Identifying and Combatting Counterfeiters

Edward Laliberte
Northrop Grumman Systems Corporation
Charlottesville, Virginia

Abstract
This paper explores the process of identifying and evaluating potential counterfeit parts. The military customer is aware that counterfeit parts are a problem and has created Defense Federal Acquisition Regulation Supplement (DFARS) 252.246-7007 to add protection and avoidance of the use of counterfeit parts in military products. Thus, defense subcontract manufacturers need to understand and assure no counterfeit parts get into any product. This paper provides a real example of identifying a counterfeit part and the process taken to resolve the issue. The topics that will be addressed include:

i) Defining what, who, and how of counterfeit parts,
ii) Using an industry analysis tool to understand the counterfeit risk,
iii) Uncovering anomalous electrical behaviors,
iv) Researching the manufacturer's part markings,
v) Informing management about the potential counterfeit part,
vi) Involving a third party to analyze and test for authenticity,
vii) Expanding the team to address the issue with the customer and distributor, and finally,
viii) Providing lessons learned and suggested future measures for avoidance.

Introduction
Several industry sources have estimated that five percent or higher of electronic parts in distributers' supply chains are counterfeit. Most of these counterfeit parts are repackaged used parts that are obsolete by the original manufacturer or parts that are expensive or limited in supply, e.g. military-grade electronic components. The use of counterfeit parts raises concerns about national security (spying) and endangers lives (erratic unpredictable behavior).

To help protect against counterfeit part use in military products, the Department of Defense (DoD) issued a final rule amending the Defense Federal Acquisition Regulations Supplement (DFARS) in 2012 to include clause 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System. The revised DFARS regulations addressed contractor's responsibilities for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts. Also, the DFARS 7007 clause recommended the use of trusted suppliers and created requirements for contractors to report counterfeit electronic parts and suspect counterfeit electronic parts. Per 246.870–2 Policy, "a counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas:

1) The training of personnel.
2) The inspection and testing of electronic parts, including criteria for acceptance and rejection.
3) Processes to abolish counterfeit parts proliferation.
4) Processes for maintaining electronic part traceability.
5) Use of suppliers that are the original manufacturer, sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources.
6) The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts.
7) Methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit.
8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
9) Flow down of counterfeit detection and avoidance requirements.
10) Process for keeping continually informed of current counterfeiting information and trends.
11) Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information.
12) Control of obsolete electronic parts." [1]

Definitions

As defined in the 252.246-7007 clause:

"Counterfeit electronic part means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f) (2) of Pub. L. 112-81). The term "electronic part" includes any embedded software or firmware.

Obsolete electronic part means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.

Suspect counterfeit electronic part means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic."[1]

What, who, and how of counterfeit parts

As shown in Figure 1 and noted in the UK Electronics Alliance (UKEA) position paper, producing and selling counterfeit parts is big business.

Alliance for Grey Market and Counterfeit Abatement (AGMA), based in the USA, estimates that, in 2006, up to 10% of technology products sold worldwide are counterfeit, which amounts to $100 billion of sales revenues.[2] [3]

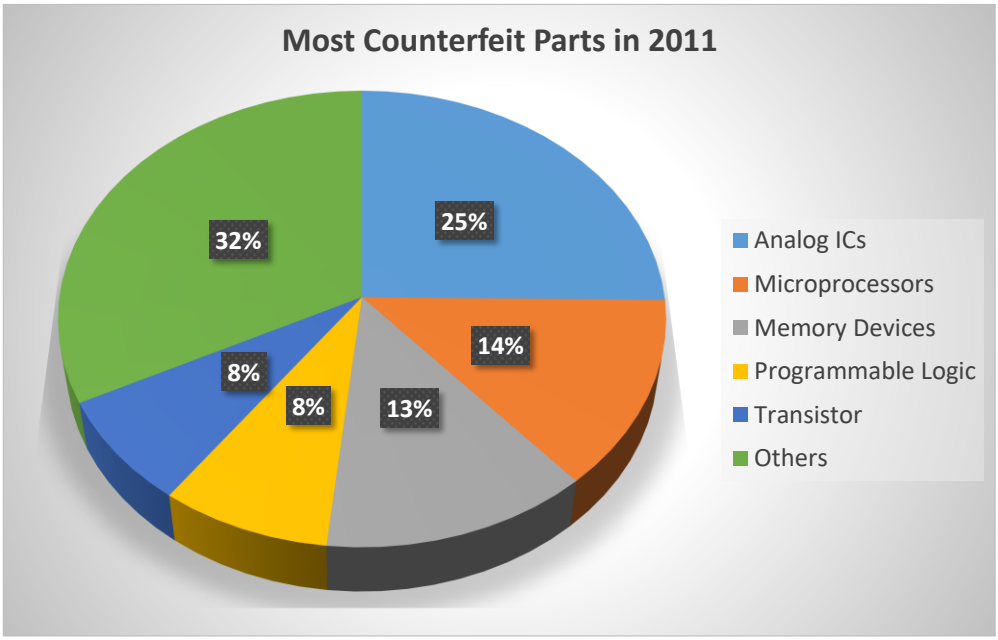


Figure 1: Breakdown of Counterfeit Parts Reported in 2011 [4]

Realizing that counterfeit parts exist is important for all personnel to understand, so training is essential. However, identifying counterfeit parts at incoming inspection can be difficult because counterfeiters are doing better jobs in marking and packaging the counterfeit parts. Also, not all parts that experience some anomalies or erratic behavior are necessarily counterfeit as manufacturers sometimes experience defects in their process. Therefore, the best approach is to be cautious when approaching suspect counterfeit parts like a detective solving a crime and not jump to quick conclusions.

Using an industrial tool to understand the risks

If a part has some visual anomalies (e.g. bent pins, poor markings, multiple date codes in same package, etc.), the inspector should be suspicious and ask for mission assurance and engineering guidance. If a part is thought to be suspect counterfeit by an inspector, mission assurance should review the potential counterfeit risk of a part by reviewing GIDEP reports such as the list in Table 1 for the EP610DI-30 Ultra Violet (UV) Erasable Programmable Logic Device (EPLD) component. If access to the GIDEP reports (http://www.gidep.org/) is not available, the engineer could use any number of available industry part search tools offered by distributors or private held companies to determine the risks as shown in Figure 2.

Table 1: List of GIDEP Reports for EP610DI-30 Component

MPN	Notification Date	Counterfeit Methods	GIDEP Source
EP610DI-30	3-Jan-11	Different Supplier, New Parts (Third Party)	B7C-A-11-002
EP610DI-30	3-May-12	Different Supplier, Old Parts (Third Party)	B7C-A-11-002
EP610DI-30	30-Oct-14	Same Supplier, Old Parts (Third Party)	SP-A-15-01
EP610DI-30	11-Mar-15	Same Supplier, Old Parts (Third Party)	SP-A-15-02
EP610DI-30	15-Jul-15	Same Supplier, Old Parts (Third Party)	AAN-U-15-268

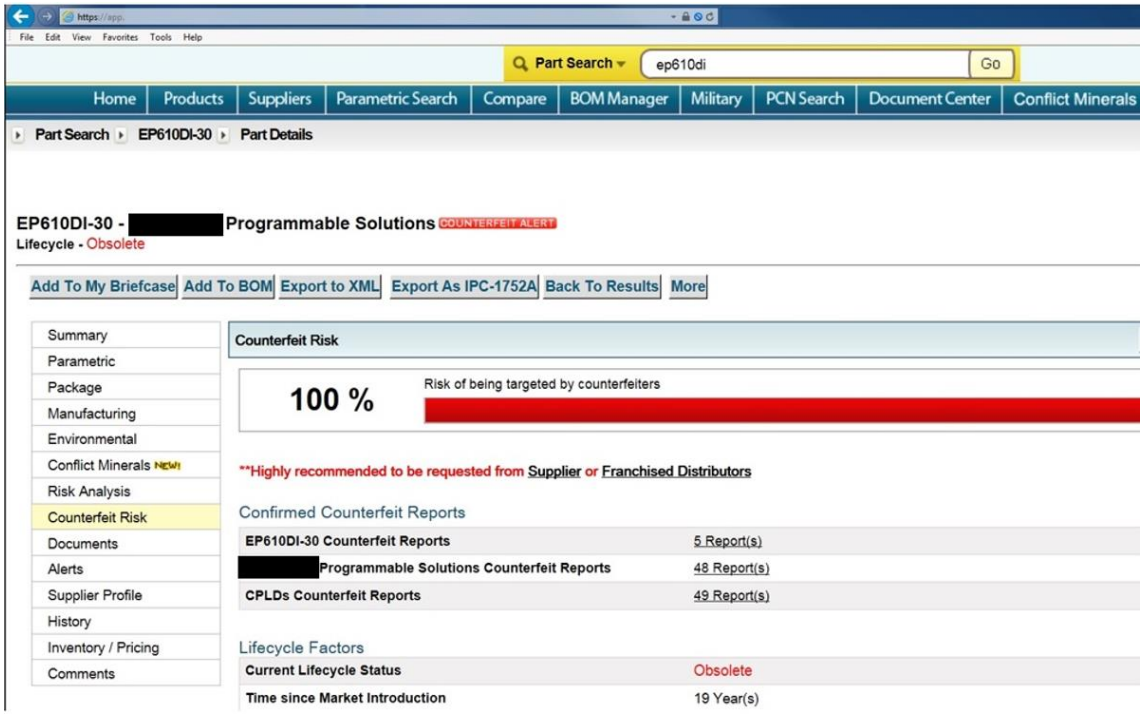


Figure 2: Counterfeit Risk Assessment for EP610DI-30 Component

The engineer should review current and prior manufacturer datasheets of the particular part paying particular attention to the part markings and packaging per the datasheet. In addition, the engineer should review all product change notices (PCNs) from the manufacturer to determine whether a manufacturing site change was made, whether the part is obsolete by the manufacturer, or any other relevant changes. As shown in Table 2 for the EP610DI-30 component, there were several packaging and labeling changes, acquisitions, and assembly line changes. All of these changes should be reviewed carefully and understood in order to explain any differences between parts received at incoming inspection that may result in some visual anomalies between parts that raised suspicion. The PCN identifying part obsolescence should be scrutinized more heavily because diminishing manufacturing source and material supply (DMSMS) is a primary driver of counterfeit parts.

Table 2: List of PCNs for EP610DI-30 Component

Type of Change	Description	Notification Date	Source
Vendor Acquisition	Company Y Completes Acquisition of Company T	28-Dec-15	News Release
Vendor Acquisition	Company Y Completes Acquisition of Company A	11-Dec-15	ADV1508
Labeling, Packing, Product Code, Vendor Acquisition	Company Y Completes Acquisition of Company M. Now all Company M products are sold and supported under Company Y name	29-Nov-13	ADV1314
Packing	Company M is implementing the shipment box dimension and desiccant count changes in an effort to streamline packing and logistics.	31-May-13	ADV1305
Vendor Acquisition	Company M Completes Acquisition of Company B	14-May-13	News Release
Assembly Site	Company M is expanding its manufacturing capacity at Company Ltd (Thailand) and second source Company Ltd2 (Malaysia) and third source Company Ltd3 (Taiwan).	30-Apr-13	ENP-PCN-2013-02
Labeling	Company M will be extending the maximum storage shelf life for all products from 18 months to 36 months.	17-Mar-11	ADV1101
Vendor Acquisition	Company M Completes Acquisition of Company H	14-Dec-10	News Release
Labeling, Packing	Company M will be extending the maximum storage shelf life for all products from 18 months to 36 months.	14-Dec-09	ADV0908 Rev 1.0.0
Packing, Labeling	Company M is implementing enhanced labels for the moisture barrier bag and inner box.	17-Sep-09	ADV0908 Rev 1.0.1
Obsolescence Notices	Company M discontinued some of products	13-Jul-06	PDN0605
Vendor Acquisition	Company M Completes Acquisition of Company G	8-May-00	News Release
Vendor Acquisition	Company M Completes Acquisition of Company F	1-May-00	News Release
Vendor Acquisition	Company M Completes Acquisition of Company E	11-Oct-99	News Release
Vendor Acquisition	Company M Completes Acquisition of Company D	1-Jun-99	News Release

Uncovering anomalous electrical behaviors

If the test technician experiences a higher than usual failure of a particular device during board test, he should ask an engineer to investigate the component failure. Before investigating the electrical anomalies, the engineer should review the latest manufacturer's datasheet and research latest PCNs and counterfeit risk as discussed above. Continuing with the EP610DI-30 UV EPLD component example, the test technician experienced a high failure rate during test. The engineer compared the output signals of the problematic EPLD parts as shown in Figures 3 and 4 to the output signals of a known good EPLD part in Figure 5. Comparing the timing of the two output signals of Figures 3 and 4 to Figure 5, the timing of "F1_17.5KHz" and "F2_17.5KHz" output signals is slightly different causing the /FAIL output signal to pulse.

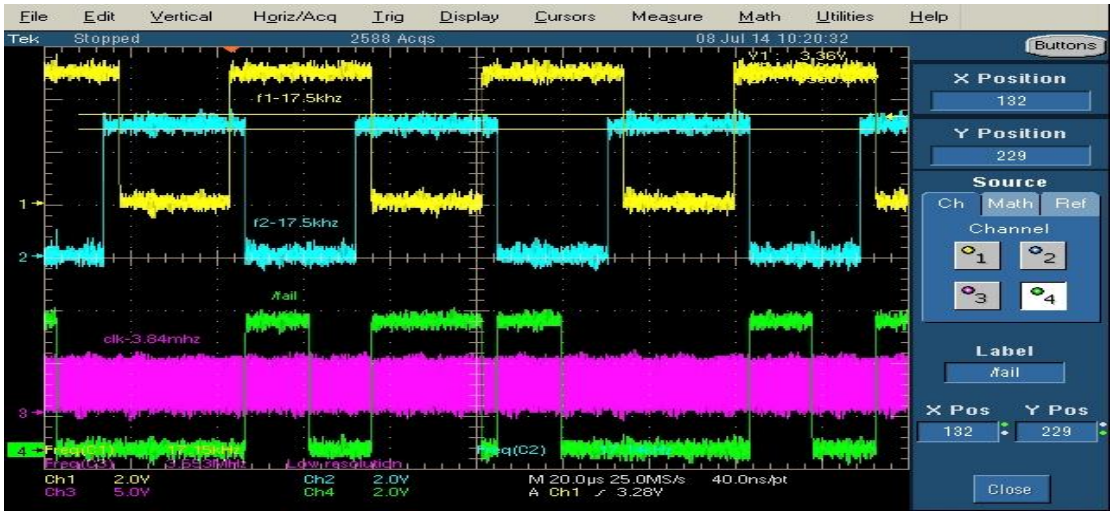


Figure 3: EPLD Failure # 1

Figure 4: EPLD Failure # 2

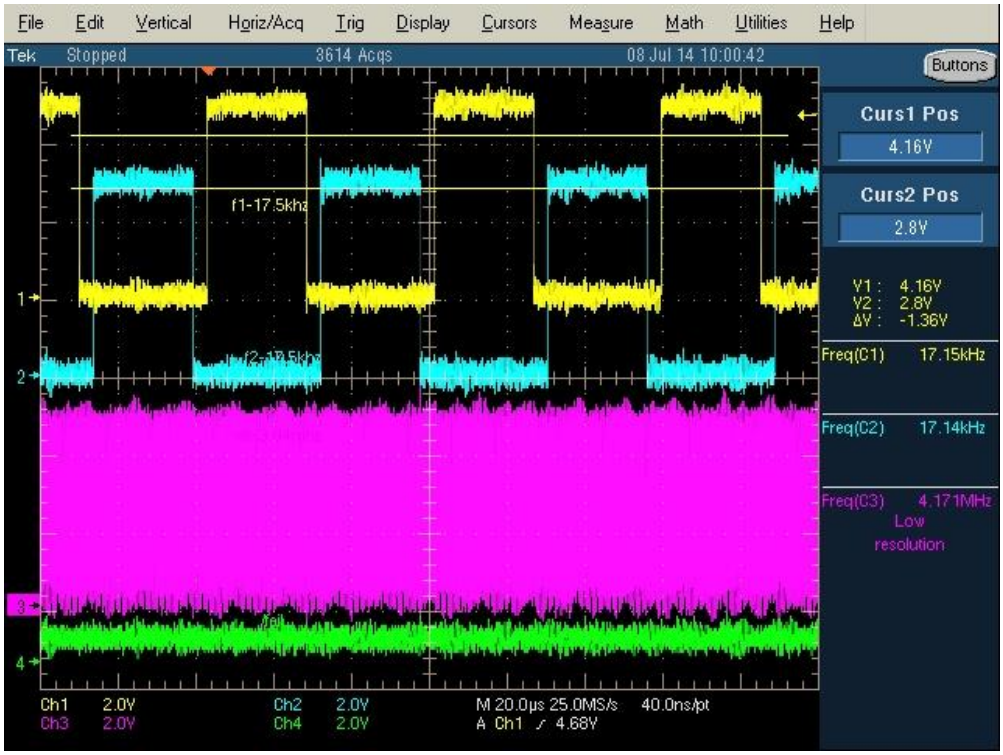


Figure 5: Known Good EPLD

Both EP610DI-30 UV EPLD components depicted in Figures 3 and 4 verified at the Data IO Programming Station with the correct checksum. The engineer erased one of the problematic EPLD components in the UV eraser for 25 minutes. The EPLD component was then reprogrammed and verified successfully. However, the part timing appeared even worse than the original condition, shown in Figures 3 and 4. The EPLD component was then put into the UV eraser for 1 hour and reprogrammed. Finally, the EPLD component started to perform similar to the known good EPLD component. Even though

the parts were programmed and verified, apparently some internal fuse links were not cleared during the erasing of the EPLD component resulting in unpredictable behavior. Also, UV erasing a "new" EP610DI-30 EPLD component for 1 hour prior to programming the part is not a standard procedure. Typically, only 10 to 20 minutes under the UV lamp is all that is needed to do a reliable erasure. Therefore, further investigation into the authenticity of the components needed to be performed.

Researching the manufacturer's part markings

With the different date code markings, the topside date code part markings were researched to determine whether the markings were valid. According to a document published by the manufacturer, the products topside markings transitioned to include a new prefix and suffix in addition to the nine-character date code field effective on February 14, 2000.
The manufacturer's website decodes the eleven-character date code field of "A X□Z□□YYWWT":

A	=	Fab Process Identifier
X	=	Test site identifier
□	=	Based die identifier
Z	=	Die revision
□□	=	Fab process code
YY	=	Year
WW	=	Work Week
T	=	Internal Identifier

As shown in Figure 6, the parts in stock with date code of BHA070216 are not valid since the date code of 0216 is work week 16 of 2002 and the two additional characters are not included.

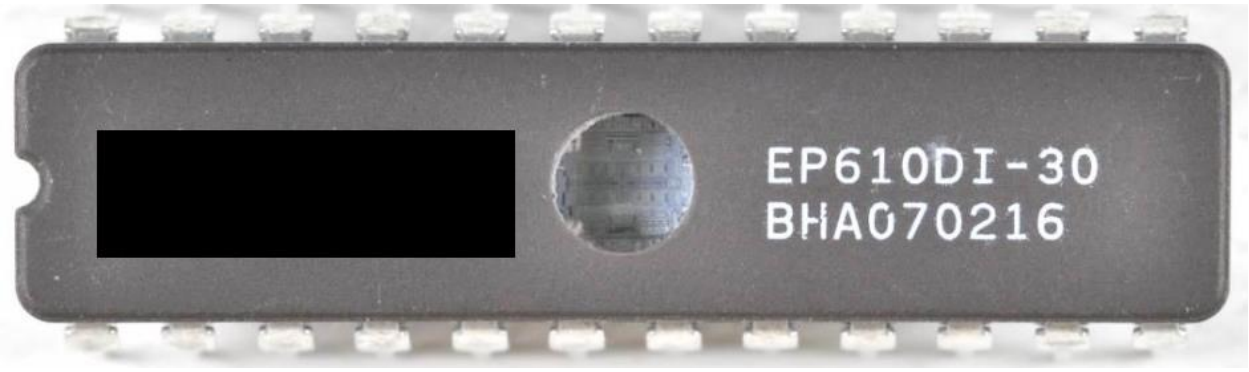


Figure 6: EP610DI-30 EPLD Part Markings

Informing management about the potential counterfeit part

Once the engineer has enough evidence that a part is suspect counterfeit, he/she must carefully inform his/her manager about the issue who works within company guidelines to inform the appropriate people to be included on the team, such as program management, upper management, mission assurance, supply chain management, customer contracts, and legal. Operations Program Management will perform a thorough investigation of where the suspect part is used. For the suspect EP610DI-30 component, the investigation uncovered an additional program specific part number that was used for another customer. Contracts personnel are involved in reviewing the contracts of all customers who are affected by receiving product that has a suspect counterfeit component. All cost associated with the investigation, control, and replacement is an unallowable expense to the business, so upper management oversight is necessary to secure necessary funds. Legal involvement is required to assure that the team is acting within the legal limits because knowingly providing products with counterfeit parts is unlawful and could result in fines and prison.

Once a component is considered suspect counterfeit, mission assurance shall quarantine all suspect counterfeit parts in a controlled access area to preclude their use. Supply chain involvement is necessary to review all purchase order history to determine what electronic components were purchased by the distributor(s) who provided the suspect counterfeit components. Also, supply chain management may decide to consult with the manufacturer or other subject matter experts. Supply chain management will solicit quotations and submit purchase orders in order to get the suspect counterfeit parts shipped to a reputable test service facility for further validation if confirmation cannot be determined by the original equipment manufacturer (OEM). Internal investigations will be conducted to determine the root cause, impact, and resolution.

Involving a third party to analyze and test for authenticity

An independent test service was contracted to analyze the authenticity of EP610DI-30 UV EPLD components. Visual inspection was performed on 100% of this lot. Several abnormalities were discovered. Inspection of the top surface found

that the package top and bottom ceramic pieces vary in color and texture. Initial inspection of the component bottom surface revealed no markings. As shown in Figure 7, several components were found to have surface alterations as well as the remains of prior markings, referred to as herein as 'ghost markings'. As shown in Figure 8, several EP610DI-30 components with date code BHA070216 had imperfections in the glass window indicating tampering. As shown in Figure 9, the scanning electron microscopy (SEM) indicated possible resurfacing and remarking. Additionally, visual inspection and x-ray analysis of the die through the package glass window revealed die to be different in size and shape.

Figure 7: Ghost Marking Appeared on Several EP610DI-30 with Date Code BHA070216

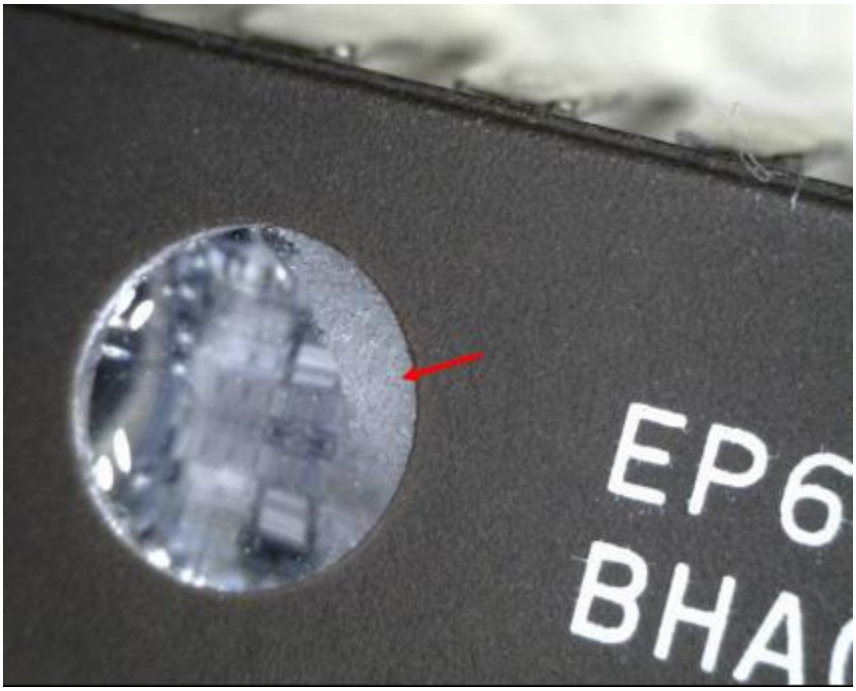


Figure 8: Imperfection in Glass Window on Several EP610DI-30 with Date Code BHA070216

Result	Indications of:
NO	Sandblasting
YES	Resurfacing
YES	Remarking

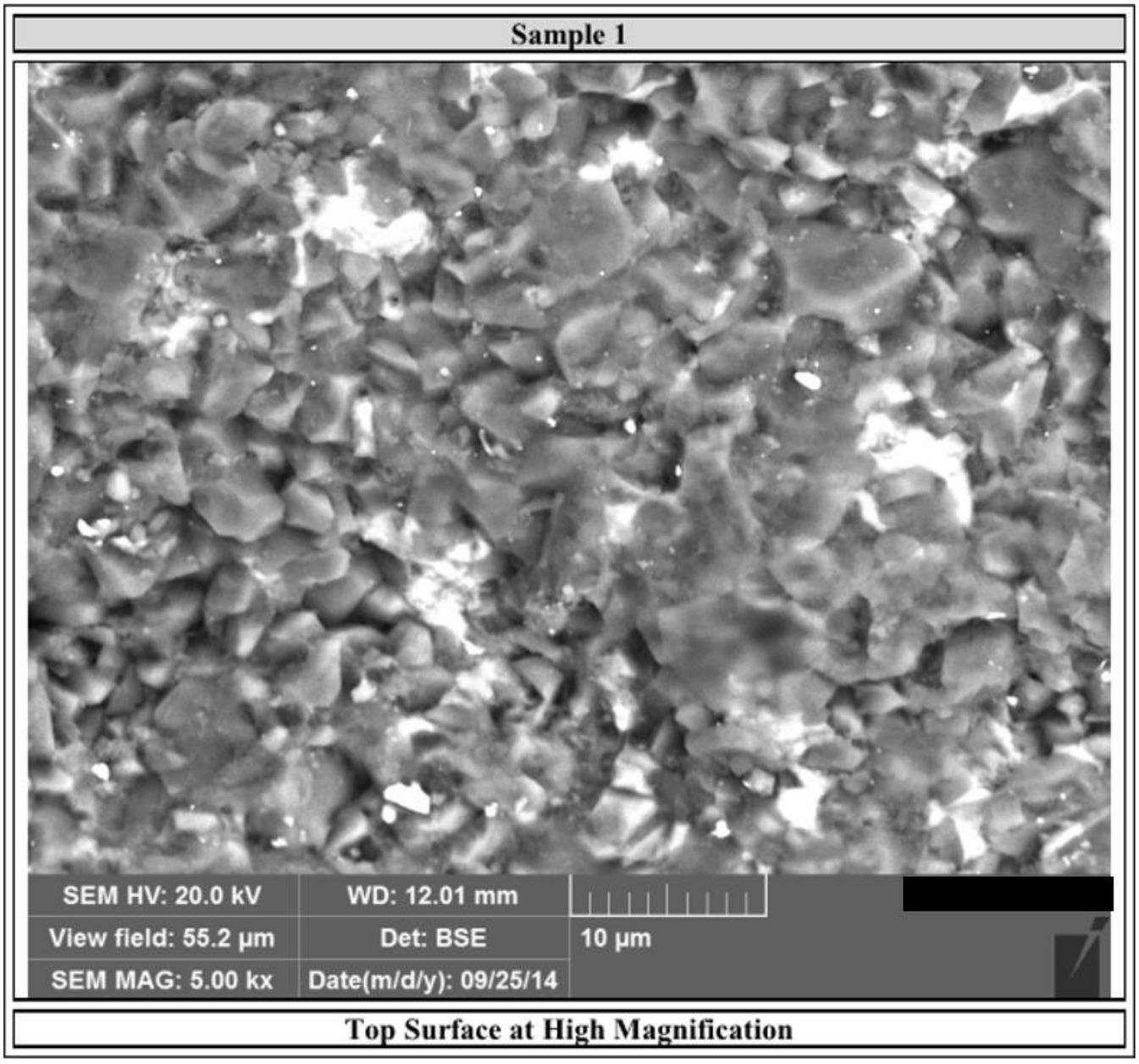
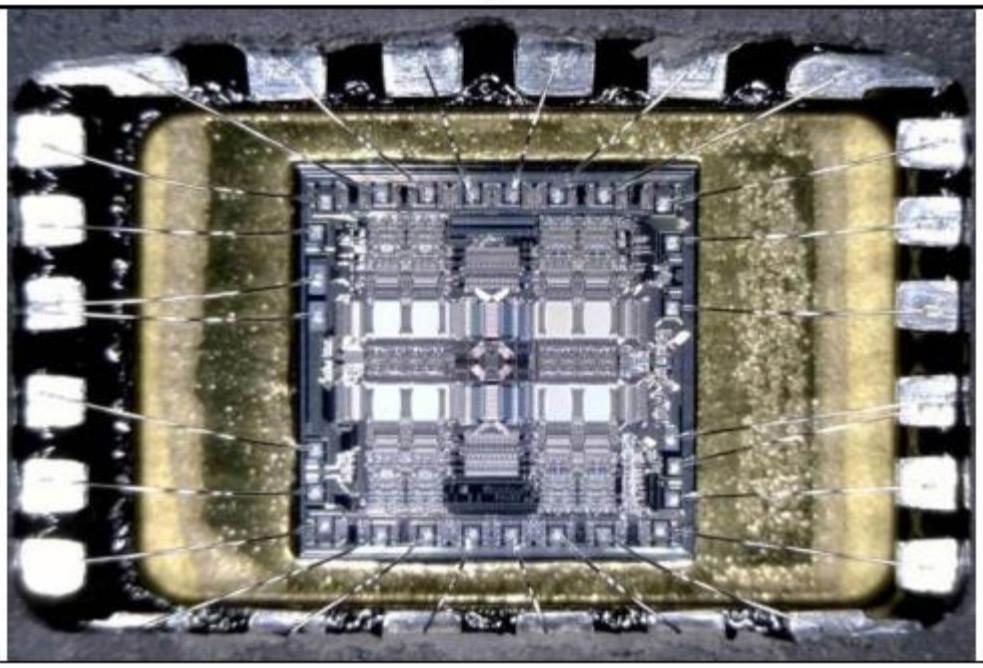


Figure 9: Scanning Electron Microscopy (SEM) Test of Date Code BHA070216

Three component samples were cut open (for Delidding and Die Microscopy) and the analysis indicated variations in die, lead frame, and die paddle/attach as shown in Figure 10. As shown in Figure 11, all three of the die samples revealed die marking from 3 separate manufacturing sites where one had "CNW62", the second had "WaferScale", and the third had "CNWA01A" marked on the die. As shown in Figure 12, samples 1 and 2 had a die developed year of 1987 while sample 3 had a die developed year of 1990. No die markings were found that could be verified against the manufacturer's part number. However, it is considered very unusual to have multiple die changes in the same date coded parts.

Sample 2



Sample 3

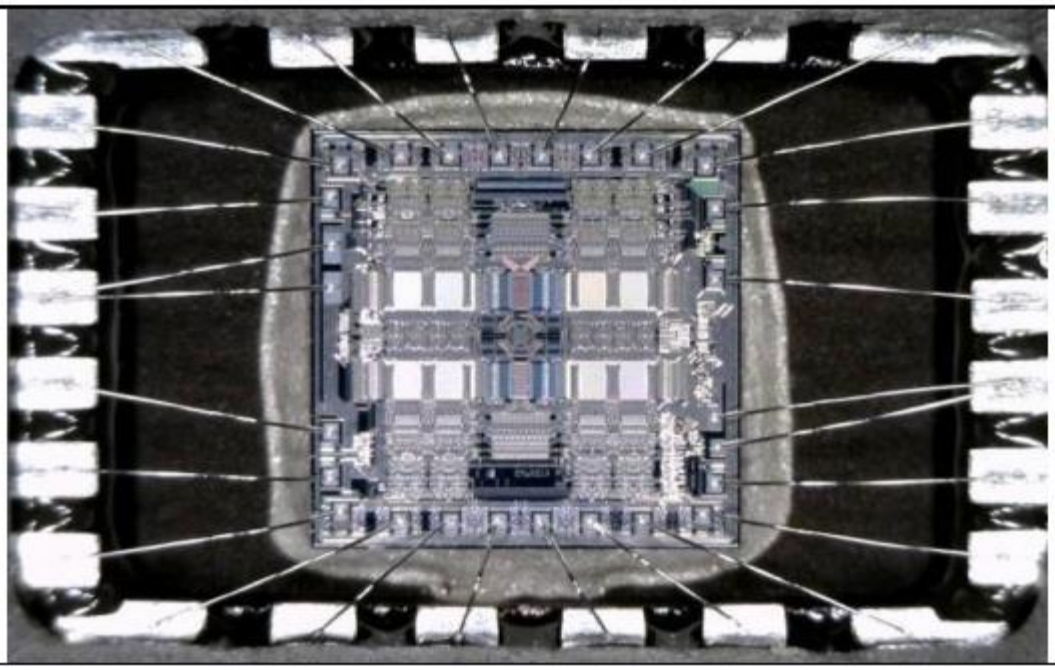


Figure 10: Different Die Paddle/Attach

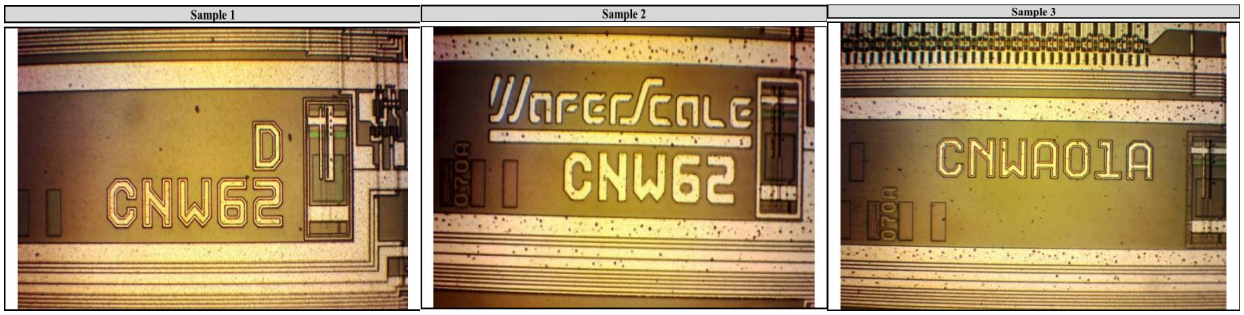


Figure 11: Die Marking Indicating Three Separate Manufacturing Locations

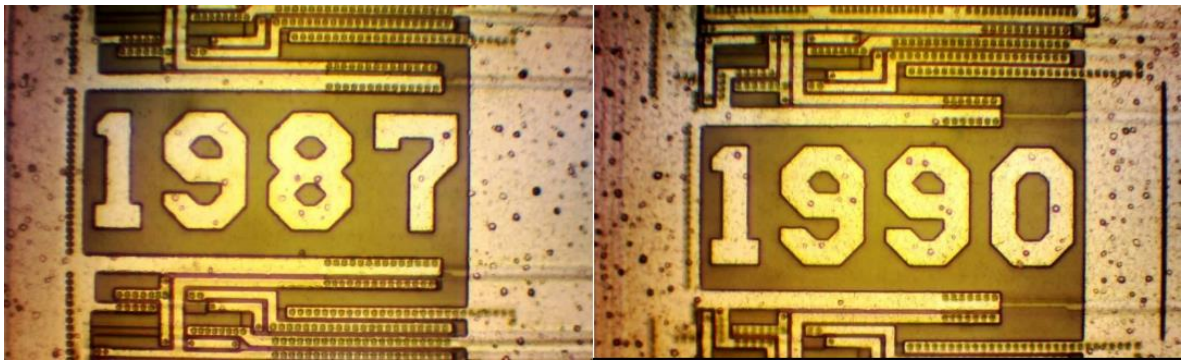


Figure 12: Different Die Year of Development

In summary as shown in Table 3, the EP610DI-30 UV EPLD components failed several of the authenticity tests. The reports found several items of concern with the three most significant issues being:

- The parts did not include any backside markings.
- The parts were not marked with the country of origin where the parts were assembled.
- The die size and markings had discrepancies within the same date code/lot code.

Table 3: Test Results by Independent Test Service

Analysis Performed	SMT Doc. ID	Sample Qty	Initials	Result
Visual Inspection	[W750-18]	81	MRD	FAIL
Real-Time X-Ray Analysis	[W750-15]	81	MRD	FAIL
Scanning Electron Microscopy (SEM) Analysis	[W750-12]	1	MRD	FAIL
Package Configuration and Dimensions	[W750-19]	3	MRD	PASS
XRF Elemental Analysis	[W750-16]	3	MRD	SEE SUMMARY
Resistance to Solvents (RTS) & Scrape Test	[W750-11]	3	MRD	PASS
Dye Penetrant	[W750-20]	N/A	N/A	N/A
Solderability Test	[W750-14]	N/A	N/A	N/A
Heated Solvent Test	[W750-09]	3	MRD	PASS
Delidding & Die Microscopy	[W750-10][-21][-22]	3	MRD	FAIL
Electrical Test		78		PENDING
Suspect Counterfeit			MRD	YES

The EP610DI-30 UV EPLD components were then sent to another independent test site for electrical testing where 70 of the 449 parts (approximately 15%) failed the electric parametric test which is a very high fall-out rate.

Expanding the team to address the issue with the customer and distributor

Upon receiving the results confirming the parts are suspect counterfeit from the independent test service, the team focused on researching the customer impact for any product that included the suspect counterfeit part. Thus, the team expanded to include reliability engineering to help with risk and safety assessments. Additional system tests were performed to determine the functionality and reliability of the suspect parts in the circuit. Thirty-two parts were randomly selected to undergo

accelerated life testing at 125ºC for 1000 hours while voltage and current going to the device were being monitored. Only 1 part showed a slight decrease in current draw during the test. After the accelerated life test, all 32 parts were then erased and reprogrammed. All 32 parts functioned properly when tested in a circuit indicating that many of the suspect counterfeit parts were reliable.

Detailed technical white papers were written for each customer affected by the suspect counterfeit component(s). The white paper included number of components in their possession, component test/inspection results and detailed risk analysis advising them on impacts to system performance in event of component failure. Making claims and accusations of fraud is taken very seriously and has legal ramifications, so additional legal representative oversight is required to review all written reports. Since the costs were unallowable (not chargeable to the customer, direct or indirect), upper management were highly engaged to assure careful due diligence. Fortunately, in this case, the component usage was not very high which greatly reduced the cost and exposure. After thorough reviews of all documentation, authorization was granted for communications with the customer who received some product with a suspect counterfeit component.

Detailed GIDEP reports were written against the distributors of the suspect counterfeit components. These GIDEP reports were thoroughly reviewed by management and legal to assure claims and statements were accurate. Each distributor with suspect counterfeit components was certified mailed a copy of the GIDEP report to allow them four weeks to respond prior to formal publish. Once the GIDEP reports were published, the distributors were blocked in the company's enterprise resource planning system (ERP), so supply chain managers cannot purchase or even request a quotation from these distributors for any electronic components.

Providing lessons learned and suggested future measures for avoidance

On January 5, 2011, a GIDEP report was received indicating EP610DI-30 components with date code of "Y BHB070211A" were suspect counterfeit. Mission Assurance searched inventory and was able to quarantine and purge all 320 parts from the distributer that had the date code of "Y BHB070211A". However, there were 655 EP610DI-30 components from the same distributer that had a different date code that remained in stock. Perhaps further scrutiny could have been performed to determine whether these other date code components were also suspect counterfeit. An investigation of the part marking by the manufacturer could have been made and then it may have become more obvious that the other EP610DI-30 components in stock were also suspect counterfeit. Although identifying counterfeit parts at incoming inspection can be difficult because counterfeiters are doing better jobs in marking and packaging the counterfeit parts, the incoming inspection drawings could include the latest manufacturer part markings, so the inspector can inspect the markings along with other visual anomalies (e.g. bent pins, poor markings, multiple date codes in same package, etc.). These suggestions are made to allow for better measures to be made in detecting suspect counterfeit as early as possible and not suggest specific policy changes or suggest that detection of suspect counterfeit parts can be caught in all cases.

Conclusions

Detecting counterfeit parts at incoming inspection is difficult because counterfeiters are doing better jobs in marking and packaging the counterfeit parts. This paper exhibited a method of identifying, elevating, and dealing with potential counterfeit parts. As discovered, the electrical parametric and accelerated life tests showed the difficulties of detecting suspect counterfeit parts because many of the parts functioned normally. Thus, the best approach to avoid receiving suspect counterfeit components is to use suppliers that are franchised by the original manufacturer with the express written authority including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. If parts can only be purchased by other distributors, extreme caution of verifying the component marking and testing the components must be taken to assure the components are authentic.

References

1. Department of Defense, Federal Register, Part IV, Vol. 79, No. 87 May 6, 2014, 48 CFR Parts 202, 231, 244, et. al. Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012–D055); Final Rule subsection 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System, subsection 246.870–2 Policy.
2. Rogowski, R. UK Electronics Alliance, UKEA Position on Counterfeit Electronic Components, RR/V2/03.03.2008 (2008).
3. Martin Goetz and Ramesh Varma, "Counterfeit Electronic Component Identification: A Case Study", SMT Magazine, July 2017 (Please indicate where Reference [4] is in the paper.
4. M. Tehranipoor, "Counterfeit Detection and Avoidance", September 24, 2014.

Acknowledgements

The author would like to thank John Early who reviewed the paper and provided further insight of the case example.

Identifying and Combatting Counterfeiters

Ed Laliberte

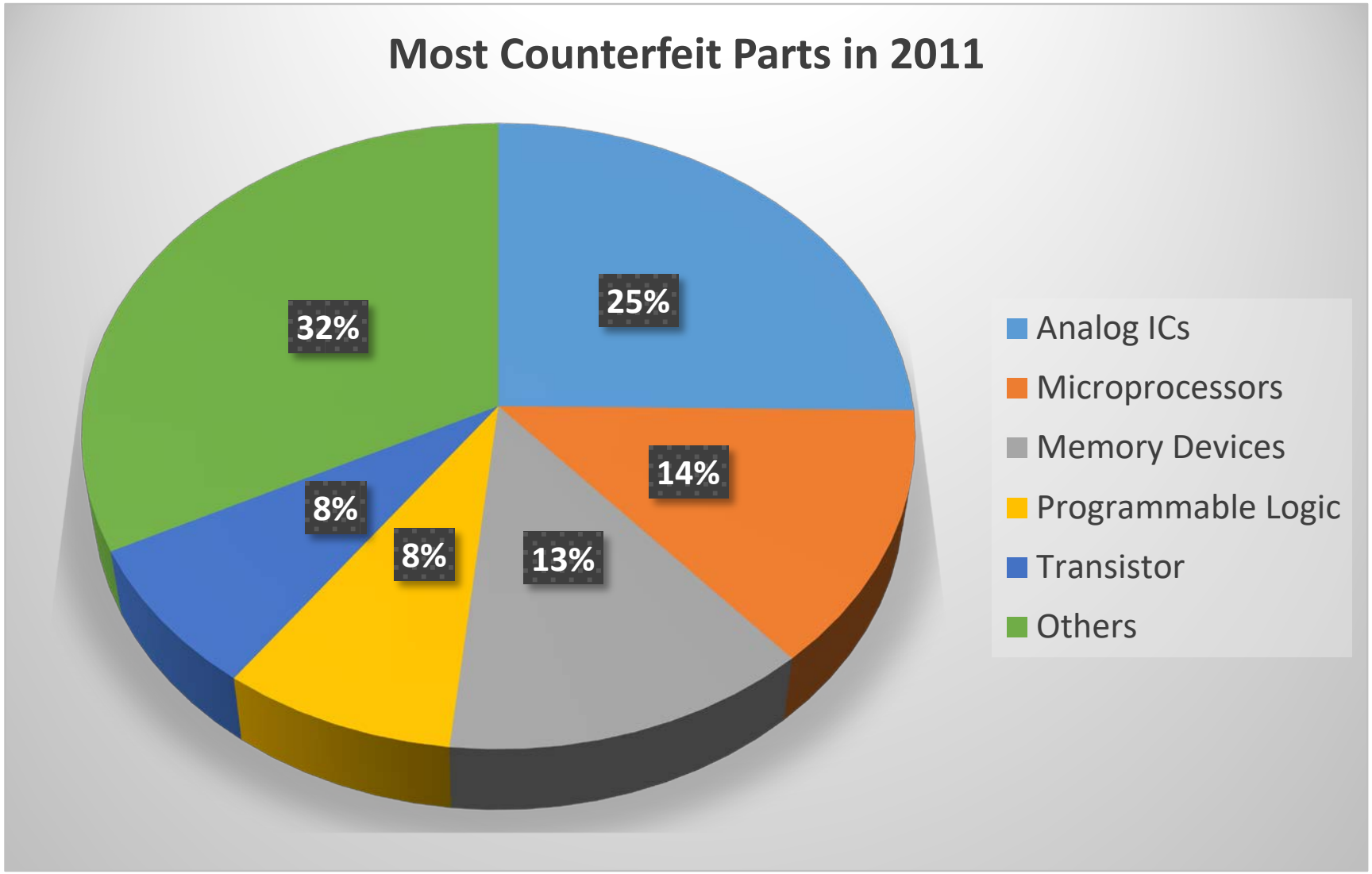
Northrop Grumman Systems Corporation

Counterfeiting Is No Laughing Matter

Counterfeiting Penalties Are Stiff

- An individual could be fined $2 million and face a jail term of up to 10 years, or both. A company will be fined $5 million. For a second offense an individual would be fined up to $5 million or imprisoned for up to 20 years, or both. A company will be fined up to $15 million.
- If a defective counterfeit part causes a personal injury or death, an individual found guilty of supplying the product will face a $5 million fine and up to 20 years in prison. A company will be fined up to $15 million.

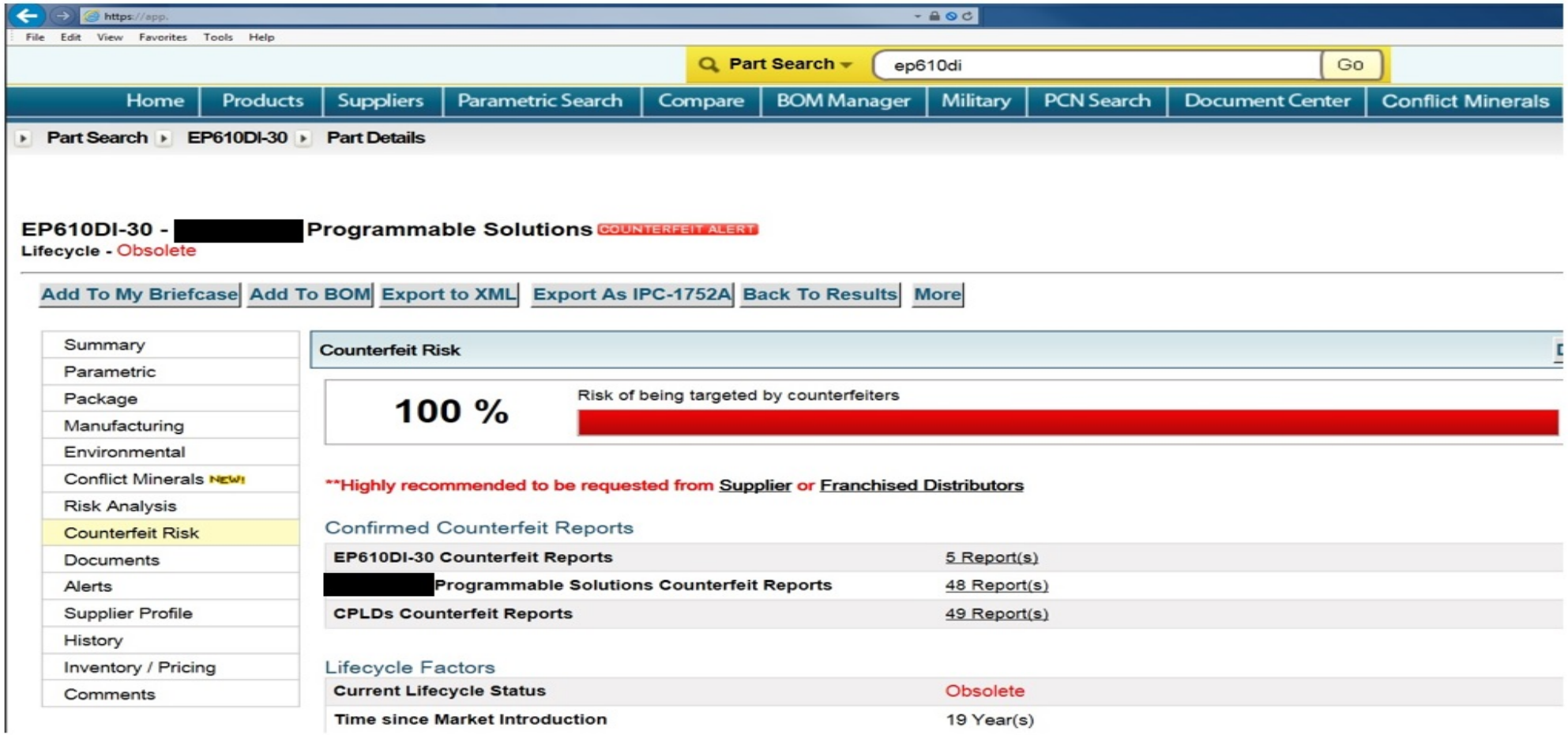
Breakdown of Counterfeit Parts Reported in 2011



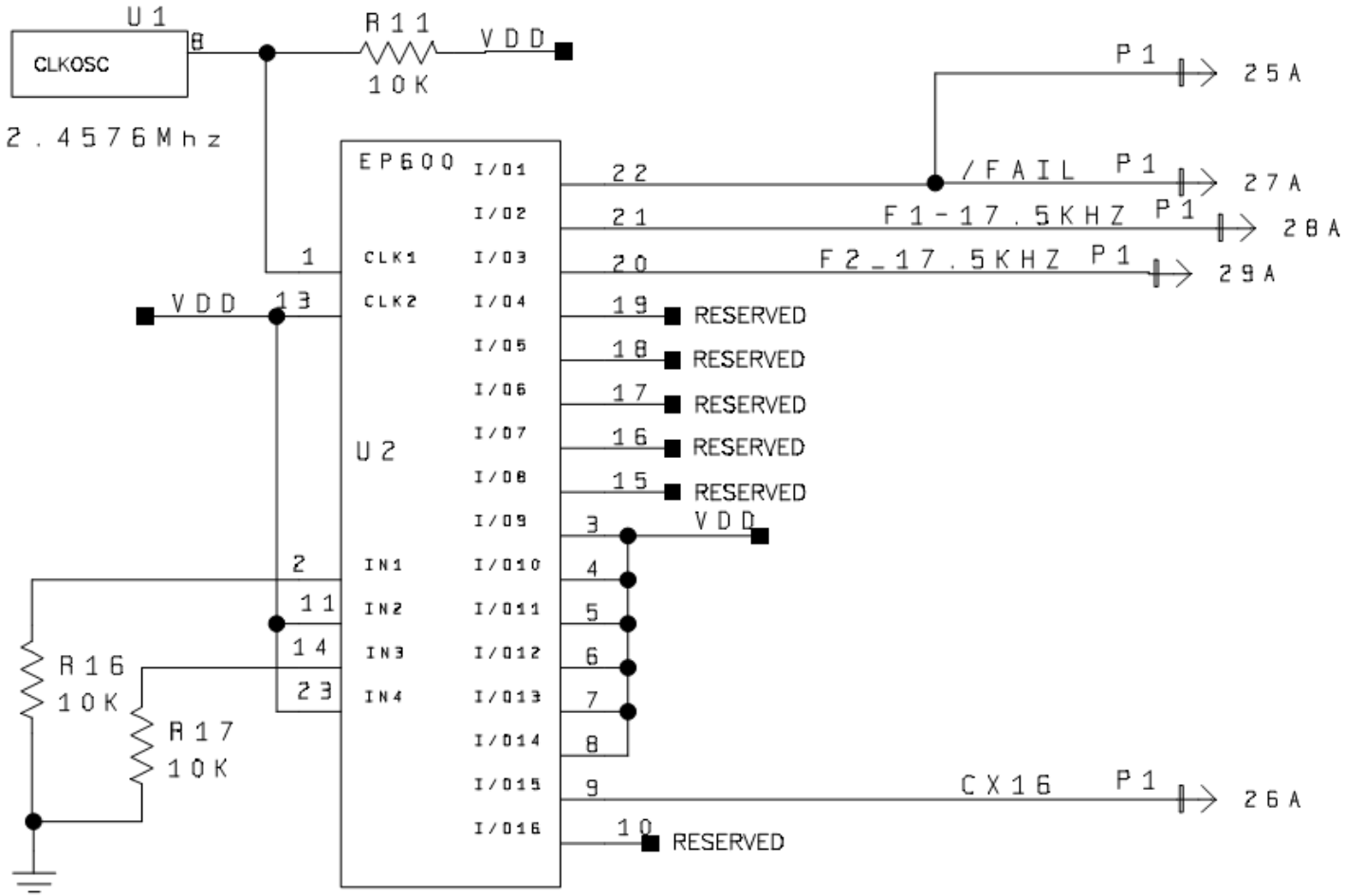
GIDEP Reports for EP610DI-30 Component

MPN	Notification Date	Counterfeit Methods	GIDEP Source
EP610DI-30	3-Jan-11	Different Supplier, New Parts (Third Party)	B7C-A-11-002
EP610DI-30	3-May-12	Different Supplier, Old Parts (Third Party)	B7C-A-11-002
EP610DI-30	30-Oct-14	Same Supplier, Old Parts (Third Party)	SP-A-15-01
EP610DI-30	11-Mar-15	Same Supplier, Old Parts (Third Party)	SP-A-15-02
EP610DI-30	15-Jul-15	Same Supplier, Old Parts (Third Party)	AAN-U-15-268

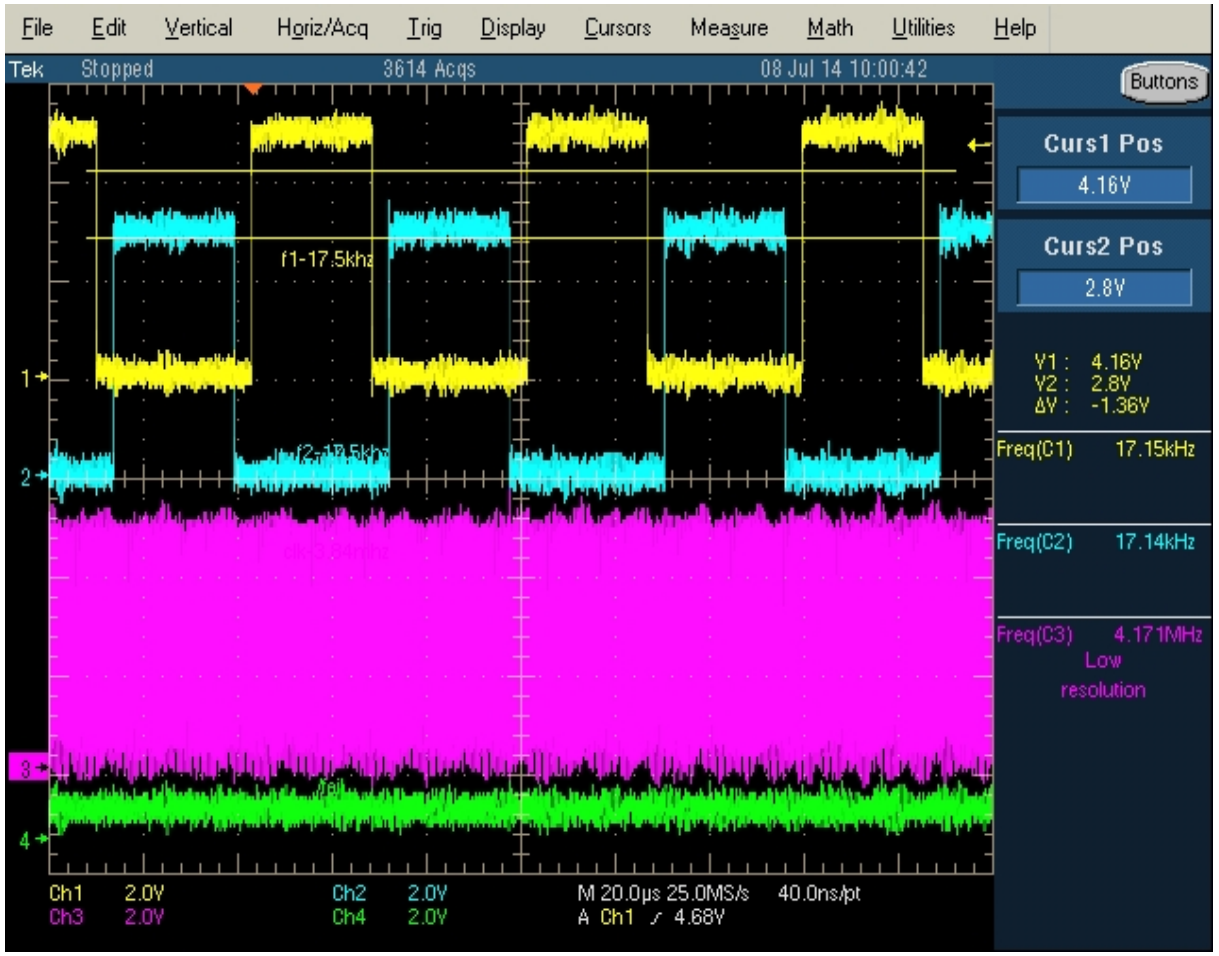
Counterfeit Risk Assessment for EP610DI-30 Component



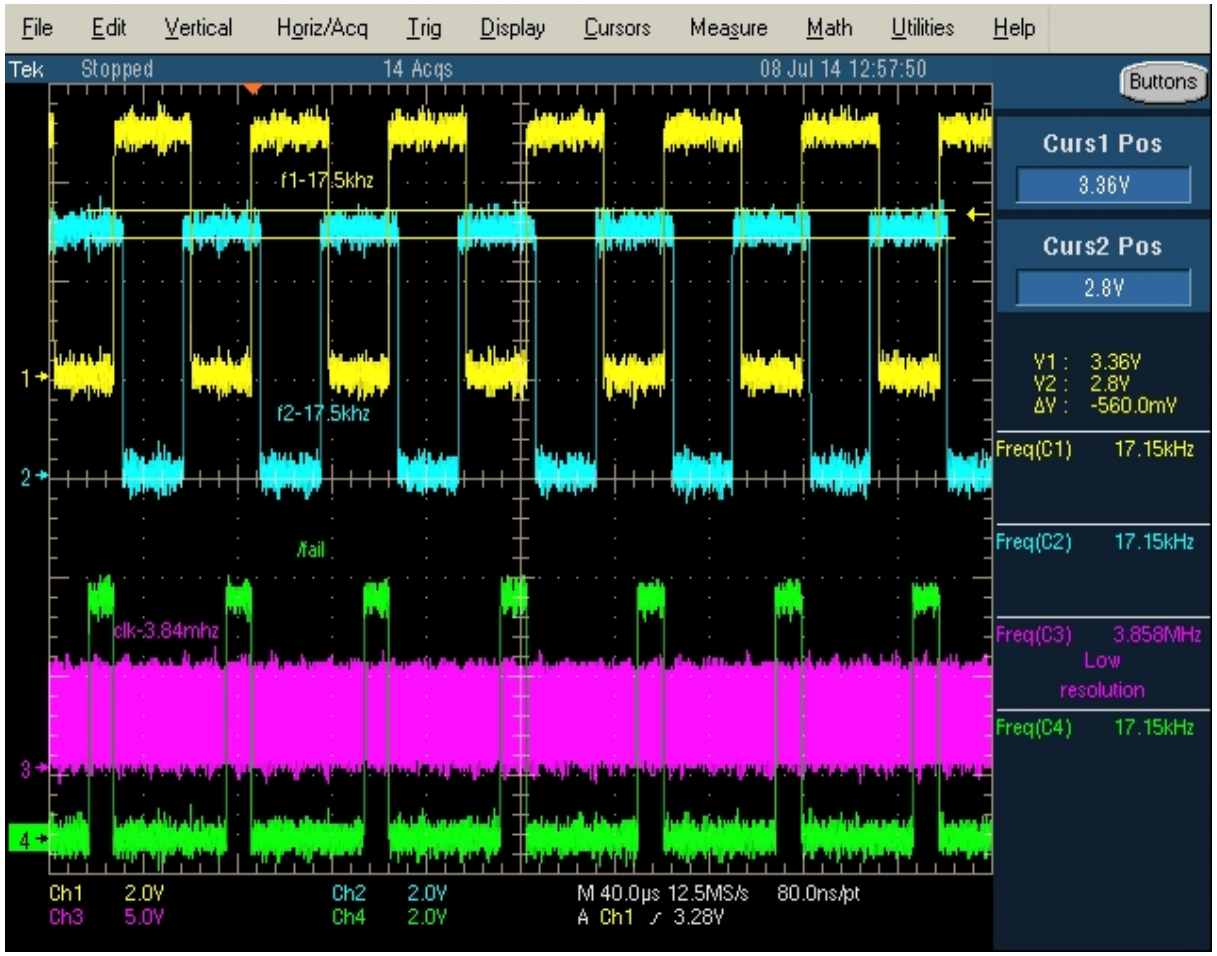
Basic Test Circuit



Comparing the Timing of EPLD Output Signals



KNOWN GOOD EPLD TIMING



EPLD TIMING FAILURE

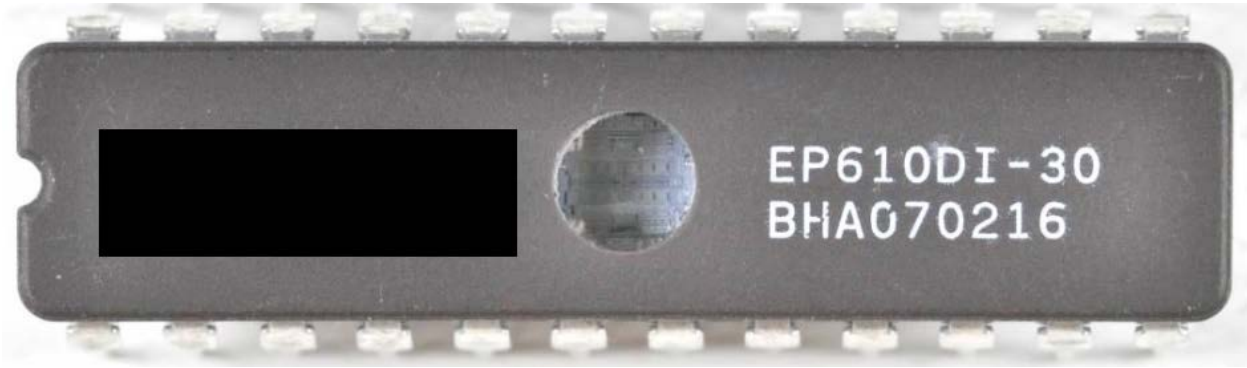
List of PCNs for EP610DI-30 Component

Type of Change	Description	Notification Date	Source
Vendor Acquisition	Company Y Completes Acquisition of Company T	28-Dec-15	News Release
Vendor Acquisition	Company Y Completes Acquisition of Company A	11-Dec-15	ADV1508
Labeling, Packing, Product Code, Vendor Acquisition	Company Y Completes Acquisition of Company M. Now all Company M products are sold and supported under Company Y name	29-Nov-13	ADV1314
Packing	Company M is implementing the shipment box dimension and desiccant count changes in an effort to streamline packing and logistics.	31-May-13	ADV1305
Vendor Acquisition	Company M Completes Acquisition of Company B	14-May-13	News Release
Assembly Site	Company M is expanding its manufacturing capacity at Company Ltd (Thailand) and second source Company Ltd2 (Malaysia) and third source Company Ltd3 (Taiwan).	30-Apr-13	ENP-PCN-2013-02
Labeling	Company M will be extending the maximum storage shelf life for all products from 18 months to 36 months.	17-Mar-11	ADV1101
Vendor Acquisition	Company M Completes Acquisition of Company H	14-Dec-10	News Release
Labeling, Packing	Company M will be extending the maximum storage shelf life for all products from 18 months to 36 months.	14-Dec-09	ADV0908 Rev 1.0.0
Packing, Labeling	Company M is implementing enhanced labels for the moisture barrier bag and inner box.	17-Sep-09	ADV0908 Rev 1.0.1
Obsolescence Notices	Company M discontinued some of products	13-Jul-06	PDN0605
Vendor Acquisition	Company M Completes Acquisition of Company G	8-May-00	News Release
Vendor Acquisition	Company M Completes Acquisition of Company F	1-May-00	News Release
Vendor Acquisition	Company M Completes Acquisition of Company E	11-Oct-99	News Release
Vendor Acquisition	Company M Completes Acquisition of Company D	1-Jun-99	News Release

Researching Manufacturer's Part Markings

Effective on February 14, 2000, the manufacturer changed their markings with an eleven-character lot code field of "A XbZaaYYWWT":

A	=	Fab Process Identifier
X	=	Test site identifier
b	=	Based die identifier
Z	=	Die revision
aa	=	Fab process code
YY	=	Year
WW	=	Work Week
T	=	Internal Identifier



As shown, the parts in stock with date code of BHA070216 are not valid since the date code of 0216 is work week 16 of 2002 and the two additional characters are not included.

Informing Management About the Potential Counterfeit Part

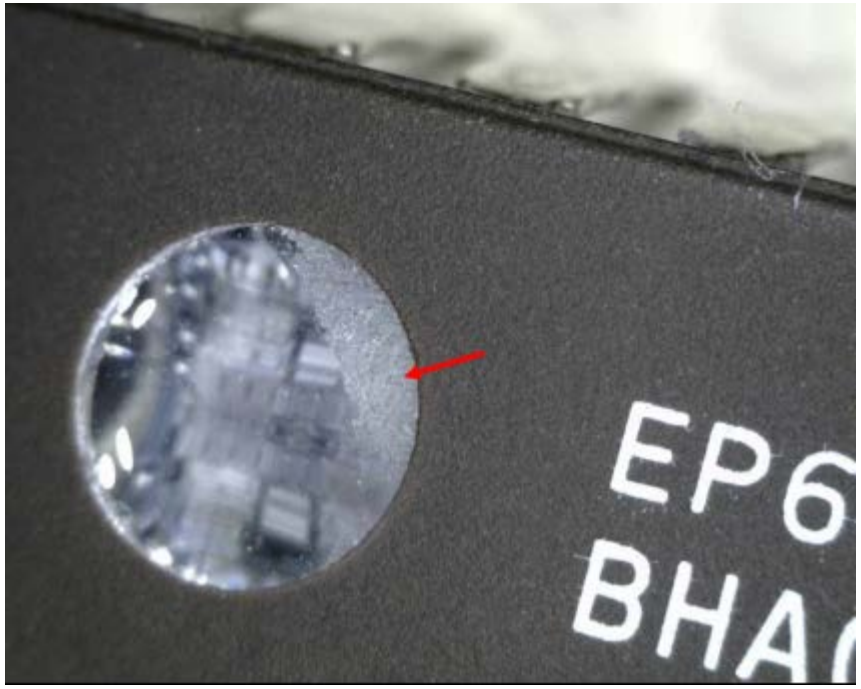
The manager will then inform the appropriate people to be included on the team to investigate the potential counterfeit component issue further. Team includes:

- Program Management
- Customer Contracts
- Upper Management
- Legal
- Mission Assurance
- Supply Chain Management

Involving a Third Party to Analyze and Test for Authenticity

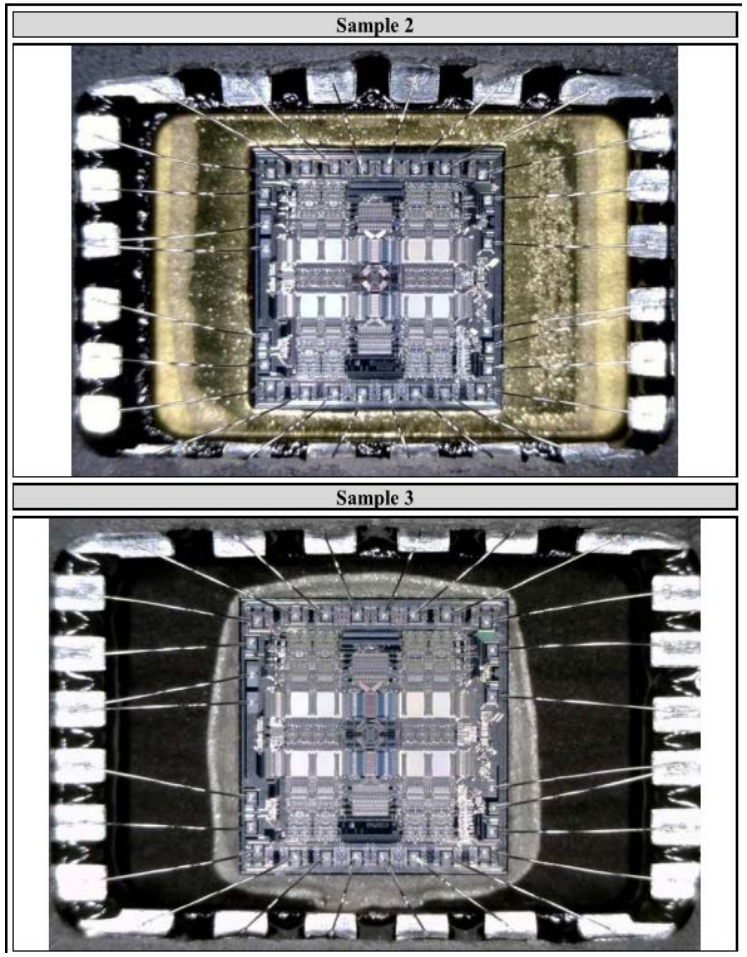
Visual inspection was performed on 100% of the potential counterfeit EP610DI-30 components with date code BHA070216 by an independent test service facility. The results showed some irregularities in the components.

Ghost marking appeared on several EP610DI-30 components.

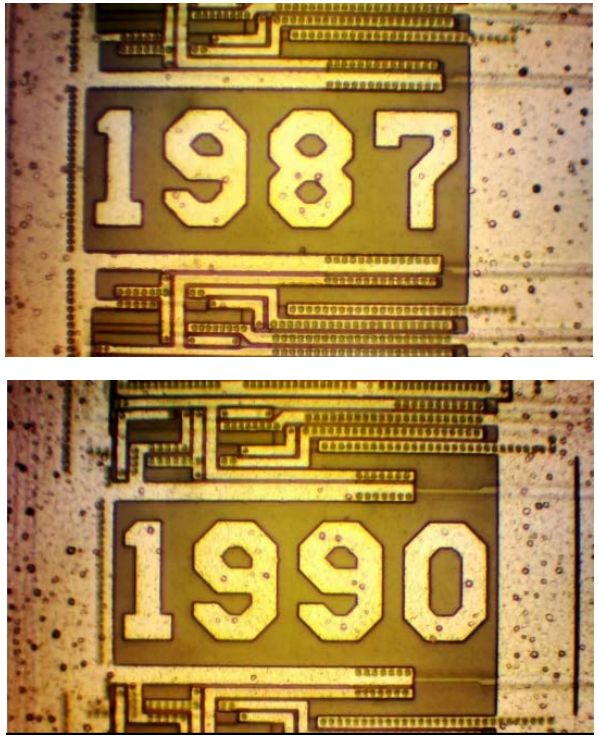


Imperfection in glass window was noticeable on several EP610DI-30 components.

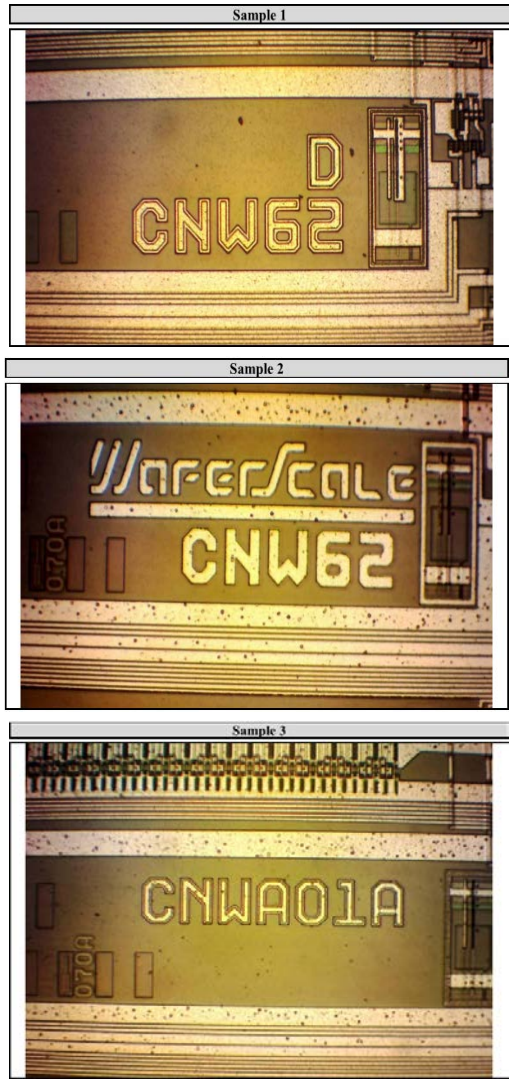
Delidding and Die Microscopy



Different Die Paddle/Attach



Different Die Year of Development



Different Die Manufacturing Locations

Test Results by Independent Test Service

Analysis Performed	SMT Doc. ID	Sample Qty	Initials	Result
Visual Inspection	[W750-18]	81	MRD	FAIL
Real-Time X-Ray Analysis	[W750-15]	81	MRD	FAIL
Scanning Electron Microscopy (SEM) Analysis	[W750-12]	1	MRD	FAIL
Package Configuration and Dimensions	[W750-19]	3	MRD	PASS
XRF Elemental Analysis	[W750-16]	3	MRD	SEE SUMMARY
Resistance to Solvents (RTS) & Scrape Test	[W750-11]	3	MRD	PASS
Dye Penetrant	[W750-20]	N/A	N/A	N/A
Solderability Test	[W750-14]	N/A	N/A	N/A
Heated Solvent Test	[W750-09]	3	MRD	PASS
Delidding & Die Microscopy	[W750-10][-21][-22]	3	MRD	FAIL
Electrical Test		78		PENDING
Suspect Counterfeit			MRD	YES

The EP610DI-30 UV EPLD components with lot code BHA070216 failed several of the authenticity tests.

Due Diligence on Researching the Customer Impact

The team expanded to include reliability engineering to help with risk and safety assessments.

- Additional system tests were performed to determine the functionality and reliability of the suspect parts in the circuit.
- Electric parametric test was performed by independent test site on all components.
- Accelerated life testing at 125^{o}C for 1000 hours was performed on thirty-two randomly selected components.
- Detailed technical white papers were written for each customer affected by the suspect counterfeit component(s).

The electrical parametric and accelerated life tests showed the difficulties of detecting the suspect counterfeit parts because many of the parts functioned normally.

Summary and Lessons Learned

This paper presentation exhibited a method of identifying, elevating, and dealing with potential counterfeit parts. The costs associated with dealing with counterfeit components are unallowable (not chargeable to the customer, direct or indirect), so having highly engaged upper management is necessary to assure careful due diligence. Lessons learned include:

- Detecting counterfeit parts at incoming inspection is difficult.
- Extreme care must be taken when verifying the component markings.
- The best approach to avoid receiving suspect counterfeit components is to use manufacturer's authorized suppliers.
- If parts can only be purchased by other distributors, testing the components must be done to assure they are authentic.

Detailed GIDEP reports were written against the distributors of the suspect counterfeit components. Once the GIDEP reports were published, the distributors were blocked in the company's enterprise resource planning system (ERP), so supply chain managers cannot purchase or even request a quotation from these distributors for any electronic component.