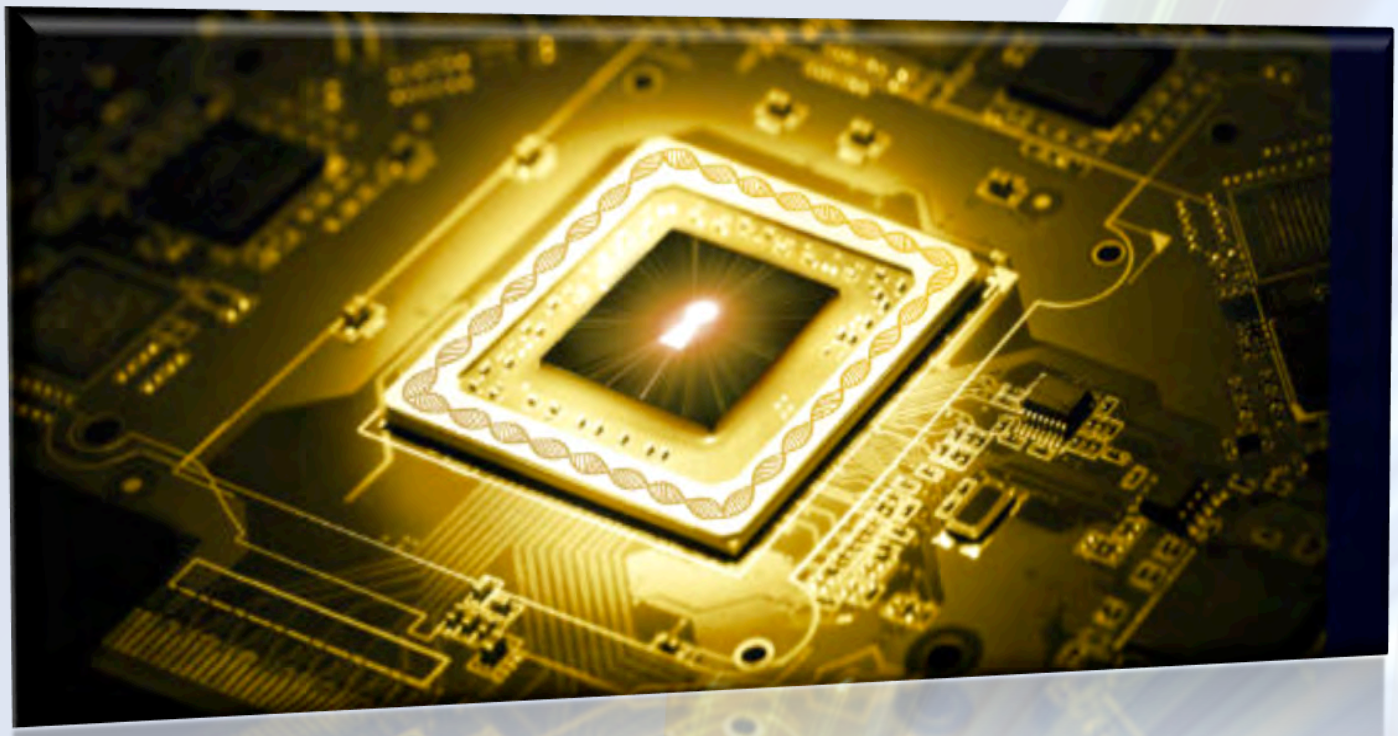
KESSLER AEROSPACE SOLUTIONS

The DoD Counterfeit Threat & Compliance

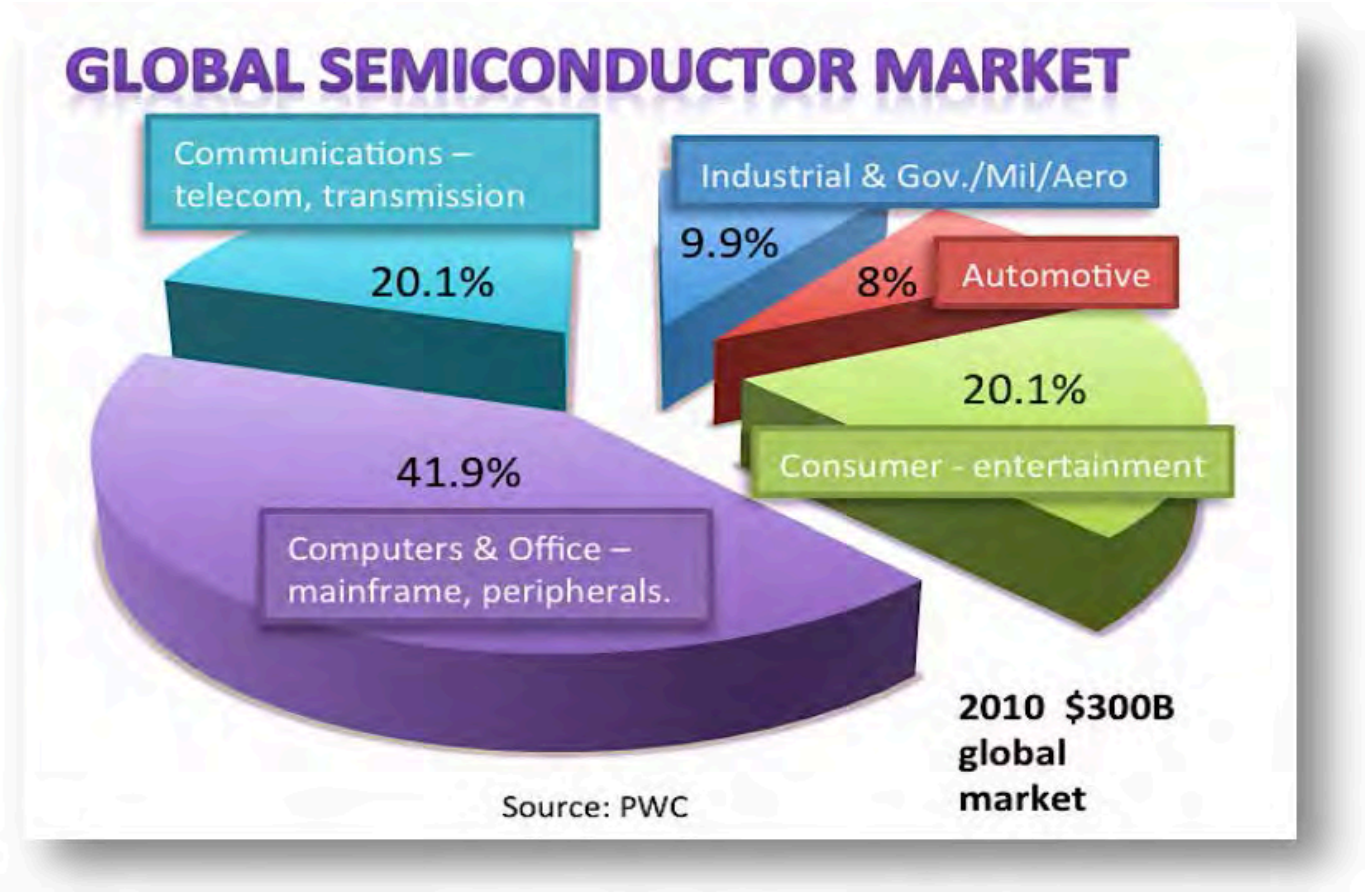
by Ron Clark Ball



Ron Clark Ball is CEO and founding partner of Kessler Aerospace Solutions where he advises clients from leading multinationals to privately held companies.

The Counterfeit Component Threat - 2013

1. Market Research - Obsolescence Management and Counterfeit



The overall market for electrical components is massive, exceeding $300 billion globally in 2010, with government and military representing just one percent of that market worldwide. Because of the continued service life of military aircraft, commonly known as “Legacy Sustainment”, the U.S. Defense and Aerospace Industry faces an ever-increasing dilemma and threat, primarily the introduction of counterfeit electronic components into the Department of Defense supply chain. Every weapons system and network are currently affected. The result has been a change to the National Defense Authorization Act. Section 818 of the FY2012 NDAA states that the DoD must "establish requirements for a contractor or subcontractor to notify its DoD customer when electronic parts are obtained from any source other than the original manufacturer or its authorized dealer."

Demand is the driving force, and the caution/ warning to alert the DoD and its contractors that they can anticipate when it will be necessary to make critical purchases, of course unless obsolete parts are eliminated from electronic equipment designs. The following recommendations are offered to DoD as it develops policy and changes to regulations in response to Section 818 of the FY2012 NDAA[1]:

- When feasible, support and fund approaches to eliminate or mitigate the use of obsolete electronic parts.
- Require proposals for production and support contracts to identify obsolete electronic parts and to establish a plan to either assure trusted sources of supply

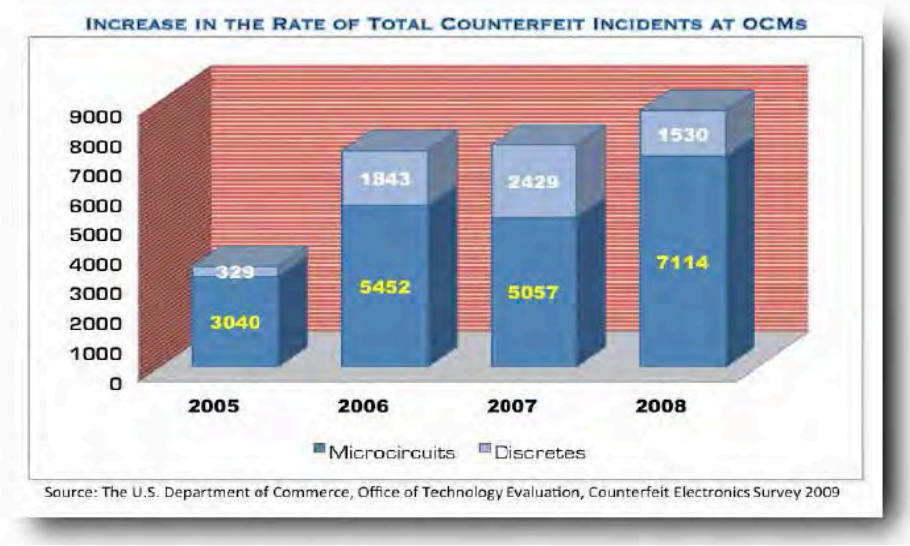
1. Proposed recommendations by DoD.

for obsolete electronic parts, or to implement design modifications to eliminate obsolete electronic parts.

- Include provisions such that the identification of obsolete electronic parts at the time of proposal for production and support contracts serve as notification to DoD of anticipated potential use of electronic parts purchased from suppliers other than the original component manufacturer (OCM) or its authorized dealers.
- Include provisions such that costs to remedy a counterfeit part escape will be considered allowable costs provided all of the following conditions are met:
  - The contractor's proposal identifies obsolete electronic parts and includes a plan to assure trusted sources of supply for obsolete electronic parts, or to implement design modifications to eliminate obsolete electronic parts.
  - The DoD customer elects not to fund or otherwise entertain design modifications to eliminate obsolete electronic parts.
  - The contractor applies inspections and tests intended to detect counterfeit electronic parts when purchasing electronic parts from other than the OCM or its "authorized dealer".
  - A counterfeit electronic part escapes detection, despite the application of inspections and tests intended to detect counterfeit electronic parts[2].

The initiatives above will provide some breathing room for the DoD and its contractors to establish plans for addressing part obsolescence and to weigh the cost of design mods to eliminate obsolete parts as opposed to the risk of purchasing obsolete parts through questionable supply chains and the cost to minimize such risks.

Industry, government and academic studies have increasingly detailed the growing threat and negative impact of the infiltration of counterfeit parts into product supply chains. The Department of Commerce's Bureau of Industry and Security (BIS), at the request of Naval Air Systems Command (NAVAIR), released a study in January 2010 (BIS Study) that quantifies the extent of infiltration of counterfeit electronic parts into U.S. defense supply chains. The BIS study documented a growth in incidents of counterfeit parts across the electronics industry from 3,300 incidents in 2005 to more than 8,000 incidents in 2008. This sharp increase in incidents, in only three years, clearly indicates that the volume of counterfeit parts is increasing and mitigation plans must be developed and implemented. The introduction of counterfeit parts, whether they are electronic, mechanical or other, adversely affects the U.S. supply chain.



2. Proposed recommendations by DoD.

WIDESPREAD IMPACT

For Government:

- National security or civilian safety issues
  - Trojan Horse
    - Designed to fail
    - Designed to penetrate and capture
- Costs of enforcement
- Lost tax revenue due to illegal sales of counterfeit parts

For Industry:

- Costs to mitigate this risk and lost sales
- Costs to replace failed parts
- Punitive damages for not complying with mandates of the law
- Lost brand value or damage to business image

For Consumers:

- Costs when products fail due to lower quality and reliability of counterfeit parts
- Potential safety concerns
  - The escalating infusion of counterfeit parts means that every aerospace and defense manufacturer is at risk. Electronic parts, for example, are integral to the function of every aerospace and defense industry platform delivered to government and civilian customers[3].

Profit is the driving force for counterfeiters of electrical components. However, there are unique conditions exist that make aerospace and defense products susceptible to counterfeiting, including a long life-cycle and diminishing manufacturing sources and material shortages issues. Aerospace and defense products are generally designed for a long life cycle. The B-52, for example, went into service in February 1955 with an anticipated retirement date of 2040. Other examples of long-flying aircraft are in Table 1.

Table 1: Examples of Life Cycles of Aircraft

Aircraft	In Service Date	Anticipated Retirement Date
DC-3	DEC 1935	Not Determined
B-52	FEB 1955	2040
C-130	DEC 1957	Not Determined
B737	FEB 1968	Not Determined
L-1011	APR 1972	Not Determined
F-16	AUG 1978	Not Determined
Space Shuttle	APR 1981	Retired 2011

3. Robert Metzger - Rogers, Joseph, O'Donnell.

The number of high-risk suppliers to the U.S. government, including companies that sold suspect counterfeit product to military and commercial electronics channels, soared by 63 percent from 2002 to 2011. This large and growing trend highlights the need for members of all tiers of the supply chain to implement tighter supplier-monitoring and procurement procedures in order to meet increasingly stringent regulations, according to information and analytics provider IHS.

9,539 suppliers in 2011 were reported for known involvement in high-risk, fraudulent, and suspect counterfeit-part transactions or for conduct identified by the government as grounds to debar, suspend, or otherwise exclude from contract participation. This was up from 5,849 in 2002. In all, 78,217 potential high-risk entities and suppliers to U.S. government agencies, defense contractors and subcontractors, as well as all military and commercial electronics application markets, were reported during the period from 2002 to 2011. The deluge of high-risk suppliers that may have violated regulations or acquisition policies comes at a time when the defense supply chain has been infiltrated by counterfeit parts that present a risk to national security as well as human health and safety. As recently reported by IHS, reports of counterfeit parts in the electronics supply chain quadrupled from 2009 to 2011. Much of the recent scrutiny has come as a direct result of a breakdown in supply traceability and the use of untrustworthy or unauthorized sources for critical components—characteristics not uncommon for the types of suppliers reported.

The combination of rising counterfeit activity and increased government scrutiny underscores the critical need for companies to implement tighter processes and procedures in the use of Trusted Suppliers, Approved Vendor Lists, and Authorized Sources for parts and materials.

2 Senate Armed Services Committee Hearings & China

All Missiles, Weapons Systems and Aircraft are Affected. The question of the day: "How much of our Nation's Defense is infected?"

The Senate Armed Services Committee hearings of November 2011 concerning the serious electronic counterfeit problem within the Department of Defense was initiated in part because of that work, and his own, self-funded, personal investigation into China's overwhelming dominance of the worldwide electronic counterfeit component market. That investigation was done at great personal risk, yet significantly increased governmental awareness as to not only the seriousness of the problem, but the complexity as well. Highlighted by the committee were the potential deleterious implications for our nation's defense. As discussed in the final report released by the SASC Chair, Senator Carl Levin, the findings of the committee were the following:

Conclusion 1: ***China is the dominant source country for counterfeit electronic parts that are infiltrating the defense supply chain.***

Conclusion 2: ***The Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country.***

Department of Defense Actions on Counterfeits

Conclusion 3: ***The Department of Defense lacks knowledge of the scope and impact of counterfeit parts on critical defense systems.***

Conclusion 4: ***The use of counterfeit electronic parts in defense systems can compromise performance and reliability, risk national security, and endanger the safety of military personnel.*** The investigation uncovered dozens of examples of suspect counterfeit electronic parts in critical military systems, including on thermal weapons sights delivered to the Army, on mission computers for the Missile Defense Agency's Terminal High Altitude Area Defense (THAAD) missile, and on a large number of military airplanes. The potential impact of suspect parts on the performance and reliability of defense systems is significant. For example, according to the Missile Defense Agency (MDA), if suspect counterfeit devices installed on the THAAD mission computers had failed, the THAAD missile itself would likely have failed. According to the Navy, had counterfeit parts contained in electromagnetic interference filters failed on an SH-60B helicopter, the aircraft's ability to conduct night missions and surface warfare missions involving Hellfire missiles would have been severely compromised.

Conclusion 5: ***Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.*** Taxpayers should not be burdened with covering the costs of a contractor's failure to detect counterfeit electronic parts in their own supply chain.

Defense Industry

Conclusion 6: ***The defense industry's reliance on un-vetted independent distributors to supply electronic parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel.*** The Committee identified approximately 1,800 cases of suspect counterfeit parts in the defense supply chain. More than 650 companies, each of which relied on their own network of suppliers, supplied those parts. The DoD and defense contractors are frequently unaware of the ultimate source of electronic parts used in defense systems. The suspect counterfeit parts that were used in Electromagnetic Interference Filters (EIF) destined for the Navy's SH-60B helicopters, for example, changed hands five times before the parts were bought by the Raytheon subcontractor who built the EIFs. Those parts originated with Huajie Electronics in Shenzhen, China, a fact that neither DoD nor Raytheon was aware of prior to the Committee's investigation.

Conclusion 7: ***Weaknesses in the testing regime for electronic parts create vulnerabilities that are exploited by counterfeiters.*** The Committee reviewed test reports associated with the approximately 1,800 cases of suspect counterfeit parts identified in the investigation. Those reports reveal wide disparities in testing used by companies in the defense supply chain. Some companies require a range of testing, for example, exposing a part to aggressive solvents to determine whether markings are authentic or de-lidding part samples to examine their die. Other companies, however, are willing to accept parts that have only been subject to basic

functional testing. The investigation also revealed deficiencies in the process used to determine whether and how parts are tested. For example, in the case of the counterfeit memory chips sold to L-3 Communications, the supplier in China selected and sent L-3 Communications' U.S.-based distributor a sample of 18 parts to test. Once those parts were tested and validated as authentic, the China-based supplier sold the company more than ten thousand of the chips. L-3's process at the time allowed the company to accept those chips without additional testing from an independent laboratory.

Conclusion 8: The defense industry routinely failed to report cases of suspect counterfeit parts, putting the integrity of the defense supply chain at risk. The vast majority of the approximately 1,800 cases of suspect counterfeit parts identified in the investigation appear to have gone unreported to DoD or enforcement authorities. For example, in the case of the suspect counterfeit part contained in the Navy's P-8A airplane, Boeing failed to notify the Navy of the problem until the Committee began inquiring about the suspect counterfeits. Similarly, in the case of the suspect counterfeit memory chip contained in the C-27J, L-3 Communications did not notify the Air Force until the day before Committee staff was scheduled to meet with the Air Force program office responsible for that aircraft. Many cases also go unreported to the Government-Industry Data Exchange Program (GIDEP), a DoD program where government and industry participants are required to file reports about suspect counterfeits.

3 SASC Hearing Aftershock

Following the SASC's Report, the 2012 NDAA (National Defense Authorization Act (NDAA) was dramatically beefed up to address the counterfeit problem. In addition to imposing substantial prison sentences, up to life in prison, and significant fines, up to $30 million, for knowingly, or recklessly distributing counterfeit parts resulting in a Class A Mishap (Death or damage exceeding $1 million), addressed the specific requirements that would be imposed on all defense contractors. The largest contractors that were put on notice include, but are not limited to Raytheon, Lockheed Martin, Northrop Grumman, etc., and that those contractors are required to:

- Inspect and test electronic parts
- Abolish counterfeit parts proliferation
- Enable parts traceability
- Use trusted suppliers
- Report and quarantine counterfeit (and suspect) parts
- Identify and rapidly confirm or deny suspect counterfeit parts
- Design, operate and maintain systems to detect and avoid counterfeit and suspect parts

At this writing, with the only exception being Raytheon, the prime defense contractors have failed to implement any significant counterfeit programs, a typical example of their slow pace is Lockheed Martin, the largest Defense Contractor who's corporate policy on counterfeit avoidance is two pages in length, most of which are definitions, and concluding that the focus should be "supplier oversight," an ineffective policy considering the severity of counterfeit migration into the obsolescence part supply chain for DoD Legacy Systems (Fighter Aircraft, Tankers, Missiles, Helicopters, Ships, Submarines, and their related systems and networks).

However, the government is continuing with a deluge of new regulations including those of the 2013 NDAA requiring "Item-Unique Identification Requirements" (IUID). One of the key strategies to deal with the threat of counterfeit parts is to improve marking techniques so that purchasers or users can verify authenticity and to use techniques for item-unique marking that will be difficult for counterfeiters to mimic. Already, there is rulemaking underway on this subject. And, the Defense Logistics Agency (DLA) has launched a controversial initiative to require a specific marking technique for key electronic components. The DLA mandate requires mission-critical devices sold to the DoD to be marked with botanically derived DNA-based materials unique to each supplier. This was accomplished by the Defense Logistics Acquisition Directive (DLAD) 52.211-9074, which applies only to procurements made by the DLA and initially addresses items falling within Federal Supply Class (FSC) 5962 which have been determined ''high risk items.'' FSC 5962 devices are high-reliability and mission-critical.

The focus of the new DLA initiative on this class of parts reflects both their importance to the successful operation of electronic systems in which they are installed as well as a determination that these microcircuits are at high risk of counterfeiting. A goal is to improve the ability of prospective customers and users to authenticate parts without potentially expensive, disruptive or even destructive test methods. Congressional support for the item-unique identification initiative, linked to efforts by DoD to 'combat the growing problem of counterfeit parts in the military supply chain, has injected a new urgency to the pending IUID rulemaking effort. DLA's ''mandate'' requires authentication marking of new purchases of FSC 5692 microcircuits using only the DNA marking technology, ''SigNature DNA,'' provided by one company, Applied DNA Sciences, or its licensees. Although questioned considerably by the SIA, the selection of this method was justified by DLA on the basis of a DLA required R&D program conducted between November 2010 and April 2011, in which approximately 55,000 microcircuits were marked with the SigNature DNA and successfully distinguished in detection and comparison tests. Whether the technology can hold up over time remains unclear.

Kessler Aerospace Solutions
250 North Orange Avenue
STE 1200
Orlando, FL 32801
(850) 889.2555