Securing Microelectronic Supply Chains with Dendritic Identifiers

Michael N. Kozicki

Arizona State University
Electrical, Computer and Energy Engineering
Tempe, AZ, USA
kozicki@asu.edu

Densec ID, LLC
Hardware Technology Development
Phoenix, AZ, USA
michael@densecid.com

To combat the problem of counterfeit microelectronic components, industry and government organizations are developing standards and guidelines for detecting and preventing their use. These efforts require the adoption of technologies and controls to ensure the authenticity and traceability of electronic parts throughout the supply chain. The security and efficiency of distributed ledger technologies (DLTs) such as blockchain make them highly attractive for handling information in product protection schemes, but the database is only one aspect of the digital identity dyad. Items in manufacturing supply chains must also have a physical element that connects them to their presence in the Cloud, usually via some form of digital trigger. In non-integrated circuit (IC) applications, these triggers are often QR codes or RFID tags, but neither of these are appropriate for the individualized and secure tracking of ICs; QR codes are too easily replicated, and radio tags do not have a suitable form factor for ICs and small components. Our development work has therefore focused on a machine readable digital trigger that is compatible with ICs and other parts, the Dendritic Identifier (DI). This trigger is naturally item-unique without the effort associated with individualization, secure enough to resist replication and tampering, and sufficiently inexpensive and scalable to allow it to be deployed on most parts. In a typical use scenario, one or more DIs would be applied directly to IC packaging elements or other components at trusted points in the manufacturing process, and, depending on the use case, either removed when safe to do so or remain with the product to permit security and traceability to end-of-life.

This talk will describe the benefits of dendritic topologies as item-level "fingerprints", including their high information entropy coupled with a low structural entropy which makes them both unique and digitally robust. It will also describe a simple and inexpensive "direct to object" formation method based on the Saffman-Taylor instability in polymer mixtures and metallic inks and will demonstrate computer vision-based approaches to pattern reading. Examples of the use of the technology on components used in IC packaging will also be given.