Extension MEDIA

Scan this QR code to subscribe

Engineers' Guide to Military & Aerospace

New Mil/Aero Requirements are Changing the Game

40G-100G Network-Centric Operations

Cost Advantages in the Command Center

Annual Industry Guide
Technology used in military and aerospace electronic design

EECatalog www.eecatalog.com/military

Featured Products

Rugged and Secure Storage Products from Elma Electronic

VPX Backplanes from SIE Computing Solutions

From VersaLogic Corp: Intel® Core™ 2 Duo processor on standard EBX footprint

Sponsors

ADLINK TECHNOLOGY INC.
Connect Tech
ELMA Your Solution Partner
EMERSON Network Power
GE
PDSi Pinnacle Data Systems, Inc.
SIE COMPUTING SOLUTIONS
THEMIS
VERSALOGIC CORPORATION

Counterfeit Components and Detection Technology

By Tom Adams, consultant, SMT Corporation

The most frequently encountered counterfeit electronic components are plastic-encapsulated microcircuits, or PEMs. There are also counterfeit ceramic packages and counterfeit passive components such as resistors and capacitors, but in measuring the overall threat to military and aerospace applications from counterfeits, PEMs are at the top of the list with regard to sheer volume.

Most counterfeit PEMs are components that have already seen a lifetime of service. They are pulled from scrapped circuit boards that are shipped by the container to China, where they are crudely refurbished with no attempt to avoid internal damage. They are then re-marked with a false label before being re-introduced into the global supply chain as factory-new product.

PEMs typically fail because an internal defect has broken or shorted an interconnection;only rarely does the die itself fail. The counterfeiter who is refurbishing a PEM cares nothing about the die or the internal interconnects (some of the rarer made-from-scratch counterfeits do not even contain a die). He cares only about the buyer's acceptance of the external appearance, which must appear new and unused. He is not concerned that a component may already be electrically dead, or that it may fail after brief service.

The risk from counterfeits has grown dramatically in recent years because almost every component type entering the scrapping process is being harvested and returned to the global supply chain. The problem is further exacerbated by the fact that the counterfeiter is constantly improving the processing technologies that create these dangerous fakes.

Counterfeiters can now turn out a bogus PEM so close in appearance to a genuine one that new technology had to be developed to unmask the phonies. But new and more sophisticated tricks to fool the seasoned component inspector are already beginning to appear.

"What is taking place is an accelerating race between counterfeiting technology and detection technology," says Tom Sharpe, vice president of the Connecticut-based independent stocking distributor SMT Corporation, which has pioneered many of the latest detection technologies. "The greatest risk in military and aerospace systems is the counterfeit component that looks new and passes functionality testing – but later fails prematurely without warning."

As of mid-2011, the list of detection technologies include but are not limited to the following:

- Optical microscopes
- Real-time X-ray
- X-ray fluorescence testing
- Decapsulation for die verification
- Solderability testing
- Basic electrical testing
- Acoustic micro-imaging
- Plating thickness testing
- Scanning electron microscopy
- Energy dispersive spectroscopy
- Enhanced chemical resistance testing
- Specific variations of electrical testing

Properly administered based on component type, a rigid application of various combinations of these inspection processes makes it very difficult for questionable components to sneak past a well-trained, alert inspector.

It becomes easier to understand how pristine-looking PEMs can be short-lived or DOA when one examines the refurbishing process they go through in China.

In open-air work areas laborers hold scrap PCBs over fires and other heat sources to reflow the solder and harvest all components. The liberated components are bagged, washed (often in nearby streams), dried on sidewalks and sorted by component package type into individual piles.

These piles are then fine-sorted to separate individual component part numbers. When sorting is finished, one pile may hold hundreds – if not thousands – of the same part manufactured over a span of 10 years or more. Since these components were originally mounted on circuit boards in many different appliances produced over a period of many years, they are generally not electrically identical due to the constantly evolving nature of die and software revisions. If the pile of components contains hundreds of component #XYZ, for example, there may be six different die revisions represented in a single pile of harvested parts. Additionally, the intermixed parts may be rated to operate at different speeds and / or at different temperature levels.

What is certain is that many of these #XYZ components will contain damage inside their plastic packages. Most of the damage will consist of delaminations and voids that promote corrosion of bond pads, wire interconnects and the like. These components have already experienced a previous lifetime in a service environment of unknown humidity, temperature extremes and thermal cycles. They have now begun a new life after being burned off scrap PCBs, washed in a river and dried on a sidewalk.

The #XYZ component pile then goes back into the counterfeiter's workshops, where the top markings are removed with sandpaper, a new "black-topped" surface is applied to cover sanding marks and new part markings are applied. The new markings will be inked-on or laser etched to reflect one single homogenous newer lot/date code. The components are then re-packaged to appear new and factory original in authentic-looking manufacturer packaging. What is especially dangerous in military and aerospace use is that most of these PEMs will work for an unknown period of time because they started out as the same or similar part number that has been re-printed on them.

Since 1994, the U.S. military has been required to use commercial off-the-shelf (COTS) components so a maker of military electronics systems may wind up buying components that have been upgraded merely by being falsely relabeled.

How can one of these components wind up in a system onboard a helicopter? Basically, by being sold multiple times after it leaves China. For example, a buyer may need a specific component to meet the design requirements of a navigational or communication system. He may find part #XYZ for sale at an acceptable price, and if the parts pass his vendor's anti-counterfeit inspection, they will go into production. Since 1994, the U.S. military has been required to use commercial off-the-shelf (COTS) components so a maker of military electronics systems may wind up buying components that have been upgraded merely by being falsely relabeled. If, as is often the case, anti-counterfeit inspection consists only of close visual inspection and basic electrical testing, the counterfeit part may wind up in the helicopter.

Figure 1. Thorough optical inspection is an initial step in SMT's evaluation of components. [Photo courtesy SMT Corporation]

A first step in counterfeit detection is optical inspection [Figure 1] to look for any of the large number of telltale signs have been catalogued over the years. One recent threat is the development by counterfeiters of a highly engineered blacktop that is sprayed

onto the sanded-down component's top surface and cannot be removed with traditional resistance-to-solvents testing; It is visually identical to the finish coat placed on PEMs by manufacturers. If the label is credible, the component is likely to pass even fairly rigorous inspection. But it is easily detected by a refined heated solvent process that will remove the highly engineered blacktop while having no affect at all on genuine components.

Careful visual inspection can also find evidence such as that shown in Figure 2. Here the counterfeiter re-marked the top surface of the component to indicate a manufacturing year of 2006. He left untouched the bottom surface, which still bears the original date of 1997.

Figure 2. Clumsy re-marking of a counterfeit: the top surface has a manufacturing date of 2006, while the bottom has 1997. [Photo courtesy SMT Corporation]

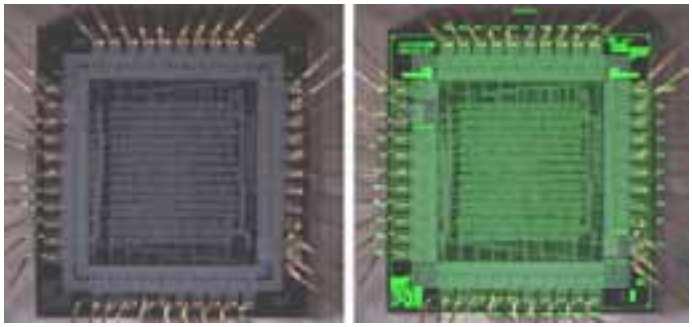

Figure 3. De-encapsulating this part allowed comparison with the manufacturer's materialization mask, overlaid at right. [Photo courtesy SMT Corporation]

Figure 3 (left) is the light microscopy image of a PEM after it has been de-encapsulated, or decapped, by the use of boiling nitric acid, which removes the plastic package but leaves the die and the wire bonding intact. The purpose of decapping is to compare the die markings with the exterior part markings and the manufacturer's materialization mask – (the green overlay in this photo). Here the mask (right) matches the die perfectly, meaning that the PEM contains an authentic die.

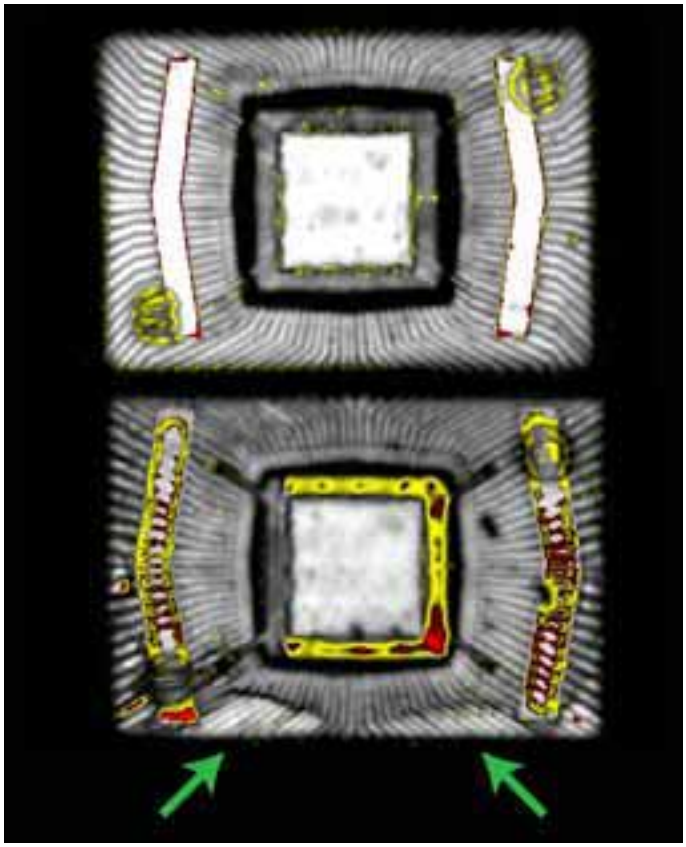

Figure 4. Acoustic micro-imaging shows internal differences between a genuine part (top) and a similar counterfeit part (bottom) having defects (red and yellow). [Acoustic image courtesy SMT Corporation]

The acoustic microscope image of two PEMs of the same type is shown in Figure 4. The part at top is new, while the one at bottom is suspect. Acoustic microscopes pulse ultrasound into the sample and receive echoes of varying intensity from material interfaces. In these images, the highest intensity echoes are red and yellow, and indicate internal gaps. The new part at top has minor red and yellow areas along the tape and around the die; these are normal features, and not defects.

But the suspect component has more significant gaps along the tape and, more importantly, on the die paddle around the die. These are often the signs of a component that has already seen years of service. While these defects do not prove that the part is a counterfeit, they make it much less attractive for inclusion in a critical military or aerospace system. In addition, there are two hard-to-explain light gray areas (arrows) along the bottom edge. These unusual anomalies could easily be damage related to their rough handling while being refurbished.

Type of Counterfeit	Risk to User
Made from scratch, has no die.	No risk. Will fail electrical tests.
DOA before refurbishing.	No risk. Will fail electrical tests.
Refurbished, wrongly labeled.	High risk of field failure.
Refurbished, correctly labeled.	Highest risk of field failure.

Figure 5. Risk impact of four classes of counterfeit components. [Table courtesy SMT Corporation]

The various levels of risk from counterfeit components are summarized in Figure 5. The first two categories include components that are electrically dead. They may pass incoming inspection with their surface appearance, but they will be detected and rejected during the first electrical test they encounter.

A counterfeit that is labeled with the wrong die revision or runs at a different speed may result in unexpected performance issues even if it does not fail quickly.

A correctly labeled counterfeit is likely to have internal defects such as those shown in Figure 4. Such a component is entering its second lifetime of use where, for example, a die-paddle delamination may grow underneath the die and curtail heat dissipation to the point that the die fails.

The biggest problem facing the electronics industry is further refinement of the counterfeiting craft. Very recently, counterfeits have begun to appear in the supply chain that have not been previously used. The leads are perfect and there is none of the traditional blacktop resurfacing being utilized. These parts are being stripped of their original markings using a variety of newer processes that do not leave obvious signs. Fortunately, new techniques have already been developed to unmask even these counterfeit components.

Tom Adams is a freelance writer and photographer based in New Jersey, U.S.A. He has written more than 500 articles for technical and scientific trade magazines. His articles have appeared in more than 50 magazines in 15 countries in North America, Europe and Asia.