DETECTION & AVOIDANCE OF COUNTERFEIT COMPONENTS

Understanding Inspection Test & Authentication Methods
Counterfeit electronic parts continue to pose one of the greatest threats plaguing printed circuit board assembly. With the constant consolidation of suppliers within the semiconductor industry and the increased regulatory pressure to assure authenticity, the Department of Defense issued new DFARS regulations in 2016. These regulations further expanded on the detection and avoidance policy for counterfeit electronic parts. Understanding the differences in the Inspection Test & Authentication (IT&A) methods available is critical to aligning your company’s overall risk mitigation strategy and compliance.

**BACKGROUND**

Many factors of the rise in global supply chain challenges are linked to obsolete and counterfeit components. With aging military technologies and obsolete parts no longer available from OEMs, the door has been opened for counterfeits.

Data from a survey¹ requisitioned by the U.S. Department of Navy, Naval Air Systems Command (NAVAIR) revealed that 39 percent of the companies and organizations participating in the survey encountered counterfeit electronics during the four-year period that the survey data was collected.

The report points to “demonstrated weaknesses in inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols, and communication within and across all industry and government organizations” that have led to the increase of counterfeit parts in the supply chain.
On August 2, 2016, the US Department of Defense (DoD) issued a Final Rule that “further advances” DoD’s ongoing effort to eradicate the dangers of counterfeit electronic parts from the DoD supply chain. The Final Rule creates a new DoD Federal Acquisition Regulation Supplement (DFARS) clause, 252.246.7008, which requires that contractors source electronic parts from one of three categories.

**Category 1** Original Manufacturers (OEM)
**Category 2** Contractor Approved Suppliers (CAS)
**Category 3** Appropriate Inspection Test & Authentication (IT&A)

This requirement applies to all contracts involving the sourcing of electronics, including contracts with small businesses and commercial item contracts. The term “trusted supplier” is no longer an acceptable term with regards to risk mitigation of the supply chain.

**Suspect Components Identified Through Testing**

Devices were provided for risk mitigation of suspect counterfeit parts. IEC Analysis & Testing Lab conducted non-destructive and destructive tests which identified a false lid. IEC confirmed the suspect counterfeit parts and minimized the supply chain risk for the customer.
SELECTING SUPPLIERS FOR YOUR SUPPLY CHAIN

The DFARS does give some guidance on how to define, select, and approve suppliers to ensure compliance. Below is a high level summary of the three steps.

**STEP 1**
Obtain electronic parts that are in production from the original manufacturer (OEM) or authorized aftermarket manufacturer. This includes suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers.

**STEP 2**
If electronic parts are not available from the original manufacturer, parts can be obtained from a Contractor Approved Supplier (CAS). For identifying and approving a Contractor Approved Supplier, the contractor should use established counterfeit prevention industry standards and processes (including Inspection Test & Authentication (IT&A) methods), such as the DoD adopted standards.

**STEP 3**
If an electronic part can not be sourced from the first two steps, the contractor must provide notification and be responsible for inspection, testing, and authentication in accordance with existing applicable industry standards. The contractor must have documentation available to the Government upon request.
NOT ALL STANDARDS AND TESTING METHODS ARE CREATED EQUAL

The Inspection Test & Authentication (IT&A) methods to be followed for electronic part testing is dependent on the industry standard that is selected. There are a wide variety of standards that cover general inspection methods, guidance on counterfeit policies, and advanced testing methods on how to test a part for authenticity. Some common sources of standards include the Independent Distributors of Electronics Association (IDEA), JEDEC, IPC, SAE International, and the Defense Logistics Agency (DLA).

Each standard defines their own criteria for sampling quantities, non-destructive and destructive tests as well as references other accreditations, certifications, and suitability requirements. Not all IT&A methods are the same in terms of the detail and rigor provided to ensure due diligence is performed.

The graphic to the left shows a comparison of some common standards, comparing their level of complexity regarding test methods and procedures. For example, IDEA 1010 outlines some basic testing methods for determining authenticity whereas the DLA Military Standards contain four times the amount of recommended tests, including advanced methods such as Scanning Electron Microscopy (SEM) and Fourier transform infrared spectroscopy (FTIR).
Confidence of authenticity increases as more testing procedures are performed on a greater sample of devices. However, with additional testing comes an increase in time and expenditure needed to validate parts. Balancing acceptable risk with schedule and investment should be based on your end-use application. It is important to work with an experienced lab that has not only the suitability to test across the spectrum of standards, but can also provide guidance distinguishing the differences between each testing method to select the ideal method based on your specific application.

It is important to note that DFARS 252.246.7008 does not specify which Inspection Test & Authentication (IT&A) methods must be followed. However, the Department of Defense (DoD) has defined its own program with the Defense Logistics Agency (DLA) regarding a Qualified Testing Suppliers List (QTSL). The purpose of the QTSL program is to establish and maintain a list of pre-qualified sources for certain electronics components that are purchased and managed by the DLA. Only labs on this list can perform military standard testing on components for the DOD. Suppliers on this list have demonstrated through external audit acceptable counterfeit mitigation practices and quality assurance procedures that are consistent with industry standards.
RISK MITIGATION FOR YOUR SUPPLY CHAIN

Understanding the DFARS is one of the first steps in developing a risk mitigation strategy for your supply chain. Your supply chain partners are an integral part to your compliance and more importantly, the quality of the products being manufactured. Having a robust supplier qualification process as well as being knowledgeable about the various testing standards will allow you to assess their capabilities with more confidence, especially when dealing with products that have obsolete or end of life parts.

IEC Electronics is the only Electronics Manufacturing Service (EMS) provider with an on-site testing laboratory approved by the DLA for their QTSL program. The Analysis & Testing Lab at IEC conducts exhaustive testing using destructive and non-destructive testing methods, including enhanced destructive physical analysis (DPA) testing per DLA Military Standards such as MIL-STD-1580 and upscreening per MIL-STD-202. IEC’s team of experts can develop and execute a custom risk mitigation plan for your supply chain, ranging from individual part screening to full system assembly manufacturing.

Delidding/Decapsulation Performed to SAE AS6171 Standards

Example of destructive physical analysis conducted in the DLA approved Analysis and Test Laboratory at IEC Electronics utilizing SAE AS6171/4 - Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation in order to examine the internal structure and to determine if the part is suspect counterfeit.
The DFARS continue to evolve as the risk of counterfeit components increases within the electronic parts supply chain. The introduction of the requirement of contractors to justify their Inspection Test & Authentication (IT&A) process has highlighted that not all standards are created equal and it is important to understand how the standard selected could cause potential liabilities to the company in the future. Utilizing a supply chain partner who is knowledgeable in this area can minimize supply chain risk by providing expertise to help define how to detect and avoid counterfeit electronic parts in your supply chain.

For more information about IEC Electronics, please contact us at:
www.iec-electronics.com
info@iec-electronics.com
(505) 345-5591

Sources: