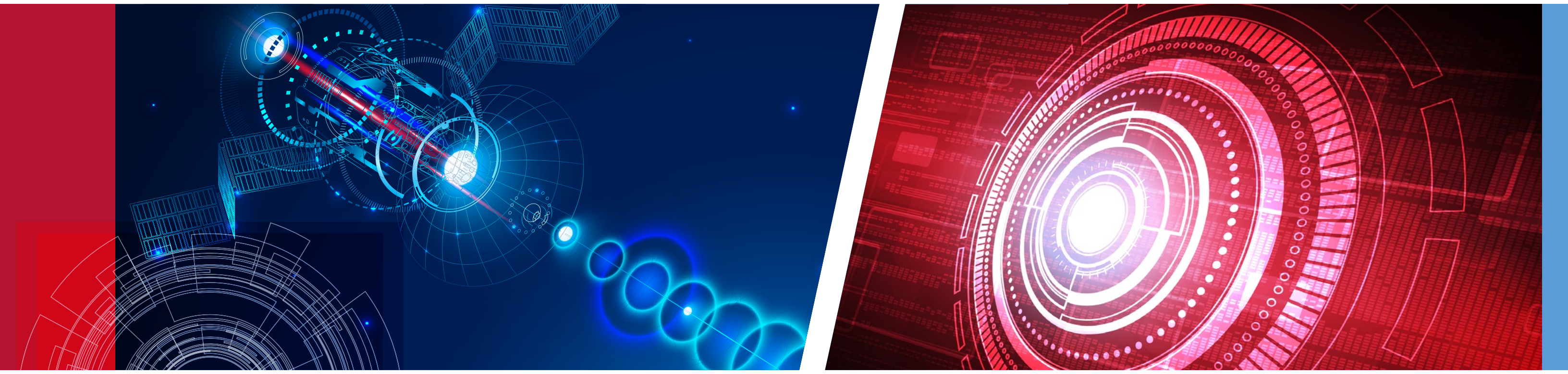
ASSURED ELECTRONICS INSIGHTS



BUYERS AND SELLERS BEWARE:

LITTLE-KNOWN RISKS LURK IN THE DEFENSE ELECTRONICS SUPPLY CHAIN

Increasing supply chain resilience is on everyone's mind these days. But the risks lurking in the defense electronics supply chain extend well beyond the issues that have garnered the headlines.

In fact, every DoD mission that relies on electronics systems is prone to several little-known risks in the supply chain of the underlying printed circuit board assemblies (PCBAs).

The following are some of the less-publicized risks in the PCBA supply chain that have the potential to cause major problems, as well as recommendations regarding how the U.S. Government can address them.

COUNTERFEIT RISKS RISING

The transition to lead-free electronics has been in progress for more than a decade. However, aerospace and defense companies have been held back from using lead-free electronics because the DoD has never tested and certified them as being reliable.

Original equipment manufacturers (OEMs) with legacy designs based on leaded components now face an increasing risk of counterfeits as the supply of leaded parts dwindles. Brokers can help find leaded components, but this unregulated market has many non-transparent and unqualified players. The general lack of traceability in electronics components exacerbates the problem.

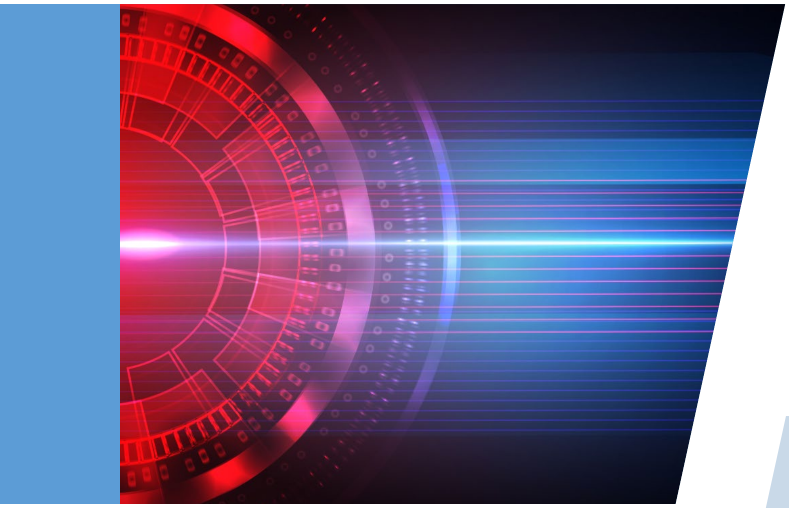
Lead-free components with reliable functionality are often available, but there is no current guidance on which systems are allowed to use lead-free parts. Specialty manufacturers offer an array of services to convert commercial, off-the-shelf lead-free systems into leaded ones, but these strategies have limitations as well.

MANUFACTURING CAPABILITIES FALLING BEHIND THE GLOBAL COMPETITION

New electronics technologies and components often require new manufacturing equipment to assemble them. But many electronics manufacturing services (EMS) companies, also known as contract manufacturers, have thin profit margins and lack the capitalization to purchase and install it. State-of-the-art techniques that are being adopted in other nations are not yet widely available in the United States, and the lack of a strong national policy framework encouraging such investment means the U.S. is falling behind in global competition.

MANUFACTURING KNOWLEDGE BEING LOST

Meanwhile, as thousands of Baby Boomers retire every year, a great deal of industry knowledge and experience is being lost, and skilled replacements are hard to find. This is especially problematic in the electronics field because, while the customer may provide some of the specifications for a PCBA, many decisions are left up to the manufacturer. Any wrong decisions can lead to latent defects that are undetectable until the product has been deployed.



INFORMATION MANAGEMENT IS SPOTTY

Information management is another area rife with risk. When problems arise, it would be helpful to be able to isolate the provenance and other details of various components. But manufacturers vary widely in their ability to trace the source of components; detect and mitigate counterfeits; and protect intellectual property.

Emerging environmental regulations will add to the data burden, as they are expected to require end-to-end tracking of materials used in electronics.

Cyber security requirements such as NIST 800-171 and the new the Cybersecurity Maturity Model Certification (CMMC) are completely changing the way EMS companies handle their data and deal with their customers, employees, and supply base. Given the limitations of self-assessment to demonstrate compliance – which is the current plan – there will continue to be wide variations in how EMS companies address key compliance issues.

ITAR IS NOT AIRTIGHT

The U.S. International Traffic in Arms Regulations (ITAR) control the manufacture, sale, and distribution of national security-related products and services. ITAR registration is managed by the State Department, and, except where exports are involved, it merely requires self-certifying the company's ownership structure. The processes for actually controlling access to data vary widely due to the self-certifying nature of the process. For example, ITAR-controlled design files are often improperly shared with non-ITAR fabricators and subcontractors, even when the customers have directed the vendors to be more careful.

MITIGATING ELECTRONICS MANUFACTURING RISKS

Fortunately, many of these risks can be mitigated without exorbitant investments; rather, it's a matter of building up existing partnerships and resources.

- **COUNTERFEIT RISKS AND LEAD-FREE:** The Solder Performance and Reliability Assurance Project, funded by the DoD and being carried out by major universities and defense corporations under contract with the U.S. Partnership for Assured Electronics (USPAE), is working to provide data-based criteria for aerospace and defense electronics engineers to confidently adopt more lead-free technologies. Congress needs to continue funding this project, and DoD needs to implement the results rapidly. Until this transition is complete, the dwindling supply of leaded parts will continue to add unnecessary cost, schedule, and reliability risks to many DoD programs.

- **WORKFORCE:** To ensure the next generation of workers can learn the skills needed in the factories of the future, Congress should create tax incentives for businesses and individuals to invest in high-quality training and certification programs offered by industry associations. The government should also ensure that federal contracting requirements contain language supporting these programs.

- **MANUFACTURING CAPABILITIES:** The U.S. must adopt a "silicon-to-systems" policy approach that strengthens the entire electronics manufacturing ecosystem, supporting not just semiconductors but also printed circuit boards and hardware assemblies. Addressing electronics manufacturing more holistically is the only way to wean the U.S. off a dangerous reliance on foreign suppliers.

- **INFORMATION MANAGEMENT AND CYBER SECURITY:** The electronics industry's "Trusted Supplier" standard, known as IPC-1791 and developed jointly by industry group IPC and the DoD, provides assurances that cyber and physical security, ITAR, and supply chain risks are being minimized through extensive audits and certifications. Members of the USPAE, which fosters collaboration between the electronics industry and the DoD, are required to be certified to this standard. Other quality-system certifications such as ISO 9001 and AS 9100 also provide assurances of a well-run organization.

Unfortunately, PCBAs have historically been viewed as a commodity by many organizations, with purchasing decisions delegated to non-technical buyers with little industry experience. But with new technologies, new requirements, and rising risks of latent defects, PCBA manufacturing has become a complex and high-risk proposition. It's time for DoD mission leaders to become more familiar with these risks and how they could affect warfighters and weapons systems, and then to focus more time and energy on fixing them.

The author, Matt Turpin (Matt Turpin | LinkedIn), is a consultant and longtime leader of the electronics manufacturing industry, having led several companies over a 40-year career. He currently serves as a senior advisor to USPAE.

FOR MORE INFORMATION:

www.USPAE.org

Phone: (202) 661-8098

Email: info@USPAE.org