How does a reputable component supplier guard against counterfeit components?

Welcome to Brainstorm!

The detection of counterfeit components has become increasingly difficult. The majority of parts have the same or similar markings as their qualified counterpart. In many cases, the identification of major manufacturers is applied despite manufacturers' efforts at product differentiation.

How does a reputable component supplier guard against counterfeit components?

Peter Murphy, President, Astrodyne Corporation

Counterfeit parts represent a threat to legitimate manufacturers of electronic equipment around the globe and aggressive measures are mandatory if product integrity is a priority. Many of the industry's best known companies have ended up with these parts without being aware that their well managed supply chain had holes in it. This is a particular problem in the current economic downturn as suppliers have reduced inventories in order to deal with uncertainty in the demand channel. Reduced inventories mean increased lead-times and purchasing professionals are often sent scrambling for components.

Counterfeit parts can take many forms such as knockoff lookalikes with pirated logos, rejected components salvaged from scrap bins, parts pulled off of boards that were rejected or "third shift" components that, despite assurances, have not undergone required inspection and test. Regardless of the source, an uncompromising prevention program has become a requirement for electronic manufacturers.

At Astrodyne we have implemented a comprehensive procedure to deal with the counterfeit parts phenomenon:
• Only authorized distributors, validated by original manufacturers are utilized.
• Regular audits are conducted at distributor sites where parts, packaging and manufacturer invoices are inspected.
•Product documentation is examined in great detail where evidence of counterfeiting such as broken English, printing errors, inaccurate specification references and incorrect part numbers may be identified.
• Incoming visual AQL inspection checks of logos, part numbers, date codes etc are

compared for accuracy and authenticity.• Physical dimensions and weight are checked.
•For some component types, small sample destructive analysis is performed.
•Pins and leads are checked for signs of prior insertion.
•Components are examined for signs of modification such as irregular surfaces around logos.

If the company suspects the possibility of counterfeiting, many options are available including:
• X-Ray or other noninvasive analysis.
• Chemical analysis of mold compound.
• Leak testing sealed components.
• Inspection of internal elements such as die device for critical dimensions.
• Electrical testing to compare performance to specification.

In summary, Astrodyne employs strict adherence to an approved vendor list and active inspection programs to greatly reduce the likelihood of counterfeit components entering our inventory. This is not only our process; it is our commitment to our customers that we will do everything in our power to insure the integrity of our power products.

R. Dale Lillard, President, Lansdale Semiconductor Corporation

The only way a manufacturer can confidently be sure that an end user of its product is not getting a counterfeit is to sell the product directly to them without using a middle sales channel and to never restock returned product for resale.

This can be difficult for large manufactures who use distributors in their sales channel. Precautions must be taken to ensure that the distributors recognize their responsibility in preventing counterfeit product being returned to them for restocking. In light of the magnitude of the problem, I recommend that restocking be discontinued as it is very difficult for them to detect counterfeits, and once the product leaves the control of the distributor or manufacturer, it can be replaced with counterfeits and the substitution not be detected. Warehouse security also needs to be enhanced to make sure product is not replaced with counterfeit parts by unscrupulous employees which might not be caught by standard inventory count monitors.

Manufacturers must control reject material and establish a process that ensures that all scrap product in any form is truly destroyed, ensuring that it does not leave the operation and fall into counterfeiter's hands. Monitors should be in place ensuring inventory flow-thru balances out so that all rejects are accounted for and destroyed, particularly by subcontract manufacturers.

The manufacturer must also ensure that their sales channel follows the guidelines and audit them accordingly. They must not sell product that is not sourced directly from the manufacturer. No one would accept a knee replacement if it was not from the original manufacturer or a blood transfusion with blood not from the blood bank. So why would we accept electronic products from unauthorized sources, particularly military products whose failure can have life or death consequences?

Denis Farison, ST Microelectronics

Counterfeit products, most of which will perform poorly, will also increase downtime, maintenance and replacement costs for end users. Organized counterfeiters have learned to break the level of security where authentication of a peripheral relies on a simple memory chip containing the security keys, and this presents a costly threat to brand owners' image and revenues.

ST's AuKey turnkey solution represents a major step in terms of security, to help brand owners authenticate their products. Relying on ST's ST23 highly secure microcontrollers, AuKey is significantly more effective in differentiating genuine items from unauthorized copies than conventional techniques, which are often susceptible to being easily and cost-effectively broken or cloned.

ST's AuKey turnkey solution offers hardware-authentication devices comprising a secure operating system (OS) running on top of the latest-generation ST23 secure microcontrollers to increase protection for the embedded security keys. The most advanced security crypto algorithms are supported by AuKey, including the AES shared-key system and Elliptic Curve Cryptography (ECC). The microcontroller and OS, together, also secure the chip's data-read and data-write mechanisms. This level of protection delivers a significant increase in security at a highly competitive cost.

AuKey can be quickly designed into various products, including computer accessories, add-in cards, gaming peripherals, printer cartridges, toners, disposable medical equipment, network infrastructure products, metering devices, and many other types of assemblies and systems.

AuKey's secure microcontroller-based security also provides freedom and flexibility for brand owners through its customizable security architecture, configurable key-management mechanism, and chip-personalization tools. In addition, support for secure application firmware downloads allows authorized updating or restoration of settings in the field.

AuKey is based on ST's range of proven ST23 highly secure microcontrollers, which are in full production now and are packaged in the industry-standard SO-8 format.

Source URL (retrieved on *03/09/2014 - 3:57pm*):
http://www.wirelessdesignmag.com/articles/2009/12/how-does-reputable-component-supplier-guard-against-counterfeit-components