

Counterfeit? But They Passed Testing!

by Christopher Torrioni
SENSIBLE MICRO CORPORATION

Summary — *With all the awareness and improvements in counterfeit avoidance practices, why are so many companies still getting burned with substandard or bogus components? They aren't being thorough enough in terms of strict sampling and supplier evaluations.*

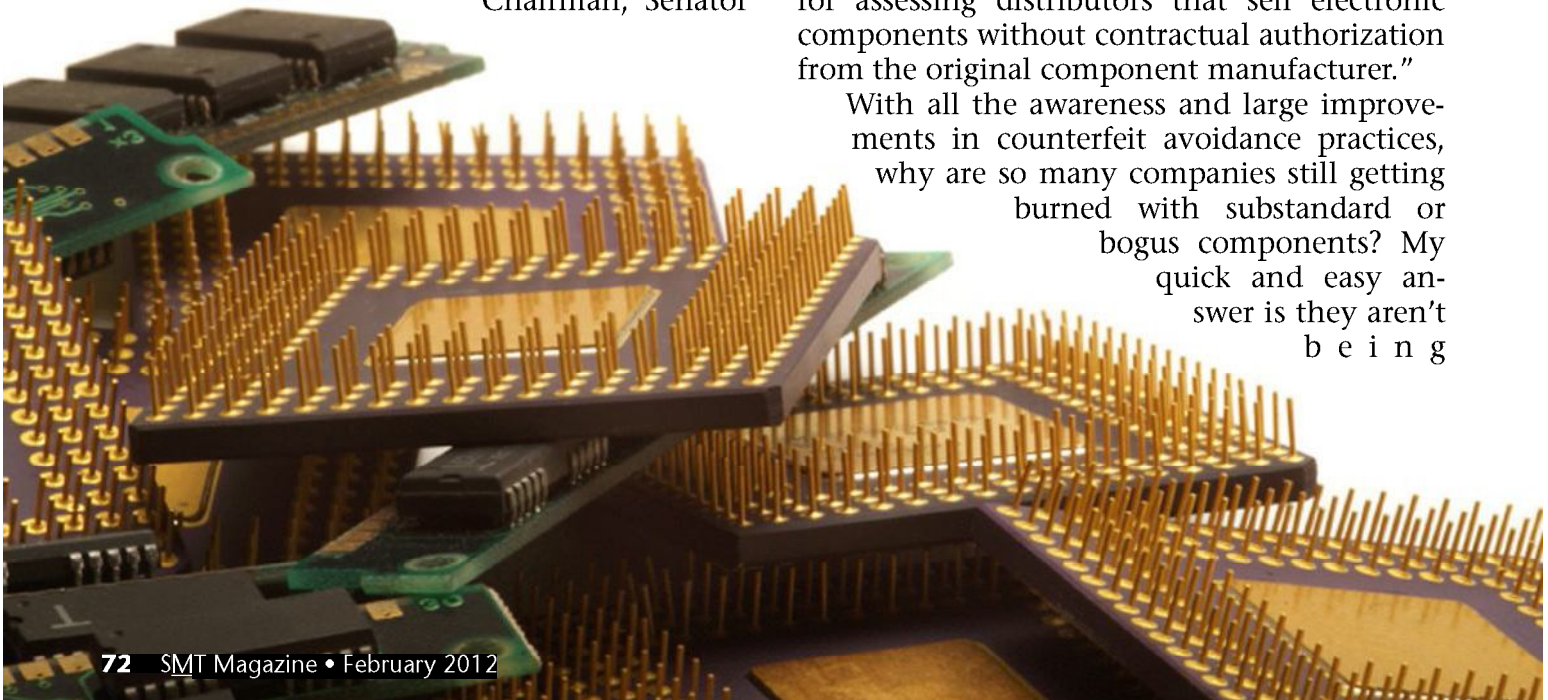
Substandard and counterfeit electronic parts have flooded the market during the past decade, sparking a national movement from industry players and market experts to address an effective solution. Although a few industry groups have implemented best practice anti-counterfeit procedures (IDEA-1010 and CCAP-101) and defined what classifies under the "counterfeit" umbrella, it is the United States government that is subsequently applying intense pressure to get the growing problem under control.

This past November, the Senate Armed Services Committee completed an investigation into occurrences of counterfeit electronic parts in the military supply chain. Lead by Chairman, Senator

Levin and Ranking Member, Senator McCain, the committee held their first hearing to explore the shocking results and question industry experts. On the surface, it seems major changes are finally underway. Congress has since approved the National Defense Authorization Act for Fiscal Year 2012, which includes requirements to define the term counterfeit and establish a standard for the detection and avoidance of counterfeit parts. The standard will be issued by SAE, similar to AS5553 already in existence for electronic manufacturers, but will pertain to distributors only. The new standard, AS6081, is still being developed by the G19 Committee and is expected to be released sometime in 2012.

Last month, SAE released ARP6178, Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors. According to SAE's website the scope of the standard is "for all organizations that procure electronic components from sources other than the original component manufacturer. It is especially applicable for assessing distributors that sell electronic components without contractual authorization from the original component manufacturer."

With all the awareness and large improvements in counterfeit avoidance practices, why are so many companies still getting burned with substandard or bogus components? My quick and easy answer is they aren't
b e i n g



COUNTERFEIT? BUT THEY PASSED TESTING! *continues*

thorough enough in terms of strict sampling and supplier evaluations. But, as we all know, there is nothing quick or easy about stopping the wave of counterfeits entering the supply chain. In the meantime, more and more OEM and EMS providers are running super lean, keeping long-term forecasting at bay and still supporting legacy builds. Critical shortages that require non-franchised solutions are consistently abundant, opening up a slew of quality issues for those that are sourcing from bush-league suppliers who do not care or do not know how to navigate an ever-graying market of trouble.

With so many layers of mitigation that can be applied to ones checklist, I suspect most companies get lost on what inspection and test efforts should be focused. For instance, we see a large number of companies strictly performing a basic parametric electrical test while de-capping one or two samples out of the lot to verify die authenticity. Although there is value in these procedures, they simply are not 100% effective in the determination of a component's integrity.

The re-grading of COTS components to military or industrial levels is the scariest form of counterfeiting in the market today and most difficult to detect. Counterfeiters have become highly sophisticated at remarking products, leaving traditional methods for visual inspec-

tion and basic electrical screening as obsolete methodology. We see the same trends for FP-GAs and memory, where slower clock speeds are remarked to faster callouts. The RoHS market has been especially affected; usually a surplus of leaded material is in abundance which drops component costs drastically and can be easily sourced. Counterfeiters then remark the product with the known RoHS callout. Unfortunately, there may not be enough data on the internal die to make a clear determination and basic electrical screening would most likely pass test parameters which could later fail in the field or cause mayhem during assembly.

In my experience, supplementing traditional screening practices with more in depth analysis can provide clear determinations on the integrity and authenticity of a component in question. Below is a summary of methods that should be considered in an effort to keep your supply line free of substandard and counterfeit components. Implementing these practices or aligning yourself with a supplier that is able to provide them for you is essential in today's market.

External Visual Inspection

A stereo microscope with zoom lens and image or video capture capability is a must have to clearly detect and document any abnormalities. Encapsulated chips should be free from any foreign substances such as epoxy (blacktopping) or sanding marks (part marking removal process). A given lot should be consistent all the way through in terms of pin one orientation, mold cavities, and part markings (matching date and lot codes, country of origin). Leads or contacts should be free of solder residue; contacts should be straight and appear new showing original OCM tooling marks in the bends of the leads.

If possible, communicate with the OCM to confirm if part labels showing manufacturer part number and lot codes are authentic. Labels are highly counterfeited as well so only use as one piece of the puzzle, not a sole determining factor.

Marking Permanency

Sophisticated counterfeiters are using newer methods of remarking that are resilient to ac-



COUNTERFEIT? BUT THEY PASSED TESTING! *continues*

etone swabbing. By baking the epoxy finish on to the parts and laser etching the markings, counterfeiters have achieved visually appealing results. A heated chemical test (HCT) will dissolve the epoxy finish and can reveal original laser etching (ghost markings) or other evidence such as sanding marks.

X-Ray Testing

X-ray is a powerful mitigation procedure. However, it is more effective if you have a known good sample to compare the lot with. We use this method in counterfeit analysis, but can also be an effective tool if you have older or refurbished products needed for field repair and just want to check the integrity of the wire bonding. During counterfeit analysis, we also can check the die location and size over an entire lot, confirming if any inconsistencies are occurring.

Decapsulation and Die Verification

Although decapping can confirm if you have authentic internal die, it is dependent on how much information is available on the die for giving clear determinations. If a component has been re-graded, it is possible only the series of the callout is listed on the die. Decapping is used as just one procedure in an arsenal of avoidance techniques and should not be used as a sole determination.

XRF (X-Ray Fluorescence Analysis)

XRF is one of the most effective tools you can have in your anti-counterfeit arsenal because it tells you the elemental composition of the device. Last year, we received in suspect tantalum capacitors and were able to confirm the elemental makeup of the components were vastly different from a known good lot. Although the capacitors passed electrical screening, it was XRF that produced a clear red flag for rejection.

Parametric Electrical

I do not recommend using electrical screening as a sole determining factor. Again, if a part has been re-graded, they will most likely pass screening and can make it into the field where a latent failure can occur. One of the major problems with re-graded components is a commer-

cial item is being used in a rugged environment, such as high temperature or extreme vibrations, even though it has not been built or tested to withstand such variables. However, parametric electrical is a great tool in evaluating if any ESD shorts are occurring in the device. Sufficient labs will test the input/output ratings against the temperature grades and speed to confirm all are within OEM spec documentation as well.

Scanning Acoustic Microscope (C-SAM)

By using high-frequency sound, C-SAM is able to penetrate internal defects not detected by traditional X-ray. Component's exposed to moisture and temperature fluctuations over time may result in delamination, causing cracks or stressing of the internal die. Although no signs of failure may be occurring at time of electrical test, this is a great indicator of possible potential failures in the field if signs of delamination or showing.

Always remember, counterfeit avoidance and mitigation is about having a robust program in place that collects data from many key areas, not relying on just one or two procedures. Start with the most basic and cost effective processes and work your way up to the more in depth items. Having a full arsenal of avoidance practices at your fingertips can provide you clear determinations that can keep a supply line free of substandard and counterfeit components. **SMT**



Christopher Torrioni is President and co-founder of Sensible Micro Corporation, a professional stocking distributor and sourcing partner to hundreds of global OEM and EMS manufacturing companies. He obtained his Bachelor's Degree from the University of Central Florida and brings 11 years of industry knowledge and experience in electronic component supply, market news, procurement pitfalls and quality assurance standards. Torrioni is also a corporate sponsor to the SMTA Tampa Bay Chapter, as well as the Tampa Chamber of Commerce and Tampa Bay Technology Forum.