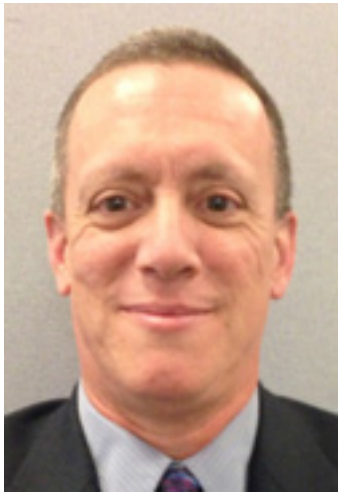
Protection against counterfeit product issues for military programs

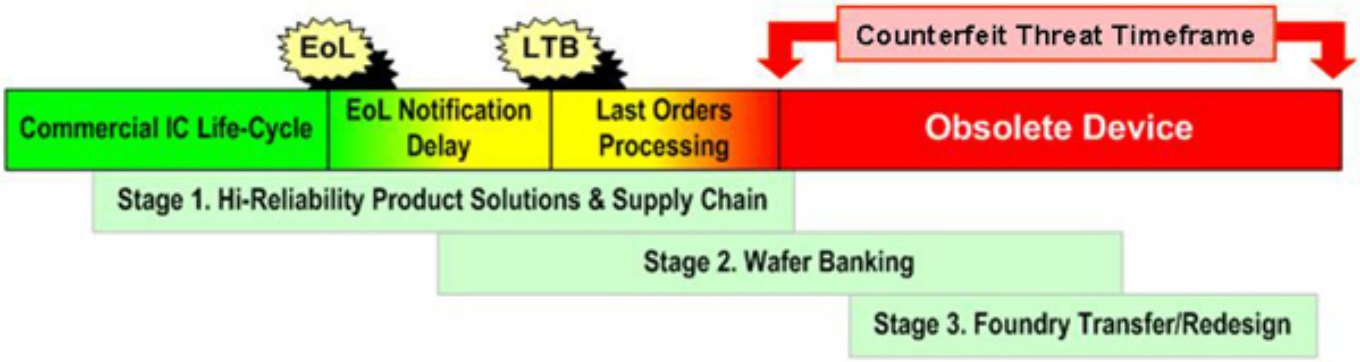
Michael Sarpa, e2v



Counterfeit material in the semiconductor supply chain is increasingly problematic for the military and aerospace community. With the immense costs and significant program delays inherent in a system redesign, military program managers search high and low for parts to meet the original specification requirements, often resulting in risky purchases from less-than-reputable brokers. This article provides a brief historical background on counterfeit parts, highlights some of the chronic issues, and offers some approaches to combat this ever-increasing problem.

Counterfeit parts: a background

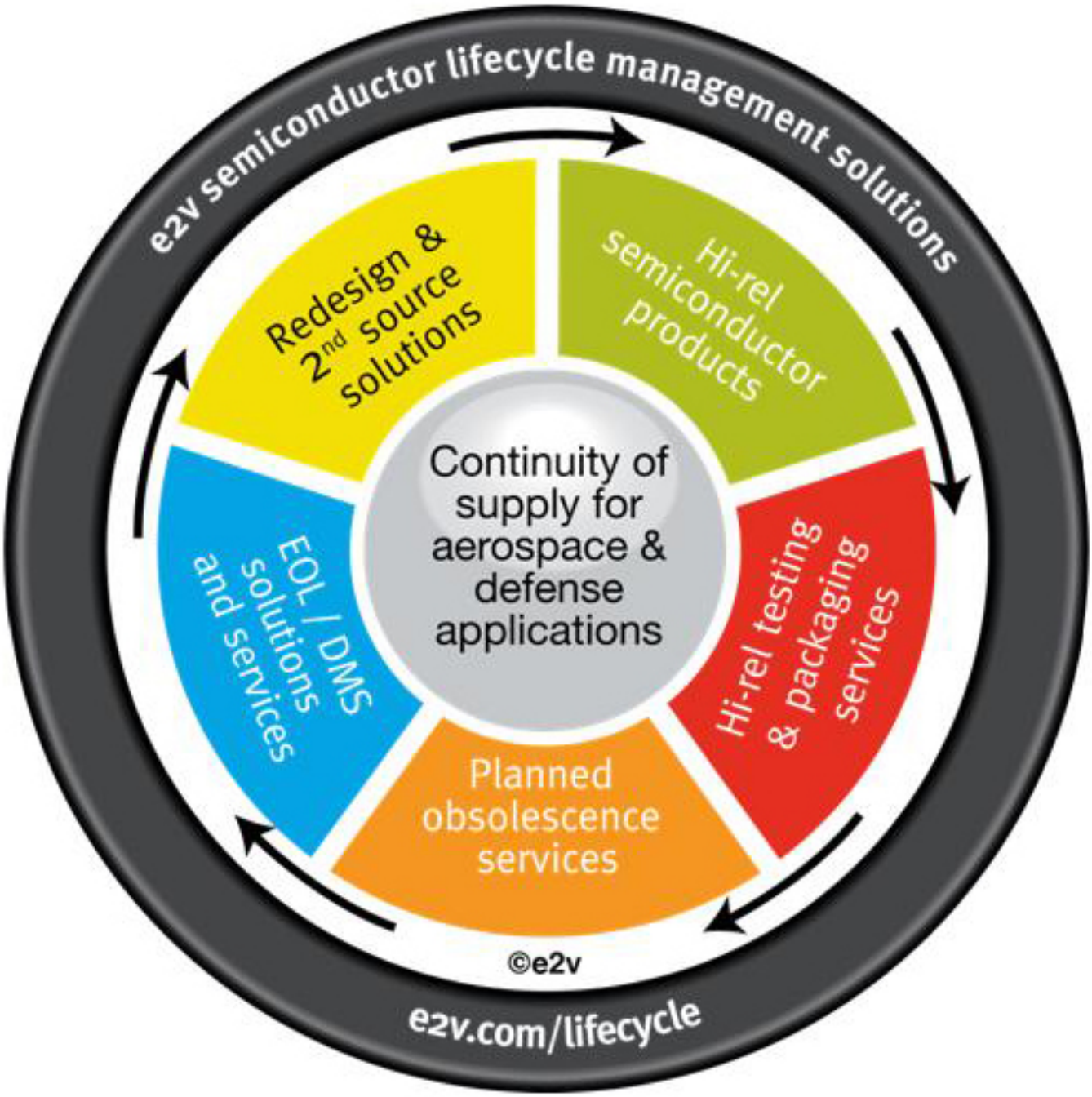
Throughout history there are countless examples of unscrupulous businesses regularly exploiting vulnerabilities and using any way they can to make a quick buck. This is a chronic problem within the semiconductor industry where it is relatively easy to obtain the basic materials to produce counterfeit products that are difficult to distinguish from authentic versions. Buying semiconductor lead frames, packages, trays/tubes and other necessary materials in volume is not a large investment for the counterfeiter. Although the capital investment required to purchase equipment used to produce quality semiconductors can be quite expensive; it takes a minimal investment to get access to stripping and remarking equipment to make parts appear to be authentic devices. Consequently, opportunists see unfulfilled demand and an opportunity to exploit buyers, especially when authentic parts are of limited availability.



Product Lifecycle Timeline

Volume production phase
During the production run of an original semiconductor device, there is really no opportunity for counterfeiters to prosper, especially in the military and aerospace community. While a consumer OEM may buy from the gray market to save a few dollars with the intent to increase margins, a military or aerospace contractor cannot take these risks, and as such will only buy through authorized vendors (OEMs and Distributors), so as to ensure that the product is safely tracked, stored, and handled. During this phase, the contractor expects the product to be supplied with full traceability, including certificates of conformance and warranty guarantees from the original supplier. When quality issues arise, devices can be returned to the original manufacturer for replacement or if needed, failure analysis. Corrective actions can be implemented to prevent future quality issues.

After the last time buy
Military programs often have not even reached the production stage when critical devices are discontinued. While original semiconductor manufacturers almost universally offer Last Time Buys, the program offices lack the funding necessary to supply a long-term program that may run for 15 years or longer. Once the original supplier will no longer accept additional orders and the authorized distribution channels run out of product, the window of opportunity opens for counterfeiters to offer “solutions” to purchasing departments that are scrambling to find alternative sources to meet program requirements. Many aftermarket companies offer devices; and it can be hard for a military contractor to differentiate between suppliers who offer qualified devices versus those who push counterfeit devices.



e2v aerospace and defense Semiconductor Lifecycle Management

Counterfeit material influx

Most counterfeit material enters into the supply chain when contractors are desperate to meet program requirements. Risky purchases from unscrupulous suppliers leave the contractor with no recourse when the product purchased fails to meet the electrical or quality requirements. Consequently, they have wasted program funding to purchase unusable product coupled with the risk of such being passed on to the US warfighter. Restricting purchases to only those aftermarket suppliers with a proven quality history can eliminate this risk, and these validated suppliers use two main ways to provide certified material.

Aftermarket original devices

“Original devices” – defined herein as devices using wafers fabricated at the original manufacturer’s fab facility – are primarily obtained from aftermarket suppliers such as e2v aerospace and defense. These original devices are mainly produced using two methodologies: – 1) production devices, where the aftermarket supplier buys certified excess finished goods from the original supplier, and 2) wafer storage, where the aftermarket supplier buys and stores original wafers, and then uses their certified facilities to assemble, test and verify the devices. The key for both of these methodologies is traceability, as any supplier offering these “original devices” should be able to provide a clear paperwork trail to the original wafer fabrication and/or assembly facilities. In addition, the aftermarket supplier should be fully certified to supply products to original Defense Logistics Agency (DLA) specifications, and should be capable of passing all DLA qualifications.

Reengineering replacements

The second method is for an aftermarket supplier to reengineer devices to meet the original manufacturer specifications and requirements. This approach is more costly than purchasing original devices, but is usually dwarfed by the costs associated with a complete system redesign and requalification, and avoids the risk of purchasing devices from unknown sources. In this methodology, the contractor commits funding to essentially design devices from scratch by using currently available materials and wafer fabrication facilities to duplicate the performance of the original device. The aftermarket supplier must have the knowledge and expertise to re-create the design, but more importantly, have the processes in place to fully test and certify the devices to the original specifications, and be able to be fully certified to the original DLA SMD or slash sheet specifications.