No procurement officer sets out to buy counterfeit, re-marked or substandard parts, but the choices they make can leave them – and the entire supply chain – vulnerable.
—Ed Smith

opinion

Breaking the Counterfeit Code of Silence

By ED SMITH, *President, Avnet Electronics Marketing Americas*

One counterfeit electronic component is discovered every 15 seconds, according to estimates by market intelligence firm IHS iSuppli, which recently revealed that the number of reported counterfeit electronic component parts reached record levels in 2011. At first glance, this appears to be pretty bleak news for the electronics supply chain. But I have a bit of a different perspective on this. In fact, I think this might actually be a good sign.

No, I am not suffering from jet lag. Let me explain. The key phrase in the iSuppli announcement is: "the number of reported counterfeit electronic component parts." I believe that for many years now, our industry has in some way unwittingly propagated this scourge by keeping it veiled in secrecy and shame. The stigma of being associated with counterfeit product kept good people from speaking up. Suppliers never want to publicize the fact that their parts have been compromised, and OEMs don't want to admit that they have been duped by a gray-market dealer. So, the nasty business is swept under the proverbial rug, and the criminals who made and distributed the parts are free to continue along their malevolent way.

I would like to believe that the iSuppli report is an indication that members of the electronics supply chain are finally coming to the realization that we cannot possibly win this battle, unless those that have been victimized speak up. I think the recognition that today's counterfeiters can be extremely sophisticated, and often very cunning, makes it somewhat easier to admit. Falling prey to these offenders isn't like getting burned by a con man selling cut-rate components from the back of a truck. Today, counterfeiters will go so far as to set up entire shadow companies. In 2004, for example, NEC discovered that counterfeiters had set up a parallel NEC brand.

They carried NEC business cards, signed production and supply orders, and shipped product in official-looking boxes labeled NEC. Though most of the bogus NEC product consisted of finished goods, it is easy to see how one could be fooled into thinking they were dealing directly with actual NEC representatives.

Recognizing Risk

I sincerely doubt that any OEM procurement officer sets out to buy counterfeit, re-marked or substandard parts, but the choices they make can leave them — and the entire supply chain — vulnerable. For years, distributors such as Avnet have contended that buyers who source from anyone other than a direct manufacturer or franchised distributor are putting their supply chain at risk. Many buyers disregarded this assertion by rationalizing that our motivation was to reduce competition from independent sources. That was never the case, and now a study by the U.S. Department of Defense (DoD) has confirmed our suspicions with hard numbers. According to the May 2012 report by the Senate Armed Services Committee titled, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," an "overwhelming majority" of the more than one million counterfeit parts identified in an investigation of the DoD's supply chain were sourced from independent electronic parts distributors.

Top 5 most commonly counterfeited semiconductor types:

- Analog integrated circuits
- Microprocessors
- Memory integrated circuits
- Programmable logic devices
- Transistors

Source: IHS 2012 Parts Management Report

There is a high probability that most of those independent distributors had no idea the product they were selling was illegitimate. Therein lies the unavoidable Achilles' heel of unauthorized distribution channels. They simply do not know where their product comes from. Without a verifiable paper trail, there is no way to confirm that parts have not been tampered with, repackaged or outright faked. Nor can the seller ensure that, along the way, all intermediary sources stored and handled the components in accordance with the original manufacturer's quality guidelines, which also puts the parts at risk for potential failure.

As a result of the DoD's findings, the FY12 National Defense Authorization Act included a stipulation that electronic components currently in production must be sourced directly from the manufacturer or from their authorized distributors. This is a positive step, but it fails to address the primary motivation for sourcing outside

authorized channel — demand for obsolete or hard-to-find components.

Making the Tough Choice

In another report, IHS iSuppli revealed that 57 percent of reported incidents of counterfeit parts involved obsolete or end-of-life (EOL) parts. You can imagine the desperation buyers must feel when they learn that a key component is no longer available. Suddenly, the weight of keeping millions of dollars worth of production lines moving sits squarely on their shoulders. It's easy to see how due diligence and supplier vetting could fall by the wayside, as getting product becomes the overriding concern.

If these buyers had been thinking clearly, however, they would have realized that any factory-original parts that are in the supply pipeline are flowing through either authorized distributors or certified aftermarket manufacturers, not the gray market. My advice to buyers in this situation is to remember that they don't just need parts; they need quality, reliable, factory-original parts. There is a difference.

← *Play Video: Gerry Fay interviews Ed Smith on keeping counterfeits out of the electronics supply chain.*

Options, Options, Options

At Avnet, our goal is to ensure that our customers can always satisfy their bill of materials (BOM) requirements without risking the integrity of their supply chain. This starts with state-of-the-art inventory and product life-cycle management. Avnet maintains a team of analysts whose sole purpose is to stay in tune with the pulse of the market and communicate regularly with suppliers about component transitions.

For customers in markets such as military or medical with product lifetimes that are dramatically longer than typical component life cycles, we can execute end-of-life

bridge buys to ensure an ongoing supply, and we can provide a variety of financial and logistical solutions to store forecast product. Avnet also works with suppliers to develop product-continuity programs in which we will coordinate the manufacture and supply of the components for longer periods of time.

Our established relationships with certified and reputable aftermarket component remanufacturing companies enable us to steer customers to dependable sources of aftermarket parts using original OEM dies. In addition, our top-notch technical support team can help identify alternative parts that can be retrofitted for the existing design, or facilitate a complete board redesign. This can be an expensive proposition and is certainly not an ideal solution, but from a total cost standpoint, it's still better than dealing with the liability of using counterfeit parts.

Avnet has also developed a sophisticated parts-return process to ensure that customers do not unwittingly return product to us that they have sourced from an unauthorized supplier.

Facing Reality

As an industry, we are definitely making strides in the fight against intellectual property theft and counterfeiting, but we must remember the saying: "The devil wears many masks." The NEC example I cited earlier should be a cautionary tale for our industry. Buyers today must constantly be on alert, especially when sourcing in regions that do not have the same rigid intellectual property protections and enforcement that we take for granted in the United States.

If a new sales rep approaches you, check him or her out first. Consult the manufacturer's website to see where the rep's sales office is located. If the new rep's site is not listed, follow up with the manufacturer. Use your common sense and follow your gut. If a deal seems too good to be true, it probably is. We often get a feeling that something is not right, but don't follow it because we have no proof or we are in too much of a hurry and, maybe sometimes, because it is easier to turn a blind eye than to take responsibility.

Any buyer who is honestly committed to maintaining the integrity of the electronics supply chain will take the time to scrutinize an unknown source. Today the stakes are too high to leave to chance. This is not just an economic issue; counterfeit product can put personal safety and national security at risk. Admitting there is a problem is definitely a step in the right direction, but, as an industry, we still have a long way to go to cleanse the supply chain, and much of the onus for this falls on buyers. The simple fact is that — like any business — a counterfeiter's existence is directly tied to the demand for its product. As long as there is a market for these bogus parts, counterfeit networks will continue to thrive. ■

Buyers must maintain discipline in their procurement. A lack of due diligence can put buyers in the cross hairs of negligent and unscrupulous dealers.
— Bryan Brady

opinion

The Enemy Within

New Laws Wage War on Counterfeits in DoD Supply Chain

By Bryan Brady, *Vice President, Defense/Aerospace, Avnet Electronics Marketing Americas*

With the passage of the 2012 National Defense Authorization Act (NDAA), the U.S. government officially threw down the gauntlet in the nation's fight against counterfeit electronics. The legislation, which outlines processes for the detection, correction and avoidance of counterfeit electronic parts, marks the most profound shift in defense procurement policy since the Federal Acquisition Streamlining Act of 1994, which promoted the use of commercial-off-the-shelf (COTS) components in military-grade systems. Though legally the new regulations apply only to those who participate in the mil/aero supply chain, the law establishes a sourcing framework that can help anyone involved in the manufacture, procurement, sale or specification of electronic components to better combat the counterfeit menace.

For example, after several studies by the Department of Defense (DoD) and Government Accountability Office (GAO) revealed that "unvetted independent distributors are the source of the overwhelming majority of suspect parts in the defense supply chain," the NDAA specified that electronic parts that are in production or available in stock be purchased directly from the original manufacturer, authorized distributors or from trusted suppliers that obtain parts "exclusively" from the original manufacturers or their authorized dealers. For parts out of production, defense contractors and subcontractors are instructed to buy only from "trusted sources."

This is a significant policy shift for the government, which has long relied on independent distributors for

fulfillment of legacy components. The hazards of this approach became clear when, over time, buyers began extending their RFQs beyond their stable of known and trusted independent distributors to sources about whom they knew little more than a Web address. This conduct fails to recognize that the unauthorized channel today is not what it used to be. There are certainly still a number of reputable independent distributors who buy and sell only factory original goods. But there is also a growing slate of parts brokers, who use the reach of the Internet to find and market goods, with little attention paid to the legitimacy of the supplier or their parts. And then there are, of course, the counterfeiters; those whose business is built entirely on selling fake, re-marked or substandard components. A lack of due diligence can put buyers in the cross hairs of these negligent and unscrupulous dealers.

Trust, But Verify

The moral of the story here is that although the Internet can be a phenomenally useful sourcing tool, buyers must maintain discipline in their procurement. This includes establishing and adhering to an approved vendor list that is regularly scrutinized. According to Section 818 of the NDAA, among the requirements these suppliers must meet are a formal, DoD-approved counterfeit-avoidance policy with rigorous inspection and testing procedures.

Visual inspection to identify component nonconformance issues has been the de facto standard in the industry for years. However, as counterfeiters employ more sophisticated equipment and advanced labeling techniques, visual inspection is becoming increasingly unreliable. More aggressive testing, such as destructive physical analysis (DPA) may include resistance to solvents, X-ray florescence analysis, real-time X-ray analysis, scanning electron microscopy and die verification. These options must, most often, be performed by an outside lab, and can be costly and time consuming.

Currently, there are also a number of new verification tools and techniques under evaluation for identification of counterfeits. These include DNA marking (Applied DNA Sciences Inc.), quantitative optical inspection (Covisus Corp.) and advanced electromagnetic scanning (Nokomis Inc.). Only time will tell, which, if any, of these approaches will prove most viable. But, it's good to know that additional detection technologies are on the radar.

Walking the Walk

At Avnet, we recognize that more stringent inspection and testing is something the entire industry should embrace. Though the fact that we buy only from the original manufacturer or other franchised distributors gives us a certain degree of

confidence in the pedigree of our product, in today's world, nothing can be taken for granted. Therefore, our materials control process includes traceability mechanisms such as bar codes and date coding to verify that we are in control of the product we have in stock. We also have a strict return policy of accepting only factory-sealed product. This ensures that we are not inadvertently taking in suspect parts through our return process. We are also auditing the materials handling and return policies of our direct manufacturers.

If an OEM, contractor or subcontractor must source from an "at-risk supplier," there are precautions they can take to minimize the chances of acquiring fake or substandard parts. SAE International, a global association of experts in the aerospace, automotive and commercial vehicle industries, recently released an update on its AS5553 Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition standard. The AS5553A guideline includes risk mitigation methods in electronic design and parts management, supplier management, procurement, part verification, material control and response strategies when suspect or confirmed counterfeit parts are discovered. Other useful SAE resources are the SAE ARP6178: Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors; and SAE AS6081: Counterfeit Electronic Parts: Avoidance Protocol, Distributors [independent/broker]. SAE is also currently collaborating with the Electronic Components Industry Association (ECIA) to create a detection-and-avoidance standard for franchised distributors.

I strongly believe that if all parties in the electronics supply chain were to abide by these few rules, we could make a significant dent in the counterfeit trade. However, avoiding counterfeit parts isn't just about from whom you source, it's also about how you source and manage parts.

Taking Control

It has been well documented that majority of counterfeit parts come from unauthorized suppliers, and generally these are sources that are brought into play when there is a need for hard-to-find or legacy parts. So, what if we could eliminate or at least minimize the need to source parts that are no longer in production.

There is no avoiding the reality that long field-life systems in mil/aero, medical and industrial markets will outlast the average chip's life cycle by years, and often decades. But, a more proactive approach to parts management can significantly reduce the need for those desperate forays into the murky waters of today's broker market.

This preemptive strategy should start in the very earliest design phase. Engineers must use the intelligence available to them to ensure that they are designing

with product offering the greatest life-cycle support. Though mil/aero engineers have the option of designing with COTS product, this does not mean that they have to. There is still a robust, billion dollar mil-certified supplier base out there, as well as other manufacturers that have committed to extended-support product lines, such as TI. Whenever possible, designers of long field-life products should pursue these avenues first.

Stacking the Deck

Life-cycle analysis should also be a priority for engineers. For mil/aero manufacturers, it is difficult enough to get through their very long design cycle without having to deal with multiple technology turns, but if they start the program with a part that is already in or close to end of life, they are stacking the deck against themselves. While many manufacturers and distributors will push product-change notices (PCN) and last-time-buy (LTB) notifications to customers, OEMs should not rely entirely on these advisories. It is also advisable for these companies themselves to take on the responsibility of tracking life-cycle information on critical components.

To help customers mitigate the risk and expense of obsolescence, Avnet maintains a team of market analysts whose sole purpose is to follow technology trends. When Avnet suspects that a component commonly used by a number of its customers may be at risk, we will notify customers so they can make informed component choices, to maximize the life expectancy of a systems' bill of materials (BOM).

Many customers today are also averting obsolescence by designing with open architecture to allow for easier part replacement and planning new technology insertion through the production and support life of the program.

If a suitable form, fit and function replacement is not possible, Avnet recommends that customers consider the services of a continuing, or after-market, semiconductor manufacturer. These companies are authorized to recreate an integrated circuit using the original manufacturer's die and/or intellectual property, ensuring the performance characteristics and specifications of the original devices, and alleviating concerns about traceability.

The bottom line: Today, members of the supply chain have more tools and information at their disposal than ever before to help them avoid counterfeit components. If, as an industry, we commit to adopting the standards and techniques available, we can minimize the need to source from higher-risk suppliers and dramatically weaken the hold the counterfeit market has on the electronics supply chain. ■