RoHS Compliance and Counterfeit Components

By Michael Baker and Joel Deutsch
E-Certa, Inc.

Counterfeit components throughout the supply chain are causing a myriad of problems for the industry including functionality, reliability, inventory management headaches, extra time and resource allocation not to mention all the extra cost involved in testing, detecting and trying to diminish the negative effects. Another, more subtle but just as real and costly effect, are the problems that counterfeits can cause for OEMs trying to comply with RoHS. Counterfeit components not only affect functionality and reliability of electronic goods, but can also cause RoHS compliance issues such as stiff penalties, goods recall, prison time and extreme mental duress.

Counterfeit goods are entering the supply chain from various sectors of the industry. There are true counterfeits, which are functioning reverse engineered copies of the original. Other types include factory inferior parts that were meant to be destroyed that find their way back into the gray market, also there are "lookalike" parts manufactured in factories in parts of the world with little or no monitoring regulatory body in place. Another type of counterfeiting is for parts that are the original part but may be re-marked or re-labeled to meet date or lot code requirements restricted by the OEM. The part may be the same and, for all intensive purposes, be a suitable functioning part. However, with the changes manufacturers had to undertake in the last few years to handle RoHS restrictions, re-marked parts may not pass compliance testing. These parts can come from anywhere in the world including China and the U. S. While most likely originated through the independent/broker market, it is possible that these parts can make their way into the franchised mainstream distribution sector by use of outside procurement sourcing used to satisfy their current demand deficiencies.

Sometimes it is not possible to find a necessary component from an approved and trusted supplier. Buyers are forced to search outside their qualified list of vendors. Other factors can also influence buyers to make quick decisions to purchase products from the gray market. Commission driven incentives and salesman's hopes to deliver product not readily available in mainstream procurement channels can lead to calculated risks...but that's why we're here today.

It is now critically important to know the exact and true material content of every component in your current inventory. If you have a component that you are procuring from a source that is not on your approved and qualified list of vendors, then it is practicable to have it tested for more than just functionality. You also need to check it's material content.

An article titled "Counterfeiters Compliant" by Rob Spiegel in Electronic New says that there are reports of counterfeit material coming from China. "I've heard reports of counterfeit Pb-free solder in China," remarked Michael Kirschner, president of Design Chain Associates in San Francisco. "A factory manager in China recently said, 'Look, if you need a certificate of compliance, we'll get you one.'" Kirschner believes OEMs will have to use gray market parts, because there may be cases where there will be no alternative source during gaps in supply. In these cases, testing will be critical. "If you desperately need parts and you buy them with no reason to trust what they are, you will have to test them both for functionality and for material content," Kirschner said.

In a different article by James Carbone titled "Watch Out for Bogus RoHS Parts" Thomas Valliere, also of Design Chain Associates says "There is a huge incentive for unscrupulous people to counterfeit, especially when it is hard to identify counterfeit parts just by looking at them." He says traceability and accountability will be difficult with the new RoHS-compliant parts. There are also some honest mistakes resulting in a mixed stock of compliant and non compliant parts. Some manufacturers are making both kinds of parts and some older non compliant parts are still in

inventories. Valliere says many—but not all—counterfeit RoHS parts will find their way into the supply chain via electronics brokers.

To use due diligence as a defense in a RoHS violation case, you must have more than a list of C of Cs. It is not enough to simply take the word of an unqualified vendor and potentially put components with hazardous materials into the marketplace. You must show that you have taken all "reasonable steps" to ensure your product's compliancy. "A certificate of conformity is not necessarily enough" said U.K.'s NWML RoHS technical manager Chris Smith. In an article titled Conformity Certificates will not Satisfy RoHS by Steve Bush, Smith states that "There needs to be a risk assessment of the quality of that information." Reasonable steps to make sure all of your components are RoHS compliant must include chemical testing to be sure of a component's content in cases where there is any doubt.

--Now picture a more challenging scenario, which was taken from a series of Dionics news releases which were edited by the Electronicstalk Editorial team. A component manufacturer has been selling a part for many years. It's a popular device, used in various applications, but it contains Pb - a substance controlled by the RoHS Directive. After much research and reliability testing, the manufacturer releases a Pb-free variant and adds a 'G' suffix to the original part number. However, despite this new introduction, there are still considerable volumes of the original product within the supply chain. It would be relatively easy for the forger to 'tweak' the original part number to create a RoHS compliant counterfeit. The goods are already in the original packaging, as they are - to all intents and purposes – original. This 'factory new' product would be considerably more difficult to identify. Moreover, electrical testing won't reveal the fake, as it isn't really a counterfeit in the traditional sense. It will still perform as its data sheet suggests it should - it simply contains Pb on its terminations. Disturbingly, this illegal use of Pb would probably only be identified by laboratory

analysis, or a future audit by the enforcement authorities.--

Electronic News reports "in one of the strangest twists in the industry's move to green components, some of the companies hawking counterfeit parts are claiming their parts are RoHS compliant. This bizarre development is occurring as OEMs are hip-deep in evaluating the level of trust they can put in their suppliers. If they can't trust a supplier to deliver RoHS-compliant parts, they will likely need to test the components as part of their due diligence to prove to EU governments that their products are compliant. The counterfeiters are not likely to make the trust cut, which means a lot of testing will need to be done to determine the content of these parts."

Another problem is a counterfeit conversion technique that E-Certa, a qualified known RoHS conversion center, calls "overcoating". Overcoating is a technique that is currently being used as a method to mitigate tin whiskering. Parts that are plated with tinned solder types are dipped in a higher Pb concentration solder to create a pressure stress barrier hindering the growth propensity of tin whiskering. However, according to the iNEMI Tin Whisker User Group's report titled "Recommendations on Lead-free Finishes for Components Used in High-Reliability Products" there is evidence that this technique may not be effective when performed on the new 99 percent tin RoHS compliant product entering the supply chain today. Based on the iNEMI report and on the NASA Office of Logic Design paper "Tin Whiskers-A "New" Problem" it is Joel Deutsch's opinion at E-Certa that a valid tin whisker mitigation technique should include a qualified stripping process to the original substrate, which creates inter metallic bonding with copper instead of the original tin/Pb finish. This practice along with proper annealing and robotic hot solder dipping techniques should be used to form an effective tin whisker mitigation approach. E-Certa is jointly working with Sanmina SCI to conduct a study and appropriate testing to validate these theories.

Using this overcoating technique with another purpose in mind, some claim to convert

components to RoHS compliant by simply overcoating the Pb lead with a compliant solder. However, there are some major issues with this technique concerning RoHS compliance. First, the Pb is never entirely removed. The troubling fact here is that these parts in some cases can pass an XRF screening, but are most certainly not compliant. Though this procedure in small quantities may pass XRF inspection, they will absolutely fail destructive testing, which will be the final method used in any litigation claims against non compliant product. If destructive testing is ever done for the device, the Pb will show up and the OEM will be held accountable. The second problem is that during the dipping process, the inter metallic bonding that is formed adherently still carries trace amounts of the original factory plated coating. It should be noted that XRF scanning will show failure from larger quantities (500 pieces and above) processed in this false manner due to Pb leeching consistent with repeated hot solder dip procedures. If you are going to convert your parts it is strongly suggested that you use a qualified facility, preferably with licensing of patented procedures. They should employ robotic dipping techniques to produce a repeatable effect that assures coplanarity and solderability. Also, they should have SOPs for maintaining solder pot integrity that include regularly scheduled checks and have had their processes tested with an accredited industry laboratory.

Many different forms of counterfeiting are in the supply chain that can affect the RoHS compliant status of a part. Mis labeling, overcoating and false C of C statements are a few of the ways counterfeiters might get you into trouble with RoHS regulations. As stated in the EU Environmental Protection Agency's document " The Restriction of use of Certain Hazardous Substances in Electrical and Electronic equipment Regulations 2006", it will be the duty of the Secretary of State to enforce the regulations. He has the authority to issue notices to producers of electronic goods requesting evidence of compliance and also to make test purchases to screen for compliance violations. The U.K.'s National Weights and Measures Laboratory set the standard for RoHS enforcement with their issue of the

"RoHS Enforcement Guidance Document" in May 2006. Outlined in the guide are selection methods for RoHS compliance screening which include the use of market intelligence, random selection, products known to contain materials of high concern, high volume products, short life products, consumer products unlikely to be recycled, notification of concern from external parties and notification of concern from other member states. The guide discusses the use of ED-XRF testing as means to detect RoHS elements, specifically for Pb in the solder on electronic components.

The penalties for non compliance may be severe, including punitive damages, product recall and possible prison time. Compliance violation cases will be sent to the country in which the offending party has it's head office. Penalties vary widely from country to country, the stiffest fines being in Ireland with it's 15 million Euro maximum and up to 10 years prison time. Courts will also be able to stiffen penalties for egregious cases in most countries. All cases found to be in violation will, of course have their non compliant product pulled from the market which could be the harshest sting of all for some companies. Fortunately, there are some steps you can take to protect your product from recall and yourself from litigation, while realizing your due diligence obligations in the process.

Many are screening their own inventories with hand held XRF devices. This method is effective for screening large areas of the board for gross violations of the RoHS limits. However, there are considerable issues with relying solely on this method for a RoHS compliance plan. In an article by Rob Speigal titled Testing for Compliance Heats Up Jeff Shaffer, SVP of product at Newark InOne says "Some companies have a gun and they point it at the component and it will say that bromide is present, so they're rejecting the component. But the test cannot identify whether it's banned substance." Some bromides are fine, others are not. Also,the testing beam emitted by hand held XRF is not small enough to test the solder joints on most IC package types. As a result, it factors in the area of the board surrounding the IC when calculating elemental content levels. This can skew the results. In order to get

a more precise reading for an individual component, a smaller test area (collimator) is needed. OEMS who are using hand held equipment as a final analysis may be acting on inaccurate results.

A desktop XRF machine can solve this problem because it has a smaller collimator size and the sample to be tested is secured on a fixed platform. Furthermore, it is important to have a sample at a fixed distance and for a period of no less than one minute to obtain the 1000 ppm level of accuracy needed for RoHS compliance. Only a properly calibrated desktop XRF instrument can do this which enables it to detect the RoHS elements with the accuracy needed for such low-level detection. This is not as easy as it sounds, the key being a proper calibration and a specific program that defines the elements searched for. Contrary to some beliefs, a desktop XRF machine is not as "turnkey" as it may sound when it comes to RoHS testing. While it is true that it can detect the approximate percentage of Pb in a sample on an out of the box standards free calibration, several extra steps are needed to determine all RoHS restricted elements and their precise values. First, a proper calibration through use of reference foil standards is needed to "fine tune" the instrument to be able to detect with the accuracy required by RoHS limits. Secondly, you need to tell the machine exactly what it is looking for through use of a program that defines the characteristics of the spectra involved and distinguishes between them. Then, you must cross reference the machine against test items that you know the value of, preferably obtained through destructive analysis. Finally it is important to perform a matrix of tests to determine that the levels detected are repeatable and accurate. Only with this criteria and a XRF technician with proper training and experience with spectrometry related to RoHS can one achieve the desired level of accuracy needed to determine RoHS compliance.

Companies considering the task of investigating suspect parts should examine the advantages of using an accredited independent 3rd party laboratory to help identify accurate material content. An outside lab gives the OEM an unbiased result and is a better means of meeting due diligence

obligations. It is not a good or preferential practice to use self proclamation as an ethical means to material declaration and RoHS compliance documentation due to conflicting interests.

OEMs have have a mountain of a task when it comes to controlling their inventory for RoHS compliance. An effective plan starts with a solid foundation. If they have not already done so, companies should consider establishing a RoHS compliance committee that takes into consideration all concerns regarding RoHS compliance. A counterfeit detection procedure should be included in the RoHS compliance plan and should be considered when developing supply chain audit procedures and inventory reviews. Let's take a look at a comparison between a few different approaches to the problem of RoHS compliance to investigate solutions to integrate counterfeit detection into RoHS compliance plans.

The first approach that an OEM might take in dealing with RoHS is to compile a list of C of C's and possibly material declarations that they have received upon purchase of their components. They create a database of all their inventory showing it's RoHS compliance status. This method is acceptable only if they are 100% positive that all of their inventory is perfectly organized, there is no possibility of mixed lots, that nothing has been purchased on the gray market and that all of their vendors are as confident as they are. Since it is next to impossible to prevent ALL errors at ALL times, this method is only for those that want to play roulette with RoHS. If one counterfeit or mistakenly identified part comes through, all of a sudden you're non compliant and don't even know it. As so often the case, shortcuts can leave you lost.

The second approach might be to perform in house inventory testing and documentation. This requires buying testing equipment, almost certainly hiring and training new technical staff as well creating a manageable data and records system. XRF equipment alone can range from $20K to $30K for hand held screening guns and from $35K to $150K for desktop machines. For companies with

endless resources, the financial aspect of creating an in house testing and data system may not seem like an impossible task. On the contrary, smaller companies probably do not have the ability to effectively take this approach. Another problem with this approach that affects both large and small companies is that there could be potential conflicts of interest. The deadlines and pressures associated with electronic device deployment can put OEMs in a position to make critical decisions on the fly. It is not inconceivable that in order to meet corporate goals, the decision to put a questionable component into a device (complete with C of Cs and material declaration) might be made. It's a calculated risk..right? So, while this method may be feasible for some, there are still risks involved as well as ethical concerns when making self declarations.

The third approach is to select components from the inventory that may be in question and have them tested by an independent 3rd party lab. This method distinguishes between parts that are from trusted and reliable vendors and those purchased on the gray market. Also, testing may need to be done for components that were once Pb and now are issued factory new as RoHS compliant due to the possibility of mix ups and common human error. Taking this approach allows the OEM to use an accredited laboratory to test for compliance through XRF screening or destructive ICP/MS testing where necessary. This targets particularly suspect components and leads to a rock solid data base of accurate documentation of RoHS compliance. Furthermore, if there ever were an instance of RoHS violation, the OEM would surely have performed their "due diligence" requirements. The RoHS directive states that any person under proceedings for an offense may use the due diligence defense that they relied upon reasonably verified information supplied by another, not that they relied upon information supplied by themselves!

So, after reviewing these three solutions to RoHS compliance we can see that OEMs level of protection against counterfeits and possible RoHS violations can be greatly enhanced by a plan that

includes documentation, in house screening and 3rd party laboratory testing. While it may not be necessary to have your entire inventory tested by an outside lab for RoHS compliance, it is recommended that selected components, especially those in a high risk category for counterfeits be fully tested by an independent lab.

For parts acquired through anything less than 100% trusted channels, simply testing for fit form and function is no longer the sole concern. Material content is of equal importance. RoHS penalties vary from country to country and many include prison time. In the future we can expect the introduction of more environmental restrictions and penalties from the rest of the world. Your RoHS compliance program should include counterfeit detection and prevention. A little extra expense up front to detect "compliance counterfeits" can be invaluable to insure the success of devices in the world marketplace.

Some companies have led the way in developing counterfeit protection to the industry and the clients who are affected. We'd like to give special thanks to Broker Forum, Broker Lynx, E.R.A.I. and Classic Components for their concerted efforts to detect and prevent counterfeit components from entering the supply chain. Thanks for attending!