

Advisory Board Brief

Counterfeit Electronic Components – A Growing Concern



By Mark Tayles, President, Enabler Tech

One conservative estimate is that the U.S. Department of Defense (DoD) unwittingly purchased between \$70M & \$100M of counterfeit semiconductor components just in 2005. That according to Jack Stradley (Chair of the Semiconductor Industry Association's (SIA) Anti-Counterfeiting task force) and Dale Karraker (of the Defense Sustainment Consortium). Considering the typical program life of military programs and the often 'constant readiness' nature of DoD weapons systems – this could certainly be considered a wake-up call to a growing problem within the electronics industry.

Late last October, Rochester Electronics Inc. hosted an anti-counterfeit symposium at their headquarters in Newburyport, Mass. The impetus for the event was the establishment of an anti-counterfeiting task force by the SIA (<http://www.sia-online.org/home.cfm>). Attending the conference was a cross-section of sourcing and quality professionals including: semiconductor companies; electronic OEMs; distributors; contract manufacturers (CMs); and representatives from U.S. government agencies such as the DoD, the Navy, ARINC and others. John Szczepnik of Texas Instruments (senior vice-president of sales and marketing) opened the conference with a galvanizing keynote address.

It is estimated that counterfeit goods amount to between five to seven percent of global trade, or an incredible \$350B - \$500B annually. The first step to tackling any problem is defining it. As such, the SIA Anti Counterfeiting task force has defined counterfeiting along the following three dimensions: substitute or unauthorized copies of a product; a product in which the materials used or the performance of the product has been changed without notice by other than the original manufacturer of the product; a standard component misrepresented by the supplier.

What might be a surprise to some is counterfeiting of semiconductors isn't a new problem. Counterfeiting goes back to the early days of the industry when the majority of product was being purchased for military applications. Genuine devices were expensive (due to the rigorous screening and qualification requirements) and some of the less scrupulous manufacturers would deliver devices where all mandatory testing had not been completed. This led to the introduction of independent quali-

cations, audits by independent inspectors and regulated Certificates of Conformance (C of C) and paperwork traceability extending through the supply chain.

Exposing the scope and complexities of counterfeiting within the electronic component space has some natural resistance. The original semiconductor manufacturers have been reluctant to disclose counterfeiting instances, in case it should affect customer confidence or their stock prices. Equipment manufacturers are reluctant to admit they have purchased counterfeit devices in case it impacts confidence in their ability to manufacture and deliver equipment with the right quality and reliability. Since both sellers and buyers have this reluctance to disclose counterfeiting instances, the authorities that could act to shut down the counterfeiting operations have rarely been asked to do so.

TI is one semiconductor supplier that is working vigorously to protect its brand and to ensure customers are protected from counterfeit products. For example, the company has registered its trademark with U.S. Customs and Border Protection, which can hold suspect parts at the border at TI's request, according to Szczepnik. The company has also joined the Quality Brands Protection Committee, which promotes IP (intellectual property) protection in China, and is working with the SIA's recently formed anti-counterfeit task force.

So what are some of the dynamics that are at play? Driven by 'cheaper' as in the 'faster-better-cheaper' mantra, many semiconductor manufacturing operations take place in low labour-cost regions of the world. It is estimated that more than 45 percent of semiconductor manufacturing is carried out in the Far East, with China and Taiwan having the most significant production facilities. Some manufacturers own facilities in these regions but many use subcontractors for the diffusion, assembly and testing operations of their products. There are many companies that are completely 'fabless' and rely totally on subcontractors for their device diffusion and assembly. Unless the subcontract operations are managed and controlled effectively by the original semiconductor company, it is possible for the less scrupulous subcontractors to allow product or rejected material to escape to counterfeit operations. Certainly 'outsourcing' will only continue to grow in

Counterfeit Electronic Components — A Growing Concern

»»» Continued from pg. 6

prevalence, but similarly this 'arms length' dimension of outsourcing opens up many avenues for counterfeiting to flourish.

During the symposium, some of these avenues were discussed. For instance, product 'skimming,' occurs when an original semiconductor manufacturer uses a subcontractor for diffusion and/or assembly and testing of devices. They must be extremely careful to monitor and fully control the subcontracted operations. If they don't, it is possible for the less scrupulous subcontractors to over produce or to claim they achieve a lower production yield than the actual. All the extra devices produced can then enter the market through the broker chains.

Other avenues run the gamut from: inadequate controls during disposal of scrap and rejects; unauthorized (and uncontrolled) reclamation of used components; re-branding to a higher performance specification (to sell at higher cost); and falsely claiming conformance for certain environmental compliance (e.g. claiming RoHS certification).

So we've identified a complex problem. Now we have to come up with a solution? Not surprisingly, the solution is also complex.

Many at the symposium argued that the most economic solution should start with a company's sourcing strategy. There are definitely adequate 'channels' for these counterfeit components to find their way onto circuit boards. For instance, sales brokering networks exist to source and supply 'difficult to find' product (it is extremely rare for counterfeit components to be supplied by manufacturer authorized sources). There is no guarantee that devices procured through broker networks (or companies that are not authorized by the original manufacturer) have been stored and handled as required to ensure quality and reliability is not compromised. For a company to state unequivocally that they will procure from only authorized sources could be a powerful start to guarding against counterfeit components.

The short discussion contained in this article was intended to raise awareness about this growing problem. Rochester Electronics' white paper, titled *Defending Against Counterfeit Electronic Parts and Gray Market Practices* is available at www.rocelec.com. Rochester Electronics is represented in Canada by Enabler Tech, www.enablertech.com.

'[The] arms length dimension of outsourcing opens up many avenues for counterfeiting to flourish.'

Continued on pg. 10 »»»