Counterfeit threat for electronic industry on rise: plug it

Author: Author is Secretary of Hologram Manufacturers Association of India (HoMAI) since 2006 and also serves as Editor of The Holography Times.

C S Jeena

Brief Abstract:
Counterfeiting is not a new term for electronic industry as counterfeit electrical and electronic products now occupy second place after pharmaceuticals estimated to range anywhere between US$11 billion to $20 billion worldwide every year. However, counterfeit electronic parts have been much in the public eye in recent weeks. On March 28, 2014 one of Indian Air Force Aircraft (C-130J Super Hercules) crashed near Gwalior city killing five crew members. There were controversial news reported in media about the counterfeit electronics being the reason for C-130J air crash. Over the past several years the electronics industry has seen a marked increase in the availability of counterfeit electronic components. Counterfeiters have attacked every commodity of electronics, from simple components such as capacitors, to complex integrated circuits such as microprocessors. In expensive commercial devices, as well as high cost military components, have seen counterfeiting on the rise. This article highlights the serious risk, its impact and the possible proactive steps that can be taken to curb this menace.

Introduction:

Imagine incidents such as an aircraft crashing due to malfunctioning counterfeit parts, a medical equipment blurs off in the middle of the surgery, a missile misses the target and hits the own camp and a heavily invested satellite fails reaching its destiny or a fake mobile battery exploding even as one is using the phone. The counterfeit electronic parts are available everywhere from sophisticated semi-conductors and chips used in commercial and military electronics as well as the normal day to day used electronics items, and they represent a serious hazard if used in critical systems such as aircraft navigation, life support, military equipment, or space vehicles.

After the crash of the C-130J Super Hercules near Gwalior there were controversial news reported in the media about counterfeit electronics being the reason for this unfortunate incident. Actually, certain avionics displays fitted in this aircraft as original equipment were manufactured by L3 Display Systems Corporation, a US Company[1]. In *November 2010,* the company become aware that its in house failure rate for a chip installed on display units used in C-130J and C-27J had more than tripled from *8.5 percent* to *27 percent*. When sent for testing, the parts were found as suspected counterfeit. Although, the company did not give any recall notice, But when this matter became known to the public, the US Senate Armed Services Committee decided to investigate the matter and released its report on *May 21, 2012*. The report admitted that counterfeit electronics parts were breaking into the defense supply chain and could endanger the lives of troops and allies. While the report focuses on the risks posed to military systems, there is no reason to believe that the risks are any different for non-military systems[2].

1. *"Did IAF's 'US-made' C-130J Super Hercules that crashed have fake Chinese parts?," Chidanand Rajghatta,TNN | Mar 30, 2014 available at http://timesofindia.indiatimes.com/india/Did-IAFs-US-made-C-130J-Super-Hercules-that-crashed-have-fake-Chinese-parts/articleshow/32977838.cms*
2. *"Inquiry into Countefeit Electronic Parts in the Department of Defense Supply Chain: Report of the Committee on Armed Services United States Senate" hereinafter the "SAAC report," available at http:// www.armed-services. senate.gov/Publications/ Counterfeitpercent20 Electronic20percent20Parts.pdf.*

Table 1: Counterfeit Computer Hardware and Mobile Phone in India

Particulars		Computer Hardware	Mobile Phones
Estimated sales to Industry	Grey Market (percentage)	26.4	20.8
	Sales loss	INR 47.25 billion	INR 90.42 billion
Estimated tax loss to the Government	Direct tax loss	470 million	4.96 billion
	Indirect tax loss	11.87 billion	26.78 billion
	Tax loss to the exchequer	12.34 billion	31.74 billion

*The loss has been calculated for the year 2012

Size of counterfeit electronic components problem:

The making of counterfeit electronic parts has become a very big business. In fact, counterfeit electrical and electronic products now occupy second place after pharmaceuticals. Worldwide counterfeiting of electrical products is estimated to range anywhere between US$11 billion to $20 billion annually. In North America alone, the electrical product counterfeiting is estimated to be in the $300 million to $400 million range and rapidly growing[3]. Research from the Mobile Manufacturers Forum (MMF) says around 148 million counterfeit or substandard mobile phones were sold worldwide in 2013, mostly in developing countries[4].

Although not much has been done in India to assess the impact of counterfeit electrical components, there is a study by FICCI CASCADE that focused on computer hardware and mobile phones. According to this study counterfeit computer hardware constitutes 26.4%, or ₹ 47.25 billion by value, of the total market size estimated at ₹ 179.01 billion for 2012. Similarly, the Grey market for Mobile Phone constitute 20.8%, or ₹ 90.42 billion by value, out of total market size estimated at ₹ 434.09 billion in 2012[5]. *(See Table 1).*

Most commonly counterfeited electronics items

From components such as fuses, cables and circuit breakers to household equipment, professional work tools and automotive and aviation spare parts, nothing is safe from counterfeiting. While the appearance and packaging can be very convincing, the products themselves are often sub-standard and may represent a severe safety hazard, causing accidents and costing lives. *(See table 2 and Table 3)*

Reason / factor for increase in electronic components counterfeiting:

The problem is, increasing because of various factors, including global as well as local such as;

3. *"Sharks in the Water," By John Estey, National Electrical Manufacturers Association, T&D World Magazine (May 2007) available at http://tdworld.com/business/sharks-water*
4. *"Counterfeit/Substandard Mobile Phones, A resource guide for Government," White paper published by Mobile manufactures Forum available at http://www.mmfai.org/public/docs/eng/MMF_CounterfeitPhones_EN.pdf*
5. *"Socio-Economic Impact of Counterfeiting, Smuggling and Tax Evasion in Seven Key Indian Industry Sector," published by FICCI Committee Against Smuggling and Counterfeiting Destroying Economy (CASCADE) available at http://www.ficci.com/spdocument/20190/Executive-Summary-invisible-enemy-aug-8-2013.pdf*

Table 2: Percentage of Market Revenue for Most Commonly Counterfeited Product Types by Application Market in 2011 (Percentage Share of Revenue in Millions of U.S. Dollars)

Part Type	Industrial	Automotive	Consumer	Wireless	Wired	Computer	Other
Analog IC	14%	17%	21%	29%	6%	14%	0%
Microprocessor IC	4%	1%	4%	2%	3%	85%	0%
Memory IC	3%	2%	13%	26%	2%	53%	1%
Programmable Logic IC	30%	3%	14%	18%	25%	11%	0%
Transistor	22%	12%	25%	8%	10%	22%	0%

Source: IHS iSuppli March 2012

Table 3. Top 5 Most Counterfeited Semiconductors in 2011 (Percentage of Counterfeit Part Reports)

Rank	Commodity Type	% of reported Incidents
1	Analog IC	25.20%
2	Microprocessor IC	13.40%
3	Memory IC	13.10%
4	Programmable Logic IC	8.30%
5	Transistor	7.60%

Source: IHS Parts Management 2012

1. **Global number of illegal manufacturing due to shortcoming of existing legislation:** According to Electronic Industries Association of India ELCINA, the component industry has suffered because duty-free imports of about 217 categories of electronic components like capacitors, resistors and transformers were allowed from 2005 under an information technology agreement with the World Trade Organization (WTO-ITA1). Many of India's more than 1,000 small companies manufacturing electronic components have shut operations[6]. In an investigation spanning six months, the Directorate of Revenue Intelligence has found that for over 3,673 items brought from China, the importers usually declared 1-9 *percent* of the actual value of the goods[7].

2. **Easy availability of material due to global E-Waste handling:** China may be a principal source of counterfeit parts, but the United States and other countries in the developed world generate the electronic waste ("e-waste") from which semi-conductors and other micro-electronic parts are extracted by counterfeiters. The parts recovered from the salvaged electronics waste which are non-functional are processed by the counterfeiters to give a look of an original component[8].

3. **Inadequate surveillance efforts by brand owner to identify counterfeit products**;

4. **Tampering/Repackaging:** Counterfeit electronic component enter the supply chain through local manufacturing, importing from China in the form of fake packaging or in original packaging sourced from mechanics or service stations;

5. **Higher margins:** In comparison to genuine electronic component makers, a counterfeiter earns anywhere from 35 *percent* to 75 *percent* on selling counterfeit electronic parts.

6. **Consumer Education:** Lack of consumer education to identify authentic electronic

6. *"Dragon on the Rampage: A flood of cheaper Chinese goods, sometimes better than their Indian counterparts, is forcing small manufacturers to shut shop and turn into traders," by Taslima Khan, Edition: Mar 2, 2014 published by Business Today available at http://businesstoday.intoday.in/story/chinese-imports-hitting-india-msme-sector/1/203041.html*
7. *MP3 player for Rs 2, LED torch for Rs 8: Undervalue Chinese imports, make a killing, C Unnikrishnan, TNN.*
8. *"U.S. e-waste drives counterfeit components problem," by Victoria Fraza Kickham, published by Global Purchasing available at http://globalpurchasing.com/latest-news/us-e-waste-drives-counterfeit-components-problem*

Table 4: Impact of counterfeit component components

Consumers	Legitimate Manufacturers	Government / Social
Loss of Life	Loss of revenue	Loss of revenue
Loss of Job	Increases warranty costs and so the maintenance cost	Funding of criminal enterprises
	Financial Liability due to law suites	
	Loss of brand integrity and goodwill	
	Expected life of the product decreases	

parts and about the ill effects of counterfeit parts.

Impact of counterfeit electronic component = huge social and financial liability:

When counterfeit electrical devices, components and spare parts enter manufacturing supply chains, they can add fire, shock and explosion risks that may cost workers their lives, cause serious property damage and involve unpredictable financial liability. One fake component can void guarantees for entire systems and installations, resulting in severe financial losses and liabilities. Manufacturers, installers, specifiers and employers can be held responsible for incidents and accidents linked to counterfeit components. Counterfeit electrical products do not comply with performance and safety specifications; they are not tested or approved. Counterfeit aviation parts, for example pose a serious risk to the safety of military, civil and commercial aviation industry.

Steps in combating electronic counterfeiting[9]

Several studies have been done to measure the impact of the problem, but suggested solution has invariably focused primarily on enhanced effectiveness of law enforcement. It is important that a holistic solution is developed in this fight. The solution to this ever-growing menace lies at the very core of the product, i.e. a dire need to create an end-to-end holistic brand protection strategy[10];

As a first step, every CEO or Brand owner should take head on the threat of brand attack and prepare a Brand Risk Management (BRM) plan as an intrinsic part of the overall business plan, review and report. The team may comprise the CEO/ Brand owner, Brand Managers, Head of Marketing, Product Development, Sales, Logistic, Packaging, Manufacturing or an outside consultant accountable for the brand. The idea is to curb the penetration of counterfeits, across levels.

The anti-counterfeiting strategy can be broken into various stages such as:

i. **Anti-counterfeiting policy and brand protection program**
By establishing and pursuing an anti - counterfeiting policy and brand protection program a company is able to provide proof that all due care was taken to limit or reduce counterfeiting and protect trademarks and brands. Together they provide a shield for liability, and also a protection against loss of reputation and adverse public opinion. The brand protection program and anti-counterfeiting policy should list pro-active measures that are put in place toidentify and report fake products. They help limit the negative effects of counterfeiting and reduce reaction time should such an event occur.

Elements to consider include:

- supply chain processes, inspection, audits and quality control
- Identification and evaluation of risks and threats
- Detection and reporting processes, including handling of counterfeit products
- Overall risk-management and adequate response procedures

The policy also needs to address product labelling (including anti-counterfeiting technologies) and training of staff on how to recognize counterfeit products. Furthermore, it should provide assistance and training programs to officials tasked with enforcing seizures of counterfeit products. The latter because only the manufacturer of the genuine product knows whether an item is fake or genuine. Part of this may include the setting up of a product database, online reporting mechanisms, and simple protocols that provide investigators with tips on how to spot fakes.

9. *Brand Protection: Challenges and Solutions, Pradip Shroff, Published at The Holography Times, Volume 4, issue 13 available at http://www.homai.org/AdminPanel/PDF/Issue13.pdf*
10. *ISO Standards 12931 "Performance criteria for authentication solutions used to combat counterfeiting of material goods", http://www.iso.org/iso/catalogue_detail?csnumber=52210*

ii. Register trademarks and copyrights

Register trademarks in all countries you sell, manufacture, and license or distribute products in. This is essential to protect trademarks and brands. Also, apply for patents and register designs. For details and registration procedures, consult a trademark attorney.

iii. Adopt ISO standards and Join trade associations

ISO has developed new Standards 1293 "Performance criteria for authentication tools used in anti-counterfeiting or material goods": The new ISO 12931 is already published and would be a very useful document for any-one who wants to follow globally accepted standards and approach to fighting against the counterfeit. The ISO document can be seen on http://www.iso.org/iso/catalogue_detail?csnumber=52210[10]. It is strongly recommended that all brands who want to have a safety net of a global standard, should plan to comply with this standard.

Similarly, SAE International, a global association of more than 138,000 engineers and related technical experts in the aerospace, automotive, and commercial-vehicle industries has come up with the first revision to its counterfeit parts avoidance technical standard **"AS5553 Fraudulent/Counterfeit Electronic Parts;Avoidance, Detection, Mitigation, and Disposition.[11]"** This new revision in particular provides terminology references and reporting mechanisms to facilitate the flow-down of the standard globally. Further, try to join anti-counterfeiting association or your local chamber of commerce, such as FICCI CASCADE, as these national and international trade bodies can guide and provide best practices against combating counterfeiting. For example, The National Electrical Manufacturers Association is so concerned about this influx of counterfeit products that its board of governors has made it one of its top-three priorities to focus the attention of government, the supply channel and the public on the harm caused by counterfeit electrical products[12]. In India, FICCI CASCADE[13] is doing similar work.

iv. When fake products are found

After contacting the relevant law enforcement authorities, consider reaching out to a member of the IEC Conformity Assessment System[14] (For India it is BIS). They can direct you to one of the national certification agencies and laboratories who might be able to help you set up a testing and inspection program to avoid future problems, as well as product training for manufacturing staff and law enforcement agencies.

v. Anti-counterfeiting technologies[15]

There are a number of anti-counterfeiting technologies that can help better protect and authenticate products. And while they can't completely eliminate counterfeiting, they can make it less attractive and less profitable, increasing the level of risk for the counterfeiters. Use a secure, anti-counterfeiting device comprising overt, covert & forensic security features like security hologram seals and labels, tamper evident security films and light-sensitive ink designs. While there a number of technologies available in the market, it is advisable to choose smart and at the right time while keeping track of some basic guidelines like:

- Instead of focusing on features, find a vendor who can provide you overt as well as covert technologies as it is important to select a solution using multiple technologies.
- Seek help from an established trade association to select ethical vendor, best practices and resources to fight counterfeiting.
- Select the technology in terms of the difficulty in replicating and tamper evidence offered, uniqueness, availability of suppliers, ease of identification and user friendliness.
- Solutions should also have feasibility of being integrated with the automated production/ packaging line if required, especially wherever the volumes are very large

  Try to combine low and high security elements to enhance protections, for example, by integrating sequential or unique numbers in the solution.

vi. Market surveillance, quality control, inspection

- Establish classical market surveillance, including at customs barriers and ports
- Obtain and test samples from open markets, websites and auction sites. Make it known that you run such tests
- Keep a database of companies and manufacturers that

have been suspected to counterfeit your products

- Send "Cease and desist" letters for every infringement to establish brand and trademark protection measures
- Tighten supply chain, production and delivery path of genuine products
- Establish factory, pre-shipping and port of entry inspections (as counterfeit products sometimes hide in genuine shipments) consider involving an IEC Conformity Assessment System member for inspection and testing pre-shipping and at market entry point.

vii. Interception and cooperation with law enforcement

Registered for customs watch programs. Organizations including Interpol, World Trade Organisation, World Customs Organization, World Intellectual Property Organization and International Chamber of Commerce are working closely together to improve international cooperation and border enforcement through increased customs co-ordination and exchange of information and best practices. The IEC and its Conformity Assessment System members concretely support these efforts on the ground through inspection and testing.

Conclusion:

While the trade of counterfeit electronic parts has dramatically increased, tackling counterfeits is not impossible. Counterfeiting is a problem that needs to be addressed quickly and decisively. Ideally, as a first move, more effective partnerships should be built between law enforcement agencies and the private sector with focus on intelligence sharing, awareness and product identification training.

- Manufacturers should create a team that focuses on anti-counterfeiting strategy
- Selection of right anti-counterfeiting strategy should be employedUse first level of authentication features to empower your customers to identify your genuine products
- Track supply chain at distributor end
- Information to customer

In our view a company that implements the suggestions outlined in this article will definitely see a marked improvement in their fight against counterfeiting. In case you need more information, please e-mail to us at info@homai.org and we will be happy to work with you to eliminate the menace of counterfeiting.

Resources

1. *"Counterfeit Electronic Parts: What to do Before The Regulations (and Regulators) Come?," Federal Contracts Report, 97 FCR???,6/21/2012, The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com*
2. *"Counterfeit Chips on the Rise," IEEE Spectrum (June 2012), available at http://spectrum.ieee.org/computing/hardware/counterfeit-chips-on-the-rise.*
3. *KPMG Study: Managing the Risks of Counterfeits in the IT Industry (on file with the authors) available at:http://www.agmaglobal.org/press_events/press_docs/Counterfeit_WhitePaper_Final.pdf ("No anticounterfeiting effort is entirely foolproof, but the better ones can make a significant differences."*
4. *ChinaWTO.com, "Trade Regulations, Customs and Standards," at http://chinawto.com/wto/index-e.asp?sel=info&info=regulation.*
5. *"Counterfeit threats for electronic parts," by Nicole Faubert (December 30, 2013) available at http://thecounterfeitreport.com/article/253/Counterfeit-threats-for-electronic-parts.html*
6. *"The Counterfeit Repair Parts Tsunami," by Robert M. Williamson available at http://www.swspitcrew.com/articles/Counterfeit%20Parts%200911.pdf*
7. *"Counterfeit components: Methods to protect against fake parts," avilable at http://www.eeherald.com/section/sourcing-database/component_sourcing_guide2.html*
8. *HOMAI – Hologram Manufacturers Association of India, www.homai.org*
9. *How to Select a Security Feature - a Structured Guide for the Selection of a Security Technology for Documents and Items of Value, Published in June 2009 by the Document Security Alliance (DSA) and North American Security Products Organization (NASPO)*
10. *The Serious Risks From Counterfeit Electronic Parts, Forbes*
11. *"SAE International's counterfeit electronic parts risk mitigation standards," at www.sae.org*
12. *NEMA, Public Policy, Anti-Counterfeiting, https://www.nema.org/Policy/Anti-Counterfeiting/pages/default.aspx*
13. *FICCI Committee Against Smuggling and Counterfeiting Destroying Economy (CASCADE), http://www.ficci-cascade.com/*
14. *"Piracy in Electrical and electronic products: Anti-counterfeiting best practice and strategies," International Electrotechnical Commission available at http://www.iec.ch/about/brochures/pdf/conformity_assessment/IEC_Counterfeiting_brochure_LR.pdf*
15. *"Steps to Identify Authentication Solutions to Curb Counterfeiting," C S Jeena, published at The Holography Times, Volume 7, Issue 20 available at http://www.slideshare.net/cjhomai/steps-to-identifyauthenticationsolutionstocurbcounterfeiting*