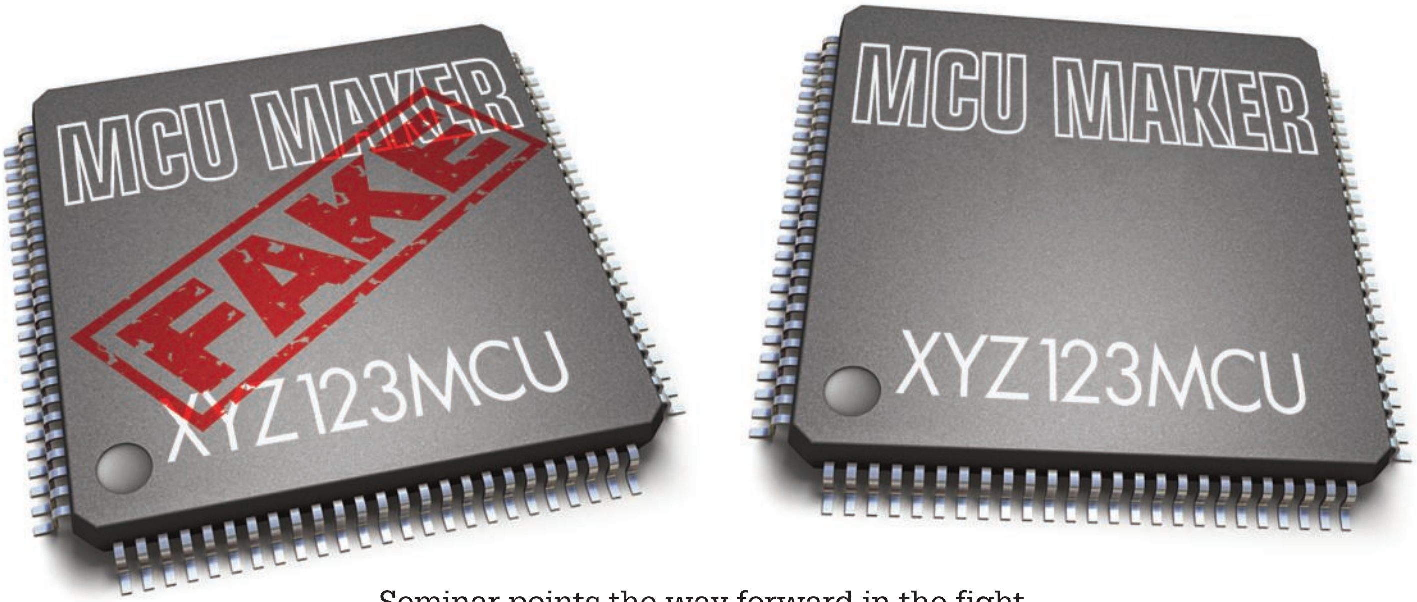
# FORCING out FAKES



Seminar points the way forward in the fight against counterfeiting. By **Graham Pitcher**.

Counterfeiting is a huge business. While most of the fake goods in circulation are targeted at consumers, there are electronic components out there which could have serious consequences if used in, for example, military systems.

Here's a snapshot of how it affects the consumer world. Alibaba, the Chinese e-commerce site which raised $25billion in its recent IPO, spent more than £100million last year in fighting counterfeiters. It now has more than 2000 staff involved in the process and claims to have removed 90m listings of counterfeit goods from its website.

The insight was provided by Ian Blackman from the International Institute of Obsolescence Management (IIOM) as he introduced ESCO's recent anti counterfeiting forum. "Companies need to know about counterfeiting" he told attendees, "because customers will ask them how they are managing the risk; not managing it could have a significant impact on their business. They need to understand and manage the risk in the supply chain," he warned.

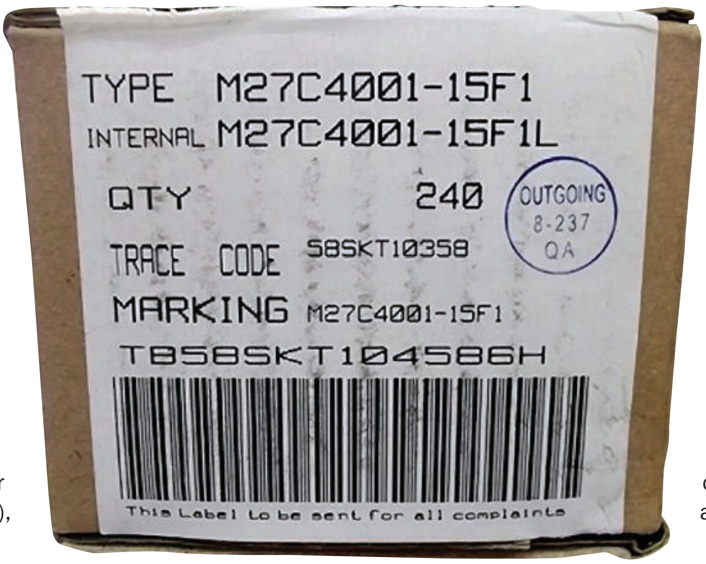
The latest forum – the sixth such event to be held – was entitled 'Building resilience against counterfeits in the electronics supply chain'. And while much of the focus in the fight against counterfeiting is at the component level, there are a range of complementary products whose provenance can be just as uncertain. The list of technologies runs from amplifiers to transistors by way of connectors, cables and PCBs.

Peter Marston, business development and technical consultant with end of life semiconductor specialist Rochester Electronics (**www.rocelec.com**) told the audience that the defence industry didn't dominate semiconductor consumption. In fact, he said, less than 1% of semiconductors are now bought for military applications. However, these applications are often targets for counterfeit parts because of their long design life. A compounding factor, he contended, was the decline in second sourcing.

He pointed to four main factors affecting the prevalence of counterfeiting: obsolescence; product shortages; the drive for companies to buy components more cheaply; and what he called 'dumb' e-procurement. But he didn't excuse semiconductor manufacturers from the problem. Issues here included inadequate control of scrap products.

Obsolescence has been compounded by the growth in the number of markets with long term outlooks, including transportation and avionics, as well as industrial and medical. "And poorly handled returns through the distribution channel have not helped," he noted.

The grey market, or brokerage, is



*Counterfeiters pay close attention to how they package fake components.*

*Courtesy: Astute Electronics*

another minefield. Pointing to a growth in brokerage, Marston said there was a mistaken belief that 'authentic' meant 'reliable'. "A used part is an unreliable part," he pointed out.

Amongst the sources of such product are: recycling from waste; stolen goods; and unlicensed manufacturers. "There is no assurance that such product will meet manufacturer's specifications," he warned.

Picking up on the theme, Mark Shanley, global business manager for Astute Electronics (**www.astute.co.uk**), advised companies to take the following steps:

- work with trusted sources
- audit your partners' processes
- don't search for components using Google; cheap parts found in this way will be cheap for a reason
- follow standards, and
- train your staff.

All companies should have a counterfeit product mitigation plan, he contended. What is such a plan? "It's a series of processes and procedures based on recognised industry standards and customer requirements which provides risk mitigation against procurement and distribution of counterfeit products. The implementation of strict supply chain controls is the most critical part of the plan," he continued, "because prevention is key."

His advice when you encounter counterfeit components? "Report any known issues to make sure the market isn't recontaminated."

Keeping suspect components out of your board or subsystem is one thing, but what about the cables that join them together? Peter Smeeth, from the Approved Cables Initiative (**www.aci.org.uk**), told the audience that 70% of all cable sold in the UK was imported, adding that half of that amount may not be up to standard. The result, he suggested, could be things such as alarms that don't sound when they should and sprinklers that don't activate.

Dr Jeremy Hodge from BASEC – the British Approvals Service for Cables, **www.basec.org.uk** – took the discussion forward. He pointed to such issues as incorrect polymers used for cable sheathing and jackets, incorrect conductors and false marking.

Echoing the warnings of those from the semiconductor sector, Dr Hodge advised users to beware of low prices, unfamiliar brands and poor – or no – markings on cable.

Companies can prevent counterfeit components getting into their products by adopting industry standards. Kevin Beard, president of certification specialist NQA (**www.nqa.com**) suggested that significant challenges need broad based solutions. "Accredited certification is a key component in building industry trust," he asserted.

Looking to strengthen certification processes, NQA has updated AS9100 and AS9120 – both targeted at aerospace – as well as ISO 9001 to address what Beard called emerging supply chain challenges. These will include changes to quality management standards addressing counterfeit parts and obsolescence management. "AS9100 will have stronger wording, more aligned to counterfeit prevention," he said. "It will have augmented traceability and inspection wording."

In the future, AS9100 will include enhanced wording on key QMS processes, he added. These will include risk based purchasing controls, as well as requirements for counterfeit prevention processes.

As many speakers mentioned, obsolescence and counterfeiting go hand in hand. Stuart Kelly, chair of the IIOM's obsolescence management group, said: "Over the life in service, a substantial number of components will become no longer available from the original manufacturer. And 60% of counterfeit components are targeted at obsolescence."

What can designers do to help ease the process of dealing with the situation? Kelly suggested a robust obsolescence management plan will help. "Do a risk assessment," he said. "If the risk of a component becoming obsolete is low, you will have established there will be a cost effective solution when obsolescence strikes – but get it wrong and you open the door to counterfeiters."

Of course, there is a chance the assessment will determine a component is at high risk of obsolescence. "These parts will be critical to a system," Kelly said, "and should be monitored continually. Counterfeiters will target high risk items that are declared obsolete and will become hard to find."

The good obsolescence manager, Kelly asserted, should understand the risk and mitigate that risk using a range of approaches.

Highlighting the problems with electrotechnical products, Kevin Smith, deputy director of trade association BEAMA (**www.beama.org.uk**), said that almost 75% of respondents to a survey reported the availability of 'a lot' or 'some' sub standard parts. "There are, potentially, significant quantities of non compliant and unsafe products circulating within the UK." His advice: "Know the products you're buying and be confident in the person you're buying from."

**"Counterfeiters will target high risk items that are declared obsolete and will become hard to find."**
**Stuart Kelly**

▪ **For more on anti-counterfeiting, go to www.anticounterfeitingforum.org.uk**