

## Advisory Board Brief



### Anti-Counterfeiting Measures on the Increase

By Mark Tayles, President and Founder of Enabler Tech

A year ago, I devoted a column to the growing problem of counterfeit electronic components. Compared to other columns I've written, it was by far, the one that generated the most reader feedback. I had obviously struck a nerve with *Canadian Electronics* readers. Unanimously, those readers that I heard from, all had personal anecdotes on how counterfeit parts had entered their supply chain. In each instance, the intent (on the counterfeiter's part) was intentional, and often deviously creative.

With this edition's column, I revisit the topic and update readers on the state of affairs as it relates to counterfeiting.

Not surprisingly, the problem continues to grow. To quantify, it is estimated that approximately 8 percent of global merchandise trade is counterfeit which would amount to whopping \$1.2 trillion figure in 2009. Given the nature of this surreptitious market, a number of industry groups have tried to conservatively estimate

companies greatly reducing the number of 'non-franchised suppliers (a.k.a. brokers) and/or limiting the number of purchasing staff that have access to brokers.

The recently formed ACTF (Anti-Counterfeiting Task Force) of the SIA (Semiconductor Industry Association) has already started hands-on training for U.S.-based 'ports of entry personnel. This training is on recognizing and identifying counterfeit components. Jack Stradley of Rochester Electronics (and founding chair of the ACTF) has reported a five-fold increase in 'port of entry stops due to counterfeit suspicion, after personnel have received training. At the time of writing, Stradley surmised that all these 'stop shipments were likely counterfeit product.

One example of a typical 'stop was Texas Instruments seizure of 30SMJ320C30GBM40s in March at a U.S. Customs port. After initial contact by Customs, TI determined that these

#### Intel has gone on record as urging contracts to be awarded to component vendors who have demonstrated advanced anti-counterfeiting measures in the components that they sell.

the size of the counterfeit electronic components market. One recent study by Rochester Electronics (and using Technology Forecasters data), estimates that approximately 23 percent of semiconductor purchases are from 'non-franchised sources. If we use an industry estimate that between eight and 15 percent of these products are counterfeit, then the most conservative figure would be that over \$4.5 billion of counterfeit microchips worldwide, enter our supply chains, each year.

Compounding the problem in electronic components are a couple of 'industry specific nuances. EOLs (end-of-life notifications) and PCNs (part change notifications) are growing at an annual rate of over 19 percent (faster than the overall market), creating an atmosphere of desperation, as OEMs and contract manufacturers (CMs) scramble to find obsolete raw component inventory. Further compounding the problem, is that the most voluminous electronic components (MLCCs and R-chips) are void of any part markings altogether. Considering that an electronic system or subsystem is only as strong as its weakest link, what are suppliers, OEMs and CMs to do?

Certainly the most direct method is cutting the 'chance of incidence off at the source: that is, instituting a policy of only sourcing from franchised distributors. To limit their 'downside liability, we have heard of some

military marked components were actually remarked commercial grade DSPs. Further investigation revealed that the broker in the U.S. who was importing the goods had originally exported them to China without the proper export licenses. TI is currently working with ICE and DCIS on this case.

It will be a while till personnel at all 327 U.S. ports are trained, but it is a start. Not surprisingly, Europe has a similar task force under the SIA. Even in China, the Chinese Reliable Electronic Component Supplier's Classification (RECS) by China's Ministry of Industry is a jointly administered program by the China Electronic Purchasing Association (CEPA) and the China Quality Association for the Electronics Industry (CQAE). Rochester Electronics is among the first to receive this certification. The program is meant to send a strong message to Chinese OEMs and ODMs about the importance of staying within the authorized channel for purchasing electronic components.

Proactive and vigorous reporting of counterfeit events is another tactic in the overall war on counterfeiting. One large multinational defense/aerospace OEM was noteworthy in its strategy of issuing GIDEP (Government-Industry Data Exchange Program <http://www.gidep.org/>) alerts on every suspect part

Continued on pg. 21

### Anti-Counterfeiting

Continued from pg. 6

that they received. This public forum for information exchange shines light on the shady activities of counterfeiters, and helps other companies 'stay out of harms way.

From a perspective of allowing OEMs (or other supply chain participants) to verify the authenticity of components, SEMI ([www.semi.org](http://www.semi.org)) is working with the SIA to drive a 'secure serialization standard. This standard would allow brand owners to securely serialize their products using any method (e.g. bar code, number, RFID tag, et cetera) of carrying a unique code on a product, its label or package. According to Dave Brown, senior principal engineer Intel Security and Product Fraud Countermeasures, such a scheme would allow anyone within the supply chain to verify the authenticity of the product. Furthermore, he believes that brand owners will end up assigning this serial number to an 'object based on its value. For example, an expensive processor might have a secure serialized number on each of: the device itself; on a tray of devices; and on the outside package of the shipment. Due to the inexpensive (and tiny) nature of some electronic components, an 'object in the case of passive components may be at the reel level?

Another tactic to address this seemingly impossible task of marking miniscule passive components (e.g. tiny 01005 form-factor chip resistor measures a mere .4mm x .2mm x .12mm), advocated by Dennis Zogbi, is taking a page out of the analogous industry of pharmaceuticals. Zogbi is the president and founder of Paumanok ([www.paumanokgroup.com](http://www.paumanokgroup.com)), the passive component research company.

The pharmaceutical industry has a similar challenge of guaranteeing that medication is authentic. Billions of tiny pills are produced monthly (and often in subcontracted factories). Zogbi is suggesting the industry introduce taggants (microtags) into the ceramic slurry during the production of these passive components. These taggants would be nano-sized silica based particles that are doped with rare earth dyes, quantum dots or other proprietary types of luminescent chemicals. These silica nano-particles demonstrate a unique response when exposed to a specific excitation frequency. Any such strategy would have to be inexpensive, to guarantee market success. Zogbi believes such a scheme holds promise.

Of course, for any such combination of the tactics described above to be successful, relies on awareness across the entire supply chain. Additionally, a supportive posture within the supply chain is critical. Intel for one, has gone on record as urging contracts to be awarded to component vendors who have demonstrated advanced anti-counterfeiting measures in the components that they sell. Perhaps we will see a time where CMs adopt a 'no-broker stance and will not be economically rewarded by their OEM clients for buying 'seemingly cheaper parts through non-franchised sources?

<http://www.enablertech.com>