IN SEARCH OF A WORKABLE COUNTERFEIT RISK MITIGATION STRATEGY:

Lessons Learned in Review of the Current State of the Electronics Industry as Regards Counterfeit Mitigation Requirements for Suppliers

Kevin Sink
VP of Quality
TTI, Inc
Fort Worth, Texas, USA
kevin.sink@ttiinc.com

ABSTRACT

The complexity of the electronics supply chain has necessitated the development of multiple, sometimes differing, standards to mitigate the risk of obtaining counterfeit electronics. To manage the counterfeit issue, OEM's are applying diverse strategies to manage the risk through proscriptions to their suppliers. A review of the documents received by an authorized distributor over a 3 1/2 year period both substantiates some, and refutes other, commonly held beliefs as regards the state of counterfeit risk mitigation in the electronics industry.

The research categorizes the market segments deploying such methods and analyzes documents received for their distinction as regards type of supplier, type of product, invocation of external documents and common restrictions imposed. Given the results, recommendations are made to the industry.

KEY WORDS

Counterfeit electronics, independent distributor, authorized distributor, counterfeit risk mitigation, Section 818, AS5553, AS6081

METHODOLOGY

To analyze the management of counterfeit mitigation of the supply base, 53 documents received by an authorized distributor between January 1, 2010 and June 30, 2013 were reviewed to categorize and evaluate the present and evolving state of mitigation requirements imposed on the supply base by purchasing organizations.

The documents represent the breadth of document types received by the authorized distributor over this time period. Excluded from the set were (1) the results of on-site audits conducted only to evaluate the counterfeit program (2) and QMS (Quality Management System) audits which included counterfeit mitigation as one section of an overall audit. Such audits, while addressing counterfeit mitigation, do not necessarily establish the expectation of the organization, but rather serve to establish confidence or lack thereof in the supplier's system.

Each document was reviewed and categorized as summarized in Table 1.

Table I

Table of Categorizations
Customer Type
Document Type
Separate Policy for Supplier Types?
Single Policy Address Supplier Types?
Policy Address Specific Parts/Part Types
External Standard/Document Referenced
Restrictions
Notes

Customer Type was recorded to determine the industries which are formally addressing counterfeit electronic part mitigation and to determine if the scope is widening. Document Type is categorized to enumerate the basic approaches being used to formally express the counterfeit mitigation expectations of customers. Within the text, the document was noted if it was addressed to a specific segment of the supply chain, such as the OCM, the Authorized Distributor or the Independent Distributor. This was done to asses the level of complexity being applied in the customer's counterfeit risk mitigation approach. If the document was addressed to all suppliers, it was then categorized to determine if the elements within the document addressed the supply chain members with different expectations. Similarly, the text was analyzed to see if the customer approached the management of specific parts or part types differently which would give evidence of the sophistication of the customer's plan to apply more restrictions to higher risk parts either by application or frequency of counterfeit in the market. The reference to a specific industry standard was noted in those cases where the document called out the standard as the model for their expectations. Finally, reviewing the text revealed if the document imposed any specific restrictions on the supplier other than to have a counterfeit risk mitigation plan. In the notes, specific citations were lifted from texts to illustrate common or best practices. In the citations presented herein, the company names are redacted and presented as "XYZ".

Hypotheses

1. Most customers of electronic components addressing counterfeit risk with their suppliers are in the military/aerospace market.
2. Most customers apply one policy to their entire supply base.
3. No distinction is made in requirements for different types of supplier (OCM, Authorized Distributor, Independent Distributor / Broker).
4. No distinction is made in requirements for parts of differing risk levels (based on reported incidents).
5. No distinction is made in requirements for parts used in low risk versus high risk applications.

RESULTS

Customer Type

Typology of the customers revealed that 67% (33 of 49) customers were in the mil/aero segment, primarily OEM's. While 8 contract manufacturers (CM's) were identified, most of these have a segment of their business model dedicated to mil/aero business. Unexpected in the data was the identification of five OCM's – companies producing "components" or small units integrated into larger systems. These OCM's would assemble units of a few components that they market as a single unit – such as an off-the shelf power supply, or a catalog cable assembly.

Table II

Industry	Number	%
Mil/Aero	33	67%
CM	8	16%
OCM	5	10%
Automotive	1	2%*
Medical	1	2%*
SDB	1	2%*
Total	49	

* rounded down

Document Type

Typology of documents revealed a commonality of approaches across the customer base. Three styles emerge as dominant approaches: the *Clause*, to be called out as a requirement on a purchase order (40%), the *Survey* (36%) and the *Policy*, either with or without required acknowledgements (22%). Analysis of changes in document type over time revealed no significant pattern other than the deployment of these documents increased to a higher level in 2012 and is continuing at a steady rate in 2013.

The most frequently used document type was the *Clause*. Clauses were sent either as a separate, stand alone document or were incorporated into a compendium of all clauses the customer might invoke.

Closely following the clause approach is the *Survey* (36%). The survey asks if the supplier has certain elements in place to satisfy the expectations of the customer. This approach has the advantage of allowing the customer to develop a risk assessment based upon the responses. However, only 1 of the 19 survey documents had a numerical ranking approach that could develop a counterfeit risk mitigation score. The remainder of the surveys exhibited no known ranking mechanism. Experience tells us that, at best, one can use the survey result to make broad judgments ranging from Low Risk (supplier demonstrates thorough and competent answers to each question) to High Risk (Supplier answers vaguely or poorly) and a limited range in between. Unfortunately many of these surveys have only Yes/No boxes and the added understanding that could be attained is lost in the restrictive form.

Similar to the *Clause* approach is the *Policy* (22% total). These documents express the customer's expectation as a requirement of their supply base, but are deployed in expectation that they are used in all transactions for said customer not on a purchase order basis. This is similar to the "Supplier Quality Manual" approach used for QMS requirements. Two thirds of these policies contained a signature page for supplier acknowledgement of the requirements.

A unique approach was also found in the data. One customer required the supplier to complete a certificate testifying that the supplier is either the OEM (context suggests OCM) or an authorized/franchised distributor or that the supplier purchases only from authorized/franchised distributors.

Table III

Document Type	Number	%
Clause	21	40%
Survey	19	36%
Policy w/Acknowledgement	8	15%
Policy	4	7%
Certificate	1	2%
Total	**53**	

Separate Policies for Supplier Types

Two classifications consider the level of sophistication of the requirements vis-a-vis the supplier type in the supply chain. US Senate Committee findings advise that "virtually all" of the counterfeit parts tracked through the defense supply chain during its investigation were supplied by Independent Distributors (Brokers)[1]. Conversely, the risk of acquiring a counterfeit part from the original component manufacturer or their authorized distributors is nominal (The source results of the 2009 U.S. Department of Commerce study are hotly debated due to its method of self identification of source without validation as it stands alone amongst studies to portray a noticeable risk).

Of the 53 documents reviewed, only 6 were stand alone policies based upon supply chain type (OCM, Authorized Distributor, Independent Distributor). Of those documents that were not specific to a supplier type (47), 30% (14) addressed the different supplier types specifically and distinctly within the requirements.

Table IV

Separate Policy for Different Supplier Types?	Number	%
No	47	89%
Yes	6	11%
Total	**53**	

Table V

If one Policy, does it address Different Supplier Types?	Number	%
No	33	70%
Yes	14	30%
Total	**47**	

Separate Policies for Specific parts or Part types

Recognizing also that certain types of products are more commonly counterfeited than others (Integrated circuits account for 82% of reported counterfeits in the ERAI (Electronic Resellers Association Inc.) database[2]), the documents were examined to determine if different (more intensive) requirements were given for the riskiest parts or part types. None of the documents referenced a specific part number, though one did distinguish between applications. Five documents did apply different requirements to different part types, citing specific test requirements. The most strenuous tests cited were for active components (integrated circuits).

Table VI

Different Requirements for Different Parts or Part Types?	Number	%
No	48	91%
Yes	5	9%
Total	**53**	

External Standard / Document Referenced

To determine the influence of external industry standards or documents on the requirements imposed on suppliers, the documents were classified based upon their invocation of a standard for part of the requirements. In some cases, more than one document was invoked and as such, the total number of invocations (58) was greater than the number of documents reviewed (53).

Over half of the documents (29) invoked no industry standard and while this leaves flexibility to the supplier to comply, these documents were generally those with the most cursory approach. One third of the invocations cited AS5553, the oldest published SAE standard for counterfeit mitigation. Three citations were made of AS6081, the standard for Independent Distribution and two for IDEA STD-1010B, the inspection standard for Independent Distribution from IDEA (Independent Distributors of Electronics Association). Notably, five of the documents invoked, and in some cases verbatim, Section 818 of the 2012 NDAA (U.S. National Defense Authorization Act).

Table VII

External Document	Number	%
None	29	50%
AS5553	19	33%
AS6081	3	5%
Section 818	5	9%
IDEA-STD-1010B	2	3%
Total	58	

Restrictions

The documents were reviewed for the invocation of restrictions to determine the commonality in supplier control mechanisms. While 51% of the documents recorded no restrictions, it must be mentioned that of the 27 in that category, 18 were formatted as surveys, vehicles better suited for gathering information than disseminating requirements.

By far the most common restriction was the requirement that suppliers purchase directly from the OCM or the OCM's authorized distributor only. While four documents made no other accommodation at all (Example 1), 25% of the total documents (13) required a supplier to obtain permission from the customer in order to purchase an item from an Independent Distributor (Broker) (Example 2). Only one of these 17 documents indicated that a list of approved brokers existed at the customer, leaving one to conclude that such purchases would be reviewed on a case by case basis. Some of these customers called out specific forms and back-up data to be provided in the request package.

> *Example 1: To further mitigate the possibility of the unintentional use of counterfeit parts or materials; the Supplier shall only purchase authenticated parts/components directly from the Original Equipment Manufacturers or Original Component Manufacturer (OEM/OCM) or through the OEM/OCM authorized distribution supply chain.*

> *Example 2: An Independent Distributor may only be used to resolve obsolescence or schedule issue. Prior approval must have been obtained via the Supplier Initiated Non Conformance (SINC) process (FMxxxx).*

Only XYZ approved Electronic Independent Distributors shall be used.

Although the influence of Section 818 is evident in the language of several documents, only one specifically called out "Trusted Supplier" and that document used the language of Section 818 verbatim.

Table VII

Restrictions	Number	%
None	27	51%
No Broker w/o permission	13	25%
No Brokers	4	8%
Have a Documented Pgm	4	8%
AS5553 requirements	1	2%*
Traceability	1	2%*
N/A	1	2%*
New Parts Only	1	2%*
Trusted Supplier	1	2%*
Total	53	

* Rounded up

Other Observations

Cost Indemnification

Pursuant to Section 818's requirements for the Prime Contractor to assume full responsibility for ALL costs related to a counterfeit event in a military product, several documents attempt to pass on the cost liability down the supply chain.

Example 3:
Supplier shall be liable for all costs incurred by XYZ and shall reimburse XYZ for all damages and expenses associated with correcting the defect, failure, authenticity and conformance of the Product(s) including field support, logistics, repair, refurbishment, exchange and any other costs associated with correcting the defect, failure, authenticity and conformance.

One customer made an allowance that considered the change in status of a part from a suspected counterfeit to a confirmed counterfeit.

Example 4:
If suspected counterfeit Material is furnished under this Agreement, such Material shall be impounded by XYZ and the seller shall compensate XYZ for the material cost. If material is confirmed to be counterfeit, Seller shall be liable for all ancillary costs including, but not limited to impoundment, investigation, removal and replacement.

Uniquely, one customer acknowledged the distinction of intent in the counterfeit responsibility.

Example 5: If the delivery of counterfeit parts is the result of Supplier's intentional or fraudulent acts, Supplier shall also be liable for the cost of impoundment and removal of counterfeit parts.

Certificates of Conformance

Often in the discussion of authenticity is the Certificate of Conformance. While these documents can be useful in traceability, they are easier to counterfeit than the parts. As such, one customer had a unique requirement:

Example 6: Certificates of conformance from non-franchised distribution sources are not adequate to meet the supply chain traceability requirements, therefore will not be accepted.

CONCULSIONS

Returning to the hypotheses:

1. **Most customers of electronic components addressing counterfeit risk with their suppliers are in the military/aerospace market.**

This hypothesis is supported by the data, showing that 2/3 of the customers are in this industry, with products ranging from aircraft to radar and satellites, land vehicles, ships and submarines. When we consider that many of the contract manufacturers addressing the risk are doing so on behalf of their mil/aero business, the percentage is even higher.

Only one medical company and one automotive company were represented. This may reflect either a lack of awareness in these industries, or their tendency to frequently buy directly from the OCM's, either because of volume or because of strict external oversight and product liability. While these are reasonable conclusions, more study is necessary to draw them with any degree of certainty.

2. **Most customers apply one policy to their entire supply base.**

This hypothesis is supported as only 20 of the 53 documents address different types of suppliers within the supply base.

3. **No distinction is made in requirements for different types of supplier (OCM, Authorized Distributor, Independent Distributor / Broker).**

This hypothesis is supported among the total population, but a sizable number (20) do make a distinction in their policies based on the supplier type, applying more stringent requirements to the Independent Distributor. Of these documents, most require the supplier to obtain written approval from the customer in order to purchase a part from an Independent Distributor. Not mentioned, but assumed in this approach, is some investigative work by the customer of

the independent distributor or the need to purchase from said broker.

Example 7: Parts shall be purchased directly from the OCM/OEM or through their authorized Franchised Distributors. Independent Distributors shall not be used without written consent from the Buyer.

Example 8: To further mitigate the possibility of the unintentional use of counterfeit parts or materials; the Supplier shall only purchase authenticated parts/components directly from the Original Equipment Manufacturers or Original Component Manufacturer (OEM/OCM) or through the OEM/OCM authorized distribution supply chain.

Example 9:
3.1 EEE parts purchased from an OCM
3.2 EEE parts purchased from an OCM Authorized Distributor
3.3 EEE parts purchased from a non-OCM authorized distributors
3.3.1 EEE parts where the non-OCM authorized distributor acquires parts directly from the OCM or OCM authorized distributor
3.3.2 All other EEE parts purchased from a non-OCM authorized distributor

4. **No distinction is made in requirements for parts of differing risk levels (based on reported incidents).**

This hypothesis is supported. Only 9% of the companies made a distinction in the requirements for different types of products. While several external databases and services document counterfeit occurrence and risk by part type and part number, very few companies are formally employing risk based mitigation based on the type of part. Those that are generally have the most advanced counterfeit mitigation programs, applying mitigation based on part type risk.

5. **No distinction is made in requirements for parts used in low risk versus high risk applications.**

This hypothesis is supported: Only one customer made reference to the application of the part in their requirements. This customer was in the medical industry. Experience with this market segment tells us that there is often a distinction between *life critical* or *implantable* devices and those that are not. This is part of the common categorization for is industry and regulations for different applications are regularly addressed throughout their models. While this might be true in some companies outside the medical industry, this is not a common approach.

Other Conclusions

Aside from the hypotheses stated at the beginning of the paper, a few other conclusions can be made from the data.

The most accepted and invoked industry standards are those published by SAE.

SAE's AS5553 is by far the most invoked standard (33%), However, this standard is written primarily for entities building or repairing end items such as the OEM (see figure 1 in AS5553A). The invocation of SAE's AS6081 (5%) was anticipated to be small given its relatively recent publication in November 2012. However, one of these three supplier documents cited AS6081 before it was published and available to greater industry. One of the remaining two invoked AS6081 for all distribution, both independent and authorized. While this invocation is not correct, we should acknowledge that at this time, the standard for Authorized Distribution is not yet complete.

Both the invocation of Section 818 specifically, and the increase in the total number of documents in the last half of 2012, speaks to its influence on the mil/aero industry to address the counterfeit risk. However, while it may have prompted action, the SAE documents were by far the dominant models invoked.

Table VII

External Document	Number	%
None	29	50%
AS5553	19	33%
AS6081	3	5%
Section 818	5	9%
IDEA-STD-1010	2	3%
Total	58	I

The restriction of purchase from Independent Distributors is the most common restriction invoked.

Most of those companies with such restrictions acknowledge that avoiding such suppliers is not always possible and therefore create a path for their use with the approval of the customer. Assumed in this approval process is the research of the actual exhaustion of the authorized channel and then a risk review of the proposed broker should the authorized channel truly be exhausted.

These results are encouraging and clearly show an appreciation of the risk levels of the multiple potential supplier types as regards counterfeit risk.

Assumption of All Related Costs

In those documents requiring the supplier to bear all costs related not only to the replacement of the counterfeit product, but any associated remediation costs, the language of the 2012 NDAA is clearly evident.

The problem with such requirements is that the source of most counterfeits into the supply chain today is through independent distributors[3]. Most of these companies are small concerns and the mitigation costs of one event could likely bankrupt the supplier. While such statements are good in theory, they do not reflect the practical

ramifications of such an event. Further, the proposed related DFARs' exempt small businesses, throwing contractual validity of such clauses into question.

As such, there appears to be a need in the industry for an insurance mechanism to cover such costs should an event occur.

RECOMMENDATIONS

The data supports that the most active market segment regarding counterfeit risk mitigation is that of mil/aero. 1) Other industries are advised to likewise address this issue. While these industries may not have a life threatening risk if a counterfeit is employed, the costs of poor reliability, warranty and reputation should be considered and may be substantial enough to warrant the development of mature counterfeit risk mitigation programs.

2) For those companies not addressing the risk levels associated with different supplier types (OCM, Authorized Distributor, Independent Distributor), it is recommended that their programs evolve to separate the requirements to apply more scrutiny to those with higher risk of counterfeit. This will resolve the issue of increasing cost and complexity in low risk transactions and create subsequent mitigation protocols that are substantive for those of higher risk.

3) While a separate policy for different part numbers might not be feasible, the most mature programs have differing requirements for different part types. Adopting this approach will concentrate one's efforts in the highest risk areas, better utilizing one's limited resources. Currently, and for the anticipated future, this is the IC (Integrated Circuit).

4) While AS5553 is the best known standard, it does not properly address the unique characteristics of the common upstream part suppliers in the supply chain. For purchases through Independent Distributions, AS6081 is recommended. For the lowest risk portion, the authorized channel of the OCM and its authorized distributor, the strategy can be less complex. However the forthcoming AS6496 will address Authorized Distributions. Applying a complicated counterfeit risk mitigation requirement to the OCM who manufactures the component from raw materials is likely an addition of bureaucracy and cost to the transaction. While substandard raw materials (counterfeit?) could theoretically be employed, the level of discussion in the industry in this regard suggests this is a nominal concern.

Finally, 5) companies would do well to recognize that most counterfeits come from very small players in the supply chain, often from abroad. Even if one could execute a claim against said player, the likelihood of recovering the sizable cost of a counterfeit incident from this player is very low. Customers would do well to employ other strategies to protect themselves financially.

ACKNOWLEDGEMENTS

The author would like to acknowledge the tireless dedication of many individuals in the industry to develop methods and standards to address counterfeit electronic risk, and specifically Mr. Phil Zulueta who chairs SAE's G-19 committee. The author would also like to thank Dr. Bill Cardoso whose prompting spurred this analysis.

REFERENCES

1 Committee on Armed Services, United States Senate, Inquiry into Counterfeit Electronics Parts in the Department of Defense Supply Chain,, Report 112-167 May 21, 2012 p. 10

2 Fred Schipp, Counterfeit Electronics Parts, Risk to Government, ASNE Trusted Technologies Conference April, 2011

3 Henry Livingston, Observations from Counterfeit Cases Reported Through The Government–Industry Data Exchange Program (GIDEP), BAE Systems 9/6/2011