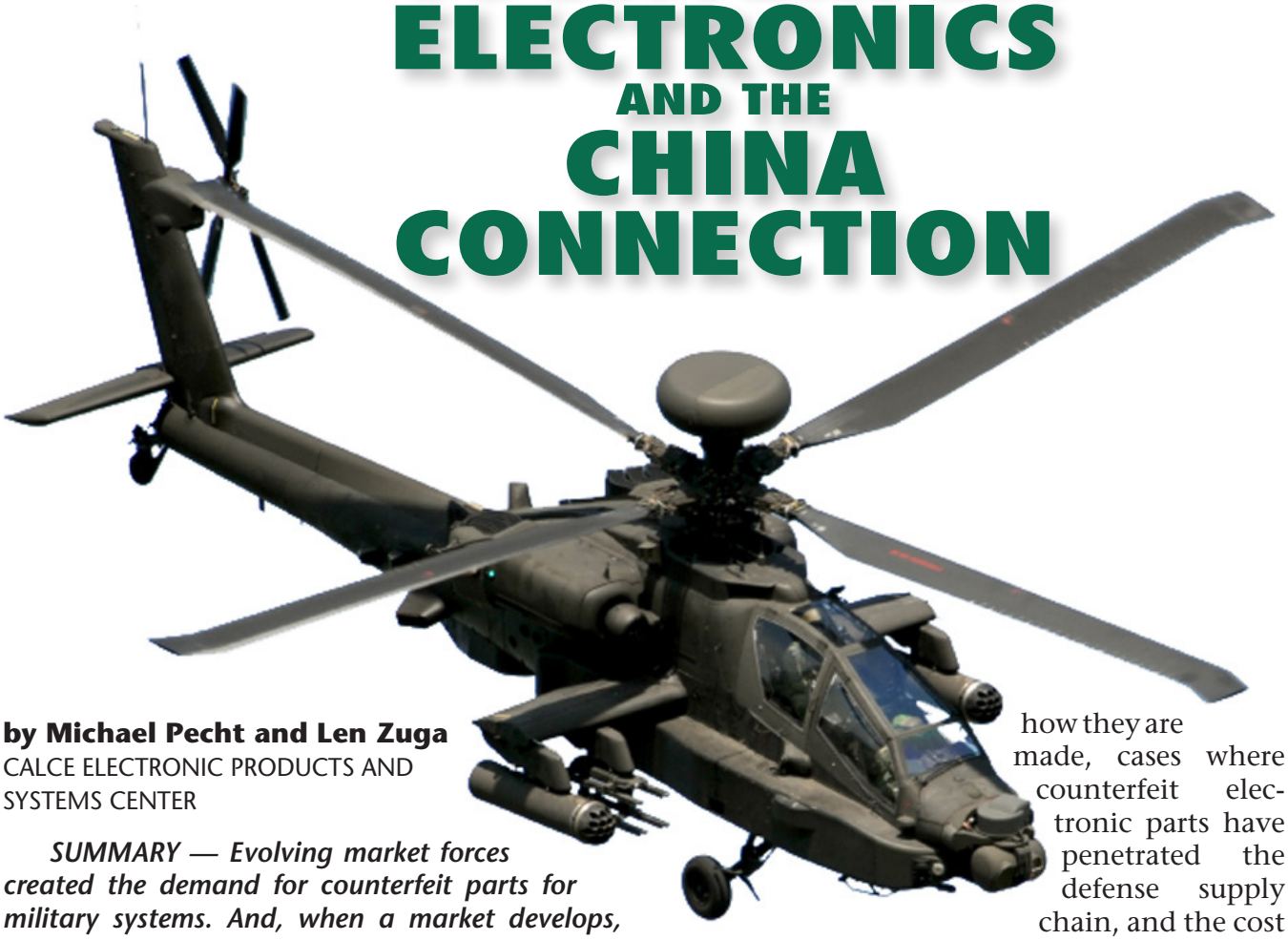
COUNTERFEIT ELECTRONICS AND THE CHINA CONNECTION



by Michael Pecht and Len Zuga
CALCE ELECTRONIC PRODUCTS AND SYSTEMS CENTER

SUMMARY — Evolving market forces created the demand for counterfeit parts for military systems. And, when a market develops, suppliers will rise to serve that market. The military market, with its demand for obsolete parts, the cost and schedule pressures it places on manufacturers, and the overall degradation of its supply chain management and supplier controls, is the true cause of its own undoing.

In November 2011, the Senate Armed Services Committee identified China, among other countries, including the United States, as a major source of the counterfeit electronics making their way into U.S. military systems and other critical systems. The failure of counterfeit parts in these systems could be catastrophic and could even be responsible for the death of military or civilian personnel.

In a four-hour hearing before the Senate Armed Services Committee, witnesses testified about the sources of counterfeit electronic parts, how they are made, cases where counterfeit electronic parts have penetrated the defense supply chain, and the cost of counterfeit electronic parts and their potential impact on defense systems. Listening to the questioning and testimony, anyone who worked in the defense electronics industry in the pre-COTS era could not help but wonder what happened to the robust quality assurance, supply chain management, and part traceability systems that were mandated by government design specifications and quality management programs of that time. Yes, "old timers" acknowledge that these systems were costly, but post-COTS parts procurement practices often result in even more costly correction and remediation for each incident of counterfeit components that have found their way into military systems of late.

Senator John McCain, Chairman of the Armed Services Committee, asserted that, with respect to electronic parts counterfeiting, "The

Chinese government can stop it." However, Senator McCain fails to recognize (or is reluctant to acknowledge) that the root cause of the problem is not the Chinese. The team at the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland is routinely asked to investigate counterfeit electronics. CALCE has found that the responsibility for counterfeiting most often lies with unauthorized U.S. suppliers (distributors and other mid-tier suppliers), as well as the system manufacturers who fail to vet their suppliers and ascertain the pedigrees of the parts that they procure. These mid-tier suppliers often commission the counterfeiting of parts from businesses in foreign countries, including Vietnam, the Philippines, China, and Thailand. In other words, U.S. military contractors who knowingly or unknowingly procure counterfeit parts from unauthorized U.S. parts distributors (brokers) who commission the counterfeiting of these parts specifically to sell to military contractors are the root cause of counterfeiting.

In essence, evolving market forces have created the demand for counterfeit parts for military systems. And, when a market develops, suppliers will rise to serve that market. The military market, with its demand for obsolete parts, the cost and schedule pressures it places on manufacturers, and the overall degradation of its supply chain management and supplier controls, is the true cause of its own undoing. Add to this mix the offshoring of scrapped electronics to China's parts reclamation mills rather than responsible domestic recycling, and the supply source of obsolete electronics components is created in China.

Counterfeit electronics are increasingly found in weapons systems as well as commercial avionics and some automotive systems. In fact, the Senate committee's investigation identified approximately 1,800 instances of suspect counterfeit electronics being sold to the U.S. military. Data extrapolations indicate that the total number of such parts could be greater than 1 million. Semiconductor industry analysts at IHS Suppli reported in February 2012 that incidences of counterfeit parts have soared dramatically in the last two years. Based on reported data alone, IHS iSuppli noted a four-fold increase from 2009 to 2011. This marked the first time that the number of reported incidents in a single year exceeded 1,000, a total that, when traced through all impacted bills of materials, could encompass millions of purchased parts.

IHS iSuppli also acknowledged that "the surge over the past two years is the latest development in a rapidly escalating global supply chain trend toward increased counterfeiting and piracy of global products, with counterfeit part reports having risen by nearly a factor of 700 over the last decade." The bulk of these incidents were reported by U.S.-based military and aerospace electronics firms.

> ***"Counterfeit parts incorporated into our military systems could endanger the lives of our troops or cause other catastrophic consequences. The real blame lies with brokers and military contractors brokers who placed expediency and profit above all else."***

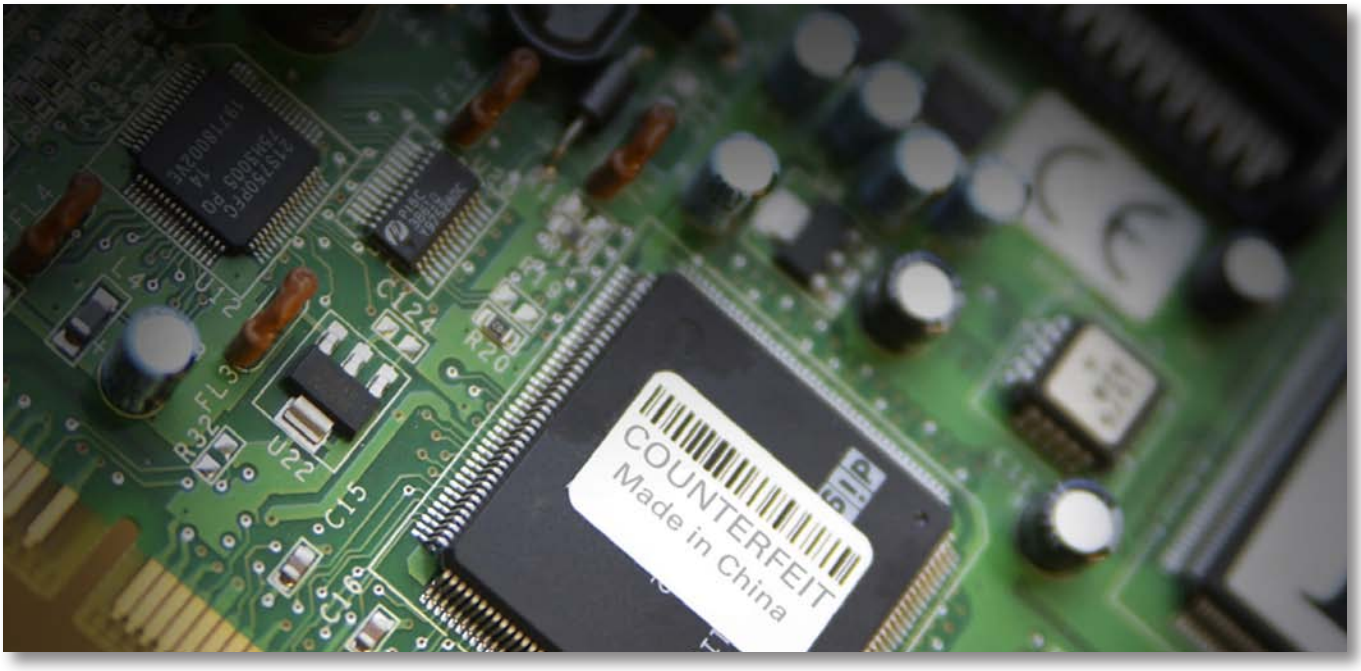
For example, Raytheon Missile Systems purchased some 1,500 Intel flash memory (semiconductor) devices for incorporation into the Harm Targeting System (HTS) which is installed in F-16 fighter planes to identify and track enemy radar systems. Raytheon purchased those parts from a U.S. broker rather than from the original device manufacturer or its authorized distributor. This is analogous to purchasing a Gucci handbag on Canal Street in New York City or across the street from the Rosslyn Metro in Washington, D.C.—the purse is very likely to be counterfeit. Without checking the devices ahead of time, Raytheon installed those Intel chips on 28 circuit boards destined for HTS modules. The military can be grateful that the boards immediately failed, because Raytheon had to examine the boards to determine the root cause of the problem, and only then did they learn that the parts were all counterfeit. Imagine if the boards had worked (for a while) and were installed in a weapons system in the field!

The broker that Raytheon bought the parts from, VisionTech Components Inc., has since been charged with the selling of counterfeit parts, and the guilty parties have been sentenced. During the legal process, it was learned that VisionTech personnel had the ability to alter the labels and identities of electronic parts. VisionTech also gave instructions to people in China on how this counterfeiting should be accomplished and how such parts should be shipped to the U.S. In other words, the parts were commissioned by a U.S. company. In fact, the parts were not necessarily "made/fabricated" in China, but were "altered" (mostly cosmetic changes) in China and in the U.S.

VisionTech is not the only U.S. parts broker that has duped military contractors by selling them counterfeit electronics. Another broker had its own component alteration equipment for making cosmetic changes. The team at the CALCE Electronic Products and Systems Center encountered nearly 30 major counterfeit parts in 2011 alone (most of which the U.S. military is unaware of).

The fact that China's parts strippers and their buyers have the ability to re-label parts at a low cost is not a sufficient reason for the U.S. to blame China, as that same ability also exists here in the U.S. Instead, Senator McCain and others, including the U.S. Justice Department, should hold companies like Raytheon accountable, because what they did is unconscionable. It is also surprising that Intel has not said anything about the possibility of their parts being counterfeit. Surely they should know about the possibilities based on demand patterns for these parts, since they have representation on the U.S. Semiconductor Industry Anti-Counterfeiting Task Force. It appears that in this case the contractor and brokers were willing to deliver at any cost, the military and law enforcement had no checks, and the members of the semiconductor industry wanted to hide their heads.

As a result of the November 2011 and subsequent Senate Armed Services Committee hearings, the National Defense Authorization Act for FY 2012, which was signed into U.S. Law on December 31, 2011, includes Section 818, a provision to ensure the "Detection and Avoidance of Counterfeit Electronic Parts." Section 818 represents an admonishment of the DoD to reinstitute the once effective, but now atrophied, supply chain management and quality control system of decades past. It is a step in the right direction, but let there be no mistake: The responsibility rests with the manufacturer. The rather sobering investigation and remediation costs associated with counterfeit components that find their way into defense and high-reliability systems should be incentive enough



Typical Industry Costs	
External visual inspection & paperwork check	$50/hour
Marking permanence	$50/hour
Scanning acoustic microscopy	$800
XRF check of terminations	$500
X-ray check of internal die	$500
De-cap inspection	$1,000
Electrical testing	$50/hour plus test program non-recurring engineering (NRE)
Test program NRE	$4,000 for simple logic device; $30k for complex VLSI logic, processor, and mixed signal; and additional cost of any extra hardware/load boards

Table 1: Typical industry costs for quality assurance.

to restore the health of an ailing supply chain management system.

To give one example, the authors were recently asked to consult on an undocumented case of suspect counterfeit cabling for use in undersea applications in the oil and gas industry. The buyer's need for expediency for the delivery of a mere $6 worth of cable ended up costing the manufacturer well in excess of $100,000 to date in investigation, buyer-supplier meetings, travel, and remediation at the component level. Furthermore, the charges are still accumulating, there is lost goodwill, and the manufacturer will never again be a trusted supplier to its aggrieved buyer.

Without actual manufacturer-supplied data for the costs of each incident of counterfeit parts remediation, as in the suspect counterfeit cabling case described above, it is impossible to add up the corrective action costs for those incidences of discovered counterfeit parts. However, CALCE's data indicate that the representative component vetting costs shown in Table 1 are reasonable insurance costs against having to incur such disproportionate remediation costs, as in the suspect counterfeit cabling case above. In essence, the old adage "do it right the first time" is far less costly than remediation.

Table 1 shows individual component quality assurance costs resulting from a counterfeit component that are replicated throughout any bill of materials. Risk analysis and reliability engineering evaluation can be applied to identify critical suppliers and components to which the above activities should be applied over and above the certifications and traceability paper trails provided by the supplier.

Thanks to the National Defense Authorization Act for FY 2012, as it was in the pre-COTS era, it is once again the responsibility of each manufacturer of defense equipment to ensure the quality and reliability of the parts that are used in defense weapons systems. Under the provisions of the act:

- Contractors are now responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit parts.
- Contractors are also responsible for any rework or corrective action that may be required to remedy the use or inclusion of such parts.
- Defense contracts will no longer allow billing the government for remediation costs of counterfeit electronic parts and suspect counterfeit electronic parts or the cost associated with rework or corrective action to resolve the use or inclusion of such parts.
- Qualification procedures and processes must be established to use trusted suppliers and procure electronics from authorized suppliers.

Counterfeit parts incorporated into our military systems could endanger the lives of our

troops or cause other catastrophic consequences. The real blame lies with brokers and military contractors brokers who placed expediency and profit above all else. Such behavior falls in the same criminal category as sending U.S. military secrets to China and other countries.

The provisions of Section 818 of the National Defense Authorization Act for FY 2012 are still based on trust—a trust that the manufacturers have indeed lost over the last three decades. They will have to once again work hard and spend appropriately on infrastructure to regain that trust that was once inherent in the defense procurement processes of the pre-COTS era. The authors are by no means advocating a return to the cumbersome, highly bureaucratic, and costly supply chain management practices of the pre-COTS era. That system was based on domestic sourcing of parts in the Cold War era that tolerated such inefficiencies. As argued by Pecht et al. in their 1997 paper *An Assessment of the Qualified Manufacturer List,* that system also encouraged the use of obsolete technology which prohibited access to reliability improvements provided by newer technologies.

The causes that have allowed the counterfeit problem to occur today are three-fold:

1. Systems engineering in technologically advanced platforms has resulted in system design and manufacturing responsibility fragmentation and a dramatic proliferation of offshoring of both engineering design, which increasingly introduces supply chain management complexities.

2. The lost basic expertise in the government procurement management system, aptly illustrated in the November 2011 Senate Armed Services Committee testimony, has gutted government regulatory and oversight capabilities.

3. Cost and expediency incentives have become powerful and major drivers at the contractor level.

The competitiveness factor, once seen as a major positive factor in driving down procurement costs has merely shifted the insurance costs from front-end management to after-the-fact remediation. The authors therefore submit that the combined government procurement establishment and the defense industrial base manufacturers must jointly establish a more effective, but affordable, source control system much like those of highly reliable consumer electronics producers such as Apple, Dell, and Intel, and require every point in the supply chain to inform buyers and systems manufacturers of the source of all the materials (tin, tantalum, gold, and tungsten) throughout the supply chain. Given that this model serves the consumer industry well with reliable yet affordable electronics, it can also be affordable for the defense industrial base. **SMT**

Professor Michael Pecht has an MS in Electrical Engineering and an MS and Ph.D. in Engineering Mechanics from the University of Wisconsin at Madison. He is a Professional Engineer, an IEEE Fellow, an ASME Fellow, an SAE Fellow and an IMAPS Fellow. He is the founder of Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland, which is funded by over 150 of the world's leading electronics companies. He is also a Chair Professor in Mechanical Engineering and a Professor in Applied Mathematics at the University of Maryland.

Len Zuga is an emerging technologies, technology transfer, and industrial base development analyst in the context of the global political economy. He is a partner of the consulting firm Technology & Business Insider (TBI), and a consultant to the CALCE Electronics Products and Systems Center at the University of Maryland. Responding to an obvious post-9/11 need, Zuga joined Battelle Memorial Institute in November of that year and applied his experience to government-sponsored research focusing on the global electronics industry for the next nine years. Zuga is co-author of the book, with Professor Michael Pecht, "China's Electronics Industry (2009)."