Counterfeit Detection Strategies: When to Do It / How to Do It

By:

Greg Caswell
Senior Member of the Technical Staff
DfR Solutions
5110 Roanoke Place, Suite 101
College Park, MD 20740
301-474-0607
gcaswell@dfrsolutions.com

Abstract

Counterfeit components have been defined as a growing concern in recent years as demand increases for reducing costs. In fact the Department of Commerce has identified a 141% increase in the last three years alone. A counterfeit is any item that is not as it is represented with the intention to deceive its buyer or user. The misrepresentation is often driven by the known presence of defects or other inadequacies in regards to performance. Whether it is used for a commercial, medical or military application, a counterfeit component could cause catastrophic failure at a critical moment.

The market for long life electronics, based on commercial off the shelf (COTS) parts, such as those used in medical, military, commercial depot repair, or long term use applications (e.g. street and traffic lights, photovoltaic systems), seems to create a perfect scenario for counterfeiters. With these products, components wear out and need to be replaced long before the overall product fails. The availability of these devices can be derived in many ways. For example, a typical manufacturer may render a component obsolete by changing the design, changing the functionality, or simply discontinuing manufacture. Also, the parts that are available after a design has been discontinued are often distributed by brokers who have very little control over the source or supply. Recycling of devices has also emerged as a means of creating counterfeit devices that are presented as new. And finally, as demand and price increase, the likelihood of counterfeits also increases.

This paper will address the four unique sources of counterfeit components and insight into how they occur. Detection methodologies, such as visual inspection, mechanical robustness, X-Ray, XRF, C-SAM, Infrared Thermography, electrical characterization, decapsulation, and marking evaluations, will be compared and contrasted, as well as multiple examples of counterfeit parts identified by DfR.

Introduction

Counterfeit components have been defined as a growing concern in recent years as demand increases for reducing costs. A counterfeit is any item that is not as it is represented with the intention to deceive its buyer or user. The misrepresentation is often driven by the known presence of defects or other inadequacies in regards to performance. Whether it is used for a commercial, medical or military application, a counterfeit component could cause catastrophic failure at a critical moment.

The market for long life electronics, based on commercial off the shelf (COTS) parts, such as those used in medical, military, commercial depot repair, or long term use applications (e.g. street and traffic lights, photovoltaic systems), seems to create a perfect scenario for counterfeiters. [4, 5] With these products, components wear out and need to be replaced long before the overall product fails. The availability of these devices can be derived in many ways. For example, a typical manufacturer may render a component obsolete by changing the design, changing the functionality, or simply discontinuing manufacture. Also, the parts that are available after a design has been discontinued are often distributed by brokers who have very little control over the source or supply. And finally, as demand and price increase, the likelihood of counterfeits also increases.

There are four common sources of counterfeit parts: inside jobs, competitors, used, and fraudulent sources. An inside job is characterized by parts that failed a production test and should have been disposed of but rather are packaged and labeled as

good parts of the same type. Depending on the reason that the part failed the production test, an inside job counterfeit may operate in benign environments, but may not function in the more demanding environments that would be in the specification sheet. The most straightforward way to identify an inside job type of counterfeit is to perform rigorous testing of the part in all environments and functions listed on the specification sheet.

Another type of counterfeit is that of a part from company B being misrepresented as a part from company A. This may or may not lead to field failures. A common method of identifying these types of counterfeits is to scrutinize the packaging. Many large companies have complex labeling schemes that may be difficult to replicate.

A used counterfeit is a part that is used but represented as new through being desoldered off of failed circuit boards. The parts may find their way back into the supply have an unknown history and unknown life expectancy. Additionally, the process of desoldering may cause additional damage. A careful inspection of the leads and package for damage or wear and tear should identify a used part. This particular counterfeiting problem has been exacerbated by WEEE as more devices are being salvaged and resold as new rather than having to deal with the disposal of the materials.

A fraudulent counterfeit is a part that is packaged to appear original and new. Fraudulent parts will contain either an empty package or wrong chip. These types of counterfeits will fail immediately, as the functional component is completely phony and serves no purpose other than to grossly appear authentic. These parts only need to appear authentic long enough to be purchased, since they will be detected when they fail to function. This is the most likely type of counterfeit found from goods purchased in the spot market, where the vendor may disappear after the sale is complete and payment is delivered.

The impact of this activity can have a profound impact on you, the user. The following chart illustrates the various risk-at-failure scenarios as a function of the sources of components.

Clearly the potential risk increases with each supplier category. Similarly, the potential risk to your business increases with the risk of using sources of supply that are less trustworthy as shown in Figure 1.

In the growing world of lead-free, there is now concern over counterfeit RoHS notification. As more companies are required to transition to lead-free, there is an increased likelihood that bogus test reports will accompany a component. Major manufacturers who post such data are unlikely to take part in fraudulent activity, but small vendors may be cornered into falsifying RoHS compliance data when faced with the possibility of lost sales due to RoHS noncompliance.

Source of Components	Probability of Counterfeit	Risk of Failure
Component Manufacturer	.02%	$10K to $100K
Licensed Distributor	.2%	$100K to $1M
Broker (Known)	2.0%	$1M to $10M
Broker (Unknown)	20.0%	$10M to $100M

Figure 1 – Probability of Failure vs. Source

As the user of these devices it is necessary for you to make the risk/reward assessment to determine how much you should spend on methods to identify and detect counterfeit components. Some companies take a very simplistic black or white approach to this issue. In other words, they either do nothing or overcompensate for the level of defect identification procedures implemented. DfR suggests a more meaningful approach be taken. If we take a simple ROI for a typical product of 5-10 to 1 then you should be spending between $5K and $10K if your cost to fail is $100K. More, if your sources of supply require you to use brokers in an effort to meet delivery schedules. The quantity of different part types procured can also add a dimension to this issue as the higher quantity of line items on Builds-of-Materials (BOMS) may drive the increased use of brokers in a tight economy. Higher component throughput also increases risk and the amount of time and effort to mitigate counterfeit components should be increased accordingly.

What drives these choices? Let's take a typical 200 line item BOM, with a mix of active, passive and mechanical components. It is not uncommon to encounter a few devices that are on distributor allocation of have exceedingly long lead times. OEM's or Contract Manufacturer's (CMs) will then

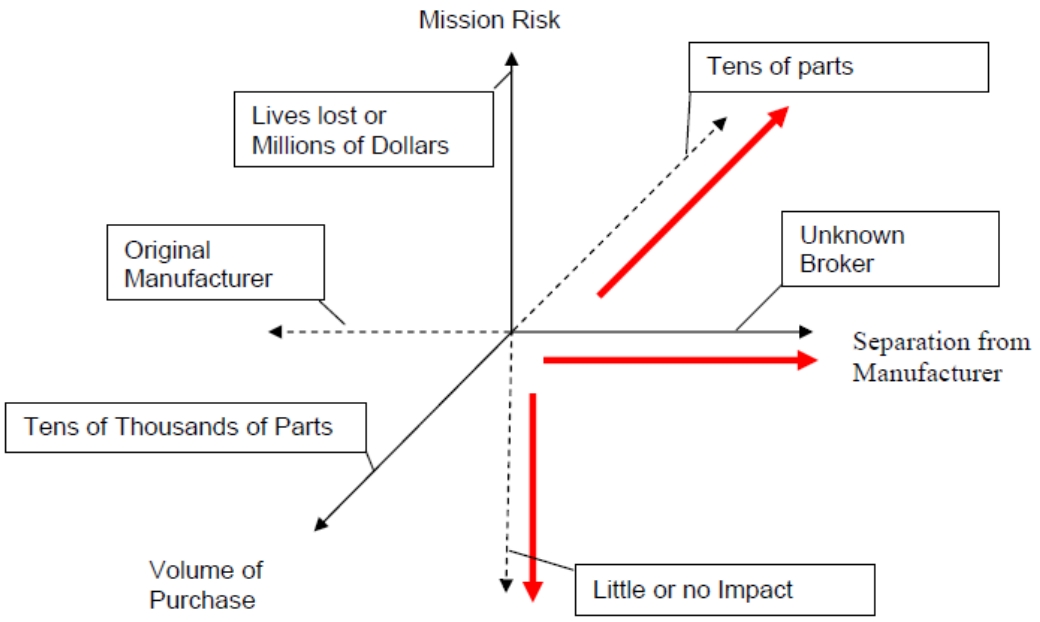

Figure 2 – Risk versus Cost Tradeoff

explore the use of brokers in these circumstances to alleviate the lead times and facilitate on time deliveries, rather than having the other 197 line items sit on the shelf for that long timeframe, costing money.

So what are the risks? Counterfeiters have also improved their production methods so that detection can be virtually impossible to the naked eye. With this highly developed ability to imitate electronic components, it is no surprise that counterfeiting is such a widespread phenomenon. Many attribute the recent and steady increase of counterfeits to increased access to components via the internet. With e-commerce booming as a convenient and less expensive purchasing alternative, the internet has become a hotbed for counterfeit activity.

Based upon your risk aversion approach, you can identify and help facilitate methods of counterfeit device detection. This activity can range from Visual/X-ray audits of suspected counterfeits to full scale characterization testing of every part over the full temperature range.

Having skills in design management can also aid in counterfeit prevention. Manufacturers should monitor and manage product and component lifetime, limiting the need to replace components before the end of the overall product's lifetime. When design components become scarce or unavailable, the design should be updated to assure these obsolete parts are not used. Also, anti-counterfeit measures can be designed into the part to make forgery more difficult.

Most counterfeits are finally detected when they fail during use. However, visual inspection could raise the suspicion of forgery long before the component fails. Differences in manufacturing specifications such as molding die locations, ink precision or durability, font, or date or lot code standards can indicate possible counterfeit parts. Although knowledge of exterior labeling and marking standards is helpful in detecting a counterfeit, the body of knowledge required to become an expert on all standards is extensive. Some counterfeiters have such advanced techniques that the counterfeit marking may be of higher quality (more durable, vibrant, or sharp) than the original. Overall, visual inspection is an important tool in counterfeit detection, but by no means is it the only or best way to identify forgery.

There are more conclusive methods than visual testing to determine the authenticity of components, many of them diagnose non-destructively. Infrared imaging or SQUID microscopy can be used to identify and monitor the active parts of an IC with questionable components on it. If a known authentic IC is compared to a suspicious one, these imaging techniques will show any current location or size differences. X-ray inspection is the next step and will show any size or configuration abnormalities in die, wire bonds, or bond pads.

How To Do It

Visual Inspection

Overall, visual inspection is an important tool in counterfeit detection, but by no means is it the only or best way to identify forgery. So what should you be looking for? [1, 2]

Visually inspect the exterior of the components using a low power microscope (3-10X) and examine the quality of the markings. Original components tend to be clean with the markings legible and identical. Conversely, counterfeit parts may or may not be as legible due to a lack in equipment to properly remark the device. During this visual inspection you should also examine the leads on the devices. Reclaimed parts often have less co-planar leads as a function of being desoldered as the leads are very difficult to keep straight. Non-co-planarity is a good indicator that the parts have been removed from a board and reclaimed. Also, visually inspect the contact points of the leads as they should show no signs of excess solder where it would have been connected to the circuit board. Figure 3 shows two Samsung parts; the left is a known good part while the right is not. The only visible difference is the registration of the marking which is a millimeter lower.

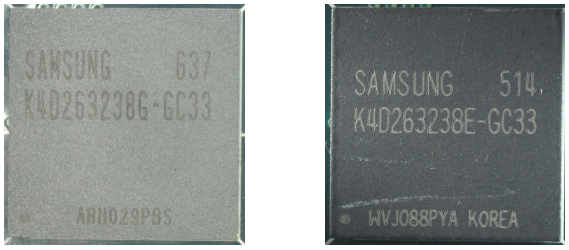

Figure 3 – Marking Registration Differences

Blacktopping of packages is another counterfeiting process. In this, original marking is covered with new marking, more recently with original materials being reground. Doing so has made detection more difficult and expensive to detect. Figure 4 shows a couple of examples of blacktopping.

Ball Grid Array reballing is a routine operation to salvage BGAs after once being soldered to a circuit board. If done well it is extremely difficult to determine if a device has been reballed. However, using visual inspection one can look at features such as excess solder around the ball attachment area, evidence of pad wicking, signs of flux residue, or visible damage to the component package itself

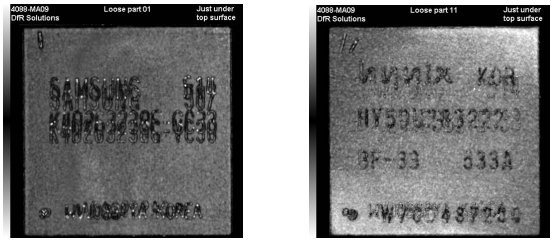

Figure 4 – Examples of "Blacktopped" Devices – (left is changed date code) (right is date code mismatch)

. These visible signs are indicators that a part may have been reballed and then sold as new. Conversely, BGAs that have "lead free" balls have also been counterfeited as parts having Sn/Pb balls. Not catching this problem can result in "head in pillow" solder attachment as shown in Figure 5. X-Ray Fluorescence (XRF) is a method for determining solder ball composition quickly.

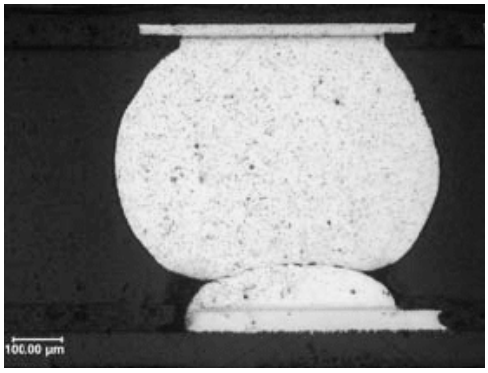

Figure 5 – Lead Free Ball on Sn/Pb Pad

X-Ray

"False" counterfeits are parts that are suspected to be false, but are in fact authentic components. This situation could result from miscommunication in manufacturers' product change notices (PCNs) and are a time-consuming and costly way to discover a design or specification change in a component.

Figure 6, below shows the result of a miscommunication in a PCN that resulted in the suspicion of counterfeit. The 3 amp diodes with new date codes experienced a dramatic increase in failure rates compared to those in use with older date codes. During X-ray microscopy, the new diodes were found to have smaller die which most likely caused increased current density and therefore increased failures.

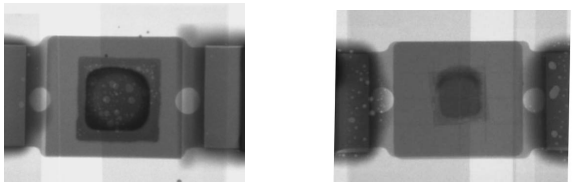

Figure 6 – X-Ray showing Diode Differences

If you use X-rays as the method for identifying counterfeit components you should be able to identify: die presence/absence and dimensions, die attach material, leads and bond wire layout, and bent or deformed leads. At a higher magnification you should be able to see cracks in the die or the package, the bonding sites (either wedge or ball), thicknesses and the bond wire placement and thickness.

Electrical Characterization

Sometimes electrically characterizing a suspected component will facilitate identification as a counterfeit. Figure 7 shows a comparison between a known good capacitor structure and a suspected counterfeit. The upper images show good capacitor characteristics with regard to capacitance and also dissipation factor. The lower images illustrate the problem device out of tolerance. Utilization of other methods identified in this paper could then be used for further confirmation. Similarly Figure 8 shows two different diodes, initially confirmed as a counterfeit due to significantly reduced breakdown voltages. The subsequent X-ray images show two completely different packaging implementations and die structures, resulting in the different voltage levels.

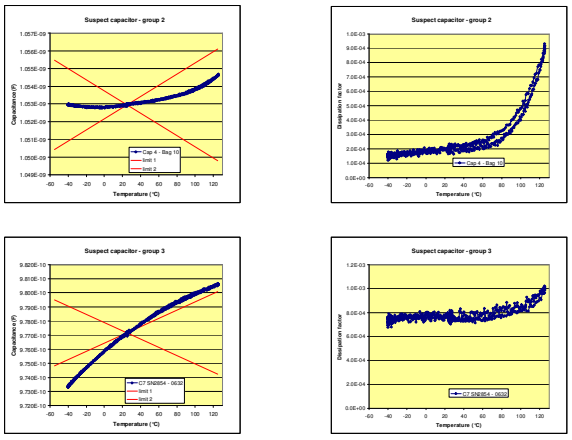

Figure 7 – Electrical comparison of Good vs. Counterfeit Capacitors

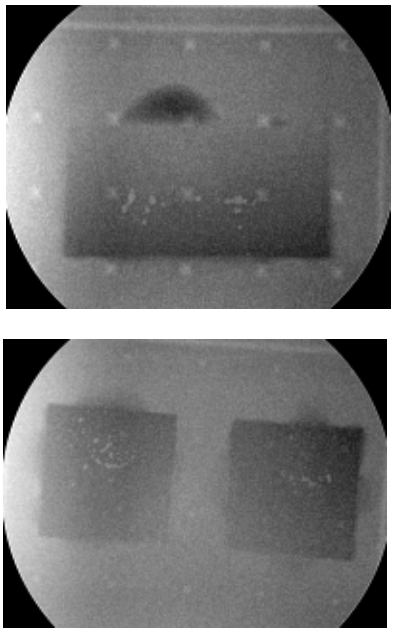

Figure 8 – Good Diode (top image) 280V breakdown voltage; Counterfeit Diode (bottom image) 50V breakdown voltage

X-Ray Fluorescence (XRF)

X-ray fluorescence spectroscopy (XRF) can be used to detect poor quality or counterfeit parts by measuring the elemental composition of materials present in the parts and comparing them with an authentic part. XRF can be a useful tool to detect counterfeit passives. XRF is of particular use when comparing the lead finish on parts as it will detect whether a part is RoHS and lead free compliant, or whether the part is being identified as lead free when the leads indicate that the part had been used in a tin/lead application.

Scanning Acoustic Microscopy

Scanning acoustic microscopy (SAM) can be used to detect anomalies such as popcorn cracking in molding compounds, and interfacial delamination such as delamination between die and leadframe, that are often caused due to reclamation of parts from discarded electronics. It has been most effective in uncovering distinct differences in device surface coatings which resulted in the identification of many counterfeit devices.

In addition, there are other more expensive methods to determine the authenticity of components, many of which diagnose non-destructively. Infrared imaging or SQUID microscopy can be used to identify and monitor the active parts of an IC with questionable components on it. If a known authentic IC is compared to a suspicious one, these imaging

techniques will show any current location or size differences.

Infrared Thermography
Infrared Thermography uses an infrared imaging and measurement camera to visualize thermal energy emitted from an object. Infrared energy, is light that is not visible because its wavelength is too long to be detected by the human eye. In the infrared world, everything with a temperature above absolute zero emits heat and the higher the object's temperature, the greater the IR radiation emitted. Infrared thermography cameras produce images of invisible infrared or "heat" radiation and provide precise non-contact temperature measurement capabilities making infrared cameras extremely cost-effective, valuable diagnostic tools in many diverse applications.

This technique can be used to identify counterfeit components through a comparison of a known good device (possibly installed in a circuit board) to one that is considered a counterfeit. The devices will produce uniquely different thermal images**.** (See Figure 9)

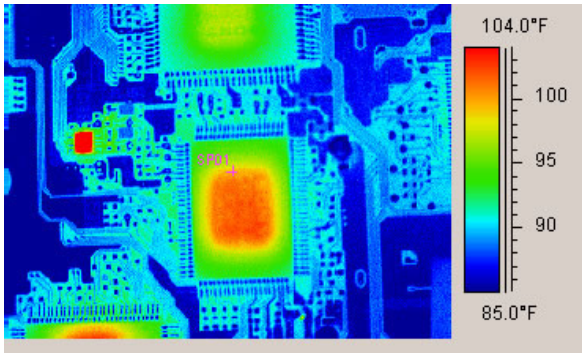

Figure 9 – Infrared Thermography

SQUID Microscopy
Magnetic current imaging using a superconducting quantum interference device (SQUID) is a technique that uses detection of magnetic fields to image current paths within electronic devices or circuit boards. This technique has been successful in non-destructively identifying the location of low leakage currents, even when the failure site was between a power and ground plane. The use of low voltage and low current is vastly superior to thermal imaging, which often results in irreplaceable damage to the failure site and masking of the true root cause of failure. (3)

Decapsulation
Decapsulation is another tool for ascertaining counterfeits, and will allow internal visual inspection but at the cost of destroying the part. Cross sectioning /FIB are additional destructive tools which are invaluable to counterfeit detection.

When To Do It

The costs involved in each of the counterfeit detection techniques vary essentially as a function of their ability to confirm a counterfeit component. Depending on you application, you can decide which approach(es) provide you with the best value. Let's compare each approach as a function of identifying a specific generalized component issue.

Visual Inspection
- $1K to $3K
- Identify color differences in parts
- Ascertain marking imperfections/changes/blacktopping
- Lead finish and variability
- Co-planarity of leads – reused parts

X-Ray
- $1K to $3K
- Verification of die and wire bonding pattern
- Internal construction of component
- Die bonding delamination issues
- Die attach voiding

Electrical Characterization
- $3K to $6K – passives, simple actives
- One temperature for evaluation
- $15K to $80K – characterization of complex IC, fixturing, test equipment
- Potential for circuit board design, layout and fabrication costs to enable testing

- COMMENT: you can't afford the risk associated with buying expensive ICs from unknown suppliers

Mechanical Robustness

- $2K to $5K
- Thermal cycling or other testing to verify component is not counterfeit

Destructive Physical Analysis (DPA)
- $7 to $10K passives
- $8 to $12K actives
- Step by Step analytical approach to identifying whether a device is counterfeit using all tools available.

Conclusion

DfR has demonstrated in this paper that counterfeit components reaching your system are a very real possibility. We have illustrated several approaches for obviating these issues and have presented the cost tradeoffs for you to use in assessing your own operation. The risk needs to be managed through an assessment process where the probability of a counterfeit occurring in the application, the volumes of parts involved and the mission risk are examined. Doing so will facilitate clear boundaries and guidelines for mitigation. Clearly the costs involved are not prohibitive and should be addressed as a function of the risk.

References:

(1) Lowry, Robert K., "Counterfeit Electronic Components-an Overview," presented at the Military, Aerospace, Spaceborne and Homeland Security Workshop (MASH), 2007

(2) Federico, Joseph G, "Stopping Counterfeit Parts Before they do Damage," US Tech, October 2009

(3) Hillman, Craig, "A Novel Approach to Identifying and Validating Electrical Leakage in Printed Circuit Boards through Magnetic Current Imaging," ISTFA 2004: Conference Proceedings from the 30th International Symposium for Testing and Failure Analysis, Oct 2004, Pages: 82-87

(4) King, Rachael, "Fighting a Flood of Counterfeit Tech Products," Business Week on-line, March 1, 2010

(5) Spiegel, Rob, "Distributors Fight Counterfeit Components," EDN on-line, April 6, 2010