

NEW TRENDS IN COUNTERFEIT COMPONENTS

Article reprinted courtesy of Integra Technologies

New Trends in Counterfeit Components

Over the past several years the electronics industry has seen a marked increase in the prevalence of counterfeit electronic components. Counterfeiters have attacked every commodity of electronics, from simple components such as capacitors, to complex integrated circuits such as microprocessors. Inexpensive commercial devices, as well as high cost military components, have seen counterfeiting. Today the problem continues with no indication of improvement. Today's counterfeit components are demonstrating that the counterfeiters are continuing to improve their techniques.

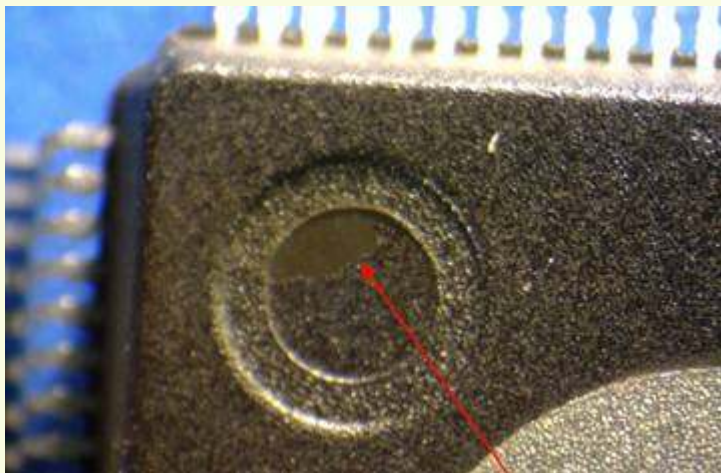
There are as many types of counterfeit devices as there are counterfeiters in the world. To help explain the issue and to manage the associated risks, one suggested method is to divide counterfeit parts into two major categories; non-functional counterfeits and functional counterfeits.

Non-functional counterfeit parts have, in recent years, been the most common type. These were the first major wave of counterfeit parts that primarily came out of China, recovered from salvaged electronics waste. This type of counterfeit device has only the appearance of the correct device, often with the wrong die internally and a remarked package. The counterfeiter's process is board removal, sanding, blacktopping and remarking followed by a detailed cleanup of solder and the package to make it look new. Today these parts are typically caught early on by a careful visual inspection with industry methods such as those documented in the IDEA standard 1010. On the occasions that they are not visually detected, then package de-cap or very basic tests such as a curve trace will identify the units. Even in the event that they reach the application board, these non-functional counterfeits will fail in system, hopefully before they can cause damage to the system board. They are clearly troublesome and can cause serious delays to manufacturing schedules but, they don't typically pose a great risk in the field. Pictured are examples of crudely done counterfeit parts with clear indications of sanding, blacktopping



and marking quality concerns.

SOT with sanding and crude laser marking



PQFP with clear indications of a blacktop



PQFP with sanding marks showing through the blacktopping

The more difficult class is the functional counterfeit devices. These **functional counterfeit devices** are becoming more prevalent since counterfeiters are now being caught more often, with the improved inspection methods at OEMS and independent distributors. To get past today's rigorous inspection techniques, counterfeiters have had to improve their methods. The best way to get past inspection and testing is to provide a part that looks right and functions correctly. There are many types of these functional counterfeit devices and each new type may require new methods to be detected. I will summarize a few functional counterfeit types and ways that testing laboratories such as Integra Technologies have been able to identify them.

Refurbished devices are one of the greatest problems. These parts are often the correct device and may even still have the original marking on the package. These refurbished units are a great risk since they are often subjected to excessive heat during removal and may have been introduced to harsh chemicals during the refurbishment process. Counterfeiters have become masters of reworking a package and the solder on the leads. They can make a board pull look new and unused. Even the best visual inspection techniques can have a difficult time identifying these refurbished parts with certainty. Typically, we find suspicious observations such as solder that looks too new, the absence of test contacts on leads, or questionable scratches and solder inconsistency. The units have the correct die internally, so decap provides no assistance in the detection. After careful visual inspection, an additional test that provides value with plastic parts is SAM (Scanning Acoustic Microscopy). SAM can look internal to the package to see if severe internal package damage is present. Also effective is electrical testing since device failure rates provide an indication of handling issues. At Integra we have commonly seen 20% or even higher failure rates with refurbished parts. It is important to realize that entire lots should be rejected since the high failure rates indicate systemic issues, which may indicate likely long term reliability concerns with all the units.

Often related to refurbished parts are new **remarking techniques**. The old method of blacktopping has been replaced by newer improved remarking techniques. Methods have been developed by counterfeiters to completely remove ink marking. Typically no remnant or shadow of the original marking remains, so the new markings look completely normal. Also in use by counterfeiters is surface sandblasting and laser ablation of surface markings. Even removal of laser marking can be accomplished without leaving sanding marks. Chemically impervious black-topping materials are in use that have similar material composition to the original plastic package. These blacktop materials are not dissolved by mil spec marking permanency or even acetone tests. Blacktop removal now must resort to more aggressive chemical removal methods such as Dynasolve. Pictured is a refurbished device with the correct die and nearly perfect marking. Only a Dynasolve was able to reveal that the units were blacktopped and remarked.



Another method available to counterfeiters is **die salvaging** from packages with subsequent die reuse in newly manufactured packages. For a few years a USA based company made a business out of this process. The company, MVP Micro, now shut down, chemically decapped devices, removed the die, and then had the die built into new packages in China. The result is a newly packaged device with the correct die internal. All the packaging and marking is new, so nothing raises inspection suspicions. However, there is great concern in using the parts since the chemical decapsulation process causes damage to the die, and their reliability is greatly diminished. An internal visual inspection of the die will not typically identify the recovered die. An extensive SEM DPA analysis could possibly detect the recovered die, but SEM analysis is not typically part of counterfeit device inspection. The best method of detection is a robust electrical test at temperature since the parts are not screened at temperature, and the manufacturing issues result in high failure rates due to the poor quality and reliability of the recovered die.

Also closely related to recovered die are units that are **newly manufactured from acquired die**. The new die can be purchased from reputable sources or illegally obtained from IC manufacturers manufacturing rejects. Leftover failed die can be effectively used by the counterfeiters since the finished unit will look correct in every way. Once again, the only effective method to identify these units is a robust electrical test since visual identification techniques are ineffective on newly packaged units.

Counterfeiters are becoming masters of **device substitutions**. In a way, they are working as component engineers trying to determine the device that will work as the best substitute for the requested device. Using device substitution techniques, they are able to replace one transistor with a similar function. It is a relatively easy task to identify a similar device and remake the component, since die markings on such components are not common. At Integra we have seen devices such as opAmps, replaced with similar performing opAmps with only small parametric differences detected at test. There is great danger in these situations since the replacement part may have much lower power handling capability or may not be able to withstand the required voltages or application environment. The counterfeiter's methods also extend easily to simple components such as capacitors, resistor and diodes. These simple device types often have minimal or no marking present on the packages.

As an example of a more complex device substitution, take the Atmel 28C16. The package condition and ink markings are very good on each of the counterfeits and without the benefit

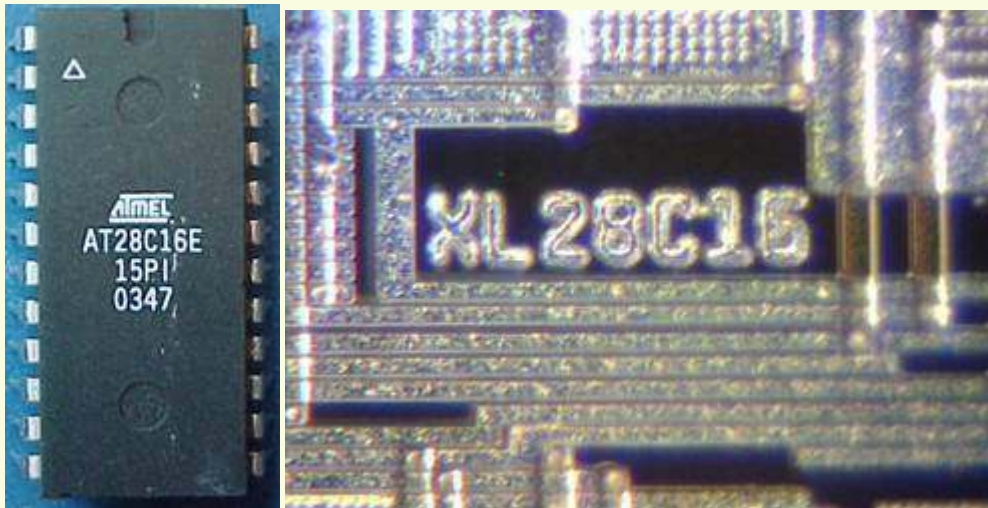
counterfeit. Both counterfeits have the 28C16 part number with the genuine device, not even using the generic 28C16 Atmel number. Also, in both cases the counterfeit devices are completely functional units. They both pass the basic functional tests only failing a few of the parametric tests. The first counterfeit sent had Catalyst die internal and only failed a write cycle parameter that was caused by a slight difference in datasheet specs. Since Catalyst doesn't exist anymore, a visual inspection of the die with the correct part number might not have been identified as the wrong die. The second counterfeit device sent was both Atmel and the 28C16. However it was an older generation of the device and again the wrong die. It passed functional testing, but failed power supply current test limits. In both cases, without a robust electrical test these units could have easily ended up in systems. They might have even worked well in the application, however, we don't want counterfeiter's making our component decisions.



Genuine - Atmel Device



Counterfeit - Marked Atmel with Catalyst Die



Counterfeit - Marked Atmel with Old Generation Atmel Die

One last type of functional counterfeit that continues to be an issue is **manufacturing rejects**. These failed devices are occasionally showing up in the secondary components supply chains. Most manufacturers have tightened their procedures to ensure that failed devices are not reused; however, it is difficult in Asia to have complete assurance that a failed device is destroyed. Some of the units can get diverted or smuggled out and eventually are sold as new. These failed units are often nearly functional, and with the true manufacturer marking they look in every way like real units. The risks are also significant for eventual re-use of rejected wafers, or re-use of the remaining failed die left over after assembly. Robust electrical test is the only effective method to identify manufacturing rejects that could be sold as good units.

Counterfeiters are going to continue to find new ways to attempt to slip parts through our best inspection and test methods. It is also likely that they will be successful at times since detection methods will always be playing catch-up with their newest techniques. Clearly, buying parts on the secondary market is a risk and anyone who must deal in the secondary market should use the best inspection and test methods to minimize their risks.
