

COTS and Counterfeit Semiconductors: Cause or Effect

by John O'Boyle, QP Semiconductor

April 2006



About the Author

John O'Boyle is director of business development for QP Semiconductor. He also manages strategic planning for the company's business, mission-critical, military/aerospace and high reliability industrial programs. Throughout his career, O'Boyle has held engineering, marketing, and business development positions. He holds BSEE, MSEE and MBA degrees from Santa Clara University.

The original goal of commercial-off-the-shelf parts (as it pertains to semiconductor devices) was to provide the same state-of-the-art semiconductor technology to military OEMs as was available to commercial OEMs and at prices more closely aligned with similar commercial devices. While much good has come from the basic COTS idea, a "price umbrella" has been created as older devices (both COTS and former mil-spec) become obsolete and more difficult to obtain. This article illustrates some of the unforeseen problems created by a diminishing supply of certain of these devices, and provides a look at what we consider the largest unforeseen result of the success of COTS. That is, the rapid growth in the counterfeit device market.

In the current environment of diminished supply and strong demand, there exist many unscrupulous parties who repackage or remark old commercial parts as "mil-spec", packaging and marking other parts with similar functional performance (often from a different vendor), and even remarking completely different parts and selling them as mil-spec. Obviously, the ramifications of deploying counterfeit devices into military, high-reliability applications can be severe, from hardware failure to personal injury.

Of course, this situation is not unique to the semiconductor industry, and crosses many industries and technologies. As noted on the CBS television program "60 Minutes", counterfeit watches, baby formula, clothing, shoes, medicine, sports equipment, automobile parts, commercial and military aircraft parts, and many other items are being copied. Basically, anything that can be made cheaply and sold for a profit is a target for counterfeiting. If the copied article has some brand recognition, or is in short supply and has relatively high demand, it is even more likely to fall victim to counterfeiting. Recent headline-making examples include the "pirating" of DVD movies and popular music artists' CDs. Older counterfeit products with high brand recognition include Rolex watches, Louis Vuitton women's accessories, and even Callaway "Big Bertha" golf clubs.

60 Minutes has also reported on the discovery of "unapproved parts" (specifically counterfeit aircraft parts) showing up fairly widely. Unapproved parts is the term the Federal Aviation Administration uses for components not certified as airworthy. These parts are also referred to as "bogus parts" in the industry. They range from fraudulently produced knockoffs made from inadequate or substandard alloys, to recycled pieces misrepresented to hide defects, age, or crash damage. There have been fatal commercial and military helicopter crashes attributed to the failure of such counterfeit hardware. For people with no qualms about putting the flying public at risk, it is a lucrative market.

The growing counterfeit problem has recently been observed within the military semiconductor market. It has been reported that the Defense Supply Center Columbus (DSCC) returned several lots of defective ICs to their original manufacturer (that is to the company whose logo was on the packages) for a refund. The OEM later discovered the parts were counterfeit. There was no record of how the parts came into DSCC's possession. Even the agency in charge of keeping an eye on this situation can be tricked.

COTS and Counterfeit Semiconductors: Cause or Effect

by John O'Boyle, QP Semiconductor



Figure 1: Note incorrect date code, incorrect header, and solder dewetting.

QP Semiconductor has encountered a similar situation. The company's procurement group ordered a quantity of LM710, high-speed, monolithic voltage comparators. The parts went through the normal testing procedures. When they didn't work properly, the engineering team began troubleshooting and failure analysis. The investigation revealed that the LM710s were fraudulent, and had the incorrect type of header seal. The team could clearly see solder dewetting on the leads, indicating improper manufacturing controls. These parts would have never been released from QA had the vendor been a bona fide supplier of parts to the defense industry.

The coup-de-grace was the erroneous date code marked as 1999 (Figure 1). QP Semiconductor was aware that the original vendor had stopped making the parts in 1996 and had shipped the last ones in 1997. The date code is clearly visible. Someone with a sharp eye can see the incorrect header. Opening the metal can revealed a part with a 710 marking code but the wrong version number. The correct device would have been marked 710D.

In another case, QP Semiconductor bought some Cypress Semiconductor CY7C403 devices. Having learned from the previous LM710 experience, the engineers this time became suspicious as soon as the devices were found to be faulty when first tested. A major clue was that the logo marking appeared slightly smudged. It was compared to the actual logo for the time period. The suspect logo was the proper shape, but produced quite poorly. The date code was also suspect, indicating 1998 -- after Cypress had closed the factory where the parts were made about 5 yr. earlier (Figure 2). Checking further, a semiconductor chip marked as "402" and the manufacturer logo on the die itself was "ldt" joined by a mask date of 1986 (Figure 3). This was a classic case of a counterfeit device.

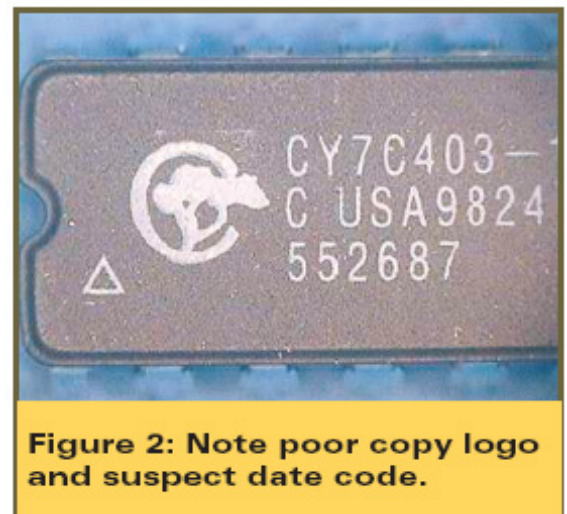


Figure 2: Note poor copy logo and suspect date code.

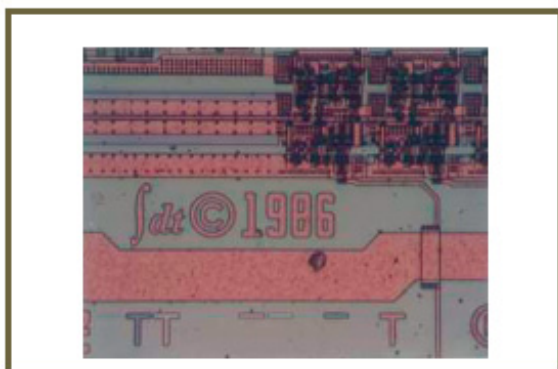


Figure 3: ldt logo inside "Cypress" labeled part.

In a final example, QP Semiconductor had been approached by a customer to develop replacement parts for an older customer custom (CC) device that was in short supply. The request was for form, fit, and function to the original device. QP Semiconductor obtained several aftermarket devices (without Certificates of Compliance) to measure them and determine how the actual device worked on the test bench.

The original parts were fairly simple LED drivers -- five drivers in a 16-pin DIP, but they didn't work. The LM710s and CY7C403s above at least worked marginally, but the LED drivers were hopeless. The package had a Signetics logo, or at least a passable imitation, and the date code indicated 1996 (Figure 4).

COTS and Counterfeit Semiconductors: Cause or Effect

by John O'Boyle, QP Semiconductor

Page 3 of 4



Figure 4: Correct (left) and counterfeit (right). Note logos.

However, Signetics no longer existed in 1996, the company having been sold to Philips. Both images in **Figure 4** show the part in question and the part number CC1368F can be seen. The image on the right is the counterfeit part with the poor quality Signetics logo. The image on the left is the real part with the correct Philips logo. The code “C7C9746F” is the military date code, in which the first C

indicates the device test location, the 7 is the last digit of the year of manufacture, the next letter is the quarter in which fabrication was completed (or started, manufacturer’s discretion), the package assembly year and week, and the letter indicates the inspection code. The fake part was made in quarter F, the sixth quarter of the year, another sign this was a fake.

When the cover of the suspect device was removed, an incredibly complex chip with several thousand transistors appeared, probably fabricated in a 0.65 μm process, and an “ST” trademark showed a mask date of 1989 (**Figure 5**). Some genuine devices from the customer were obtained and found to be fabricated in a much older process (3 μm) and comprising only a few hundred transistors, which is what would be expected of this type of device.

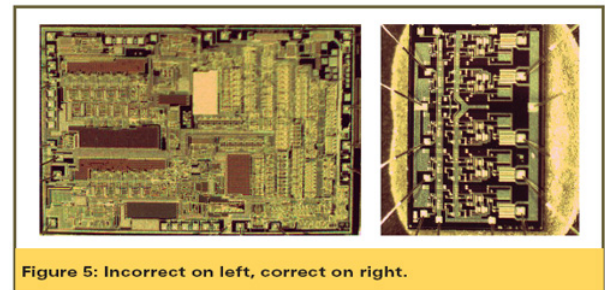


Figure 5: Incorrect on left, correct on right.

When attempting to locate obsolete devices it is (or was until recently) natural to assume that the parts are genuine. But since the profit margin for counterfeit devices or outright fakes is so large, people will continue to imitate and sell them. As long as there is a ready demand from customers, there will continue to be a supply. To make it more difficult for counterfeiters, insist upon valid Certificates of Compliance (C of C) that go back to the original military manufacturer. People are too willing to accept an interim C of C and that helps no one but the counterfeiter. Make sure the suppliers are reputable as well. In one case, a company had a valid C of C for 100 genuine parts which it received and resold. This one valid C of C was then used for numerous subsequent lots of 100 pieces (all counterfeit) which were resold as valid, a practice called French Laundering. Be alert for this trick as well.

Some in the mil-spec industry have recommended strengthening the rules and making tougher specifications. This is not necessary. The rules and practices in place are already sufficiently solid. It is just that companies buying obsolete semiconductors should not circumvent these practices. Besides, making the specifications more stringent will only further entice the counterfeiters. If the rules are tougher, legitimate companies will have higher compliance costs that will raise prices to the OEMs and also raise the “price umbrella” for the counterfeiters, encouraging them even further.

By comparison, the FAA requires a “Yellow Tag” on all parts used in the repair of aircraft. These tags verify that the part is genuine, manufactured in compliance with all the appropriate specifications and in compliance with the aircraft specifications. Yes, yellow tags can be counterfeited, but they still provide a trail back to the counterfeiter and allow investigation and eventually prosecution. They raise the bar higher, since someone actually making the counterfeit part must also forge the yellow tag.

Should semiconductor devices be certified with a similar system, perhaps green tags instead of yellow? Or is the present Certificate of Compliance enough of a safeguard? Right now, Certificates of Compliance are the best means of providing an “evidence trail” of authenticity. They should be adopted more strenuously across the industry to provide a stronger deterrent to counterfeiting.



COTS and Counterfeit Semiconductors: Cause or Effect

by John O'Boyle, QP Semiconductor

Page 4 of 4

NOTES:

For more detailed information on Products and Manufacturing Services,

visit our website at www.QPSEMI.com

QP Semiconductor, Inc.

2945 Oakmead Village Court

Santa Clara, CA 95051

Telephone: (408) 737-0992

Fax: (408) 736-8708

