Observations from Counterfeit Cases Reported Through The Government–Industry Data Exchange Program (GIDEP)

Henry Livingston, BAE Systems Electronic Systems

The Government–Industry Data Exchange Program (GIDEP) is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment.[1] GIDEP Failure Experience Data (FED) reports provide information about problems, potential problems and failure experience data on parts, components, materials, manufacturing processes, specifications, computer software, test equipment and safety. FED is exchanged to improve quality, reliability, and delivery schedules and to reduce costs. FED reports include "Alerts" and "Problem Advisories".[2]

BAE Systems reviewed all GIDEP Alerts and Problem Advisories on unlimited distribution[3] that document counterfeiting incidents over the past decade. This population of GIDEP reports consists of three-hundred-sixty-nine (369) reports discussing one or more counterfeit incidents.[4] BAE Systems offers the following facts and observations from the GIDEP reports.

Electronic components are the most frequent targets for counterfeiting

A recent study[5] conducted by the Department of Commerce, Bureau of Industry and Security (BIS) provides statistics on the extent of the infiltration of counterfeits into the U.S. defense and industrial supply chains. The data gathered for this study show that microelectronics comprised the vast majority of all reported counterfeit cases between 2005 and 2008[6].

Ninety-nine percent (99%) of the GIDEP reports concern counterfeit electronic components – microelectronics, passive components, relays, and magnetic components. Microelectronics (microcircuits and discrete semiconductors) comprise ninety-seven percent (97%).

Counterfeit parts find their way into the supply chain through Independent Distributors and "Brokers"

Categories of suppliers of electronic components include "Original Component Manufacturer (OCM)", "Authorized or Franchised Distributor", "Aftermarket Manufacturer", "Independent Distributor", or "Broker/Broker Distributor".[7] The BIS study[8] reveals that suppliers other than the original manufacturer or its authorized suppliers were identified as the primary sources of counterfeit electronic components. This study, however, did not quantify the number of counterfeit incidents associated with each category of supplier.

The specific supplier or category of supplier was identified within seventy-nine percent (79%) of the GIDEP reports.[9] In *all* of these instances, the supplier(s) associated with the sale of suspect counterfeit product was an "Independent Distributor", or "Broker/Broker Distributor".[10]

Despite the inspection and testing protocol applied by Independent Distributors and "Brokers", counterfeit products continue to escape detection

The BIS study[11] reveals that the most common methods of uncovering counterfeits were parts returned by customers as defective and the discovery of parts with poor performance. This finding indicates that despite the inspection and testing practices employed by suppliers other than the original manufacturer or its authorized suppliers, a significant risk remains that counterfeits may escape detection by these suppliers.

Within several of the GIDEP reports, the supplier of the suspect counterfeit (an Independent Distributor or broker) frequently describes themselves as a supplier in good standing by virtue of its quality system status and its membership in prominent industry organizations specializing in counterfeit avoidance best practices. Some GIDEP reports reveal that the supplier did not perform tests or inspections to intercept counterfeits. Many of the GIDEP reports, however, include the supplier's description of testing and inspection protocols applied with the expectation that counterfeit product would be detected. Despite the inspection and testing protocols applied by these Independent Distributors and brokers, counterfeit products escaped detection and were first identified to them by their customers.

Current industry and Government inspection and test methods are designed to verify the integrity and performance of authentic parts; not to detect counterfeits.[12] While adjustments to and combinations of these methods can detect suspect counterfeits, they are not foolproof. SAE standard AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, was developed for use by organizations that purchase electronic components, such as aerospace and defense equipment producers. In addition to other key elements of a robust counterfeit avoidance program, AS5553 includes a recommended suite of inspections and tests designed to detect counterfeit electronic components. This suite of inspections and tests includes low cost and expedient techniques that reveal easily detectable counterfeits, but also includes more rigorous, costly and time consuming methods to (a) detect more subtle variants of counterfeiting that can affect performance in the end use application and (b)

reveal defects from damage induced by inadequate handling and storage, termination refurbishing, or reclamation.

Close examination of the GIDEP reports reveals that the testing and inspection approach applied by the supplier did not include important methods described in AS5553, particularly the more rigorous, costly and time consuming methods that have greater potential to detect more subtle variants of counterfeiting that can affect performance in the end use application and defects from damage induced by inadequate handling and storage, termination refurbishing, or reclamation.

Techniques used in the counterfeiting industry are continuously advancing. Though counterfeit detection methods have been developed in recent years, counterfeiters continue to hone their craft to counter these methods. Examination of the GIDEP reports reveals that the supplier was not applying methods to counter newer and more advanced counterfeiting techniques discussed at various industry conferences, symposia and training programs available to Independent Distributors and brokers.[13]

CONCLUSION

Exposure to counterfeit products is an inherent aspect of supplies provided by sources other than the original manufacturer or its authorized suppliers. The most effective approach to avoiding counterfeit electronic components is to purchase electronic components, where possible, directly from the Original Component Manufacturer (OCM), its authorized distributors, or through suppliers that furnish electronic components acquired from the OCM or its authorized distributors. When purchases from sources of supply other than the OCM and its authorized distribution chain are necessary, due diligence must be performed to avoid counterfeits, including an assessment of supply chain traceability information associated with the product, risk mitigation associated with the end use application of the product, and inspections and tests specifically designed to detect and intercept counterfeits.[14]

ACKNOWLEDGMENTS

The author wishes to thank Mr. James Stein, Defense Standardization Program Office and Program Manager of GIDEP, for his assistance during this study, and to thank the many GIDEP members that contributed reports documenting counterfeiting incidents. The sharing of such high quality and timely information through GIDEP is an excellent example of partnership necessary to keep U.S. Government and Industry stakeholders informed of the counterfeiting problem and to provide critical information necessary to manage the problem more effectively.

Henry Livingston is an Engineering Fellow and Technical Director at BAE Systems Electronic Systems. He leads and supports a number of BAE Systems activities associated with specifying components and evaluating their suitability for military and aerospace applications. Henry has published papers on component reliability assessment methods, obsolescence management, semiconductor industry trends and counterfeit electronic components. Henry Livingston was recognized at the DMSMS and Standardization 2009 Conference for his leadership role in the detection, mitigation and reporting on burgeoning problem of counterfeit parts with the government and industry.

REFERENCES

[1] Government–Industry Data Exchange Program (GIDEP), http://www.gidep.org/

[2] A GIDEP "Alert" reports a problem with parts, components, materials, specifications, software, facilities, manufacturing processes or test equipment that can cause a functional failure. A GIDEP "Problem Advisory" reports a problem with parts, components, materials, manufacturing processes, specifications software, manufacturing processes or test equipment that has an unknown or low probability of causing problems for other users.

[3] Some GIDEP reports are not accessible to Industry members, such as "Limited distribution Agency Action Notices". BAE Systems is an Industry member of GIDEP and, therefore, this analysis does not include these reports. Pursuing sourcing data and other information for counterfeit instances described within such reports will require research by GIDEP and the assistance of agencies originating these reports.

[4] The oldest report reviewed was published 18 April 2002; the most recent report reviewed was published 1 September 2011.

[5] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010. pp.166–172.

[6] Supplementary data furnished by the Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation.

[7] Refer to "GIDEP Interim Policy Change for Reporting Suspect Counterfeits" dated 15 September 2010, and definitions within SAE standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.

[8] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010. pp.177–178.

[9] Twenty percent (20%) of the GIDEP reports were issued by a testing services organization. According to these reports, this organization did not know who the supplier was. Pursuing sourcing data for the parts described within these reports will require the assistance of this organization and its customers. The remaining one percent (1%) of the GIDEP reports do not identify the specific supplier or type of supplier.

[10] One GIDEP report published in 2011 describes a counterfeit part incident concerning a supplier that is an overseas business unit of a large electronic component distributor. Though its parent company is an authorized distributor for many products, this overseas business unit is an Independent Distributor.

[11] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010. pp.175– 176.

[12] "Avoiding Counterfeit Electronic Components – Part 2 Observations from Recent Counterfeit Detection Experiences", BAE Systems, May 2007.

[13] Examples include:
"Engineered Blacktop Material Analysis", SMT Corporation, August 2009.
"Counterfeit Components Avoidance Workshop", Components Technology Institute, Inc., August 2010.
"Counterfeit Parts Avoidance Training for EEE Parts", Jet Propulsion Laboratory, June 2011.
"Electrical Test Methods for Counterfeit Device Avoidance", Integra Technologies LLC, DMSMS & Standardization 2011 Conference, September 2011.
"The Latest Counterfeit Processes are Beginning to Move Away From the Traditional Methods and These Will Prove Much More Challenging to Detect", SMT Corporation, DMSMS & Standardization 2011 Conference, September 2011.
"Manufactured Counterfeits", American Electronic Resource Inc., DMSMS & Standardization 2011 Conference September 2011.

[14] "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components – Recommendations on Policies and Implementation Strategy", BAE Systems, October 2010.