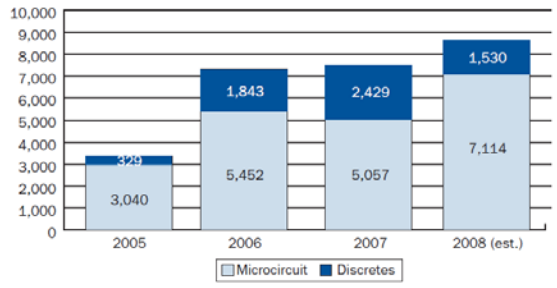
Dealing with Counterfeit and Malicious Hardware

An AIAA Information Paper

ABSTRACT: The American Institute of Aeronautics and Astronautics (AIAA) recognizes that a global economy, pressure on cost and schedule, and limited resources have changed the way that oversight is conducted in support of development, production, and sustainment programs today. While the prime contractor for an aerospace and defense program may be based in the United States, its supply chain is truly global. Beyond programs for the U.S. government or U.S. companies, many foreign contracts require the use of domestic vendors and suppliers in support of the project. This further complicates the ability of companies to verify the integrity of items provided to them. On the commercial front, the move to outsourcing maintenance, repair, and operations (MRO) work has limited the oversight of companies contracting the work as well as those agencies responsible for overseeing the adherence to requirements, such as the FAA. Considering the growing reliance on foreign vendors and MRO companies to provide hardware, software, and maintenance services, the impact on safety, reliability and national security implications must be addressed.

BACKGROUND: Increasingly cost-conscious program management, pressure on profit margins, and substantial penalties for missed or late milestones have resulted in efforts to reduce cost and schedule impacts wherever possible. An increased reliance on a global supply chain has also taxed the ability for companies and agencies to verify the integrity of work and the authenticity of hardware. A 2010 report by the Department of Commerce Bureau of Industry and Security found serious flaws in acquisition, verification, and testing, and in the overall industry/government process for identifying and reporting counterfeit or malicious electronic hardware. As noted in Figure 1, there has been a considerable increase in the number of counterfeit incidents being reported, and this estimate is likely to be conservative, as not all incidents of counterfeit parts are reported.

Figure 1: Increase in the Rate of Total Counterfeit Incidents at OCMs (DOC Study, Figure II-4 Total Counterfeit Incidents – OCMs [2005 – 2008])[10]



Source: The U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009

When considering the impact of counterfeit or malicious hardware, the GAO (GAO-10-389) says that counterfeit items "…have the potential to seriously disrupt the Department of Defense (DOD) supply chain, delay missions, and affect the integrity of weapon systems." Since 2006, the Missile Defense Agency (MDA) has dealt with seven instances of counterfeit parts on six different assemblies that involved nearly 1,300 parts. In many cases, these were the result of procuring parts from unauthorized distributors.

Beyond the impact to national security assets and system readiness, there is the concern over the safety and security of commercial airlines, flight systems, and networks, including Air Traffic Management (ATM). A 2008 incident investigated by the FBI highlights the threat faced by procuring hardware even from trusted suppliers. Counterfeit CISCO hardware originating from China was sold by Gold/Silver partners to numerous U.S. government, military, and intelligence agencies. The concern of the FBI is that the counterfeit equipment may be state-sponsored to aid in accessing otherwise secure systems. As

stated in the FBI presentation: “The threat is real. Compromised hardware of potentially hostile foreign origin sits within secure networks of the U.S. government, military, and intelligence services.” As airliners and our ATM systems move to cloud computing and greatly expand the use and incorporation of software and networks systems, the threat of a breach that could compromise the safety and integrity of an airplane’s control system or of FAA radar support needs to be addressed.

In addition to systems being compromised through electronic hardware, there is a growing concern over the safety of mechanical parts routinely replaced on aircraft. In 2007, the FAA warned about the risks of outsourcing maintenance, with the FAA itself estimating that some 520,000 counterfeit parts make their way into aircraft each year. The FAA’s Suspected Unapproved Parts Program (SUP) has identified instances of counterfeit aviation parts, as well as fake data plates and history cards to make old parts look new. With limited ability to monitor and regulate foreign repair shops, there is a significant risk of a “revolving door” for used parts being reused and passed off as new parts to exist in the MRO arena.

There is no silver bullet when it comes to dealing with counterfeit or malicious hardware. Issues begin with the fact that there are multiple definitions for “counterfeit” over different organizations. The difficulty in capturing the full impact of counterfeit items on the industry is increased by the fact that not all instances of counterfeit parts are reported. This stems from both a concern over loss of confidence in products from companies as well as no requirements or method for centralized reporting. In response to these issues, AIAA has several recommendations intended to help address growing concerns over safety and reliability concerns.

AIAA recommends a standardized definition for “counterfeit” that will be recognized by all impacted organizations and agencies. This definition, in conjunction with a centralized federal reporting mechanism for collecting information on suspected/confirmed counterfeit parts, would allow for a better understanding of the scope of the problem as well as increase awareness of vendor or parts issues.

Along with a definition and centralized reporting site is the need for increased, possibly mandatory, reporting of instances of malicious or counterfeit hardware. Improved quality assurance methods and use of technology could detect corrupt parts *before* they make their way into the hardware, thereby helping reduce the perception of finding issues *after* the failure or breach has occurred. Industry adoption of technologies such as DARPA’s Integrity and Reliability of Integrated Circuits (IRIS) could help with early identification and removal of compromised items from the supply chain.

Getting even further out in the procurement process would be to address the creation of an “Approved/Qualified Suppliers List” as recommended by Society of Automotive Engineers (SAE) standard AS5553. Allowing procurement to only occur with approved vendors would not fully eliminate the issue but would result in a reduced set of vendors required to be monitored. Testing and screening of items could also be pushed to the supplier, meeting DOD or commercial standards, and providing validation of parts prior to being received and incorporated. Holding vendors accountable for items that they procure must also be part of the acceptance process.

This issue threatens to only grow in scale and impact as challenges to cost and schedule push for even more savings. Testing, procurement, and communication/sharing will need to be improved to allow for an already taxed system to work smarter, not just harder, in addressing this safety and security threat.