Counterfeit Electronic Components -- An Overview

Robert K. Lowry
Technical Affiliate, Oneida Research Services, Inc.
315-736-5480
www.ors-labs.com
and
Consultant in Electronic Materials
321-777-9949
www.electronic-materials.com

A police raid on a suspected counterfeiter in Guangdong province found $1.2 million in fake computer parts and documents—enough to produce complete servers, personal computers, and the packaging, labels and warranty cards for them. All the parts were neatly labeled with the logo of Compaq Computer Corp.

Electrolyte made from a stolen and defective formula found its way into thousands of capacitors used on PC motherboards, causing the components to burst and leak and the computers to fail, eventually costing more than $100 million to rectify.

Authorities in Suffolk County, N.Y. seized counterfeit electrical safety outlets—used in bathrooms, kitchens, and garages to guard against electrical shock—bearing phony UL logos. The bogus parts had no ground-fault-interrupt circuitry. Had they been installed anywhere near water, the results could have been fatal.

Dozens of consumers worldwide were surprised, or worse, injured, when their cellphones exploded, the result of counterfeit batteries that short-circuit and suddenly overheat.

These are just a few examples of the worldwide proliferation of counterfeit electronic components. From five to twenty percent of electronic components in distributors' supply chains are probably counterfeit. Counterfeits cost industry up to $100B per year.

Counterfeits decrease customer satisfaction and increase costs for legitimate manufacturers. They reduce yields, cause field failures, necessitate product inspection, and prompt litigation if/when they cause injury or take down high-value systems.

The pervasiveness of electronic component counterfeiting is increasing: "If you can make it, they can fake it." Even if counterfeiting stopped today, it would take years to flush all counterfeits from supply chains.

Counterfeit components can be defined as "items produced or distributed in violation of international property rights, copyrights, or trademark laws, or otherwise mis-represented in violation of intellectual property or other property law", and "electronic components whose materials, performance, or characteristics are knowingly mis-represented by the vendor, supplier, distributor, or manufacturer." These are not pure legal definitions, but suffice for practical purposes.

Entire truckloads of product have literally been hijacked off the street, or purloined from stock in "inside jobs" by employees. Stolen product appears in distributor supply chains at significantly marked down prices. Since it has original markings it is often impossible to distinguish from legitimate product.

A rich source of material for counterfeiters is electronic scrap. Manufacturers or distributors discard huge amounts of scrap or obsolete product, test failures, and excess inventory, without physically destroying it. Counterfeiters intercept this material, even retrieving some of it by dumpster diving.

Another rich material source for counterfeiters is product at the end of service life. Environmental regulations cause many countries to ship containers full of electronic waste to Asia to avoid local disposal. Counterfeiters re-mark this with different part numbers, recent date codes, uprated characteristics, etc. and return it to supply chains.

Otherwise-legitimate product is often sanded to remove original brands, blacktopped, and re-branded. Sometimes blacktopping is added on top of the original brand with new brand information applied to the blacktopping.

Midnight fabs also source counterfeit material. A contract fab may run two shifts for a customer, then continue running the same product on an unauthorized third shift, often with lower quality materials and lesser-trained personnel. This product is marked just like the legitimate product, but sold at discount, and is prone to quality issues.

About seventy percent of counterfeit product comes from China. Shenzhen, a port city in Guangdong province near Hong Kong, is a nucleus of counterfeiting activity. Untrained workers on city streets remove components from old boards and sort them in the sun and the rain with bare hands into paper cups. There are few if any precautions for ESD or contamination control. Product is displayed in huge bins along block after block of city streets: a gigantic electronics flea market. Read about the Shenzhen SEG Electronics Market at http://www.bunniestudios.com/wordpress/?p=147

Counterfeiting ranges from mom-and-pop shops in peasants' huts to organized crime rings. Contracts have been put out on the lives of security officers of legitimate companies who were getting too close to identifying organized crime rings.

Googling "Shenzhen electronic components" gives many links like:
"ShenZhen LanXinWeiYe Electronics Co., Ltd. Part Number Available **...**" Many of the links are broken, suggesting short term (shady?) businesses. Mobility is a counterfeiter's tactic. They often shut down only to re-open at different locations under different names.

Unlike in the west, where counterfeiting is at least naughty or immoral if not illegal, in China it is part of the entrepreneurial spirit. Authorities make few efforts to stop it.

Vulnerabilities of supply chains to counterfeits include:

- Instant pudding mindset: accelerated build schedules, JIT, faster/better/ cheaper.

- Excellent quality from legitimate manufacturers which enables time and cost reduction by eliminating product inspection, but no inspection leaves supply chains vulnerable to counterfeit entry.
- Offshoring and production outsourcing sacrifice control over product manufacturing and flow.
- Convoluted distributor supply chains are vulnerable to counterfeit entry. Worldwide, the Electronics Re-sellers Association (ERAI) has 1,100 members. Brokers' Forum, an internet trading platform, has 3,500 members. Product wending its way through these supply chains may go through five or more intermediaries. Few have supplier relationship or product inspection programs, leaving many opportunities for counterfeit product entry.

The first line of defense to assure product authenticity, implementable immediately, is incoming product inspection. An inspection protocol is outlined on page 4.

If brokers or distributors are not capable of product inspections beyond reading documents and external information on components, several commercial laboratories offer excellent inspection and materials and electrical test services.

Effectively addressing the counterfeit problem requires focused effort, paradigm shifts, and even paradigm reversals.

Component manufacturers must tightly control product flows and confirm physical destruction of scrap, overages, surpluses, and discarded products. They must share data sheets and product characteristics freely with users. They must consider gamma marking or other proprietary tagging methods that are hard to counterfeit. They must task their Security Departments to fight the problem by pursuing counterfeiters and working with US Customs to interdict counterfeit shipments. For application-critical components, serious thought should be given to repatriating manufacturing.

Component users must soften instant pudding expectations by planning more lead time in schedules with less emphasis on JIT, allowing time to verify authenticity. They should re-think price willing to pay (away from always lowest cost; "pay me now, or pay me later"). Users across the board must get positive control of scrap and waste product and assure physical destruction at disposal. Users minimize chances of receiving counterfeits by purchasing directly from original manufacturers or authorized distributors.

Distributors and brokers must implement initiatives to "know thy supplier" and secure their supply chains. Incoming product inspection is essential, either in-house or at commercial labs offering services. ERAI is offering relevant regional training classes to member distributors. Standard 1010A published by Independent Dealers in Electronics (IDEA) is a good resource for product inspection guidance.

The counterfeit component problem will not diminish soon. It takes awareness, supply chain scrutiny, robust inspections, and aggressive pursuit of offenders to curtail it.

A Product Inspection Protocol to Assure Electronic Component Authenticity

A. Read product documentation, shippers, etc. in excruciating detail. Check for stilted language expression, print fonts, information layout, and compare identifying product information against that on original purchase orders, etc.

B. External visual inspection and materials analysis of product.

1. Check logos, part numbers, date codes branded on product versus shipping documents and original purchase order information. Use logo libraries.
2. Measure physical dimensions (especially thickness) and weight of units.
3. Inspect marking workmanship: legibility, sharpness, clarity, etc.
4. Inspect for evidence of physical alteration: sanding, blacktopping, etc. Acetone will attack many blacktopping materials. Acoustic microscopy can image original, legitimate laser brands non-destructively through blacktopping.
5. Conduct marking permanency test on inked brands with 3:1 by volume mineral spirits: isopropyl alcohol.
6. Inspect laser marks for burn holes caused by aftermarket laser mark equipment.
7. Inspect pins and leads:
    a. Straightness
    b. Coplanarity
    c. For marks or gouges made by physical removal from sockets.
    d. For solder workmanship or any indication solder has been removed from or added to pins
8. Analyze lead finish by X-ray fluorescence or laser ablation/MS for the chemical element lead (Pb), pertinent to:
    a. Pb-free requirement for WEEE/RoHS, or
    b. Pb-containing finish to aid solderability or avoid tin whiskers for Mil-aero.

C. Non-destructive internal imaging. X-ray or acoustic microscopy for presence of die, wire bond workmanship, etc.

D. Destructive Physical Analysis and Internal Visual Inspection.

1. Chemically analyze mold compound to authenticate composition of plastic encapsulant, by infrared spectroscopy or acoustic impedance.
2. Fine/gross leak test and residual gas analysis of hermetically sealed units
3. Decap plastic unit. Delid hermetic unit.
4. Do die visual inspection. Compare logos, part numbers, other identifying information to original order documentation in (A) and external markings in (B1).
5. Inspect die for device critical dimensions, wire bond quality/ workmanship, die mount anomalies, etc.

E. Advanced analytical techniques. Apply as appropriate to obtain more detailed information about device construction at die level.

F. Electrical test. Test electrical function or parametrics and compare to specified requirements on data sheets for authentic product.

It may not be necessary to do all tests in the protocol to assure product authenticity. Extent of inspection is determined by each product situation and expectations and needs of the customer. Time, cost, and complexity of testing generally increases in A-F order of the protocol, although electrical tests can be done as appropriate throughout the testing protocol.