Technology Today

2012 Issue 1

In the broadest sense, *counterfeiting* is the deliberate misrepresentation of an item with the intent to deceive a customer or an end user. Counterfeiters have found discarded commercial electrical and electronic products to be a good source of raw material for their illegal activities. By modifying external markings, for example, counterfeiters can "manufacture" practically any part and sell it to unsuspecting customers through oftentimes deceptive and misleading advertisements/websites. However, the parts sold can be used or damaged, be incorrect or even be functionally different. Customers are lured into buying these counterfeits when they attempt to acquire parts that are in short supply, are obsolete or are no longer available with the required package type or materials from the original component manufacturer (OCM) or authorized distributors.

A U.S. Department of Commerce study released in January 2010[1] reported that the number of documented counterfeit incidents has risen dramatically, more than doubling from 3,369 incidents in 2005 to 8,644 incidents in 2008. In this study, an incident consisting of at least a single encounter with a suspected/confirmed counterfeit could have involved just one part or thousands of parts. The increase in incidents can be attributed not only to the growth in the number of counterfeit parts but also to better detection methods and/or improved tracking of counterfeit incidents. The study indicates that counterfeit activity reported by manufacturers of discrete components is highest for electromechanical devices and high-power semiconductors. Manufacturers of microcircuits cited microprocessors as the most prevalent counterfeit part. Asia was identified by OCMs as the predominant regional source.

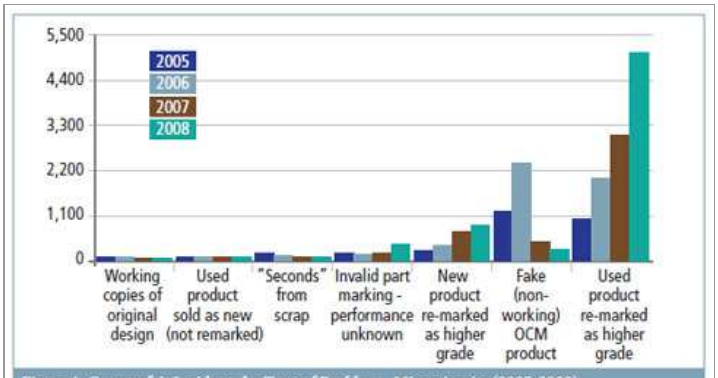

Figure 1. Counterfeit Incidents by Type of Problem – Microcircuits (2005-2008). (Source: U.S. Department of Commerce, Office of Technology Evaluation, Counterfeit Electronics Survey, November 2009.)

From 2005 to 2008, most counterfeit activity was concentrated on parts selling from a few pennies to hundreds of dollars; however, there has been a steady increase in the number of counterfeits in the $500 to $10,000 range. Figure 1 shows the exponential growth of counterfeit incidents involving microcircuits, with “used product re-marked as higher grade” representing the largest growth area.

Threat

Counterfeiting can have a major impact on end product reliability and overall mission assurance. Incorrect or inferior parts fraudulently represented as quality products can not only cause system malfunction, but can also damage other components in the system, resulting in costly diagnostics and repair, injury to employees, and/or mission failure. Relabeled components can mask electrical performance or design changes made by the OCM, resulting in intermittent performance issues or hard-to-find functional errors. Most troubling is the latent damage to components that may occur when using unsophisticated methods for removal, cleaning and re-marking. For example, cleaning chemicals used to remove markings can also penetrate the package and damage the semiconductor structures, inducing faults that may affect device functionality later in life. Improper handling by the counterfeiter can damage a part through electrostatic discharge (ESD), or it can damage fragile leads or interconnect structures. Components are often exposed to excessive temperatures when being removed from a circuit card assembly, significantly reducing reliability and life expectancy.

Counterfeit Detection

The simplest form of counterfeiting is relabeling an item by physically removing the original marking and re-marking by using a method similar to that of the original part manufacturer (such as laser etching or ink stamp printing). In some cases, tampering can be detected during high-magnification visual inspection, revealing faint remnant scratches in the part’s surface or irregular patterns around the edges of the part, which are formed when the original markings are removed by the counterfeiter. By simply coating the surface, original part markings can be masked, then re-marked with new part numbers, date codes or higher functional speed coding (Figure 2).

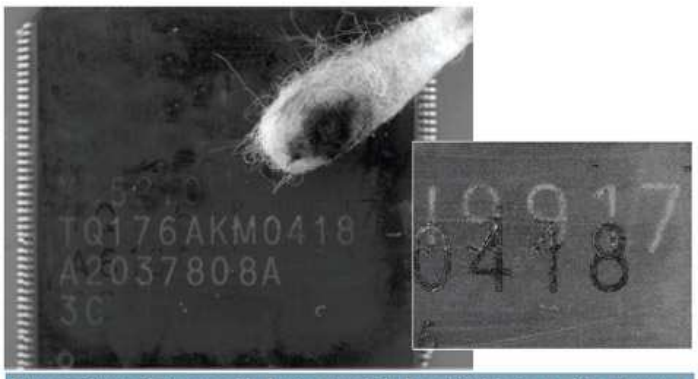

Figure 2. Counterfeiters use a black top coat to hide the original device marking. However, the top coat is removed by using an acetone-soaked cotton swab to reveal the concealed device markings.

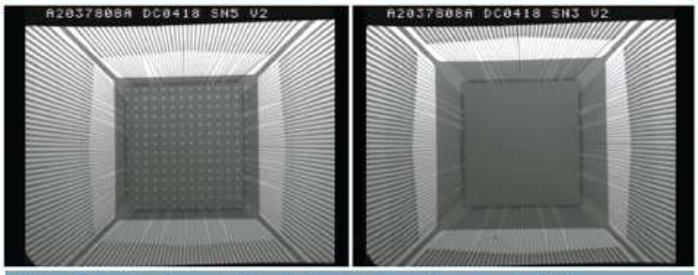

Figure 3. X-ray imaging reveals two different metal lead frames used within the same date code and assembly lot.

In some cases, the marking techniques used by the counterfeiter appear so authentic that more in-depth analysis methods are required to determine part authenticity. X-ray radiographic imaging often reveals differences in the metal lead frame pattern and die size within the assembly lot (Figure 3). This may not constitute absolute evidence of the parts being counterfeit; however, it does raise suspicion as to their authenticity since it is unusual for a manufacturer to introduce significant design changes within a single production lot.

In some situations, the only way to determine if a part is authentic is to disassemble a sample and expose the semiconductor device surface to uncover its die markings. These markings are then compared to the external package marking to identify discrepancies.

There are reports of counterfeiters modifying authentic devices to comply with customer requirements. In Figure 4, a modification was made to the leads of a packaged semiconductor in order to meet the customer’s lead length requirement, and it was misrepresented as new material.[2] Upon further inspection and analysis, it was determined that the leads were not homogeneous. The standard Kovar® lead material ended midway along the lead length and then transitioned to a low carbon steel lead.

Raytheon’s Response

Raytheon is addressing the threat of counterfeit hardware through strict management and control over the acquisition process and by using only original component manufacturers (OCM) and authorized distributors whenever possible. Because parts become obsolete, it is

sometimes necessary to purchase parts from sources other than an OCM and authorized distributors. In this case, a comprehensive series of authenticity tests are employed based on industry standards such as SAE AS5553 (Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition.)[3] A counterfeit part detection plan may include any or all of the following non-destructive or destructive test methods.

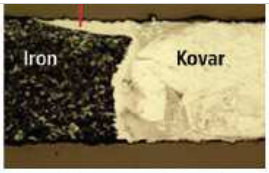

Figure 4. The Kovar lead exiting the package is welded to a low-carbon steel lead. The Kovar portion is tin-lead over nickel plated, and the steel portion of the lead is tin-lead over copper plated.

Non-destructive test methods:

Review documentation for inconsistencies and incorrect data.

Visually inspect for package defects such as sanding marks and top coating.

Record digital imaging documentation of package and external markings for reference purposes and compare to a known reliable device if available.

Chemically cleanse the part's surface to look for evidence of surface top coating.

Measure mechanical dimensions and compare them to the manufacturer's specifications to determine if the part has been physically altered.

Perform an x-ray examination of the lead frame, bond wire and die configuration, and make comparisons to known reliable devices if available.

Perform scan acoustic microscopy to detect delamination from excessive heating during the board removal process.

Perform DC electrical pin-to-pin testing to verify continuity with comparison to a known reliable device and to detect evidence of ESD damage.

Perform x-ray fluorescence (XRF) assessment of external lead plating material and make comparisons to part requirements.

Perform functional electrical testing (ambient and rated temperature) if the authenticity is still in question and no other option is available.

Destructive test methods:

Decapsulate and perform an internal inspection of die markings and workmanship and make comparisons to the part's external surface markings for discrepancies.

Perform scanning electron microscope inspection of bond and die surface as well as material identification and comparison to known reliable device if available.

No single test can detect all forms of counterfeiting; however, applying non-destructive inspection methods such as real-time x-ray and high-magnification optical inspection is a good first step in determining if a part is counterfeit. Discrepancies in markings, documentation and historical data raise suspicion and require additional investigation. Reviewing part history and data from external reporting services, such as the Government and Industry Data Exchange Program (GIDEP), provides additional information on possible counterfeiting history. In some cases, materials and construction analysis are required.

The Need for Continued Vigilance

As detection and avoidance methods improve, counterfeiters adapt and become more sophisticated. Information exchange and training across government, industry, academia and standards organizations are essential to combat this threat.

Raytheon has established the Enterprise Counterfeit Material Avoidance team to develop policy and procedural requirements and maintain constant vigilance to ensure supply chain integrity. This team of experts is involved with industry committees on the subject of counterfeit product detection and prevention and has developed a Counterfeit Product Risk Mitigation and Prevention Policy[4] with requirements to address counterfeit product avoidance and mitigate the risk of purchasing and introducing counterfeit material into Raytheon products.

The team has also developed a product information database as the central repository for information related to the investigation, analysis,

reporting and corrective actions associated with counterfeit product incidents. Engineering plays a key role in combating counterfeit parts by designing out obsolete components, managing parts obsolescence, and ensuring robust product life-cycle plans are developed and executed. Buying only from OCMs or authorized distributors helps to secure the supply chain from the introduction of counterfeit parts.

Counterfeiting is an ongoing issue requiring continued vigilance and knowledge sharing, both internal and external to Raytheon, to address the ever-evolving threat.

[1]*Defense Industrial Base Assessment: Counterfeit Electronics*, U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation, January 2010.
[2]GIDEP Alert C5G-A-11-01, *Suspect Counterfeit Linear Microcircuit*, 08 June 2011.
[3]ASM Aerospace, *Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition*, AS5553.
[4]Raytheon Policy 000000243-RP *Counterfeit Products Risk Mitigation and Prevention*.

Ken Rispoli

CONGRESSIONAL HEARING

2011 was a dynamic year on the counterfeit electronic parts front at Raytheon. In addition to finalizing and releasing a comprehensive enterprise policy regarding counterfeit product risk mitigation and prevention, Raytheon supported a dozen information requests as part of an investigation by the U.S. Senate Armed Services Committee (SASC).

The SASC effort was focused on investigating the risk of counterfeit electronic parts within a select group of companies that support Department of Defense programs. Raytheon's support of the SASC effort culminated in November during a formal hearing in Washington, D.C. Raytheon was asked to participate in the hearing given our company's experience in dealing with counterfeit electronic parts, and for our proactive response to the overall threat. The SASC hearings resulted in legislation regarding counterfeit electronic part prevention as part of the 2012 National Defense Authorization Act, signed into Law by President Obama in late December.

In parallel, Raytheon has enacted counterfeit prevention procedures; updated supply base requirements, terms and conditions; evaluated and down-selected an exclusive group of electronic parts brokers; and participated in several industry forums regarding counterfeit electronic parts. Raytheon will continue to improve its processes and risk mitigation strategy to address the growing threat of counterfeits and to maintain our company's position as one of the leaders in this area.

Top of Page
