

“Could cause missiles to misfire, radar systems to crash”

Counterfeit products emerge in the market almost right after originals are launched. The top five types of semiconductors reported as counterfeits represent US\$ 169 billion in potential annual risk for the global electronics supply chain, according to information and analytics provider IHS. How do we ensure that a counterfeit product does not turn a missile into a ticking time bomb? John Cronin, vice president of operations, North Shore Components Inc., the USA, speaks with Dilin Anand of EFY



JOHN CRONIN
VICE PRESIDENT OF OPERATIONS,
NORTH SHORE COMPONENTS INC.

Q. What level of damage can we expect from electronic systems running on counterfeit components?

A. Many components that are counterfeited are usually of a very high technical level. These may have a critical function in the product that these are contained in. The real concern started when the Department of Defence (DoD), the USA, realised that counterfeit components could cause severe problems. These could cause missiles to misfire, radar systems to crash or night vision goggles to cut off in the middle of military activity.

Q. What are these parts counterfeited with to have such an impact on systems?

A. In most cases, a part is selected whose physical characteristics might be identical or the electrical side may be similar. In some cases, a commercial version of the chip is taken and a military part number is put on it. Parts are disguised as if these were tested to extreme levels. These may pass testing, but when pushed to an extreme level, these components may fail, possibly taking down systems that these have been placed in.

Q. How do these counterfeit components make their way into military electronics?

A. Many products used today in the US military are legacy or older products, whose components are no longer made. Therefore the military depends on surplus and excess inventory, and components that tend to be expensive. This factor got the attention of counterfeiters and led to this being the class of products that were counterfeited first.

Q. How do manufacturers end up with counterfeits of their own components?

A. In the system of returns, an authorised distributor may send parts to a customer who may then return these, and the authorised distributor may not inspect the product properly. In some cases, they end up taking back counterfeit material instead of actual material, and therefore end up participating in distributing counterfeits. This gives a false sense of security to original

equipment manufacturers that they are buying through authorised distribution channels.

Q. Were these counterfeits first found only in the supply chain or in military systems too?

A. When this concern about vulnerability to counterfeits came up, the DoD required all of their contractors to review their products and come up with a list of affected equipment. And they soon started finding counterfeit components throughout both the systems and the supply chain. Concerns were so great that the DoD issued regulations requiring their contractors to ensure they had counterfeit mitigation processes in place.

Q. When looking at electronic components, where does the testing begin?

A. Ninety five per cent of the discovery is made during visual examinations. Simply by using a razor blade and scraping the surface of the part, you can see if the paint chips off. This should not happen, obviously.

In other cases, the part marking might come off. Another way is to use a cotton swab with certain chemicals on it and swipe it over the top and see if it erases the part number. These are the easy ones. Sometimes these parts are laser-marked, and therefore might not be easily noticeable as counterfeits.

It is also possible to test using X-rays. This may verify if the die is consistent throughout the part we are working with and if all connectivity is there. Another type is decapsulation tests, where we remove the covering of the part and visually see the die; we can document what is actually on the die itself. We also authenticate the markings on the die.

Q. What kind of visual markings do you usually pick up?

A. Sometimes, using a microscope we can see if they have sanded the part or pick out if they have over sprayed while doing the black topping, or if they have filled up voids in the part. At times if we look very closely at the markings, we can see a second marking underneath. ●