Detection & Avoidance of Counterfeit Components:
Understanding Inspection Test & Authentication Methods
Detection & Avoidance of Counterfeit Components: Understanding Inspection Test & Authentication Methods

With the constant consolidation of suppliers within the semi-conductor industry and the increased regulatory pressure to assure authenticity, the Department of Defense issued new DFARS regulations which further expands 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

There are many factors of global supply chain challenges rising that are associated with obsolete and counterfeit components. With aging military technologies and obsolete parts no longer available from OEMs, the door has been opened for counterfeiters.

Data from a survey 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.
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 on the right 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).
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. Suppliers on this list have demonstrated acceptable counterfeit mitigation practices and quality assurance procedures that are consistent with industry standards.

**DFAR LANDSCAPE TO LEARN**

In addition to the Final Rule, there are four other FAR or DFARS Cases that relate to counterfeit electronic parts of interest as well:

- FAR Case 2013-002: Expanded Reporting of Nonconforming Items
- DFARS Case 2016-D013: Amendments Related to Trusted Suppliers
- DFARS Case 2016-D010: Cost of Remedy for Use or Inclusion of Counterfeit Electronic Parts
- DFARS Case 2015-D020: DoD Use of Trusted Suppliers for Electronic Parts

**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. 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.
Detection & Avoidance of Counterfeit Components:
Understanding Inspection Test & Authentication Methods

FEATURED WEBCAST TO LEARN MORE:

“Should Your Organization Be Concerned About DFARS 252.246.7008 and Its Supply Chain Impact Regarding Obsolete and Counterfeit Components?”

Military & Aerospace Magazine hosted a roundtable discussion on April 4, 2016 regarding the impact of the recent DFARS on the supply chain. Supply chain experts from Lockheed Martin, Global IC Trading Group, Secure Components, and IEC participated in discussing and answering questions related to:

- The three tier supply chain model for sourcing electronic components
- Compliance to the DFAR regarding Inspection Test & Authentication (IT&A)
- Alternatives to redesign approaches with regards to improved sustainability
- Corporate flow down, liability, and business risk

SUMMARY

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.

Sources: