This article is part of the IEEE Reliability Society 2008 Annual Technology Report.

# Response to Counterfeit ICs in the Supply Chain

Gary F. Shade
Insight Analytical Labs (IAL)
Email: gshade@ial-fa.com

**Introduction**

Webster [1] defines a counterfeit item as "made in imitation of something else with intent to deceive". In the case of electronic components, this is done with increasing regularity to meet market demand with products at inflated prices often substituting complete frauds that do not match the form, fit, or function of the intended component. The counterfeiters attempt to deceive the consumer into thinking they are purchasing a legitimate item, or convince another supplier that they could deceive others with the imitation. An example of a remarked IC is shown in Figures 1(a) and 1(b). The IC was remarked to match a more desirable memory, thus increasing its present value.

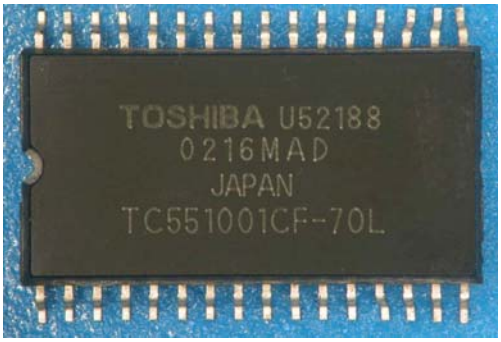


Figure 1(a): Optical photographs of two packages with same date code show very similar markings, but mold marks are missing on one device.


Figure 1(b)

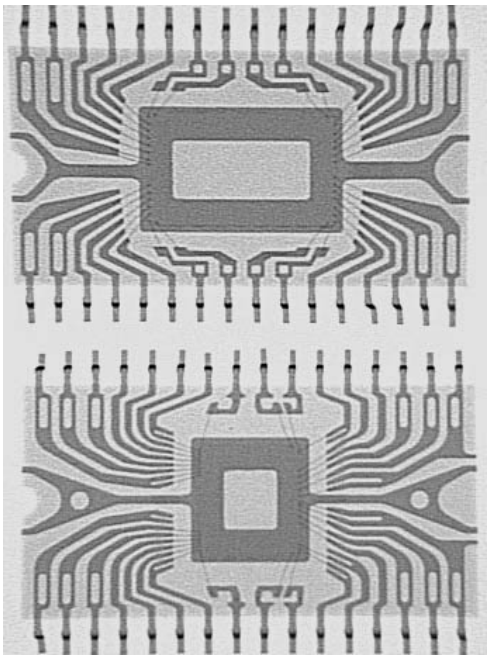

Figure 1(c): X-ray inspection of packages in 1(a) and 1(b) indicates two products that are clearly different. One has been re-marked and mixed in with authentic components to prevent detection.

Counterfeiting of electronic components is occurring in increasing numbers requiring resources to maintain or improve quality levels. The presence of counterfeit components in the supply chain (and in use) has an impact to all who supply and use these components and their assemblies. Procurement methods coupled with failure analysis, utilizing industry experience and a disciplined approach can provide great improvements in reducing this impact. This article addresses this topic to promote awareness of the problem as well as offer some solutions. Each example presented will raise many questions, and only some will be answered here. It is

sufficient that those who use or analyze electronic components learn to be aware of conterfeiting and to take appropriate action.

**Examples from the supply chain**

The traditional opportunities for counterfeiters increased as semiconductor technology spread across multiple continents making basic IC processing more accessible. Now the opportunity is expanding even further as mature products are discontinued in favor of more profitable ones and supply chains reach across the globe and across many different languages, cultures and legal systems to meet demands. Thus, the ability to analyze and detect counterfeit components can be critical in insuring high quality.

In the past, it was assumed that most counterfeit parts were copies (or clones) of high value components to be sold as the original for the full price. These clones were made by (often intensive) reverse engineering and reproduction of an IC. They were meant to operate like the original but each was produced without the experience and quality of the original manufacturer. This limited the choices for components likely to be counterfeit. With the maturing of the Electronic component industry, and its expanding range of low-cost commodity products, the opportunities for counterfeiters have increased. In addition, there are increasing numbers of components that are obsolete or have dwindling supply driving their value higher. Due to shortages, any electronic device can potentially increase in value and be a target for counterfeiting. To compound this, the worldwide shift towards lead-free solders has provided additional opportunities for fraud as manufacturers struggle in some cases to provide both leaded and lead-free products. This situation is leading to increased use of traditional counterfeit methods such as remarking the product type or speed of high-end components. At the same time, new methods are appearing such as modified RoHS markings and other fraud of low cost components. As a result, the quantity and variety of counterfeit ICs entering the supply channels is increasing.

The next example shown is an IC marked as Lattice seen in Figure 2. Two parts are shown side-by-side from the same lot packaging. Notice that both parts have alpha-numeric markings indicating the same device type and assembly lot. Oddly, only one has a pin-1 indicator and the mold marks are only partially visible on the second unit. This is very unlikely to occur within the same assembly lot. Internal inspection after decapsulation [2] added more concern as the die on the right was produced by AMD a foundry known to be used by Lattice for this MACH production, but not until the late 1990s. (See figures 3 and 4). The date on the die is 1991 indicating the die is not likely to be authentic. The conclusion is the package has been sanded to remove old markings. Next it is remarked to look like the more recent (and valuable) one beside it. In addition to these observations, the product undergoes several tests to determine its authenticity. Each test result is then used to determine the overall confidence. Some products require many tests before authenticity can be determined.


Figure 2: Sample with no Pin-1 marker, very odd. Notice both parts appear to be from the same date code and assembly lot, yet the one on the right is missing the pin-1 dimple and most of the mold marks. Lighting has been adjusted to enhance the markings.

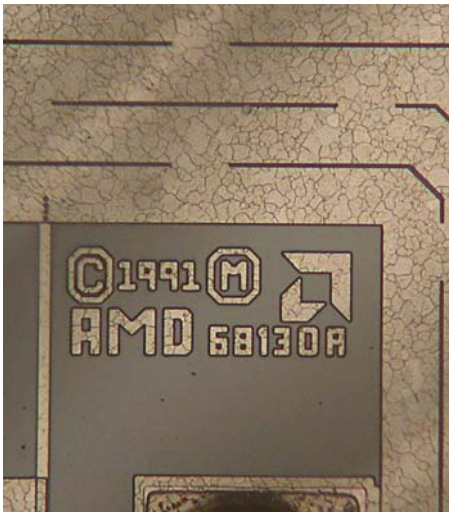


Figure 3: After decapsulating the part in figure 2, the die markings are visible showing the AMD logo, Mask set number and copyright date.

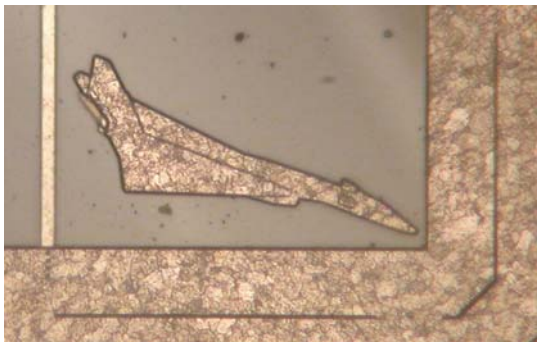

Figure 4: Also visible after decapsulation is a second AMD logo of an aircraft representing the "Mach" name.

**Current Observations**

Today's leading edge process technology is becoming more difficult to copy with 7-10 layers of copper metallization, 45nm geometries and sophisticated packaging. These same products often use sophisticated anti-counterfeit measures that are a challenge to overcome for all but a few counterfeiters. These difficulty factors appear to be expanding the market for forgeries of mature, less complex components. Such components are still in very high demand and can be easy to introduce into the supply chain.

To date, over 150 product types have been inspected for authenticity by the author's company. From these, forgeries have been observed that range from complete frauds (do not match the form, fit or function of the original) to subtle changes of the date code. The former are not likely to elude detection for long, but may pass through one or more distributors before being detected. More typical are parts that have the correct package type, but are remarked to indicate a match to a desirable part. Visual inspection alone will not detect these and they are often mixed in with authentic parts to further reduce detection. Remarked components recently detected have been from different date codes that are re-marked at the package level to appear from the same date code and revision level. Figures 5(a) and 5(b) show an example of detecting remarking. The top surface has been polished or ground away to remove the original marking and then a textured, black paint was sprayed on to refresh the surface. Careful inspection is required to observe the black paint as seen in this figure. Next, the package is re-labeled to match the original. The ink on counterfeit components may or may not meet mark permanency tests required by the industry.

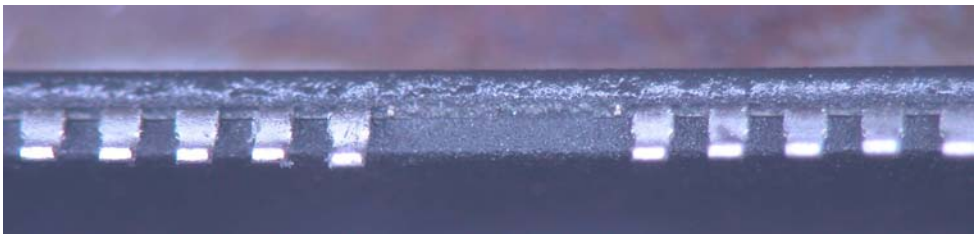

Figure 5(a): Example of paint at package edge from remarking.

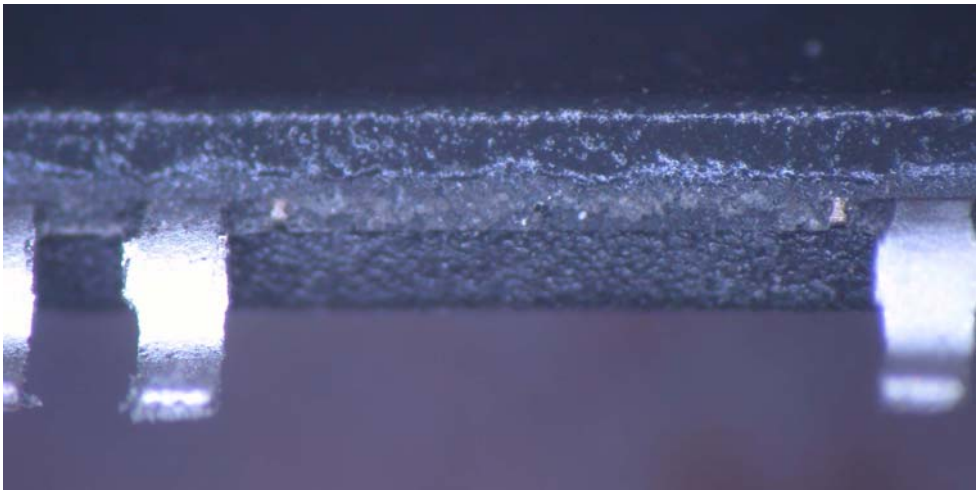

Figure 5(b): Example of package remarking. Close-up view of figure 5 (a).

**Impact and Summary**

The size and impact of the counterfeit problem is difficult to measure. This past year (2007), the U.S. and European Union worked jointly to seize 360,000 counterfeit ICs and computer network components bearing over 40 different trademarks. These products were selected for the joint operation because they presented either a safety or security risk (along with infringing intellectual property rights) [3]. Globally, all forms of counterfeiting are on the rise. Experts estimate the total as 5-7% of total world trade [4].

The range of impact; however, is quite wide. Suppliers must now take extensive measures to secure supply channels to protect their image. Board and system manufacturers in turn need to qualify suppliers, with inclusion of methods for detecting counterfeit products. Component suppliers (brokers, distributors, etc.) need additional inspections to screen potential counterfeit products from reaching their customers. Finally, Failure Analysts need to apply additional measures to determine if failures are caused by the wrong component, potentially one that appears and operates similarly to an authentic device. Such counterfeit failures have been seen at IAL in the normal course of analysis.

**References**

[1] “counterfeit”. Merriam-Webster Online Dictionary. 2008. Merriam-Webster Online. 05 May 2008 < http://www.merriam-webster.com/dictionary/counterfeit>

[2] Microelectronic FA Desk Reference, 3rd Edition, 1993, Mechanical and Chemical Decapsulation, ASM, Thomas W. Lee, pp. 61-90.

[3] ”The United States Mission to the European Union.” United States Mission to the European Union. 22 Feb. 2008 17 Apr. 2008

<http://useu.usmission.gov/Dossiers/IPR/Feb2208_Operation_Infrastructure.asp>, (This website is produced and maintained by the Public Affairs Office, United States Mission to the European Union)

[4] “Counterfeit”, Wikipedia, The Free Encyclopedia. Apr. 16, 2008 <http://en.wikipedia.org/wiki/Counterfeit>.

Additional reading on Counterfeiting:

[A-1] Shade, Gary F., and Brian Wilson. "Response to Counterfeit Integrated Circuit Components in the Supply Chain, Part I." Electronic Device Failure Analysis Magazine. Vol 10, No. 4. Nov. 2008: 16-22.

[A-2] Grow, Brian, Chi-Chu Tschang, Cliff Edwards, and Brain Burnsed. "Dangerous Fakes." Business Week 2 Oct. 2008: 1-8. Business Week. 2 Oct. 2008. 4 Oct. 2008 <http://www.businessweek.com/print/magazine/content/08_41/b4103034193886.htm>

[A-3] US Government. Immigration and Customs Enforcement (ICE). "Value of CBP, ICE seizures of counterfeit goods in FY2007 is up 27%. Nearly $200 million in goods confiscated as a result of enforcement actions." Press release. 28 Jan. 2008. 11 July 2008 <http://www.ice.gov/pi/news/newsreleases/articles/080128washingtondc.htm>.

[A-4] Jorgensen, Barbara. "Chip makers step up anti-counterfeiting efforts." 31 Oct. 2006. EDN-Electronic Design News. Reed Elsevier Inc. 11 Nov. 2008 <http://www.edn.com/index.asp?layout=articleprint&articleid=ca6386712>.

[A-5] "Beware Counterfeit electronic components." DataWeek 7 Apr. 2004: 1-2. Electronics and Communication Technology. 7 Apr. 2004. TechNews Publishing Ltd. 17 Nov. 2008 <http://dataweek.co.za/article.aspx?pklarticleid=2922&pklcategoryid=31>.

[A-6] "Counterfeit Components: The Trends, the Threats and One Promising Solution." Counterfeit. BP council. 18 Nov. 2008 <http://www.bpcouncil.com/apage/609.php>.

[A-7] Miller, Joanna. "Hidden No More." Mar. 2005. Schofield Media. 15 Aug. 2008. 24-28. <http://www.planetxs.com/images/march 2005 usbr article.pdf>.

[A-8] Thompson, Brad. "Counterfeit." 1 Feb. 2005. Penwall Publishing. 18 Nov. 2008 <http://www.tmworld.com/article/ca500057.html>.

[A-9] "Anti-counterfeiting Standards Task Force Launced at SEMICON West 2007." Aug. 2007. SEMI. 19 Nov. 2008 <http://www.semi.org/en/p042417>.