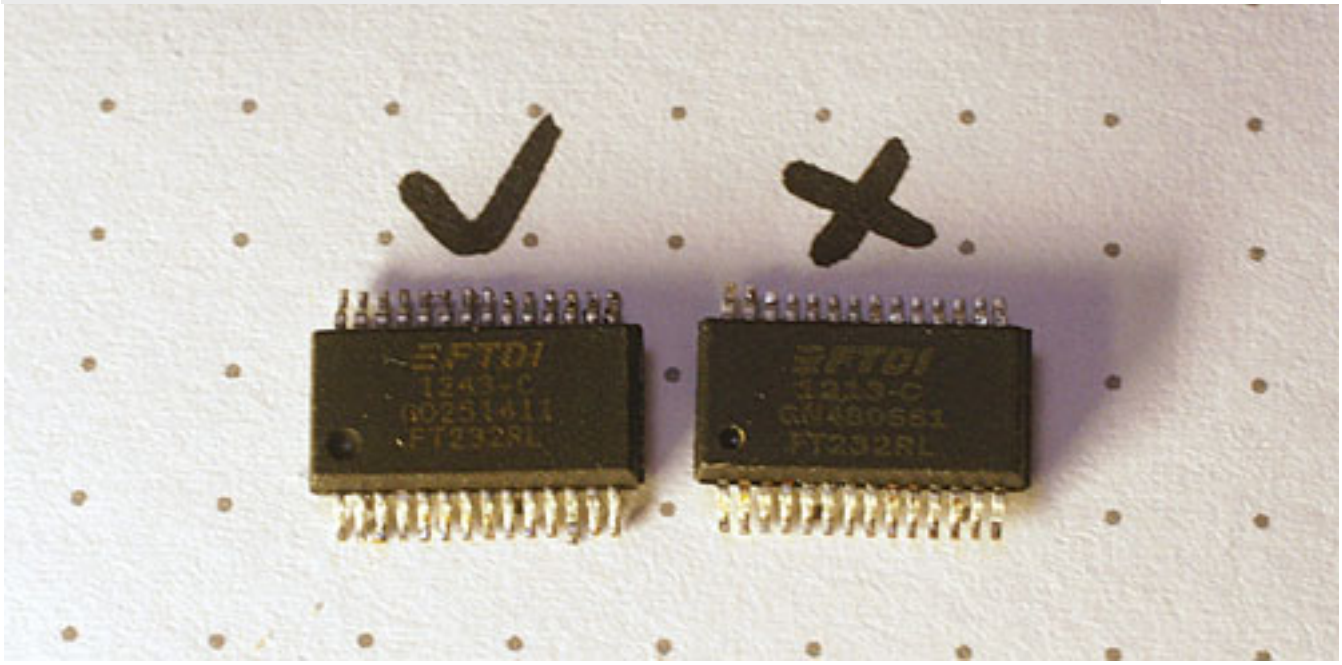
National DEFENSE
NDIA
NDIA's Business and Technology Magazine

E-Waste Export Controls Key to Battling Counterfeiters

March 2016

By Tom Sharpe



A genuine FTDI chip (left) versus a counterfeit FTDI chip (right)

The technology sector and government agencies have been working hard in recent years to combat electronic component counterfeiters, based primarily in China. It's a fight we must win because counterfeit components threaten the reliability of technology critical to our national security as well as our health and safety.

The risks were first documented in a U.S. Senate Armed Services Committee study that identified more than 1 million individual suspected counterfeit electronic parts in weapons systems ranging from night-vision goggles to missile control systems. More than 90 percent of the counterfeits were traced to China. Adding to the national security threat, counterfeit microchips can help hackers and cyber terrorists launch attacks.

The threat extends beyond national security to include a variety of products and systems that create public health risks. Counterfeits have been found in all sectors of the electronics industry to include medical and healthcare technologies, airport landing systems, braking systems for high-speed trains and the defense and aerospace industry, according to the Semiconductor Industry Association.

To date, we have seen significant new initiatives to improve detection of counterfeiters as they enter the supply chain. The Defense Department has implemented many newer procurement policies and contract requirements with suppliers designed to ensure delivered raw components or components within delivered systems are authentic parts, which can be traced to an authorized distributor or manufacturer.

In the cases where obsolete electronic components are required, which are no longer in production and must be procured from non-authorized sources, there are significant requirements for both authentication and functional testing.

This is a critical initiative, but it's not perfect. Counterfeiters are a resourceful enemy adept at finding ways to subvert these measures.

Many larger U.S. companies whose products are being counterfeited within China have been hiring investigators based there to crack down on counterfeiters. Yet a recent Associated Press investigation details how fraud and corruption are undermining this approach. In some cases these investigators "were themselves manufacturing or selling counterfeit versions of their clients' own goods."

It is clear we are battling an enormous, well-funded criminal enterprise located in a country that historically has turned a blind eye to the intellectual property rights of others.

Emerging technologies will prove to be giant steps forward in detection. The Defense Advanced Research Projects Agency is funding the development of new technologies aimed at detecting counterfeits in the supply chain. Independently, Battelle Labs has spent the past several years and many millions of dollars developing the Battelle Barricade detection system.

Enforcement also plays an important role. The Department of Justice has recently secured convictions and/or guilty pleas of individuals knowingly trafficking in counterfeit parts aimed at U.S. military applications.

These are some of the many challenges underscoring how anti-counterfeiting measures must constantly evolve and adapt. All of these efforts are part of the solution. However, they share a common weakness — they only take aim at counterfeits once they are already in the supply chain. We must also attempt to prevent counterfeits by cutting off a large portion of the raw materials needed to produce them.

Counterfeiters use e-waste exported from our own shores as a primary source of cheap raw materials with which to create counterfeits. The United States is the world's largest producer of e-waste, and much of it ends up exported to developing countries for cheap processing.

As a result, counterfeiters thrive on a vicious cycle in which we export e-waste that comes back to undermine national security. As Pogo said, "we have met the enemy — and it is us."

Several years ago, I got a first-hand and unforeseen opportunity to see how it works while on a business trip to China, where the counterfeiting industry is centered in Guangdong Province. Components are pulled from piles of e-waste by workers in

backyards and open-air dumps. Circuit boards are heated to "reflow" the solder and make components easier to remove. Parts are washed in rivers and laid out on sidewalks for sorting.

The actual counterfeiting process is equally harsh. Parts are sanded or put through an acid bath, then re-coated and re-marked through a process called "blacktopping." This process exposes these highly sensitive chips to moisture, static electricity and other damaging conditions. Acid baths used in some remarking processes can eat away at a microchip's internal parts.

A purchasing official may believe they are buying a brand-new part that has been manufactured in a pristine, clean-room environment. What they get instead is a counterfeit, pulled from e-waste then re-marked. It is virtually impossible for even a trained eye to detect the finished counterfeit.

The United States needs to fight counterfeiters with every weapon available to us. Yet we continue to allow export of untested, nonworking e-waste that provides them with an ample supply of cheap raw materials. U.S. e-waste exports are massive — nearly 800,000 tons annually by conservative estimates.

Our trade laws typically prevent exports that undermine our national security. E-waste exports clearly fit that description, and Congress must act to amend current trade policy.

To go on the offensive, Congress must enact legislation that requires domestic recycling of untested, non-working e-waste. This approach keeps these materials within our borders and out of the hands of Chinese counterfeiters. U.S. e-waste recyclers are well equipped to do the job with secure systems already developed and in use at many processing sites around the country.

There is no magic bullet in the fight against counterfeiting. Improving supply chain procedures, improving detection and increasing enforcement are all important parts of the solution. To win the battle, we need a smart, "all-of-the-above" hard-liner strategy that most certainly includes common sense export reforms on these e-waste export feedstocks.

Tom Sharpe is vice president of SMT Corp., an electronics distributor, counterfeit mitigation and electrical testing laboratory for the defense and aerospace industry.