A Rochester Electronics White Paper

Counterfeit and Substandard Semiconductors:

The Solution to the Threats

Worldwide Corporate Headquarters

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

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

Executive Summary

Counterfeit semiconductors are entering the worldwide supply chain in unprecedented numbers, and those numbers are increasing at an exponential rate. Also entering the world supply chain are substandard components that were originally viable but have been damaged through improper handling, storage, and shipping methods employed by unauthorized distributors. All of these components are causing production and maintenance failures that range all the way from inconvenient to deadly. Added to the already overwhelming mix of components that just don't perform properly – or at all – are components armed with malicious "extras" that can destroy systems, cause malfunctions, or covertly gather proprietary information. Counterfeit and substandard semiconductors are causing loss of revenue and loss of company credibility in virtually every industry. Malicious insertion threatens national security.

Technology is making it easier for "entrepreneurs" to produce and market counterfeit and substandard semiconductors, and, though technology may contribute to methods we can use to detect the "bad" ones from the genuine, it will take good, old-fashioned cooperation, info-dissemination, and application of best practices to prevent further encroachment of this destructive industry. Most purchasing officers are unaware that "testing" provided by unauthorized distributors is inadequate at best, and is never a viable option for assuring quality. To be effective, testing must always be done with the test programs and equipment of the original component manufacturer. Unauthorized sources do not have access to such intellectual property.

The most reliable way to avoid purchasing substandard and counterfeit semiconductors is to purchase only from original manufacturers or their authorized distributors.

Counterfeit and substandard semiconductors are increasingly present in today's worldwide supply chain.

It might be interesting to calculate how many semiconductors we rely on during a typical day … coffee maker, radio, TV, cell phone (and the satellite that sends the signal), automobile, traffic lights, airplane, computer, maybe a CT scanner or blood analysis machine. Virtually every industry today uses semiconductors: aerospace, industrial, medical, military, security, contract manufacturing, space, telecom, utilities, transportation, communications, and more.

It is estimated that the annual sales of semiconductors increases at a substantial rate each year. It has already exceeded $US300 billion and will approach $US400 billion in the not-too-distant future. Unfortunately, the percentage of sales that involves counterfeit and substandard parts is also expected to increase – exponentially.

The U.S. Immigration and Customs Enforcement (ICE) reports that, between November 2007 and May 2010, ICE and U.S. Customs and Border Protection (CBP) made over 1,300 seizures involving 5.6 million counterfeit semiconductors. The counterfeits were marked with the trademarks of nearly 100 North American, Asian, and European semiconductor companies and were destined for importers in the United States and fifteen other countries.

Despite the efforts of industry and international government officials, these seized components represent only a small percentage of the parts that actually make their way undetected into the international marketplace. It is difficult to gather exact figures; counterfeiters, of course, will not divulge their success stories. But their victims are also reluctant to admit being caught in the counterfeit trap for fear of degrading customer confidence, lowering stock price, and compromising brand strength.

Counterfeit sales of all products (including pharmaceuticals, jewelry, electronics, and other goods) has been estimated to be 7% of total sales. Seven percent of the total projected semiconductor sales for 2010 is over $US20 billion. This represents a considerable number of dangerous parts.

Here are some recent counterfeit semiconductor incidents that were cited in a press release issued in September 2010 by the U.S. Department of Justice:

- 2010 — Defendants imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors, and others, marketing some of these products as "military grade." They and others generated nearly $US16,000,000 in gross receipts from the sales of counterfeit integrated circuits, having imported from China and Hong Kong nearly 60,000 integrated circuits bearing counterfeit marks, including military-grade markings, valued at approximately $US425,293.
- 2009 — Defendants and others engaged in a "bait-and-switch" fraud involving devices to be used in the controllers of high-speed trains. They shipped 13 devices to the buyer that conformed to product specifications, and then shipped 1,987 counterfeit devices.
- 2009 — Defendants, who are now cooperating with law enforcement authorities, sold a military-grade counterfeit device to a government undercover agent during a criminal investigation.
- 2009 — Defendants sold 350 counterfeit parts for integration into a beam steering control module board within the multiple sub-array of the testable antenna for the U.S. Navy Cobra Replacement Program (ballistic missile defense).
- 2008 — Defendants sold 1,500 counterfeit parts to ultimately be used to support production and repairs of A9 (missile) circuit card assemblies for classified application.
- 2007 — Defendants sold 75 counterfeit parts intended to be used for production of ship-based antenna equipment, the Identification Friend Foe (IFF) system, which is used to determine an in-flight aircraft's identification and intention.

Despite the fact that the penalties for counterfeiting are substantial in some regions of the world, the crime continues to rise as the profit that counterfeiters make can be large. The UK Intellectual Property Office (IPO) estimates that the profit margin on counterfeit semiconductors is considerably greater than the profit margin for narcotics.

Penalties in the United States are:

- *Conspiracy:* a potential statutory penalty of up to five years of incarceration, a fine of $US250,000, a three-year term of supervised release, and an order of restitution.
- *Trafficking in counterfeit goods:* a potential statutory penalty of up to 10 years incarceration, a fine of $US2 million, a three-year term of supervised release, an order of restitution, and an order of forfeiture and destruction for articles bearing or consisting of counterfeit marks and for any property used to commit or facilitate the commission of the offense.
- *Mail fraud:* a potential statutory penalty of up to 20 years incarceration, a fine of $US250,000, a five-year term of supervised release, and an order of restitution.

Authorized distributors give you peace of mind – unauthorized distributors can't.

Most major semiconductor manufacturers do not have the resources to sell to the thousands of equipment manufacturers who use their parts. To make sure their parts are available to their customers, they authorize – or franchise – distributors to handle the sales. Franchise or license agreements protect end-customers because their provisions guarantee product integrity and traceability:

- Authorized distributors provide certificates of conformance and traceability documentation.
- Authorized distributors maintain the original manufacturer's warranty.
- Authorized distributors enforce proper storage, handling, and shipping facilities and procedures.
- Authorized distributors provide failure analysis capabilities and can handle corrective actions.

In addition, most original manufacturers audit their authorized distributors on a regular basis to ensure that high standards are maintained and high product quality is assured.

Because unauthorized sources do not have franchise agreements with original manufacturers, they cannot guarantee traceability or credibly offer the original warranty; they are not required to prove that they provide proper handling, storage, shipping; and they are not required to provide test capabilities. Many unauthorized distributors and brokers do not maintain inventory; they simply "source" components on an as-needed basis from other unauthorized sellers. Procurement specialists who buy from unauthorized sources are at high risk for obtaining counterfeit and substandard semiconductors.

The negative impacts of counterfeit and substandard parts are far-reaching and compounding.

In the early days of semiconductor manufacturing, most components were slated for military application. The parts were expensive because they were complex; they had to meet qualifications that would ensure they would work at high speeds in high-stress conditions such as extreme temperatures and intense vibration. Counterfeiters began making profits by producing substandard parts and selling them under false pretenses. When these parts began to have a negative impact in the field, methods for proving authenticity were introduced into the supply chain in the form of independent qualifications and audits, regulated certificates of conformance, and other traceability paperwork. As the authentication procedures became more sophisticated, however, the counterfeiters easily shifted gears and learned how to dodge the obstacles. For example, counterfeiters who are remarking a component first sand off the original marking. Then they have to resurface the component (it's called "blacktopping"). As blacktopping inconsistencies began to raise red flags during inspection, counterfeiters become progressively clever at creating blacktopping that looked totally legitimate. Sometimes the blacktopping obliterates shallow surface indents that are part of the manufacturing process – another dead give-away that the parts aren't legitimate. So the counterfeiters just learned to approximate the original look of the indents. As their expertise improved, counterfeiters expanded their markets to produce semiconductor parts for other industries.

There is a wide variance in the levels of dysfunction of counterfeit and substandard parts. Some parts simply do not function at all. In these cases, the parts can immediately be replaced before they are put into production. The financial losses may be substantial, but are limited to the price paid for the components coupled with production downtime while new parts are procured. Original manufacturers, of course, do not honor warranties on components purchased through unauthorized distributors. In other cases, however, parts appear to be totally functional, so production continues. Malfunctions may be detected in the testing of finished products, or they may be detected in the field – in one month or two, or maybe even longer.

Even though the ***purchase price*** of a counterfeit or gray market component can be less than the purchase price from the original manufacturer, the ***actual cost*** of a counterfeit or substandard semiconductor can by expressed by the Rule of Exponential Increase:

Stage at which a fault is detected in a semiconductor:	Cost of replacement:
before it is used	**$X**
at the sub-assembly stage	**$10X**
at the final assembly stage	**$100X**
when the product is in the hands of the dealer or distributor	**$1,000X**
when the product is in the hands of the ultimate customer	**$10,000X**

Expenses can increase at an insidious rate: return of defective product, the purchase of new raw materials, the manufacture of replacement product, personnel to handle the claims, and possible legal actions by end users. In some cases, manufacturers have even been bankrupted. At the very least, counterfeit component issues can diminish stockholders' returns and cause delays in an original manufacturers' schedule for the development and distribution of new products.

And that's just the monetary downside. Can your company support the loss of reputation and good will and brand equity that can result from a counterfeit disaster? Especially in our current economy, customers are driven to change providers to avoid the repeat of a bad experience.

The new counterfeit-related threat is malicious insertion.

An even more sinister sideline of the counterfeit industry is a technology known as malicious insertion. In this fairly sophisticated form of counterfeiting, which is usually effected for military and communications applications, components are outfitted with hidden capabilities intended to cause the shutdown or the malfunction of the equipment in which they are installed. Additional capabilities may allow the gathering of sensitive intellectual property or intelligence.

As long as counterfeiting remains profitable, it will continue to escalate.

Counterfeiters are shrewd and opportunistic businessmen. They are quick to identify factors in the market and quick to capitalize on them. And they are quick to change their focus in order to remain viable when they encounter any obstacles. They see a demand and they create a supply. Of course, the parts they sell do not operate the same as the genuine parts. Often, by the time the buyer realizes the parts are not genuine, the counterfeiter is untraceable. He hasn't disappeared, however. He has simply moved his operation and changed his name. It's so easy to do on the Internet. The profits are high and the risks are much lower than they are, for example, in the illegal trade of drugs or weapons.

Three major market conditions attract counterfeiters:

- **Obsolete and discontinued devices:** Counterfeiters provide components that are no longer available from the original manufacturer.
- **Manufacturing shortfall that create component shortages:** Counterfeiters provide components when there are device shortages caused by insufficient manufacturing output.

- **High-value products:** Counterfeiters sell devices that cost them little to source but can be sold at the high market price of the genuine devices.

Here are factors and conditions that make counterfeiting tempting and profitable:

- Incorrect and inexpensive “reverse engineering” can lead to the production of components that do not operate as the originals.
- Phony labels, certificates of compliance, and traceability documentation can be made relatively easily through the use of digital photography, digital printing, and widely available, easy-to-use computer software. The cost for a complete setup is low, the equipment takes up little space and is portable, and the quality of the output is adequate.
- Computer hacking can lead to the illegal acquisition of confidential information as well as the alteration of company information.
- The Internet provides a perfect marketplace for counterfeit and gray market products. It’s easy to set up a reliable-looking site. The entire sale can be handled online. And it’s easy for the counterfeiter to “escape” when complaints start coming in. He just shuts down the site and opens up another one in another name.
- The improper disposal of electronic “scrap” provides free inventory for counterfeiters. Many companies ship their scrap overseas for disposal not realizing that disposal verification will be falsified, and the “scrap” will be scavenged, cleaned up a bit, relabeled, and sold as new on the gray market.
- Most manufacturers subcontract the production of semiconductor parts. It’s quick money for an unscrupulous subcontractor to produce an unreported overrun and offload it onto the gray market.
- Requirements of legislation such as the European Union’s Waste Electrical and Electronic Equipment Directive (WEEE) and Restriction of Hazardous Substances (RoHS) Directive encourage counterfeiters to provide falsified paperwork stating that devices are compliant. Counterfeiters sell older leaded components as lead-free, or offer the lead-free parts to exempted industries that need components with SnPb (tin-lead) plating for their high-reliability products. The European legislation has also forced equipment manufacturers to ship electronic waste “offshore” for recycling leading to “salvaged” components being reintroduced to the market as counterfeits.”
- Many countries do not have strong legislation that regulates counterfeiting, theft of intellectual property, or exports. Often, the legal system cannot keep up with the development – and movement – of the semiconductor “manufacturing” industry. Even if there are laws in place, there is little chance for enforcement. This combination of circumstances creates fertile environments for counterfeiters.
- Global outsourcing has produced a complex supply chain in which intellectual property (IP) is widely exposed. In countries where there is little concern for the protection of IP, its availability simply becomes a business opportunity.
- Global outsourcing also sends components through multiple hands before they reach their final destination. Along the way, there is no guarantee of proper handling and storage, adequate inspection, or requisite testing.

Procurement personnel are increasingly tempted (or forced) to turn to the gray market where they risk aquiring counterfeit and substandard parts.

Production comes to a grinding halt when the right parts are not on the shelf. When parts are not readily available from the original manufacturer, buyers often have to be inventive in their search for inventory, but their efforts can be hampered by purchasing protocols and policies. Often, ambitious production schedules can’t wait for long lead times. And there is a constant pressure to lower production costs. In fact, in some industries, particularly in the military, procurement personnel have been forced to base purchase decisions on lowest price. This practice leads them right into the hands of counterfeiters and purveyors of substandard parts.

Genuine and counterfeit semiconductors are manufactured in low-labor-cost regions of the world.

It is estimated that more than 45% of the world's legitimate semiconductors are manufactured in regions of the world where low labor costs are available. The size of this labor force is increasing every year in many areas of the world. Experts estimate that the majority come from China; however other countries are also involved: Taiwan, India, Nigeria, Southeast Asia, the United Arab Emirates, Turkey, Brazil, South Africa, Ukraine, and Russia. Many U.S. manufacturers, for example, own facilities in these countries. Many other manufacturers subcontract to independent companies in these countries for diffusion, assembly, and testing of their products.

Some counterfeiters find ways to take advantage of the fact that the expertise, the facilities, and the IP are locally available. The fact that so much scrap electronic material is exported to certain countries for "disposal" just makes opening a counterfeit operation that much easier. The raw material is there for the taking and sorting. In addition, counterfeiting in most of these countries is not considered or treated as a "bad" endeavor. Authorities often turn a blind eye to "entrepreneurs."

In 2003, when China became a member of the World Trade Organization (WTO), the Chinese government changed export laws to remove stringent export regulations and allow almost anyone to export. This has enabled countless counterfeiters to set up shop – from street-corner operations to sky-scraper-dwelling super dealers.

There are lots of ways to produce a counterfeit or substandard part.

There are many methods of producing counterfeit parts; some are sophisticated and some are remarkable unsophisticated. Some substandard parts are actually authentic parts that have been damaged through improper handling, storage and shipping procedures, including exposure to contaminants or electrostatic discharge (ESD). Parts can be subject to assembly problems due to incorrect dry packaging.

Once the counterfeit parts make their way into the supply chain, there is no way to identify them or keep track of them. Often, for example, gray market distributors take parts as returns back into stock without verifying authenticity, and mix them in with other similar parts. Even they can't tell which are "good" and which are not.

But that is just the beginning of the ever-increasing, ever-more-sophisticated counterfeit game. The Semiconductor Industries Association (SIA) Anti-Counterfeiting Task Force (ACTF) has determined the following three-point definition of counterfeiting:

1. A substitute or unauthorized copy of a product
2. A product in which the materials used or the performance of the product have been changed without notice by an entity other than the original manufacturer
3. A substandard component misrepresented by the supplier

Here are some methods currently in use to produce counterfeit and substandard semiconductor components:

- **Re-marking to indicate higher performance capabilities:** This most common counterfeit scheme targets markets that require devices that perform at extreme limits of temperature, speed, and vibration. These devices are expensive because they are complex and require stringent testing during the manufacturing flow. Often, these components are used in military applications. Counterfeiters purchase lower-cost, lower-performance components, re-mark them, and sell them as their higher-priced, higher-performance counterparts.

- **Re-marking to suit customer need:** Often, manufacturers produce a number of similar parts that share performance similarities. Some may work in some applications but not in others. Slight differences can cause all kinds of problems, even ultimate failure. Counterfeiters often mark one semiconductor so it can masquerade as the one that really fits the situation. Sometimes the switch is not immediately discovered.
- **Counterfeits from scratch:** Counterfeiters manufacture a device that looks like and seems to function like the genuine item, but almost always is of substandard quality. Because the parts are marked and sold as if they were produced by the original manufacturer, the counterfeiter can sell them at a higher price than if they were marked with a less-prestigious brand. Once these counterfeit parts make their way to an equipment manufacturer, the original manufacturer cannot warranty them, or take them back as a return. Such operations range from one-man shows to organizations that counterfeit an entire company's identity, from product right down to website and business cards. This category also includes components that are produced or distributed in violation of intellectual property rights, copyrights, and/or trademark laws.
- **Product skimming:** Original semiconductor manufacturers are most often "fabless" and use subcontractors for diffusion and/or assembly and testing of devices. If they are not monitored carefully, dishonest subcontractors can produce more parts than they report to their customer. Often these "overruns" are produced on a second shift, perhaps by personnel with less expertise using lower-quality materials. The overrun can be sold without the knowledge of and the authorization by the original manufacturer on the gray market where they are, to make matters worse, subject to improper handling and storage.
- **Scrap and reject components:** Components that are rejected during the manufacturing process are usually sold to companies that salvage precious materials from the parts before they are disposed of. These companies provide certificates of scrapping to the original manufacturer. However, some salvagers provide the certificate and then send the rejected components into the supply chain.
- **Reclamation of used components:** Vast quantities of electronic equipment are scrapped, and much of it contains working semiconductors. In an effort to decrease the amounts of toxic e-waste, the European Union has instituted the Waste Electrical and Electronic Equipment Directive (WEEE Directive), which burdens the original manufacturer with the disposal of used products when they become electronic waste. This, together with similar, less-formal directives across the globe, has encouraged the development of "disposal companies," many of which operate in low-cost-labor countries across the world. Companies send their waste for "documented disposal" without realizing that most of their scrap will be scavenged for "usable" parts. The counterfeiters often target complicated components that are not easy to duplicate, but are easy to refurbish and sell as "new." The parts are not protected on their journey as "trash" across the ocean, and they are not handled under ESD-protected conditions as they are "processed." Because these parts often retain their original markings, they are difficult to spot as counterfeit or substandard when they return to the market. In addition, women and children often make up a substantial portion of the workforce who perform the processing procedures. They suffer significantly elevated levels of lead in their blood, which can cause health problems for both mother and baby during pregnancy as well as lowered IQ potential in children. The chemicals emitted from the burning of the final, unused scrap even adversely affect the health of people in the e-waste city communities who are not involved in the "business."
- **False conformance documentation:** The European Union, in 2003, adopted a directive commonly referred to as Restriction of Hazardous Substances Directive (RoHS). This legislation restricts the use of six substances, including lead, in the production of electronic and electrical equipment. Counterfeiters

simply falsify conformance documentation and sell less-expensive illegal parts to unsuspecting buyers. Counterfeiters also falsify certificates of conformance and safety approval documentation. Documentation can also claim that parts have been tested or screened to a higher standard than is true; for example, commercial parts can be sold as military grade.

- **"Stretching" a certificate of compliance:** Unauthorized source will purchase a small quantity of legitimate components from an authorized source. The components come with a totally legitimate certificate of compliance. Then the unauthorized source purchases a much larger quantity of the same components from an unauthorized source. The "good" and the "bad" components are mixed together and sold under false pretences using the certificate of compliance that covers only a small percentage of the total "order."

It's not always easy to detect a counterfeit or substandard part.

One of the treacherous aspects of counterfeit and substandard semiconductor devices is that they are not easy to identify, especially as components become smaller and more complex. The smaller the device, the more difficult it is to use sophisticated marking techniques.

Inspection protocols can be applied to determine authenticity; however, because there are so many different counterfeiting methods and variations within those methods, definitive authenticity verification is not easy to achieve.

Parts can be tested for quality and reliability; however, there are some caveats. The accuracy and usefulness of test results are dictated by the quality of the test. The only reliable tests are tests done with the exact same test protocols, equipment, and specifications used by the original component manufacturer. Unauthorized distributors and third-party test houses do not have access to this intellectual property (IP). Poorly conceived, inadequate test protocols do not result in accurate results. Only highly trained, experienced engineers have the skill and knowledge necessary to select and implement the proper test methodologies for each component. In addition, there is a difference between quality and reliability testing, though both are important in analyzing and projecting the life cycle performance of a semiconductor. Quality is the ability of the device to perform its specified function under specified conditions when it is first used. Reliability is the ability of the device to perform its specified function under specified conditions for a stated period of time.

In most cases, testing adds additional cost to the purchase price of a component. The overall cost of testing must balance with the required quality and reliability level for the end-use of the component. Cost of testing by independent and third-party test labs are frequently dictated by competition and the demand for quick turnaround times; and cost-cutting shortcuts can negatively impact the quality of the test process.

Basically, there are three main types of testing that can be applied to check authenticity, quality, and reliability :

- **Visual Inspection:** Check paperwork for authenticity. Check the appearance of the device and the packaging. Pay particular attention to logos, surface textures, and inconsistencies in date and lot codes. For example, sometimes information can be gained by testing markings with solvents. It is helpful to be able to compare suspect parts to known authentic parts. If there are aspects that just don't seem "right," it may be that only the original manufacturer can confirm authenticity. The original manufacturer can verify the date and lot code markings, certificate of conformity, and layout and assembly materials. X-ray inspection may reveal the presence and size of the die, whether it is the correct one and whether it is authentic, and the layout and condition of the bond wire. Visual inspection cannot identify damage caused by improper handling, shipping, and storage, or exposure to electrostatic discharge.

- **Electrical:** To be of definitive value, electrical testing requires cooperation from the original manufacturer. Independent test houses are usually not equipped with test protocol or equipment to test devices to the specifications of the original manufacturer. DC electrical tests may be quick and cheap, but they don't adequately measure performance variations at extreme high and low temperatures. AC electrical and functional tests are not sufficient to test such complex devices. In addition, electrical testing may not detect damage caused by improper handling, shipping, and storage. And some electrical testing may cause additional damage.

- **Destructive Physical Analysis (DPA):** Components can be taken apart and examined under various scope instruments to establish condition and assess any internal damage. This process is expensive and, of course, renders the inspected device unusable; therefore, only spot-checking is an option. In cases where unauthorized distributors mix all acquisitions, including returns, in one storage "bin," any percentage of components could be counterfeit.

- **Reliability testing:** This testing is complex and expensive and requires expertise, equipment, and time. Only highly experienced engineers know the type and level of testing to apply to a given part to ensure it will perform properly in the application for which it is intended. This most often calls for the cooperation of the original manufacturer, so that the parts can be tested using the same protocols and test equipment that were used when the part was manufactured. In addition, reliability testing should not be considered the same as quality testing. Reliability testing assesses the performance of a specified function of a device under specified conditions over a specified period of time. This is a "long-term" view of a device's performance. Quality testing assesses the performance of a specified function of a device under specified conditions when it is first used. This is a "snapshot" view of a device's performance.

Industry and government must work together to counter the counterfeiters.

Because they are afraid of jeopardizing company credibility, both original semiconductor manufacturers and the original equipment manufacturers who use semiconductors are often reluctant to admit to encounters with counterfeit components, or to report these encounters to governmental agencies. Most are even reluctant to admit that a problem exists. This lack of communication means that there are few successful prosecutions of counterfeit criminals.

Counterfeiting will increase until the problem is exposed, information is shared, and manufacturers and government agencies work together to find solutions. As more and more companies realize the seriousness of the situation, they are beginning to share information and report incidents, but this cooperation must continue to increase in order for the industry to remain one step ahead of the counterfeiters.

The United States agencies that deal with counterfeit products coming into the country include the Federal Bureau of Investigation, the U.S. Immigration and Customs Enforcement (ICE), the U.S. Customs and Border Protection (CBP), the Federal Aviation Administration (FAA), and the Department of Defense (DOD). These agencies cannot do their jobs without cooperation and information from semiconductor manufacturers and equipment manufacturers. If you have been involved in a suspected or confirmed counterfeit incident, you can report to the following agencies:

Defense-related counterfeits:

Defense Criminal Investigative Service (DCIS)
(800-424-9098 — http://www.dodig.mil/hotline)

Aviation counterfeits:

Federal Aviation Administration

(FAA) Suspected Unapproved Parts Program
(800-255-1111 — 9-awa-avs-aai-safetyhotline@faa.gov)

Commercial counterfeits:

FBI (find your local FBI office at http://www.fbi.gov/contact/fo/fo.htm)
Also, visit Cybercrime.gov to learn more on reporting counterfeit incidents.

There has been an increase in cooperation among international agencies. For example, U.S. law enforcement authorities are working with China's Ministry of Public Security (MPS) to combat the manufacture and export of counterfeit network hardware from China. According to a May 6, 2010, FBI press release, "This ongoing work is being facilitated by the IP Criminal Enforcement Working Group of the U.S.-China Joint Liaison Group for law enforcement, which is co-chaired by the Criminal Division and the MPS. The Working Group is dedicated to increasing cooperation in intellectual property enforcement efforts and pursuing more joint IP criminal investigations with China."

The Anti-Counterfeiting Trade Agreement (ACTA) is currently being negotiated, reportedly between the governments of the United States, the European Commission, Japan, Switzerland, Australia, New Zealand, South Korea, Canada, and Mexico. The agreement will address counterfeiting as well as a wide range of issues regarding the protection of intellectual property. Most of the details – including the definitive names of participants – are still being deliberated and have not been published; however, it is encouraging to see the issues being addressed in a cooperative global arena.

There are ways that semiconductor manufacturers can protect themselves.

While it is not likely that the counterfeiting of semiconductors can be stopped completely, steps can be taken by original component manufacturers – and are being taken – to negatively impact the success of the criminal endeavor.

Semiconductor manufacturers can work within the industry to help expose, thwart, or at least hinder, and sometimes even eliminate counterfeit operations.

- Original component manufacturers (OCMs) should ensure that trademarks, product branding marks, and chip designs are legally registered, and technologies are patented. This documentation helps legal authorities prove and prosecute infringement by counterfeiters.
- OCMs should share – with original equipment manufacturers and government agencies where appropriate – information that will help in the identification of suspect or counterfeit parts; for example, techniques and materials used in marking a device, surface finishes used, and part number and date code/lot number information.
- OCMs should cooperate with international trade organizations and government agencies in their efforts to enforce laws that affect the business of counterfeiting. In some cases, OCMs are in an excellent position to help governmental agencies in developing legal cases against suspected counterfeiters.
- OCMs should offer all available assistance to manufacturers who suspect they have received counterfeit components, even when they were purchased from an unauthorized source. In many cases, in order to prosecute counterfeiters, authorities require information about the device that can be provided only by the OCM, such as certificate of conformity details, date and lot code markings, or chip layout and assembly materials.
- OCMs should align themselves with industry-wide, international semiconductor associations. For example, in the United States, the Semiconductor Manufacturers Association (SIA) has established the

Anti-Counterfeiting Task Force (ACTF) that is solely focused on raising awareness and developing methods and procedures for countering the rise of the problem. The Electronic Components Industry Association (ECIA), also a U.S. organization, joins SIA in working with companies, other associations, and legal authorities. In Europe, the European Semiconductor Manufacturers Association (ESIA) and the Component Obsolescence Group (COG), among others, also work against counterfeiting.

- OCMs who have their own fab operations should take great care to dispose of all scrap securely and thoroughly.
- OCM's who are "fabless" must be extremely rigorous in their control of subcontractors to ensure material is not duplicated or lost, expected yields are met, and all scrap is securely disposed of.
- Wherever possible, OCMs should implement technologies that help to authenticate components and make it difficult to fake them. There are some new technologies emerging – hidden, encrypted information on chips, extra-sophisticated coded markings, and radio frequency tagging. However, these authentication techniques almost certainly add cost to components. This may be justified with high-value devices but is unlikely to be acceptable with less expensive components.

There's really only one way to be sure you're not purchasing counterfeit/substandard parts.

Counterfeit components will probably always be out there on the market. The methods for determining the authenticity of components are costly, time consuming, and not even close to foolproof.

Does that mean that your inventory will inevitably be infiltrated by dangerous substandard and counterfeit parts?

No. There are certain simple and inexpensive "best practices" that can help protect your company against acquiring substandard and counterfeit semiconductors.

Because more and more counterfeit components have lately been making their way into the Department of Defense supply chain, the Naval Air Systems Command (NAVAIR) requested that the U.S. Department of Commerce Bureau of Industry and Security's (BIS) Office of Technology Evaluation (OTE) conduct a survey to assess the situation – in commercial, industrial, and defense supply chains. This survey is documented in *Defense Industrial Base Assessment: Counterfeit Electronics* / January 2010.

The bottom-line advice in this document, which contains over 240 pages of data and analysis, is simple:

"Buy parts directly from OCMs and authorized distributors, rather than from parts brokers, independent distributors, or the gray market." *(page 198)*

For example, Rochester Electronics, the world's most comprehensive continuing source for end-of-life and mature semiconductors, is authorized by over 60 component manufacturers to support their customers' continuing requirements. Rochester acquires all remaining finished devices, wafer/die, and available intellectual property in order to manufacture the exact same device and provide a reliable, continuing source of semiconductors used in critical systems worldwide in any quantity and for as long as needed. All components are 100% manufacturer traceable and certified. Rochester's product offering includes 20,000+ Rochester-manufactured device types, from commercial to space-level; device re-creation; as well as more than ten billion die and five billion finished devices, in stock and ready to ship. Rochester is certified to ISO-9001:2008, EN 9120:2002 and JISQ 9120, and QML MIL-PRF-38535, as well as AS9120.

In addition, Rochester's Original Engineering–Driven Test Protocol^{TM} guarantees "quality of test" by providing high-quality, high-performance, and thoroughly tested replacements for end-of-life and mature semiconductor devices. Rochester acquires intellectual property from the original semiconductor manufacturer through continuing manufacturing agreements, including proprietary testing techniques, test programs, tooling, and test equipment required for precise and comprehensive testing of the semiconductor devices. When the original test programs and/or test systems are unavailable from the original manufacturer, Rochester's dedicated test engineers develop new test programs based on the latest revisions of the data sheets. If necessary, Rochester engineers convert test programs to existing test platforms using proven, in-house custom conversion software tools. In some cases, Rochester engineers are able to alter or adapt the original manufacturer's program; for example, a part that was originally tested for commercial use may require upgraded testing for military use. Unauthorized sources and third-party test houses do not have access to any of this intellectual property.

Rochester was instrumental in the formation of the Semiconductor Industries Association's Anti-Counterfeiting Task Force (ACTF). Also in conjunction with SIA, Rochester developed and now hosts and funds the *Electronics Authorized Directory,* a comprehensive, worldwide directory of authorized semiconductor distributors. The directory provides two quick and easy worldwide search tool options to help buyers find authorized distributors: search by semiconductor manufacturer, or search by part number. This directory makes it easy to buy only from legitimate sources and eliminate the potential risk of purchasing counterfeit or substandard parts. Purchasing officers can access the Electronics Authorized Directory at www.authorizeddirectory.com.

Rochester is also active throughout the international semiconductor industry in efforts to inform component manufacturers, equipment manufacturers, government agencies, and the general public about the product risks and dangers of counterfeit and substandard components as well as strategies for procuring only viable semiconductors. The company has introduced Captain Rochester, a strong and knowledgeable industry hero who promotes safe and secure methods for procuring semiconductors. As an entertaining and informative icon, he has become a symbol of what is right about the industry (www.captainrochester.com).

The Department of Commerce survey recommended the following best practices for companies that deal with electronic parts. All quotes in this list are directly from the survey. (Note: for a free summary of this survey, contact sales@rocelec.com)

- Implement "institutionalized policies and procedures … on how … to avoid purchasing counterfeit parts; test, handle, and track incoming and outgoing parts; and manage and dispose of suspected counterfeit components." *(page 193)*
- Train all personnel who handle electronic components (purchasing, quality assurance, and receiving) on how to inspect parts and identify possible counterfeits. *(page 194)* Provide "clear, written guidance on what steps to take if they suspect a part is counterfeit." *(page 206)*
- Report all suspect and confirmed counterfeit components to federal authorities and industry associations. "Communication within and between industry segments is inconsistent." *(page 183)* "Few companies … notify federal authorities, making law enforcement action less likely." *(page 183)* In 2008, only 3 percent of all incidents recorded by survey respondents were reported to the government. *(page 184)* This is mostly due to the fact that "Organizations do not know which authorities to notify." *(page 186)* (Note: For information on where to report, see "Industry and government must work together to counter the counterfeiters." in this document.)
- Maintain an internal database of suspected and confirmed counterfeit parts. [It's also a good idea to maintain a reference library of pictorial and written descriptions of all known authentic parts for comparison.]

- "Buy parts directly from OCMs and authorized distributors, rather than from parts brokers, independent distributors, or the gray market." *(page 198)* This policy may not be practical for organizations "that work on systems that require out-of-production or obsolete parts." *(page 198)*
- Require suppliers to trace parts back to OCMs – certificate of conformance.
- Establish a list of trusted suppliers – use the following criteria: *(page 200)*
  - Number of years in business
  - References from past/present customers
  - Counterfeit screening, tracking, and testing procedures
  - Adherence to industry and government standards
  - Membership in industry associations
  - Previous problems recorded
  - Quality of warehouse/storage facilities
  - Existing counterfeit avoidance policies
- Use a third-party escrow service to hold payment while parts are tested for authenticity.
- Ensure that procurement schedules are realistic.
- Establish contracts with suppliers that include improved notices for final life-time part purchase opportunities and of termination when electronic components will no longer be manufactured. "Organizations should also have proactive obsolescence management plans when parts go out of production." *(page 200)*
- Physically destroy all defective, damaged, and substandard parts.
- Increase the use of authentication technologies by part manufacturers and/or their distributors. "Organizations trust the integrity of the supply chain and the products that flow through it." *(page 182)* Therefore, no one is checking!
- Employ testing protocols that conform to the latest industry standards.
- Verify the integrity of test results from contract testing houses.
- Perform supplier site audits; evaluate product return, buy back, and inventory control practices, and quality processes. "Inventory should be kept under strict control. Parts for different customers should be kept separate… Parts purchased from different suppliers should not be co-mingled." *(page 205)*

These recommendations are also being made by the automotive and avionics industry standardization organizations in their AS5553 document and are likely to appear soon as an International Electrotechnical Commission (IEC) TC107 standard.

The short life cycles of parts used in the production of products that have long life cycles has created an industry situation formally known as Diminishing Manufacturing Sources and Material Shortages (DMSMS). Traditionally, the approach to this condition has been reactive, but that has proven to be less than effective and has opened the door to the acquisition of substandard and counterfeit components. Unauthorized solutions to an "emergency" semiconductor shortage that offer low cost and quick turnaround may sound really good, but should raise red flags. The old adage still applies: If it sounds too good to be true, it's probably not true.

A proactive approach to DMSMS should begin with system design. Even if the system is up and running, however, proactive strategies can eliminate stressful and expensive system re-designs. Companies can do a little research to determine the life cycle status for every component on a bill of materials (BOM). Some companies offer free BOM analysis. Rochester Electronics offers such a service. Customers receive a detailed report that shows life cycle status for each part, as well as Rochester's inventory and manufacturing capabilities. With this information in hand, customers can map out procurement strategies that will ensure a constant supply of viable, guaranteed parts. Production lines are never held up, and the quality of products is never in jeopardy.

Conclusion

The counterfeiting of semiconductor components is escalating at an unprecedented rate. With increasingly sophisticated methods, counterfeit components are produced in many areas of the world and distributed globally. Additionally, unauthorized distributors render genuine parts substandard through improper handling. To make matters worse, semiconductors are being altered through a practice known as "malicious insertion" to cause damage or failure to the parts in which they are installed, or to gather intelligence.

There are many methods and many levels of counterfeiting, but there are two facts that are pertain to all of them:

- Counterfeits cause loss of revenue and reputation for both original component manufacturers and the equipment manufacturers who use their components.
- There are no certain methods for identifying all counterfeits.

Governments and industry are working together to slow down the counterfeiting machine, but they will never be able to bring it to a halt. Original component manufacturers, industry associations, and government agencies must work together to identify counterfeit inventory and prosecute those who produce and distribute it.

The only sure way to avoid purchasing counterfeit and substandard semiconductor components is to purchase from the original manufacturer or their authorized distributor.

www.rocelec.com