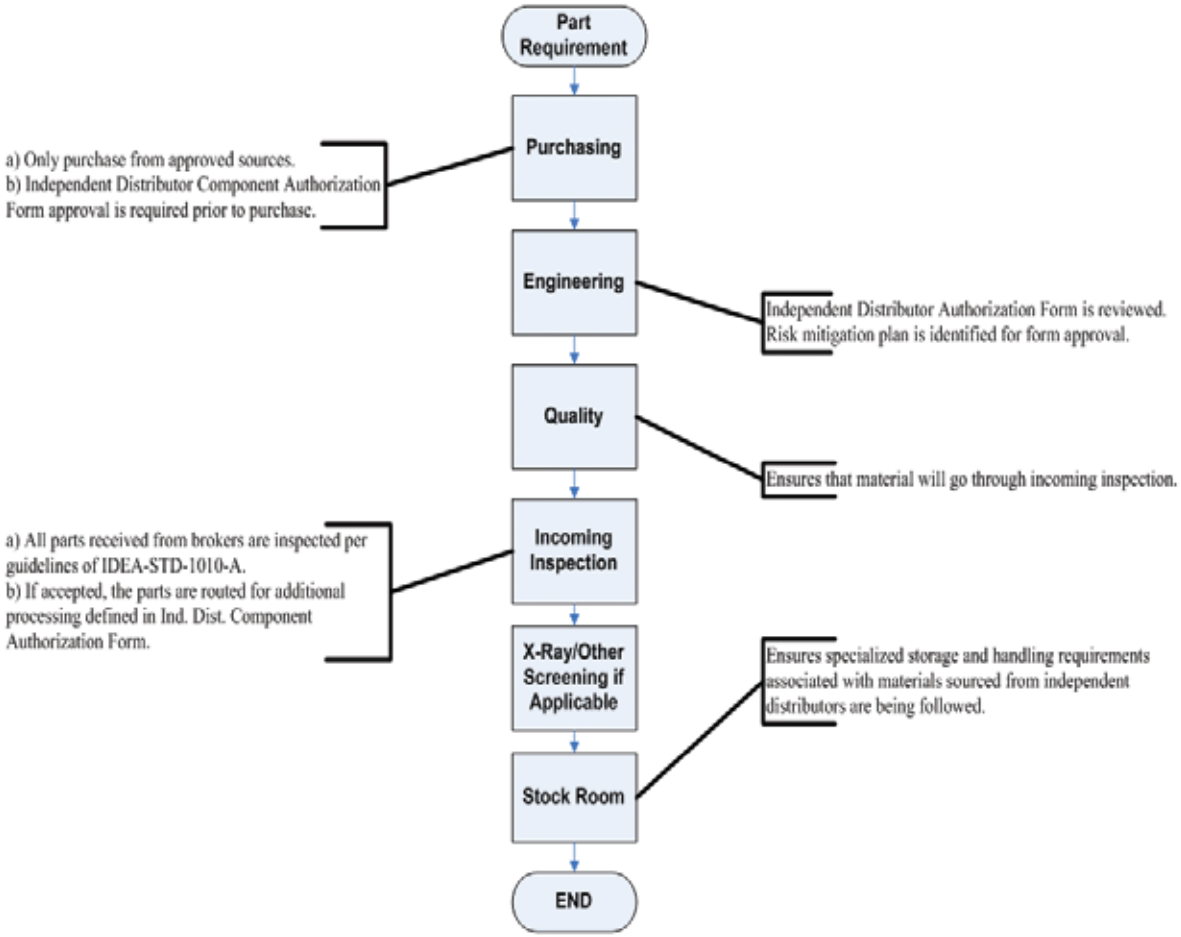
Acknowledging the additional risks associated with materials procured from brokers, Curtiss-Wright has implemented enhanced controls for this aspect of the supply chain, in order to mitigate these risks.

For instances where sourcing materials from independent distributors is considered necessary, Curtiss-Wright initiates an authorization process. This process requires Procurement, Engineering and Quality representatives to confirm that all other viable options have been explored. In addition, risk mitigation processes are defined for the required material, prior to use within Curtiss-Wright products.

Means of risk mitigation may include:

- Comparison to known acceptable materials.
- Verification with original manufacturer.
- 3rd party destructive physical analysis.
- 3rd party electrical/functional testing.
- In house electrical/functional testing within the application.

Figure 2: Independent Distributor Process



Component Inspection

Incoming inspection sampling plans are standard practice for Original Equipment Manufacturers. Component inspection is intended to verify accurate delivery and acceptable quality of the received materials.

Curtiss-Wright recognizes that materials sourced through independent distributors require additional controls to assure quality:

- Flags are set within the Curtiss-Wright MRP system for 100% inspection.
- Materials are inspected as per the guidelines of IDEA-STD-1010-A by trained Quality Assurance personnel. Depending on the material type, this may include on-site X-ray inspection or 3rd party destructive physical analysis.
- Moisture sensitive components are subjected to a bake process and repackaging.

All materials received by Curtiss-Wright are assigned Material Receipt Record numbers. This allows materials to be tracked from the time of receipt through to final assembly. If at any time inspection or test shows a specific lot of components to be suspect, Curtiss-Wright will implement containment procedures.

Once identified, suspect components are rejected as non-conforming materials. A Quality Notification is logged within the Quality Management System and the parts are transferred to the control of the Material Review Board (MRB).

Non-conforming Materials

The MRB has the authority to subject the components to further analysis when required. Options available to the MRB include:

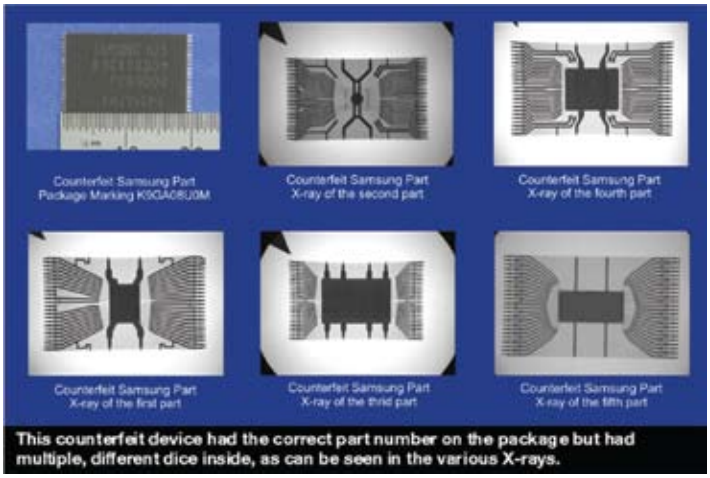
- Comparison to known good materials.
- Verification with original manufacturer.
- 3rd party destructive physical analysis.
- 3rd party electrical/functional testing.

Control of non-conforming materials include:

- Identification and segregation of the non-conforming materials to prevent inadvertent use and shipment.
- Documenting the non-conformance.
- Assessment and disposition of the non-conforming materials.

Components deemed acceptable by the MRB are reintroduced to the process for receiving and stocking the materials.

Figure 3: Semiconductor Insights Counterfeit Analysis (Source: EE Times, Aug. 2007)



Production Test and Quality Monitoring

Curtiss-Wright performs functional testing on all of its products. For ruggedized boards, Environmental Stress Screening (ESS) may also be included as part of the standard production test flow.

Depending on the quality of the suspect component, the 100% production test approach offers another level for detection. If suspect materials do not meet the functional characteristics of an authentic device, assembly level production testing offers another opportunity to prevent these parts from being populated in shippable product.

To augment the effectiveness of production testing and repairs of fielded product, all test failures are logged within the Quality Management Database. Components that have been removed and deemed to contribute to test failures are retained to undergo further analysis by Curtiss-Wright's Failure Reporting, Analysis and Corrective Action System (FRACAS).

Failure Reporting, Analysis and Corrective Action System (FRACAS)

FRACAS is a closed loop failure reporting system. It provides a process for collecting data, performing analysis of failures to determine cause, and implementing corrective actions when a trend is identified relating to manufacturing and test processes. The FRACAS system is established and

implemented for all Curtiss-Wright testing activities during the production and in-service phases of product life cycle.

FRACAS data is analyzed and reported at each Curtiss-Wright Monthly Quality Review. Failure trends are investigated. If the root cause is determined to be severe in its impact to the reliability of fielded product, Curtiss-Wright initiates a Problem Resolution Board (PRB) to determine the appropriate corrective action. The PRB is composed of senior management and therefore has the authority to initiate product recalls as required by the circumstances.

Quality Management System

Curtiss-Wright's Quality Management System (QMS) is certified to the SAE AS9100 standard. To ensure the effectiveness of the QMS, Curtiss-Wright:

- Identifies the processes needed for the QMS and their application throughout the organization.
- Determines the sequence and interaction of these processes.
- Determines criteria and methods needed to ensure that both the operation and control of these processes are effective.
- Ensures the availability of resources and information necessary to support the operation and monitoring of these processes.
- Monitors, measures and analyzes these processes.
- Implements actions necessary to achieve planned results and continual improvement of these processes.

All of the supporting processes used to mitigate the risks of suspect materials are controlled by and compliant to the QMS.

Summary

Counterfeit materials will continue to challenge the defensive capabilities of manufacturers in the military and aerospace industry. With industry-leading obsolescence and supply chain management, combined with thorough inspection, testing and quality assurance procedures, Curtiss-Wright Controls Embedded Computing is committed to delivering reliable, high quality product to its customers.

Contact Information

The most recognized body that provides a means of tracking counterfeit material occurrences is the GIDEP (Government-Industry Data Exchange Program). The GIDEP provides a conduit for the electronics industry (and others) to report suspect or counterfeit parts experiences. Curtiss-Wright Controls Embedded Computing is an active member of the GIDEP.

For more information on the Government-Industry Data Exchange Program, visit http://www.gidep.org.

ERAI (Electronic Resellers Association Inc.) is a global trade association that monitors, investigates, reports and mediates issues that are affecting the global supply chain of electronics. ERAI currently focuses much of their time and attention to the detection and prevention of counterfeit computer components.

For more information on ERAI, visit http://www.erai.com.

To learn more about Curtiss-Wright Controls Embedded Computing, visit http://www.cwcembedded.com.