Counterfeit components: Risky business

Story

September 11, 2020

By Marti McCurdy

The challenge of microelectronics counterfeit prevention is to detect fake OEM parts, but what if the part is an actual OEM's part and yet still counterfeit? Not only is it possible, it's common. The most counterfeited product in the global microelectronics market is not always a fake. Very often it is a true OEM original but has been altered and is not suitable for the full requirements of system performance and use in a critical military system.

How can one identify questionable microelectronic parts? How can one know if the speed grade – or any other binning parameter purchased – will work as marked for any product not bought through an authorized distributor?

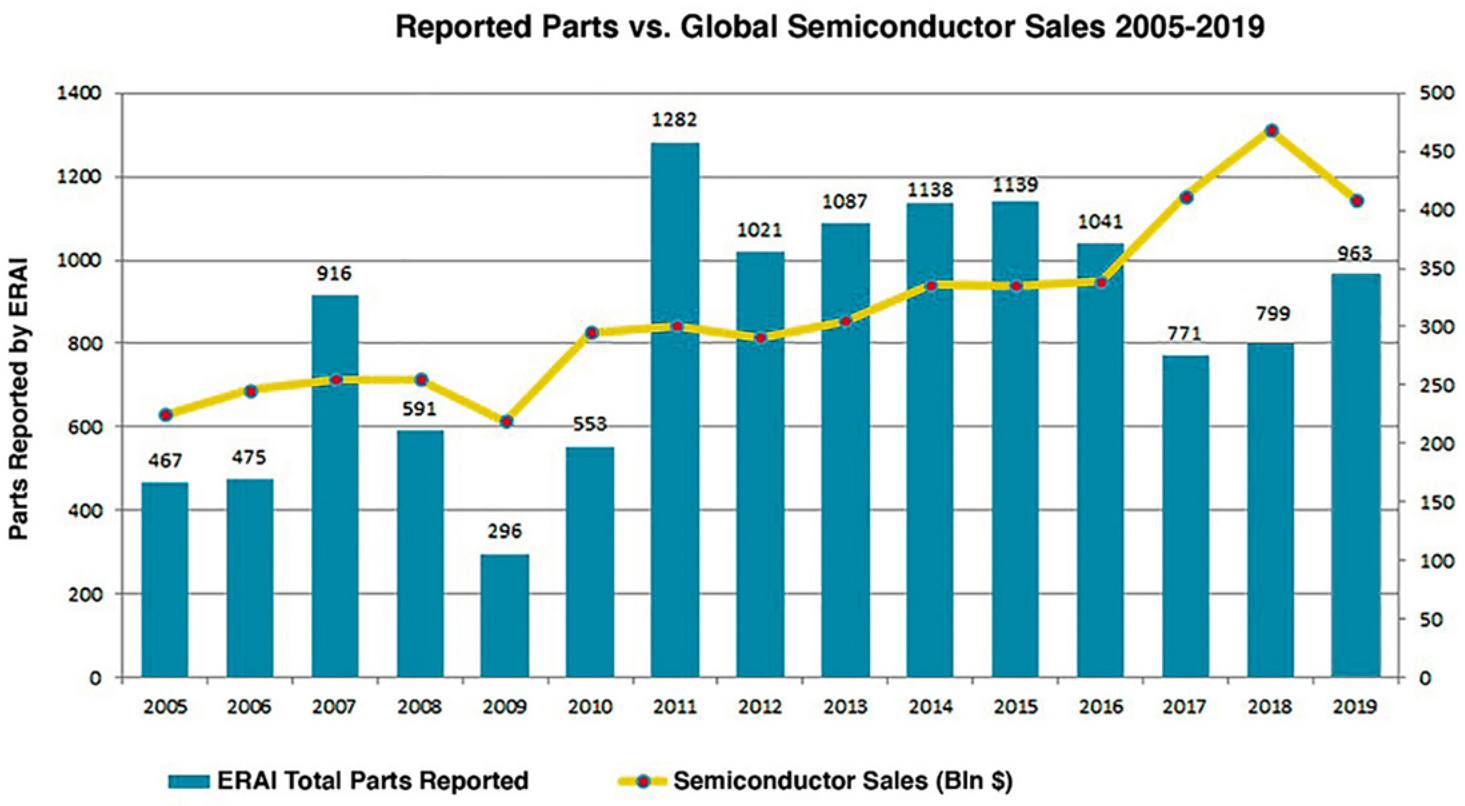
For example, take an FPGA [field-programmable gate array] that has four speed grades. Speed grade #1 is priced at $350.00; speed grade #2 at $3,500.00; speed grade #3 at $35,000 and so on. In this example, the core/parent part numbers are consistently the same, with the last -XX being the unique identifier for binning (ex: SE123456789-01). The counterfeiters take the speed grade #1, change the last -01 to an -03 marking, and ostensibly make it a speed grade #3.

While it is an original, it is just incorrectly marked, resulting in an inadequate product for the buyer and a large profit margin for the counterfeiters. This defect cannot be detected through standard methods of counterfeit detection; it can only be detected through a thorough electrical test of the device. It must be a thorough test, not a continuity test, not a simple rack-and-stack test, and not a test from a lab that lacks the instruments to test the device at its peak ratings. This identification requires a true test using automatic test equipment, at speed, full throttle.

This caution applies to all components but is more prevalent and undetectable where components contain high-speed SerDes [serializer/deserializer] and high-performance DDR3 and DDR4+ memories.

Real cost of counterfeit components

Electronic parts counterfeiting was estimated to have cost U.S. semiconductor manufacturers around $7.5 billion in 2018; 69.9% ($5.24 billion) of those fake parts were integrated circuits (ICs), according to ERAI. (Figure 1.)



[Figure 1 | Reports of nonconforming or suspect counterfeit semiconductor parts vs. sales, 2005-2018. Graph courtesy ERAI.]

Even the U.S. Department of Defense (DoD) supply chain is vulnerable to the risk of counterfeit parts: The DoD estimates that as much as 15% of all spare and replacement parts for military electronics turn out to be counterfeit.

ICs are especially difficult to protect from counterfeiting because often they come from an overseas manufacturer and are resold by several subcontractors before a large military supplier like Lockheed Martin or Boeing embeds them in technology that it then sells to the U.S. government.

In 2018, Operation Chain Reaction (OCR) – a coordinated effort led by Homeland Security Investigation (HSI) along with the Intellectual Property Rights Center (IPRC) and 16 federal law-enforcement agencies – initiated 24 criminal investigations, conducted 15 criminal arrests, and helped secure 18 indictments and seven convictions. The 2018 OCR effort also performed 68 counterfeit-goods seizures, with the contraband valued at approximately $4.9 million. OCR is primarily focused on microelectronics, in part because they are used in virtually every system and they are easy to counterfeit. Counterfeit microelectronics pose a significant health and safety threat, with the use of substandard parts potentially having catastrophic outcomes: delayed DoD missions, unreliable weapons systems, imperiled warfighter safety, and lowered integrity of sensitive data and secure networks.

The U.S. Naval Air Systems Command (NAVAIR) Aging Aircraft Program estimates that as many as 15% of all the spare and replacement microchips the Pentagon buys are counterfeit. Incidents involved in counterfeit parts include a naval destroyer that failed a training launch of a Tomahawk missile; counterfeit components installed into a communications array of Coast Guard helicopters; and the discovery of counterfeit ICs in the navigation and targeting program of U.S. Navy F-14 Tomcat fighter aircraft.

How it's done

In 2019, Rogelio Vasquez, the owner of PRB Logics (Costa Mesa, California) – which billed itself as a "distributor of obsolete electronic components," – admitted to trafficking more than 9,000 integrated circuits with a total value of $894,218 between July 2009 and May 2016. Over seven years, Vasquez bought old, used, and previously discarded ICs from Chinese suppliers; these parts had been refurbished and marked with counterfeit logos. The circuits had undergone a process known as "blacktopping," in which existing markings on old, used, or discarded components are sanded off and remarked. The devices were painted and outfitted with altered dates, lot codes, and countries of origin and sold as new. Vasquez admitted that he instructed a Chinese testing laboratory to provide two reports on his components – one accurate report and one "sanitized" – that excluded any results that indicated the components were used, remarked, or in poor condition. Vasquez sold the counterfeit electronics as new parts made by manufacturers such as Xilinx, Analog Devices, and Intel. In 2012, Vasquez acquired and sold counterfeit circuits from China and sold components to a U.S. defense subcontractor that later ended up in a classified Air Force weapon system.

In another well-known instance, from February 2007 through April 2012, Peter Picone of Massachusetts purchased millions of dollars' worth of integrated circuits bearing counterfeit markings of approximately 35 major electronics manufacturers – including Motorola, Xilinx, and National Semiconductor – from suppliers in China and Hong Kong. Picone resold the counterfeit integrated circuits to domestic and international customers, including to defense contractors that intended to supply them to the U.S. Navy for use in nuclear submarines and other critical applications.

One more example: In 2015, federal agents arrested three Chinese nationals for crimes that included selling 45 counterfeit Intel microchips to an undercover agent with the understanding the chips would be used by the U.S. Navy for a project involving submarines. Had those parts been

installed in a missile-guidance system, the missiles would either not function at all or would likely not proceed to their intended target; they likely would have struck a completely unintended destination, according to a senior engineer at the U.S. Air Force Research Laboratory.

Detection can be difficult

Counterfeit parts are dangerous not because they don't work outright, but because they nearly work, a condition some refer to as the "walking wounded." They may perform intermittently, not to spec, or not at all. The components can degrade system performance, cause intermittent performance snags or delays, and – above all – slow memory components and throttle down all other chips on the system. Problems may not even arise until the parts have been in the application for some time. Counterfeit parts can fail at any point; they may work during testing and use where conditions are ideal, but fail under extreme environments, wider temperature and voltage ranges, or under stressed performance conditions such as those in military and space applications.

Secure sources

Of the electronic components being counterfeited, Xilinx is known to be the most copied brand with more than twice the number of "fakes" as compared with other manufacturers, according to reports from the ECIA [Electronic Components Industry Association]. How do companies make sure that their parts are what they say they are? Makers and distributors must manage their supply chain very tightly, perform in-house testing to qualify components, and assume full ownership of failures.

Control is the key: As the OEM guarantees supply chain and component integrity, OEM-accredited and OEM-authorized testing and screening assures that components are suited for their performance, that they are not "walking wounded," and that they are undamaged by improper testing and handling of the components post-sale by labs that may not have the proper diagnostic resources to even power up the devices as required.

Testing the device according to the data sheet, verifying the operational parameters and function at speed or temperature, and the explicit description of the part is paramount. Short of all of these, the end product is at risk, with no recourse and no insurance. Clearly, that's a risk not worth taking, especially when lives are on the line.

Marti McCurdy is the owner and CEO of Spirit Electronics, a value-added supplier of high-reliability components and supply-chain solutions. She is a U.S. Air Force veteran who served the military and the space industry around the world throughout her career, starting with working on jamming radar systems for fighter jets to being a Level 3 ultrasonic specialist performing ultrasonic inspections in more than 20 countries.

Featured Companies

SPIRIT ELECTRONICS

SPIRIT ELECTRONICS
11202 N 24th Ave
Phoenix, AZ 85029
Website

Categories

COMMS - POWER ELECTRONICS

Topic Tags

POWER ELECTRONICS