Electronic Component Authenticity via Electrical Signal Measurement and Artificial Intelligence with Deep Learning

Yung-Hsiao (Steven) Chung, Global ETS-USA
steven@gets-usa.com
Feng Yu, Global ETS-USA
Junjie Xiong, University of South Florida
Stephen E. Saddow, University of South Florida
saddow@usf.edu

Counterfeit electronics are both an extremely serious and common issue in the global systems supply chain which increases the risk of critical system errors and failure which can even be life-threatening. Systems affected range from modern mobile devices (cell phones, tablets, etc.), computers and laptops, medical diagnostic and treatment systems, air traffic control and GPS systems, etc. Critical systems have a long-life cycle and often use obsolete 'legacy' devices which makes them a target for counterfeit parts due to economic reasons. For example, reproducing legacy parts is both expensive and time consuming due to advances in the manufacturing chain that made these parts obsolete in the first place. In addition, using obsolete parts often leads to quality conformance issues even if the part is legitimate since some of the electronics might have been sitting on the shelf for over 20 years.

Purchasing electronic parts directly from part manufacturers and their authorized suppliers is the lowest risk step in the procurement of parts for critical systems. However, for various reasons, such as obsolete parts, short lead times, etc., parts are often purchased from unauthorized sources or brokers. This alone may put an entire system that uses the replacement part at risk.

Some manufacturers create an ID code in the device memory or micro-controller to prevent counterfeit electronics from being inserted into critical systems. This ID code is a serial binary code stored in an un-erasable or unchangeable register. Users must use technical ways such as JTAG, SPI or I2C to find this information. Such actions are usually performed by professional engineers and require extra setup and lead time.

Global's Advanced Pin Correlation system is an easy and convenient tool for performing quality conformance and counterfeit IC (integrated circuit) detection based on our deep learning model system using neural networks. This authentication system first conducts a quick open/short circuit check, leakage current check and supply current check to make sure all readings are within specification. Then it uses a matrix scan approach to scan from pin to pin to get physical characteristics (impedance based) which are processed and fed into our deep learning system to train our model, which is capable of producing the corresponding golden chip library. IC's usually have multiple pins that serve as electrical inputs/outputs and connect to the system through a printed circuit board. Due to this physical setup, it is rather simple to construct an

automated test and diagnostic system to rapidly scan between pins thus forming an ‘electronic signature’ of the device under test (DUT). The automatic test would first transfer the scanned data to the diagnostic System and then speculate on the appropriate model to formulate its electronic signature. This is then rapidly compared to a known good device (KGD). Consequently, fast assessment of the authenticity of the part is thus possible.

Although it is still not considered as functional testing, qualified personnel can perform quick screen testing using this system without a strong electronics background thus saving a lot of time and money to set up and develop a testing method for microelectronics. Our approach offers two principal benefits:

1. Rapid ‘signature-based’ identification of a part to determine its authenticity, and
2. Reduced-skilled operators vs. highly skilled electronics experts that both increases measurement cost and slows down part assessment.

After the introduction of the deep learning model, automated golden-chip library vs. a manual and empirical library improves library universality and speeds up library creation, minimize the risk of manual error. In this paper we will present compelling data for our novel method to rapidly and accurately assess electronic device authenticity using AI and Deep-Learning signature analysis.