

Extent of problem unknown

**FAKE PARTS ARE SEEPING INTO MILITARY AIRCRAFT
MAINTENANCE DEPOTS**

Date: March 28, 2008

An unknown number of counterfeit aircraft parts are being fastened into U.S. military weapon systems after infiltrating supply depots, posing new safety risks and potentially driving up maintenance bills by hundreds of millions of dollars annually, according to Pentagon officials.

This practice is an unintended consequence of two converging trends: globalization and Defense Department acquisition policies instituted in the 1990s that encourage use of commercial-off-the-shelf technology, according to Robert Ernst, head of aging aircraft studies for the Navy.

“This is one of the emerging threats to our supply chain. It’s one of the things we call a disruptive technology,” said Ernst during a March 20 interview. “We’re getting so many changes, because we’re in a global economy, [that] we have to manage things a little bit differently, and it really is turning our acquisition process and supply process on its ear.”

Ernst -- along with several other military safety officials who wished to remain anonymous -- worries that the potential of fake parts in the inventory is so high that some aircraft may contain numerous counterfeit parts, ranging from microprocessors to fasteners. This, they argue, opens the door for disaster since military parts must be able to withstand shock, vibration, electromagnetic and temperature stress levels far greater than their commercial counterparts.

“If you get a flood of counterfeits going in, if you have multiple failures on an old weapons system with poor reliability, it doesn’t take a lot of ‘what ifs’ to have a serious reliability -- and possibly a safety-impact,” said Ernst.

“If I have a part that gets into a weapon system that not only doesn’t work, but fails prematurely or it has adverse impact, then that’s a safety issue and I really get upset,” he added.

Ernst estimates that such components are leading to a 5 percent to 15 percent annual decrease in weapon system reliability based on studies by the Aerospace Industrial Association.

“I know the Navy spends about \$1.4 billion a year on depot level repairables. A 10 percent increase. That’s a big chunk of change,” said Ernst.

However, since tiny computer chips and fasteners are incredibly difficult to inspect, the true percentage of counterfeit parts entering U.S. inventories is still unknown.

The Pentagon has acknowledged the importance of making sure all aviation parts come from trusted vendors, but has not committed the resources needed to fight the problem effectively, in-part because no one has studied the true size of the problem, argues Ernst.

“We are getting service participation from DLA [Defense Logistics Agency], from OSD [Office of the Secretary of Defense], from the Navy, but we’re still not getting the right level of senior involvement, because I don’t think we’ve defined the problem,” said Ernst. “We’ve got some people from OSD but we don’t have [senior leaders] pushing it.”

Several private groups -- led by the Aerospace Industries Association -- have taken note of the issue and are beginning to study the effects of a globalized economy on aircraft safety. The Commerce Department also has initiated a study into counterfeit aviation parts along with NASA and the Federal Aviation Administration, added Ernst .

“We are conducting a study to try to measure the penetration of counterfeit electronics into DOD supply chains, including part supply chains for military aviation. We have no statistics at this time and lacking that we are not able to speak with great authority on the depth and breadth of the problem,” reads a March 27 e-mail from Commerce department spokesman, William Houston.

At press time,(March 27), numerous Air Force and Pentagon officials have not returned multiple phone calls and e-mails asking for comment. A DLA spokeswoman told *Inside the Air Force* that she was unaware of any agency studies on counterfeit parts.

Ernst, however, pointed out that, in 2007, the Air Force disbanded its aging aircraft mitigation office at Wright Patterson Air Force Base, OH, and spread its responsibilities -- including the study of counterfeit parts -- amongst Air Force Materiel Command’s three Air Logistics Centers.

“We need to quantify [the problem] and we need to get in senior-level acquisitions people, to flow this down to our programs, not just as another stupid rule, but here’s what we need to look for” to strike the balance between safety and cost effectiveness, said Ernst.

So far, counterfeit parts have been showing up primarily on supplies for older aircraft, as the military has shifted toward buying lower-cost, civilian technology for some -- non-safety critical -- systems, instead of buying parts designed to military specifications, which come at a far higher cost in money and development hours.

While this commercial approach has, in some cases, lowered procurement costs and streamlined the bloated acquisition process, it also has opened the door for enterprising middlemen around the globe to sell a range of false parts to government vendors.

Brokers sometimes purchase out-of-production parts from black market sources -- most often in Asia -- and resell them to government suppliers or sometimes directly to the military for installation on older aircraft, according to Ernst.

Some of these parts are shoddy, reverse-engineered copies while others are used parts that have been repackaged; none are up to DOD safety standards. Ernst has discovered “new” replacement parts that had only 30 percent of their service lifetimes left; other times the parts did not work at all.

“There’s a real opportunity to make money in the counterfeit parts area,” said Ernst.

In January, two Texas businessmen were indicted for supplying DOD, other government agencies and defense contractors with what the Pentagon thought were Cisco Internet cards. It turned out that the cards were Chinese-made knockoffs. The men allegedly put Cisco labels on the cards, wrapped them in Cisco packaging and then sold them to the government. The fraud only was revealed when a Chinese source tipped off the FBI.

During a separate Navy investigation into lead-free parts, Ernst and his team looked up a supplier’s business address, only to find that it was a private home in Bakersfield, CA.

“People were just seeing that: ‘Hey, I can buy parts off [the Internet] and I can sell them for a mark-up to the government,’” said Ernst. “You can buy commercial parts real cheap and generally the cost of a military industrial part is about two or three times what a commercial one is, and you could say ‘sure it is’ [a military-grade part] and [DOD] probably wouldn’t catch that.”

Another issue is the threat of malicious software -- known as malware or spyware -- being inserted into counterfeit microcircuits that fifth-generation fighter jets, such as the F-22A Raptor and F-35 Lightning II, rely on far more than their predecessors.

In September 2007, the Defense Science Board published a report stating that the Raptor’s systems are among the best-protected against a software attack since its commercial-off-the-shelf systems exceed DOD security standards and the only foreign software in the Aircraft is kept separate from all other systems on the plane (*Inside the Air Force*, Nov. 2, 2007, p1).

However, the report cautions that the DOD microchips are an extremely attractive target for the world’s best -- and often state-sponsored -- hackers, and that the likelihood they will develop new ways to infect commercial microchips used by the military is very high.

“The problem is serious indeed . . . exploitable vulnerabilities may lie undetected until it is too late,” the report states. “Because of the high degree of interconnectedness, penetration of one application could compromise many others.”

The report goes on to say that attributing malicious code is extremely difficult because it can simply look like an error in the code’s script, making it easy to deny harmful intent. This limits legal actions that may be taken, including removing the chip’s producer from the supply chain.

The report concludes that “current systems designs, assurance methodologies, acquisitions procedures and knowledge of adversarial capabilities and intentions are inadequate given the magnitude of the threat.”

The notion that the scope of the counterfeit problem has yet to be revealed was backed up by numerous calls to congressional staff and researchers familiar with the defense acquisitions process. None had heard anything about counterfeit parts in military aircraft.

“This is a constant source of concern, and I don’t think that anything out of the ordinary would be done about it unless some problem pops up. It’s just the standard operating procedure to verify the parts that you get,” said Dan Else, aviation researcher with Congressional Research Service, adding that he has heard nothing to suggest that the standard vetting procedure is not working.

Nonetheless, “counterfeit parts in aviation pops up occasionally . . . and it seems to almost always be the case of somebody being unscrupulous and faking the serial numbers on the parts, faking the documentation on [parts’] lineage” to get the parts past the vetting process, said Else. “Of course this is nothing that would be advertised, and I’ve got no insider information on it.”

A major challenge to setting up a system to track counterfeit parts is getting all necessary members of government and industry together to create one blueprint for dealing with counterfeit parts, according to Ernst.

Most important is creating a set of industry-wide standards designed to identify which parts are most frequently counterfeited, and then developing procedures to vet the origins of parts and hold suppliers accountable for ensuring the quality of their goods.

The other is figuring out how to implement quality standards without sacrificing the benefits of buying commercially available parts.

“Can we convince the policy and legislative people and the American people as a whole that we’re not just adding extra tests to gold-plate certain things, but that we’re trying to strike a good balance?” said Ernst. “That’s your challenge. Because we’re very good in government at adding requirements, and adding requirements adds costs.” -- *John Reed*