Feature

Printer-friendly version

Dodging Counterfeit Electronic Components Is Far More Difficult Than in the Past

April 13, 2011

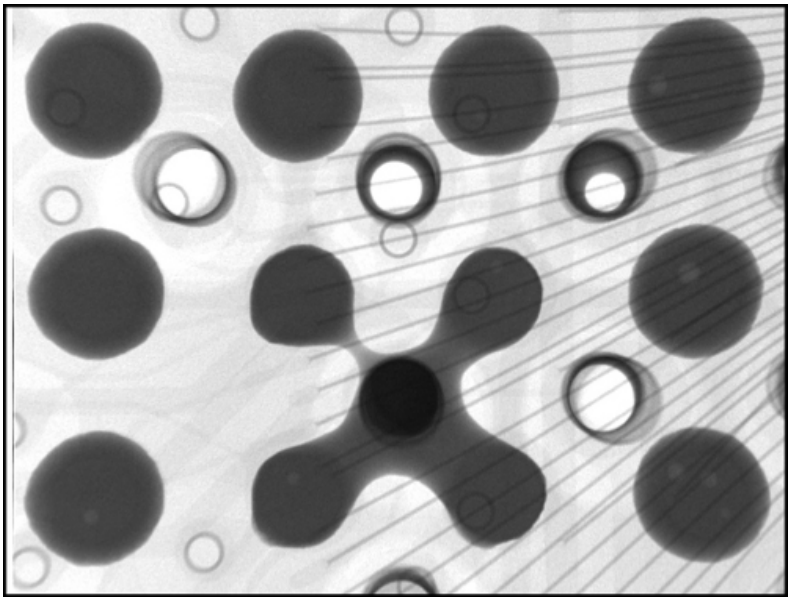
By: Tom Adams, SMT Corp.

Find more content on: Business/Market Trends,Components,Design,Feature,Integrated Circuits,Semiconductor Technology

Find Qualified Medical Device Industry Suppliers at Qmed: Design engineering,Semiconductors

The counterfeiters are becoming increasingly harder to detect. Unfortunately, the devices they're selling aren't getting any better.

A counterfeit electronic component operating in a medical electronics system may make itself known when the system experiences an unexpected failure. The failure may be relatively innocuous—a monitoring device that suddenly begins to display meaningless numbers—or it may be directly life-threatening, such as a functional failure in a defibrillator. Even after the failure has occurred, the failed component may not be recognized as counterfeit unless it's inspected for that purpose.



1. Shown is a real-time X-ray image of part of a plastic BGA.

Because of the nature and complexity of the global electronics component supply system, it's fairly easy for counterfeit components to be unknowingly purchased by practically any system assembler. The ways in which counterfeits are produced, and the rapidly increasing skill of the counterfeiters in disguising their bogus components make the problem even more severe.

Many counterfeit components find their way into the inventories of independent distributors who fill the critical role of supplying manufacturers with new components that are either obsolete, allocated, or on long lead-times from the factory. To protect their customers from the increasing counterfeit threat, some distributors have begun thorough incoming inspection processes to detect

Most Rece
Most Emailed
Technological Ac
Healthcare and P
The Platform Alte
and Highly Integ
May/June 2011 C
Agile Software D
Regulated Applic
Dodging Counter
Far More Difficul
Battery packs an
always make a g
Not complying w
design could be
Bluetooth in 467
2016

counterfeits and remove them from the supply chain. As the quantity of counterfeits has grown, and as counterfeiters have become more sophisticated, this effort has grown into a sizable laboratory in some cases.

Inspection often involves not only components that the distributer is considering for purchase, but also components that OEMs have acquired from other sources, and even counterfeit components that have been declared genuine by private test labs.

In the global supply network the vast majority of counterfeit electronic components are plastic-encapsulated microcircuits (PEMs) that began life on a previously used circuit board that was ultimately scrapped, and probably within a western country. When the electronic equipment is discarded, their boards are harvested and shipped in vast quantities to China. Trucks haul the export containers from the docks of Hong Kong harbor to the town of Shantou where most of the component harvesting and counterfeit processing is performed within mainland China.

In one case in particular, workers were heating printed circuit boards, one at a time, over small fires until the solder reflowed. The board was then struck against a hard surface to make the components fall off and the components were then gathered off the ground. The individual components were then packed in bags, washed in streams and rivers, dried on sidewalks, sorted, and returned to the counterfeiter's workshop where the original part markings were sanded off. The surface of each component was then painted to resemble the original component color and cover sanding marks. After drying, the parts were then remarked using an ink or laser-etch process.

All of this rough treatment would be damaging even to brand new components—never mind components that have already seen a lifetime of service. Some of the components are already defunct, since they came from failed systems. The rough "sorting" of the components is especially significant. This work is done by women and children, who pay attention only to the dimensions of the components and the number of leads. All of the ones that look the same go into the same pile. Aside from the fact that some of the components are unquestionably dead electronically at this point, a single pile may contain components having different revision codes, or even different functions. But every component in a pile will get the same new matching part-marking.

The purpose of all of this work is to make each component as cosmetically similar as possible to the new component that it's impersonating. The point at which these counterfeits have value is at the moment when they are sold to a buyer as factory-new components. At that time, the counterfeiter's work is, so to speak, finished. If he is selling, for example, what purports to be a reel of PQFPs made by National Semiconductor, he will also counterfeit, or have someone else counterfeit, the reel and its labels. What the buyer examines will appear to be a new reel that holds new National Semiconductor PQFPs. If the counterfeiter is worried that his cosmetic work may not be quite up to standards, he may go out and purchase a few genuine National Semiconductor PQFPs and put them at the beginning, middle and ends of the reel. The sharp-eyed buyer who examines the first or last 30 or 40 components on the reel will be satisfied. The remaining 99% of the reel, however, holds counterfeits.

Not all counterfeit components are PEMs. There are counterfeit BGAs (as shown in Fig. 2) and flip chips (both technically PEMS), counterfeit ceramic-packaged microcircuits, and counterfeit passive components, such as resistors and capacitors. There are also counterfeit components that are created completely by the counterfeiter. These might be new-looking PEMs that have a lead frame and new, unused external leads—but no die!

Counterfeit components may begin their journey when they are sold over the counter in the town where they were created. From there they may be sold multiple times until they wind up in the inventory of an independent distributor. Not all independent distributors are concerned about the authenticity of the parts they sell, or are they willing to perform the multitude of tests required to verify authenticity. Counterfeits can thus easily wind up in all products, including medical products.

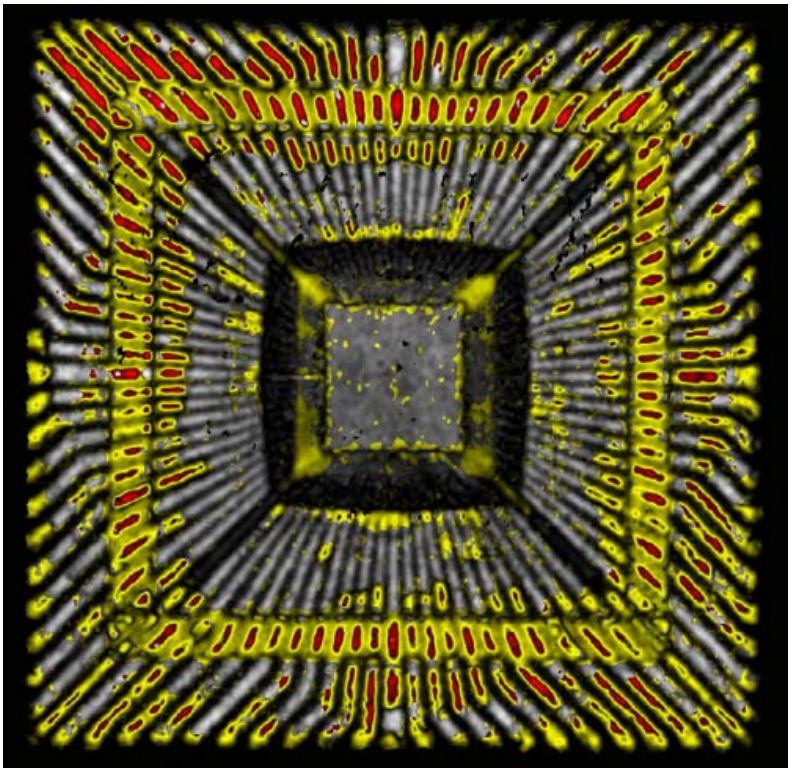
What makes counterfeits so dangerous in medical products is the impossibility of predicting their behavior. A refurbished counterfeit, even though it's mounted on a new board, is already elderly. An assembler of medical electronic systems who is unwittingly mounting counterfeit components is risking an unpredictable percentage of field failures in a relatively short time frame. Some counterfeits unquestionably live through a second installation and may still function properly for some time. But there are many that do not.

The counterfeits that have already experienced a normal service life, have endured the rigors of refurbishing, and that appear to operate normally are the most dangerous. Exposure to humidity, thermal cycling, and contaminants gradually degrade any PEM. Moisture and contaminants form tiny electrolytic cells on internal surfaces. Moisture ingression, thermal cycling, and corrosion can easily remove the insulating mold compound between two adjacent internal lead fingers and cause a short. It might attack and break a wire where it's bonded to a pad on the die. Or corrosion might create a large delamination that blocks heat dissipation and causes the die to overheat and fail. The damage might even cause the component to fail intermittently, a condition that might be diagnosed as a software problem.

The risk of unanticipated electrical failure is greatly increased by the remarking process applied to counterfeits. A given component may have been temperature-screened for use in commercial applications, but the counterfeiter may apply a new marking showing that the component was screened for industrial or even military applications. Or he may simply apply a new marking that indicates the component was made in 2009 instead of 1997. Or he may re-mark the component to indicate that it operates at a higher speed than it actually does. Critical system failures are often caused by those counterfeits that function electrically but that have subtle differences that the assembler probably will not think to test for because they are assumed to be brand new parts.

The device shown in Fig. 3 is a good example of such a part. It's an acoustic image, made by an acoustic micro imaging system that pulses high-frequency ultrasound into the part and receives the return echoes from internal interfaces. At the center of the image is the die, from which lead fingers radiate outward. What is actually being imaged here is the interface between the mold compound in the package and the die/lead frame. Gray regions mean that the mold compound is well bonded to the material

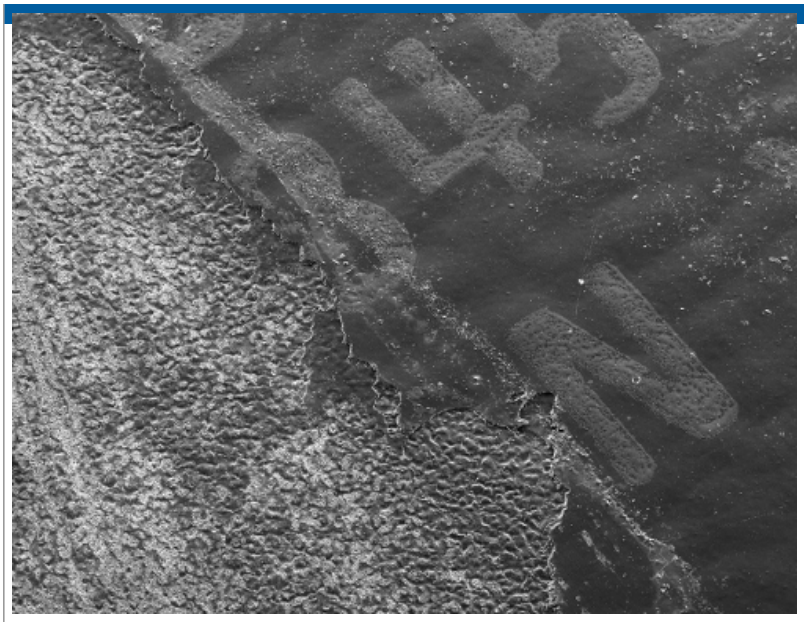
beneath it. Red and yellow regions mean there is a disbond or delamination between the two materials. The numerous red and yellow defects are what one would expect to see in a refurbished part. Some of the defects seen here are likely harmless, but others, such as those around the periphery of the die, could easily cause electrical failure.



2. Acoustic image of a component in which numerous defects (red and yellow) could cause electrical failure.

Recently, counterfeiters greatly improved the cosmetic appearance of their products by developing a blacktop material that very closely resembles the factory finish of a genuine component. The part is first sanded to remove the original surface (the scratch marks from this process are very diagnostic of counterfeits), and the new blacktop paint is sprayed on, allowed to dry, and a new part marking is applied to the surface. Routine optical inspection by the buyer wouldn't reveal that a lot of incoming parts was counterfeit. The sides of the component, however, may reveal that the part is counterfeit because the paint over-spray often extends part of the way down the sides. But even this indicator may be missing from carefully prepared counterfeits.

To overcome this problem, SMT's lab began experimenting with a new solvent that under proper test conditions would remove the new counterfeit epoxy coatings while having no effect on the surface of a genuine component. The suspect component is partly immersed in the solvent and heated to a specific temperature for a specific time. If the component is counterfeit, the layer of blacktop will be removed completely. Fig. 4 shows the results. The solvent has removed the blacktop from the left side of the component in the figure, where sanding scratches are visible on the surface of the mold compound. At the right, the blacktop and portions of the bogus marking can be seen.



3. A scanning electron micrograph (SEM), in which highly engineered blacktop has been removed (on the left), reveals sanding marks in the mold compound.

Because counterfeiters are becoming more sophisticated in their camouflage techniques, multiple technologies are needed today to identify counterfeits. The full range of capabilities includes electrical testing, light microscopy, acoustic microscopy, solderability testing, solvent testing, decapsulation for die verification, various types of x-ray, and others such as data sheet comparison and BGA co-planarity measurement.

All of these methods have specific procedures that are invaluable in specific situations. For example, on a counterfeit PEM where the heated solvent had already removed the false topcoat and counterfeit markings, acoustic micro imaging was used to penetrate slightly into the surface of the mold compound where it revealed the original etched part marking. Much of the etched depth had been sanded away, and the etched marking was not visible optically, but the acoustic image made it legible.

In the past, buyers could often identify and reject counterfeit components when they spotted misspelled company names or misshapen lettering. Such crude counterfeits may still turn up today. But the huge volume of more carefully disguised counterfeits flowing through supply chains today require much more than casual visual inspection for the buyer to identify them as fakes.

***Tom Sharpe** is the vice-president of SMT Corp., located in Sandy Hook, Ct., a company he co-founded in 1995. He's also the current vice-president of IDEA (Independent Distributors of Electronics Association), where he has served continuously on the Board of Directors since 2003.*

Author:
Tom Adams, SMT Corp.