DfR Solutions
reliability designed, reliability delivered

White Paper

Counterfeit Parts
The Cost to Your Business - and How DfR Solutions Can Help

By Greg Caswell and Dr. Craig Hillman

5110 Roanoke Place, Suite 101 College Park, Maryland 20740
Phone (301) 474-0607 Fax (240) 757-0053
www.DfRSolutions.com

Counterfeit Parts
The Cost to Your Business - and How DfR Solutions Can Help

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. 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.

5110 Roanoke Place, Suite 101 College Park, Maryland 20740
Phone (301) 474-0607 Fax (240) 757-0053
www.DfRSolutions.com

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

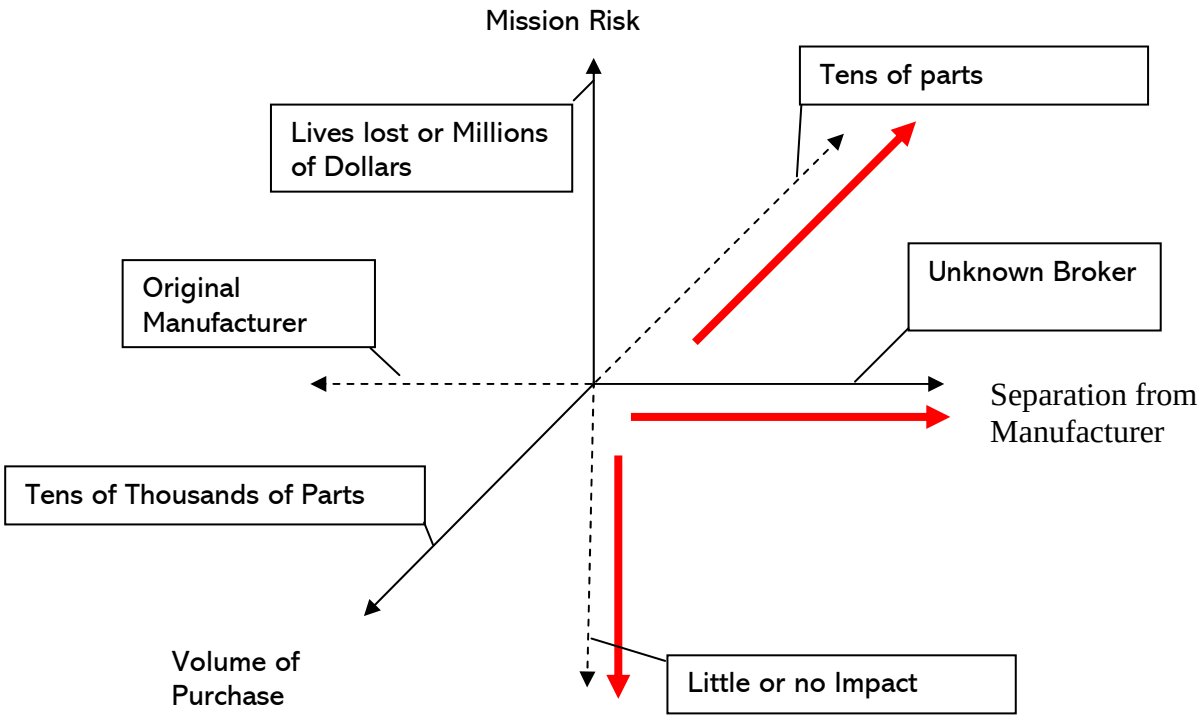

Figure 1- Counterfeit Risk (red arrows denote increasing risk)

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 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.

How can DfR Solutions help? Based upon your risk aversion approach, DfR 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. Our knowledge base can help identify and mitigate issues before suspect components get installed into a product and fail test, thus reducing your costs significantly.

DfR's skills in design management can also aid in counterfeit prevention. Manufacturers should monitor and manage product and component lifetime so as to limit 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 so as to not require these obsolete parts. 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. Hiding abnormalities within a circuit board or component is a popular method of counterfeit since extra effort must be taken in order to identify them.

The bottom line is-let DfR help you reduce your exposure to counterfeit parts through the use of our knowledge base and skills in counterfeit device identification. It will save you money and make you more competitive.

For more information contact Greg Caswell at gcaswell@dfrsolutions.com or at 301-474-0607.