The Growing Threat of Counterfeit Electronic Parts in the Critical Infrastructure Supply Chain of the United States and Allies

SMT Corp., Sandy Hook, Connecticut
May 15th, 2023

Counterfeit Electronic Parts Threat Overview

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, including 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 two primary counterfeiting mechanisms:

- the harvesting of used printed circuit boards to reclaim valuable electronics that are reconditioned and sold as new or something different; and
- the cloning of components either by illicitly obtaining Intellectual Property (IP), reverse engineering, or via functional emulation.

This report addresses several aspects of counterfeit electronic parts and provides recommendations to protect products and systems in critical U.S. applications.

Types of Counterfeit Electronic Parts

Currently, the most comprehensive counterfeit mitigation standard is SAE International AS6171; Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts:

> *AS6171 standardizes inspection and test procedures, workmanship criteria, and minimum training and certification requirements to detect Suspect / Counterfeit Electrical, Electronic, and Electromechanical (EEE) parts [referred to in this report generically as electronic parts]. The requirements apply once a decision is made, primarily out of necessity, to use parts that do not have traceability back to the original component manufacturer (OCM) or authorized distribution. The tests specified by this standard may also detect occurrences of malicious tampering, although the current version of this standard is not designed for this purpose.* (SAE International, 2018)

AS6171 defines five categories of counterfeit components:

1. **Recycled:** A part that has been reclaimed/recovered from a system and then modified to be misrepresented as a new and/or genuine part from an authorized manufacturer.
2. **Remarked:** A part from an authorized manufacturer which has had the legitimate part marking replaced with a forged marking in order to represent the part as something it is not.

3. **Out-of-Specification/Defective:** A part that is identified as nonconforming by the authorized manufacturer in accordance with the specification, and then misrepresented as conforming.
4. **Cloned.** A reproduction of a part produced by an unauthorized manufacturer without approval or design authority that replicates the authorized manufacturer's part.
5. **Tampered.** Typically applied to cloned chips, tampering is modification of the chip for sabotage or malfunction.

Although recycling and misrepresenting genuine parts remain the most common forms of electronics counterfeiting - cloning and tampering are becoming more prevalent - and represents an increased risk to critical infrastructure.

Reverse engineering is one of the methods for cloning an authentic chip. In this technique, the counterfeiter physically removes the silicon die from the component package and will "delayer" the die. Once the chip has been completely delayered, the counterfeiter can then build a clone component using the reverse engineered, layer by layer silicon recipe (Blyler, Dangers of Counterfeit Semi Chips, 2020).

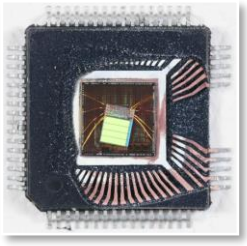
Another cloning technique is via functional emulation. Rather than reverse engineering the silicon die, a counterfeiter uses a similar silicon technology or die layout to achieve similar electrical functionality. The components are then packaged and marked to look like authentic devices. From an external perspective, the functional emulation clone device looks and functions like authentic devices.

Finally, cloning can be achieved by illicitly acquiring the original manufacturer's IP (silicon mask files or recipes). This IP is a fabrication recipe that would allow a counterfeiter to illegally produce cloned components, provided they have access to adequate fabrication resources.

Clones and altered counterfeit chips are one of the key cyber-attack surfaces that Warren Savage, Chairman, CEO and President of IPextreme, identified in his keynote address at DesignCon 2020. "Such compromised chips are a serious problem for the semiconductor industry. For example, a counterfeit chip in a tank could feed sensitive information such as [location or armament] to an adversary. Rogue code in a fake semiconductor could shut down the air supply of an airliner. A counterfeit chip could be used to shut down a car in a ransomware attack." (Blyler, Dangers of Counterfeit Semi Chips, 2020)

As an example of a possible cloned and tampered with counterfeit, SMT Corp., a recognized industry leader in counterfeit electronic parts mitigation, discovered a suspect counterfeit microcontroller (marked fraudulently as a ST Micro part number), in 2019, that was found in a point-of-sale (POS) device used for payment transactions.

Fake Microcontroller Device Package



Fake Device with Floating Memory

SMT Corp. was able to extract and reverse compile code in the flash memory of this device and found references to the POS equipment maker which was based in China. The code could have been used to exfiltrate financial information from debit and credit cards.

There is particular concern about microcontroller counterfeits because of the potential for hardware trojans (hidden memory sectors or built-in sub-routines) that could allow third parties to extract data from systems. Microcontrollers are often interfaced to communications systems such as wired/wireless networks that can be remotely accessed.

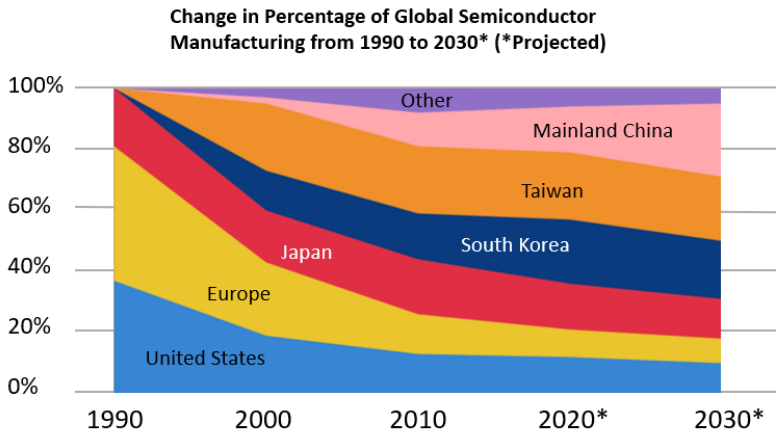
According to Dr. Nicolas Williams, Director - Electronics Test & Analysis Labs at SMT Corp., widely recognized as the gold standard for counterfeit mitigation and electronics authentication and test, "the complexity of cloned devices being introduced into the defense supply chain has been steadily developing since the early 2010s. In 2012, SMT Corp. detected a cloned Inverter, a basic electronics logic device. In 2017, flash memory counterfeits were being discovered. In 2019, Microcontroller counterfeits became common. Today, we are seeing complex Field Programmable Gate Arrays (FPGAs) and modules. The complexity of electronics components being counterfeited is growing exponentially".

The Market for Counterfeit Electronics

Due to their potentially high value, electronics are of particular interest to counterfeiters. As of 2022, the total global electronics market was estimated at $1.5 trillion, and is anticipated to reach $2.1 trillion in 2030, expanding at a CAGR of 5.5% (MarketWatch, 2023). The sustained growth of the electronics market, the increase in electronics complexity and density, the global "chip war", geopolitical instability, and other factors provide increased incentive for would-be electronics counterfeiters. In a 2022 report, the Electronic Reseller Association International (ERAI) suggests that the number of counterfeit electronic products in circulation is increasing, and that businesses lose approximately $250 billion each year to counterfeit electronics products (Akhoundov, 2022).

The global electronic components market size supporting the electronics product market was valued at $186 billion in 2022. It is projected to reach $329 billion by 2031, growing at a CAGR of 6.5% during the forecast period (Straits Research, 2023). In 2019, the worldwide fake semi market was estimated at $75 billion according to Industry Week. (Blyler, Dangers of Counterfeit Semi Chips, 2020)

A 2021 study from the Boston Consulting Group and the Semiconductor Industry Association demonstrates how much chip production has moved away from its traditional strongholds – among them the United States - in recent years. As the figure shows, in 1990, Japan, Europe and the U.S. dominated semiconductor manufacturing; but with South Korea, Taiwan and mainland China entering the market, the three initial manufacturing locations were reduced to a combined market share of roughly 35% in 2020. The decline is projected to continue, if more slowly, through 2030. Even with some growth in the U.S. market driven by onshoring campaigns, most chip fabrication will continue to be from outside of the U.S. and Europe - with sources in Asia projected to dominate approximately 80% of the world's semiconductor manufacturing (Buchholz, 2021).



In 2022, ERAI, which tracks only a fraction of counterfeit electronics, reported a 35% increase in the number of reported counterfeit parts from 2021 to 2022 despite global semiconductor sales rates being flat during the same period (Akhoundov, 2022).

Impacts on the U.S. DoD Electronics Supply Chain

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.

Nick Martin, Director of the Defense Microelectronics Activity (DMEA) says that "Our DoD weapons systems are long in the tooth in terms of time in the field, and we need to make sure that there's specific reliability requirements for the components that we put into them. Counterfeits or even cloned components will compromise the reliability" of this equipment (Gould, 2022).

Government-Industry Data Exchange Program (GIDEP) Program Manager Jim Stein notes that the Defense Department has seen counterfeits increase in number and sophistication over the last two decades, with batches of counterfeits increasingly hidden in authentic parts, making them harder to find (Gould, 2022).

Although standards are being proactively adopted by defense systems manufacturers such as Raytheon Technologies, Lockheed Martin, Northrop Grumman, L3Harris and General Dynamics, the implementation and enforcement of these standards across the aerospace/defense sector is slow and inconsistent.

Furthermore, the defense supply chain is extremely complex. For example, the F-35 relies on more than 1,700 suppliers at all levels providing roughly 300,000 parts. The Air Force's network is even broader; the service said it depends on about 12,000 direct suppliers. But further down the supply chain, the network expands to about one million companies (Gould, 2022). Beyond the aerospace/defense sector there are few, if any, standards being adopted for counterfeit mitigation.

Real World Implications of Counterfeit Electronics

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).

In response to the recent death of an F-16 pilot, the Air Force Research Laboratory (AFRL) filed suit against multiple defense companies, alleging that "counterfeit parts" in a jet ejection seat system may have contributed to the death of the pilot in June 2020". The suit contends that after 1st Lt David J. Schmitz's death, AFRL determined his ejection system's "malfunctioning" Digital Recovery Sequencer (DRS) contained "six suspected counterfeit Metal-Oxide Semiconductor Field-Effect Transistors (MOSFET), three suspected counterfeit serial flash memory chips, and a suspected counterfeit parallel flash memory chip." (Gnau, 2022). The ejection seat is installed on aircraft across the Air Force including the F-15, F-16, F-22 and F-117 fighter jets, the A-10 attack plane, and B-1 and B-2 bombers, according to the manufacturer. (Cohen, 2022)

In 2018, Bloomberg Businessweek reported that the Chinese government inserted a stealth doorway into servers made by the Oregon-based company Elemental Technologies in the form of a tiny microchip. According to the report, the servers — with chips inserted at factories run by manufacturing subcontractors in China — could be found in Defense Department data centers, CIA drone operations and the onboard networks of U.S. Navy ships (Gould, 2022).

The Fukushima nuclear disaster of 2011 was partly attributed to the use of counterfeit electronics. The backup generators for the cooling systems of the nuclear reactors failed to function due to counterfeit electronics, which were not designed to withstand the conditions needed for the job. This led to multiple explosions, injuries, and radiation exposure, resulting in the deaths of two workers and the evacuation of tens of thousands of people.

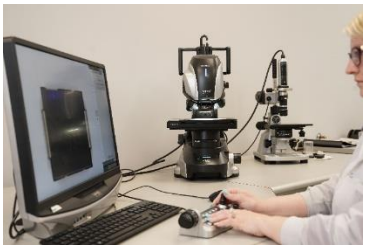
Counterfeit Mitigation Techniques

Counterfeit parts are increasingly difficult to detect because of more complex counterfeit technologies and techniques, as well as the increasing complexity of global supply chains.

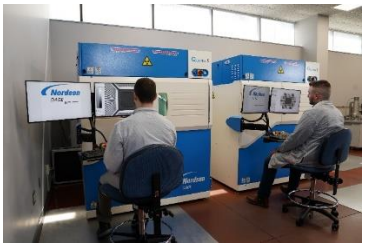
Published in late 2012, SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors, was adopted by some of the major component manufacturers and prime defense contractors as the required level of testing for material sourced from non-authorized distribution channels. Due to the increased sophistication of counterfeit electronics, SAE released AS6171 in 2016, subsequently revised in 2018, which is more robust than AS6081. Even with the release of the more robust standard, SMT Corp. reported that for 2022, 89% of the authentication tests performed were at the older, AS6081 standard as opposed to the AS6171 standard.

As explained by Jason Romano, Chief Investigator and Subject Matter Expert at SMT Corp., “the minimum required counterfeit mitigation testing recommended by AS6171 is Moderate Risk Level 2, which requires both external and internal physical inspection of the component. Counterfeit components can have inconsistent markings, discoloration, resurfacing material, tooling marks, and numerous other subtle defects on the exterior package. To determine authenticity, a high-intensity digital microscope is used to examine each component for such defects, down to the sub-micron level. Clues of tampering require a trained eye and precise equipment to identify. The standards specify inspection tests that encompass basic visual inspection to more complex internal inspections. Additional tests and inspections can be performed to further increase the level of confidence.”

Some of the inspection tests required by AS6171 are depicted below (pictures courtesy of SMT Corp.):



External Visual Inspection



2D and 3D Radiological Inspection

Scanning Electron Microscopy

As a minimum, Moderate Risk Level 2 requires electrical testing of the static DC electrical parameters for active, complex devices or value measurements for passive components. This minimum level of required testing provides test coverage for the general component functionality. AS6171 includes optional recommended electrical testing such as measuring key electrical parameters, testing electrical

components over operating temperature range, and burn-in. These additional tests are requirements for higher risk levels as determined by the Adjusted Risk Score per AS6171.

Current Policies

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. GIDEP publishes data on companies that have been confirmed to pass through counterfeit parts yet there is no standard that enforces the avoidance of these companies.

The Fiscal Year 2023 NDAA also prohibits the federal government from entering or extending contracts with companies to procure electronic parts, products or services that include semiconductor parts or services from certain Chinese entities. The semiconductor prohibitions will not take effect until five years after the enactment of the Fiscal Year 2023 NDAA. Even with that, the volume of components (especially DMSMS parts) will make it difficult or impossible to eliminate China as part of the supply base. This means that testing of foreign sourced electronics is expected to increase.

For the 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.

The U.S. Defense Logistics Agency (DLA) has defined standards, such as AS6171, but adoption across the defense industry is slow and inconsistent, primarily left to defense industry prime contractors to proactively determine testing thresholds and applicability. Adoption beyond DoD programs to other U.S. critical infrastructure applications is uncommon and not yet required.

Research and Development Initiatives

Other methodologies being explored to determine if chips are authentic is via embedded hardware security primitives and sensors (does not apply to passive electronics). Hardware-based security primitives employ instance-specific and process-induced variations in electronic hardware as a source of cryptographic data. Hardware primitives include physical unclonable functions (PUFs) and true random number generators (TRNGs) to produce device-specific electronic fingerprints and random digital signatures. These fingerprints and signatures are used to generate cryptographic keys and IDs commonly used for device authentication, cloning prevention, etc. (Blyler, Staggering Chip Shortages Have Led to Counterfeit Tech. Can't We Test for Fakes?, 2021)

Research into more sophisticated chip fingerprinting and validation is important to the future of component authentication, however there is still far to go to achieve a consensus across the semiconductor industry, the vast majority of which are outside of the U.S. Furthermore, even if such a consensus was reached, it would be years before it would affect most of the current obsolete and diminished material supply.

According to Dr. Williams at SMT Corp., "For electronics PUFs and TRNGs, and similar concepts such as DNA marking to be a viable counterfeit mitigation solution, it will require buy-in from the entire electronics components industry. Such a broad, industry wide agreement will only be feasible if mandated and enforced by multiple governments. Typically, agreements of this scope and scale will take a considerable amount of time to be drafted and agreed upon. Additionally, to be successful,

manufacturers would have to be involved in DMSMS / obsolescence management, sharing, and confirming key information about unique ID markers (PUFs, TRNGs, etc.) so that third parties such as defense contractors, counterfeit mitigation testing labs, and component distributors would be able to use this shared information to detect counterfeit electronic components. Historically, original manufacturers have been reluctant to be involved in counterfeit mitigation efforts as from their perspective there is no financial incentive to support such efforts and there is only potential liability from their involvement."

Conclusions and Recommendations

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, national security, and safety threat. As has been previously noted, electronics authentication standards exist, but are primarily applied to 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. In the near term, a comprehensive approach to counterfeit mitigation in the U.S. supply chain needs to consider sourcing, testing and risk avoidance.

Protecting U.S. infrastructure and avoiding the risk of counterfeit electronic parts in the supply chain necessitates consideration of the zero-trust policy being evaluated by DoD, which would assume no microelectronics are safe and all must be validated – as reported by Defense News in December 2022 (Gould, 2022). This entails allowing microelectronics into the supply chain only if testing demonstrates component authenticity, that there are no exploits built into them, and that they meet all requirements – including performance over environmental extremes. A zero-trust policy targeting components of unknown origin, and parts from regions where counterfeits are known to be active, is a prudent consideration.

About SMT Corp. *(https://smtcorp.com/)**:** SMT Corp., located in Sandy Hook Connecticut, is an AS6081 / AS6171 accredited and industry recognized expert with full on-site sourcing, authentication, and electrical testing services to mitigate the risk of counterfeit, cloned, altered, or substandard products from entering the Aerospace and Defense industry critical supply chain.*

References

Acqusition.Gov. (2019). *Section 889 Policies.* Retrieved from Acquisition.GOV: https://www.acquisition.gov/Section-889-Policies

Akhoundov, D. (2022). *2022 Annual Report*. Retrieved from ERAI Blog: https://www.erai.com/erai_blog/3181/_2022_annual_report

Blyler, J. (2020, March 12). *Dangers of Counterfeit Semi Chips*. Retrieved from DesignNews: https://www.designnews.com/cyber-security/dangers-counterfeit-semi-chips

Blyler, J. (2020, June 30). *Threats to Chip Supply Chain Prompt Action.* Retrieved from DesignNews: https://www.designnews.com/design-hardware-software/threats-chip-supply-chain-prompt-action/gallery?slide=1

Blyler, J. (2021, August 4). *Staggering Chip Shortages Have Led to Counterfeit Tech. Can't We Test for Fakes?* Retrieved from DesignNews: https://www.designnews.com/electronics/staggering-chip-shortages-have-led-counterfeit-tech-cant-we-test-fakes

Buchholz, K. (2021, August 17). *Chip Production Shifts Away From Traditional Strongholds*. Retrieved from Statistica: https://www.statista.com/chart/25552/semiconductor-manufacturing-by-location/

Cohen, R. S. (2022, September 13). *An F-16 pilot died when his ejection seat failed. Was it counterfeit?* Retrieved from AirForce Times: https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/

Collins Aerospace. (2020, Novermber 20). *The Evolution Of The ACES Family Of Ejection Seats*. Retrieved from Collins Aerospace: https://www.collinsaerospace.com/what-we-do/Industries/military-and-defense/interiors/aces-5-next-generation-ejection-seat/aces-5-updates/articles/archive/2020/11/evolution-of-the-aces-family-of-ejection-seats/

Gnau, T. (2022, September 15). *AFRL concerned about alleged 'counterfeit' ejection seat parts, federal lawsuit contends.* Retrieved from Dayton Daily News: https://www.daytondailynews.com/local/afrl-was-concerned-about-alleged-counterfeit-ejection-seat-parts-federal-lawsuit-contends/W3XLBRJRPBCOZKAW6WGQDW4YKM/#:~:text=AirForceResearchLaboratoryAFRLinvestigatorswereconcerned,federal

Gould, S. L. (2022, December 5). *Fake parts: A Pentagon supply chain problem hiding in plain sight.* Retrieved from DefenseNews: https://www.defensenews.com/pentagon/2022/12/06/fake-parts-a-pentagon-supply-chain-problem-hiding-in-plain-sight/

MarketWatch. (2023, April 20). *Global Electronics Market 2023-2030: Size and Forecast*. Retrieved from MarketWatch: https://www.marketwatch.com/press-release/global-electronics-market-2023-2030-size-and-forecast-2023-04-20#:~:text=Asof2022theglobalElectronicsmarketwas,aCAGRof5.5duringtheforecastyears

SAE International. (2018, April 18). *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts AS6171.* Retrieved from SAE Aerospace Standard AS6171: https://www.sae.org/standards/content/as6171/

Senate Armed Services Committee. (2012, May 21). *SENATE ARMED SERVICES COMMITTEE RELEASES REPORT ON COUNTERFEIT ELECTRONIC PARTS.* Retrieved from Untied States Sentate Committee on Armed Services: https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

Straits Research. (2023). *Electronic Components Market*. Retrieved from Straits Research: https://straitsresearch.com/report/electronic-components-market