EMGT 835 FIELD PROJECT

Counterfeit Components: A Method to Identify and Manage Risk for the Government contracted manufacturers and challenged small businesses.

By

Richard K. Yeager

Master of Science

The University of Kansas

Spring Semester, 2011

An EMGT Field Project report submitted to the Engineering Management Program and the Faculty of the Graduate School of the University of Kansas in partial fulfillment of the requirements for the degree of Master of Science.

_____

Herbert Tuttle **Date**
Committee Chair

_____

Raymond Dick **Date**
Committee Member

_____

Mike Kelly **Date**
Committee Member

Table of Contents

Acknowledgements

I have been working on this research paper for several years and if it were not for the enthusiasm and continued encouragement of my committee members, Herbert Tuttle (Chair), Dr. Ray Dick, Mike Kelley, I would still be working to finish. Thank you! I especially appreciate Herb Tuttle's gentle prodding and Parveen Mozaffar's (Academic Services Coordinator) endless patience with my stopping and starting. During this process I have had to move from Overland Park, Kansas to Washington D.C. and establish a new life. Herb and Parveen have been my trusted guides during this time. I would like to thank Belinda Thompson, John Minihan, Roy Brown and Curt Gittenger at Honeywell FM&T for their help and guidance in understanding the component procurement and evaluation processes and Joanyuan Lee and CALCE at the University of Maryland for access to their library.

Finally, I thank my wife of 35 years, Karen for her unconditional love and support. She kept reminding me that I was just about done, even when I was starting over again and again.

Executive Summary

Counterfeit electronic components have been infiltrating the electronics supply chain and as a result many manufacturer restrict their purchased to authorized distributors or original component manufacturers Military manufactures also require authorized distributors and original component manufacturer (OCMs), but need to support older systems that use obsolete parts or resold parts forcing them to purchase parts from other sources. Most small disadvantaged suppliers are not authorized distributors or OCMs and have difficulty selling material to military manufacturers. In addition, military manufacturers have obligations to use disadvantaged suppliers, but do not want the risk associated with non authorized dealers.

This research paper develops a method to identify risk associated with small disadvantaged suppliers and gives both the manufacturer and the supplier a risk assessment to grade suppliers. With this information a military manufacturer can evaluate each supplier and quantify risk associated with that supplier and compare it to other suppliers. The evaluated supplier has a list of fault modes that can be prioritized and used to improve its position against other suppliers. The result is that each company is examined in nine categories and a numeric risk level associated with each category are established and documented. Both the manufacturer and the supplier have a quantifiable record to communicate with each other.

Chapter1- Introduction

Beginning in the mid 1990's military weapons manufactures began converting from the traditional military-specified (mil-spec) components created after World War II to incorporation of commercial off the shelf electronic components (COTS). Secretary of Defense William Perry issued a directive to reduce costs by using COTS material. His expectation was that commercial component manufacturers' quality levels improved to a level that the use of highly qualified and costly mil-spec material was not required. Furthermore, the life cycle of components and weapon systems development are getting shorter due to advancements in technologies that made systems obsolete only a few years after their introduction into the theater.

Military use of COTS parts expanded markets for suppliers, but also attracted hucksters that found monetary advantage in counterfeiting component for systems manufactures. The necessity to support older systems created a market to supply hard to find components that were needed quickly. These hucksters found ways to counterfeit components and sell them to unsuspecting manufactures, then disappear. The effects of a counterfeit component in a weapons system could be catastrophic. Most weapons manufacturers therefore required that the suppliers deal directly with the original components manufacturers (OCM) and document this with a certificate of compliance (C of C). This works well if a company requires large quantities of components. Large companies that supply components tend to need large orders and do not support older

components and they tend not to be “minority or disadvantaged “, which makes it difficult for government contracted weapons manufacturers to meet their obligations to buy from minority owned businesses. Low volume weapons manufacturers have a greater problem because they need smaller numbers of components and they need them quickly. Traditionally, small to medium minority or disadvantaged suppliers have filled this niche market. But with the increasing influx of counterfeit components in the market, the small supplier is under greater pressure to assure that the parts are authentic. This requires more resources to evaluate and certify the authenticity of the material purchased. The medium to small business needs to balance cost of verification with the risk that the material is counterfeit. This field project identifies the resources that are commonly used by medium and small suppliers to combat the issues of counterfeit components and compares them with military manufactures requirements. With this information, develops a tool to establish risk levels for both the small disadvantaged minority business and the systems manufacturer, thus meeting their government obligations. In addition the tool provides information for the small disadvantaged minority businesses to evaluate their own status for the meeting the manufacturers validation process.

Chapter2 - Literature Review

INTRODUCTION

Understanding the processes dealing with counterfeit electronic components and how they affect government contracted manufactures and small businesses begins with a literature review of common definitions, processes used to quality components, where and how counterfeit component originate and mitigation technique. A beginning must start with a common understanding of counterfeiting. Articles discussing counterfeiting either imply an understanding of what counterfeiting is or present a definition. The definition of counterfeiting and specifically a definition of counterfeit electronic components are important because they define the boundaries of counterfeiting. First, a general definition of Counterfeiting:

> "Counterfeiting is an infringement of legal rights of an owner of intellectual property. Counterfeit goods mean any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country(of importation)". (Chatterjee 2010)

The definition applies any product sold that has a trademark but does not describe the features that constitute an infringement of a trademark or intellectual property. Therefore it is necessary to apply a definition of a counterfeit electronic

component. A counterfeit electronic component is defined as an electronic part that is not genuine because:

- The component is an unauthorized copy.
- The component does not conform to original OCM design, model, and/or performance standards.
- The component is not produced by the OCM or is produced by an unauthorized contractor.
- The component is off-specification, defective, or the component is a used OCM product sold as "new" or working.
- The component has incorrect or false markings and/or documentation.

Processes that produce a counterfeit component can be characterized from the above definition. An unauthorized copy of a component is a component that is produced by an aftermarket manufacturer without the approval of the original component manufacturer. (Crawford 2010)

After the Second World War the military developed a series of specifications that protected itself from counterfeit material by controlling all aspects of the design, testing and acceptance of electronic parts, known as “Milspecs”. The Milspecs were necessary because the design requirements for weapons and their components were too complex and costly for any single commercial part manufacturer to absorb the cost of failure. (Baron 2006) The government paid for the development of weapons components in order to assure a supply of high quality material. The commercial component industry improved during the

1980's fueled by the development of the computer industry. Cheap high quality computer parts drove the cost of a computer down and the quality up. In the early 1990's military budgets were being slashed due to the end of the cold war. A 1994 memo from Secretary of Defense, William Perry changed the government's approach to purchasing commercial material in weapons. The "Perry Memo" asserted that business policies needed to change because they no longer made sense for new technologies and instructed all armed forces to transition to Commercial Off the Shelf parts or COTs. The memo directed that all the old Milspecs be replaced with commercial specifications where practical. This redefined the procurement processes for military components. (Baron 2006)

Commercial of the Shelf components required by the military were more likely targets for international counterfeiting due to the globalization of the electronic component market and the internet, the preferred tool for purchasing components. Component providers work in small offices all over the world using the internet to conduct business. (Pecht 2006) This made it easy to set up an internet company, sell counterfeit electronic components then disappear. The next step may well be the counterfeiting of a whole company. In 2004 NEC discovered a parallel counterfeit NEC brand set up in China with links to more than 50 electronic factories in mainland China, Hong Kong and Taiwan. (Lague 2006)

The military manufacturers have reacted by requiring only material from Original Component Manufacturers or authorized distributors of the OCMs components.

As the systems that the manufacturers aged the need to support them required that replacement parts be acquired. Medium to Small companies called “Brokers” supported the military manufactures by purchasing out of date material from companies liquidating old inventory and overstock material and reselling it to them when needed to service old systems. These companies tend to be disadvantaged minority owned companies. (Grow 2008) The manufactures needed their services to repair their old systems and at the same time fulfill their obligations to use disadvantaged companies. (Livingston 2007) This relationship worked well until counterfeit components became more and more difficult to distinguish from the authentic parts.

The Commerce Department surveyed three hundred eighty seven companies and organizations in the industry on the issues of counterfeit components. The report divided the industry into five segments; original component manufacture (OCM), distributers and manufactures, circuit board assemblers, prime and subcontractors and Department of Defense (DOD) agencies. Each segment was examined for: a) Levels of suspected/confirmed counterfeit parts, b) Types of devices being counterfeited, c) Practices employed in the procurement and management of electronic parts, d) Recordkeeping and reporting practices, e) Techniques used to detect parts, and f) Best practices employed to control the infiltration of counterfeits. It also provides a baseline definition of a counterfeit component. The condition of the OCM, distributers and manufactures are important in the understanding of risk levels needed for this paper. With this information an

FMEA can assign a level of risk and establish categories for evaluation by both the contractor and small business.

Counterfeit electronic components have been infiltrating U.S. manufacturing from many sources. The most common suspected sources are China, Taiwan, Philippines and Malaysia, see figure VII-15. (Crawford 2010) Inside these countries are small shops that process used components into new looking parts. Many of the parts are from the very computers, televisions and other electronics that we throw away. The material is shipped to cities in the Far East and dismantled. (Hammond 2010) The circuit boards are removed and stripped of their components by low paid worker using crude and dangerous processes; see Figure I-1, Figure I-2 and Figure I-3.

Figure I-1

Hammer on monitor (Hammond 2010)

Figure I-2

Disassembly (Hammond 2010)

Figure I-3

Removing parts (M. H. Crawford 2010)

After the parts are made to look new, they are remarked and sold on the internet. These parts are not functional, but by the time a buyer detects that they are counterfeit, the company has reinvented itself or gone out of business. These parts are fairly easy to detect, but cost the buyer time and money. The more dangerous sources of counterfeit components take functional parts that are low grade and remark them as high grade material. These parts are harder to detect because the only way to be certain that they are good is to perform testing on the components. The testing is expensive and takes time to perform, so when parts are detected as counterfeit a considerable amount of time and money has already been lost. The most sophisticated counterfeiters obtain rejected Die to make their own look alike part. (Grow 2008) These parts require inspection of the internal chip to verify they are counterfeit. The more difficult counterfeit part to detect is a plastic body integrated circuit that must meet humidity requirements. If the part is

not kept under strict humidity control it can crack when installed and if not detected fail at a critical time during the products' performance. Many parts are the correct parts, but have had the solder coat on the leads recoated to accommodate a need for tin lead finishing. This requires testing of the leads and if not caught can lead to a condition called tin whiskering.

The following is information on counterfeit electronic component from the Commerce Department on the scope of the problem, the contributing behaviors, factors and findings. (M. H. Crawford 2010)

SCOPE OF PROBLEM

Thirty nine percent of those questioned had encountered a counterfeit component. Forty six percent of original component manufactures experienced a counterfeit discrete component and fifty four percent experienced a counterfeit microcircuit. Twenty two percent of authorized distributors and eighty three percent of unauthorized distributors experienced a counterfeit component. Thirty four percent of the board assemblers, twenty five percent of Prime/Sub contractors experienced a counterfeit component. The Department of Defense reported that seventeen point seven percent of DLA Organizations and thirty two percent of Non-DLA Organization had experienced a counterfeit component. These numbers illustrate that counterfeit components have occurred in all parts of the supply chain. The unauthorized distributor encountered the most, see figure I-4.

Figure I-4

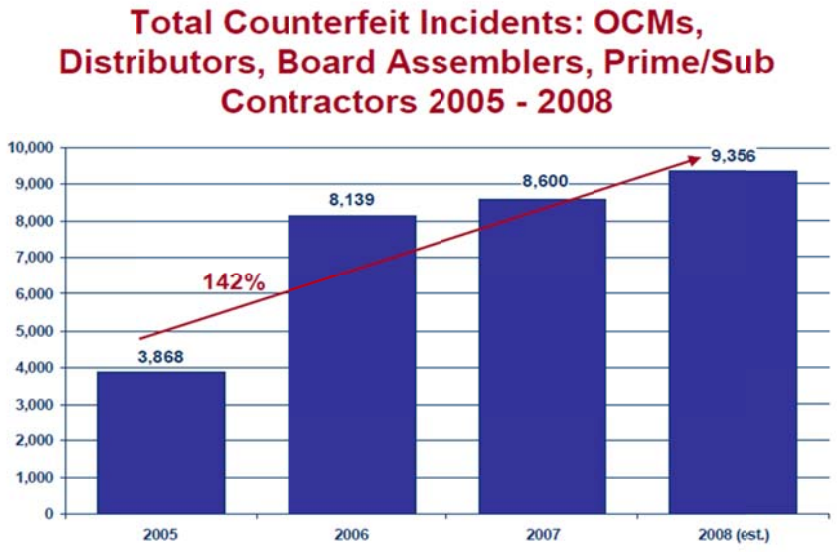
Organizations Encountering Counterfeit Electronics

Type of Company/Organization		Encountered Counterfeits	No Counterfeit Incidents	Total
Original Component Manufacturers	Discrete Electronic Components	18	21	39
	Microcircuits	24	20	44
Distributors	Authorized Distributors	10	35	45
	Unauthorized Distributors	44	9	53
Board Assemblers		11	21	32
Prime/Sub Contractors		31	90	121
Department of Defense	DLA Organizations	3	16	19
	Non-DLA Organizations	11	23	34
Total		152	235	387

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* August 2009.

Total counterfeit incidents increased one hundred forty two percent from 2005 to 2008, see figure I-5.

Figure I-5



(M. H. Crawford 2010)

In figure I-6 the red highlighted products were considered safe products, but the numbers of counterfeit incidents have increased dramatically.

Figure I-6

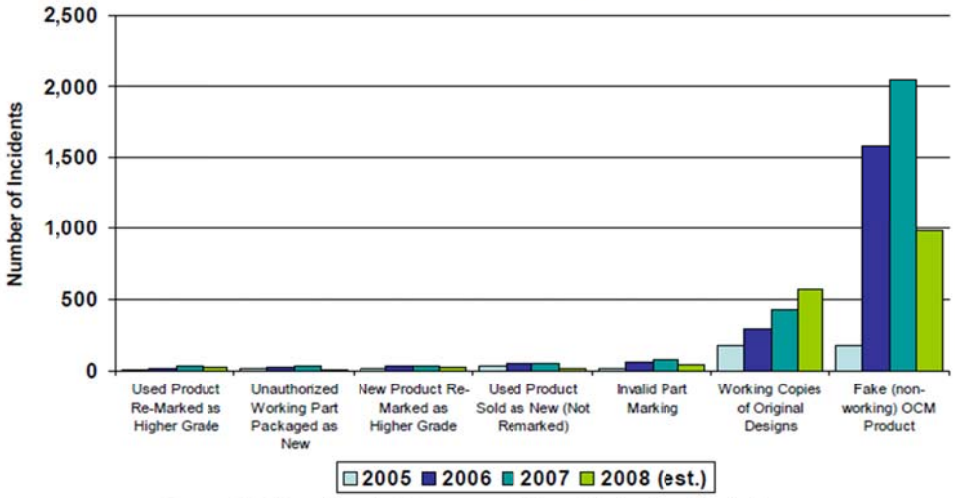
Types of Counterfeit Incidents (2005-2008)

Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	1739	4860	3841	2839
Consumer	154	345	398	531
High Reliability – Industrial	**49**	**81**	**164**	**488**
Qualified Manufacturers List (QML)	**49**	**77**	**161**	**261**
Critical Safety	**42**	**63**	**93**	**277**
Qualified Products List (QPL)	**16**	**39**	**111**	**144**
High Reliability – Medical	1	24	58	105
ITAR Controlled	15	10	67	19
Commercial Aviation	9	15	17	27
High Reliability – Automotive	2	6	8	25
Generalized Emulation Microcircuits (GEM)	0	0	0	2

(M. H. Crawford 2010)

Figure VII-12 shows that most discrete counterfeit components are non-functional or working copies of original designs.

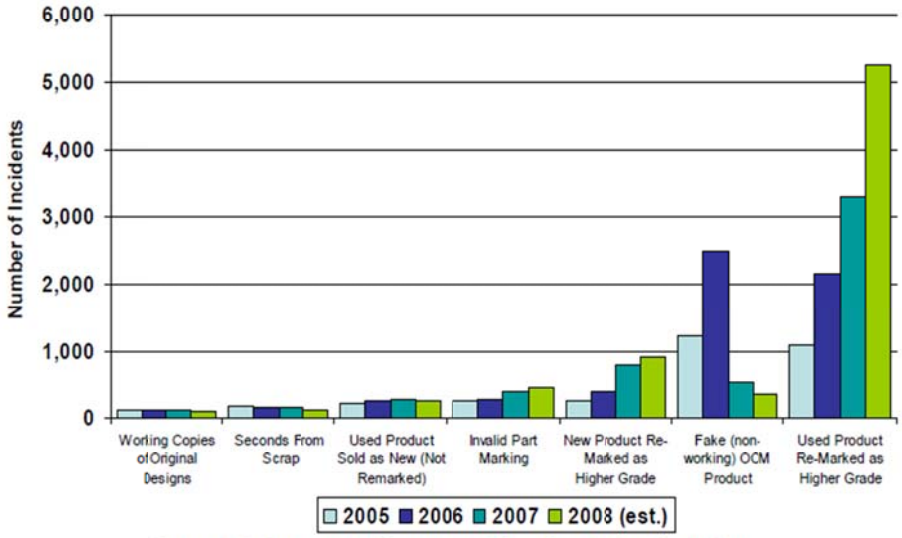
Figure VII-12: Counterfeit Incidents by Type of Problem – Discretes (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure VII-13 shows that most microcircuit counterfeit components are non-functional or remarked used product to a higher grade.

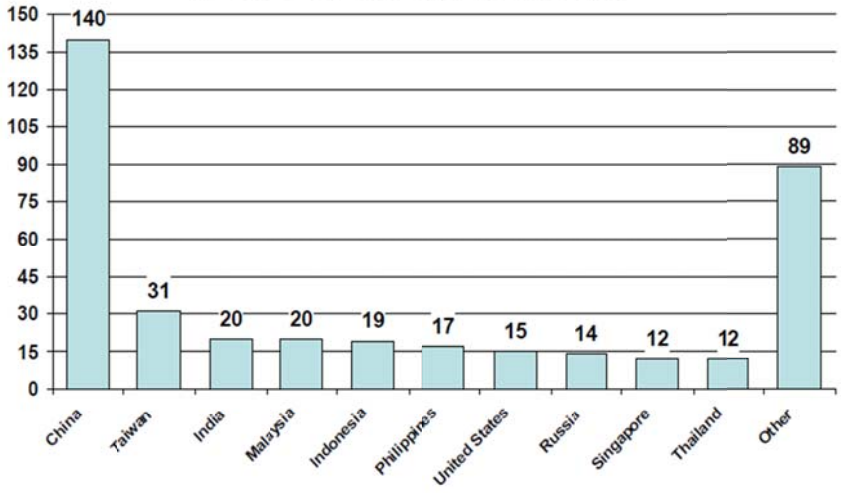
Figure VII-13: Counterfeit Incidents by Type of Problem – Microcircuits (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure VII-15 shows that the leading source for counterfeit components is China, but counterfeit components can come from other countries even the United States.

Figure VII-15: Top Countries Suspected/Confirmed to be Sources of Counterfeits*

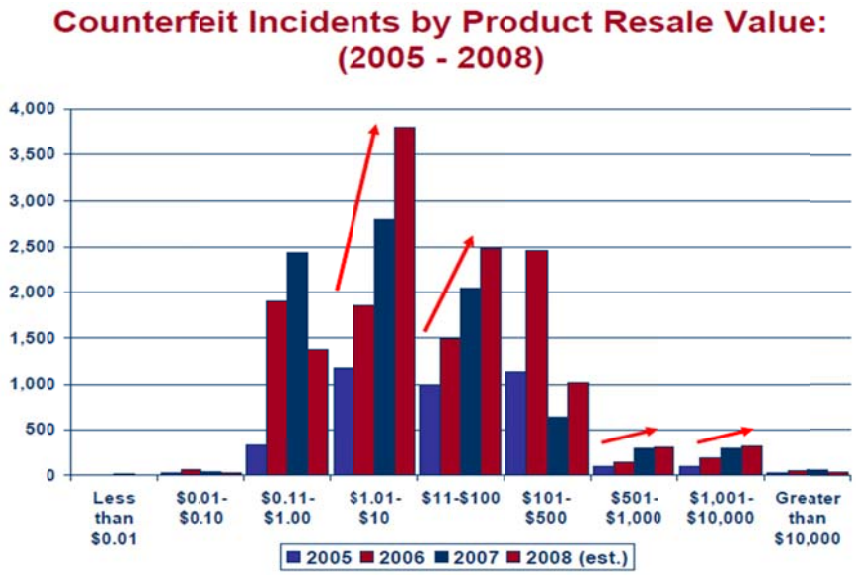


* Each company was asked to provide their top five suspected countries

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure I-7 shows the counterfeit incidents by product resale value. Note that the highest occurrence is in the one to ten dollar amount. This price range is desirable because of the money and time it takes to find and prosecute a counterfeiter; most companies just eat the cost and move on.

Figure I-7



(M. H. Crawford 2010)

ACTIONS CONTRIBUTING TO PROBLEM

Counterfeit parts enter the supply chain for several reasons; Figure VII-28 lists the top ten. Note that the top two reasons involve brokers, which involve small minority owned businesses. Two important issues are inadequate inventory management and the use of gray market parts. Inventory management is important in that most distributors accept returns from customers, buy back excess inventory from customers and then restock the returns. Inventory control and return policies are listed in Figure I-8, Note that the highest level of customer

returning counterfeit parts is with the distributors at thirty one percent, the next being seventeen percent from OCMs.

Figure VII-28: Top Ten Reasons For Counterfeits Entering the Supply Chain	
Less Stringent Inventory Management by Parts Brokers	179
Greater Reliance on Gray Market Parts by Brokers	168
Greater Reliance on Gray Market Parts by Independent Distributors	152
Insufficient Chain of Accountability	141
Less Stringent Inventory Management by Independent Distributors	139
Insufficient Buying Procedures	124
Inadequate Purchase Planning by OEMs	117
Purchase of Excess Inventory on Open Market	113
Greater Reliance on Gray Market by Contract Manufacturers	107
Inadequate Procuction by OCM	105
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, May 2009.	

Figure I-8

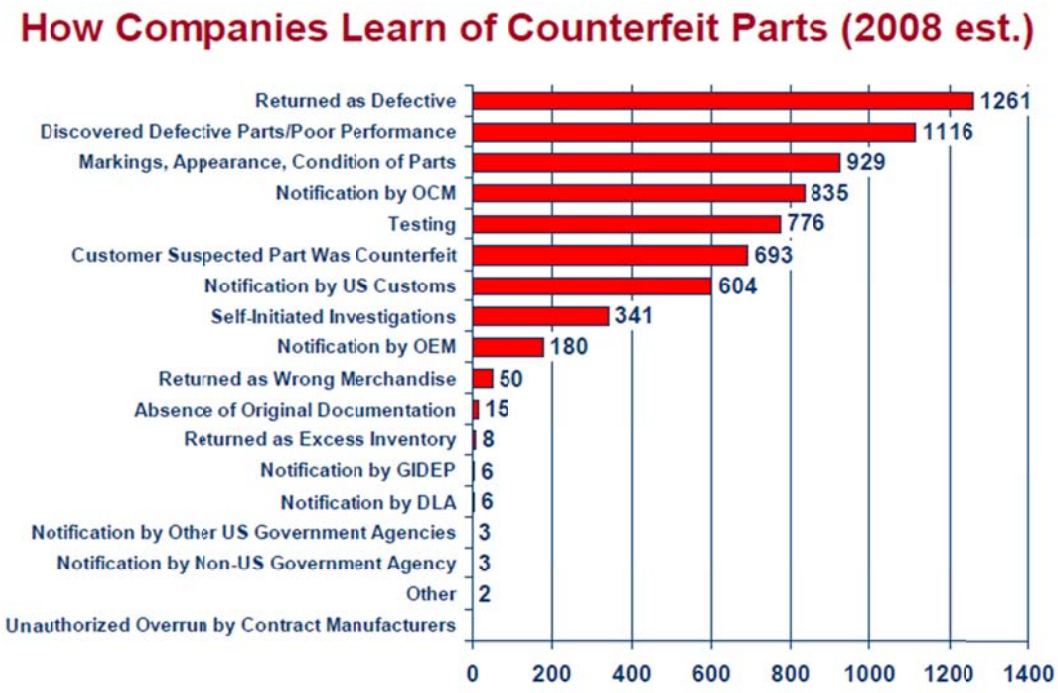
Inventory Control and Return Policies

	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
Accept Returns From Customers	96%	100%	84%	81%
Buy Back Excess Inventory From Customers	25%	46%	16%	7%
Restock/Re-circulate Returns or Excess Inventory From Customers	61%	54%	13%	21%
Have Cases of Individual Customers Returning Counterfeits	17%	31%	3%	2%

(M. H. Crawford 2010)

The way a company finds a component reflects the company's commitment to a system for detecting counterfeit component. Unfortunately most parts are discovered when they are returned or installed and found defective, figure I-9 lists the how companies learn of a defective part. Finding the part after it is installed is the most expensive place to find. Note that the top in the list are also the most expensive way to find them.

Figure I-9

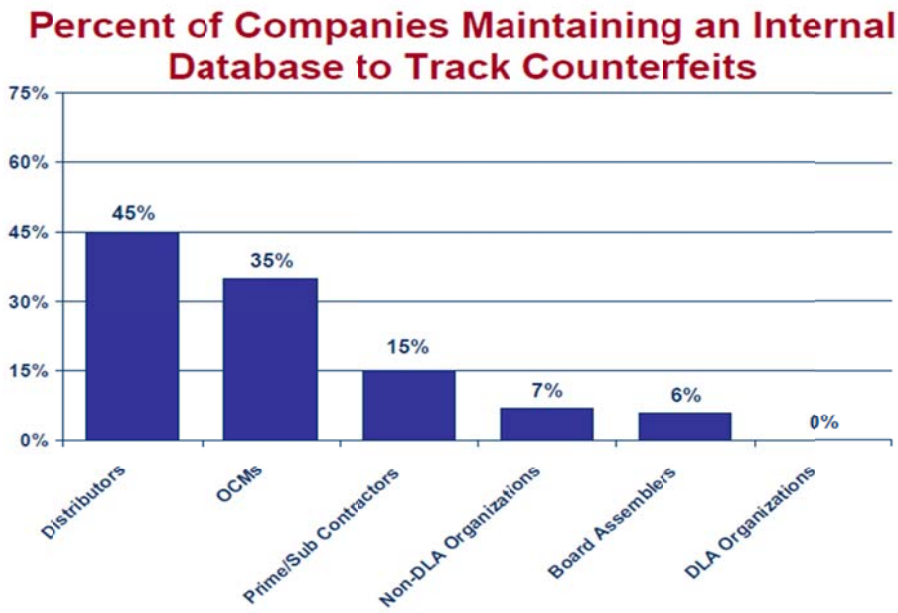


(M. H. Crawford 2010)

Most companies do not use an internal data base to track counterfeit components. Only forty five percent of distributors, thirty five percent of OCM's and fifteen percent of Prime/Sub Contractors maintain a internal database. Only eighteen percent of discrete manufactures and sixteen percent of microcircuit manufactures

audit their inventory. (M. Crawford 2010) Most important is that very little notification occurs when a counterfeit part is found, see figure I-10.

Figure I-10



(M. H. Crawford 2010)

Preventative actions both internal and external are listed in figure I-11 and I-12. Note thirty five percent of the companies take no actions at all. These charts identify policies important for small businesses, such as training staff, keeping procedures current, testing inventory, and customer interaction.

Figure I-11

Varying Internal Actions Taken to Prevent Infiltration of Counterfeit Parts

Action	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors	DOD
Performing screening and testing on inventory	27%	8%	41%	37%	21%
Training staff on the negative economic and safety impacts of counterfeit products	31%	65%	28%	36%	15%
No internal actions taken	**35%**	**19%**	**34%**	**32%**	**72%**
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	35%	76%	25%	23%	11%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	34%	44%	22%	17%	11%
Other	8%	12%	9%	17%	0%
Revising procurement procedures to reduce purchases from independent distributors and brokers	-	-	13%	4%	11%
Embedding new security measures in existing product lines	12%	4%	3%	2%	2%
Adding security markings to existing inventory	12%	0%	0%	2%	8%

(M. H. Crawford 2010)

Figure I-12

Limited External Actions Taken to Prevent Infiltration of Counterfeit Parts

Action	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
No external actions taken	**35%**	**29%**	**59%**	**69%**
Tightening contractual obligations of contract manufacturers with regard to disposal of "seconds," defective parts, and overruns	29%	11%	3%	12%
Educating customers/suppliers on the negative economic and safety impacts of counterfeit products	31%	52%	16%	9%
Educating customers about risks associated with grey market products	40%	57%	28%	8%
Other	6%	5%	3%	9%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	19%	30%	25%	6%
Referring customers to authorized after-market manufacturers	27%	21%	9%	5%
Prohibiting authorized distributors from buying back excess inventory on the grey market	31%	10%	6%	5%
Prohibiting authorized distributors from buying back excess inventory from their customers	6%	5%	0%	3%

(M. H. Crawford 2010)

BEST PRACTICES

The counterfeit Electronics Study (M. H. Crawford 2010) identified fifteen best practices.

- Establish clear written policies and procedures
- Increase internal/external communication
- Institute counterfeit part training programs
- Ensure physical destruction of defective parts
- Inspect all returns and buy-backs to verify authenticity
- Buy parts from OCMs and authorized distributors when possible
- Establish lists of trusted and unapproved suppliers
- Implement contract requirements for counterfeit avoidance policies and practices
- Scrutinize suppliers with cheap prices/short lead times
- Require traceability of part back to the OCMs
- Verify parts meet purchase order requirements and documentation (inspections/testing)
- Establish strict inventory controls
- Remove counterfeits from regular inventory; quarantine
- Maintain internal database to track counterfeits
- Report counterfeits to law enforcement and industry associations/databases

Chapter 3 - Research Procedure

The methodology for this research procedure involved the following:

- Identifying key risk categories for small business manufacturers
- Developing a survey for small businesses using these risk categories
- Conducting a survey of three small businesses using the survey.
- With the data, establishing risk level for each category for a FMEA.
- Finally each company was compared and contrasted for the use of a manufacturer purchasing a product.

The FMEA was translated into a list for a small business to use to perform a self assessment to prepare for a manufacturer audit.

Chapter 4 - Findings

Three small businesses were examined, one minority family owned (company A), one privately owned (company b) and Hub Zone Certified Small business owned by an investment group (company C). Each company was examined in nine categories; Policies and Procedures, Training, Communications, Procurement, Record Keeping, Storage, Inspection, Testing and Management of Detected Counterfeit Parts. Each company was chosen for its' particular sector in small business. The following is a summary of each company and the analysis for each FMEA. A summary of the RPNS are available in Appendix, A-2.

Company A is minority family owned supplier of electronic components. Annual gross income is approximately $500,000 per year. The business is housed in two small buildings in the Ft. Lauderdale, Florida area. The company is ISO 9000:2000 compliant, certified small disadvantaged minority owned business and CCR registered. All policies and procedures are kept in paper form using a binder system with updates made by the receiving inspector/quality manager. Training is performed as needed by the company owner. Communications are mainly verbal and paper. All procurement is performed using computers that have custom software written by a local friend of the family. Sources are screened using a preferred vendor list kept by noting bad experience with source. Uses credit checks to verify capability of source. Primary records are paper stored in a 300 square foot room in a building on site; some records are electronically stored on hard drive and backed up. Very little product is stored on site. The receiving, inspection, testing and storage area are all located in an approximately 700 square foot room. Detection on counterfeit components is the responsibility of the operator that does receiving inspection and quality management. There is no apparent area for segregation of counterfeit material. The results of company A are summarized in figure I-13a and the FMEA for company A follows in figure I-13b.

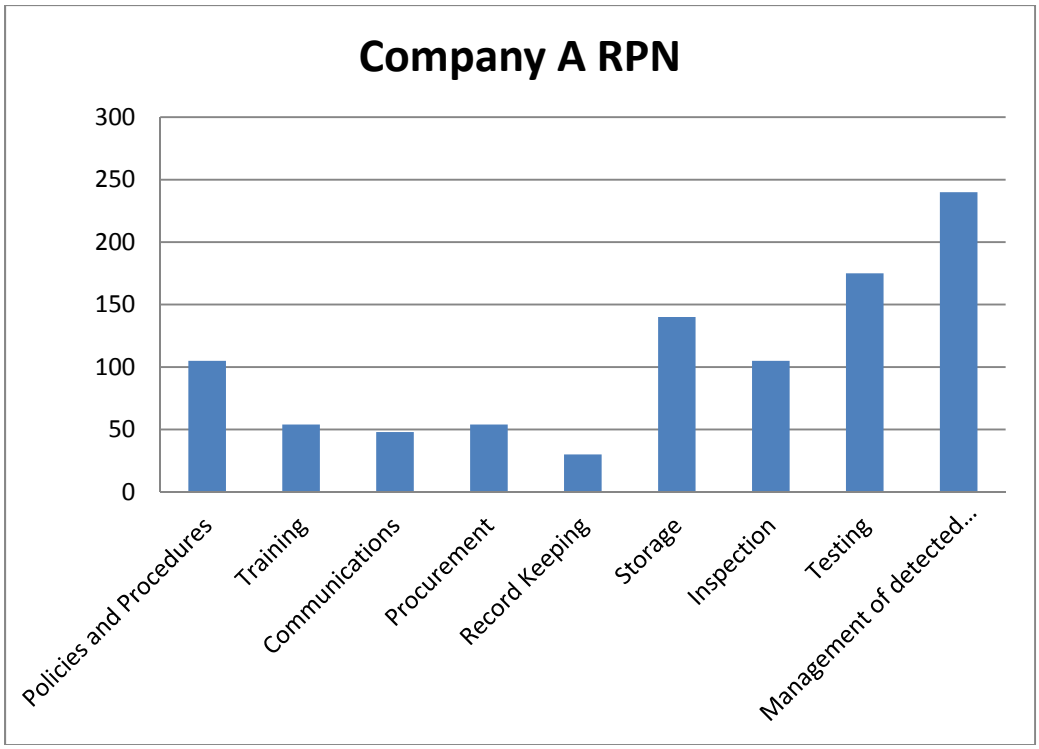

Company A RPN
300
250
200
150
100
50
0
Policies and Procedures
Training
Communications
Procurement
Record Keeping
Storage
Inspection
Testing
Management of detected...

Figure I-13a

Small Business Risk Analysis

Category	Counterfeit Component Risk Analysis
Company:	Company A

Prepared by:	Richard Yeager	Page:	of
Date (Orig):		Rev.	

Key Process Step or Input	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes	OCC	Current Controls	DET	RPN	Actions Recommended	Resp.	Actions Taken	SEV	OCC	DET	RPN
What is the Process Step or Input?	In what ways can the Process Step or Input fail?	What is the impact on the Key Output Variables once it fails (customer or internal requirements)?	How severe is the effect to the customer?	What causes the Key Input to go wrong?	How often does cause or FM occur?	What are the existing controls and procedures that prevent either the Cause or the Failure Mode?	How well can you detect the Cause or the Failure Mode?		What are the actions for reducing the occurrence of the cause, or improving detection?	Who is Responsible for the recommended action?	Note the actions taken. Include dates of completion.				
Policies and Procedures	M,P,K,A,H,	$F	7		3		5	105				0	0	0	0
Training	NT,RT	$R	6		3		3	54							0
Communications	NX	$R	4		4		3	48							0
Procurement	IV	$R	6		3		3	54							0
Record Keeping	PAS	$R	5		3		2	30							0
Storage	SI	$F	7		4		5	140							0
Inspection	NII	$F	7		5		3	105							0
Testing	NDPA,NET,NIF,NTT	$F	5		7		5	175							0
Management of detected counterfeit components	NMDQ,NADB	$R	8		6		5	240							0

Figure I-13b (Pereira 2010)
Page **26** of **47**

Company B is privately owned and located in the suburbs of Detroit. The company does approximately $750,000 a year gross sales. It is a member of ERAI, IDEA and is ISO 9000:2000 certified. All policies and procedures are kept electronically with controlled copies updated automatically when changes are approved. Training is performed by external certified contractors and all records are kept and tracked electronically. All communication, procurement and record keeping are performed using a commercial software package that tracks all aspects of the business process. Procurement verification of suppliers is electronic using currently available searchable database provided by GIDEP, a preferred supplier list and a credit check. Storage, Inspection, testing and counterfeit component management is performed in a 600 square foot climate controlled room by the receiving inspection/quality manager. Very little product is stored at the facility. Segregated Counterfeit material is kept in a small locked cabinet in the receiving area. The results of company B are summarized in figure I-14a and the FMEA for company B follows in figure I-14b.

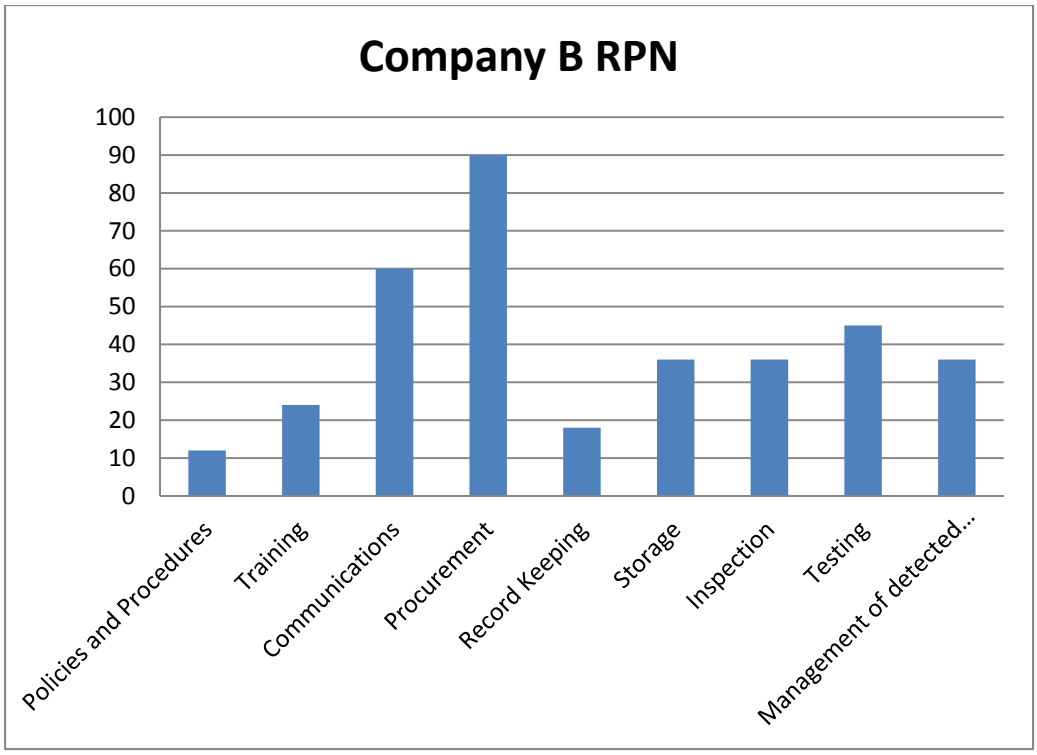

Company B RPN
100
90
80
70
60
50
40
30
20
10
0
Policies and Procedures
Training
Communications
Procurement
Record Keeping
Storage
Inspection
Testing
Management of detected...

Figure I-14a

lean six sigma academy

Small Business Risk Analysis

Category	Policies and Proceedures		Prepared by:	Richard Yeager	Page:	of
Company:	Company B		Date (Orig)		Rev.	

Key Process Step or Input	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes	OCC	Current Controls	DET	RPN	Actions Recommended	Resp.	Actions Taken	SEV	OCC	DET	RPN
What is the Process Step or Input?	In what ways can the Process Step or Input fail?	What is the Impact on the Key Output Variables once it fails (customer or internal requirements)?	How Severe is the effect to the customer?	What causes the Key Input to go wrong?	How often does cause or FM occur?	What are the existing controls and procedures that prevent either the Cause or the Failure Mode?	How well can you detect the Cause or the Failure Mode?		What are the actions for reducing the occurrence of the cause, or improving detection?	Who is Responsible for the recommended action?	Note the actions taken. Include dates of completion.				
Policies and Procedures	A,RD	$R	2		3		2	12							
Training	NT	$R	3		2		4	24							0
Communications	NX	$$	3		5		4	60							0
Procurement	IV	$$	3		6		5	90							0
Record Keeping		$R	2		3		3	18							0
Storage	SI	$$	3		3		4	36							0
Inspection	NII	$$	3		3		4	36							0
Testing	NET, NIF, NTT	$$	3		3		5	45							0
Management of detected counterfeit components	NMDQ	$R	4		3		3	36							0

Figure I-14b (Pereira 2010)
Page **29** of **47**

Company C is a Hub Zone Certified Small business located in St. Petersburg, Florida, owned by an investment group grossing approximately $5 million dollars a year. The company has an offshore affiliate located in the Far East. The company is ISO 9000:2000 certified, member of ERAI and IDEA. All policies and procedures are kept and tracked electronically. Training is performed via external certified contractors and tracked in a commercially available software package. Communication is tracked electronically. Procurement sources are verified using GIDEP databases and verifying government reports. All record keeping is electronic. All incoming material is stored in a small 600 square foot room separate from inspection. Inspection is performed by a dedicated inspector in a small 300 square foot climate controlled room. X-ray and basic electrical testing was being developed in a separate 600 square foot climate controlled room. All counterfeit material is segregated in a locked storage cage. The results of company C are summarized in figure I-15a and the FMEA for company C follows in figure I-15b.

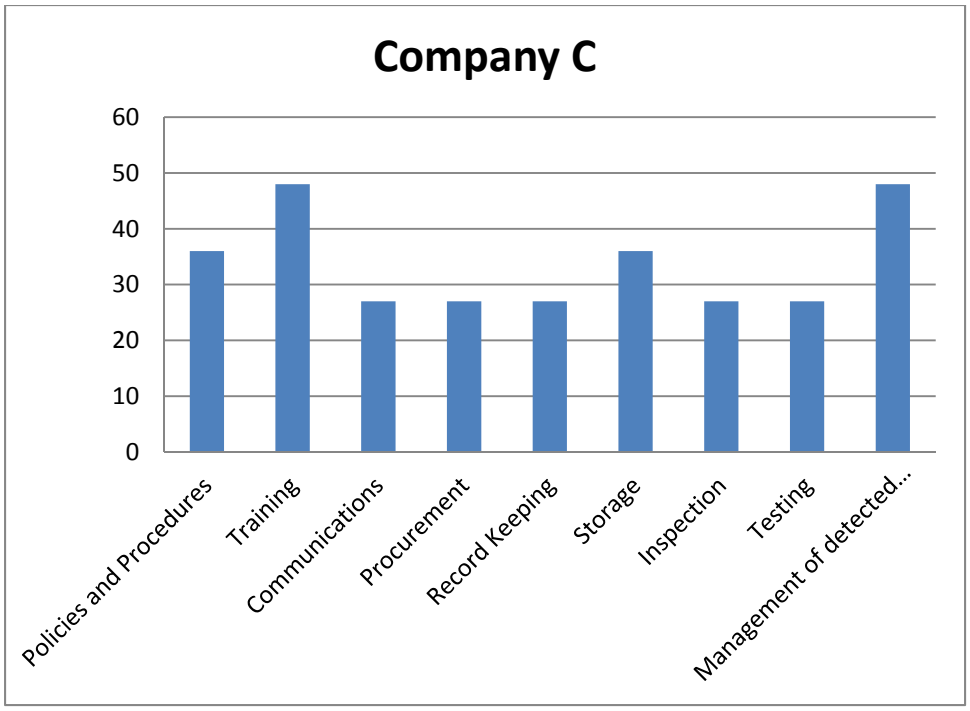

Company C
60
50
40
30
20
10
0
Policies and Procedures
Training
Communications
Procurement
Record Keeping
Storage
Inspection
Testing
Management of detected...

Figure I-15a

lean six sigma academy

Small Business Risk Analysis

Category	Policies and Proceedures
Company:	Company C

Prepared by:	Richard Yeager	Page:	of
Date (Orig):		Rev.	

Key Process Step or Input	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes	OCC	Current Controls	DET	RPN	Actions Recommended	Resp.	Actions Taken	SEV	OCC	DET	RPN
What is the Process Step or Input?	In what ways can the Process Step or Input fail?	What is the Impact on the Key Output Variables once it fails (customer or internal requirements)?	How Severe is the effect to the customer?	What causes the Key Input to go wrong?	How often does cause or FM occur?	What are the existing controls and procedures that prevent either the Cause or the Failure Mode?	How well can you detect the Cause or the Failure Mode?		What are the actions for reducing the occurrence of the cause, or improving detection?	Who is Responsible for the recommended action?	Note the actions taken. Include dates of completion.				
Policies and Procedures	RD	SR	3		3		4	36				3	3	3	27
Training	NT	SR	3		4		4	48							0
Communications		SR	3		3		3	27							0
Procurement		SR	3		3		3	27							0
Record Keeping		SR	3		3		3	27							0
Storage	SI	SR	3		4		3	36							0
Inspection		SR	3		3		3	27							0
Testing		SR	3		3		3	27							0
Management of detected counterfeit components	NMDQ,	SR	3		4		4	48							0

Figure I-15b (Pereira 2010)

All facilities provided external certified testing of parts and including destructive part analysis. Only company C had x-ray capability on site with trained personal. The following tables (figure I-16 and figure I-17) are the potential failure codes and the potential modes developed for each category used in the FMEAs. Figure I-16 defines the possible outcomes from a failure to detect a counterfeit component. An undetected counterfeit to the customer is the worst, next is the part detected in the facility and the best outcome would be before it gets to the facility.

Figure I-16

Potential Failures	Potential Code
Undetected counterfeit part to customer.	$F
Part detected before it gets out of facility, but company must obsorb all costs.	$$
Part detected before it gets out of facility, but must negotiate return of purchase costs.	$R

Figure I-17 is a table of the possible failure modes associated with the best practices suggested by the Department of Commerce. The failure modes are meant to be a starting point and as a company is audited new modes may be discovered. This is the approach of an FMEA in that the small business is expected to fill out the corrective action side of the FMEA. The figure I-17 also serves as a check list for the small business to review for the next audit.

Figure I-17

Input Category	Failure Mode	Mode Code
Policies and Procedures	Missing or sub standard policy or procedure to detect counterfeit components.	M
	Missing or sub standard policy for avoidance of counterfeit components.	A
	Missing or sub standard policy for handling of counterfeit components.	H
	Missing or sub standard management involvement	MI
	Missing or sub standard policy for updating policies of counterfeit components.	UP
	Missing or sub standard policy for following published standards of counterfeit components.	PS
	Missing or sub standard policy for tracking incomming and outgoing material.	TR
	Missing or sub standard policy for reporting, managing and disposal of detected parts.	RD
Training	Inadequate training to identify possible counterfeit parts.	IT
	No hands on training.	IH
	Not everyone gets training.	NT
	Training not kept up to date. No refresher course.	RT
Communications	No communication between employees about concerns and issues they have incountered.	NC
	No communication to and from customers or external data bases.	NX
Procurement	Inadequate verification of source	IV
	No traceability of parts.	NTP
	No trusted supplier list or insufficient list requirements.	NTL
	No certificate of Conformance.	NCOC
	No escrow service.	NE
	Inadequate security.	NS
Record Keeping	system is paper only slow to respond to changes.	PAS
Storage	Inadequate or not organized.	SI
Inspection	No check of information on parts.	NIC
	No scope or camera to verify parts.	NIH
	No library to check parts against.	NIL
	Not trained by certified instructor.	NII
Testing		
	No marking check with chemical rub.	NMC
	No Distructive Physical testing or insufficient.	NDPA
	No Electrical testing or insufficient testing.	NET
	Inadequate facilities and Inventory storage.	NIF
	No third party testing or insufficient quality.	NTT

Figure I-17(continued)

Input Category	Failure Mode	Mode Code
Management of detected counterfeit components		
	No Quarantine area for part or turn over to FBI, ect..	NMDQ
	No internal data base to check for companies, individuals, countries or parts as known or suspected counterfeiters or counterfeit parts.	NMDB
	No access to U.S. customs reports, GIDEP reports or industry associations and data bases.	NADB

The FMEA rates the company A as the most risky company with five categories of concern; policies and procedures, storage, inspection, testing and management of detected counterfeit components. Company B is second with two areas of concern: Procurement and communications. Company C would be the best of class with conformance to all best practices suggested by the Department of Commerce report.

Chapter 5 – Summary

After the Second World War, military component procurement depended up the use of mil-specs until Secretary of Defense William Perry ordered the use of commercial off the shelf (COTS) parts in 1994. Mil-specs controlled the design, testing and acceptance for procurement of a component. In order to facilitate

COTS parts Perry ordered the mil-specs be replaced with commercial specifications where practical. Budgets during the mid 90s were being cut due to the end of the cold war and commercial parts were considered a cost effective way to support new systems. At this time the growth of the personal computer market drove the quality levels to a level that made using COTS parts an option. The internet developed into the preferred tool for purchasing components. Using the internet made part procurement a global business. Small shops in China and all around the world were counterfeiting electronic parts. This forced manufactures to restrict purchasing of components to OCMs and authorized distributors. But defense contractors had systems to support that required small quantities of obsolete parts. Small minority owned businesses had supported the military's needs and at the same time the military manufactures met their contractual obligations to buy from disadvantaged businesses. The contractors need a way to evaluate the risk of using a small minority business. The minority businesses need a way to demonstrate that they have the appropriate safeguards in place.

Most of the world's counterfeit parts come from China, but not exclusively. Many of the counterfeit parts come from the very electronics we discard in America. Parts are scavenged in small shops using cheap labor under very dangerous conditions. The parts are reconditioned and are non-functional. They are made to look like new and sold to unsuspecting customers on the internet. Other parts are functional, but are remarked to look like higher quality parts and some shop even have the ability to use die to package into look alike parts. As the

level of counterfeiting sophistication increases industry has not reacted as quickly. The Department of Commerce studied the state counterfeiting and published a report in 2010. From this report nine categories were identified for use in an FMEA to evaluate risk, they were; policies and procedures, training, communications, procurement, record keeping, storage, inspection, testing and management of detected counterfeit parts.

Three small businesses, Company A, B and C were examined for compliance/risk to the nine categories. Company A was a small family owned business, Company B was a larger privately owned business and Company C was the larger Hub Zone Certified Small business. Company A was identified as the largest risk followed by Company B and the least risk was Company C. A table of possible failure modes was developed from the FMEA for each business to address for future audits.

Chapter 6 – Conclusions

A business contemplating using a small privately owned business to provide materials should perform a risk analysis for best practices and expect to have to budget for costs of development of areas that require resources that the small business cannot afford. Costs associated with upgrading the deficient areas must be weighed against the risk of noncompliance using the FMEA. A visit to the small business is a must; most issues are readily apparent with a simple analysis and can be prioritized for the owner. As the business grows, the more attention it pays to best practices and concerns of new techniques than just trying to survive.

The smaller business should be given less risky parts, such as discretes and made to prove their capability. After an audit of the external testing resources the small business may be able to handle microcircuits. With the risk analysis performed periodically progress can be evaluated from the baseline FMEA. This should be done with all companies and shared with the purchasing agents of the purchasing company. Keeping purchasing informed of the quality levels of each small business can minimize risk when part schedules are short and the purchasing agent needs to make a quick decision.

Suggestions for Additional Work

1.) Government agencies could establish a standardized risk assessment tool to document the possible modes of failures that are being reported by the public and publish an annual report.
2.) Industry councils could develop a suggested tools and processes for a standardized risk assessment.
3.) Small business could develop an internal risk assessment list that is prioritized to work on deficient area and communicate these issues to employees.

References/Bibliography

Baron, Sally J. F. "COTS FOUNDATIONS:ESSENTIAL BACKGROUND AND TERMINOLOGY." *INTERNATIONAL PUBLIC PROCUREMENT CONFERENCE PROCEEDINGS.* Unknown: INTERNATIONAL PUBLIC PROCUREMENT CONFERENCE, 2006. 98,99.

Chatterjee, Kaushik. *SOLVING THE COUNTERFEIT ELECTRONICS PROBLEM.* Research, College Park, MD: Center for Advanced Life Cycle Engineering (CALCE), 2010.

Crawford, Mark. *DEFENSE INDUSTRIAL BASE ASSESSMENT:COUNTERFEIT ELECTRONICS.* Government, Washington,DC: U.S. DEPARTMENT OF COMMERCE,BUREAU OF INDUSTRY AND SECURITY,OFFICE OF TECHNOLOGY EVALUATION, 2010.

Crawford, Mark H. "Counterfeits and the U.S. Industrial Base." *Semicon West.* Washington D.C.: Office of Technology Evaluation, Bureau of Industry & Security, U.S. Department of Commerce, 2010. 34.

Grow, Brian. "Dangerous Fakes." *Business Week*, October 8, 2008: 4,5.
Hammond, Robb. *China's New Export Laws are Placing Lives in Jeopardy.* unknown unknown, 2010. www.aeri.com/chinese-counterfeit-parts.asp (accessed March 7, 2011).

Lague, David. "Next Step for Counterfeiters:Faking the Whole Company." *The New York Times*, 5 1, 2006: 1,2,3.

Livingston, Henry. "Avoiding Counterfeit Electronic Components." *IEEE TRANSACTIONS ON COMPONENTS AND PACKAGING TECHNOLOGIES, VOL 30,NO1*, 2007: 187-189.

Pecht, Michael. "Bogus!" *IEEE Spectrum*, May Unknown, 2006: 4,5.

Pereira, Ron. *Lean Six Sigma Academy.* 06 28, 2010. http://Issacademy.com/2007/06/28/10-steps-to-creating-a-fmea/ (accessed Feburary 28, 2011).

Glossary - Principal Symbols and Nomenclature

(M. Crawford 2010)

After-Market Manufacturer: A company engaged in the manufacture of electronic products
initially but no longer produced by an original component manufacturer.

Authorized Distributor: A company that is authorized by an Original Component Manufacturer
(OCM) or Original Equipment Manufacturer (OEM) to market, store, and ship OCM/OEM products.

Best Practice: An efficient and effective standard process that can be adopted by multiple
organizations.

Brokers: Companies/individuals engaged in the marketing of electronic parts, often scarce parts.
Brokers frequently do not actually possess in inventory the parts being sought, but act as "middle
men" to arrange the sale of the part from a third party.

Burn-In Testing: A test which involves running a system or device for a period of time to ensure
that all components are working properly.

Certificate of Conformance: Document certified by a competent authority that the supplied
good or service meets the required specifications.

Contract Manufacturer: A manufacturer that produces made-to-order custom electronic parts,
including assembled electronic boards, for a private or government customer. Parts and board
products manufactured by the contract manufacturer are not brand-name products marketed and
sold by the contract manufacturer.

Counterfeit: An electronic part that is not genuine because it 1) is an unauthorized copy; 2) does
not conform to original OCM design, model, and/or performance standards; 3) is not produced by
the OCM or is produced by unauthorized contractors; 4) is an off-specification, defective, or used
OCM product sold as "new" or working; or 5) has incorrect or false markings and/or documentation.

Critical Safety Parts: Parts whose failure would cause loss of life, permanent disability or major
injury, loss of a system, or significant equipment damage.

Die: A single integrated circuit (or chip) cut from the wafer on which it was manufactured.

Defense Microelectronics Activity (DMEA): A Department of Defense facility located near
Sacramento, CA, which manufactures integrated circuit products and electronic systems for U.S.
Government national security applications.

Decapsulation (decapping): When the packing of a component is opened in hermetic conditions to allow for the examination of the die and internal features of the package.

Discrete Electronic Component: Individual components such as capacitors, diodes, resistors,
transistors that can be mounted on a circuit board to form a working electronic system.

Electronic Testing: Evaluating the functionality of a discrete component or IC part and determining whether the electrical parameters of the part conform with the alternating current
(AC) and direct current (DC) characteristics specified by its manufacturer. Measurements can be
made at room temperature or over the recommended operating temperature range for the part.

End-User: The person or entity that uses a product.

Excess Inventory: Legitimate, genuine new electronic part product held by OCMs, OEMs,
authorized distributors, contract manufacturers, and U.S. government agencies.

FEDLOG: A Defense Logistics Agency system used to retrieve management, part/reference
number, supplier, Commercial and Government Entity (CAGE), freight, Interchangeability and
Substitutability (I&S) and characteristics information recorded against National Stock Numbers
(NSNs).

First Article Testing: A series of inspections and tests designed to ensure parts conform to
drawings or part specifications.

Generalized Emulation of Microcircuits (GEM): Reengineered integrated circuit products
whose manufacture has been authorized to meet the need for replacement parts for product that
is obsolete. These replacement products are designed and tested to emulate all the functions of
microcircuits that are no longer in production.

Gray Market: The trade of parts through distribution channels which, while legal, are unofficial,
unauthorized, or unintended by Original Component Manufacturers.

Hologram: Three-dimensional printing used to validate authenticity.

Incident: Occurrences, reports, or transactions pertaining to electronic parts suspected and/or confirmed to be counterfeit. For example, a report involving 10 copies of a single electronic part model equals one incident. Occurrences, reports, and transactions involving three separate electronic part models equal three separate incidents, regardless of the volume counterfeit parts for any given model.

Independent Distributor: A company that markets and distributes electronic parts often acquired as excess inventory from OCMS, OEMs, contract manufacturers, U.S. Government organizations, and other entities. Independent distributors maintain inventories of parts and typically have controlled environments for part storage.

International Traffic in Arms Regulations (ITAR): U.S. Department of State regulations controlling the export and import of defense-related articles and services on the United States Munitions List.

Inventory control point (ICP): An organizational unit or activity within a Department of Defense supply system that is assigned the primary responsibility for the materiel management of a group of items either for a particular Service or for the Defense Department as a whole. Materiel inventory management includes cataloging direction, requirements computation, procurement direction, distribution management, disposal direction and, generally, rebuild direction.

Legal Action: Filing of warning letters, civil complaints and lawsuits; filing criminal complaints; support of criminal investigations and prosecution by law enforcement agencies.

Life of Type or Life Time Buy: A final purchase by a DOD organization of an electronic part prior to the cessation of production by its manufacturer.
.

Microcircuit: A miniaturized electronic device containing multiple solid-state circuits that works in conjunction to form a complete device with defined functions, and that has been manufactured on the surface of a thin substrate of semiconductor material. In these devices many active or passive elements are fabricated and connected together on a continuous substrate, as opposed to discrete devices, such as transistors, resistors, capacitors and diodes that exist individually.

Mined Die: An integrated circuit product removed from its original OCM package and placed in a new package.

Non-Conforming Parts: Parts that do not meet standard requirements or conditions.

Non-U.S.: Foreign country where microcircuit production, purchase, or company incorporation is
located.

Original Component Manufacturer (OCM): A company that manufacturers discrete electronic
components and/or microcircuits.

Original Equipment Manufacturer (OEM): A company that supplies equipment to other companies to resell or incorporate into another product using the reseller's brand name.

Pedigree Paperwork: Documentation that tracks a part's history back to its original manufacturer.

Physical Evaluation: A process of confirming that materials used in a discrete component or IC
part are genuine. It can involve destructive tests such as decapping the component's package to
validate its authenticity; evaluation of materials used in a device's packaging materials (including
connection leads and encapsulant); and examination of discrete and IC parts to verify it is genuine using various techniques including layer by layer destructive examination.

Pre-Stock Testing: Testing of products, through any means, before they are placed in a company's inventory.

Prime Contractor: A lead contractor that directs and manages the delivery of large projects or
products. Typically, prime contractors rely on subcontractors to provide part or all of the major
components, designs, parts, or subsystems required to complete and deliver a working product.

Product Quality Deficiency Report (PQDR): A form used by the military services and the
General Service Administration to record and transmit data on defects or nonconforming conditions detected on new or newly reworked Government-owned products, premature equipment failures, and products in use that do not fulfill their expected purpose, operation or
service.

Radio Frequency Identification (RFID): Any method of identifying unique items using radio
waves.

Scrap: Defective, damaged, or used electronic parts or systems from which electronic parts may
be scavenged.

"Seconds": Off specification, sub-standard product made by Original Component Manufacturers/Original Equipment Manufacturer that is normally destroyed by OCM/OEMs.

Subcontractor: A company that provides parts, subsystems, or systems required by a prime

contractor for completion of a product or project.

Thermal/Temperature Cycling: Determines the ability of parts to resist extremely low and extremely high temperatures, as well as their ability to withstand cyclical exposures to these
temperature extremes.

U.S. Munitions List: Articles and services designated by the President of the United States with
concurrence from the Department of Defense as being specifically designed or configured for
military applications; there are no equivalent civilian or commercial products.

Visual Inspection: Non-destructive evaluation involving visual examination for correct labeling,
shape, size and dimension, form, fit, color, security coatings, etc. Visual inspection can include
use of other non-destructive evaluation such as X-ray, XRF (X-ray fluorescence), and scanning
acoustic microscopy.

Appendices

Appendix A-1

This is the method for creating an FMEA from the Lean Six Sigma Academy. **(Pereira 2010)**

10 Steps to Creating a FMEA

June 28, 2007 By Ron Pereira 12 Comments

A Failure Modes Effect Analysis (FMEA) is an extremely powerful tool that all people can and will benefit from no matter your occupation or status in life.

Tonight, we shall discuss the history of the FMEA, the different types of FMEA, and finally how to actually construct one. At the end of the post is a free FMEA template for your downloading pleasure.

History

The FMEA is not a new tool. The aerospace industry used the FMEA during the Apollo missions in the 1960s. Later in 1974 the US Navy developed MIL-STD-1629 which discussed the proper use of the tool. And around this time the automotive folks latched onto the tool and never let go. Today, the FMEA is universally used by many different industries.

Type of FMEA

There are three main types of FMEA in use today.

1. System FMEA: Used to analyze complete systems and/or sub-systems during the concept of design stage.
2. Design FMEA: Used the analyze a product design before it is released to manufacturing.
3. Process FMEA: Used to analyze manufacturing and/or assembly process.

The Process FMEA is probably the most commonly used and is also the least complex, in most cases.

10 steps to creating a FMEA

1. **List the key process steps in the first column**. These may come from the highest ranked items of your **C&E matrix**.
2. **List the potential failure mode for each process step**. In other words, figure out how this process step or input could go wrong.

3. **List the effects of this failure mode**. If the failure mode occurs what does this mean to us and our customer… in short what is the effect?
4. **Rate how severe this effect is** with 1 being not severe at all and 10 being extremely severe. Ensure the team understands and agrees to the scale before you start. Also, make this ranking system "your own" and don't bother trying to copy it out of a book.
5. **Identify the causes of the failure mode/effect** and rank it as you did the effects in the occurence column. This time, as the name implies, we are scoring how likely this cause will occur. So, 1 means it is highly unlikely to ever occur and 10 means we expect it to happen all the time.
6. **Identify the controls in place to detect the issue** and rank its effectiveness in the detection column. Here a score of 1 would mean we have excellent controls and 10 would mean we have no controls or extremely weak controls. If a SOP is noted here (a weak control in my opinion) you should note the SOP number.
7. **Multiply the severity, occurrence, and detection numbers** and store this value in the RPN (risk priority number) column. This is the key number that will be used to identify where the team should focus first. If, for example, we had a severity of 10 (very severe), occurrence of 10 (happens all the time), and detection of 10 (cannot detect it) our RPN is 1000. This means all hands on deck… we have a serious issue!
8. **Sort by RPN number and identify most critical issues**. The team must decide where to focus first.
9. **Assign specific actions with responsible persons**. Also, be sure to include the date for when this action is expected to be complete.
10. **Once actions have been completed, re-score the occurrence and detection**. In most cases we will not change the severity score unless the customer decides this is not an important issue.

Dynamic Document

The single biggest failure people make with FMEAs is to spend time completing the document and then storing it in a file cabinet somewhere. The FMEA is the ultimate dynamic document meaning it lives as long as the process or product it is associated with does. Please use them!

Appendix A-2

Graph of the results of the FMEA by category for each company.