Stemming the counterfeit tide

By Bruce Rayner

Counterfeit components have been a thorn in the side of the electronics industry for decades. And every year the incidents seem to grow more common—and more costly.

One estimate suggests that counterfeit parts account for more than $5 billion, or about 2 percent, of the total available market for semiconductors worldwide. The Semiconductor Industry Association claims counterfeiting costs U.S.-based semiconductor companies more than $7.5 billion each year.

Law enforcement and government agencies are collaborating to catch fakes before they enter the supply chain. Between 2007 and 2010, the U.S. Immigration and Customs Enforcement agency (ICE) worked with U.S. Customs and Border Patrol on more than 1,300 seizures involving 5.6 million counterfeit semiconductors. The confiscated counterfeits bore the trademarks of 87 North American, Asian and European semiconductor companies.

A 2010 government case against chip broker VisionTech Components of Clearwater, Fla., charged two company officials with knowingly importing more than 3,200 shipments of counterfeit semiconductors into the United States, marketing some of the products as "military grade" and selling them to the U.S. Navy, defense contractors and others. The case involved the coordination of multiple government agencies, including the Department of Justice Task Force on Intellectual Property, the Naval Criminal Investigative Service (NCIS) and ICE.

New efforts to keep fakes out of the military supply chain have made headway, but are they enough to protect against tomorrow's threats?

VisionTech "set a ticking time bomb of incalculable damage and harm to the U.S. military, U.S. servicemen and -women, the government, all of the industries to which VisionTech sold goods, and consumers," the U.S. attorney who prosecuted the case wrote in the government's sentencing memo.

Congressional response

In 2011, electronics counterfeiting caught the attention of the Senate Armed Services Committee. A series of hearings explored the extent and severity of the counterfeit problem within the military and government sectors, and a congressional investigation documented more than 1,800 instances of counterfeit electronic parts in the defense supply chain. Some of those parts had wound up in military equipment operating in the field.

One case involved suspect counterfeit parts in forward-looking infrared radar (FLIR) units supplied to the U.S. Navy by Raytheon Co. Some of the FLIR units had been installed on helicopters deployed to the Pacific Fleet. In another case, suspect counterfeit parts were used in color multipurpose display units (CMDUs) that L3 Communications had installed on U.S. Air Force C-27J aircraft. Two of the C-27Js had been deployed in Afghanistan.

In the case of the CMDUs, the counterfeit parts were traced back to a company in China that had sold them to a U.S. independent distributor. The U.S. company in turn had sold the parts to L-3 Communications, according to an Oct. 31 letter to Michael Donley, secretary of the Air Force, from Senate Armed Services Committee Chairman Carl Levin and Ranking Minority Leader John McCain. "More than 500 of those [CMDUs] were sold to both L-3 Communications Integrated Systems, the prime contractor on the C-27J, and Lockheed Martin, the prime contractor to the C-130J," Levin and McCain wrote.

HIGHLIGHTS OF THE LEVIN-McCAIN AMENDMENT TO THE FY 2012 NDAA

- Prohibits contractors from charging the DOD for the cost of fixing the problem when counterfeit parts are discovered.
- Requires the department and its contractors whenever possible to buy electronic parts from original component manufacturers and their authorized dealers, or from trusted suppliers that meet established standards for detecting and avoiding counterfeit parts.
- Requires contractors and military officials who learn of counterfeit parts in the supply chain to provide written notification to the contracting officer, the DOD inspector general and the Government-Industry Data Exchange Program.
- Requires the secretary of Homeland Security to establish a methodology for the enhanced inspection of electronic parts after consulting with the secretary of Defense as to the sources of counterfeit parts in the defense supply chain.
- Mandates that large defense contractors establish systems for detecting and avoiding counterfeit parts, and authorizes reductions in contract payments to contractors that fail to do so.
- Requires the DOD to adopt policies and procedures for detecting and avoiding counterfeit parts in its direct purchases, and for assessing and acting on reports of counterfeits.
- Adopts provisions of a bill sponsored by Sen. Sheldon Whitehouse, D-R.I., to toughen criminal sentences for counterfeiting of military goods or services.
- Requires the DOD to define "counterfeit part" and to include in that definition previously used parts that have been misrepresented as new.

SOURCES: OFFICE OF SEN. CARL LEVIN; TITLE VIII, SUBTITLE C, SECTION 848 OF THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2012

The investigation culminated last month in an amendment to the National Defense Authorization Act (NDAA) for Fiscal Year 2012 co-sponsored by Levin and McCain that would "bolster the detection and avoidance of counterfeit electronic parts." The amendment, which was signed into law on Dec. 31, puts the responsibility squarely on the shoulders of contractors such as Raytheon and L-3 to ensure that counterfeits never make it into equipment deployed to the field.

The Levin-McCain amendment requires the contractor to absorb the cost for any equipment rework or refurbishment resulting from counterfeits. It also calls for a fine of up to $5 million and 20 years in prison for individuals convicted of selling counterfeits to the U.S. government that are used in critical infrastructure or national security applications. Guilty companies could be fined up to $15 million.

The amendment further requires contractors to obtain electronic parts from original manufacturers, their authorized dealers or other "trusted suppliers." Those trusted suppliers can include independent distributors as long as they have adequate policies and procedures in place to detect counterfeits.

Because military systems are often deployed for decades, replacement parts are typically out of production and often not available from either the original component manufacturer (OCM) or a franchised distributor. A few franchised distributors, such as Rochester Electronics, specialize in obsolete parts for defense systems. But when those sources don't have the parts—or, more precisely, don't have them when the customer needs them—the only recourse for defense contractors is to buy from independents and brokers on the open market.

While the vast majority of independents are aboveboard, most do not have the systems in place to catch counterfeits. In fact, some independent distributors have estimated their incoming inventory to be as high as 35 percent counterfeit, according to Leon Hamiter of Components Technology Institute Inc. (Huntsville, Ala.).

Catching the fakes is expensive. Outlays for the equipment needed for physical inspection and test can run into the hundreds of thousands of dollars. The instrument roster includes high-powered laboratory-grade microscopes, X-ray fluorescence equipment, scanning electron and acoustic microscopes, and decapsulation test equipment. In addition to

absorbing the capital costs, companies must invest to hire and train staff for both physical and electrical testing.

Contractors and defense agencies are reviewing their relationships with independent distributors and brokers in light of the Levin-McCain amendment. "Many are cutting their approved vendor lists to just three or four independents," said Tom Sharpe, vice president of independent distributor SMT Corp. (Sandy Hook, Conn.).

Sharpe hopes SMT will be one of the few independents that make the cut, though a few years ago it would not have been considered a standout. In 2005 and 2006, SMT unknowingly sold counterfeit parts to a defense contractor. The contractor discovered the fakes during a stock sweep and in early 2007 filed two Government Industry Data Exchange Program (GIDEP) reports against SMT.

Appearing in the GIDEP database amounts to being blacklisted by the defense community. But "that event was the best thing that ever happened to SMT," Sharpe said. "It made us reassess our capabilities and develop a mitigation strategy."

SMT took a year off from selling to the military to enhance its ability to identify counterfeits. It invested more than $1 million in test and inspection equipment, earned certification to three industry quality standards, trained and certified its quality-control lab staff, and built new capacity and processes.

The company reentered the defense market in July 2008 and has since gained a reputation as a leader in authenticating semiconductors, according to a number of industry sources.

SMT has contributed to the industry's understanding of counterfeit practices by documenting some of the more advanced methods used to resurface and remark semiconductor packages. In 2009, it identified a surface recoating material that is immune to acetone surface permanency testing. And last year, it uncovered two new processes used by counterfeiters: one for removing part markings without requiring surface recoating, and the other to remove and recondition the surfaces of ceramic components.

"There's no college degree in detecting counterfeit parts," said Sharpe. "You need to be looking at parts and work with the stuff every day."

The counterfeiting problem is hardly confined to the public sector. About 98 percent of all semiconductors are sold to commercial customers in all market segments—including the automotive, industrial and medical sectors, in which safety and quality standards are rigorous. And there are plenty of cases in all of these sectors of counterfeits' causing system failure.

The recommendations made in Levin-McCain are as valid for commercial applications as they are for the military. All companies should source only from OCMs or their franchised distributors whenever possible. And if there's no alternative to the open market, they should source only from "trusted sources" that have robust test capabilities.

Still, there's no telling how long today's test regimes will protect the electronics supply chain, as counterfeiters are constantly refining their capabilities. As soon as companies identify a counterfeiting technique, counterfeiters respond with even more sophisticated approaches.

One of the most serious new threats is the "clone" component—a part manufactured to look and function exactly like the OCM's product. Typically, clones pass both physical and electrical testing. Taking the concept a bit further is "malicious insertion," whereby malware is embedded in a piece of industrial equipment with the intent of causing a malfunction or to gather intelligence. Targets include commercial companies, the military and the government.

One suspected example of malicious insertion, reported roughly a year ago, involved software embedded in a piece of industrial equipment manufactured by Siemens. The software contained a sophisticated worm known as Stuxnet that was allegedly responsible for causing malfunctions of nuclear centrifuges at an Iranian nuclear enrichment plant. Israel has been implicated in that attack, according to *The New York Times*.

A November report by the Office of the National Counterintelligence Executive titled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace" argued that the pace of industrial espionage against U.S. corporations and government agencies is accelerating. While the report did not mention clone components specifically, it did address the increased incidence of malware.

Don't let your guard down. ■

Bruce Rayner (*bruce@afitplanet.com*) is a contributing editor to *EE Times*.