THE REAL DEAL

With RIF and SBIR support, a new detection system undercuts a flood of electronic counterfeits

For most people, the subject of counterfeit products evokes visions of sidewalk vendors selling Nike replicas and Louis Vuitton knockoffs. Luxury goods are the most counterfeited products in the world, posing at least an ethical problem if not an economic one. But, as it turns out, electronic counterfeits are closing the gap on major black market products, and when it comes to that industry, the stakes are much higher. A counterfeit electronic part can affect public health. It can impact warfighters who might be using compromised equipment. It can pose huge risks to national security.

In 2012, a year-long Senate Armed Service Committee investigation found counterfeit parts from China on the Air Force's largest cargo plane, as well as in a Navy surveillance plane and in assemblies meant for Special Operations helicopters. The counterfeits were discarded parts that had been refurbished and resold back into the United States supply chain. The investigation report highlighted the risks and challenges this rash of counterfeit goods pose to the country.

"The failure of a single electronic part can leave a soldier, sailor, airman, or Marine vulnerable at the worst possible time," the report said. "Unfortunately, a flood of counterfeit electronic parts has made it a lot harder to prevent that from happening."

But it's not just that the quantity of counterfeits was rising in the U.S., it was that new levels of sophistication made them more difficult to detect. Traditional approaches through sample inspection and electrical and visual testing just weren't cutting it anymore.

"The counterfeiters and other people trying to get these bad parts into the systems, they're able to counter those tests," said Walter Keller, CEO of technology company Nokomis, Inc., based in Charleroi, Pennsylvania. "There are ways you can fake an electrical test to make it seem like a part is in good condition when it's really degraded to the point of not functioning. There are ways to remake it so that a visual inspection is not going to detect that it's not authentic."

To combat this problem, Nokomis, Inc. created the Advanced Detection of Electronic Counterfeits (ADEC) program, a real-time, non-invasive hardware system that can immediately detect counterfeit parts. The system was developed through support from both the Small Business Innovation Research (SBIR) program and Rapid Innovation Fund (RIF), a program established to help companies get past the "Valley of Death" stage between prototype and actual production, and rapidly insert urgent technology into programs with specific defense needs.

"We're pleased that the RIF program and the SBIR program were available to mature the technology for these applications," Keller said. "We're getting real data on real parts and real systems that are critical to the nation."

ADEC takes up about the same space

as a desktop computer setup and features two pieces of equipment: a touchscreen box about the size of a small microwave, called a Signature Analyzer, and a small A-frame test chamber called an Integrated Antennae Enclosure (IAE). It works with about the same kind of press-button ease as a James Bond gadget built in the Q laboratory. Electronic chips from parts that need testing are inserted into a small drawer in the IAE and enclosed in the chamber. It only takes one operator to select the type of part that's being tested and then press the scan button on the screen. The IAE collects the low power radio frequency signals coming from the chip or part in question, and sends the data to the analyzer box. The operator can see the screen saying "scanning in process" as it compares the frequency of the item in question to frequency of what it should be—a frequency that's stored in the database, much like how a fingerprint analysis system compares prints. Within just five seconds, the screen shows either a green display that says, "Authentic Part Confirmed" or a red display that says, "Suspected Counterfeit Part Detected." When the operator gets the red display, the supplier is informed and the part is taken out of the supply chain to be assessed.

"That funding from both the RIF program and the SBIR program were critical to get to the point where we are today," Keller said.

While some electronic parts are counterfeited to make money off cheap discards, other counterfeits are made with more malicious intentions—to interfere with critical systems or acquire government intel, which are major cybersecurity concerns. The ADEC system combats both problems. It scans electronic components to determine two things: First, whether they are authentic or counterfeit, and second, if they are degraded or not functioning properly. So it's both detecting malignant counterfeits and also providing quality control.

The key to ADEC is the particular technology that works like a fingerprinting system. All electronics have an unintended and unique electromagnetic signature, a radiated emission that is distinct from a transmission signature.

"When I was younger, I remember my grandmother would turn on the vacuum cleaner or the blender and we'd see the static go across the TV," said Eli Polovina, VP of operations at Nokomis. "That's the unintended feature coming off of the electronics."

ADEC doesn't analyze the content of a system, so even in the detection process, sensitive information isn't being compromised. It's purely looking at the design, function and construction of the part.

"It's using that as the baseline, so if there are any changes—if the part's degraded, if it's been plucked off another board and tried to be resold as new, or if it's simply not designed to do what they sold it for—we're able to see that based off the actual internal workings of the chip," Polovina said. "It's virtually impossible to fake this. In order to get that signature exactly like the authentic, you would basically have to recreate the authentic, so at that point it doesn't matter if it's a counterfeit or not; it would function the same as the original one."

When Nokomis was founded in 2002, the company understood both the fundamental dynamics of electronics and the potential for capturing those unintended signatures. That's the problem it worked to solve—but it wasn't easy. Even while people in the electronics industry knew the signature existed, no one was certain how to capture and utilize it. At the time, Polovina said, organizations like the Defense Advanced Research Projects Agency (DARPA), that often worked on these big problems, were skeptical that a sensitive enough technology could pinpoint those signatures.

Walter Keller

The reason it's so hard? The system captures 3 billion data points to measure the frequency of a part—its

unintended signature.

"It's almost like a big data problem that you hear about people trying to solve on the internet," Keller said. "How do you parse through all this data where you're really drinking from a fire hose? It took hours and hours of time spent by some pretty smart people to come up with completely new techniques that didn't exist previously."

The prototype Nokomis created was called the Hiawatha, an ultra-sensitive RF and microwave collection system and the baseline technology that would later support the ADEC system. The ability to detect these electronic signatures led to SBIR funding in 2007 to develop and integrate a system that could confirm electronic devices used as IED triggers at hundreds of meters. In 2011, under another SBIR award, Nokomis incorporated the Hiawatha into other projects.

That same year, in 2011, the Missile Defense Agency (MDA) and the National Center of Defense Manufacturing and Machining met with Nokomis to see if the Hiawatha could be used to detect counterfeits. The company then received SBIR Phase III funding through the newly established RIF program, to design a method to identify counterfeit electronic components and, through the 2014 solicitation, the company received another RIF award to develop a system that allows 100 percent of parts procured by the AF Sustainment Center to be screened at nearly any point along the supply chain.

The technology was successful, but it wasn't very portable; it was housed in a 50 x 18 x 14-foot anechoic chamber. The MDA wanted Nokomis to convert the technology to a desktop environment. Nokomis developed an integrated antennae enclosure slightly larger than a desktop computer and a signature analyzer that used the Hiawatha sensor technology, along with all the other components necessary to make an integrated system work within a desktop space.

The highly portable ADEC system from Nokomis.

Nobody was doing this kind of work before Nokomis, but the success of the sensor technology and the critical need for it made it a surefire candidate for urgent development with RIF funding. Since its implementation, ADEC has successfully detected anomalous parts in critical warfare systems that have since been taken out of inventory.

"That funding from both the RIF program and the SBIR program were critical to get to the point where we are today," Keller said. "If we had gone through a standard R&D process it would have taken several years to get to this point. Within a year we were funded and had the baseline of a system done and ready for testing. You almost can't quantify how much benefit the RIF and SBIR programs provide in terms of technology development for very hard-to-solve problems. Now we have a new technology that's not just a breakthrough in finding counterfeits but is going to be transformative in the diagnostics of electronic part anomalies of many kinds."

Photos courtesy Nokomis, Inc.

Modernization Priorities: Cyber and Microelectronics

RIF Award: 2011 Navy SSPO: "Advanced Detection of Electronic Counterfeits" (N00024-12-C-4516) – SBIR Phase III

RIF Award: 2014 Air Force PEO Space: "Counterfeit / Fraudulent Parts Screening Using Advanced Detection of Electronic Counterfeits" (FA8222-15-C-0008)

Enabling SBIRs: DTRA topic DTRA06-007, "IED Electronic Signature Detection" (Phase II contract: HDTRA1-07-C-0053)

Air Force topic AF071-219, "Remote-Controlled Improvised Explosive Device (RCIED) Detection Identification and Classification Algorithms (RADICAL)" (Phase II contract: FA8650-08-C-1402)

Air Force topic AF093-013, "Automated Analysis of RF Effects Data" (Phase II contract: FA9451-11-C-0143)

The content in this article does not constitute or imply endorsement by the Department of Defense or the Military Service(s) of the provider or producer of the technology, product, process, or services mentioned.