A Rochester Electronics White Paper

The Cost of Counterfeit Semiconductors to the Electronics Industry

Worldwide Corporate Headquarters

Rochester Electronics, LLC · 16 Malcolm Hoyt Drive · Newburyport, MA 01950

phone 978.462.9332 · *web* **www.rocelec.com**

Introduction

Semiconductors provide “smart functionality” to all electronic systems. These devices are key to every segment of the electronics manufacturing industry, which today exists across the globe.

The high demand worldwide for semiconductors has made the market attractive to counterfeiters. Statistically, it has been proven over the years that counterfeit devices have a substantially high failure rate. Any semiconductor failure is costly, but in any of the many life-critical applications, failure can be catastrophic.

These failures can be expensive, but the actual costs precipitated by the counterfeit industry are far more wide spread, and directly affect every aspect of the electronics industry.

Several industry factors work in favour of the counterfeiters:

- To provide the low-cost semiconductor components to as large a customer base as possible, semiconductor manufacturers make use of the lower-labour-cost areas of the world where security may not be highly enforced.
- Semiconductor technology is continually evolving, and many of the devices are manufactured only for a short period of time, sometimes as short as one to two years. At the same time, demand for these components can continue for many years – even twenty or more. This provides a ready market.
- Due to the frequent upgrading of manufacturing facilities and to the nature of the larger-volume markets where semiconductors are used, the demand and supply frequently go through major peaks and troughs with times of product surplus and product shortage. During times of shortage, counterfeiters can make large profits.
- Counterfeit semiconductors are difficult to identify.
- The Internet makes marketing easy and anonymous.

In this paper we will look at the costs incurred throughout the electronics industry because of counterfeit components. And we will demonstrate what values can and cannot be measured.

Cost to the Semiconductor Manufacturers

Semiconductor manufacturers are the organisations most directly affected by the counterfeiters. An analysis of reports received by original manufacturers from customers, together with data that are available from test houses, indicates that counterfeiting activity accounts for more than 2% of the worldwide semiconductor total available market (TAM). Based on this analysis, it can be estimated that the value of counterfeits that make their way into the supply chain will be over $US5 billion in 2011. This is the first clearly visible measure.

Semiconductor manufacturers are developing and employing solutions and techniques that make their components more difficult to counterfeit; however, much of the effort they employ is unproductive even though it still imposes a significant cost, which they must pass on to users through the selling price. And, often, these solutions work only for a short time because the counterfeiters continually update their techniques to work around the technologies developed by manufacturers. Because electronic equipment manufacturers are very sensitive to higher prices for semiconductors, and because these protective solutions are expensive, some manufacturers are reluctant to use them, especially on lower-cost devices. The cost of counterfeit protection measures can add from a fraction of a cent to over ten cents per device. Here are some anti-counterfeiting measures:

- Only some semiconductor manufacturers have their own manufacturing facilities; others use subcontractors for wafer production, assembly, and test. These subcontractors operate in many parts of the world, and manufacturers often use multiple subcontractors in different countries for the production of a single device. Manufacturers must exercise stringent controls to ensure security during initial manufacture, subcontractor operations, and shipment. Security measures must protect the products themselves as well as critical intellectual property (IP), both of which can be vulnerable to opportunistic counterfeiting operations.

- All semiconductor manufacturers must be aware of the dangers of counterfeiting. To protect themselves, companies must develop and implement security policies and procedures, and make sure personnel are trained to carry them out. Additionally, staff must be trained to recognise and check suspect returned product, to analyse devices, and to prepare reports that may assist government agencies to carry out productive raids, seizures, and prosecutions. Manufacturers must also supply feedback to their customers to maintain assurance of their credibility of supply.

- In order to fight against counterfeiters, manufacturers must be able to assist in the identification and prosecution of offenders. Prosecutions can proceed only when the original manufacturer has registered all IP and trademark information with the appropriate authorities. In Europe, this means that trademarks must be registered in all twenty-six countries of the EU. Applications for Action must be lodged with border control authorities before they can carry out raids and seizures on suppliers of counterfeits. This calls for considerable resources from company legal and security teams. The number of people directly involved depends on the size of the company and the nature of the business; it can vary from one person for the smaller manufacturers to more than ten for the largest. Assuming an average of three people per semiconductor manufacturer, for around 300 manufacturers worldwide, it can be estimated that at least 900 appropriately qualified people would be employed just on anti-counterfeit activities. If we assume an average salary and associated support expenses to be $US150 thousand per person per year, the total cost is at least $US135 million, not including the cost of any extra testing and evaluation equipment required.

- Some manufacturers are working to develop sophisticated identification technologies that can be included in the production of components. These technologies are difficult for counterfeiters to reproduce. One example is hidden, encrypted, on-chip performance designation and more sophisticated coded marking. Another example is radio frequency tagging of devices and packaging. This is an emerging process, and another measure that adds additional cost to semiconductor components.

Beyond these identifiable costs to semiconductor manufacturers are many other expense factors that are not so visible. Companies stand to lose incalculable income through the loss of credibility and brand image they suffer when counterfeits are discovered. Costs also rise when companies become reluctant to use some of the lower-labour-cost manufacturing sources because they are concerned that the security of the offshore manufacturing facilities and processes cannot be guaranteed.

Cost to Semiconductor Distributors

Franchised and authorised distributors, who procure their entire product from the original manufacturer or their authorised sources, are the least affected by the counterfeiting issue. These distributors also control their warehousing and shipping security. Because of these practices, their entire inventory is traceable. As a further protection, many authorised distributors provide their staff with counterfeiting awareness training.

Unauthorised sources, however, purchase from many different sources. Inventory is not traceable to the original manufacturer. These sources are most likely to acquire counterfeit parts or substandard parts that have been damaged because of improper handling.

Cost to the Electronics Equipment Manufacturers

When an equipment manufacturer sources semiconductors directly from a distributor authorised by the original manufacturer, no testing is necessary to determine the viability of the components because they are traceable and guaranteed.

But, when an equipment manufacturer sources product from unauthorised source, significant additional costs must be incurred to validate the components. Some equipment manufacturers test inventory themselves; however, due to the improved capability of counterfeiters and the cost of the necessary testing equipment, most are now using independent test houses.

Some testing can give a reasonable assurance about the credibility of a device, but the counterfeiters know and understand the capabilities of the test methods and are continually working on ways to deceive purchasers.

True, reliable testing of components can be done only by experienced engineers using the original manufacturer's equipment and test protocols; this, of course, can be done only with authorisation of the original manufacturer, and most test houses do not work closely with original manufacturers.

Here are some typical tests and test costs from these test houses:

- External visual inspection and paperwork check – more than $50 per hour
- Marking permanence – more than $50 per hour
- Scanning acoustic microscopy – more than $800 per hour
- XRF check of terminations – more than $500 per test
- X-ray check for internal – more than $500 per test
- De-cap inspection – more than $1,000 per test
- Electrical testing – more than $50 per test plus nonrecurring engineering (NRE) costs for developing and/or adjusting the test programme
  Sample NRE costs and additional costs:
  - $4,000 for simple logic devices
  - More than $30,000 for complex VLSI logic, processors, and mixed signal devices
  - Cost of any extra hardware/load boards

Because counterfeiters indiscriminately mix good and counterfeit parts together in the same lot, all components in a lot must be tested, at an expense that adds significantly to the price of components.

There are also semiconductor-related costs incurred by an equipment manufacturer that are not so visible or well understood:

- Purchasing staff must be trained about the dangers of counterfeit devices.
- Goods inwards staff must be trained to check incoming material, especially product sourced from non-authorised sources.
- Purchasing controls and protocols must be established and monitored. This may include limiting the sources of supply.
- When a counterfeit lot is detected, either by a distributor, test house, or at incoming inspection, there is likely to be a loss of manufacturing time and output while replacement components are sourced.
- If a counterfeit part does get through to production, the costs to the equipment manufacturer increase exponentially:
  - 10 times the original device price if the counterfeit is found at board test
  - 100 times the original device price if the counterfeit is found at equipment final test
  - 1000 times the original device price if the counterfeit is found after the equipment is in use

It should be remembered that the identified test costs apply only to purchases from non-authorised sources. However, due to concern about supply, the costs of training personnel, the extra vigilance, and the need for test house services or in-house test equipment, additional expenses are being imposed throughout the industry.

Cost to the Electronics Equipment Users

Counterfeit components cause extra expenses throughout all levels of the electronics industry. Equipment users are no exception:

- Semiconductors for repairs and scheduled maintenance must be purchased with the same care and attention expended by the original equipment manufacturers when they purchased the original components.

- Counterfeits that are not detected and make their way into manufactured equipment are likely to cause equipment failures. These failures increase downtime, especially when replacement parts must be sourced.
- A more sinister development in counterfeiting semiconductors is the malicious implanting of hidden bugs and/or encryption designed to initiate equipment malfunction or to allow non-authorised detection of intellectual intelligence.
- Semiconductors are used in many life-critical applications in which failure could cause a catastrophic accident. Because the rate of failure of counterfeit components is high, equipment manufacturers can be open to significant implications that could lead to major increases in legal protection fees.

Conclusion

Counterfeit semiconductors not only constitute a danger to the entire worldwide electronics industry, they also add cost to every level of the industry involved.

Most semiconductor and electronics equipment manufacturers are working to overcome the counterfeit problem, but the costs are high, and the entire industry must pay.

There are some counterfeit identification and mitigation solutions in place, but none can provide 100% assurance because counterfeiters are continually improving their own technologies in order to “keep up.” Costs for these solutions are added to other hidden costs that cause uncertainties throughout the industry.

The only sure way to avoid purchasing counterfeit semiconductors is to purchase devices only directly from the original manufacturers or their authorised sources. If all equipment manufacturers followed this rule, it would be possible to significantly reduce or even eliminate counterfeiting and save substantial costs throughout the entire electronics industry.

sales@rocelec.com
http://rocelec.com/