

VIEWPOINT

How to meet the traceability challenge

Despite the ID chipping of components manufacturers will still need component traceability to protect their production lines from the threat posed by counterfeiters, writes **Debbie Rowland**, sales manager at Charcroft Electronics

While everyone agrees that counterfeiting is a risk that cannot be ignored there is little agreement on the most effective way to tackle the problem. Only Japan, for example, has ratified the Anti-Counterfeiting Trade Agreement (ACTA) which aims to provide a global framework for cross-border protection of intellectual property (IP) for all types of goods, including electronic components.

The other 30 countries which are signatories to ACTA are still facing stiff opposition from groups as diverse as civil rights activists and the global medical charity, Médecins Sans Frontières.

Even within the confines of the electronics industry, different proposals around the theme of traceability are being put forward by government agencies, non-government organisations and supply-chain partners. These proposals range from relatively simple processes to the stuff of science fiction.

Perhaps the most advanced approach is the Supply Chain Hardware Integrity for Electronics Defence (Shield) programme from the US Defense Advanced Research Projects Agency (Darpa).

In February 2014, Darpa issued a release asking for proposals for the creation of a 100x100-micron authentication 'die-let' which could be co-packaged inside an electronic component. The Shield die-let would be fully isolated from the host component and include a full encryption engine in addition to anti-tamper sensors.

Scanning the die-let with a smartphone or similar device would upload a serial number to a central database, which would send back a challenge to the die-let; it would reply with an encrypted response including data from passive sensors monitoring for factors such as exposure to light, an indicator of tampering.

A slightly different approach in component-level authentication is the use of uncloneable 2D labels which can be printed on anything from the components themselves to the packaging in which they are shipped.

Featuring a barcode matrix, similar to a smartphone QR code, the label would be created as a high-resolution image but randomly printed at a lower resolution. Trying to recreate the original high-resolution code from the blurred copy would definitely challenge potential counterfeiters.

While these examples focus on component-level anti-counterfeiting measures, other approaches focus on the reliability and rigour of the processes used to track a component throughout the supply chain.

The importance of the traceability process is highlighted by the fact that the IECQ has introduced the Counterfeit Avoidance Programme (CAP) as part of its Approved Process Scheme. The CAP includes independent surveillance of a company's counterfeit avoidance processes in order to qualify for the IECQ CAP Certificate of Conformity.

This approach is reflected by the Aerospace Industry Association (AIA) which suggests that the US Department of Defense's Trusted Supplier evaluation methods should focus 'on the robustness of the processes used by buyers to assure material authenticity' rather than approve companies as trusted suppliers.

This shift recognises that the suitability of a supplier is specific to the level of risk and the application in which it is applied.

The need for tighter traceability is also having an impact on suppliers which do not operate solely in high-reliability sectors like defence and aerospace. A new type of distributor has been added to the traditional models of franchised, authorised, non-franchised and broker: Hybrid or blended distributors have begun to add franchised lines to their linecards which previously operated mostly in the non-franchised supply chain.

Other distributors, again operating in the non-franchised supply chain, are also offering in-house component testing as an alternative to providing traceability back to the original component manufacturer.

It is not just the non-franchised and hybrid distributors who are working hard to prevent counterfeit components from reaching customer production lines: even franchised distributors are finding that providing complete traceability is not always a simple process.

Matching manufacturer Certificates of Conformity (CofCs) to back-to-back

Debbie Rowland



orders and shipments is relatively easy but the process of storing a CofC and then sending a copy with each shipment of a scheduled order is clearly not so straight-forward. This is why some distributors are beginning to charge fees of up to £15 to provide a copy of the manufacturer CofC with the customer's delivery.

It seems likely that customer demand for more rigorous traceability will mean that most distributors will have to implement a storage and retrieval process similar to the one Charcroft introduced in 1985. By copying and archiving a copy of the delivery note or CofC received with every delivery, it is possible to access and supply the batch number and date code for any part, shipped to any customer since the archive began in 1985. More recently, the process has been managed digitally, creating a database which is searchable by the component part number, batch number, date code and customer order number.

With more than a million suspect electronic parts found in the Pentagon supply chain during a two-year investigation by the Senate Armed Services Committee it seems that every stakeholder in the electronics industry will need to address the challenge of counterfeit components.

Whether the industry opts for the sophistication of an ID chip implanted into a component, or the more basic approach of a rigorous documentation process, it seems likely that customers will continue to look for traceability to protect their production lines from the threat of counterfeit components.

ELECTRONICS WEEKLY 6th Floor, Davis House, 2 Robert Street, Croydon CR0 1QQ, England www.electronicsworld.com
EDITORIAL 020-8253 8671 **electronics.weekly@metropolis.co.uk** Managing director Kevin Crook kevin.crook@metropolis.co.uk 020 8253 4600 Publishing director Nick Stimpson nick.stimpson@metropolis.co.uk 020 8253 8895 Editor Richard Wilson richard.wilson@metropolis.co.uk 020 8253 8670 Components editor David Manners david.manners@metropolis.co.uk 020 8253 8664 Technology editor Steve Bush bush@metropolis.co.uk 020 8253 8665 Web editor Alun Williams alun.williams@metropolis.co.uk 020 8253 8666 Production editor Sue Proud sue.proud@metropolis.co.uk 020 8253 8667 Editorial Assistant Alison Noble alison.noble@metropolis.co.uk 020 8253 8671

CIRCULATION: UK SUBSCRIPTIONS One year UK £102, Europe £133. Rest of the world £165 USA £140 and Canada £152. Please forward your remittance with subscription order.
Electronics Weekly Subscriptions Dept, Abacus e-Media, Chancery Exchange, 10 Fumival Street, London EC4A 3YH. Telephone: 0208 950 9117. Email: metropolis@abacusemedia.com. To apply for a free copy of the magazine in print or digital versions go to: www.electronicsworld.com
 Registered at the Post Office as a newspaper. SSN 0013-5224. Electronics Weekly is published by Metropolis Business Media (part of Metropolis International Group Ltd), 6th Floor, Davis House, 2 Robert Street, Croydon CR0 1QQ. A member of BPA. Electronics Weekly is a trademark of Metropolis International Group Ltd.

ADVERTISING Display: Commercial manager Steven Ray steven.ray@metropolis.co.uk 020 8253 8652 Senior sales manager Lisa Duncan lisa.duncan@metropolis.co.uk 020 8253 8658 Account manager Robert Houghton robert.houghton@metropolis.co.uk 020 8253 8649 Classified/Recruitment Key account manager Paul Pastor paul.pastor@metropolis.co.uk 020 8253 8651 Ad production: Production designer Victoria Heath victoria.heath@metropolis.co.uk 020 8253 8655 Ad operations: Farhan Qureshi Web analytics manager farhan.qureshi@metropolismedia.co.uk 020 8253 8654

Follow us on twitter
 Join us on LinkedIn



Charcroft Electronics
www.charcroft.com