EBN

DNA Tagging:
Secret Weapon Against Industrial Espionage

Bruce Rayner,
Contributing Editor, EETimes
1/24/2012

Counterfeiting is a serious problem, and by all accounts it's getting worse, especially in the military and aerospace sector.

Keeping one-step ahead of the bad guys in the detection of fake parts requires sophisticated equipment that few companies can afford. Yet, based on language in the National Defense Authorization Act of 2012 (NDAA 2012) that President Obama signed into law on the last day of 2011, companies that serve the military market have no choice but to pay the price -- one way or another.

The Act specifically states that contractors "are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts." If they don't they foot the bill for the rework. They are also required to source from "trusted suppliers," which the act defines as original component manufacturers or authorized distributors. If the parts aren't available from either of these two sources, then contractors can source from "additional trusted suppliers." Exactly what that means is yet to be determined -- perhaps in a court of law.

Because of the magnitude of the problem, companies are coming up with creative solutions to reduce the threat of counterfeiting. Stony Brook, NY-based Applied DNA Sciences is looking to solve the problem once and for all. In a two-month proof-of-concept project funded by the Defense Logistics Agency in 2011, the company supplied ink containing its proprietary plant-based DNA to a chip maker that used it to mark the packages of its finished semiconductors. When the chips entered the supply chain, distributors were able to identify 100 percent of the marked chips to confirm their authenticity.

The success of that exercise led to an 18-month pilot program that will test the technology on a commercial high-volume scale. Separately, Applied DNA Sciences is providing Connecticut-based independent electronics distributor SMT Corp. with DNA ink to mark the components that pass its counterfeit testing program. SMT is a leader in the testing and detection of counterfeit parts.

Just this week, the company followed up with the announcement of a joint venture to take its patented technology to the next level -- or to be more precise, to the nano level. As part of a government-funded program, the company is partnering with the College of Nanoscale Science and Engineering (CNSE) at the University of Albany to tag chips at stages in the fabrication process. Calling it "nanosecurity," Applied DNA and CNSE issued a press release last week Tuesday touting the new "nano-chip anti-counterfeiting program." CNSE expects the process will be validated within a few months.

What's frightening about this announcement is that this is the first time I've heard of the threat of counterfeiters infiltrating a fab and managing to lay down a counterfeit layer of transistors or metallization. Or counterfeiters that have managed to insert a counterfeit chip during the construction of a 3-D system on an SOC or MEMS component. It's just unheard of.

The threat that the NDAA 2012 bill addressed is stone-age in comparison. It's the result of poverty-stricken women and children scavenging e-waste from landfills in China, stripping old components off

PCBs, sanding off the labels, replacing them with new labels, and selling them as “new” parts to unethical brokers. It’s downright primitive compared to the threat that CNSE and Applied DNA are addressing.

What’s behind the need for nanosecurity is not a fear of counterfeiting but fear of state-sponsored industrial espionage at next-generation multi-billion dollar fabs outside of the control of the United States. The US intelligence and military community wants assurance that it can "obtain the highest performance integrated circuits (IC’s) and systems-on-chips (SoC’s) while ensuring that components have been securely fabricated according to design," according to a report on the Trusted Integrated Chips (TIC) Program, published in October by the Safe and Secure Operations Office of the Intelligence Advanced Research Projects Activity (IARPA).

The TIC’s objective is to obtain near 100 percent assurance that when fabricating state-of-the-art ASICs -- as well as SOCs, MEMS, and other sophisticated 3D semiconductor structures -- that US intellectual property is protected, US chip designs are secure, and not compromised by the insertion of “malicious circuitry.”

IARPA is looking forward to the day when the electronics industry will be able to combine digital SoCs with non-digital System-in-Packages (SiPs) to create tiny high-value systems such as sensors, actuators, and biochips.

Put more bluntly, IARPA wants a fool-proof way to make sure its ultra-high-tech, multimillion-dollar, black-program components don’t get altered during fabrication outside the US. That is, it wants to prevent somebody on the inside from inserting what it calls “malicious circuitry.”

One way TIC proposes to do this is to physically separate the two stages of chip fabrication. Let offshore fabs lay down the transistors, but bring the wafers back to a secure US location for the metallization process. There are variations on this theme whereby chips are partially fabricated in multiple locations but final integration or packaging is conducted in a secure US facility. DNA-tagging would be used at each stage in the transfer process to ensure that part of the chip is authentic. This is not how chips are fabricated today, and the separation of the processes creates major challenges, especially as the technology advances.

IARPA is funding a five-year, three-phase program to validate the “split-manufacturing” approach for wafer processing. Phase 1 focuses on logistics and compatibility at the 130nm level. Phase 2 will targets 65nm and Phase 3 22nm. CNSA is awaiting word from IARPA regarding funding for its partnership with Applied DNA Sciences.

Of course, the threat of malicious insertion is not exclusively a defense concern. It has implications in the commercial world as well. For instance, consider telecommunications chips or industrial equipment that have rogue circuitry maliciously embedded in them. You could envision a scenario where a competitor or perhaps a foreign government could eavesdrop, access data, and control or even shut a system down at will.

Scary stuff.