Counterfeiting and Semiconductor Value Chain Economics

Supply Chain Risk Insight into Market Sense and Respond Actions of Counterfeiters

Rory King
Global Director, Supply Chain, IHS Inc.

321 Inverness Drive South
Englewood, Colorado, 80112

Abstract

Counterfeit parts have proliferated dramatically in recent years, presenting huge challenges for electronics manufacturing and specifically military and aerospace application. This session will offer unique new market trends, observations, and best practices on the issue of economics, semiconductor value chains, obsolescence, counterfeit electronics, and market impacts such as fact-based insight into market indicators like correlation among counterfeits, semiconductor factory utilization, component obsolescence, semiconductor availability, price volatility, and supply-and-demand equilibrium.

1. Introduction

While counterfeiting is a decades old issue, growing safety and securing concerns as well as scrutiny over supply chain and procurement practices around counterfeit or suspect counterfeit electronics become widely known as a result of the November 8, 2011 hearing of the U.S. Senate Armed Services Committee on Counterfeit Electronic Parts in the Department of Defense Supply Chain. Subsequent to the hearing, the National Defense Authorization Act (NDAA) of 2012 included Section 818, Counterfeit Detection & Avoidance. Generally speaking, some key supply chain implications considered at all tiers of the global defense supply chain included:

- Contractor responsibility for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit parts
- Contractor responsibility for any rework or corrective action that may be required to remedy the use or inclusion of such parts
- Defense contracts no longer allowing the cost of counterfeit electronic parts and suspect counterfeit electronic parts or the cost associated with rework or corrective action to resolve the use or inclusion of such parts
- Qualification procedures and processes must be established to use trusted suppliers and procure electronics from authorized suppliers

Cost is a major concern for the defense industry. As publicized at the U.S. Senate Armed Services Committee (SASC) hearings in 2012, a single counterfeit incident – like that of the THAAD missile system – can cost in excess of $2 million dollars. According to the Missile Defense Agency, if the devices had failed, the THAAD missile itself would likely have failed. "The cost of that fix was nearly $2.7 million," stated Senator Carl Levin (D-MI).[i]

Human safety and national security also come to the forefront when the potential impact of counterfeiting is assessed. Counterfeits not only pose an increasing risk to the safety of men and women in uniform, but they also endanger civilians in other parts applications subject to counterfeiting such as medical devices, consumer products, or perhaps automobiles.

Counterfeiting is a challenge to companies of all sizes and across all industries – from the small domestic manufacturer to the global organization, and all entities in between. This paper discusses supply chain risk and an apparent relationship between counterfeit supplier behaviours to rapidly sense and respond to semiconductor market economic conditions, as measured through counterfeit incident reports and component production, inventory, and obsolescence insight -- over time.

2. Sophistication of Counterfeiters

As Vivek Kamath, Vice President for Supply Chain Operations for Raytheon Company stated, *"What keeps us up at night is the dynamic nature of this threat because by the time we've figured out how to test for these counterfeits, they've figured out how to get around it. And it's literally on almost a daily basis they change and the sophistication of the counterfeiting is amazing to us."*[ii]

To illustrate the apparent sophistication of counterfeiters to sense and respond to market conditions, consider the Lehman Brothers bankruptcy filing in the United States and resultant downturn of the global economy. As the largest bankruptcy filing in U.S. history, the incident – which took place on September 15, 2008 – correlates with a pronounced decline in

semiconductor factory production. In Figure 1 you can see that semiconductor factory utilization remained fairly steady until the economic collapse triggered by Lehman Brothers filing Chapter 11 bankruptcy, after which there was an immediate precipitous drop in semiconductor factory utilization. This is the reaction of semiconductor producers to demand side weakness.

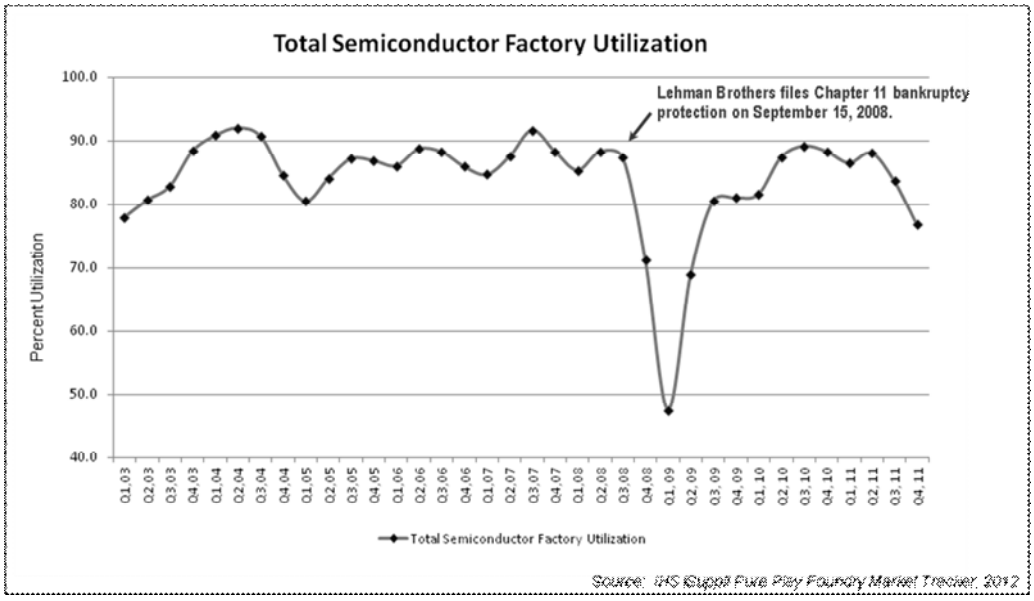

Figure 1 – Total Semiconductor Factory Utilization

Original Component Manufacturers (OCMs) responded to the event by trying to maintain profitability in the face of big slashes in demand and cancellations of orders. They also started issuing end of life (EOL) notices to discontinue their products. IHS tracks these notices and, as you can see in Figure 2, the number of EOLs skyrocketed just after the filing by Lehman Brothers, which at the time was holding over $600 billion in assets. This pronounced spike illustrates how component manufacturers ultimately discontinued their products in an effort to work smarter and leaner in the midst of a tumultuous business environment.

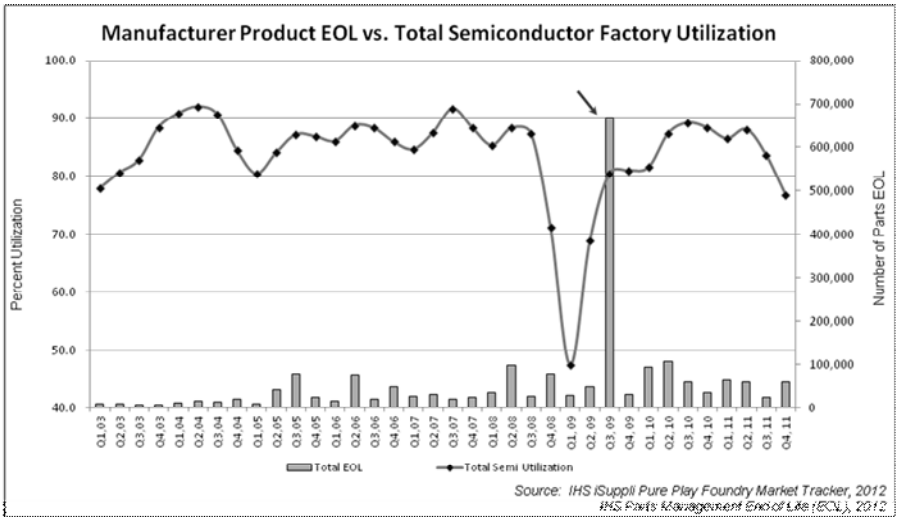

Figure 2—Manufacturer Product EOL vs. Total Semiconductor Factory Utilization

So how did counterfeiters respond to the bankruptcy filing and subsequent increase in EOLs? As illustrated in Figure 3, counterfeiters responded to the event as an opportunity supply counterfeit product to buyers, many of whom may not have been aware of authentic product being discontinued by the OCMs.

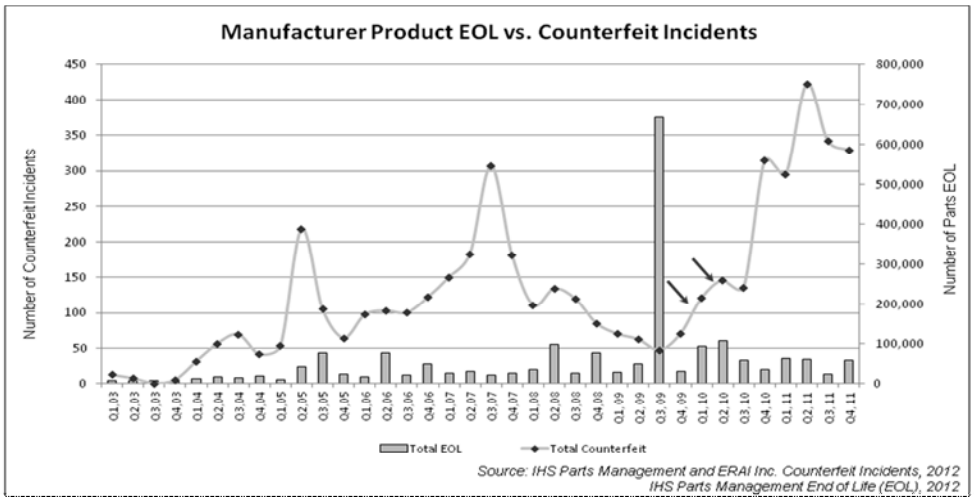

Figure 3—Manufacturer Product EOL vs. Counterfeit Incidents

Now, much discussion over counterfeit parts is around ***obsolete components,*** but in reality the problem runs much deeper. As reported by IHS, a total of 57 percent of counterfeit-part reports from 2001 through 2012 have involved obsolete or end-of-life (EOL) components, as presented in the figure below. Another 37 percent were active parts.[iii]

If you look at Figure 4 you'll see overall inventory trends (in the shaded areas of the chart) and a line showing counterfeit products trending along with ebbs and flows in inventory. This represents inventory of active, commercial electronic components. Keep these points in mind as we move on to Figure 5.

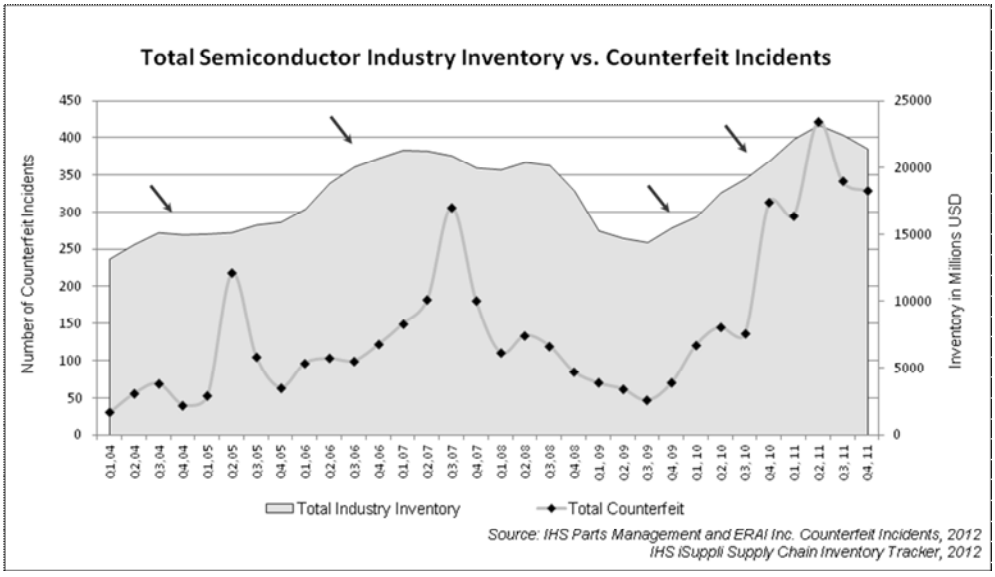

Figure 4—Total Semiconductor Industry Inventory vs. Counterfeit Incidents

In Figure 5, you will notice that semiconductor factory utilization is the top line, but instead of EOLs what you now see are the counterfeit trends. The interesting correlation is how these trends fluctuate right along with the ups and downs of semiconductor factory utilization. As utilization ebbs and flows, the counterfeiting activity reacts similarly.

In other words, the counterfeiters are sensing market demand and supply factors much like the original manufacturers of components. Counterfeit suppliers introduce a greater number of counterfeit products to market (as measured by counterfeit incident reports) in concert with legitimate producers responding to an uptick or forecast of semiconductor demand. As the market picks up, the counterfeit incidents increase.

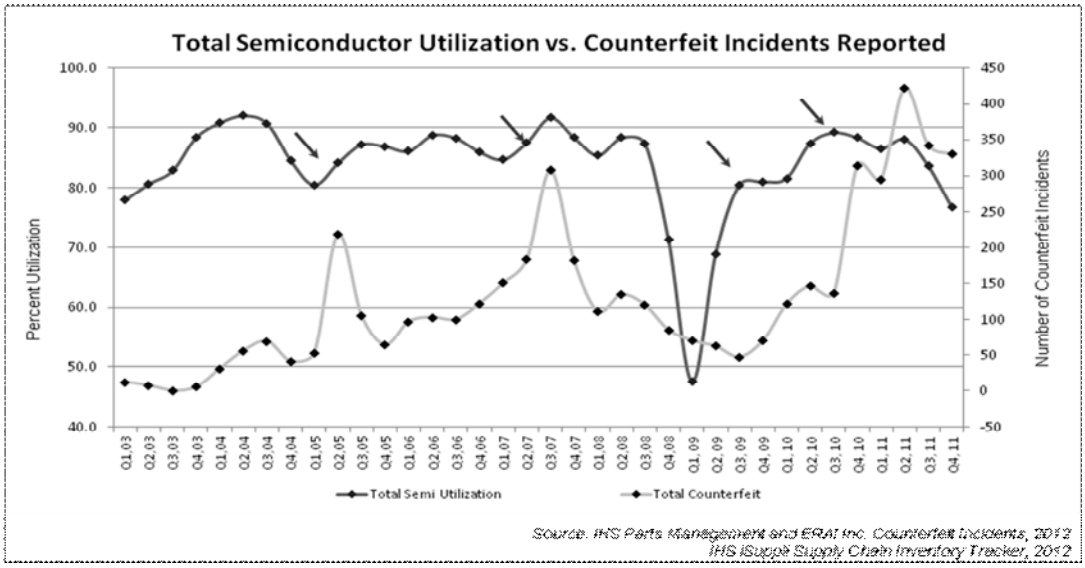

Figure 5—Total Semiconductor Utilization vs. Counterfeit Incidents Reported

3. Top Counterfeit Parts Classes

Counterfeiters are more prolific than ever in a handful of parts classes. Entering 2012, the top five commodities subject to counterfeiting according to IHS were:[iv]

- **Transistors – 7.6%**
- **Programmable Logics Integrated Circuits – 8.3%**
- **Memory Integrated Circuits – 13.1%**
- **Microprocessor Integrated Circuits – 13.4%**
- **Analog Integrated Circuits – 25.2%**

In Figure 6, using IHS iSuppli Application Market Forecast Tool (AMFT), one can plot the counterfeit incidents by component classes against the semiconductor application markets where those components are consumed. The top five

component families are listed on the left side of the chart while the relative percentage distribution of where those products are used is reflected on the graphic's horizontal axis. For example, 14% of analog integrated circuits products are in the industrial market; 17% in automotive; 21% in consumer; 29% in wireless; 6% in wired; and 14% in compute. (It's important to note that medical device, military and civil aerospace components fall under the industrial market segment or the 14% of the analog integrated circuits products.)

Cumulatively, analog integrated circuits are the biggest target for counterfeiters and represent a roughly $47.7 billion semiconductor application market. It is possible to imagine the potential risk and cost implications of issues associated with damages resulting from those counterfeit parts. While a great deal of attention is placed on defense supply chains, the issue plainly doesn't just threaten the men and women in armed services or national security, but it poses potential risk and disruption to businesses and consumers who rely on products throughout these application markets.

The potential challenges are apparent for other application markets. The consumer electronics segment in 2011 consumed $9.8 billion worth of analog integrated circuits, or 21 percent of the global market. Automotive electronics amounted to $8 billion, or 17 percent; computing represented $6.7 billion, or 14 percent; industrial electronics was at $6.5 billion, or 14 percent; and wired communications was $2.9 billion, or 6 percent.

Percent Distribution of Total Market Revenue by Application Market for Most Commonly Counterfeited Product Types in 2011
(% Share of Revenue in Millions of U.S. Dollars)

Application Market →

Top Part Type Reported in Counterfeit Incidents	*Industrial Market*	*Automotive Market*	*Consumer Market*	*Wireless Market*	*Wired Market*	*Compute Market*	*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%

The top five components most counterfeited represent $169 billion of revenue.

Source: IHS iSuppli Application Market Forecast Tool (AMFT), 2012

Figure 6—Percent Distribution of Total Market Revenue by Application Market for Most Commonly Counterfeited Product Types in 2011

4. High-Risk Suppliers

Even in the face of increasing government regulation and scrutiny, the number of high-risk suppliers abounds. These firms engage in high-risk, fraudulent, and suspect counterfeit product or conduct, as identified by the U.S. government. There are literally tens of thousands of these

high-risk providers, and their numbers are growing daily. They push the issue of counterfeiting well beyond just the production of fake parts. As you can see in Figure 7, we're talking about thousands of organizations emerging on an annual basis, and not just in an aggregated, collective fashion either. The environment literally changes daily and impacts every link in the supply chain.

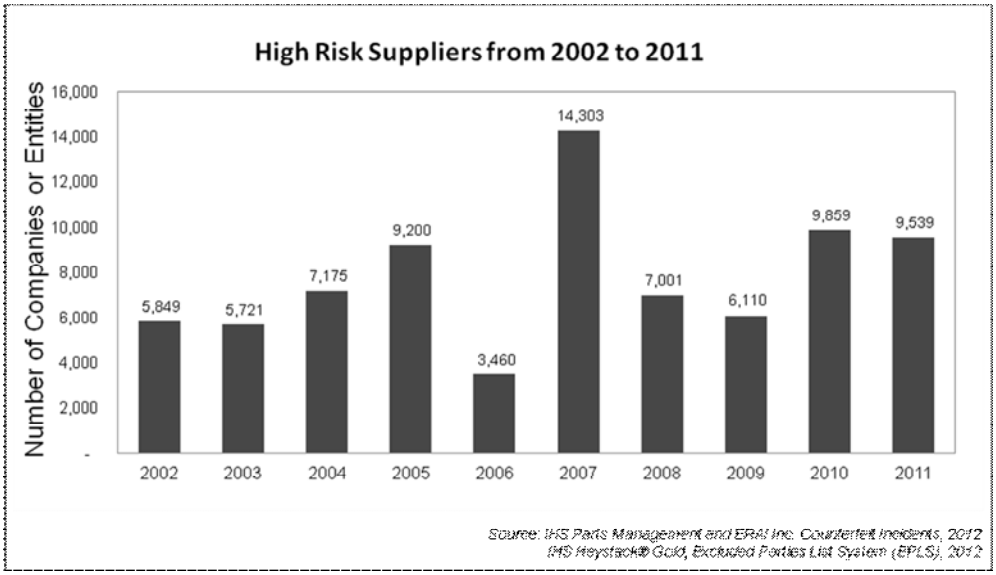

Figure 7—High Risk Suppliers from 2002-2011

5. The Monetary Impacts of Counterfeiting

Concerns over the impact of counterfeits are well known throughout industry. One general example draws from an IHS and *Supply & Demand Chain Executive* survey of 1,001 practitioners, executives, academics, vendors and other industry professionals. Summarized key findings on the impact of counterfeits experienced or believed by these survey respondents include those shown in Figure 8. As was apparent, counterfeits cause a wide range of potential issues from serious financial and brand consequences to daily operational cost, service, and safety disruption.

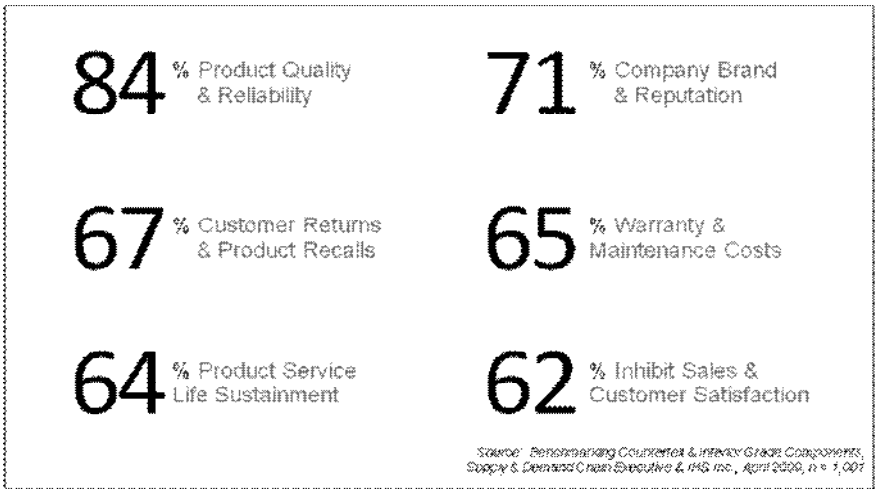

Figure 8—Significant Costs of Counterfeit Risk[v]

6. Conclusions

Counterfeiting concerns and impacts continue to be widely discussed, documented, and shared throughout industry on a worldwide basis. Through unique information and insight now available to plot real counterfeit incidents reported by industry against semiconductor factory utilization, inventory, product lifecycle, and application market forecasts one can begin to see the degree to which counterfeit behaviours appear to correlate with semiconductor industry responses to marketplace economics.

When this insight is analyzed, it seems apparent that counterfeiters sense and respond to marketplace dynamics in a sophisticated manner, by taking such action as supplying counterfeit product to market in concert with semiconductor factories increasing capacity to do satisfy demand. While these correlations seem apparent, other interesting questions that cannot be proved emerge as well – for instance, could these factories (or their equipment or entire replicas thereof) be the sources of illegitimate product entering the counterfeit supply chain?

In conclusion, some key points can be considered as organisation assess risk vulnerabilities and implement counterfeit detection and avoidance measures:

- Counterfeiters are not simple individuals with rudimentary capabilities; they are sophisticated operators and they are in tune with the market.
- Counterfeiting is not exclusively a military and defense parts issue, but rather counterfeit parts impact all commercial & military markets.
- Counterfeiting is not restricted to old, obsolete components, but rather counterfeiting impacts active components (in fact, nearly half are active parts).
- Counterfeit detection and avoidance is not just a "cost burden," but counterfeit risk mitigation creates significant cost avoidance.
- Counterfeit mitigation is not just about "the parts," but counterfeit mitigation requires knowledge of high-risk suppliers.

---

i HEARING TO RECEIVE TESTIMONY ON THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN, Tuesday, November 8, 2011, U.S. SENATE COMMITTEE ON ARMED SERVICES, Washington, DC

ii HEARING TO RECEIVE TESTIMONY ON THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN, Tuesday, November 8, 2011, U.S. SENATE COMMITTEE ON ARMED SERVICES, Washington, DC

iii Rory King and Mark Snider, IHS Inc. with ERAI Inc., 2012

iv Rory King and Mark Snider, IHS Inc. with ERAI Inc., 2012

v Supply & Demand Chain Executive and IHS Inc., Benchmarking Counterfeits and Inferior Grade Components, 2009