

A Rochester Electronics White Paper



Defending Against Counterfeit Electronic Parts and Gray Market Practices

Worldwide Corporate Headquarters

Rochester Electronics, LLC · 16 Malcolm Hoyt Drive · Newburyport, MA 01950 USA
phone 978.462.9332 · *fax* 978.463.2224 · *email* sales@rocelec.com · *web* www.rocelec.com

Defending Against Counterfeit Electronic Parts and Gray Market Practices

1. Executive summary

Counterfeiting, especially the fraudulent manufacturing, distributing and selling of fake semiconductors, is a growing problem throughout the electronics industry. It has a negative effect on reputable component manufacturers and distributors, causes purchasing dilemmas for component buyers, problems for equipment manufacturers and trouble for equipment operators. In a worst case it may cause manufacturers to be driven out of business and catastrophic disasters through equipment failure.

2. The counterfeit issue: the facts

a. Definitions

The Semiconductor Industries Association Anti Counterfeiting task force has made the following 3-point definition of counterfeiting:

1. Substitute or unauthorized copies of a product
2. A product in which the materials used or the performance of the product has been changed without notice by other than the original manufacturer of the product.
3. A substandard component misrepresented by the supplier

b. A brief historical look at counterfeiting

Examples of counterfeiting of semiconductors go back to the early days of manufacturing when the majority of product was being purchased for military applications. Genuine devices were expensive, due to the rigorous screening and qualification requirements, and some of the less scrupulous manufacturers would deliver devices where all mandatory testing had not been completed. This led to the introduction of independent qualifications, audits by independent inspectors and regulated Certificates of Conformance and paperwork traceability extending through the supply chain.

c. The picture today: facts, figures, market data

The use of semiconductors has grown dramatically over the last 30 years with an estimated worldwide value in 2006 of around US\$245 billion. Today the major users are the computer and telecommunications industries who account for more than 60% of the

output. Military requirements, where quality, reliability and product performance are tightest, now represent less than 1% of semiconductor usage.

The major semiconductor manufacturers do not have the resources to handle selling to many thousands of equipment manufacturers who use their devices. There are established distribution outlets that stock and resell the small lot quantities that many of the lesser volume users require.

The stringent environmental performance and long term reliability needs of the military users are not required by the telecommunications and computer industries where shorter equipment life and benign operating conditions are the norm. Component price and technical capability of the devices drive these non-military customers.

Manufacturers of semiconductors have geared their production to the needs of these latter markets. Many of their production operations take place in the lower labour regions of the world. It is estimated that more than 45% of semiconductor manufacturing is carried out in the Far East, with China and Taiwan having the most significant production facilities. Some manufacturers own facilities in these regions but many use subcontractors for the diffusion, assembly and testing operations of their products.

Assessing the real value of counterfeit semiconductors entering the global market is extremely difficult. The original semiconductor manufacturers have been reluctant to disclose counterfeiting instances, in case this should affect their customer confidence or stock price. Equipment manufacturers are reluctant to admit they have purchased counterfeit devices in case it impacts confidence in their ability to manufacture and deliver equipment with the right quality and reliability. Since both sellers and buyers have this reluctance to disclose counterfeiting instances, the authorities that could act to shut down the counterfeiting operations have rarely been asked to do so.

Other industries such as clothing and wristwatch manufacturing, where counterfeiting has been prevalent for many years and values are better recognized through the efforts of customs and trading standards authorities, indicate that counterfeit product sales could be as high as 7% of their market. At the moment, it is unlikely that the counterfeit level for semiconductors is so high, but if it were, it would be approaching the region of 10 to 15 billion dollars.

3. Why is this problem so widespread?

All sectors of the semiconductor market are affected by counterfeit device to greater or lesser degree. Counterfeiters identify factors in the market, which allow them to capitalize on selling their wares wherever they can identify a demand.

There are three major situations where counterfeiting occurs.

a. Manufacturing shortfall/product shortages.

Counterfeiting operations identify where they can sell their fake wares when there are device shortages caused by insufficient manufacturing output of a certain semiconductor.

b. High value products

Counterfeiting operations identify where they can sell devices that cost them little to source but can be sold at the high market price of the genuine devices

c. Obsolete and discontinued device

Counterfeiting operations find ways of delivering “products” that have been discontinued by the original manufacturers.

In each of these cases the devices delivered are unlikely to operate as genuine parts and very often, by the time the user has identified there is a problem, the source of the device has vanished or is untraceable.

4. Types of counterfeiting and how does it occur?

As was stated earlier, the semiconductor industry is a global industry with worldwide manufacturers and manufacturing operations. It is also an industry that makes extensive use of subcontract facilities. There are but a few of the major manufacturers who have all their own production facilities. Many (especially the younger companies) are “fabless” and rely totally on subcontractors for their device diffusion and assembly. Unless the subcontract operations are managed and controlled effectively by the original semiconductor company, it is possible for the less scrupulous subcontractors to allow product or rejected material to be sold to counterfeit operations.

There are many ways counterfeit devices are produced.

a. Total counterfeiting

This is the complete manufacture of a device by a counterfeit operation to look like and to function the same way as a genuine item. The counterfeit operation is trading on the good name of the original manufacturer to secure business, usually at a higher price than they would otherwise be able to receive for the devices if sold as their own brand.

b. Manufacture at subcontractors (product “skimming”)

When an original semiconductor manufacturer uses a subcontractor for diffusion and/or assembly and testing of devices, they must be extremely careful to monitor and fully control the subcontracted operations. If they don't, it is possible for the less scrupulous

subcontractors to over produce or to claim they achieve a lower production yield than the actual. All the extra devices produced can then enter the market through the broker chains.

c. Inadequate control during disposal of scrap and rejects

Reject devices are produced at various stages throughout the manufacturing operation. These devices are worthless as far as operating in equipment but it is possible to salvage some of the precious materials used in their manufacture. For this reason most of the manufacturing rejected devices are sent to companies for crushing and precious metal salvage. These salvaging operations provide a certificate of scrapping to the original manufacturer to certify scrapping has been done. However, there have been instances where the salvager has provided the certificate without scrapping devices which were then sold into the counterfeiting chain.

d. Reclamation of used components

There are vast quantities of electronic equipment that are scrapped but contain working semiconductors. This product is usually dumped in landfill sites or crushed at refuse locations. However, it is possible to reclaim some valuable materials from this equipment where suitable recycling operations exist. With the introduction in Europe of the WEEE legislation, this recycling will increase. Semiconductors are products that should not be removed from soldered boards and re-used as the assembly and removal operations can seriously damage their electrical performance, reliability and operational life. There are, however, operations that remove device from scrap equipment with the intention of reselling them.

e. Re- branding to sell at higher cost

Certain counterfeiters target markets where the price of devices is high due to high performance requirements and the need for stringent testing operations in the manufacturing flow. Examples are devices required to operate at extended temperature ranges such as industrial or military or the higher speed versions of memories and processors. Counterfeiters obtain the lower cost, lower specification versions, re-mark them and resell at the higher price.

f. Falsely claiming conformance for e.g. RoHS

The legislation introduced in Europe to ban the use of certain hazardous materials is presenting a new opportunity for counterfeiters. Here they provide paperwork stating that devices are compliant with the European legislation for old, and otherwise unusable product, that is non-compliant.

Counterfeit products enter the market supply chain through the sales brokering networks that exist to source and supply “difficult to find” product. It is extremely rare for them to be supplied by manufacturer authorized sources.

5. The impact of counterfeit parts in the supply chain

a. Quality issues

There are significant quality concerns with any product that is not supplied either direct from the original manufacturer or supplied through the original manufacturer approved channels. Incorrect handling of semiconductors can introduce potential weaknesses and early failure mechanisms due to contamination and electrostatic discharges and assembly problems due to incorrect dry packaging. The original manufacturers understand these problems and take steps to ensure they do not introduce them. The original manufacturers also choose their distribution outlets carefully and from time to time will audit them, to ensure they are storing and handling all devices correctly.

There is no guarantee that devices procured through broker networks and companies that are not authorized by the original manufacturer have been stored and handled as required to ensure quality and reliability is not compromised.

b. Cost and reputation.

The cost of product supplied from a counterfeit source is almost always going to be less expensive than that from the original manufacturer. Exceptions to this may occur at times of original product shortage or in the case of obsolete and discontinued products.

Counterfeiting operations trade on the good name of the original manufacturer who has spent considerable time and resources to develop the devices and the market for their product. The original manufacturer will also have spent a considerable sum on ensuring that devices are properly specified for and work reliably in the intended applications. They expect to recoup the costs of carrying out these tasks from selling devices. The counterfeit operations do not have these development charges and by lowering the market price, it reduces the recovery of costs by the original manufacturers. This in turn impacts on the original manufacturers’ ability to generate new products and returns for their stockholders.

c. The human impact

Production of counterfeit device does mean some labour requirements are necessary and delivery channels require the efforts of a number of people. It is estimated that there could be in excess of 10,000 brokering and non-franchised distribution operations working around the world. However, both the counterfeit manufacturing and supply

route channels may be run as criminal operations where few people have the financial and social security benefits of the bona fide semiconductor industry.

6. Effective detection

Identifying and detecting counterfeit semiconductors is an increasingly difficult task due to their complexity and size. The encapsulation of many devices is too small to allow sophisticated marking techniques and even with the older, larger packaged devices it is relatively easy for counterfeiters to replicate the original manufacturers marking. Where device have been screened for high reliability performance, or tested to function at higher temperatures or faster speeds, checking by other than the original manufacturer is virtually impossible. Paperwork intended to guarantee compliance can be forged easily.

a. Testing

Three types of testing are required to check for counterfeit product:

1. Visual
2. Electrical
3. Reliability

Visual checking should be for paperwork, device packaging and device appearance and marking. Initially this can be carried out by the buyer but if there is any inconsistency or uncertainty the original manufacturer will need to be involved. It is only the original manufacturer who will be able to confirm specific details such as the certificate of conformity data, date and lot code markings, chip layout and assembly materials. Some disassembly of product may be necessary to check the last two items.

Electrical testing will almost certainly require help from the original manufacturer. While there are independent test houses that can check electrical performance they are unlikely to be able to test device in exactly the same way as the original producer.

Reliability testing is a complex exercise and one that takes considerable expertise, equipment and time.

b. Anti-counterfeit Identification Technology

This is an emerging process being developed by the original semiconductor manufacturers. Various techniques are being developed. These range from hidden, encrypted, on chip performance designation and more sophisticated coded marking of devices to radio frequency tagging of devices and packaging.

7. Protective measures

There are ways all industries can work to address the problems of counterfeiting and legally protect themselves from the counterfeit operations.

a. The legal shield

Companies can legally register their trade and product branding marks. Technologies can be patented and chip design can be registered. Counterfeiters will ignore all of these legal entities unless they see registrations being enforced, prosecutions being successful and sufficiently punitive penalties being imposed.

To date there have been very few cases of successful counterfeit prosecutions in the semiconductor industry. This is partly due to the reluctance of the original device manufacturers and the purchasing operation of equipment builders to admit the problem. Until the industry openly admits the problem is occurring, and makes the enforcement industry aware of the problem and works together to address the problem, counterfeiting will grow.

Recently, both original and contract manufacturers have started to reveal specific instances of counterfeit part usage. In general, the admittance of the problem will further the prevention of counterfeit part use in the industry by raising alerts and specifically, it will help a manufacturer's reputation and brand through honest discourse.

b. The role of OCMs

Historically many of the semiconductor component manufacturers (OCMs) have refused to assist an OEM when the OEM has purchased product from a non-authorized source. This situation will need to change if the industry is to be successful in securing prosecutions of the counterfeiters, Only the OCM has the detailed knowledge of the device that will be legally required for enforcement.

c. Industry-wide initiatives (SIA, NEDA)

In the United States, the Semiconductor Manufacturers Association (SIA) now recognizes counterfeiting as a major threat to the sustainability of their industry. During this year (2006) they have established an Anti-Counterfeiting task force/working group where many of the major semiconductor manufacturers working together to discuss the problem, raise the awareness of the issue and develop countering methods and procedures. They recognize that they cannot achieve success on their own so will be working with other trade bodies such as the US distributors association, NEDA and the legal authorities, especially those from the Department of Defense. However, since the manufacture of semiconductors is a global business it will also be necessary for them to see support from similar trade associations and legal authorities around the world in addition to developing close links with equipment manufacturing companies and their trade bodies worldwide.

8. The solution: effective management of the supply chain

The initiative of the SIA is only in its infancy at this time but the problem of counterfeiting is well established and growing rapidly. Equipment manufacturers should take steps to limit the impact of counterfeiting on their manufacturing and equipment operation to ensure they don't upset their customers. To do this they should establish an effective procurement process. There are certain key elements for this process to be successful.

a. The importance of authorized channels

Purchasing direct from the original manufacturer or the original manufacturer authorized and franchised sources is by far the most secure way of ensuring only genuine product is delivered.

b. How to deal with the open market

On the occasions when it is not possible to obtain a device from the original source and a non-authorized source has to be used it is suggested that the following be adopted.

Use a source that is known and has been reliable in the past.

Only pay for product after it has been delivered and sufficient time passed for it to be checked and validated.

Inspect delivered product and paperwork thoroughly as soon as it is delivered. Check for any anomalies in paperwork, wherever possible tracing the route through which devices have passed during the supply chain.

Ensure all devices appear to be identical. Check devices to see that marking is correct, does not appear to have been altered or remarked and that date code is identical for all.

If any doubts about product authenticity are raised contact the original device manufacturer to seek their assistance.

c. Working together: reporting, sharing information.

For the industry to be successful in countering counterfeiting it is essential that everyone is made more aware of the problem. OCMs and OEMs need to be more open with each other and be prepared to work together to identify counterfeiting instances and prosecute offending sources and manufacturers.

Trade associations and data reporting authorities such as GIDEP can help in raising awareness of the issue by establishing databases for notification of validated counterfeiting instances.

9. Conclusion

Counterfeiting of semiconductors is a growing problem. It damages the credibility of the genuine manufacturers and takes valuable income and profit from them. This loss of income limits the resources they have to develop new products and continue to move the industry forward.

It can also damage the equipment industry as the unintentional use of counterfeit device could lead to their equipment malfunctioning. In a safety critical operation this could have disastrous consequences.

Many facets of the industry are reluctant to admit they have encountered the problem. Until this situation is resolved, and companies are more prepared to disclose situations the legislative and punitive authorities are hampered in their efforts to identify and prosecute the counterfeiters.

The issue is a worldwide one due to the global manufacturing nature of the industry. It is essential that all countries recognize the problem and attack the counterfeiting operations consistently. Only with worldwide co-operation will anti-counterfeiting be wholly successful.

If devices are procured from a questionable source, the risk is high. Without traceability, a device must be subjected to the fullest extent of all legitimate, supplier-approved testing, especially in mission-critical situations.

Ultimately, there are only two fail safe ways to ensure that the components being purchased are legitimate: buy directly from the original manufacturer or enlist the help of authorized distributors and manufacturers such as Rochester Electronics.