As originally published in the IPC APEX EXPO Proceedings.

Counterfeit Electronic Components Identification: A Case Study

Martin Goetz and Ramesh Varma
Northrop Grumman Corporation
Linthicum, MD

Abstract
Counterfeit electronic components are finding their way into today's defense electronics. The problem gets even more complex when procuring DMS (diminishing manufacturing source) parts. This paper will provide a brief introduction to counterfeit prevention and detection standards, particularly as they relate to the Aerospace and Defense sector. An analysis of industry information on the types and nature of counterfeit components will be discussed in order to illustrate those most likely to be counterfeited, followed a specific case at a major defense contractor. The case involved two circuit card assemblies failing at test, whereby their root cause for failure was identified as "unable to write specific addresses at system speeds". The error was traced to a 4MB SRAM received from an approved supplier. Fifteen other suspect parts were compared with one authentic part directly purchased from a supplier approved by the part manufacturer. Defects or anomalies were identified but not enough to unequivocally reject these parts as counterfeit as the defects could have also happened in the pre-tinning process, which is a program-specific requirement if the parts were stored for more than 3 years. Through the subsequent analysis, subtle differences between the authentic and suspect parts were identified and isolated. The methodologies and process chosen to identify counterfeit parts will be reviewed and an assessment of the results will be presented along with the defects found in relation to the defect types reported in relevant test standards.

Introduction
The Defense Federal Acquisition Regulations DFARS 252.246-7007Contractor Counterfeit Electronic Part Detection and Avoidance System defines a counterfeit part as:

> *an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified* ***electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts*** *represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.*[1]

Highlights for the DFARS Case 2012-D055 final Rule include:

- applying requirements to the acquisition of electronic parts and assemblies containing electronic parts, including commercial items (COTS)
- defining "Counterfeit" and "Suspect counterfeit", is limited to electronics, including embedded software and firmware
- The costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use of inclusion of such parts are unallowable (unless electronic parts were provided as GFE and timely notice of discovery was provided by contractor)

Based on the highlights for the ruling and the impact that counterfeit parts could have on the performance of fielded systems, it should be obvious in terms of the importance of understanding, identifying and addressing suspect counterfeit parts in the Aerospace and Defense industry. Although the current definition and ruling applies to electronics, the expectation is the definition will eventually broaden to include non-electronics, i.e. optics, mechanics, MEMs, and materials. Therefore, a robust process to ensure parts that are received and used in systems to support the Aerospace and Defense industry is paramount to not only the business and industry, but to the users of the products that rely on these systems, especially the warfighter.

Counterfeit parts business is a multi-billion-dollar industry
The discussion of recognizing that counterfeit parts have been introduced into the supply chain is not new, with various companies, and technical journalspublishing as early in 2002.[2,3]In a 2006 article published by Pecht and Tiku[4]and noted in the UK Electronics Alliance (UKEA) position paper, "UKEA Position on Counterfeit Electronic Components"

> *Alliance for Grey Market and Counterfeit Abatement (AGMA), based in the USA, estimates that, in 2006, up to 10% of technology products sold worldwide are counterfeit, which amounts to US$100bn of sales revenues. However, this does not take into account consequential losses. In 2007, the US Patent and Trademark Office estimated that total 'counterfeiting and piracy (activity) drains about US$250bn out of the US economy each year and 75,000 jobs.'"*[5]

A primary driver of counterfeit parts has been part scarcity, or diminishing manufacturing source and material supply (DMSMS). Realizing that as the consumer market began to grow exponentially in the 1980's and 1990's, the supply base for manufacturing parts rated for military and high reliability applications was having a difficult time keeping up with demand, and part availability was becoming more difficult. These market forces drove the opportunity to introduce counterfeit parts into the supply chain through 'gray market electronics brokers'. According to a 2001 article on fake parts,

> *One U.S. independent distributor, which asked to remain anonymous, said it paid a broker in China $70,000 for 1206 case-size ceramic capacitors about three months ago. The 90-cent parts-which under less-constrained market conditions would have cost 20 cents-slipped through two quality inspections before arriving on the OEM's production floor.*[6]

Bad parts are not always counterfeit

It is important to recognize that, just because there are anomalies identified on electronic parts, it does not signify that the parts are counterfeit. It does, however, requirethe incoming inspection organization to assume the responsibility to make initial determination as to whether there is enough evidence to suggest the parts from a lot or shipment should be evaluated for additional anomalies. Three important points to consider when creating a system to screen for counterfeit parts are:

- They are not easy to identify even with sophisticated analytical methods
- They are in the supply chain even with authorized distributors
- They are more of an issue with obsolete parts

Background on case study

During functional test of control module boards used in a multiple sub-array of a testable antenna, two boards failed. The root cause for the failures was identified as "*unable to write specific addresses at system speeds*". When diagnosing the issue, it was narrowed down to an SRAM that was supplied by an electronics part broker (Broker).The parts in question were procured from the Broker, an approved Diminishing Material Supply (DMS)supplier, due to unavailability from a franchised distributor (Dist) of the Original Components Manufacturer (OCM).When reviewed by the internal Failure Review Board, it was determined that a comparison of SRAM parts supplied by the Broker should be compared with parts from the Distributor to determine if there were any observable differences in the parts.

Analysis Approaches and Techniques

A total of 7 different methods which ranged from nondestructive to destructive were used to make a determination about the SRAM parts being suspect counterfeit. Any individual analysis does not make a clear case on its own merits. However, in order to make a legal case for suspect counterfeit, enough due diligence is necessary. The following outlines the 7 analyses used to make the case:

1. Visual inspection by Optical Microscopy
2. X-Ray
3. De-capsulation
4. Scanning Acoustic Microscopy
5. FTIR
6. Electrical Test
7. Discussions with OCM

Visual Inspection by Optical Microscopy

Once the failure occurs on a component or subsystem, typically there is an optical inspection to determine if there was any physical damage to the part either before or during testing. Damage can occur from a variety of sources including handling, testing conditions and setup, foreign object damage or debris (FOD), fixturing, etc. Figure 1 shows a comparison of an SRAM received by an authorized distributor and the broker in question. It was noted that the lot number of the broker part was not in the OCM database.

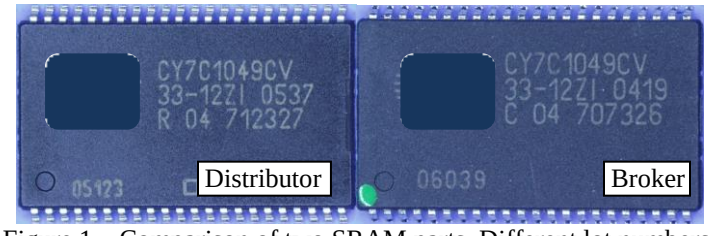


Figure 1 – Comparison of two SRAM parts. Different lot numbers.

This in of itself does not constitute a ‘smoking gun’, but it does inspire one to continue the investigation. Upon further visual inspection, it appeared the workmanship, or quality of the part around the leads suggested a difference in mold processing (Figure 2). Because visual inspection is subjective and directed by any given customer requirements, incoming inspection (5-10X at AQL) easily can miss the inconsistencies. This is especially true when suspect counterfeit parts are mixed in the same delivery packaging and 100% inspection is not performed.

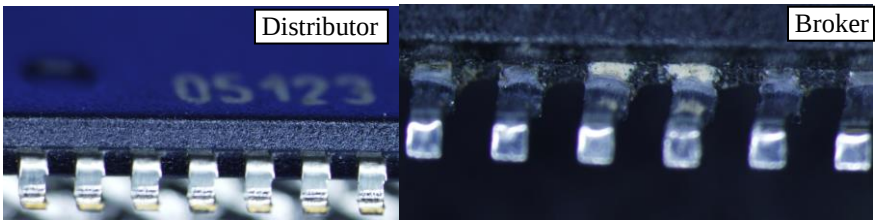


Figure 2 – Lead and mold inspection. Different mold interface and pin width.

Finally, there was a measurement of pin width between the two different leads. The leads from the distributor parts were on the order of 14.5 mils wide, whereas the lead width from the broker parts was 12 mils.The difference led to the next step in the investigation, namely X-ray.

X-Ray

A real-time X-ray inspection system, a common instrument used in manufacturing from incoming inspection, through assembly and failure analysis also comes in handy when performing investigationsof suspect counterfeit parts.In this *investigation*,X-ray quickly revealed two different leadframes were being used for assembly of the memory device. Figure 3 shows not only design differences in the lead design but also the die paddle design. It is interesting to note that the broker shipped parts used the same leadframe design as the distributor on one delivery date, while a different leadframe 3 months later.The difference in leadframe geometry could contribute to the electrical performance of the SRAM through contributions of parasitics, including wirebond length and location.

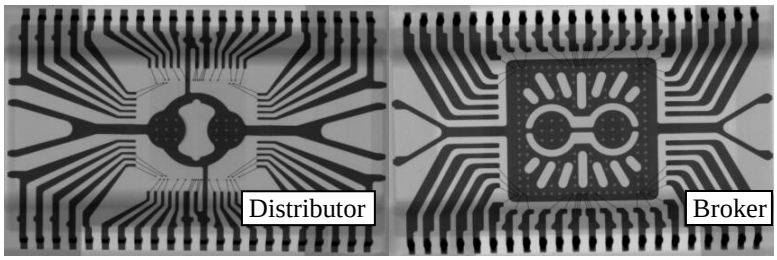


Figure 3 – X-ray of leadframe. Different lead and die paddle design.

C-SAM

C-Mode Scanning Acoustic Microscopy (C-SAM) is another tool used to detect anomalies within a particular electronic device. It is a form of ultrasound that uses cyclical sound waves to determine density differences within a sample and has been demonstrated to be an effective anti-counterfeiting screening tool. C-SAM allows a planar view of the interfaces between materials with intent to determine delamination. Using Figure 3 as a reference, the left leadframe used by the distributor and the broker (in some lots) showed acceptable delamination between the mold compound and the leadframe. However there was significant delamination between the interfaces in the right leadframe. Delamination provided a source for trapping moisture in the part, which could lead to electrical issues including short circuits.

Decapsulation

Decapsulation of the packaged devices exposes the internal components of the package. Opening devices by decapsulation allows inspection of the die, interconnects and other features typically examined during failure analysis. Device failure analysis often relies on the selective etching of polymer encapsulants without compromising the integrity of the wire bonds and device layers. This is achieved by using microwave plasma to cleanly remove encapsulant material.[7] Figure 4 reveals that through decapsulation two different die were used for this SRAM. Although revealing, it does not immediately suggest counterfeit, as it allows that there may have been die shrink. The date codes from the packages indicate the die and leadframe came from a part manufactured 2 years earlier, with a different revision, and were therefore not for the same part. This is another indicator that using older parts with a new date and lot code suggest counterfeiting.

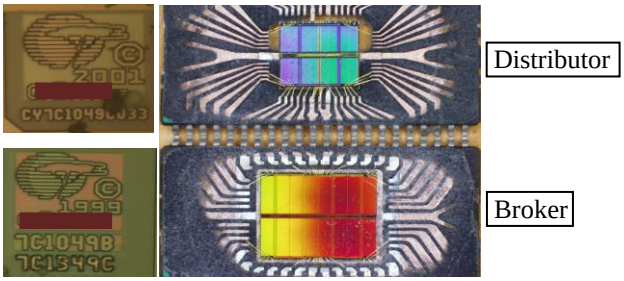


Figure 4 – Decapsulation of SRAM parts. Different leadframe, different die.

The decapsulation results led to another evaluation of the mold compound to determine if the package mold was replaced after reuse. Two areas were inspected, the mold compound surface and the laser marking. Figure 5 shows the texture of the mold compound surface of two packages, one from the distributor, and the other from the broker. It is clear under high magnification that there is a difference, suggesting two different mold compounds were used to encapsulate the die within the package from the two different sources.

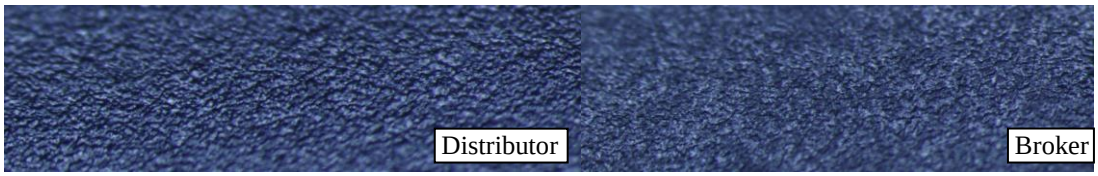


Figure 5 – Mold compound surface. Different texture, color and consistency.

Evaluating laser marking to identify anomalies involves close inspection of the surface of the mold compound. According to one OCM,

> *In the process of adding a mark, the laser can cause damage to the underlying die or wires if it gets too deep into the package or compound. Basically, the laser creates a groove by burning away the mold compound in order to make a visible marking. The groove or depth can vary depending upon the speed, power, and pulse rate of the laser marker. To measure this, special depth measuring equipment is required due to the small dimension of the groove.*[8]

As indicated by Figure 6, a clear difference is noticed by the texture of the marking. Since the depth of the etching or removing of mold compound can be detrimental to the function of the semiconductor device, it is important to control the depth. The marking from the distributor part is smooth, whereas the marking from the broker is course and the presence of glass beads in the marking area indicate improper marking.

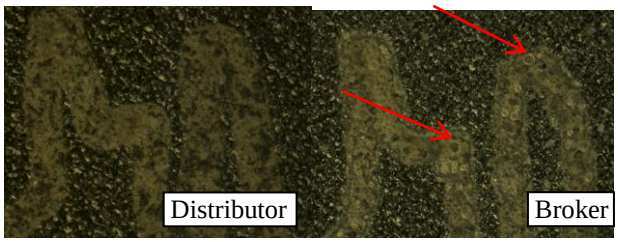


Figure 6 – Laser marking on mold compound. Smooth surface versus rough.

FTIR

Fourier transform infrared spectroscopy (FTIR)[9] is a technique, which is used to obtain an infrared spectrum of absorption or emission of a solid, liquid or gas. A FTIR spectrometer simultaneously collects high spectral resolution data over a wide spectral range. This confers a significant advantage over a dispersive spectrometer, which measures intensity over a narrow range of wavelengths at a time.[10]For this evaluation FTIR was used to evaluate the integrity of organic mold compound. When a blacktopping process is used to re-mark previously used parts, FTIR provides the ability to distinguish between two different materials. The materials that comprise the component body and any blacktopping material used to hide the evidence of counterfeiting are all organic polymers.As indicated by the spectroscopy measurement in Figure 7, there is a clear difference in response between parts. Using the Distributor part as the baseline, the response from the Broker parts suggests a different material is present. Blacktopping material is added to the baseline material and therefore would create a different response from the baseline. This measurement is one more indication of inconsistency between two different supplier parts.

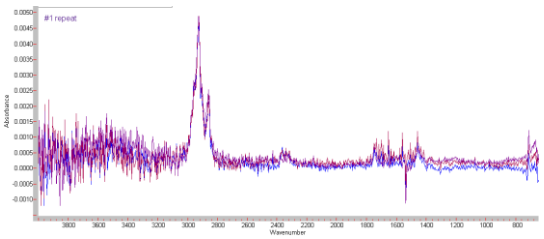


Figure 7 – FTIR spectroscopy graph. Blue identifies mold compound spectra as received from Distributor, red and purple from Broker.

Electrical Test

Engaging an outside source for electrical test provided an independent assessment of the part performance. The outside source identified multiple configurations of die from the electrical testing, however few parts failed retest. Test requirement specifications should have triggered some concern in acceptance at Receiving Inspection. However, since parts received met MIL spec.requirements as evidenced by a certificate of compliance, and the internal procurement criteria called out only MIL spec. for parts purchased out of the distribution chain, they were accepted.

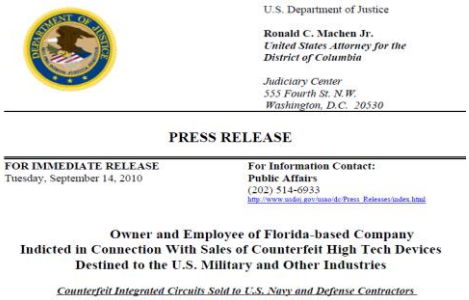
Discussions with OCM

After contacting the OCM to make some determinations about the discrepancies, Broker part # CV7C1049CV and lot# 06039 did not match with the OCM database. The OCM stated that parts with the larger die size would have a different part number CY7C1049BV33 showing the revision of the part. The two types of die seen in the Broker parts were manufactured by the OCM in 1999 and 2001 respectively. The OCM suggested retention of original labels on the reel and containers for authentication check. The Distributor generally removes these and re-labels with new distributor or customer part numbers. The Broker however retained the numbers and therefore these numbers were able to be used to track against the OCM database.

Summary and Conclusions

After the analysis was performed, it was determined by the internal Failure Review Board (FRB) that all parts from the Broker were not suspect and therefore, small lot testing may not catch counterfeit parts. It was not clear if suspect packages were harvested or re-packaged since there was evidence that both were possible through previous versions of devices as well as suspected blacktopping of the package surface. It is clear that counterfeit identification by inspection and testing is very difficult unless resources are committed to evaluate virtually 100% of parts being supplied. Records tracking were difficult because the Distributor did not keep the labels and paperwork from the original manufacturer, although they could be found through diligence before re-labeling occurred. Since the SRAMs were used for high reliability applications, the parts were scrapped. The U.S. Department of Justice filed a lawsuit against the Broker after determining that enough evidence suggested counterfeit parts were sold, primarily to defense contractors. Figure 8 shows a press release of the lawsuit with the following excerpt,

> *A December 2009 sale of 350 counterfeit OCM Semiconductor ICs to a company in New York in fulfillment of a contract with (major US defense contractor) for integration into a beam steering control module board within the multiple sub-array of a testable antenna for the U.S. Navy Replacement Program (ballistic missile defense).*[11]


U.S. Department of Justice

Ronald C. Machen Jr.
United States Attorney for the District of Columbia

Judiciary Center
555 Fourth St. N.W.
Washington, D.C. 20530

PRESS RELEASE

FOR IMMEDIATE RELEASE
Tuesday, September 14, 2010

For Information Contact:
Public Affairs
(202) 514-6933
http://www.usdoj.gov/usao/dc/Press_Releases/index.html

Owner and Employee of Florida-based Company Indicted in Connection With Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries

Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors

Figure 8 – Press release of U.S. Department of Justice lawsuit against electronics distributor.

Through the due diligence process, inspection, analysis and discussions with the OCM, Distributor and Broker, it was found that enough evidence suggested action be taken internally through legal channels in reporting these SRAM components as suspect counterfeit parts. Once the U.S. Department of Justice was notified and action was taken, the Broker was removed

from the list of possible sources for electronic devices by at least one defense contractor. Ongoing vigilance would be the only means of protecting defense related assets from being polluted with potentially defective parts from the ever-present counterfeit market.

References

1. CFR Title 48 Chapter 2 Subchapter H Part 252 Subpart 252.2 Section 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (MAY 2014)
2. Sullivan, L. (2002) HP cracks down on counterfeit pc parts in China. Electronic business news. http://www.ebnonline.com/story/OEG20020626S0013.
3. Bastia, S. (2002). Next generation technologies to combat counterfeiting of electronic components. IEEE Transactions on Components and Packaging Technologies, 25, 175-176. http://dx.doi.org/10.1109/6144.991192
4. Pecht, M., &Tiku, S. (2006) Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, 43, 37-46. http://dx.doi.org/10.1109/MSPEC.2006.1628506
5. Rogowski, R., (2008) UK Electronics Alliance, UKEA Position on Counterfeit Electronic Components, RR/V2/03.03.2008.
6. Sullivan, L., & Graham, J. (2001). Fake parts plague industry. Electronics supply and manufacturing. http://www.my-esm.com/story/OEG20010212S0054
7. http://www.pvateplaamerica.com/semi_decapsulation.php
8. Cypress Semiconductor Application Note AN98565 – Laser Marking, Document No. 001-98565 Rev. *A http://www.cypress.com/file/202711/download
9. Griffiths, P.; de Hasseth, J.A. (18 May 2007). Fourier Transform Infrared Spectrometry (2nd ed.). Wiley-Blackwell. ISBN 0-471-19404-2.
10. https://en.wikipedia.org/wiki/Fourier_transform_infrared_spectroscopy#cite_note-Griffiths-1
11. United States Attorney's Office, (14 September 2010), "Owner and Employee of Florida-based Company Indicted inConnection With Sales of Counterfeit High Tech DevicesDestined to the U.S. Military and Other Industries – CounterfeitIntegrated Circuits Sold to U.S. Navy and Defense Contractors".

Acknowledgements
Thanks to Steven Davidson from the company in Rolling Meadows for his sharp eye and editorial comments.