

## Attack of the Clones: The Rise of Increasingly More Complex Clone Counterfeit Electronic Parts

Written by Jason Romano, Dr. Nicholas Williams, and Michael Schwarm

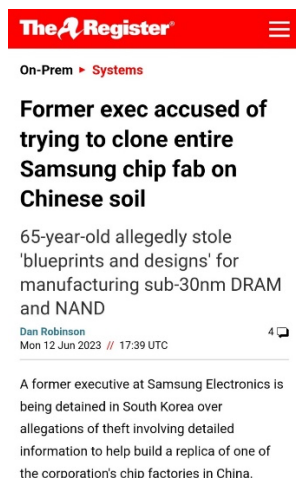
In 2012, the U.S. Senate Armed Services Committee (SASC) concluded a year-long investigation into counterfeit electronic parts. The investigation found that the total number of suspect counterfeit parts involved in the 1,800 defense case studies investigated exceeded 1 million. The investigation focused on counterfeit parts in U.S. Department of Defense applications and resulted in a Defense Authorization bill directive stating: “the Department of Defense and its contractors must attack this problem more aggressively, particularly since counterfeiters are becoming better at shielding their dangerous fakes from detection.”

Since the SASC investigation 12 years ago, more sophisticated types of counterfeit electronic parts such as cloned, complex semiconductor chips originating from China, have been detected. These types of counterfeits have become increasingly more common and difficult to detect compared to simple, remarked counterfeit parts.

### What is a Cloned Electronic Component?

Counterfeit “clones” are components manufactured by an unknown source which are fraudulently marked, packaged, and misrepresented to be factory-original devices. There are many ways to clone an electronic part including reverse engineering, IP theft, and recreating the functionality of the original device.

There are numerous reported instances of stolen chip designs and manufacturing blueprints that could have been used to enable clone counterfeit electronic components to be produced in China. These examples include employees stealing designs from ASML, TSMC, and Samsung.



**The Register**

On-Prem ▶ Systems

### Former exec accused of trying to clone entire Samsung chip fab on Chinese soil

65-year-old allegedly stole 'blueprints and designs' for manufacturing sub-30nm DRAM and NAND

Dan Robinson  
Mon 12 Jun 2023 // 17:39 UTC

A former executive at Samsung Electronics is being detained in South Korea over allegations of theft involving detailed information to help build a replica of one of the corporation's chip factories in China.

#### CHIP WATCH



DESIGN > HARDWARE

#### ASML Says Ex-Employee in China Stole Chip Data

The theft of technical data occurred in the last couple months. Tensions between US and China are high amid espionage claims.

Bloomberg News | Feb 15, 2023

### China's Largest Chipmaker Copied TSMC's Chip Designs Say Reports

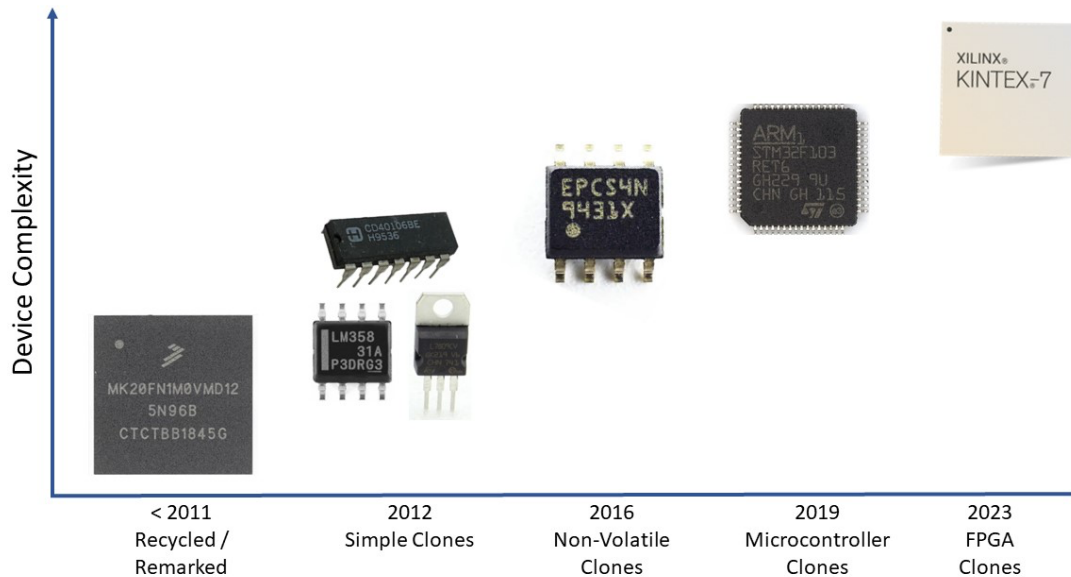
Ramish Zafar · Jul 24, 2022 08:18 AM EDT



While the most common incentive for cloning electronic parts is financial, the potential exists for more nefarious reasons such as introducing trojans that could be used as backdoors or to intentionally sabotage a system or product.

## The Evolving Threat of EEE Counterfeit Parts

In the years since the SASC investigation, SMT Corp, a leader in counterfeit electronic parts detection, has discovered and reported on increasingly more sophisticated instances of cloned electronic components. The following illustration depicts the evolution of counterfeit electronic parts since 2011.



As early as 2012, SMT Corp detected a relatively simple clone microcircuit, a Maxim Integrated RS-232 driver. Since then, the types of clones detected have become more complex and have included serial configuration devices, memory devices, and microcontrollers. Furthermore, it is well known that clones of complex FPGAs currently exist, manufactured by Chinese state-owned companies.

## Counterfeit Electronic Parts Detection

SAE standard AS6171 defines various test and inspection methods that support the detection of non-conforming electronic parts. Per AS6171, the Counterfeit Defect Coverage (CDC) across all counterfeit types (e.g. remarked, recycled, cloned), using the example of an active complex component is 87%, excluding “design recovery”. The most impactful methods to the overall detection score are external visual inspection, decapsulation/die verification, and electrical testing at ambient temperature. However, AS6171 assigns a much lower probability of defect detection, specifically as it relates to clone counterfeit parts. This is mostly based on the presumption that defects are much less detectable in cloned parts as opposed to remarked parts. While this is generally true as it relates to clones, many recent examples of testing performed by SMT Corp have demonstrated the ability to detect defects in cloned parts with more rigorous testing.



24 March 2024

For example, RAMAN spectroscopy provides the capability to identify the chemical structure of compounds. Using this method, encapsulate material composition and ink markings can be analyzed against known good data. In addition to RAMAN, Fourier Transform Infrared Spectroscopy (FTIR) uses infrared light to create a unique fingerprint of a devices chemical structure. This information can be used to compare device packages to known good device data, which has the potential to expose the use of resurfacing material or different encapsulate material.

Electrical testing of components is a valuable tool for both device authentication and to detect quality defects. Test sequences per AS6171 include electrical functional testing, which consists of applying a stimulus to a device and verifying the correct output, and electrical parameter testing, consisting of electrical parameter measurements. More comprehensive electrical testing for the detection of advanced counterfeit electronic parts and quality screening includes electrical parameter testing over temperature, temperature cycling, and burn in. Both temperature cycling and burn in can be used to expose quality defects and subpar semiconductor manufacturing in counterfeit material, as such material will often fail when stressed to the operating limits. Other environmental screening tests including leak testing and mechanical acceleration can also expose manufacturing flaws in fake parts.

### **Improving Complex Counterfeit Electronic Parts Detection**

There are several policies that could be further implemented or refined to improve counterfeit electronic parts avoidance and detection. For example, the adoption of accepted minimum industry standards such as AS6171 test methods for detection of complex clones, along with an integrated sourcing approach based on AS6081A. Also, independent pressure testing of authentication and test labs, similar to how the FBI exercises a TSA checkpoint, should be considered. Open market sourcing is not just a problem for defense and aerospace, and as such, counterfeit mitigation policies should be applied to other critical infrastructure industries such as medical, financial, energy, and transportation. For example, in 2019, SMT Corp detected a cloned microcontroller used in a point-of-sale (POS) device. This device is used for encrypting/decrypting financial information on debit and credit card transactions. Microcontroller clones create the potential for trojans (hidden memory sectors or built-in sub-routines) that could allow third parties to extract data from systems via network interface. Additionally, given that open market sourcing is sometimes unavoidable due to parts obsolescence, and current standards are not guaranteed to detect counterfeit parts, there needs to be a review of reporting and liabilities to promote a more collaborative approach across industries to improve counterfeit avoidance and detection methods.

About SMT, Corp

SMT Corp is the industry leader for sourcing & authentication of DMSMS and hard-to-find electronics components, electrical testing services, and inventory management solutions. SMT Corp is a highly accredited and recognized expert with full on-site sourcing (AS6081), authentication (AS6171), and electrical testing to mitigate the risk of counterfeit, cloned, altered and substandard products from entering the critical infrastructure supply chain.

<https://smtcorp.com/>



24 March 2024

## About Certify Holdings

Certify Holdings is a full lifecycle strategic partner for the defense and aerospace market, and other markets requiring high reliability electronic solutions. Certify Holdings supports our customers through the early project design stage with design-in support leveraging a wide range of Hi-Rel and RF electronic modules and components, throughout production with sourcing and distribution services, and into obsolescence / end of life with sourcing and authentication of hard-to-find electronics. Throughout the project lifecycle, Certify Holdings supports our customers with test solutions and services. <https://certifyholdings.com/>