Open Journal of Social Sciences
2013. Vol.1, No.7, 12-16
Published Online December 2013 in SciRes (http://www.scirp.org/journal/jss)
http://dx.doi.org/10.4236/jss.2013.17003

The Counterfeit Electronics Problem

Michael Pecht
Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park, MD, USA
Email: pecht@calce.umd.edu, diganta@umd.edu

Received August 2013

Counterfeit electronics have been reported in a wide range of products, including computers, telecommunications equipment, automobiles, avionics and military systems. Counterfeit electronic products include everything from very inexpensive capacitors and resistors to costly microprocessors to servers. This paper describes the counterfeit electronic products problem, and discusses the implication of counterfeit electronics on the electronic supply chain. We then present counterfeit detection and prevention techniques for electronics.

Keywords: Counterfeiting; Supply Chain; Authentication

Introduction

Counterfeiting is an infringement of the legal rights of an owner of intellectual property (Tiku, Das, & Pecht, 2004). Counterfeit goods mean any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country (of importation) (World Trade Organization, 2006).

Counterfeiting exists, because it is a way to make money by by-passing the research, development, marketing and sometimes the quality and reliability aspects of the original product. Sometimes these look-alike products are sold on the open-market under a slightly different brand name; other times the products are sold as the original. The first type of product usually involves the issue of intellectual property and copyright infringement and can be associated with a specific manufacturer. The latter product is usually slipped into the stream of commerce surreptitiously, often through unknowing or corrupt distribution channels and it is hard to trace it back to the original source. This paper deals with the second type of counterfeiting.

Counterfeit electronics have been found in computers and telecommunication products, as well as automobiles, avionics and even military electronics. Whenever a product can be made cheaper than the original, counterfeiting can occur. Counterfeiting has been found to be further encouraged if there is a lack of supply of the original product. In fact, products and systems that are in service for long periods of time or have long-term warranty requirements are particularly susceptible to counterfeit products. The reason is primarily associated with the obsolescence (lack of availability) of the products used in these systems. When the demand for replacement products becomes high, the price of such parts increases providing counterfeiters' opportunities for profit. In addition, replacement of obsolete products often leads to purchases from less reliable sources such as part brokers[1] and online exchange services instead of franchised[2] or independent[3] distributors. In cases of brokers and online exchange services, the actual sellers are often unidentified.

Risks from Counterfeit Electronics

It is estimated that legitimate electronics companies miss out on about $100 billion of global revenue every year because of counterfeiting (Pecht & Tiku, 2006). That figure takes into account only the profits that counterfeiters siphon off from manufacturers; it ignores the added repair and maintenance costs necessitated by defective bogus parts and the expenses of trying to identify and intercept suspected counterfeiters.

The economic repercussions of counterfeit products reach far beyond the cost of merely replacing the items. For example, an electronic component that may be worth only $2 can cost as much as $20 to replace if it is detected to be counterfeit after it is mounted onto a circuit board (Sullivan & Graham, 2001), and failures of systems that use counterfeit electronics can cause loss of mission, safety problems, and significant maintenance and logistics costs.

For the consumer, the failures of systems that use counterfeits can lead to safety and security problems. Even if the fake part works, at least initially, it still poses reliability risks, because it hasn't undergone the legitimate manufacturer's rigorous quality assurance processes (Pecht & Tiku, 2006).

When counterfeit parts make their way into safety related applications, there is risk to the system manufacturers since the original counterfeit part manufacturer(s) may not be identified or be brought into any legal or regulatory system. Even in cases of failures of electronics in commercial applications, the final products manufacturer will remain liable for failures due to counterfeit parts. They will have little chance to recoup the cost of such liabilities from a counterfeit part manufacturer. It will be hard to locate, prosecute or even recover the penalties from

[1]Part brokers are scouting agencies for "hard to find" replacement parts and components that hold inventory of possible sources of parts and not the parts themselves and may also search for parts only when the need arises.
[2]The term "franchise" refers to a continuing commercial relationship between the franchisee and the franchiser. Franchisee distributors are those who have signed selling and marketing contract with part manufacturers for the distribution of goods or services identified by the franchiser's trademark or trade name.
[3]Independent distributors are aftermarket sources of parts that offer end users parts and service. They make a one-time purchase of parts without continued commercial relationship with the manufacturer/supplier.

them.

Counterfeiting issue can also be seen as a part quality problem. Counterfeit parts can have a major variation from the original parts in material, construction and electrical properties. Even when the counterfeit parts are close to the original parts in quality—they are still not manufactured and evaluated in accordance with the manufacturer's standard qualification and acceptance procedures. These counterfeit electronic parts can be copies of original parts but can also be re-labeled or repackaged, and even be recovered from scrap and recycled.

Counterfeit parts pose another type of risk to the system manufacturers besides quality. The parts may not meet the safety or environmental rules for the market in which the product is marketed. For example, the European Union's Restriction of Hazardous Substance (RoHS) bans the use of lead and five other substances from being used in electronics equipment sold in Europe. If counterfeit parts that claim to be RoHS compliant does contain the banned substances, the company making products with those parts may be liable for breach of the law. Some analysts think that huge demand for RoHS compliant parts in Europe will lead to shortages, which would indirectly facilitate the entry of counterfeit RoHS parts in the supply chain through part brokers (Carbone, 2006).

Detection of Counterfeits

The actual extent of counterfeit electronics is difficult to estimate. For an electronics equipment manufacturer, it is challenging to identify counterfeit product from among the thousands of products used to assemble a system. In some cases, the counterfeit may have been introduced several steps earlier in the supply chain, and is part of a module or assembly sold by a reputable company. Most manufacturers do not have the resources to trace the actual origins of every part in the product. Those who put counterfeit products in the supply chain go great lengths to duplicate materials, part numbers, and serial numbers to coincide with authentic products, making counterfeits hard to detect. Sometimes the parts may actually work, at least in carrying out some functions for a short period of time. Thus, without an anti-counterfeiting inspection procedure or construction analysis whereby the product is carefully analyzed, counterfeit products can enter into the supply chain undetected and be used in a variety of applications.

The detection of counterfeit products usually occurs when there is a system failure, and the subsequent root cause failure analysis investigation reveals that a part is counterfeit. However, failures are not always easily traceable and there can often be confusion as to whether the part was defective, was damaged (in assembly or use) or is counterfeit. In many cases, without proper root cause analysis, the failure can be attributed incorrectly to other causes (Thomas, Ayers, & Pecht, 2002). Furthermore, if the counterfeit functions as the original, it can be nearly impossible to detect, until a problem occurs. It would even be harder to detect a counterfeit RoHS part since it would not necessarily lead to system failure.

Examples of Counterfeit Electronic Products

Some examples of counterfeit products that have been publicly reported are discussed in this section. These examples illustrate the ease with which counterfeit electronics can find their way into electronic systems. We have grouped the examples into three categories: relabeling, illegal manufacturing, and scrap salvaging.

Examples of Relabeling

This section describes examples of counterfeiting where lower priced or lower grade items have been relabeled to appear as a costlier or a higher grade item. This type of counterfeiting largely occurs when new version products are introduced into the market. Counterfeiters buy a different version of the parts at a lower price, relabel them, and then resell them as the version required by the customer at a higher price.

As early as in 1998, counterfeiters were repackaging 266-MHz Pentium IIs as 300-MHz chips since 300-MHz Pentium II chips cost $375 per processor, while 266-MHz Pentium II chips cost $246 per processor. If a 266-MHz rated processor is operated at 300 MHz, it runs, but reliability becomes an issue since it becomes hotter at 300 MHz and can then give incorrect answers to instructions (Cnet Networks, 1998).

In May 2003, RAM Enterprises, a distributor, was convicted for manufacture and resale of counterfeit parts, falsifying documents, making false statements and providing counterfeit parts to companies for use in commercial and military aircraft and weapons systems. RAM was found to have knowingly sold counterfeit connectors that were allegedly manufactured by Tri-Star Electronics International Inc. by including a "false certificate of conformance" for part number M39029/4-112. In another instance, RAM had used a solvent to remove color bands from approximately 6500 connectors procured from Air-Electro Inc. (a maker of mil-spec connectors) to make them appear of a higher grade (Sullivan, 2003).

In the Fall of 2003, AMD conducted some raids in Europe, where some of its low speed, low priced microprocessors were being relabeled as high speed, high priced chips. On investigation it was found that some resellers in Shenzhen, China were performing the remarking. AMD also purchased some microprocessors from the resellers and found them to be fakes (Takahash, 2004).

Examples of Illegal Manufacturing

This section describes examples where complete parts have been manufactured and labeled to appear to come from an original manufacturer. These parts are then sold as being manufactured by the legitimate manufacturer.

On October 23, 2006, GIDEP issued an alert about a silicon-controlled rectifier, JAN2N1774A, of General Electric (GE) with lot code 9240. Lockheed Martin Missiles and Fire Control had experienced a high failure rate of these parts with the GE logo. Failure analysis of the devices by Lockheed Martin revealed poor materials and workmanship in numerous areas (e.g., nail bonds to die, lead crimps, marking permanence and die attach) (Government-Industry Data Exchange Program, 2006).

In early 2006, BAe Systems and Platform Solutions received 104 pieces of the CY37032P44-125AI parts, (Cypress Semiconductors with date code 0223 and the mark lot number 709673) from Aztec Components, a part broker. This lot of parts exhibited a high reject rate during programming at a test laboratory. Cypress Semiconductors checked the date code and lot number and the logo on the top surface of the parts and found that the markings were all forged (Government-Industry Data Exchange Program, 2006).

BAE Systems and Platform Solutions found another problem with 500 pieces of Linear Technology M38510/14802BXA parts they bought from Electronic Components Inc., a broker in 2006. On visual inspection, it was found the parts to be laser-marked rather than ink-stamped as is the case with Linear Technology's parts. The die of the suspected part was compared with that of a known good part and found to be 50% smaller. Also the mask set and wire bonding material were found to be different (Government-Industry Data Exchange Program, 2006).

On February 24, 2003, Maxim Integrated Products and its wholly owned subsidiary, Dallas Semiconductor, posted an alert on its website regarding counterfeit Maxim/Dallas Nonvolatile Static Ram (NVSRAM) modules (DS1230, DS1245, DS1250) being sold in Asia. The parts had been disguised and marketed under the Dallas Semiconductor label, using Dallas Semiconductor marked shipping tubes and boxes. The alert stated that the customer returns for these imitation modules revealed a wide variation of components and assembly techniques, quite different from the authentic parts (Electronics Supply and Manufacturing, 2003).

In some cases, the copies of products had comparatively easy to identify mistakes in their labels. On Sep 28, 2005 X-bit labs reported that forged hard disk drives similar to Maxtor Corps MaXline II HDDs were being sold in the Japanese markets. The counterfeit hard disk drives had incorrect font on the label and used lower case "X" letter in the brand name of MaXLine II (Shilov, 2005). Similarly, in 2003, Agilent Technologies Inc. had an experience with counterfeit parts when a customer returned an optocoupler for failure analysis. The part, which was bought through a broker, came under suspicion when the customer found the word "Singapore" spelled incorrectly on the part (Sullivan, 2003).

Examples of Scrap Salvaging

This section describes examples where defective or outdated items meant for scrap have been salvaged and then re-circulated into the supply chain. Electronic parts that are scrapped but not destroyed are cleaned, reworked and returned to the supply chain.

On September 28, 2004, GIDEP issued an alert regarding unauthorized distribution of Philips Semiconductors Part number PCD3311CT (musical tone generator IC) (Government-Industry Data Exchange Program, 2004) after L-3 Communication Systems—East of Camden, N.J. reported numerous failures. Philips Semiconductors found that the parts appeared to be scrap material that had somehow showed up on the gray market. Philips also indicated that they have received other similar customer complaints for parts with this part number purchased from unauthorized resellers.

On April 15, 2003, GIDEP issued an alert about a precision operational amplifier, LT1097S8 of Linear Technology Corp. (LTC) with lot code 0103. Textron Systems had experienced a high failure rate of these parts. LTC's visual and destructive physical analysis revealed the parts to be counterfeit. LTC also noted that the top of some parts appeared to have been sanded down and remarked; indicating that the parts were eight years older than they actually were date coded (Government-Industry Data Exchange Program, 2003).

In January 2005, Advanced Micro Devices (AMD), working in cooperation with Taiwanese authorities, seized a total of 60,000 counterfeit AMD microprocessors worth US $9.46 million during a raid on an electronics company in Tainan, southern Taiwan. The raid turned up suspect AMD microprocessors, including K7 [AMD Athlon XP] and K8 [AMD Athlon 64] models. The defective microprocessors, which were meant for scrap had been stolen from one of AMD's three packaging plants in Asia and shipped to Taiwan for remarking (Shilov, 2005).

On June 04, 2003, GIDEP issued an alert regarding the presence of a non-Cypress die within a Cypress military package 5962-8871305RA/PALC16L8-30DMB (a 20 pin CDIP, digital memory, lot code TAH9949). This part had become obsolete in 1999, and Telephonics had purchased more than 100 parts from two different brokers in April 2003. Since Telephonics engineers could not program the part with the Cypress algorithm, they performed a failure analysis that revealed a smaller die than that of a similar part with lot code THA9916. Also, while the THA9916 part had the Cypress logo, TAH9949 part had the MMI logo. Cypress has since indicated that traceability designators for military parts were missing in the purchased parts and that the "country of origin" code was wrong (TAH instead of THA for Thailand) (Government-industry Data Exchange Program, 2003).

Prevention Efforts

There are organizations that monitor and report on counterfeit products. One of the most active is the US Department of Defense Government-Industry Information Exchange Program (GIDEP); others include the US Department of Energy (DoE) Lessons Learned Program, the US Defense Industrial Supply Center, the Electronic Resellers Association International (ERAI), and the International Anti-Counterfeiting Coalition (IACC) (Science Applications International Corporation, 2002). These programs have been effective in alerting companies of known counterfeit products, but do not solve the cause of the problem.

To stop counterfeit products being introduced into assembled systems, manufacturers of critical systems must use checks and safeguards to ensure that the parts and modules contained within their systems are not counterfeit. These safeguards can range from specially designed tests, to aggressive overt and covert authentication techniques. Such overt or covert product protection makes counterfeiting harder and more expensive. Effective overt authenticating technologies enable the public to recognize, avoid, and report instances of counterfeiting, and covert technologies can alert company representatives and enforcement authorities to counterfeiting activity. Anti-counterfeiting technologies also provide evidential support in a court of law, where issues of product genuineness and liability may have to be determined (Tiku, Das, & Pecht, 2004). Different types of authentication techniques are available like data matrix codes, RFID tags, photonic inks, and microtaggants which can be used for rapid product authentication. We go over these techniques briefly and understand their interesting features.

A tool for supply chain management and retail inventory control is radio frequency identification (RFID) (SATO America, 2006). Radio Frequency Identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. RFID system consists of a tag, reader and a database. Chip-based RFID tags contain microchip and an antenna and are used to store and transmit authenticating data such as manufacturer name, brand name, model and a unique serial number. RFID tags are attached to or incorporated into a product for the pur-

pose of identification using radio waves. RFID reader, an antenna packaged with a transceiver and decoder, emits radio wave activating the RFID tag so it can read and write data to it. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer or the database. RFID tags have many applications in automated manufacturing and logistics control. But use of RFIDs demands that companies agree on a standard encoding scheme; to date that hasn't happened (Pecht & Tiku, 2006).

Another tool is data matrix code, which is a 2D code used for storing product specific information like identification number of the manufacturer, identification number of the part type, and the serial number of the specific part (Agapakis & Stuebler, 2006). The term matrix code applies to 2-D codes that code the data based on the position of black spots within a matrix. Each black element is of the same dimension and it is the position of the element that codes the data. Data matrix codes are applied with lasers directly on the part and are durable and typically lasts the life of the part. These codes are read with a reader, which can be linked to shop floor computer networks and accessed from remote locations. They have numerous advantages over barcodes. They don't require any labels for marking. Also, they occupy one-tenth of the space of the 1D barcode while storing greater amount of information and thus can identify very small components and dense sub-assemblies, which have no space for labels.

Photonic inks are manufactured to first be invisible, and secondly to photo-decay at precise wavelengths and are used in anti-counterfeiting measures (Bastia, 2002). Apart from authentication, photonic inks can also be used to embed a 2-D barcode into the product, or the product packaging in a covert fashion. These barcodes may contain data such as point of manufacture, distribution or even product specific data such as product type or other signature data.

Microtaggants is a covert tool for product authentication. Several different taggants are available. The taggants are used to create unique code that can serve as a unique fingerprint for a product. Examples of taggants include polymer based and rare earth material based. An example of a complete system using taggants is described in next section.

Authentication technologies should be used at each and every level of the supply chain from die to the final product packaging so that counterfeit parts don't find their way into the product. In-built authentication technologies not only help in tracking and tracing of parts through the supply chain but also aids in identifying counterfeit parts. Although no authentication technique is full proof but in many cases if the cost of fraud to the perpetrators can be made high enough then that can be a deterrent.

Each of the anti-counterfeiting methods has a cost and an associated effectiveness. Nevertheless, the International Anti-counterfeiting Coalition (IACC) reported in 2001 that Fortune 500 companies each spend between $2 million and $4 million (some companies are reported to be spending up to $10 million) annually to combat global counterfeiting (Sullivan, 2002). The goal is to keep counterfeit products out of the consumers' hands and the reseller channels.

Summary and Future Directions

Counterfeiting is an infringement of the legal rights of an owner of intellectual property. High profits, low risk of detection, and weak prosecution contribute to the supply of counterfeit parts. Counterfeiting of electronic parts causes potential hazards including safety and loss of profits to companies, as well as maligning the reputation of manufacturers and distributors. All types of parts and part manufacturers are susceptible to counterfeiting, as illustrated by the examples provided in this paper. A number of laws have been enacted in the United States to penalize counterfeit activities and other IP violations. Several private and public organized groups have also taken notice of and created technological and information-sharing tools to help the industry detect and avoid the use of counterfeit parts. But these measures do not solve the cause of the problem.

As illustrated by most of the examples of counterfeiting provided in this paper, parts bought through sources other than the manufacturers or authorized distributors have turned out to be counterfeit. The original equipment manufacturers (OEMs) should particularly avoid purchasing from unauthorized sources like part brokers since they have no direct relation or any commitment to the manufacturer or the buyer of the parts. Part brokers have negligible control over their supply and can be duped into purchasing and selling counterfeits. Furthermore, brokers can close shop at any time after supplying the parts, leaving the customer without the possibility of any follow-up action (Tiku, Das, & Pecht, 2004).

There are two complementary and parallel technical efforts in mitigating the impact of counterfeit parts. The first one is driven by the part manufacturers who can make their products harder to copy and make it easier to detect duplicates. The second effort comes from the point of view of part users whose effort is self protective in making sure that they can reduce the chances of buying counterfeit parts. The authentication technologies can work for both types of efforts. The direction of scientific research needs to ensure that the authentication methods can be made compatible with the production processes without major modifications or economic impacts. The research also needs to ensure that the addition of such methods do not result in unintended quality and reliability problems for the users.

REFERENCES

Agapakis, J., & Stuebler, A. (2006). *Data matrix and RFID—Partnership in productivity. Assembly magazine*. http://www.assemblymag.com/CDA/Articles/Feature_Article/6329c0d053ccd010VgnVCM100000f932a8c0____

Bastia, S. (2002). Next generation technologies to combat counterfeiting of electronic components. *IEEE Transactions on Components and Packaging Technologies, 25*, 175-176. http://dx.doi.org/10.1109/6144.991192

Carbone, J. (2006). *Watch out for bogus RoHS parts*. http://www.purchasing.com/article/CA6333246.html

CNET Networks (2002). How to spot pentium II fakes. http://news.com.com/2100-1001-210597.html?legacy=cnet

Electronics Supply and Manufacturing (2006). Maxim spots counterfeit parts selling in Asia. http://www.my-esm.com/showArticle.jhtml?articleID=6900447

GIDEP (Government-Industry Data Exchange Program) Alert, Document no. B8-A-03-01 dated April 15, 2003.

GIDEP (Government-Industry Data Exchange Program) Alert, Document no. UL-A-03-01 dated June 04, 2003.

GIDEP (2004). *Unauthorized distribution/sale of defective product, microcircuit.* GIDEP Document No. F8-A-05-01.

GIDEP (Government-Industry Data Exchange Program) Alert, Document no. EE-A-06-06B dated March 20, 2006.

GIDEP (Government-Industry Data Exchange Program) Alert, Document no. EE-A-06-07B dated March 20, 2006.

GIDEP (Government-Industry Data Exchange Program) Alert, Docu-

ment no. M9-A-07-02 dated October 23, 2006.
(2002). Other significant activities to address S/CI issues. http://twilight.saic.com/qawg/scitrend/Sci297/sci_sec4.htm
Pecht, M., & Tiku, S. (2006). Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum, 43*, 37-46. http://dx.doi.org/10.1109/MSPEC.2006.1628506
SATO America Inc. (2006). *RFID white paper*. http://www.rfidproductnews.com/whitepapers/files/SATO_RFID_WP_020106.pdf
Shilov, A. (2006). Fake maxtor hard disk drives hit the market. http://www.xbitlabs.com/news/storage/display/20050928224555.html
Shilov, A. (2006). Only 60 thousands fake AMD chips seized, million already shipped. http://www.xbitlabs.com/news/cpu/display/20050104071134.html
Sullivan, L., & Graham, J. (2001). *Fake parts plague industry. Electronics supply and manufacturing*. http://www.my-esm.com/story/OEG20010212S0054
Sullivan, L. (2002). *HP cracks down on counterfeit pc parts in China. Electronic business news*. http://www.ebnonline.com/story/OEG20020626S0013
Sullivan, L. (2006). *Distributor RAM found guilty on raft of counterfeit charges. Electronics supply and manufacturing*. http://www.my-esm.com/showArticle.jhtml?articleID=9800040
Sullivan, L. (2006). Counterfeit parts nettle buyers. Electronics supply and manufacturing. http://www.my-esm.com/showArticle.jhtml?articleID=13100410
Takahash, D. (2006). *The billon dollar problem. Electronics supply and manufacturing*. http://www.my-esm.com/print/showArticle.jhtml?articleID=19202225
Tiku, S., Das, D., & Pecht, M. (2004). Parts selection and management to avoid counterfeit electronic parts. In M. Pecht (Ed.), *Chapter 10, in parts selection and management*. NJ: Wiley Inter-Science.
Thomas, D., Ayers, K., & Pecht, M. (2002). The 'trouble not identified' phenomenon in automotive electronics. *Microelectronics Reliability, 42*, 641-651. http://dx.doi.org/10.1016/S0026-2714(02)00040-9
World Trade Organization (2006). Uruguay round agreement: TRIPS: Part III—Enforcement of intellectual property rights. http://www.wto.org/English/docs_e/legal_e/27-trips_05_e.htm