Special Edition/July-August 2011

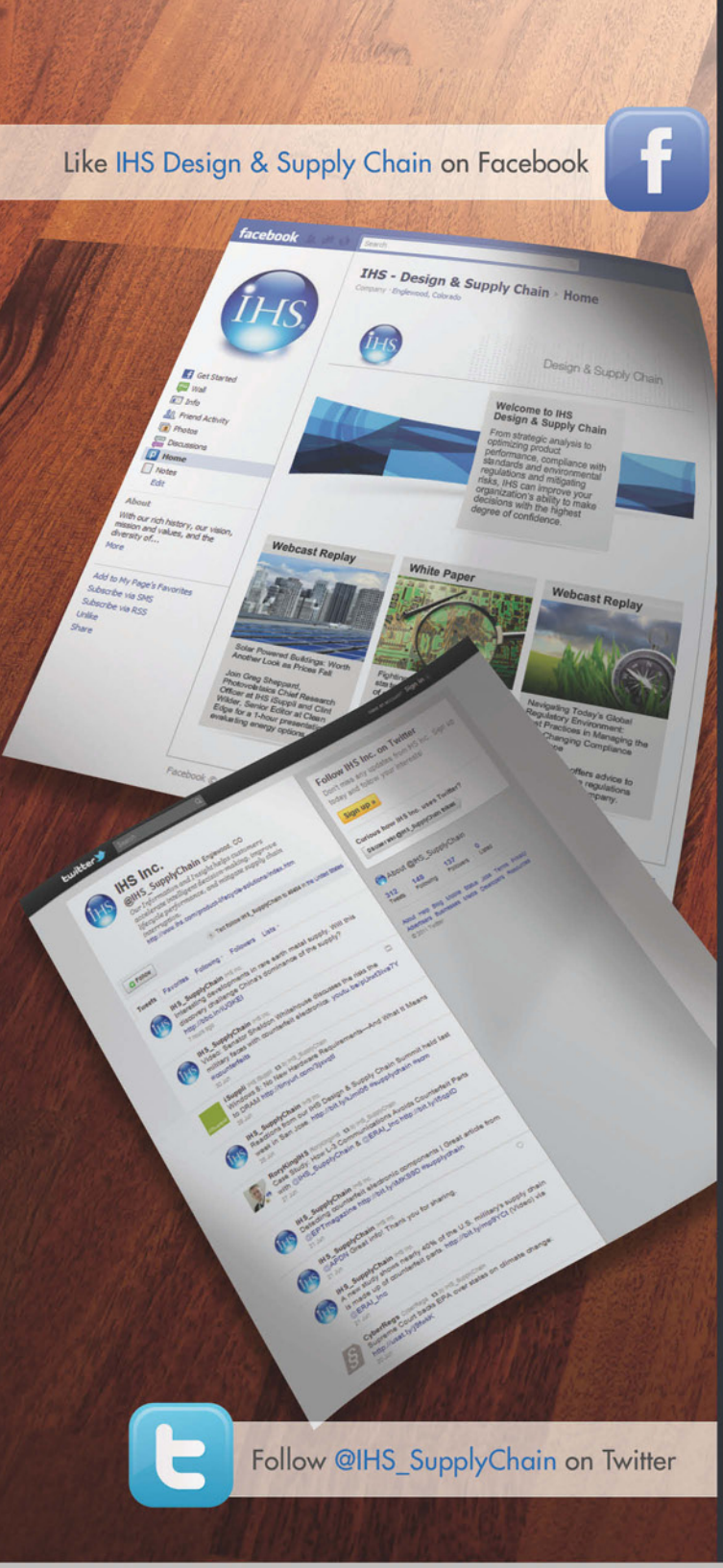
Supply & Demand Chain Executive©

Solutions-based Intelligence for Supply Chain ROI

The COUNTERFEIT Crisis

Critical strategies to meet the growing challenge

CYGNUS BUSINESS MEDIA



Billions of impressions are having an impact on the way business is done today. **IHS Design & Supply Chain** experts, partners, and customers are making their impressions known by joining the conversation. Online, interactive, and engaged. Social media is advancing the conversation.

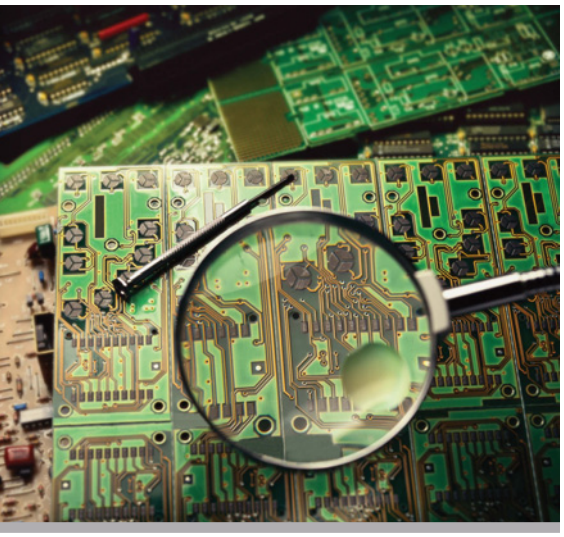
Are you?

Join the Social Conversation. Engage with IHS Design & Supply Chain

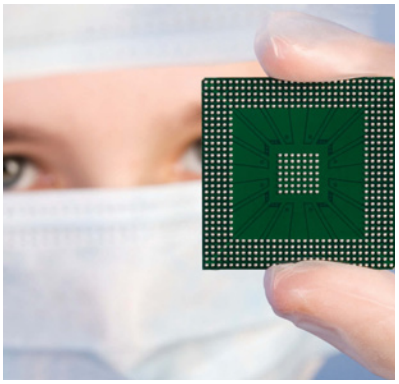
IHS is a global information company with world-class experts in the pivotal areas shaping today's business landscape: energy, economics, geopolitical risk, sustainability and supply chain management. From strategic analysis such as market forecasts and technology roadmaps to optimizing product performance, compliance with standards and regulations, and supply chain risk mitigation, **IHS Design & Supply Chain** can improve your organization's ability to make decisions with the highest degree of confidence.

IHS

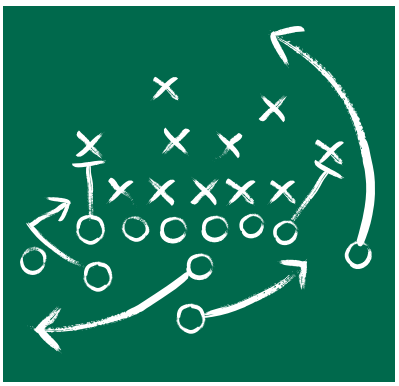
www.ihs.com



On The Cover - The Counterfeit Crisis
Supply & Demand Chain Executive hosted a discussion among a select group of electronics industry veterans with extensive professional experience on the frontlines of the battle against counterfeit and suspect electronic parts. This special edition examines The Counterfeit Crisis.



10

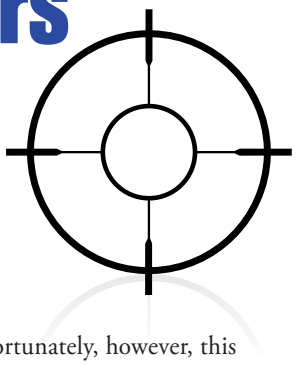


12

Features

Counterfeits in the Crosshairs

From the Editors, Supply & Demand Chain Executive



Counterfeits have come under a dramatic increase in scrutiny from Washington since a 2009 report from the U.S. Department of Commerce's Office of Technology Evaluation (OTE) blew the issue wide open, showing that counterfeit and suspect parts could impact as much as 40 percent of the Pentagon's supply chain. The study cites an Inside the Air Force article in which a Defense Department official estimated that "such components are leading to a 5 to 15 percent annual decrease in weapon systems reliability." OTE's report shows how incidents of counterfeit electronics have more than doubled, escalating over 150 percent from 2005 to 2008, based on its survey of military manufacturers, contractors and distributors.

It's widely believed that the most effective approach to avoiding counterfeit electronic components is to purchase, where possible, directly from the original component manufacturer (OCM), or from franchised or authorized distributors, resellers or aftermarket suppliers. Thus, the OTE focused attention on the critical role of procurement practices in the introduction of counterfeits into the supply chain, concluding that, "It is not uncommon ... for authorized distributors to purchase parts outside of the OCM supply chain in order to fulfill customer requirements – 58 percent purchase parts from other sources," according to the report. "Specifically, 47 percent of authorized distributors procure parts from independent distributors, 29 percent procure from brokers, and 27 percent procure from Internet-exclusive sources." Clearly, when almost half of authorized distributors procure parts from purportedly less-safe independent distributors and brokers, a policy to procure only from these distributors is only one small part of overall anti-counterfeit risk mitigation strategies.

In response, Congress has started to ratchet up pressure on government suppliers in an effort to drive counterfeits out of the military. In March, Sen. Carl Levin, (D-MI) joined with Sen. John McCain (R-AZ) to announce a Senate Armed Services Committee (SASC) investigation into counterfeit electronic parts in the DoD supply chain. The senators warned that counterfeit electronic parts pose a risk to the nation's security, the reliability of its weapons systems and the safety of its military men and women.

The SASC reportedly sent out letters to the executive leadership team at major government prime contractors asking them to provide information on any counterfeit parts they had identified that were destined for the DoD supply chain, including the part number and supplier, as well as companies that had tested those parts.

In June, Sen. Sheldon Whitehouse (D-RI) introduced bipartisan legislation to crack down on criminals trafficking in counterfeit goods in the military supply chain. The "Combating Military Counterfeits Act of 2011" – cosponsored by Senators McCain, Lindsey Graham (R-SC) and Chris Coons (D-DE) – aims to turn up the heat on counterfeiters by increasing penalties for trafficking in fake military products. "No one who has visited with our military ... can accept criminals making an easy buck selling fake versions of products intended to help our troops. Unfortunately, however, this unacceptable threat to troop safety and national security is growing," Whitehouse said.

Counterfeits have taken center stage as a mainstream business issue, focused squarely on the supply chain. The enormity of attention paid to the threat of fakes in military equipment is just the beginning, and has raised the counterfeits issue to the C-suites of recognized global companies. Senior management is looking at their companies' potential risk exposure due to counterfeits – in terms of lost sales, liability and brand damage – and beginning to sponsor corporate-wide initiatives to deal with counterfeits.

The question for many supply chain executives has become, therefore, not whether, but how to deal with counterfeits. The articles in this special edition illustrate that OEMs and their suppliers have an increasing number of tools and best practices that they can turn to as part of dedicated initiatives aimed at reducing the risks associated with counterfeits. "Fighting the Fakes" starting on page 18 shows how L-3 Communications has done that by institutionalizing award-winning business processes to thwart risks from obsolete and counterfeit components. Leveraging resources from the likes of ERAI Inc., IHS Inc., SAE International and others, companies can help ensure that they keep counterfeits – not their own corporate brands – in the crosshairs. ■

BEST-IN-CLASS Component Risk Mitigation Practices to Avert Procuring Counterfeits

An electronics industry perspective of the challenges of mitigating counterfeit parts risk

By Editorial Staff

Supply & Demand Chain Executive recently hosted a discussion among a select group of electronics industry veterans with extensive professional experience on the frontlines of the battle against counterfeit and suspect electronic parts. The roundtable came together at the initiative of Mark Northrup, director of advanced technical operations with IEC Electronics Corp., a contract electronics manufacturer based in Newark, N.Y. Northrup has more than 25 years of experience in the industry, has been helping lead the charge against counterfeits within IEC, and has written and presented on the topic before industry audiences. Participants included Clifton Aldridge's colleagues at Dynamic Research and Testing Laboratories (DRTL), LLC and representatives from Global IC Trading Group, a Laguna Hills, Calif.-based electronics distributor and a supplier to IEC, and IHS, a Denver-based provider of technology solutions for managing parts obsolescence and counterfeit parts risk.

Extent of the Threat

The discussion kicked off by looking at the extent of the challenge related to counterfeit and suspect parts in the electronics supply chain. Addressing the scope of the problem, Albuquerque-based Felipe Villescas, a senior component engineer with IEC Electronics, said that, in his experience, the number of incidents of counterfeits and suspect parts has been rising. "We're coming across a lot of counterfeits, and thank goodness we have a mitigation program to help keep counterfeits at bay," he commented. Clifton Aldridge indicated that at DRTL, he typically requires at a minimum a Destructive Physical Analysis (DPA) approach as part of the mitigation plan.

While many reasons have been cited for the increased occurrence of counterfeits (removal of trade barriers with countries where counterfeits are easily produced, increase in e-waste, easier access to markets through the Internet), Villescas added that the challenge of managing counterfeits has become more complex because of changes in the electronics distribution industry, too. For example, he said that he is starting to see some franchised distributors selling broker parts, increasing the risk of a counterfeit coming into the company. "At receiving and inspection, when they see a franchised distributor sending a broker part with a certification from the broker, they don't recognize that, they just think that it's another legitimate manufacturer source," he explained.

Villescas cited a recent incident in which he was getting product in from a distributor that is franchised and independent. The part in question was obsolete and hard to find, but a franchised distributor he contacted said that one of their suppliers had it. He didn't question who the supplier was, and didn't feel like he had any reason to. When they received the parts in the back, he went back to take a look at them because he needed a photo of a "golden part," since he couldn't find a known good part. When he looked at the box and the paperwork to make sure that everything was there, he saw that the paperwork had come from a broker. He said that he was amazed that the distributor hadn't informed him that they were going to get broker parts. Subsequently he went through a corrective action with the distributor to make sure that they identify from whom a part is coming. "They were calling a broker a 'supplier,'" he says. "You can't do that – you have to get the terminology straight so that we, the end users, know what we're getting."

The Link to Obsolescence

Brian Schirano, a subject matter expert with the Electronic Parts and Solutions Group at IHS, Inc., said that the battle against counterfeits has become more complicated as counterfeiters refine their own methodologies. "Counterfeiters are getting more sophisticated," he said. "They can take, for example, a reel of parts and drop in their counterfeits randomly. That's causing more and more people to go to 100 percent testing."

Schirano, who formerly worked in industry as a supply chain manager for electronic components, also links the rise of counterfeits to the challenge of obsolescence in the electronics supply chain. As parts reach their end-of-life and become obsolete, manufacturers must increasingly turn to the open market to find the components they need to support customers using products containing those parts – a particularly difficult challenge for products with long or repeatedly extended lifecycles.

A program for managing parts obsolescence can help alleviate this problem by allowing for longer lead times to design out or substitute for parts at risk of obsolescence, or for making lifetime buys or identifying reliable sources for obsolete parts. Schirano noted that there are a variety of technology solutions on the market to enable an effective obsolescence management program. IHS, for example, offers its IHS COMET, BOM Manager and PCNalert solutions to help companies manage their bills of materials for availability, obsolescence, and environmental and regulatory compliance. These solutions also can provide access to notices of parts that are suspected to be counterfeits or that are at high risk of counterfeiting, with the notices coming from IHS partner ERAI.

Phil Tippens uses the IHS "BoM Manger" tool at IEC Electronics to periodically upload customers' BoMs to assess component life cycle status. By using a product lifecycle management tool such as the IHS "BoM Manager" obsolete parts and parts that are nearing end of life can be identified. For the latter, steps can be taken prior to part obsolescence to consider lifetime buys, locate alternate parts, and/or plan for a redesign. These proactive steps help reduce the risk of counterfeit parts when a component becomes obsolete.

Inspecting Suppliers and Parts

Inspection loomed large in the discussion as a tool to help mitigate counterfeits risk. Justin Whitlow, supply chain manager for IEC, described the onsite inspection process that the company employs with suppliers. "We go in depth through their quality processes, we walk around the floors, we ask questions pertaining to supplier selection, and we look at their counterfeit mitigation plan," he said.

The process is guided by an inspection audit document that includes 33 questions about the supplier's quality systems and 40 questions of a process nature. Quality questions, for example, range from "Does management have a genuine commitment to develop a quality improvement program that strives for continuous improvement and zero-defect mentality?" to "Does the Supplier have a system for notifying Customers of potential Delivery Problems?" On the Process side, questions range from "Is there a part-specific or commodity-specific, documented procedure for Incoming Inspection with personnel trained and results documented?" and "Does the supplier use any substances on the banned or restricted list required by customer government?" Each question is scored, and suppliers are given a summary rating that ranges from "Excellence" (95 percent or higher on their summary score) to "Unacceptable" (below 60 percent).

Inspecting incoming parts also figured as a best practice, and the consensus among the discussion participants leaned toward 100 percent inspection. Paul Meyers, president of Global IC Trading Group, which offers inspection services, said his firm recommends 100 percent visual inspection, and Lori Leroy, a co-founder of Global IC, said 80 percent of suspect product the company finds is identified in the detailed visual or microscope inspection. "With the right processes and tools, you will get the majority at that stage," Meyers said.

In general, Global IC breaks its suppliers out into six categories based on level of counterfeit risk and

Participants in the discussion around counterfeit parts included:

Clifton Aldridge, *Laboratory Manager*, DRTL, LLC
Lori Leroy, *Co-founder*, Global IC Trading Group
Paul Meyers, *President*, Global IC Trading Group
Mark Northrup, *Director of Advanced Technical Operations*, IEC Electronics Corp
Brian Schirano, *SME - Electronic Parts and Solutions Group*, IHS, Inc
Rory King, *Director, Design & Supply Chain Solutions*, IHS, Inc
Phil Tippens, *Components Engineer*, IEC Electronics Corporation
Felipe Villescas, *Senior Component Engineer*, IECElectronics
Justin Whitlow, *Supply Chain Manager*, IEC Electronics Corp - Albuquerque

Supply & Demand Chain Executive thanks the participants in the discussion process for sharing their time and insights, and particularly thanks Mark Northrup with IEC for his initiative and assistance in coordinating with participants and setting up the discussion.

overlays a sampling plan over those six levels. "For parts coming from factory and franchised distributors, the number of X-rayed and decapped units will be less than for newer suppliers," Meyers said.

Villescas added, "It's real key to do 100 percent testing if budget permits, because at times you can encounter mixed lots." IEC has had instances where they might sample an incoming batch and find 4-5 percent failures, but then they test 100 percent and find a much higher failure rate, indicating a mixed lot of legitimate and counterfeit/suspect parts.

Villescas described IEC's standard inspection process as implemented by DRL starting out with visual inspection, marking permanency, physical dimension check and solderability. If they find anything suspicious, they can get a sense of whether they can proceed or stop. If everything looks good after the sampling, then they can move on to 100 percent inspection of the full lot. Phase II provides for 100 percent visual inspection on the remaining lot, running it through X-ray, doing a decapsulation on a sampling basis, then running through thermal cycling and C-mode Scanning Acoustic Microscopy (CSAM). Then they should be able to make a determination as to whether to move a lot into acceptance testing and qualification testing. They will terminate with another CSAM just to make sure that they there haven't been any voids after the acceptance testing.

The Standards Question

The participants generally agreed that standards were a necessary – but not sufficient – tool in the fight against counterfeits. IEC's Northrup noted that, in many respects, the standards now being applied to counterfeit and suspect parts are treading over the same ground covered in the past by military standards devoted to part traceability and targeted at substandard parts.

"We're reinventing the wheel by using the word 'counterfeit' versus just saying a substandard part that doesn't meet the original manufacturer's test requirements," he said. "'Counterfeits' is a word that gets everyone in fear-mongering mode, but the military has had a part traceability program in place. If you used it, you'd be able to determine a lot of these parts are substandard."

The AS5553 standard requires no laboratory auditing. The ISO 17O25 is the main standard used by testing and calibration laboratories for certification of proficiency, method validation, and reporting accuracy.

Meyers said that Global IC has been a strong advocate for revising the 1010 standard of the Independent Distributors of Electronics Association (IDEA), which covers inspections, to mandate some destructive analysis, including X-Ray, X-ray fluorescence (XRF), decapsulation and Dynasolve. He also is looking forward to the publication of the AS6081 standard due from SAE International and aimed at providing guidelines for distributors around counterfeits mitigation.

Meanwhile, Global IC's Leroy has been involved in the development of IDEA-QMS-9090, a quality management system written specifically for the Independent Distribution Industry. "IDEA-QMS-9090 will layer on top of ISO 9001, AS9120 and ANSI/ESD S20.20 certification, with specific components talking about supplier selection, inventory posting, customer provision and the inspection protocol," she explained. "This will provide one more layer to ensure that your suppliers are doing the best job that they can to mitigate your risk." This document is expected by Oct.1.

The Bottom Line

Northrup said that his No. 1 recommendation for any company is to form a centralized "SWAT" team that understands the tools, systems and processes available to attack this thorny problem. This team must be cross-functional, he said, with representatives from Quality to help the group understand the governing rules and documentation; from Engineering, with a background in electrical or troubleshooting or test engineering; and Sourcing, so that the company's procurement policies incorporate risk mitigation elements.

Aldridge and Northrup highly influenced IEC Electronics' decision to invest in building the necessary qualified staff in-house to perform mitigation testing at DRTL. "If you're going to go to the aftermarket, you need to invest in some form of testing to protect yourself, because it's going to be a lot less expensive than going through all the rework and recalls," he said. Leroy noted that companies must be active participants in industry, participating in associations and standards-making bodies. "It's very beneficial for us to be so actively involved in industry through IDEA," she said. "We feel like we're ahead of the game as far as the learning curve, and the information that we share within the organization with our fellow IDEA members is invaluable."

Finally, Northrup said that companies need to adopt a strategy for managing obsolescence that allows them to design obsolete parts out of their products.

"If we continue to have lifecycle products that have obsolescence to them, we're going to be on the Wild Wild West market trying to procure parts," he concluded. ■

Setting the International Standard(s) in the FIGHT AGAINST COUNTERFEITS

A trio of standards from SAE International is creating the foundation for a global response to counterfeit and suspect parts throughout the supply chain

By Editorial Staff

In September 2007 SAE International, the standards development organization, chartered a new committee, dubbed G-19, in response to the continuing – and growing – problem of counterfeit electronic parts entering the supply chain. The objective of the committee was to establish best practices in component management, supplier management, procurement, inspection, test and evaluation methods, and to provide the supply chain with a response on what they should do when they encounter a suspect or counterfeit part.

By April 2009, SAE International released a new standard based on G-19's work, AS5553,

"Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition." Just four months later, in August 2009, the U.S. Department of Defense adopted the standard, meaning that it became a flow-down requirement for companies looking to sell into the DoD supply chain, including the world's largest prime contractors in the Aerospace and Defense (A&D) sector.

The speed with which the DoD adopted AS5553 was unprecedented and is very is significant, according to Kristal Snider, SAE G-19 committee member and a co-founder and vice president with of ERAI, Inc., a privately held information services organization that monitors, investigates and reports issues affecting the global electronics supply chain, including supply of electronics, including supply of counterfeit and substandard parts. "It was telling of how serious the issue is, how real the concern is and the significance of the need for a response to the problem [of counterfeits]," says Snider, who plays an active, vocal role on the G-19 committee.

Covering the End-to-End Supply Chain

G-19's work is addressing the counterfeits issue from three different perspectives across the supply chain. AS5553 addresses the OEM/Contract Manufacturer perspective. It provides terms and definitions of suspect and counterfeit parts, and spells out requirements for a counterfeit electronic parts control plan. This plan covers parts availability, purchasing and purchasing information, verification of purchased product, in-process investigation, material control and reporting.

Two additional standards currently in development will address the Independent Distribution/Franchised Distribution perspective (AS6081, due to be published by the end of this year) and the Testing and Inspection perspective (AS6171). The goal is be comprehensive and provide mitigation and prevention at all levels of the supply chain. "Hopefully, between these three safety nets, a counterfeit part will be identified and stopped before it makes it into an end application," Snider says.

Membership in the G-19 committee reflects this end-to-end approach. Members include not only representatives from government agencies and the largest prime contractors to the DoD, but also distributors (including independent and franchised distributors), test labs, experts from the standards community, and industry trade associations like Aerospace Industries Association (AIA), the Component Obsolescence Group (COG), the Independent Distributors of Electronics Association (IDEA), the UK Electronics Alliance (UKEA), and ERAI, Inc..

In addition, even though G-19's work on AS5553 falls under the aegis of SAE Aerospace and the initiative was directed initially at A&D and High Reliability applications, the document is applicable across all sectors of the supply chain, Snider emphasizes. "We want to see this document adopted and readily utilized in all sectors."

Evolving to Keep Pace with Global Counterfeiting

Snider also notes that the AS5553 standard is not intended to be a static document. The G-19 committee specifically has set up a subgroup G-19 CI – Continuous Improvement that is in the early stages of work on a revision to the standard. "It's a living document that will be constantly evolving and

being improved," she says.

Feedback that the committee received following the release of AS5553, for example, included suggestions that it comprehensively addressed North-American supply chain, but required modifications to accomodate regional needs of the international community. The goal of the revision is, in part, to ensure that it is applicable across borders.

AS5553 also will benefit from the work being done on AS6081 (targeting Independent Distribution/ Franchised Distribution). It's important to remember that AS5553 was written from the perspective of a buying organization, while AS6081 is being written from two different perspectives, that of a buying organization as well as that of a selling organization, because distributors do both. In the process of evaluating both processes – the selling and the buying – the committee preparing 6081 has collected a lot of new intelligence about requirements that could be applicable to 5553.

For example, Snider explains that an initial concern in the writing of AS5553 was that it not be too prescriptive. "We didn't want the requirement section to be so overwhelming that it would be a deterrent for an organization and they would find it to be too onerous to adopt. But what we've found is that we do need to be more prescriptive. We need to take some of the materials that were placed in the appendices of AS5553 and move them into the requirements section," Snider says. As an example, she cites some of the requirements around part inspection that are in AS6081 but that were not included in AS5553 because they were considered too prescriptive. When it came time to write AS6081, though, the feeling was that these requirements needed to be included in the standard to ensure that it "had enough teeth."

Elsewhere, the thinking around definitions included within AS5553 continues to evolve, too. Creating definitions was initially a big problem in creating the standard, defining what a counterfeit part is, what a suspect part is. For example, there was a question of whether a part that is used, and that shows no evidence of being altered in any way, shape or form, but that is sold as new, should be classified as a counterfeit part. That will likely change in the revision of AS5553, because now the committee has further clarified the difference between a counterfeit part and a used part sold as new. Having these sorts of definitions, Snider says, will be very useful for industry to ensure that all the participants in a supply chain can be "on the same page."

> **"Hopefully, between these three safety nets, a counterfeit part will be identified and stopped before it makes it into an end application."**
>
> — Kristal Snider, co-founder and vice president, ERAI, Inc.

A Growing Threat

Snider has been involved in the electronics industry for more than two decades, and she has seen the threat posed by counterfeit parts grow from a nuisance to a major concern. "I can remember a time when I was involved in distribution, where you would get a requirement from a customer and you simply couldn't find the part. You don't see that anymore. Everything and anything seems to be available – and that's just not realistic. We know that the counterfeiters have the ability to determine what is obsolete and allocated, and make it readily available."

She adds that organizations involved in the electronics supply chain must understand how to use standards like AS5553, AS6081 and AS6171. "The goal is be comprehensive and provide mitigation and prevention at all levels of the supply chain," she says. "But it's important to highlight that we're measuring risk, we're not eliminating risk. We know that the counterfeiters are going to continue to hone their skills, and they're going to continue to get better. That's why this is going to be an ongoing effort, and why AS5553 is going to be a living document that is constantly subject to change. You are going to be constantly measuring your risk, and how you do that will change as identification techniques become better."

As it stands, Snider contends that the three standards documents together offer the best solution for the supply chain to lay a foundation for addressing the counterfeits issue. The Department of Defense is pushing the adoption of the standards down into their supply chains, but companies outside A&D – in automotive, medical devices and even consumer electronics, for example – are recognizing that the risks to brand reputation and, ultimately, sales are too high not to be driving forward with moving toward compliance with the standards. And as more companies look to shrink their supply bases and short-list a select set of reliable suppliers, the competitive advantage of moving more quickly to adopt the standards becomes more apparent. Simply put, given the continued growth in the number of counterfeit incidents, not following what's prescribed in AS5553, AS6081 and AS6171 is simply not an option in this market. ■

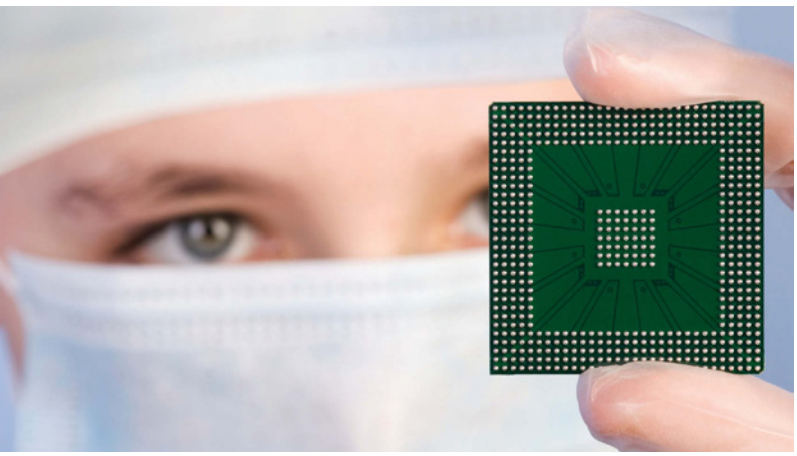
THE ROLE OF Standards Management Technology in Mitigating Counterfeits Risk

Tools that enable a practice known as 'standards management' can reduce total cost of ownership, risk, and inefficiency when implementing a myriad of standards designed to thwart counterfeits

By Editorial Staff

New standards being issued by SAE International are providing a valuable framework for managing counterfeit risk for companies involved in the supply chain for electronic components (see the article "Setting the Standard(s) in the Fight against Counterfeits" on page 8). However, to get the most benefit from a standard like SAE's AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition," companies must ensure that they have an effective standards management process in place.

SAE established the G-19 committee as a response to the growing problem of counterfeit electronic parts entering the supply chain, and an increasing number of companies are applying the standard in the context of counterfeit mitigation initiatives. However, standards management provides many benefits beyond explicity managing counterfeits, such as preventing the blind referencing of standards, duplicate purchasing of standards across an organization, lack of version control and the risk of using outdated standards, and the potential for copyright abuse – as well as the quality and liability risks associated with improper application of standards. Standards like AS5553 each include primary and secondary references to other standards and standards organizations. When compared to manually seeking out each and every individual standard and revision being referenced, the ability to store, cross-reference, and manage these in a central location can boast tremendous organizational efficiencies, while reducing total cost of ownership. Additional benefits can be found by preventing the blind referencing of standards, avoiding duplicate purchases of standards across an organization, enforcing version control, and minimizing the potential copyright abuses, as well as putting a stop to the use of outdated standards. These all ultimately increase the probability of steering clear of quality and liability risks associated with improper application of standards. Version control, for example, is one serious potential consequence of poor standards management. Without a system in place to ensure that only the most up-to-date standards are employed, companies run the risk of additional redesign cycles for compliance, putting new product launches – and revenue – in jeopardy, not to mention the costs associated with rework.



Six Steps to Effective Standards Management

As an organization looks to apply standards management to its counterfeit mitigation program, the following six objectives can provide a roadmap for effective deployment:

1 **Ensure access.** This means that those who *need* access to AS5553 and related standards in fact *have* that access where and when they need it. If people don't have what they need, they will find some other way to cope, whether or not they are in compliance with the standard or the organization's policies.

2 **Keep standards use consistent.** Dating back to the days of Eli Whitney and Henry Ford, manufacturers have recognized that consistent, repeatable processes are the key to efficiency and productivity on the plant floor. Similarly, you should

ensure that employees have consistent, repeatable processes to access the standards content they need. This kind of consistency breeds productivity, quality and speed that businesses need in order to react to a changing environment.

3 **Purchase standards from a reliable source.** Make sure that you have the licensing in place that you need, that you are covered legally and from a copyright standpoint, and that you are able to get the updates that you need in a timely manner. Your standards provider must be a good partner to your business and support your goals.

4 **Avoid copyright abuse**. Violating the copyright on a standard like AS5553 can present legal challenges to your company, and those problems are only made more serious when a lack of proper controls leads to systematic, unchecked abuses. Again, ensuring access is crucial to avoid having employees "do it their way," which exposes the company to the risk of copyright abuse.

5 **Understand usage.** Business intelligence is increasingly important to all companies. With regard to standards, doing business intelligently means being able to answer questions like: How is the information being used, who needs it, and how frequently do they need it? Do they immediately need updates, or do they need historical information throughout the lifecycle?

6 **Stay current.** This means having a reliable source: Your standards management partner must know when things change and be able to react quickly by providing the right information at the right time to the right members of your team.

Choosing the Right Standards Management Capabilities

With those six steps in mind, what do effective enabling technology capabilities for standards management look like? Chip Geisthardt, a product manager with IHS Inc., a global information company, says that today's capabilities available in its standards management solution IHS Standards Expert, are far more robust and feature-rich than libraries of documents. "Five years ago, it was a way to deliver content. Now it has become a comprehensive standards management platform – with advanced project management capabilities," Geisthardt says.

Walking through the functionality necessary for effective standards management, Geisthardt says that the breadth of standards covered in a solution should include comprehensive, up-to-date standards from multiple standards development organizations (SDO). AS5553 refers to more than 20 other standards and documents, and users should be able to access those related publications when necessary. Fast, intuitive search and discovery capabilities ensure that users have access the "right" content at the right time, and this requires robust filtering options, full-text search and redline capabilities, and the ability to mark "favorites" within the system. The system also should provide the ability to set up automated e-mail alerts when changes are made to a standard.Finally, to enable a consistent process, Geisthardt advises that a standards management tool should provide for uniform shared access to standards in way that ensures that even globally dispersed teams are able to "work off the same sheet of paper." Team members ought to have the same process for how they obtain and apply standards, and that process should be built into the tools that the team uses. IHS Standards Expert, for example, allows a team to associate standards to process documents or other project-related documentation. ""The real Significant value of the tool," Geisthardt notes, "can be found in is its project management capabilities."

Where to Get Started

Upon deciding to implement an anti-counterfeit program involving standards,organizations can follow three simple steps to deploy additional standards management capability to compliment the effort with improved efficiency and other benefits enabled by available technology:

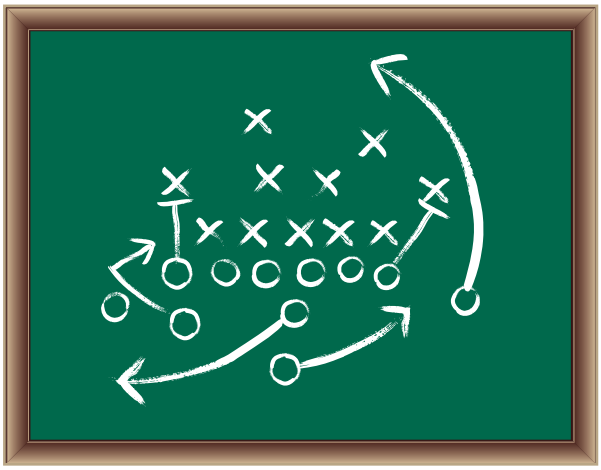
First, establish a formal priority around standards management. That means enlisting executive sponsorship that can drive this initiative within the organization, sell the importance of the standards management to other functions or business units, and endorse funding of the project at an adequate level.

Next, engage with internal specialists and external experts like IHS to look at current standards use, inventory the current library of standards, and understand how staff members access standards. Determine current and future needs for standards within the company.

Finally, the road to better standards management will involve **eliminating paper from the process, and digitizing and automating access** at the desktop level from a single reliable source (or as few sources as practical), and investing in a corporate-wide standards management tool suited to the requirements of your company and its industry.

Counterfeits represent a "real and present danger" in the electronics supply chain, and experts have argued elsewhere in this special supplement that companies must apply a range of tools in the fight against fakes. Those tools today include new and developing standards. However, companies looking to leverage standards to mitigate their exposure to counterfeit and suspect parts should also embrace effective standards management, based on a robust technology platform, in order to ensure that their risk mitigation initiative is maximally effective. ■

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, be 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 do 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 an 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.

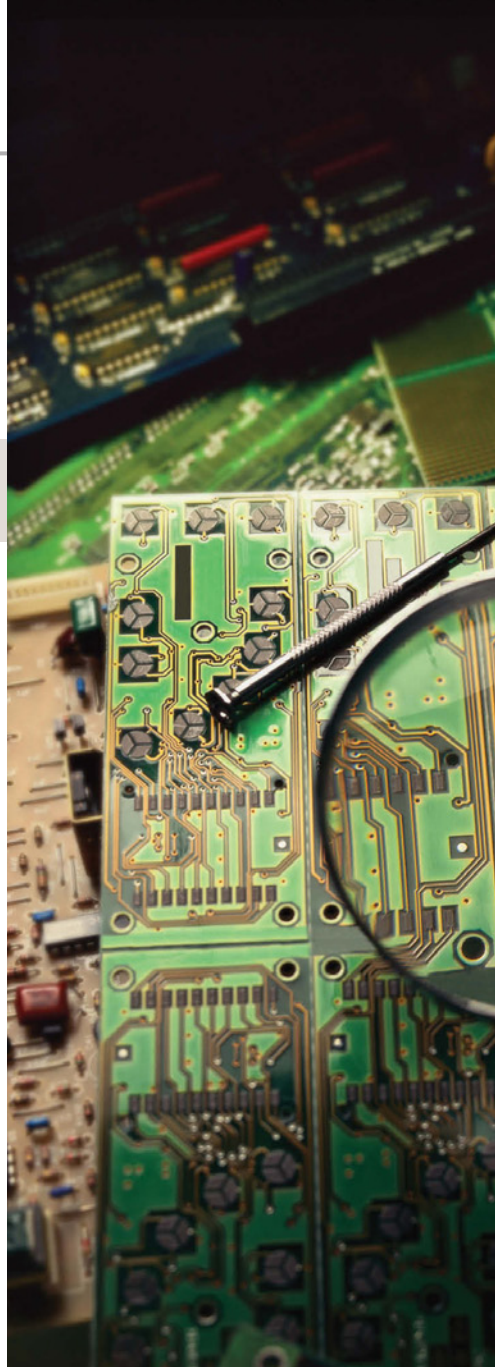
■ Of course, tackling the problem of counterfeit parts goes far beyond simply working with known entities.

■ "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."

Case Study: Fighting the Fakes

Effective strategies for mitigating the risks of counterfeit parts

By Andrew K. Reese, with Rory King



An increasing number of counterfeit parts are entering the supply chain, putting quality, brand reputation and sales revenue in jeopardy, as well as creating risks to health and safety. The electronics supply chain is still grappling with how to mitigate the dangers of counterfeits. However, many companies in the sector already are putting in place effective programs aimed at reducing, if not eliminating, the counterfeit risk. This whitepaper briefly describes the scope of the problem and the government and industry reaction, and then offers a look at how one company, L-3 Communications, is approaching this thorny issue.

A Growing Threat

Counterfeit and fraudulent goods cost U.S. businesses more than $200 billion a year and result in the loss of 250,000 U.S. jobs, according to the Federal Bureau of Investigations. Within the electrical components sector, industry estimates put the losses at up to $10 billion annually. But in addition to economic impact, counterfeit and suspect parts and components also pose a significant risk to health and safety.

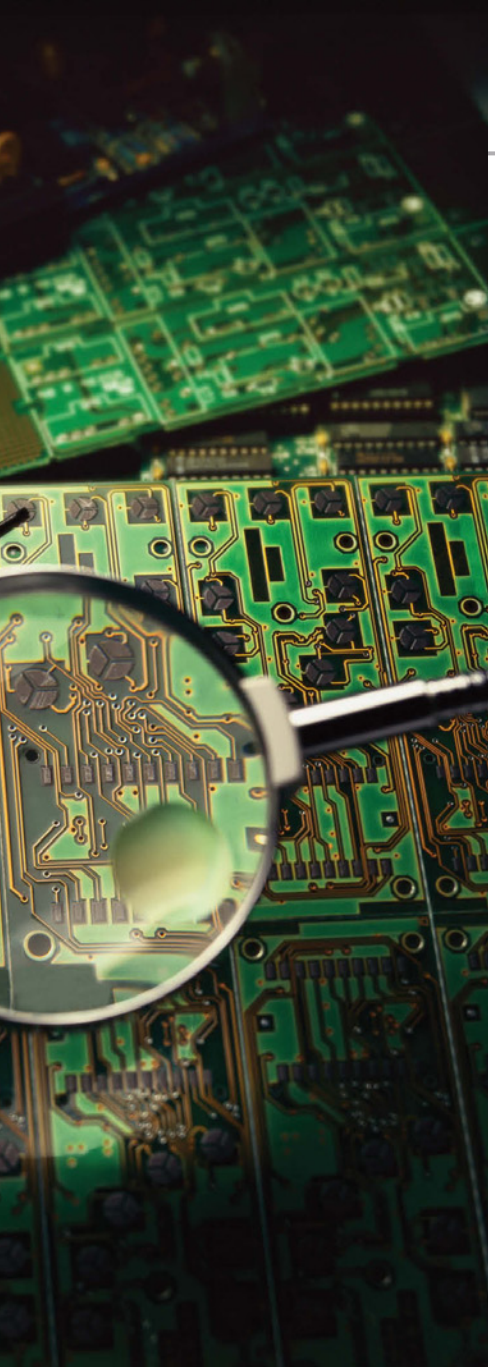
Consider that the U.S. Federal Aviation Administration once estimated that 2 percent of the 26 million parts installed on aircraft annually – a total of 520,000 parts – may be "substandard," a category that includes counterfeit and fraudulent parts. Or consider this statement from a recent report by the Electric Power Research Institute: "In the U.S. commercial nuclear industry, several CFSIs [counterfeit, fraudulent and substandard items] have been detected prior to being placed in active industry, *and several others have been detected only after installation.*"[1] Or this from the Department of Defense: the DoD reported last year that it had documented incidents of counterfeits in its supply chain ranging from GPS oscillators to rotor retaining nuts used to hold the rotor to the mast of certain helicopters – and in many cases, failure of these parts could result in failure of a mission and/or loss of life.[2]

The problem of counterfeits is growing, too, despite government and industry efforts to curtail the influx of parts into the supply chain. Within the electronics sector, the Bureau of Industry and Security, under the U.S. Department of Commerce, released a study last year showing that incidents of counterfeit electronics grew 142 percent from 2005 through 2008. Increased counterfeit incidents occurred in all the industries tracked in the study, including commercial aviation and the high-reliability medical, industrial and automotive sectors. Among the conclusions of the BIS report: "No type of company or organization has been untouched by counterfeit electronic parts. *Even the most reliable of parts sources have discovered counterfeit parts within their inventories.*"[3]

Industry Responds

Both government and industry, as well as individual companies, have responded to the rising threats posed by counterfeits. The Government Industry Data Exchange Program (GIDEP), for example, provides a Web-based system for sharing information

1. "Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items – Mitigating the Increasing Risk," October 2009. (Emphasis added.)
2. "DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts," U.S. GAO, March 2010.
3. "Defense Industrial Base Assessment: Counterfeit Electronics," January 2010. (Emphasis added.)



on counterfeits parts. Users of the system can submit information about suspected counterfeit parts, and this information is then shared through a database. Suppliers have 15 days to respond to posted information before it goes "live" in the database. The program is sponsored by the Defense Logistics Agency and NASA, as well as the Canadian Department of National Defense.

Industry groups have taken action against counterfeits, too. The Aerospace Industries Association (AIA), for example, has formed a Counterfeit Parts Integrated Project Team (IPT), with the goal of working with government agencies, OEMs, other industry associations and independent distributors on policies and standards to help mitigate the risk of introducing counterfeit parts and materials into the aerospace, space and defense supply chain.

Elsewhere, SAE International, the standards development organization, established its G-19 committee in 2007 as a direct result of the increasing volume of counterfeit electronic parts entering the aerospace supply chain. The committee is charged with developing standards to help mitigate the risks of counterfeit electronic components, including the SAE AS5553 standard applicable to the OEM and contract manufacturer (CM) community; AS6081, which prescribes counterfeit part avoidance requirements applicable to distributors; and AS6171, which applies to the testing and inspection community.

In the private sector, ERAI, founded in 1995, is an information services organization that monitors, investigates and reports issues affecting the global high-tech electronic supply chain. The company provides tools to mitigate risk from counterfeit and substandard parts, and its subscribers include OEMs, CMs, distributors, original component manufacturers (OCMs), government agencies and industry associations. It is notable that over the past decade, more than 4,000 incident reports have been made to GIDEP and ERAI, which are the two industry standard reporting entities recommended in SAE AS5553. Of these reports, 91 percent have been made via ERAI and 9 percent via GIDEP.

ERAI has an exclusive agreement with global information company IHS to bring its product and services to market. IHS provides access to a standards management platform which offers a single entry point for standards like SAE AS5553 and the numerous standards collections that are cross-referenced within, such as ESD, IDEA, IEC, ISO or JEDEC. The company also offers materials, parts and obsolescence management products and services of which ERAI has integrated its offerings, in order to provide a robust toolset for supply chain risk and counterfeit part mitigation. It's here at IHS that industry can access thousands of GIDEP and ERAI counterfeit reports in a unified manner.

In addition to these industry-wide responses to counterfeits, many individual companies in the corporate sector have undertaken initiatives to minimize their risk exposure to counterfeits. Next we'll look at how one company is approaching this challenge.

Tackling Counterfeits at L-3 Communications

Headquartered in New York City, L-3 Communications employs approximately 63,000 people worldwide and is a prime contractor in C3ISR (Command, Control, Communications, Intelligence, Surveillance and Reconnaissance) systems, aircraft modernization and maintenance, and government services. L-3 is also a leading provider of a broad range of electronic systems used on military and commercial platforms. The company reported 2010 sales of $15.7 billion.

L-3 established its Counterfeit Parts Team in 2007. In doing so, the company was influenced by requirements coming in from its customers for certificates of conformance (C of Cs). The customers had requirements for approval of the procurement process if an OEM certificate could not be provided, as well as burdensome

liability clauses for counterfeit escapes. With its customers making their own major efforts on counterfeits, L-3 faced the prospect of having to manage these requirements for commercial off-the-shelf (COTS) hardware or production lines that feed multiple customers, a particularly daunting challenge. In the face of these requirements, L-3 opted to take a proactive approach to counterfeits.

"We needed to control our own destiny by emphasizing prevention," says Rick Roelecke, director of quality assurance with L-3 WESCAM Sonoma Operations, based out of California. Roelecke is the corporate counterfeits parts lead across L-3, heading up the L-3 Counterfeit Parts Team comprised of over 35 divisional representatives. The Counterfeit Parts Team has implemented a comprehensive counterfeit mitigation program across all L-3 companies (comprising more than 100 divisions) through release of a Corporate Policy Procedure. Seizing the initiative in this way has allowed L-3 to define its own procurement guidelines around counterfeits and to identify its own approved independent distributors. The company was able to define its own risk mitigation processes to prevent counterfeit or substandard parts from reaching its customer community, and it also allows L-3 to protect its liability with regard to counterfeits.

The mission statement of the L-3 Counterfeit Parts Team (CPT) is "to define and provide guidelines for managing and controlling the risks associated with counterfeit parts." From a practical perspective, that meant establishing procedural guidelines for all L-3 divisions that address procurement practices, supplier/distributor controls and part screening requirements. The team identified and surveyed independent distributors that have systems and processes to screen for counterfeit parts, and it identified approved independent test facilities. In addition, the CPT defined purchase order and subcontract flow-down requirements. "We actually released in the L-3 community the first material and quality policy at the corporate level for this activity, and then we started developing our inspection and test guidelines to screen for counterfeit parts," Roelecke explains.

Keys to Success

Communication was critical to socializing the new policies and procedures throughout the company, Roelecke notes. The Counterfeit Parts Team assumed responsibility for communicating government, industry and customer requirements/issues and sharing lessons learned internally within L-3 via the company's intranet.

Counterfeit parts will remain a thorny challenge for the electronics supply chain. However, a disciplined, structured approach can help your company mitigate the risk of counterfeits.

At the foundation of its counterfeits strategy, L-3 had in place a comprehensive diminishing manufacturing sources and material shortages (DMSMS) program to manage material obsolescence across the company's product lines. L-3 has its more than 100 divisions submit their bills of material to a central division to create one combined obsolescence list. The company leverages IHS lifecycle management tools to manage component lifecycles and identify potential obsolescence risk, as well as the ERAI solution for managing counterfeit risk. IHS, including through its exclusive partnership with ERAI, offers tools that monitor components in a bill of material for availability, compliance, obsolescence and counterfeit risks as part of an enterprise-wide approach to product content management. Its PCNalert service provides daily updates of product change notices (PCNs), end-of-life (EOL) notices and counterfeit alerts for parts based on a company's approved vendor list (AVL) to help monitor and analyze potential sourcing and compliance risks.

The ERAI solution specifically targets counterfeit risk and alerts L-3 when a part that is going obsolete represents a risk for counterfeiting. The notices that ERAI generates to L-3 are sent out automatically to L-3's various divisions, alerting them that when they must go out to the independent market in the case of obsolete parts, which of those parts carry a high risk of a counterfeit. L-3 also tries to limit instances of going to the independent market to those cases where obsolescence is a factor and not due to schedule or cost issues.

Of course, for many organizations, fully avoiding the independent market is not always possible or practical. A company may find it necessary to go out to the independent market to avoid having to re-qualify a part in order to meet certain customers' schedules or due to cost considerations. And that really is the point of leveraging tools like the ERAI solution, so that when a reputable distributor for a specific part is identified on the independent market, the buying organization can run that supplier and that specific segment of the BOM against the ERAI list to verify it against potential counterfeit risks.

The process provides a constantly updated view of a company's product risk profile. The results of that profile for a given supplier or part can form the basis of a decision whether to add additional testing on a part – thermal screening or electrical testing, for example – beyond just marking permanency, device body visual or other standard inspection steps as part of a risk mitigation process. The key is screening a distributor even if they are on the approved list, and screening the part number, for every procurement, every time.

Companies also should look to put in place consistent policies for how it works with independent distributors. L-3 sets uniform standards for its distributors across all its divisions, but also allows the divisions to impose their own testing and screening requirements specific to their segment. A basic checklist for questions to put to a given distributor might include:

- Are they members of the Independent Distributors of Electronics Association (IDEA) and ERAI?
- Are they AS9120 and ISO9001:2000 certified?
- Are they ESD S20.20 Compliant?
- Are their inspectors certified to IDEA-3000?
- Do they have supplier controls and flow-down clauses regarding counterfeit mitigation requirements?
- Have they ever delivered a counterfeit or substandard part to a customer? If so, how did they resolve the issue?
- Do they have a die library and will they share it?
- Do they offer escrow services?
- What is their policy upon discovery of counterfeit or suspect parts in terms of impounding and reporting to organizations like GIDEP and ERAI?
- Which third-party testing facilities do they use, and which services were performed?
- Do they purchase from regions likely to be the source of counterfeits or substandard parts, such as China, India or Africa?

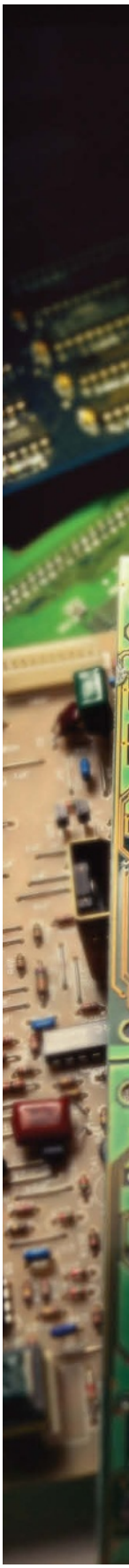
Membership in IDEA and ERAI demonstrates that they are active members of the community interested in contributing to preventing issues with counterfeits, while certifications and compliance with standards help ensure that they are staffed and equipped to properly manage and mitigate counterfeit-related issues. Properly certified inspectors that have passed the IDEA-ICE-3000 Professional Inspector Certification Exam will have knowledge of how to detect and identify counterfeit parts. Of course, surveying distributors can provide valuable feedback, but companies should also consider site visits to supplier facilities to ensure that they have the right equipment to perform inspections. And a company must be prepared to enforce a policy that precludes purchasing parts made in an "at risk" country.

How your company opts to treat counterfeits also will have an impact on how you structure your relationship with a supplier. You might decide, for example, that detecting a counterfeit and returning it to the supplier for a refund would represent too great a risk for your company. In this case, you could opt to not pay for a lot unless it has passed your independent screening houses and your reports have been approved and so forth, at which point your company would formally take ownership of the parts and pay the supplier. If, by chance, a part is found later to be suspect or substandard, many companies will impound and destroy the parts rather than return them to the supplier, considering that in the case of a part returned to the supplier, their company would be as much liable as if they had processed it themselves.

Finally, it is worth reiterating that communication is key to a successful counterfeits risk mitigation progress. That includes influencing your customer as part of your redesign process. If you are using tools like those offered by IHS to manage obsolescence, and you know you are going to have an obsolescence event coming in the future, you need to start communicating that to your customer as early as possible. You will want to educate them on your obsolescence issues, talk with them about designing those parts out of your products, and discuss how you can avoid using the independent market.

You also must continuously educate your contract manufacturers regarding your requirements and policies on the use of the independent market. Implement a system to educate your major subcontractors and critical assembly suppliers; make sure you review and approve their counterfeit risk mitigation control plans; and audit their procedures and processes. And communication must be maintained within your own four walls, with your own employees, regarding your policies and processes. Train your incoming inspection and production personnel on counterfeit and substandard part visual characteristics.

In conclusion, counterfeit parts clearly will remain a thorny challenge for the electronics supply chain. However, a disciplined, structured approach can help your company mitigate the risk of counterfeits – and help to inoculate you and your trusted supply chain partners against this modern contagion. ■



When Predators Lurk, Keep a Close Eye on the Leader

Counterfeits are on the rise, public scrutiny is intensifying, and known holes in the supply chain remain vulnerable to ambitious predators. It's time to stay close to the pack. It may be time to run towards the leaders.

The Editors, Supply & Demand Chain Executive

At its annual conference in May, the Institute for Supply Management (ISM) honored L-3 Communications as the recipient of the Annual ISM Awards for Excellence in Supply Management in the Process Category. ISM recognized L-3, a major aerospace and defense prime contractor, for its initiative to help mitigate the risks and costs associated with component obsolescence and counterfeit parts in the supply chain. "L-3 implemented executive councils comprised of senior leaders in the supply chain and quality organizations, and deployed teams to develop a disciplined and comprehensive strategy," ISM noted in announcing the honor.

In an article in ISM's *Inside Supply Management*, Ralph DeNino, vice president, procurement for L-3 Communications, highlighted the benefits that have accrued to the company thanks to its obsolescence and counterfeit parts initiative, including millions of dollars in cost avoidance due to early detection of obsolescence issues and greater than 50 percent reduction in number of components alerts. L-3's award-winning business process was featured in this edition's "Fighting the Fakes," on pg. 18.

Leaders like L-3 have linked the challenges of managing obsolescence and counterfeits in a way that should make their colleagues in other industries take note. Counterfeits are not confined to the DoD supply chain. Fakes ranging from consumer electronics to medical devices – as well as components for military equipment – are part of the flood of counterfeits that Frontier Economics has estimated will reach up to $1.77 trillion by 2015. The volatility in demand and supply engendered by the recent economic downturn and events like the tragic earthquake and tsunami in Japan have only exacerbated this issue.

Many supply chain leaders assume – or accept on face value – that their suppliers are not buying from the open market and therefore increasing their exposure to fakes. And yet statistics from a recent government study highlight that this is clearly not the case. According to the U.S. Department of Commerce, Office of Technology Evaluation, "It is not uncommon, however, for authorized distributors to purchase parts outside of the OCM supply chain in order to fulfill customer requirements – 58 percent purchase parts from other sources. Specifically, 47 percent of authorized distributors procure parts from independent distributors, 29 percent procure from brokers, and 27 percent procure from Internet-exclusive sources." Given the threat that counterfeits represent to health and safety, let alone to national security and the lives of servicemen and women, companies can no longer afford such assumptions. Rather it is time to pay attention to where the market is headed and keep pace with the herd as mounting pressure surrounds counterfeits. It's a dangerous time when the supply chain is fraught with risk exposure and significant publicity swirls global companies. Leaders like L-3 are moving in the direction of safety enabled by solutions ranging from standards like AS5553 from SAE International, and counterfeit market intelligence from companies like ERAI Inc., to BOM management, component obsolescence, and standards management solutions from IHS Inc.

Earlier this year Sen. Carl Levin, D-Mich., "[C]ounterfeit electronic arts pose a risk to our national security, pose a risk to the reliability of our weapons systems and pose a risk to the safety of our military men and women".

The stakes, indeed, are high, and the time is now to begin addressing the challenge of counterfeit and suspect parts in the supply chain. ■

AEROSPACE INDUSTRIES ASSOCIATION

Protect the Aerospace Industry & Your Business

The Aerospace Industries Association is the most authoritative and influential association representing the aerospace and defense industry. We protect the interests of the industry and help our members develop growth opportunities.

This is a turbulent time for the nation and the aerospace and defense industry - - we face numerous economic and political challenges, both domestically and internationally.

In times like these, AIA's strong representation and advocacy is essential to protecting the interests of the nation's aerospace and defense industry and helping to establish new opportunities.

AIA represents more than 330 of the leading aerospace and defense manufacturers and suppliers. Unlike many other associations, CEOs of our member companies and their senior managers define and drive our agenda.

Get closer to your current customers, competitors, and potential customers by working together to advance our industry and shape regulatory and legislative policies.

Get your seat at the table and be part of the strongest and fastest growing aerospace and defense association in the world. To learn more about the benefits of membership in AIA, please go to www.aia-aerospace.org

Solutions for Counterfeit, Substandard, and High Risk Parts

A World of Information at Your Fingertips

For more than a decade ERAI, Inc. has been the industry's primary global information services organization that monitors, investigates and reports issues that are affecting the global supply chain of electronics. It is the industry's most comprehensive source for known problematic electronic components, while leading the way in tracking and reporting information on the rapidly growing problem of corporate identity theft. Offered exclusively through IHS Inc., the **Counterfeit**, **Substandard**, and **High Risk Parts** solution provides the information, expertise, and professional staff necessary to prevent problems before they occur, thereby avoiding unforeseen financial losses.

www.erai.com