Counterfeits Threaten Security and Thwart Innovation

Peter Hlavnicka, Director, Brand Protection and Compliance Americas, Dolby Laboratories, Inc., www.dolby.com, AGMA Treasurer and Education & Program Committee Chairperson, www.agmaglobal.org

Our world is unimaginable without electronics. From laptops, tablets and smart phones to TVs, and game consoles - from public infrastructures such as air traffic control, financial and communication networks to government and military systems – we live in an interconnected, “always on” world. Due to their much higher failure rate versus genuine equipment, counterfeits pose a threat not just to consumer safety but also to national security - because when they fail the entire systems in which they are embedded may also fail.

According to a study by the U.S. Department of Commerce Bureau of Industry & Security (www.bis.doc.gov [1]), the number of counterfeit incidents reported by survey participants (including original component manufacturers, distributors, brokers, circuit board assemblers, contractors and subcontractors, and Department of Defense agencies) climbed from 3,868 in 2005 to 9,356 in 2008 - an increase of more than 140 percent.

IPC - Association Connecting Electronics Industries, in an article titled, "Preventing the Use of Counterfeit Chips," said: "Tracking the size of the counterfeit chip market is difficult, but some estimates put it as high as 5 percent of the global semiconductor market." The semiconductor industry generated approximately $250 billion in sales in 2008, so 5 percent represents about $12 billion worth of re-marked or fake components.

Counterfeits are non-genuine goods traded with breach of intellectual property (generally patents, copyrights, and trademarks). Counterfeits are inferior products sold as the genuine article and typically fail to meet the full range of genuine product specifications and performance standards.

Unauthorized Production (Replication) and Distribution

Counterfeiting of ICs and other semiconductors may be done by unauthorized reproduction of layout design/topography using the optical copying with subsequent fabrication of a semiconductor under a different company's name. Another form of counterfeiting is reverse engineering and producing what physically appears to be an identical product and selling it without authorization under the original company's name and trademark.

Re-labeling, Repackaging Existing Product

The huge accumulations of electronic scrap or e-waste have become a source of used components, which are cleaned and re-marked to disguise the parts that can differ greatly from those offered by the original part manufacturer. These tainted goods are often sold as new parts.

Counterfeit components cost the industry over $15 billion a year, a price tag that includes the cost of rework and other services. One of the notorious areas for counterfeiting is hard-to-get and obsolete parts. The victims are the industries exempt from RoHS (Risk or Hazardous Substances) laws such as military, aerospace, and medical industries which seek leaded parts that have been discontinued by manufacturers. Most counterfeit parts come from Southeast Asia, particularly China. Guangdong Province is home to Shenzhen, which has a high concentration of land-filled electronics waste. In fact, the city of Guiyu is considered the e-waste capital of the world. There, a reported 5,500 family workshops process 1.5 million tons of e-waste a year, according to according to a city Web site. Here, in what many would consider sweat shops, components are pulled off discarded printed circuit assemblies. The parts are then cleaned, re-tinned, black topped, and re-stamped. Some may have their contents erased.

Counterfeit identification such as testing may be required where component markings have been forged. For example a single lot/date code marked on counterfeit devices can disguise
• Parts originating from multiple inspection lots;
• Parts produced by multiple manufacturers;
• Different versions of the same part;
• Devices of completely different functions;

The buyer must make adjustments to physical and materials analysis evaluation criteria to detect various forms of counterfeiting. Electrical testing can help reveal suspect lots, but may not detect counterfeit parts without a test plan designed specifically for the device type under test and may not detect damage induced by inadequate handling and storage, termination, refurbishing, or reclamation.

The impact of counterfeiting is always greater than the value of the counterfeit product itself. By damaging consumers' perception of performance, reliability, and safety associated with branded devices, counterfeiting tarnishes brand image, customer loyalty and satisfaction. It also has broader negative effects such as reducing the value of intellectual capital, eroding profitability and stifling innovation. It doesn't just hurt the companies making the components, it impacts the financial health and ability to invest in future innovation of all companies across multiple industries - from intellectual property right holders of software/firmware/codec embedded in these devices, to proprietary SOC architectures.

About AGMA
AGMA is a non-profit organization comprised of influential companies in the technology sector. Incorporated in 2001, AGMA's mission is to address gray market fraud, parallel imports, counterfeiting, software piracy, and service abuse of technology products around the globe. The organization's goals are to protect intellectual property and authorized distribution channels, improve customer satisfaction and preserve brand integrity. To learn more about AGMA's initiatives or to become a member, please visit www.agmaglobal.org [2].

Links:
[1] http://www.bis.doc.gov
[2] http://www.agmaglobal.org