Sniffing out counterfeit electronics

September 7 2012, by Molly Mcmillin

At Integra Technologies, inspectors spend their days studying electronic parts to see if they are counterfeits.

Using high-powered microscopes, they look for signs that an integrated circuit, or chip, has been remarked, reworked or otherwise tampered with.

About 10 percent to 20 percent of the parts tested for counterfeiting turn out to be bogus.

It's high-stakes work requiring the skills of a detective.

Detection has never been more important, said Mark Marshall, Integra Technology's vice president of engineering.

Many of the chips are to be used by defense contractors or aviation manufacturers. Some may be installed in radars, missiles, flight control systems, communications systems, engine controls or in other critical applications.

Their failure could be not just detrimental but deadly.

"This counterfeit stuff is an ugliness that's out there," he said.

Integra Technologies' customers include defense contractors such as Boeing, Lockheed Martin, Northrop Grumman, Raytheon and Honeywell.

As counterfeiting has become more common, testing parts' authenticity is a growing portion of Integra Technologies business.

It's one of the major labs in the U.S. performing such work.

"We're busy," Marshall said.

The company, located in northeast Wichita, also conducts a variety of other types of semi-conductor testing, qualification and related technical services for a variety of industries.

Counterfeiting has gained national and congressional attention.

A yearlong U.S. federal probe concluded this year found 1,800 cases of bogus parts, totaling more than 1 million actual devices, used during 2009 and 2010.

More than 70 percent of the parts tracked were traced to China.

The investigation found bogus parts were used in military systems, including in thermal weapons sights delivered to the Army, on mission computers used on high altitude missiles and on a number of military airplanes.

For example, last year Raytheon Co. alerted the Navy that electronic parts suspected to be counterfeited had been installed on three filters used in a night vision system called Forward Looking Infrared, or FLIR. The FLIRs were installed on the Navy's SH-60B helicopter and used for anti-submarine and anti-surface warfare and surveillance.

A failure would compromise the pilot's ability to avoid hazards and identify targets and limit the helicopter's ability to be deployed in night missions, the federal investigation said.

Counterfeiting threatens national security, the safety of U.S. troops and American jobs, Sen. Carl Levin, D-Mich., said in a statement in May following the release of a report by the Senate Armed Services Committee, which launched the investigation in March 2011.

Defense contractors usually have the biggest problem, Marshall said.

They buy small volumes and need chips to last much longer than when the chips are used in consumer applications.

A fighter jet, for example, has a long lifespan and has to be supported for decades.

The problem arises when manufacturers need replacement parts, but they're no longer made, or the manufacturer hasn't made them for several years.

So they turn to brokers or independent distributors to find them.

But those parts often have changed hands multiple times, and brokers may know little about the source of the parts they buy.

Ten years ago, there wasn't a problem.

Now, brokers and manufacturers must take precautions.

"It's become a minefield," Marshall said. "Even the best brokers still end up with counterfeit parts from time to time."

Integra Technologies, an independent laboratory, works with manufacturers and with the brokers to determine the authenticity of the chips before a contractor or manufacturer buys them.

Integra does an in-depth inspection, looking for markings and checking whether parts numbers match up and the correct components are inside.

Besides visual inspections, Integra Technologies can also electronically test parts to see whether they work as expected.

Like CSI, inspectors look for clues.

"We're trying to analyze the crime," Marshall said.

It takes knowledge of what the part looked like originally.

Sometimes a legitimate part can appear counterfeit.

Sometimes counterfeit parts look good but don't work, Marshall said. Or they work, but they don't perform all the functions they're supposed to.

Other times, they work fine, but the failure rate is high.

At times, the problem isn't with counterfeiting, but with the way the chips have been handled and stored over time, he said.

Counterfeiting activity began with "e-waste," from old computers, monitors and other electronics.

The idea was to recycle and save them from a landfill. So recyclers bundled up the old electronics. Much of it went to China.

"That's what started this whole mess," Marshall said.

In the past five years, the problem has exploded - and counterfeiters have gotten smarter and harder to catch. They've improved their techniques and methods to avoid detection.

"They're much more sophisticated now," said Integra Technologies President Becky Craft. "They know people are looking."

Counterfeiters do whatever's needed to sell the parts.

"They do all kinds of things to try to legitimize them, making new paperwork and redoing whatever they need to do to the parts to make it look right," Marshall said. "They will fake everything ? the materials around the part, the boxes, the certificates of compliance. ... They make them to look like they were new and had never been used."

Sometimes they make the parts look too good, Marshall said. A 10-year-old chip, for example, should show some signs of oxidation.

Other times counterfeiters seed a shipment of counterfeit parts with legitimate ones.

Marshall serves on national and international committees to help develop processes to check for bogus parts and set standards.

Counterfeiting is a dangerous minefield for the brokers, who stand to lose money if they buy bogus parts, Marshall said. It's also expensive for the manufacturers that spend millions of dollars on testing. They also get hurt should they install bogus parts, then have to recall the equipment.

"There have been cases where they've gotten out into the field," Marshall said of the bogus parts.

Doing a recall is "staggeringly expensive," he said. "These are not going into cheap products."

In testing, there's a lot of pressure to make the right call on whether a part is bogus.

"A broker is mad if you say it's counterfeit and it's not," Marshall said. Then the customer doesn't want it.

"Manufacturers are mad if you say it's legitimate, and it's not. So you have to be right."

In addition, the parts can be rare and valuable.

They may be the last of their kind that exist, adding to the pressure to make the right call.

The U.S. government is focusing on the issue, researching cases and following evidence trails.

Some counterfeiters and dishonest brokers have gone to jail, including executives from a major counterfeiting company operating in southern California.

Some of the parts made their way into critical military applications and started failing, Marshall said.

Marshall doesn't see a solution in the short term. For the counterfeiters, "there's too much money to be made," he said.