Michael Schwarm
Chief Growth Officer, SMT Corp
mschwarm@smtcorp.com

Evolution of the Counterfeit Electronics Part Threat
Since SASC investigation of 2011/2012
July 25, 2024

In 2011, the Senate Armed Services Committee (SASC) launched an investigation into counterfeit electronic parts in U.S. defense systems [1]. Several instances were investigated, all of which were relatively simple remarked counterfeit electronic parts, which are parts that have been remarked to appear as a new or different part. The SASC investigation resulted in several actions by the Department of Defense (DOD) including flow-downs to DOD contracts requiring a counterfeit electronic parts mitigation plan. Since the end of the SASC investigation in 2012, the threat of counterfeit electronic parts has evolved. More complex remarking techniques and cloned parts have become prevalent. While some defense contractors have embraced standards that specify more effective counterfeit detection techniques, the defense industry at large has not converged on an agreed set of authentication testing standards for counterfeit parts mitigation. Furthermore, as counterfeit detection testing is an additional cost to companies, decisions on the level of testing, and the testing lab, are often based on price and turnaround time, and not the quality and reputation of the test lab.

During the SASC investigation, several cases of discovered counterfeit electronic parts were investigated. All were simple remarked parts sourced from the "open market", i.e. not the original manufacturer or their authorized distributors. Simple remarked parts are parts that have been resurfaced and remarked. This process typically results in visual anomalies such as sanding marks, paint overspray, and other defects or inconsistencies that can be discovered with relatively straightforward research and external visual inspection techniques. Typical cases investigated by the SASC included the Color Multi-function Display unit on the C-27 which was found to have remarked Samsung memory chips [2]. The investigation determined that the counterfeit memory chips had a three times higher failure rate than authentic chips. A failure of this chip could have resulted in the display going blank during takeoff or landing. Two of the C-27s with these counterfeit parts were deployed to Afghanistan. Another case identified counterfeit EMI filters, used to prevent interference to the systems core functions, in the control unit of the FLIR (Forward Looking InfraRed) sensor used on the U.S. Navy SH6B Helicopter [3]. The FLIR sensor is used for navigation at night or in fog. A failure of this system could compromise navigation.

The SASC investigation resulted in heighted government and industry awareness. It also resulted in some policy actions for DOD contracts, specifically the requirement for DOD contractors to have a counterfeit parts mitigation plan (DFARS 252.246-7007). However, specific standards for counterfeit mitigation were not defined, even though those standards now exist and have been adopted by some defense contractors since. Meanwhile, examples of counterfeit parts continue to affect defense systems and other critical applications. In 2020, Air Force pilot "Lt. Schmitz ejected from his F-16, but a malfunction kept his parachute from opening. His fall to the ground killed him" [4]. AFRL determined his ejection system's Digital Recovery Sequencer (DRS) contained multiple counterfeit electronic parts. In 2022, counterfeit parts were discovered in U.S. nuclear plants, potentially increasing the risk of a safety failure, according to the inspector general of the federal nuclear industry regulator [5]. In 2023, a Florida resident pleaded guilty to trafficking in fraudulent and counterfeit networking equipment [6]. These products ended up in hospitals, schools, government agencies, and the military. Many of the products failed or otherwise malfunctioned, causing significant damage to their users' networks and operations.

Michael Schwarm
Chief Growth Officer, SMT Corp
mschwarm@smtcorp.com

To further exacerbate the risk, in the 12 years since the SASC investigation, the threat has evolved considerably, with more sophisticated remarking techniques, and clones. A cloned electronic part is a reproduction of a part by an unauthorized manufacturer that replicates the authorized manufacturer's part. It is significantly more difficult to detect than a remarked part. Cloned parts with simple logic devices began appearing in 2012. By 2016, clones of memory chips were frequently being discovered. By 2019, clones of microprocessor chips were being discovered. Recently, a company based in China released a clone of a XILINX FPGA (Field Programable Gate Array) [7]. FPGAs are prevalent in defense and other purpose-built systems and products to implement system specific functions. Recent headlines also highlight the increasing threat of clones with reports like "Former Exec accused of trying to clone the entire Samsung chip fab on Chinese soil" [8], and "China's Largest Chipmaker Copied TSMC's Chip Designs" [9].

To combat the increasing risk of counterfeit parts, there must be a new inflection point that considers the increased threat of counterfeit parts across the supply chain for critical systems used in defense, transportation, communications, energy, security, and medical applications. There are relatively straightforward actions that can be immediately taken. **First**, agreed standards for counterfeit avoidance and detection must be mandated for systems and products in critical applications. Some defense contractors have mandated SAE standards AS6081 for counterfeit avoidance and AS6171 for counterfeit detection, however adoption of the AS6171 testing standard is still mandated by less than half of all defense contractors. **Second**, testing labs performing counterfeit detection testing need to be accredited and periodically pressure tested by an independent authority. **Third,** counterfeit parts mitigation standards must be applied to parts procured from both the open market and "untrusted" sources including parts originating from China based manufacturers. Heightening awareness across government and requiring minimum standards to combat sophisticated counterfeit parts is necessary to address the 12-year gap since the SASC investigation concluded in 2012.

References:

[1] https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm

[2] https://www.armed-services.senate.gov/download/2011/11/08/slides

[3] https://www.armed-services.senate.gov/download/2011/11/08/slides

[4] https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/

[5] https://www.reuters.com/business/energy/counterfeit-parts-present-many-us-nuclear-power-plants-inspector-general-2022-02-10/

[6] https://www.justice.gov/opa/pr/ceo-dozens-companies-and-entities-charged-scheme-traffic-estimated-1-billion-fraudulent-and

[7] https://www.cnx-software.com/2023/06/21/fudan-micro-jfm7k325t-is-a-clone-of-amd-embedded-kintex-7-325t-fpga/

[8] https://www.theregister.com/2023/06/12/samsung_china_chip_fab_clone/

[9] https://wccftech.com/chinas-largest-chipmaker-copied-tsmcs-chip-designs-say-reports/