4 March 2024

Is it time to update your counterfeit electronic parts mitigation policy? These should be your top considerations.

By Jason Romano and Kim Costa

There are many considerations when creating or updating a policy for the mitigation of counterfeit electronic components. The main intention of such a policy is applicable to components sourced from the open market (or gray market). However, the increased threat of clone counterfeits making their way into authorized distribution channels may also necessitate policies to consider components sourced from vulnerable authorized sources, for instance, authorized distribution of Chinese made semiconductors.

Developing a policy for counterfeit parts mitigation should address under which scenarios your company will source from the open market. For example, is sourcing from the open market only performed for obsolete/end-of-life components, or will you source to improve lead times or pricing? Additionally, when a part is sourced from the open market, how is the component to be authenticated? What sourcing and testing standards will be applied? Are you simply verifying the *authenticity* of the part or are you also going to also validate the *quality* of the part?

Compliance

A key consideration your policy should cover is what flow downs and regulations drive your company's policy decisions. If your company mainly supports the U.S. defense industry, the U.S. Department of Defense 'Defense Federal Acquisition Regulation Supplement (DFAR) flow down requires a risk-based testing methodology, such as AS6171.

Additionally, many defense prime contractors have their own counterfeit electrical, electronic, and electromechanical (EEE) parts mitigation policies included within their terms and conditions. Many of these policies provide more specific requirements than the referenced DFAR, however they are often derived from the same requirement to have a risk-based testing methodology.

Another consideration is your corporate attitude towards legal risk. If your company ends up sourcing counterfeit components that make their way into a system resulting in degradation, failure, injury, and/or loss of life, how will you defend the ensuing contract or legal actions? Is your policy aligned with accepted industry standard practices, or did you 'go it alone' or implement a demonstrably substandard policy?

Risk Tolerance

There are two main elements when considering your company's risk exposure when sourcing from the open market. Risk is the product of Probability of Occurrence and Impact. Probability of Occurrence is related to how often you source from the open market, what you source, and what counterfeit mitigation steps you are taking. How frequently you source from the open market is based on whether you source for obsolescence, lead times, and/or price.

The complexity of the components you need to source also drive Probability of Occurrence. Are you mainly sourcing passive components and simple logic devices? Are you sourcing highly profitable products such as microcontrollers and FPGAs? Generally, the more complex the part is, the more profitable they are to counterfeiters, hence more risk to you.

Perhaps most important is how you source since at some point you are likely to have to source complex components from the open market. Ask yourself:

- Are you sourcing from reputable sources that you have good history with?
- What level of testing are you performing on parts to ensure they are authentic and of good quality?
- What applications or products will be affected if a counterfeit part makes its way into your supply chain?
- Is it primarily a financial risk or could a counterfeit part degrade critical operations, or cause system or product failure?
- If an end use system or product fails because of what your company has supplied, will it be a total failure and/or could it potentially result in injury or loss of life?

Counterfeit EEE Parts Mitigation Testing Standards

There are many guidelines and standards that have been used over the past decade for counterfeit electronic parts detection and mitigation. As depicted in table 1, the most effective standards-based means of counterfeit detection is AS6171 High Risk Level 2 or a combination of AS6171 Moderate Risk Level 2 with Electrical testing.

AS6081 isn’t a viable option as Revision A (released in April 2023) removed the test methods and now refers to AS6171. AS6081 is still an important *sourcing* standard for independent distributors; but revision A should no longer be flowed down as a mitigation standard. Note that in the table, electrical testing is separated even though there can be various degrees of electrical testing included as part of AS6171.

Counterfeit EEE Part Type	IDEA-STD-1010-B	AS6081 (Note 1)	AS6171 Moderate Risk Level 2	AS6171 High Risk Level 2	Electrical
Recycled Counterfeit	X	✓	✓	✓	X
Remarked Counterfeit	✓	✓	✓	✓	X
Out-of-spec / Defective	X	X	X	X	✓
Cloned	X	X	X	✓	✓
Forged Documentation	✓	✓	✓	✓	X
Tampered	X	X	X	✓	✓

Table 1

It is important to note that the U.S Department of Defense DFARs flow down (252.246-7007252.246-7007) mandates a counterfeit parts avoidance system that is based on a dynamic risk assessment. While it does not mandate the common industry-accepted SAE standard for counterfeit avoidance (AS6171 specifically), AS6171 is a risk-based methodology. As such, it has been adopted at Moderate Risk Level 2 (MRL2) by several defense prime contractors as the minimum basis of their counterfeit parts avoidance programs.

Counterfeit EEE Parts Mitigation Sourcing Standards

Counterfeit avoidance is equally as important for mitigating the risk of counterfeit EEE parts. AS6081A and AS5553 are common industry applied standards for the avoidance of counterfeit electronic parts sourced from the open market. These standards address actions such as supplier evaluation, assessing and mitigating risk of counterfeit parts, control and reporting of counterfeit components, and more.

One decision many companies face in their open market sourcing policy is whether to separate sourcing and authentication. Most counterfeit parts detected at SMT Corp are parts that our customers source and bring to us for testing as a third party. We have a much lower incidence of counterfeit parts if we source from our highly scrutinized supplier base, consisting of less than 200 authorized suppliers and over 1400 restricted suppliers. Having an integrated sourcing and authentication program for sourcing parts from the open market ensures that there is no finger pointing and that one company has total chain of custody once the parts are sourced from the open market. It also means that SMT Corp holds the financial risk if the parts sourced are not authentic or are poor quality. Additionally, with SMT Corp's reputation and detailed test reports, you can have confidence that the parts we source have been analyzed and tested to the highest standard in the industry.

Avoid heating up the market!

If you source from multiple open market distributors, you need to avoid heating up the market. A case in point, you probably want to ensure you have competitive offerings from the companies you source from. However, if you go into the open market and drive demand for electronic components in relatively low supply, you will invariably drive market pricing up. Do you know how to query the open market in a way that won't drive pricing and availability? To avoid this, you should engage with an independent distributor who can offer strategic options to provide you with competitive assurances and a highly reputable and effective counterfeit mitigation program.

Other key considerations

There are several other considerations when developing your policy on sourcing from the open market.

- **Sub tier suppliers and contract manufacturers:**
    - Will you flow down your policies to your supply base, or leave it up to them to figure it out?
    - Will you flow down general requirements for them to meet?
    - Will you qualify companies that perform open market sourcing and/or testing and insist that your supply base use those same providers with the same testing and sourcing procedures?
    - For that matter, are the suppliers you have qualified for open market sourcing and authentication approved by your customers?

- **Training:**
    - If you deploy your own processes for sourcing and testing open market parts, how will you train your internal resources?
    - Do you have enough experience to effectively test, detect and dispose of counterfeit parts?
    - Do you source enough parts from the open market to exercise your processes, people and tools?

  - Does your company have the resources, knowledge, and commitment to invest in the latest capital equipment and processes and effectively use them - will you be the best at identification of counterfeit parts?

- **Future trends:**
  - Who will keep track of emerging trends and counterfeit detection methodologies?
  - How will you stay updated and relevant regarding policies that will affect your organization?

Conclusion

These are just some of the high-level considerations policy writers should address when creating and updating a counterfeit EEE mitigation policy. While developing your own counterfeit parts mitigation program is achievable, it's best to work with a company that specializes in open market sourcing, authentication, and verification to support you in development of your policy. SMT Corp. provides full service open market sourcing and authentication, as well as third party authentication and testing services. To find out more about how we can support your organization and your strategic sourcing needs, contact a member of our team today.