

# Faked in China: learning from Apple's misery

By Andy Groom

**FAKE STAFF**, fake interior decoration and a complete shop full of fake electronic devices: The recent news regarding five bogus Apple stores in China; perfect one-to-one copies of the original shops, showed once again that there are no limits to the creativity and ingenuity of counterfeiters in all industries. However, I think the electronics industry was less surprised than others. The electronics counterfeit industry is savvier than ever. Counterfeiters constantly find ever more novel ways to smuggle their illegal goods into the market. OEMs are aware of the danger of increasingly sophisticated counterfeits and the general numbers prove them right: The Rogers Review, estimated in the 2010 IP Crime Group Report that criminal gain from IP crime alone in the UK was £1.3 billion in 2006 with £900 million of that figure considered to be flowing into organised crime. And many parts of industry estimate that the figure is now even higher than this. Some industry experts go so far to suggest that counterfeit goods now represent around 10% of the entire electronics market.

As a result of this, electronics distributors have to guarantee the irrefutable authenticity of their products and one way to do this is to run an independent in-house third party testing facility. In my opinion third-party testers are the best choice to provide both an expert and objective evaluation of a component according to all necessary conformance, performance and industry requirements. However, in-depth inspection of every part in the supply chain is an impossible task. Ultra-modern counterfeit testing methods can also entail additional costs for OEMs. The Independent Distributors of Electronics Association (IDEA) has established an inspection standard, which is well recognised within the electronics industry and works very well as a fundamental checklist. This is the IDEA STD 1010. Benchmark testing standards are key to ensure the authenticity of electronic components, and the standard raises quality-conscious, upright indepen-

dent distributors to a higher level in the market, separating the wheat from the chaff. Indications of counterfeit in a component can be relatively minor. The IDEA 1010 standard details 50 inspection-checks for electronic components, characteristics of good components, and examples of quality and substandard parts. Counterfeited electronic components might be sophisticated retapes of existing IP. Then



**Groom: "In my opinion third-party testers are the best choice to provide both an expert and objective evaluation of a component."**

again they might simply be a scrap from manufacturing that is salvaged and sold as new; components from discarded computers in the supply chain being shipped as recycled e-waste, or parts being plucked from the board and illegally re-labelled. Using five different types of visual inspections most counterfeit components can be discovered with the IDEA STD 1010 examinations: part marking; surface (top and underside); edges; leads, and packaging and labels. Surface-marking-examination looks at evidence of slight standings and scratch marks, while lead-checks simply involve ensuring there is nothing missing, and that no solder/flux are on the leads, as well as looking for evidence of heating or burn marks. Experi-

enced staff are also invaluable; even if a part number marking looks fine at first glance, if not located in the position where the inspector would expect to see it rings a warning bell and the part gets scrutinised further. The next stages for proof of authenticity are more detailed and investigative checks, which go beyond the industry's inspection standards and should be done by independent third-party test houses, by various means including de-capsulation to expose the chip inside, as well as the revision number, manufacturer's log, logos and part number. Currently most counterfeiters are unlikely to go into this level of detail, (that is, assuming they put a chip inside their packaging at all).

Looking for the manufacturer's signatures to ensure the genuineness of the part does not necessarily require deconstruction. X-ray inspections are still a very effective means to detect types of counterfeited parts; most effective when x-raying the ambiguous parts side-by-side with a 'known good part'. Comparing the lead, frame, footprint and location of the die within the package gives a very accurate indication of authenticity. There are further developments occurring in authenticity evaluation; laser surface authentication for example, involves analysing the naturally occurring random structure of a chip's surface and from this generating a signature or code unique to that surface. This code can then be used to authenticate and identify the item in the same way as a fingerprint. The serial code is naturally occurring and is not added by any manufacturing step, eliminating the danger of replication.

Looking at the example of the Apple stores, no matter how safe genuine testing methods are, counterfeiters never fail to impress. While new techniques for testing emerge all the time, there really is no substitute for the fundamental testing methods. OEMs should put their trust in what they know to work best; unified industry standards and independent third party testing. The best thing a company can ever do to avoid counterfeits is simply to apply rigorous processes to make sure these fundamentals are in place. ■

Andy Groom is the Managing Director of distributor America II Europe [www.americaiiurope.com](http://www.americaiiurope.com)