11 December 2023

Why Manufacturers Must Adopt the AS6171 Standard for the Detection of Counterfeit EEE Parts

By Michael Schwarm

In the age of globalized manufacturing, the supply chain of electronic components has grown more complex than ever. The gray market presents an opportunity for counterfeit electronic parts to enter the system critical products and systems, leading to the potential for system failure, economic loss, injury and loss of life.

This blog presents why SAE standard AS6171 is currently regarded as the most accepted and comprehensive methodology to detect and ensure that counterfeit EEE components do not enter the defense systems and critical infrastructure supply chain.

The threat of counterfeit electronic parts in the U.S. supply chain continues to grow in scope and scale. The issue of counterfeit electronic parts is simultaneously a financial loss and a national security/safety threat. As has been previously noted, electronics authentication standards exist, but are only required for U.S. defense applications. Even then, adoption is slow and inconsistent and does not address other critical infrastructure applications. Emerging means of component authentication via encrypted code and DNA marking will take years to have a practical impact, if ever. For all critical infrastructures, in the near term, a comprehensive approach to counterfeit mitigation in the U.S. supply chain needs to consider sourcing, testing and risk avoidance.

The primary reasons for a company to adopt the **AS6171 testing** methodology for counterfeit electronic components detection are as follows:

1. Along with a rigorous sourcing process that supports avoidance of sourcing counterfeit EEE parts (such as AS6081), AS6171 provides a standardized, time-tested methodology for counterfeit EEE parts detection.

2. AS6171 complies with US Department of Defense (DoD) DFARs flowdowns requiring the adoption of a risk based counterfeit testing and authentication approach for the mitigation of EEE parts sources from outside of authorized distribution channels.

3. It can be tailored based on the complexity of the component and the criticality of the application it will be used in.

4. It is the most broadly adopted and mandated methodology for ensuring the authenticity of components being deployed in critical applications. As such, organizations deploying alternative “home grown” methodologies leave themselves open to significant financial and reputational risk should a counterfeit EEE component enter into a critical application.

AS6171 Background

When sourcing electronic and electromechanical (EEE) parts, the authenticity of those parts is paramount. The AS6171 standard is the industry accepted standard for testing these components, especially those bought from the open market or gray market.

11 December 2023

SAE AS6171, or simply AS6171, standardizes the inspection, electronic testing, and certification requirements for detecting Suspect/Counterfeit EEE parts. This provides the highest accepted level of assurance that components are genuine and conform to the original part numbers as specified by the original component manufacturer (OCM).

In April of 2023, **Revision A of SAE Standard AS6081** for Counterfeit EEE (Electrical, Electronic, and Electromechanical) parts, which governs the Avoidance, Detection, Mitigation, and Disposition of EEE Parts for Independent Distributors, was released. Amongst the changes in the standard was paragraph B.1.4, Test and Inspection Requirements. As a result of this change, the AS6081A standard now requires the supplier, in this case the independent distributor, to "comply with the inspection and test requirements of AS6171, to the extent specified by the [procuring] organization".

The Threat of Counterfeit EEE Parts

Counterfeit electronic parts in the U.S. supply chain continues to grow in volume and sophistication, resulting in increased risk to defense and aerospace systems, as well as other critical infrastructure including communications, transportation, medical, energy, and the financial sector.

Risks due to counterfeit electronic parts include system failure, injury, and death – which may either be a result of substandard counterfeit components or intentional system sabotage when functions (e.g., trojans) are introduced into products and systems to cause harm or to exfiltrate critical information.

Particularly at risk are industries, such as defense and aerospace, where long product lifecycles (20+ years) lead to diminished manufacturing sources and material shortages (DMSMS) and obsolescence issues because the electronics component average lifecycle is only 5-7 years (Blyler, Dangers of Counterfeit Semi Chips, 2020).

This issue drives three primary counterfeiting mechanisms:

1. The harvesting of used printed circuit boards to reclaim valuable electronics that are reconditioned (clean the leads, remark the package) and sold as new or something different; and

2. the remarking of new parts to pass them off as higher-grade parts, for example parts having an increased temperature survivability range; and

3. the cloning of components either by illicitly obtaining Intellectual Property (IP) or via functional emulation.

Defense and Critical Infrastructure Supply Chain Risk

Major defense systems are staying in service longer through extensive maintenance, upgrades, and modernization, and are significantly outliving original component production lifecycles. Counterfeit parts are increasingly entering the U.S. supply chain, primarily from China, and have been found across integrated circuits (ICs) and component parts including transistors, resistors, capacitors, fuses, etc.

According to a 2012 Senate Armed Services Committee investigation, more than one million counterfeit electronic components were used in 1,800 instances affecting military aircraft and missiles (Senate Armed Services Committee, 2012).

The same investigation found that 84,000 suspect counterfeit electronic parts were inserted into the DoD supply chain by a single electronic parts supplier, Hong Dark Electronic Trade, of Shenzhen, China. Parts from Hong Dark made it into the Traffic Alert and Collision Avoidance Systems (TCAS) intended for the widely used C-5AMP airlifter, the C-12 Operational Support Aircraft, and the RQ-4 Global Hawk unmanned aircraft system. In addition, parts from Hong Dark made it into assemblies intended for the P-3 Anti-Submarine Warfare (ASW) aircraft, the Special Operations Force A/MH-6M helicopter, and other military equipment, including the Excalibur extended range artillery projectile, the Navy Integrated Submarine Imaging System, and the Army's Stryker Mobile Gun (Senate Armed Services Committee, 2012).

EEE Parts Counterfeit Mitigation Policy

Section 889(a)(1)(B) of the Fiscal Year 2019 National Defense Authorization Act (NDAA) (Acqusition.Gov, 2019) prohibits recipients of federal contracting from using or procuring certain covered Chinese telecommunications equipment or services.

For the U.S. DoD, DFARS (Defense Federal Acquisition Regulation Supplement) clauses addressing counterfeit electronic parts are included in procurement contracts. For example, DFARS 252.246-7007, which implements Section 818 of the 2012 NDAA, states that "the contractor shall establish and maintain an acceptable counterfeit electronic part detection and avoidance system." The flowdowns establish that there should be a counterfeit avoidance program, not the inspection and test standards for such a program.

Counterfeit EEE parts mitigation standards, most commonly based on AS6171, are being proactively adopted by defense systems manufacturers such as Raytheon Technologies, Lockheed Martin, Northrop Grumman, L3Harris and General Dynamics.

In 2023, SMT Corp, a leader in counterfeit EEE detection since 2007, reported that the percentage of testing based on AS6171 for defense applications grew 3x over a 12-month period from 10% to 40% of all testing performed. This is primarily due to the recognition amongst the U.S. Defense prime contractors that AS6171 is currently the best and most accepted methodology to mitigate counterfeit EEE parts.

The superior level of effectiveness of AS6171 for counterfeit parts mitigation was reaffirmed in 2023 by the U.S. DoD Defense Microelectronics Activity (DMEA) released the **Final Report on Machine Vision Pilot (MVP) and Microelectronic Authenticity and Security, Evaluation and Research (MASER)**.

Through an assessment of the key Image Analysis (IA) and related Side Channel (SC) technologies for counterfeit detection and prevention it was found that some IA and SC technologies have shown promise. However, in their current stage of development, Machine Vision technologies do not provide satisfactory solutions for counterfeit prevention and detection in the real-world environment (TRL 7), despite demonstrating promising results in controlled laboratory environments (TRL 4). Standards-based Conventional Testing (such as AS6171) is consistently accurate, though time consuming, in the detection of variations between authentic and counterfeit parts and

demonstrated the ability to determine which parts were counterfeit in the absence of an exemplar, based on detection of physical defects.

Careful source selection and the application of Standards-based Conventional Testing, commensurate with the appropriate level of risk mitigation for the application, remains the industry best practice.

Considerations When Deploying AS6171

While there are highly regarded "gold standard" counterfeit mitigation labs such as SMT Corp and Integra Technologies that go above and beyond current standards, there are also many labs that are suspected of cutting corners. While labs that have been accredited for AS6171 testing have processes that are audited and approved, there is no guarantee that the processes are followed rigorously. In fact, only a handful of test labs are currently accredited for AS6171 and two of those have had GIDEP alerts issued in 2023 for obvious escapes in the detection of suspect components. Organizations contracting with AS6171 labs must perform a rigorous supplier qualification process to ensure the integrity and effectiveness of the test organization.

A comprehensive counterfeit EEE mitigation program must also address sourcing – counterfeit avoidance – as an integral part of the counterfeit mitigation process. There are many electronics sourcing companies that outsource their testing to a third party, and test houses that do not source their own parts. This lack of ownership enables an ecosystem in which risks are compounded, resulting in a higher risk of counterfeit parts slipping through to critical systems. GIDEP publishes data on companies that have been confirmed to pass through counterfeit parts yet there is no standard that enforces the future avoidance, or rehabilitation, of these companies.

These recommendations and standards need to be applied beyond U.S. defense applications to all critical infrastructure applications such as the mobile network grid, port security, air traffic control, financial transactions, implantable defibrillators, data centers, and the energy grid – not to mention emerging technologies such as quantum computing and artificial intelligence. Other U.S. government agencies including the Department of Energy, the Federal Aviation Administration, the Department of Homeland Security, the Food and Drug Administration, the Federal Communications Commission, and the National Transportation Safety Board must take note.

About SMT, Corp

SMT Corp is the industry leader for sourcing & authentication of DMSMS and hard-to-find electronics components, electrical testing services, and inventory management solutions. SMT Corp is a highly accredited and recognized expert with full on-site sourcing (AS6081), authentication (AS6171), and electrical testing to mitigate the risk of counterfeit, cloned, altered and substandard products from entering the critical infrastructure supply chain.
https://smtcorp.com/

11 December 2023

About Certify Holdings

Certify Holdings is a full lifecycle strategic partner for the defense and aerospace market, and other markets requiring high reliability electronic solutions. Certify Holdings supports our customers through the early project design stage with design-in support leveraging a wide range of Hi-Rel and RF electronic modules and components, throughout production with sourcing and distribution services, and into obsolescence / end of life with sourcing and authentication of hard-to-find electronics. Throughout the project lifecycle, Certify Holdings supports our customers with test solutions and services. https://certifyholdings.com/