

# Avoiding Counterfeit Electronic Components – Part 2

## *Observations from Recent Counterfeit Detection Experiences*



Henry Livingston  
BAE Systems Electronic Warfare and Sensor Systems  
(603) 885-2360 | Henry.C.Livingston@baesystems.com

### INTRODUCTION

Earlier this year, the author published a paper on avoiding counterfeit electronic components [1]. A counterfeit electronic component is one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer.<sup>1</sup> Examples include:

- Parts remarked to disguise parts differing from those offered by the original part manufacturer (e.g., original manufacturer, country of origin, specified performance)
- Defective parts scrapped by the original part manufacturer
- Previously used parts salvaged from scrapped assemblies

BAE Systems issued twelve (12) GIDEP Alerts between 6 December 2006 and 7 May 2007 reporting suspect counterfeit electronic components. Summaries and supply chain analysis for these cases are shown in Appendix A. This paper presents observations by BAE Systems from these recent suspect counterfeit incidents and closes with conclusions from these observations.

### SUPPLY CHAIN OBSERVATIONS

A comprehensive review of the twelve (12) GIDEP Alerts issued by BAE Systems (see Appendix A) yields the following observations concerning the supply chain for these suspect counterfeit devices:

- All of these cases involve microelectronic or discrete semiconductor devices acquired from Independent Distributors<sup>ii</sup>.

---

<sup>1</sup> For the purpose of this paper, the author uses a definition developed by the U.S. Department of Energy, Office of Health, Safety and Security (see “S/CI-DI Process Guide,” <http://www.eh.doe.gov/sci/>, November 2004).

<sup>ii</sup> The Independent Distributors of Electronics Association published the following definition in IDEA-STD-1010-A:  
Independent Distributor: A distributor that purchases new excess inventories from end users with the intention to sell and redistribute back into the market. End users are typically original equipment manufacturers (OEMs) and contract manufacturers (CMs) at locations all over the world. Independent distributors subsequently sell (re-distribute) the new parts from these excess inventories to other OEMs and CMs to fulfill inventory shortages with hard-to-find, obsolete, and competitively priced parts. Independent distributors do not typically have limiting contractual agreements or obligations to the components manufacturers, therefore such distributors are referred to as independent distributors.

- As of the publication of this paper, the origin of these suspect counterfeits was not known. BAE Systems was not able to determine all suppliers involved for every case.
- The Independent Distributors involved in these cases could not produce certificates of conformance or acquisition traceability provided by the original manufacturer and all previous distributors.
- A total of sixteen (16) US based Independent Distributors were associated with the supply chain. Seven (7) out of these twelve (12) cases trace back to a total of ten (10) suppliers based in China.
- The devices exchanged hands several times before they were acquired by BAE Systems.
- The same unique part type can be obtained through several Independent Distributors, all exhibiting similar evidence of remarking, refurbishing or reclamation.

### COUNTERFEIT DETECTION OBSERVATIONS

*Industry and Government inspection and test methods are designed to verify the integrity of authentic parts ... not to detect counterfeits.*

When applying industry and government standard inspection and test methods, the user must make adjustments to detect various counterfeiting techniques.

While external visual inspection can detect anomalies, the magnification levels and failure criteria defined in industry and government standards may not detect indications of resurfacing and remarking, or termination refurbishing and reclamation.

Marking permanency methods can be effective for detecting parts with forged marking. Industry standard “resistance to solvents” test methods, however, may not be aggressive enough to detect indications of resurfacing and remarking.

Both destructive and non-destructive physical and materials analysis can be very effective in revealing suspect counterfeit devices. The sample sizes specified in industry and government standards, however, assume that samples are drawn from a set of devices from known inspection lots. If

part marking has been forged, however, a single lot/date code marked on counterfeit devices can disguise parts originating from multiple inspection lots, parts produced by multiple manufacturers, different revisions of the same part, or can include devices of completely different functions. Sample sizes for such physical and materials analysis must be large enough to account for this potential. Samples should also be selected to avoid cases where a reel of counterfeit components has been "salted" with genuine components placed at the beginning or end of a reel to mislead the purchaser. The user must make the appropriate adjustments to physical and materials analysis evaluation criteria in order to detect various forms of counterfeiting.

Electrical testing can help reveal suspect lots, but may not detect counterfeit parts without a test plan designed specifically for the device type under test. DC electrical tests are frequently used as a low cost and fast detection technique, but will not detect dynamic performance deviations at temperature extremes. While AC electrical and functional tests are most likely to reveal suspect product, testing of complex devices requires intimate knowledge of the original manufacturer's test protocols. In addition, electrical testing alone may not detect damage induced by inadequate handling and storage, termination refurbishing, or reclamation.

#### *Marking quality, legibility, conditions vary significantly*

Visual inspection of marking for correct and accurate content can provide conclusive evidence of suspect counterfeits. Observations based exclusively on marking quality, legibility, and conditions, however, may be misleading.

BAE Systems experience reveals that quality in device marking, marking legibility and overall marking conditions for both authentic and counterfeit product can vary significantly. BAE Systems has observed both "bad looking" authentic parts and "good looking" counterfeit parts with respect to marking on the device.

#### *Production records may not be available for older parts*

The older the parts are, the less likely production records exist to aid in authentication. Original component manufacturer data retention practices may limit access to production records for older parts. In a few cases discovered by BAE Systems, the original component manufacturer no longer had production records to support our investigations; in these cases, however, BAE Systems found other evidence sufficient to conclude the parts were suspect counterfeit.

#### *Documentation may not be authentic*

In one specific case, a test report was provided by the Independent Distributor as evidence that parts sold to BAE Systems were authentic and as evidence of traceability back to the original component manufacturer. Feedback from the original component manufacturer revealed, however, that this test report was not valid. BAE Systems sent a copy of this test

report to the original component manufacturer who, in turn, provided BAE Systems an example of an authentic test report for the specific device type. The manufacturer did not have test data for parts with the same date code as those sold to BAE Systems. BAE Systems, therefore, concluded that the original component manufacturer did not produce this specific product with the date code received. BAE Systems also observed extensive format and content inconsistencies between the authentic test report provided by the original component manufacturer and the test report provided by the Independent Distributor. The report provided by the Independent Distributor included a "Military Certification of Conformance" label; the original component manufacturer reported that this label and its content are not used on authentic test reports.

#### *Some parts acquired through Independent Distributors show evidence of multiple exposures to tests*

BAE Systems discovered a case where additional marking on the device indicated prior multiple exposures to electrical, mechanical or environmental tests. Without knowledge of the application of these tests or their specific conditions, BAE Systems was not able to judge the potential for damage to these devices or the effect of this previous testing on total product life expectancy.

In addition to acquisition traceability documentation, the user should consider requiring documentation from Independent Distributors that reports all tests performed throughout the supply chain back to the original manufacturer. This requirement should be considered by industry and government standards organizations for incorporation into existing standards and specifications governing the procurement of electronic components.

#### *Authentic perhaps, but where have they been? ...*

Many parts acquired from Independent Distributors may be authentic, but show evidence of poor storage and handling conditions, or evidence of termination refurbishing or reclamation. To ensure confidence that parts are of the same quality and reliability as when first shipped by the original component manufacturer, users should apply a suite of test and inspection protocols to eliminate infant mortality defects associated with handling and storage, and with termination refurbishing or reclamation. Users should also consider life testing as an option to obtain a high level of confidence of failure free performance and to produce test results needed to support an assembly/system level reliability assessment.

## CONCLUSION

The most effective approach to avoiding counterfeit electronic components is to purchase product directly from the original component manufacturer, or from a distributor, reseller or aftermarket supplier who is franchised or authorized by the original manufacturer.

While mitigation methods can reduce the risk of receiving counterfeit parts from Independent Distributors, there is no fail safe method. Individual methods may not definitively distinguish authentic parts, or detect damage induced by inadequate handling and storage, termination refurbishing, or reclamation. A suite of inspections and tests are necessary to detect counterfeits and eliminate infant mortality defects, and to establish high level of confidence of failure free performance and to support an assembly/system level reliability assessment.

### ACKNOWLEDGEMENTS

The author wishes to thank the Original Component Manufacturers who supported BAE Systems during these counterfeit part investigations. Many thanks to the following BAE Systems personnel for their contributions toward these counterfeit part investigations and the observations reported in this paper ...

- Scott A. Hatch, Component Engineering
- Bruce B. Tourtellot, Component Engineering
- North O. Leppert, Component Engineering
- Joseph R. McGrail, Failure Analysis Laboratory
- David D. Mastrogiovanni, Failure Analysis Laboratory

### REFERENCES

- [1] H. Livingston, "Avoiding Counterfeit Electronic Components", IEEE Transactions on Components and Packaging Technologies, Vol.30, Iss.1, pp.187-189, March 2007.

### APPENDIX A

#### SUSPECT COUNTERFEIT ELECTRONIC COMPONENTS REPORTED BY BAE SYSTEMS VIA THE GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (GIDEP)

Full details are available to GIDEP Participants. Others may apply for membership at the GIDEP Help Desk. Visit <http://www.gidep.org/> or call (951) 898-3207

#### Suspect Counterfeit Case Summaries

J5-A-07-01: Parts marked as Philips QML product with 2003 date code, but contained Intel die manufactured in 1980

J5-A-07-02: Parts marked as Analog Devices QML product, but markings were not consistent with standard Analog Devices markings for the device and device contained PMI die of a different function

J5-A-07-03: Parts marked as Cypress commercial product, but parts were salvaged from scrapped assemblies

J5-A-07-04: Parts marked as On Semiconductor commercial product, but On Semiconductor did not manufacture these parts

J5-A-07-05 & J5-A-07-07: Received parts marked as Seeq commercial product, but parts were salvaged from scrapped assemblies and remarked to appear as legitimate/unused product

J5-A-07-06: Parts marked as Philips QML product with 9852 date code, but Philips discontinued manufacture 31 December 1997

J5-A-07-08: Parts marked as National QML product, but major discrepancies in marking format and content, including date code and manufacturing location

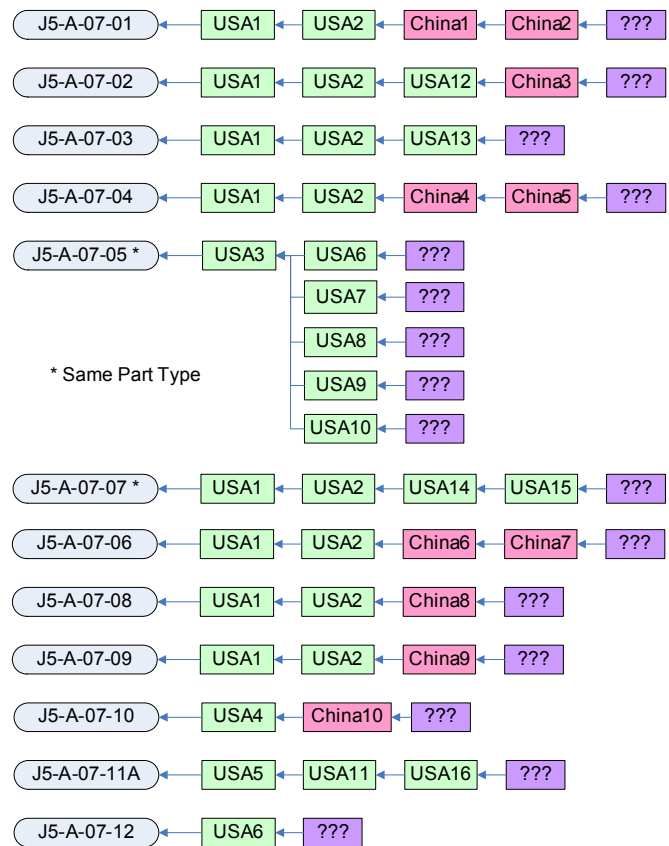
J5-A-07-09: 2001 date code, but Intersil discontinued this product in 2000; marking missing country of origin; parts had wrong lead finish

J5-A-07-10: 2004 date code, but Linear Tech discontinued this product in 2001

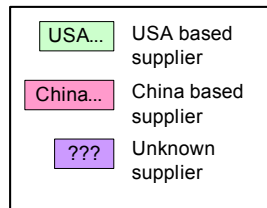
J5-A-07-11A: Parts marked as Analog Devices QML product, but incomplete or absent marking; incorrect lead finish vs part number; reclaimed or refurbished; invalid test report

J5-A-07-12: Part number and date code do not match the lot number identified in Cypress production records

#### Supply Chain Analysis



\* Same Part Type





**Henry Livingston** is a BAE SYSTEMS Engineering Fellow and presently manages Component Engineering at BAE SYSTEMS Electronic Warfare and Sensor Systems. He is Vice-Chairman of the Government Electronics & Information Technology Association (GEIA) G-12 Solid State Devices Committee and a member of the IEEE. The G-12 Committee develops solutions to technical problems in the application, standardization, and reliability of solid state devices. He has published papers on component reliability assessment methods, obsolescence management, and semiconductor industry trends.