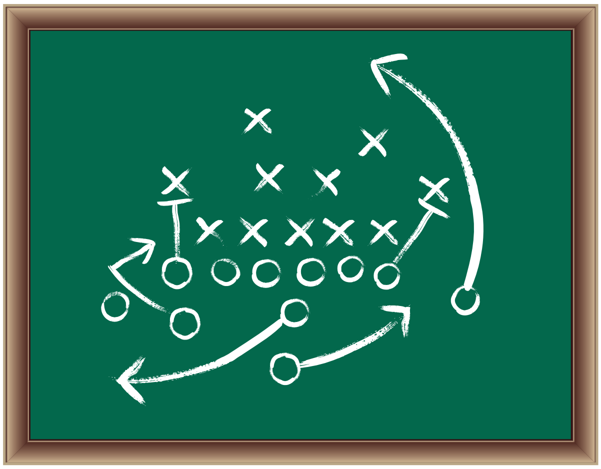
Supply Chain Best Practices for Supplier and Parts Risk Mitigation



The issue of counterfeit and inferior parts has gained C-level visibility across industries as front page articles in the *Wall Street Journal* and cover stories in business magazines have raised public awareness of the dangers that counterfeits present. Those dangers include the failure of mission-critical equipment, whether medical devices, automotive computers, or commercial or military aircraft, as well as risk to the life and health of citizens and soldiers. The dangers also threaten the brand name and public reputation of major companies that unwittingly fall prey to counterfeiters.

Counterfeit electronics in the supply chain became front page news again earlier this year when, on March 9, the Armed Services Committee of the U.S. Senate announced an investigation into counterfeit electronic parts in the Department of Defense supply chain.

In a statement by Senators Carl Levin (D-Mich.) and John McCain (R-Ariz.), chairman and ranking member of the Senate Committee on Armed Services, the two senators said:

> *Counterfeit electronic parts pose a risk to our national security, the reliability of our weapons systems and the safety of our military men and women. The proliferation of counterfeit goods also damages our economy and costs American jobs. The presence of counterfeit electronic parts in the Defense Department's supply chain is a growing problem that government and industry share a common interest in solving.*

As part of the investigation, the Armed Services Committee is even reaching out to senior executives at military contractors, calling on them to get to the bottom of these issues.

This level of scrutiny from Congress and Defense officials, along with broader cover within the mainstream business media, has raised the visibility of the counterfeits issue in corner offices and boardrooms both within and outside the DoD supply chain. The fact is that industries like medical devices and automotive rely on many of the same components or military standards as those applied to systems in the DoD supply chain. Clearly counterfeiting is not exclusive to military applications, and any company that relies on electronic components for mission-critical applications is potentially at risk of being a victim of counterfeiters.

Points of Entry

Any supply chain, regardless of industry, can have vulnerable points of entry for counterfeit parts, both intended and unintended. The Internet is perhaps the most obvious "window of vulnerability" for most companies. It's not uncommon for engineers or buyers in need of a part that is out of inventory and/or that has been obsoleted or end-of-lifed to "go maverick" – that is, go outside a company's "official" purchasing channel – and turn to the Internet.

Of course, legitimate brokers and authorized distributors may operate Web sites that can provide reliable sources. But just Googling a part number can turn up any number of unsafe supplier sources. Online broker search engines may offer access to OEMs or distributors but also to sources that are less-reliable – or completely unreliable. Many of these sites have minimal requirements for seller registration before granting access to a large audience of buyers. And counterfeiters are increasingly Web-savvy and have been known to set up their own Internet sites that go to extraordinary lengths to appear as legitimate enterprises.

Ironically, companies can unintentionally create incentives for counterfeiters while following what would appear to be normal due diligence. A well-intentioned buyer needing to source a part might surf several search engines and identify multiple sources for the part. The buyer sends out requests for quote to some or all of the sources, not knowing that all the stock listed across the different Web sites actually comes from one supplier. That supplier might have had the part in question sitting untouched in inventory for months, and then a rush of queries appears from different brokers and distributors. Suddenly this part looks like the hottest commodity in town, driving the price up and creating an incentive for counterfeiters to start producing that part.

Counterfeiters also are becoming more aggressive in how they leverage the Internet to cash in on demand – even for parts that don't exist. Mark Snider, the head of ERAI, a 16-year-old information services organization that provides tools to mitigate risk from counterfeit and substandard parts, tells the story of an ERAI member that posted their 10-digit phone number on one of the online search engines as a part number. The next day, they received more than a dozen responses offering stock on the phantom part from different manufacturers, with different date codes and in different quantities. Troublingly, several U.S.-based sources provided quotes on the "part," in addition to overseas sources.

The counterfeits challenge is only exacerbated by events like the tragedy in Japan in the wake of the earthquake and tsunami that ravaged that nation. The human toll has been terrible, and the country continues to struggle with recovery. These events have challenged the electronics supply chain, too, because of the central role that Japan plays in the production of a significant number of electronic components. Dale Ford, senior vice president for market intelligence at IHS iSuppli and a longtime observer of the industry, has described the disaster as "the broadest and deepest impact that the electronic supply chain has ever experienced in its history." Unfortunately, counterfeiters are all too willing to take advantage when this kind of disaster creates supply shortages or price spikes (see accompanying sidebar "Aftershocks in the Supply Chain" for more on the impacts of the Japan crisis on the supply of critical components).

Aftershocks in the Supply Chain

"There have been natural disasters that have had significant impact on the supply chain, including earthquakes in Taiwan, Kobe [Japan] and Silicon Valley," says Dale Ford, senior vice president for market intelligence at IHS iSuppli, the electronics industry watcher. "But with this latest disaster in Japan, more points across the supply chain have been impacted than in any of those previous disasters."

A wide range of materials and components have been affected, Ford notes, from semiconductors to batteries, from passive components to flat-panel displays. IHS, for example, provides forecasts for the supply health of key commodity components widely used in the electronics supply chain, looking at supply, pricing and lead times, for both passive and active components. IHS' forecast for memory components like DRAM or NAND Flash shows demand moderately outstripping supply for most of the remainder of 2011, and while lead times are likely to remain in the reasonable range, pricing pressure for these components will be strongly upward.

However, a look across other components and materials reveals points in the supply chain that should concern the supply chain. In the analogue area, for example, with components such as the general purpose amplifiers, comparators and voltage regulators, supply has struggled to keep up with demand even before the disaster, and these components presented a serious challenge to procurement departments throughout the past year. The Japan crisis has had the effect of ensuring that the markets for these components will see no relief throughout this year, with extended lead times and continued upward price pressure. The impact has been even more serious in several on several of the discrete components, such as IGBTs (insulated-gate bipolar transistors) or tantalum capacitors, for example.

One lesson of the events in Japan and their aftermath, Ford says, is that companies need to pay very close attention to areas where there's a concentrated supply of key electronics components used in the supply chain. "Right now we're going through the crisis with Japan and the key role that they play in many different components and materials, but there are other areas especially in Asia-Pacific where supply is concentrated," Ford says. For example, South Korea is a key memory supplier, and a key TV and flat panel supplier. Taiwan plays a role as well in LCD panels and as a manufacturer of semiconductors. Production of mobile PCs is heavily concentrated in the Shanghai area, and mobile handsets have a strong concentration in the Shenzhen area.

"We lived through another significant crisis in 2001 with the collapse of the semiconductor industry, and we learned important lessons in how to manage inventory that actually helped mitigate some of the challenges we went through with the financial crisis of 2008/2009," Ford says. "We once again will learn from [the Japan crisis] what steps we need to take to minimize our exposure to national disasters or other impacts on the supply chain. Companies are going to start looking very carefully at how they second source and where the sources of those products come from as we move forward."

5 Questions about COUNTERFEITS

Counterfeiting continues to proliferate, in part, because individual buyers and companies as a whole can be reluctant to tackle uncomfortable questions involving the buying process for electronic components. Questions like :

Are all open market sources the same?

Unequivocally, no. Without a doubt, many reliable and trustworthy independent distributors are out on the market, with solid anti-counterfeit processes in place and ready to serve their customers very well. But there are also plenty of problematic suppliers out there. Let's face it: the open market is a risky place to do business. It all goes back to having a proper vetting process in place. You need to know who your distributors are and not just rely on the Internet.

Does real stock versus available stock matter?

Yes, it absolutely does. Because if you're looking at real inventory, you're helping to remove yourself at least one step away from a counterfeiter. The fly-by-night counterfeiters don't typically carry stock of anything; they make parts to meet an incoming order. When you find distributors that have in-stock inventory, you're on safer ground.

Will a blanket policy preventing open market sourcing eliminate risk?

It will eliminate some risk, but it won't eliminate all of it. The only way to fully eliminate counterfeit parts from coming into your supply chain is to buy every single part directly from the factory. Anything outside of that could, potentially, problematic. Even authorized franchise distributors may go out to the open market to fulfill your orders – some may not want to admit to it, while in some cases they're open and honest about it. So you should go to authorized franchise sources whenever you possibly can, and it is certainly going to reduce your risk, but it's not going to completely eliminate it. You still need to follow your quality procedures and processes.

Do vetted open market suppliers require less testing?

The frank answer is, "no." Good, vetted independents can to a great job serving your needs with quality parts. But the best practice here is clear: Do not deviate from your quality procedures. It's still the open market, and you need to be very explicit about what your testing requirements are. You should document whether you're doing the testing or the supplier is doing it. Again, don't deviate from your quality process.

And, lastly, is buying only from authorized distributor practical or technically feasible?

Not always, no. It's not realistic. The truth is, anybody that's been in this market for any amount of time knows that the market has peaks and valleys that are going to make authorized distribution a more or less realistic option. The current environment, with a rebounding economy and constraints on supply – even before the earthquake and tsunami in Japan put capacity offline for many parts and materials – means that there already has been an increase in activity in the open market. Again, it goes back to vetting and finding good, known, trusted sources of supply, staying within your trusted supply chain to the extent possible, and assiduously following your quality processes.

Supply Chain Best Practices to Avoid Risk

Snider says that the best practice to avoid risk is to stay within your trusted supply chain. "Go to your normal, known, trusted source of supply, that's the road you need to travel," he says. The only way to completely eliminate any possibility of counterfeiting, of course, would be to buy every single part directly from the factory. "When you go beyond that, you're exposing yourself to at least some element of risk at every stage," Snider says.

But buying direct from the factory is not always a practical option, particularly where obsolete/end-of-life parts are concerned. The next step outside the factory walls, then, is buying through an approved vendor or manufacturer, followed by other franchised and authorized sources, and only then the open market. This latter poses the greatest risk, but buyers can mitigate their risk by thoroughly vetting their suppliers. Information that buyers should seek from suppliers include:

■ **Industry Membership and Reporting –** Is the seller a member of ERAI, and do they report instances of counterfeits to ERAI and GIDEP?

■ **Quality System and Processes –** Do they have the organizational structure, procedures, processes and resources necessary for quality management?

■ **Warranty and Insurance –** Are they covered in the event of a counterfeit escape?

■ **Supplier Qualification and Purchasing Process –** Do they vet their own suppliers to ensure the tier-twos and –threes are legitimate and have controls in place? What efforts have they made to verify a parts' authenticity before use?

■ Non-conforming Material Control – Do they check incoming product to ensure it's authentic before they pass it on to you? What do they do with non-conforming parts?

Predictive Obsolescence – A Useful Tool in the Fight against Counterfeits

Obsolescence is a fact of life in the electronics supply chain, but it also is a contributor to the risk of counterfeit and substandard parts. Discontinued parts can cost over 2,000 percent of the original price and can lead buyers to the gray market where counterfeits thrive. Moreover, out in the gray market, discarded used electronic equipment is being broken down and the individual parts removed. These parts can be put back in to the supply chain as new. And buying from non-approved sources can add unforeseen expense and time thanks to the additional requirements to verify the authenticity of a part.

Predictive obsolescence can reduce the chances of getting into these high-risk situations. Predictive obsolescence refers to the steps taken to mitigate the effects of obsolescence by applying predictive forecasters to component selection decisions. These predictive forecasters can help you avoid getting into a position where a lack of options forces you to go outside the normal, trusted supply chain, and it also helps with the management of end item lifecycles and your component lifecycles.

At its root, predictive obsolescence involves applying objectively derived information to assist with making informed decisions. The forecasters are a lifecycle code and years to end of life, also known as YTEOL. The predictive forecasters are similar to the insurance industry mortality tables that look at the life expectancy of a person as determined by factors such as diet, exercise, lifestyle and so on. The same principle can be applied to parts. As parts are introduced into the marketplace, component engineers look at several factors and assign the part a lifecycle. These factors can include, but are not limited to, parts technology family and various part attributes.

The lifecycle is broken into stages that are also represented by numeric values, typically one through five, based on the Electronic Industries Alliance EIA-724 standard (Product Life Cycle Data Model), which defines a product lifecycle curve model for use by the electronics industry to standardize the terms and definitions used to describe the lifecycle status of a product. The lifecycle itself does not indicate how long a part is expected to be available, it just indicates where the part is within its given lifecycle. Each lifecycle stage provides information that's useful when making a determination to select a part.

Lifecycle code one is "introduction," which tells us that the part is new technology, there's typically little sales information available on the part, the part will have a high price as the manufacturer is still recouping its R&D costs, and the part has little profit right now for the manufacturer. Lifecycle stage one parts can have a high mortality rate and may not make it into the next lifecycle stage. Lifecycle code two is "growth." Now that the part has increasing sales, the cost is coming down, demand and profit are growing for the parts, and the part is picking up additional manufacturing sources. Lifecycle code three is where demand and price for the part has now stabilized, the part typically has the most manufacturers and is producing the most profit.

Lifecycle code four is decline and phase out. Here we start to see sales and prices are dropping, and the part is losing manufacturing sources as end-of-life notices (EOLs) are being announced. At lifecycle code five, manufacturers have stopped production, the part may be only available now in the aftermarket, and it probably carries a high price and is more susceptible to counterfeiting.

The other predictive forecaster is the years to end of life, or YTEOL. The YTEOL is the number of years that a part is expected to be available before it becomes discontinued. Marketplace and technology factors are used to determine the part's expected availability, along with other factors such as the number and type of a manufacturer, OEM versus aftermarket, and sales data. Real-world factors can also be applied, including changes in the global availability of raw materials or manufacturing disruptions, such as the recent earthquake and tsunami in Japan.

A YTEOL report lists end item parts and their expected availability status broken out into groups of years. With this kind of a report using the forecasters, it becomes easier to see that if a given end item requirement has a lifecycle mismatch with any of its component parts. With this kind of report in hand, informed decisions can be made upfront to start building up potential inventory, finding alternates for these parts or planning for a redesign in preparation for the expected availability issues. The report also provides a good indication of when it is time to end-of-life an end item.

The critical step in incorporating predictive obsolescence into your processes is to work with your internal or external sources to make sure you have accurate, complete and up-to-date part lists. It's very critical that this information be available. If you don't own the part lists, then you need to make sure you have a mechanism in place to assure you can access them. You may need to create contracts to get the data, so additional funding might be required in your product planning. And of course you'll need an electronic component database that provides predictive forecasters, as well as a parts management software tool that's designed for predictive obsolescence and that includes workflows with the specialized analysis functionality and reports.

New Tool to Combat Counterfeit Electronic Parts

While manufacturers in a number of industries struggle with counterfeit parts, members of the aerospace and defense industry have their own unique challenges. Unlike a cell phone, which will probably be obsolete in three years, many of the products built by aerospace and defense companies have long life spans. Therefore, the need for replacement parts is much higher, and many times they're no longer available from the manufacturer of the original part. That's when procurement managers turn to brokers—and run the risk of buying counterfeit parts.

Brokers are a significant source of counterfeits—one study by the U.S. Department of Commerce shows brokers as being the largest source by far of counterfeit parts in which it was documented that they were being sold. In the past, the standard advice to avoid counterfeits was "know your supplier." But as the number of counterfeits grows to alarming levels, that's only one of many practices companies need to adopt according to SAE International, which recently released its standard AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. The standard outlines recommended practices and procedures designed to help companies reduce the chances of receiving or using counterfeit electronic components. These range from processes for determining the availability of parts and assessing potential suppliers to processes for verifying components and controlling suspect and confirmed counterfeit parts.

According to Bruce Mahone, director of Washington operations, aerospace, for SAE International, the organization's new counterfeit electronic parts standard was created at the behest of NASA, which was concerned about the rising number of counterfeit electronic parts in the supply chain.

"Not only is it difficult to get parts from the original manufacturer for older aircraft and space systems, but the counterfeit business, especially coming from Asia, is very strong," says Mahone.

Counterfeit electronic components can range from parts that are clearly fakes to those that are hard to distinguish from the real item. Types of counterfeits include parts that have been remarked, components that were salvaged from old assemblies and defective parts that should have been destroyed by the original manufacturer. Or they are parts that are sold as new, but are really refurbished, with much more limited life spans than the new components they claim to be.

AS5553 was designed to combat the influx of these types of these problem parts. Even though it was created for the aerospace and defense industry, it can be adopted by any company that is dealing with counterfeit electronic parts in its operations.

However, given the standard's stringent requirements, it may not be as practical for industries such as consumer electronics, where turnaround times are vital, unlike aerospace and defense, where the focus is on developing mission- and life-critical aircraft and spacecraft.

"Counterfeits are a concern for all electronics, but it's just a more critical, dangerous and expensive concern in aerospace," says Mahone.

Now that the counterfeit electronics standard has been published, SAE is beginning work on a companion standard that will focus on alleviating similar problems with counterfeit mechanical parts such as fasteners and fluid fittings.

The new standard will be comparable to AS5553, says Mahone. "It will be similar in a lot of ways. And the paperwork part would be similar. But the testing would be different and you'd be dealing with different types of companies. I think different people would have the expertise to not only manufacture but also try to counterfeit mechanical parts."

While work on the mechanical parts standard is in the early discussion phase, the counterfeit electronic components standard is already in use.

"It has broad support from NASA, the Federal Aviation Administration, the Department of Defense," Mahone says. "We expect it to be widely used globally and we expect it to be the global standard for avoiding counterfeit electronic parts."

In addition to the above question, it is important to verify that the stock you might be looking at on a Web site or search engine is "real stock," not "available stock." Real stock is sitting in the supplier's warehouse, ready to be shipped next day, if necessary. Versus "available stock," which could either be sitting outside that supplier's control at a vendor overseas, or might not be real at all – it could just be the bait that an unscrupulous supplier uses to attract a buyer before actually going out into the open market to source from third-parties.

Even after a supplier has answered all your concerns and you have verified that the part you are seeking is in stock, ensure that you contractually define your expectations and test accordingly. "You just can't imagine how often we see cases where, if people had just put their expectations in the purchase and sale agreement for a part, they wouldn't have any trouble," says Snider. "But a lot of people just don't do a good job with this, and it can become problematic."

And, finally, don't deviate from your testing procedures. "Trust, but verify," Snider advises. "Parts that do not have traceability need to be tested all the way to burn-in. And if you have not done that, then you have not eliminated the risk to the best of your ability." Taking a part through an intensive testing process is time-consuming and costly, he acknowledges. “But you have to think of the cost of not going through this kind of testing all the way through burn-in and then having something happen. It could have catastrophic consequences.”

It also is a best practice to preemptively check needed parts against a database of known “at risk” components, or to scrub entire bills of material through a database for the same purpose. ERAI, for example, offers a Part Search Database that buyers or engineers can use to vet out parts that they are seeking. The company offers the ERAI Material Scrubber as well, which allows a manufacturer to upload a BOM that is then scrubbed against a database of known “at risk” parts. Snider says that typically from 0.5 percent to 3 percent of a given BOM’s parts will turn up on the list, alerting the manufacturer to take particular care when sourcing out those parts. And finally, ERAI’s Parthunter service allows ERAI members to post their inventory in the company’s searchable database, with the requirement to update the in stock inventory every 48 hours so that buyers have visibility to actual inventory on hand.

Conclusion

The threat of counterfeit parts is only increasing, despite the efforts of government and industry to stamp out the problem. In the absence of a “quick fix” to the counterfeits challenge, it falls to each manufacturer and supplier to implement tools and processes like those described above to mitigate the risk of substandard or fake parts from entering the supply chain.

For his part, Snider casts the fight against counterfeit parts in stark terms. “It’s an ongoing battle of good versus evil,” he says, “a battle to stay one step ahead of the counterfeiters. And I can assure you that it is an ongoing battle.” ■

Electronics Industry Tackles Counterfeit Parts Issue

One of the groups hardest hit by counterfeit parts is the electronics industry. Dave Torp, vice president of standards and technology for IPC, which represents 2,700 member companies in the electronic interconnect industry, including original equipment manufacturers (OEMs), electronic manufacturing services (EMS) providers and component suppliers, says his organization has seen a significant increase in counterfeit parts activity. He believes the frequency of counterfeits in the supply chain is at least eight times greater than what it was five years ago.

“As the supply chain has moved from other parts of the world into the Asia-Pacific theater over the last 10 years, counterfeiting has become more prevalent, and it’s not just complex components that are being upgraded through their markings. Now we’re seeing counterfeiting of lower-level components, such as chip resistors and chip capacitors,” says Torp.

Much of the growth of counterfeit parts can be attributed to the second-hand or gray market, through which manufacturers can buy parts they can’t source directly from the supplier or an authorized dealer. As Torp puts it, these types of transactions “cloud” the supply chain.

“If an EMS loses a contract with a major OEM, it’ll sell that inventory to a broker,” Torp explains. “A broker buys it for a certain price, and then another EMS that is looking for certain components will buy them up. When that happens it starts to get hard to trace the components.”

Because brokers typically offer their products at a steep discount and operate on thin margins, they don’t question when they get an opportunity to buy cut-rate parts. Brokers are therefore an ideal entry point for counterfeiters looking to get their products into the supply chain.

Given the risks manufacturers face when buying through the gray market, why do they even do it? According to Torp, it all comes down to the pressure to deliver.

■ “The longer that you have inventory sitting on the shelf not going anywhere, the more money you lose. Let’s say you don’t have enough components to do your complete build. You’re holding onto inventory and that inventory is costing you money. It links directly to the bottom line, and the longer you have to put off a customer on a delivery, the more likely it is that the customer is going to cancel that order on you. So manufacturers are doing everything in their power to get those components in house, get those assemblies built and get them to their end customer as quickly as possible,” Torp says.

■ Manufacturers also look to the gray market for help when they need replacement parts for their products and can no longer source them from the original supplier. That’s why industry experts recommend working with the original supplier as much as possible by keeping a sufficient number of replacement parts in inventory or by checking to see if there’s an alternative source of authentic parts.

■ Of course, tackling the problem of counterfeit parts goes far beyond simply working with known entities.

■ “Until recently, the advice was to know your supplier. But we’re trying to dig a little deeper to identify how you determine if a component is or is not genuine, and then what you do after you’ve determined that it is a counterfeit component,” Torp says. “IPC has been actively engaging members and the industry with programs such as seminars and forums on key concerns like the legal issues associated with counterfeits. We’re also building direct programs that help our members understand how to prevent and detect suspected counterfeits, as well as answering the question of what to do if you encounter one.”