Combating counterfeit components—industry initiatives for a global problem

Nigel Burtt, Enjaybee Associates, Swindon, United Kingdom

The UK Electronics Alliance (UKEA) organised a seminar in a hotel near London Heathrow airport in October 2009 to discuss the problems the global electronics industry faces with component counterfeiting. It also announced its own online forum website which gives free access to a reporting facility and searchable database of suspect devices. The seminar detailed other industry initiatives that were in progress and eight presenters spoke on different aspects to this topic, providing important insights into what is a major global problem for our industry.

Keywords: Counterfeit Components, Obsolescence, Intellectual Property Crime, Grey Market Supply, Recycled Parts, Safety-Critical Systems.

On October 15th 2009, the UK Electronics Alliance[1] (UKEA) organised a seminar in a hotel near London Heathrow airport to discuss the problems the global electronics industry faces with component counterfeiting. There was a timely reminder of the seriousness of this issue presented immediately to the delegates concerning the news that three people in California had just that week been indicted by the United States Attorney's Office for dealing in counterfeit ICs that they sold to the United States Navy[2]. One of these people has now in fact pleaded guilty to the charges involved[3].

The day was opened by UKEA's Roger Rogowski who outlined the background behind the organisation of this event and the concept behind UKEA's work on this topic and others which is to share information and best practice throughout the industry, whilst also aiming to avoid any overlap of initiatives and ideas. Roger mentioned that there had been some widely seen conventional media coverage concerning the counterfeiting of medicines, where the consequences are easily understood to be potentially deadly. However, the dangers associated with counterfeiting electronic components ending up in safety-critical systems, aerospace and military products and other high reliability applications are not so widely understood, but are equally serious.

The first presentation was given by Adam Fletcher of the Electronics Components Supply Network[4] (ECSN), who were active participants in the organisation of the event, along with the Components Obsolescence Group[5] (COG.) He cited figures from the OECD in 2005 that estimated the international trade in counterfeit goods was worth around US $200 billion and a recent update[6] shows that this continues to rise. As an indication of the gravity of this as it applies specifically to electronics manufacturing, he said that it was now common for the unorthodox distribution channels commonly known as "the grey market" to be referred to in the USA now as "the orange market" instead, to indicate the perceived business risk.

He offered some examples where devices had been found to be functional and genuine articles but later discovered to have been re-marked to indicate an improved specification in order to increase the price, such as: a 120 ns access memory device marked as 80 ns; a commercial grade IC marked to indicate military grade performance; 4 MB flash memory marked as a 16 MB part.

These type of alterations can be difficult to detect reliably and are increasingly common, but also common are parts offered as new or obsolete legacy stock that have in fact been removed from products that have been disposed of as WEEE. There has been some mainstream media coverage of illicit operations, in China for example, carrying out such "re-cycling" which focussed on the local environmental damage and human health problems this causes. It is also very clear, given the rudimentary techniques used to remove the components and the lack of proper precautions to avoid electrostatic and humidity damage, that there should be product safety concerns since we know that such devices can end up in locally made equipment or sold on the global market as legacy stock or refurbished devices for use in manufacturing operations in other countries.

This topic was picked up by another speaker, Bill Goldie of Retronix, who have tackled this aspect of the problem head-on by setting up authorised operations in China to test, process and supply devices sourced locally. Their Asian facilities have found that 90% of failures of devices they have detected are from improperly recovered parts, far more than those found to be deliberately counterfeited or re-marked. Whilst several audience members were adamant that recovered devices should not be used and Asian brokers were to be avoided, certainly for their own supply chain at least, Bill pointed out that an international standard IEC62309 "Dependability of products containing reused parts—Requirements for functionality and tests" existed which indicated that the industry had already decided that devices recovered from end-of-life product could be used legitimately. The problem as he saw it was rather how to detect devices obtained from improper and unauthorised recycling operations and ensure that these could not enter the supply chain.

Peter Marston of Rochester Electronics noted in his presentation that the semiconductor industry was very aware of the problem and was already taking steps at a global level to fight it and raise awareness of the dangers it creates. Trade associations within the World Semiconductor Council[8] (WSC) in the USA (Semiconductor Industry Association[9] – SIA) and the EU (European Electronic Component Manufacturers Association[10] – EECA) have worked together to create an anti-counterfeiting task force (ACTF) which has already produced some useful and successful initiatives, such as working with US and EU border and customs authorities to provide guidance and training on the extent of the problem. They have also set up a Reliable Electronics Component Supplier (RECS) authorisation scheme working with Chinese government ministries and industry bodies to promote those suppliers who do use legitimate sourcing supply chains. The ACTF have correctly identified that the Chinese government must be part of the solution and that China recognizes the dangers from counterfeiting, since such devices are more likely to find their way into locally made product sold in its own market than into imported or exported goods.

Amongst the delegates there were a high proportion of people from companies working in the aerospace and military markets, understandably so, as they are

Figure 1. Bill Goldie presentation–Photo courtesy of Charles Battersby of Semelab and COG

perhaps most exposed to these problems given the critical nature of the products they manufacture and the effect on their supply chains that the RoHS Directive, and similar legislation subsequently adopted by other nations, has had. There were also two speakers from the industry, Jo Vann of GE Aviation and Dave Akhurst of General Dynamics.

Jo explained how the aviation industry has a mandatory requirement for full traceability of all components and material used in flight equipment and that the declarations of reliability for avionics systems depend upon the full predicted life specification of the components employed, so the use of anything other than genuine original approved manufactured parts must be avoided at all costs. The industry has developed a recent standard to tackle counterfeiting, SAE AS45553[11], which has already been endorsed by the US Department of Defence and NASA. This asks that all businesses in the supply chain develop an anti-counterfeiting plan. In Europe, the French aerospace industries association, GIFAS[12], have produced a set of guidelines for component sourcing though non-franchised distributors, taking a risk assessment approach to the problem. These two documents have led some IEC standards activity with the formation of a working group, TC107-WG2 (AQEC)[13], of which Jo is the convenor, and an ad-hoc group AHG3, to focus on the difficulties in controlling the spread of counterfeit parts to the avionics industry. The initial plan was simply to adopt the SAE document, but as a US copyrighted document this cannot be directly adopted into an IEC standard. In any case the group has already decided that it needs to widen the scope to include China and Asia, not just the USA and EU. Jo encouraged interested parties to contact her (jo.vann@ge.com) if they wished to participate in the work of the group.

Dave Akhurst looked at practical measures an OEM can adopt to help detect suspect components and showed some examples of actual devices which were not what they claimed to be and how these were discovered. He detailed the extensive procedures and processes that General Dynamics had already put in place to tackle counterfeit component supply, which had required significant investment in equipment and corporate resources throughout its organisation.

Ian Blackman of COG also gave some examples of practical strategies that businesses should adopt to protect their reputation. He said that the issue of component obsolescence, often driven by environmental regulation such as the RoHS Directive, has lead to some highly developed and lucrative counterfeiting operations. Indeed he said that it had been found that some cloned counterfeit devices actually work perfectly well in many applications, which in turn means the actual scale of the problem is impossible to accurately define.

A rather different perspective on the problem was provided by Pat Farrington of the UK government agency, the

Figure 2. Final Q&A session–Photo courtesy of Mike Judd of MJ Marketing

Intellectual Property Office (IPO). She pointed out that counterfeiting is by definition the wilful infringement of a recognised Trade Mark and as such is an offence under UK law. The IPO provides an "Intelligence Hub" to support all agencies investigating intellectual property crime and this already receives 400-500 reports each month as well as 20-30 external enquiries. She noted an interesting conundrum for the industry in that if you knowingly buy or use counterfeit parts, the title to those items does not belong to you but to the original owners of the trademark on them. It appeared that it would therefore be illegal to sell these on or to destroy or dispose of them and since you bought or used them aware of their provenance you cannot return them to the supplier you bought them from either.

An unfortunate real case of law concerning a young boy electrocuted by an unsafe non-OEM charger for a portable games console[14] was a reminder of the dangers for consumers in being complicit in accepting counterfeit products.

Roger Rogowski of the UKEA explained its initiative to bring all these strands of thought together in the form of a website forum portal (www.anticounterfeitingforum.org.uk/) which not only provides a repository for all sorts of related information on the subject but also gives industry the facility to report suspect devices and add these to an online database allowing others to search for parts already recorded as possible counterfeit items. You do not need to be a UKEA member to register[15] to use this facility and although this is a UK initiative, they welcome users from other nations and indeed Roger showed that it already has a significant proportion of registered members from the USA, Canada, Russia, Israel and Hong Kong, for example.

The seminar was completed with a question and answer session in which all the speakers participated and a hearty round of applause was given from all the delegates.

References

1. www.ukelectronicsalliance.org.uk
2. www.cybercrime.gov/aljaffIndict.pdf
3. www.cybercrime.gov/felahyPlea.pdf
4. www.ecsn-uk.org
5. www.cog.org.uk
6. www.oecd.org/dataoecd/57/27/44088872.pdf
7. www.cbsnews.com/stories/2008/11/06/60minutes/main4579229.shtml
8. www.semiconductorcouncil.org
9. www.sia-online.org
10. www.eeca.eu
11. www.sae.org/technical/standards/AS5553
12. www.gifas.asso.fr/en/index.php
13. www.iec.ch/dyn/www/f?p=102:7:0::::FSP_ORG_ID:1304
14. www.timesonline.co.uk/tol/news/uk/article2641861.ece
15. www.anticounterfeitingforum.org.uk/register.aspx