

Open Forum

Avoiding Counterfeit Electronic Components

Henry Livingston, *Member, IEEE*

I. INTRODUCTION

A COUNTERFEIT electronic component is one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer.¹ 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.

Counterfeit electronic components can jeopardize the performance and reliability of electronics. Specific incidents of suspect counterfeit components reported by the Government-Industry Data Exchange Program (GIDEP) are listed in the Appendix.

Companies that do business in or acquire electronic components from emerging economies with under developed business and legal framework are especially vulnerable to electronic component counterfeiting due, in part, to poor enforcement of laws regarding counterfeiting and intellectual property theft [1]. In many of these countries, the electronics and semiconductor manufacturing infrastructure is developing at a faster pace than legal systems [2]. This increasing infrastructure provides an improved capability to produce counterfeits of higher value and more complex components.

Obsolescence of subsystems is a risk driver for defense electronics because they are intended for use over extended time leaving them vulnerable to obsolescence of the parts, subsystems, and technologies that comprise the system. A substantial number of components required to produce and support defense electronics are no longer available from the original component manufacturer or through their franchised or authorized suppliers. Independent distributors are often used to fill this gap. The purchaser, however, takes on risk when acquiring electronic components through distribution channels other than those franchised or authorized by the original component manufacturer.

While there is no fail safe method, this paper describes some approaches to help reduce the potential of acquiring counterfeit electronic components.

II. PURCHASING PRACTICES

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

Manuscript received February 8, 2007. This work was recommended for publication by Associate Editor M. G. Pecht upon evaluation of the reviewers' comments.

The author is with BAE Systems Electronic Warfare and Sensor Systems, Nashua, NH 03060 USA (e-mail: henry.c.livingston@baesystems.com).

Digital Object Identifier 10.1109/TCAPT.2007.893682

¹For 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).

who is franchised or authorized by the original manufacturer.² Original component manufacturers have their franchised or authorized distributors which include large and small businesses, including Small Disadvantaged Businesses. Franchise agreements typically include a number of provisions that protect the user by ensuring product integrity and traceability:

- original manufacturer warrantee;
- proper handling, storage and shipping procedures;
- failure analysis and corrective action support;
- certificates of conformance and acquisition traceability.

Independent distributors, however, do not have such agreements with the original component manufacturer and, therefore, have limited means to ensure product integrity and traceability [3]. Parts brokers, for example, frequently act as scouting agencies for hard-to-find components as the need arises, rather than maintaining an inventory [1].

When considering purchases through independent distributors, electronic equipment manufacturers and Government users need to employ risk mitigation methods and strategic approaches to reduce the potential for acquiring counterfeit parts.

- What are the steps to apply before considering the use of an independent distributor?
- What traceability documentation should the purchaser pursue?
- What compliance verification methods can be used?
- What are some strategic and proactive approaches to reduce the potential of acquiring counterfeit electronic components?

III. MITIGATION METHODS

The following mitigation methods can be applied to reduce the risk of receiving counterfeit electronic components when purchasing from an independent distributor.

A. Traceability Documentation

Without certificates of conformance and acquisition traceability, the purchaser takes on unknown risks. In addition to the independent distributor's own acquisition certification, the purchaser should seek certificates of conformance and acquisition traceability provided by the original component manufacturer and other distributors in the supply channel.³

While it is prudent to expect an independent distributor to provide these certificates of conformance and acquisition traceability, independent distributors often do not have this documentation; traceability to the original component manufacturer is lost or unavailable. An independent distributor's inability to provide certificates of conformance and acquisition traceability does not imply any wrong doing and does not necessarily indicate that products offered are non-compliant. The purchaser, however, takes on unknown levels of risk.

²Counterfeiting incidents involving authorized distributors have occurred, but reported cases are rare. RAM Enterprises, for example, is alleged to have stamped connector contacts with another manufacturer's logo and physically altered other electrical contacts to resemble contacts that had previously been approved by the government. See NASA Office of Inspector General (OIG) press release (2002) and U.S. District Court for the Central District of California, June 2002 Grand Jury Indictment (filed 2 August 2002).

³MIL-PRF-38535, General Specification for Integrated Circuits (Microcircuits) Manufacturing, includes requirements for certification of conformance and acquisition traceability provided by the original manufacturer and the manufacturer's authorized distributors. Similar requirements are included in MIL-PRF-19500, General Specification for Semiconductor Devices.

B. Compliance Verification

Compliance verification methods have been used with varying levels of success.⁴ Visual inspection, performed by individuals familiar with device marking requirements, can detect anomalies. Electrical testing can help reveal suspect lots.⁵ Both destructive and non-destructive physical analysis can also reveal suspect counterfeits.

These methods may not definitively distinguish authentic parts from counterfeits without comparison to known authentic examples or assistance from the original manufacturer.⁶ In addition, these methods may not reveal potential damage caused by improper handling and storage. Without knowledge and verification of the handling, storage and shipping procedures applied throughout the supply chain, the purchaser takes on the risk of acquiring damaged parts.

The purchaser should take care to ensure that components subjected to compliance verification are the same as those to be delivered. Cases have been reported where samples from parts offered by a broker were examined to verify authenticity prior to shipment, but the parts subsequently shipped by the broker were counterfeit.

IV. STRATEGIC AND PROACTIVE MEASURES

The following strategic and proactive measures can be applied to reduce the potential of acquiring counterfeit electronic components.

A. Independent Distributor Selection

One example of an industry standard that can be used for evaluating the suitability of an independent distributor is JEDEC Standard JESD31, General Requirements for Distributors of Commercial and Military Semiconductor Devices.⁷ JESD31 includes a number of provisions that protect the user by ensuring product integrity and traceability.

Another example, developed and published for the independent distribution supply channel, is IDEA-STD-1010-A, Acceptability of Electronic Components Distributed in the Open Market.⁸ IDEA-STD-1010-A includes a collection of visual acceptance requirements to indicate the quality of electronic components, and includes inspection techniques for counterfeit detection.

Independent distributor selection should include an assessment of their ability to verify the authenticity of the products they offer, particularly through traceability documentation. Some independent distributors outsource compliance verification such as the general techniques discussed earlier.

The independent distributor's purchasing and acceptance practices should also be considered. Some independent distributors subscribe to self-policing organizations with business practice standards intended to

⁴The GIDEP documents listed in the Appendix provide insight into techniques used to detect suspect counterfeit components.

Proceedings from recent industry symposia also include information on counterfeit detection techniques, such as the Counterfeit Components Detection and Prevention Symposium and Workshop (November 29–30, 2006) organized by the Components Technology Institute (<http://www.cti-us.com/>). The Independent Distributors of Electronics Association (IDEA) published a standard which includes inspection techniques for counterfeit detection: Acceptability of Electronic Components Distributed in the Open Market, IDEA-STD-1010-A, 2006. (<http://www.idofea.org>).

⁵The Defense Supply Center Columbus (DSCC) publishes a listing of DoD approved commercial laboratories who have demonstrated suitability to test to military specifications. http://www.dsccl.dla.mil/offices/Sourcing_and_Qualification/labsuit.asp.

⁶Some original component manufacturers will provide support to users who believe they may have received counterfeit parts. One example is Maxim Integrated Products (http://www.maxim-ic.com/sales/counterfeit_parts.cfm).

⁷JESD31, General Requirements for Distributors of Commercial and Military Semiconductor Devices", JEDEC Solid State Technology Association (<http://www.jedec.org>).

⁸IDEA-STD-1010-A, Acceptability of Electronic Components Distributed in the Open Market," Independent Distributors of Electronics Association (<http://www.idofea.org>).

avoid acquiring counterfeit goods. Other practices include the use of escrow services to hold the money until the independent distributor verifies the authenticity of products offered. In the absence of an escrow service, some independent distributors use of net one or net two-day payment where the seller ships the parts and the distributor has one or two days to inspect and accept them before the distributor releases payment [4].

Electronic equipment manufacturers and Government users should vet the independent distributor in advance of procurement activity to ensure suspect counterfeiting incidents have not occurred previously with this distributor and that the independent distributor has the financial means to support any contractual guarantees expected. Purchase agreements with independent distributors should include contractual remedies, such as product certifications along with financial penalties if found to be inaccurate.

B. Outsourcing Electronic Component Procurement

Some users outsource procurement to another entity, such as an Electronics Manufacturing Service (EMS) provider or Contract Manufacturer. The selection of an EMS provider or Contract Manufacturer should include audits of their purchasing methods to ensure their procurement practices mitigate the risk of their acquiring counterfeit parts [4]. The section on "Independent Distributor Selection" is also effective guidance when selecting an EMS provider or Contract Manufacturer.

C. Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management

A significant driver for the use of independent distributors is the continued need for parts that are no longer produced by the original manufacturer. In order to reduce the likelihood of having to purchase parts through an independent distributor, electronic equipment manufacturers should proactively manage the life cycle of their products, versus the life cycles of the parts used within them.

Traditionally, efforts to mitigate the effects of Diminishing Manufacturing Sources and Material Shortages (DMSMS) have been reactive. This reactive approach to DMSMS solutions leads to decisions that put a premium on faster solution paths with attractive short-term gains in order to avoid system inoperability. The long-term solution paths, however, would lead to solutions with the capability of avoiding future DMSMS issues. The building blocks of effective proactive management of DMSMS are established during the design and development of systems. If systems are designed with the inevitability of DMSMS in mind, early solution paths with large-scale solutions can be started at an appropriately early time to enable intelligent choices without the imminent threat of system inoperability. Such generic, large-scale solutions and a consensus on where DMSMS threats are most prevalent can be better forecasted by the use of a standard set of DMSMS management practices used by the foremost members of industry.

The Government Electronics and Information Technology Association (GEIA) G-12 Solid State Devices Committee developed a set of DMSMS management practices that can be used by original equipment manufacturers (OEMs) during the design and development of electronic systems to mitigate the effects of DMSMS: "GEB1, Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Practices"⁹ GEB1 includes proactive DMSMS mitigation methods, such as technology independence (e.g., use of VHDL, software portability), technology road mapping, technology insertion, planned system upgrades, life-cycle analysis and DMSMS monitoring. While proactive mitigation methods are the primary focus of the G-12 committee's work, GEB1 also addresses traditional responses to DMSMS events, such as alternate sourcing, redesign/design modification, and reverse engineering.

⁹"GEB1: Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Practices," Government Electronics and Information Technology Association (<http://www.geia.org>).

V. CONCLUSION

In today's supply chain environment, electronic equipment manufacturers and Government users must be vigilant in order to avoid counterfeit electronic components. The vast majority of counterfeit cases reported are associated with purchases through independent distributors.

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. Because many components needed to produce and support defense electronics are no longer in current production, independent distributors are often used to fill this gap.

While independent distributors provide a necessary function within the electronic component supply chain, they are not all created equal. Electronic equipment manufacturers and Government users need to understand the independent distributor's operations and business processes. When considering purchases through independent distributors, electronic equipment manufacturers and Government users should also apply mitigation methods and strategic approaches, such as those discussed in this paper, to reduce the potential for acquiring counterfeit parts.

APPENDIX

SUSPECT COUNTERFEIT ELECTRONIC COMPONENTS REPORTED BY 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.

A. Remarked to Disguise Parts Differing From Those Offered by the Manufacturer as Implied by the Marking . . .

- Parts marked as Linear Tech "mil temperature range" product with a 2001 date code, but analysis revealed that the original marking had been obliterated. Parts had been manufactured several years earlier (B8-A-03-01).
- Parts marked as TI QML product, but contained SGS-Thomson die (CE9-A-03-02A).
- Parts marked as TI QML product, but contained die of an older revision manufactured several years earlier than the date code marked (CE9-A-03-03).
- Parts marked as Cypress QML product, but contained MMI die (UL-A-03-01).
- Parts marked as TI "mil temperature range" parts, but contained MMI die (CE9-A-04-03).
- Parts marked as TI QML product, but was another TI QML product with different performance characteristics (RM5-P-04-01A).
- Parts marked as TI "mil temperature range" parts, but were commercial parts remarked to represent TI "mil temperature range" parts (T5-A-04-01).
- Parts marked as Atmel "mil temperature range" product, but markings were not consistent with standard Atmel markings for the device (VV-P-04-01).
- Parts marked as Analog Devices commercial product, but contained Signetics die (VV-A-04-02).
- Parts marked as Xicor QML product, but markings were not consistent with standard Xicor markings for the device (HO6-A-05-01).
- Parts marked as TI QML product with a 2004 date code, but the most recently manufactured date code was 200 (CE9-A-06-01).
- Parts marked as Rochester "mil temperature range" parts, but markings were not consistent with standard Rochester markings for the device (CS4-P-06-01).

- Parts marked as Maxim commercial product, but Maxim did not produce parts with the date codes marked (J5-A-06-01).
- Parts marked as Analog Devices "mil temperature range" product, but contained Linear Tech die (PD-A-06-01 and PD-A-06-02).
- Parts marked as Linear Tech QML product, but contained die of unknown origin (EE-A-06-01A, EE-A-06-04A, and EE-A-06-07B).
- Parts marked as Minco QML product with dual marking. Though traced to Minco as compliant product, Minco did not dual mark these parts (EE-A-06-02A).
- Parts marked as National QML product, but markings were not consistent with standard National markings for the device (EE-A-06-03A).
- Parts marked as Cypress commercial product, but markings were not consistent with standard Cypress markings for the device (EE-A-06-05A and EE-A-06-06B).
- Parts marked as Renesas commercial parts, but markings were not consistent with standard Renesas markings for the device (6E-P-07-01).
- Parts marked as GE QPL product with 1992 date code, but GE was not a qualified manufacturer after 1986 (M9-A-07-01 and M9-A-07-02).
- Parts marked as Samsung commercial product, but markings were not consistent with the date of the die inside the package (T9-P-07-01).
- Parts marked as Maxim commercial product, but contained Sipex die. (UY7-P-07-01A).
- Parts marked as Linear Tech "883" product with a 2001 date code, but contained PMI die. (CT5-A-07-01).
- Parts marked as Philips QML product with 2003 date code, but contained Intel die manufactured in 1980 (J5-A-07-01).

B. Defective Parts Scrapped by the Original Part Manufacture . . .

- Parts marked as Cypress commercial product, but failure analysis revealed numerous anomalies. Investigation revealed that these parts were scrapped by Cypress as screening failures and material rejects (6L-A-02-02A).
- Parts marked as Phillips commercial product, but contained no die. Investigation revealed that these parts were scrapped by Phillips as screening failures and material rejects (F8-A-05-01).

REFERENCES

- [1] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectrum*, vol. 43, no. 5, pp. 37-46, May 2006.
- [2] H. Livingston, "The Current State of the Semiconductor Industry and DoD Weapon System Dependence On 'Off-Shore' Products," Jul. 2004 [Online]. Available: <http://www.geia.org/index.asp?bid=587>
- [3] J. Stradley and D. Karraker, "The electronic part supply chain and risks of counterfeit parts in defense applications," *IEEE Trans. Compon. Packag. Technol.*, vol. 29, no. 3, pp. 703-705, Sep. 2006.
- [4] Design Chain Associates, LLC, "Counterfeit Electronic Component Resources," 2007 [Online]. Available: <http://www.designchainassociates.com/counterfeit.html>



Henry Livingston (M'00) has over 25 years of engineering and engineering management experience in the Defense and Aerospace Electronics industry. He presently manages Component Engineering at BAE SYSTEMS Electronic Warfare and Sensor Systems, Nashua, NH. He has published papers on component reliability assessment methods, obsolescence management, and semiconductor industry trends.

Mr. Livingston is Vice-Chairman of the Government Electronics and Information Technology Association (GEIA) G-12 Solid State Devices Committee (which develops solutions to technical problems in the application, standardization, and reliability of solid state devices).