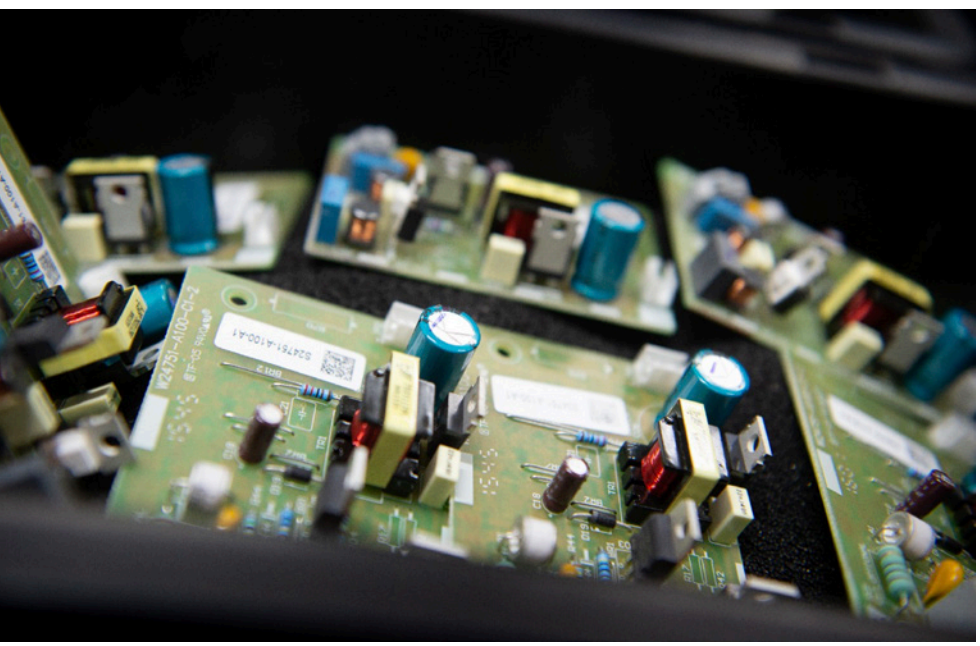
Next-Gen **Components Traceability** Prevents Damage from Cyberattacks and Counterfeits or Refurbished Components

BY TOVI YADIN, SIEMENS DIGITAL INDUSTRIES SOFTWARE



Did you lately try to purchase a new car, a new laptop, or a new phone, and you were told by the seller that you will need to wait for a few months because there are delivery issues?

We are now two years into the COVID pandemic, and even as the effects of the virus wind down, the lockdowns and slow-downs worldwide have been affecting the manufacturing and transport of electronic goods. And why is it still happening? According to EPSNews [1], the effect of Covid-19 on the production of components will inflict an even more severe shortage than the 2017–2018 crisis.

The entire market of electronics goods depends on the availability of the small building blocks of the PCB: the electronic components. When there is a shortage of electronic components, it acts like a snowball on the entire supply chain, thus affecting the availability of the final goods. People are waiting for months for their new cars, laptop, washing machines, or cell phones—all because of missing a small chip from the stock.

As a result, the gray market of counterfeit and refurbished components has become an even greater issue than it was before. When there is a vacuum of components, someone will see this as an opportunity and fill the gap. Of course, Electronic Manufacturing Suppliers (EMS) cannot take the risk of using counterfeit, refurbished, or non-authorized components. But until now, they did not really have a proper, scalable, and reliable way to ensure that their entire supply chain is authentic.

Of course, there were some methods to minimize the exposure to problematic components. But none of them could really solve the issue.

The first thing that OEMs did was to buy only from approved and known component suppliers. However, this was not enough. It still did not guarantee that all components were indeed authentic. In some cases, the supplier was unaware that the component they are selling is problematic. But more than that: in a period of low availability of components, limiting the supply chain manager to buy only from a small approved-supplier list made just-in-time supply more difficult.

The second method was to send the reel to a lab for testing. But this could not solve the entire issue. In the lab, the test is done only on a sampling. And in most of the cases, counterfeit is done in a sophisticated way that cannot be found when sampling just a single reel.

So, there are counterfeit components in our products. But why is this an issue? In many cases, the product's performance parameters will deteriorate, affecting lifetime, resilience, sensitivity to the environment, load, etc. Counterfeit components can cause unpredictable and random statistical failures that are extremely difficult to detect by conventional acceptance tests. They are difficult to pinpoint and are often dismissed as workmanship issues.

Random and evident failures are responsible for more than 30% of product recalls. In about 70% of the cases, a rework of the faulty component fixes the product but misdiagnoses the inferior counterfeit soldering leads with assembly workmanship.

Current mitigation is to buy components only from trusted sources or t0 send components to labs. Lab testing is expensive and slow, as well as ineffective

because only small samples (~0.1%) are tested when batches are a mix of authentic and fraud components.

Many manufacturers are unaware of the extent of counterfeit components in their supply chain. They may encounter statistical failures later in the product life cycle that will be written off as the "cost of doing business" when this cost can be easily avoided by good traceability methods and tools. Counterfeit materials may trigger statistical failures at any point in the product lifecycle. In some cases, the failures may lead to costs and penalties associated with Return Merchandise Authorization (RMA).

When an engineer sees a problem, he creates a solution. Several years ago, Dr. Eyal Weiss managed an extensive technological development project that included sensors, algorithms, and complex electronics manufacturing for an Israeli-based company. Everything seemed fine—but the system was not working.

"Although all the tests showed that the system was working properly when field trials began, there were inexplicable glitches that we could not locate," said Weiss.

After four months of searching, the problem was revealed: ceramic capacitors (MLCC) that were thought to be new actually came from a 10-year-old component reel.

"A project worth a billion dollars was almost canceled due to a simple capacitor costing just 3 cents. The production was done by a large and well-known Israeli company. The components were purchased from authorized suppliers. The documentation was correct—but the capacitor was a fake," explained Weiss.

Following this experience, he realized that a way must be found to test each component before it reaches the production line. It was a natural direction for Weiss to develop an AI-based, big-data–powered software to manage real-time detection of malicious code-infested and counterfeit components. This was how Cybord.ai came to life. Cybord's solution scans 100% of the components during assembly without delays, ensuring that only authentic, fresh, and untampered components are used in a product.

Counterfeit components can cause unpredictable and random statistical failures that are extremely difficult to detect by conventional acceptance tests. They are difficult to pinpoint and are often dismissed as workmanship issues.

Using AI-based image processing, which leverages data that is already collected by the pick-and-place machines, the materials traceability solution can immediately identify counterfeit components on the line. The system also provides a detailed report that can be used to make various decisions regarding quality, conformance, and sourcing.

The company participated in Siemens Dynamo [2], an open innovation program from Siemens Digital Industries Software in Israel. The Dynamo program brings manufacturing innovation from emerging companies to Siemens customers and partners. Selected companies work closely with Siemens relevant experts to develop a joint commercial offering within a 12-month timeframe.

As a result, Cybord's traceability solution [3] is now part of Siemens manufac-

turing analytics solution and is included in the Xcelerator program, which aims to provide specialized solutions for various challenges specific to electronics manufacturing, using advanced technologies such as artificial intelligence and machine learning.

The traceability solution supplies sets of reports and analytics to help the EMS factory quality manager/supply chain manager ensure the quality of the components of every reel. Specific reels on production can be blocked if the solution finds that it has too many problematic components. These reports can be given to suppliers when problem components are found.

This assurance also enables the supply chain manager to include more suppliers, which is essential in these challenging times of component shortages. With a comprehensive traceability program in place, collaboration with suppliers is enhanced by the knowledge that 100% of components are checked.

Product manufacturers can obtain an "as made" report for each assembled PCB, with full information on all the assembled components. In this way, full historical traceability data is recorded. If an issue is reported along the product lifecycle, it can be traced back to the components that were used to create it. The cost of recalls can be reduced when OEMs can identify the products that were assembled using parts from the suspect reels.

In today's environment, when the odds of coming across counterfeit, refurbished, or non-authorized components is higher, electronics manufacturers need solutions that enable a greater level of automated material traceability to ensure that only new, genuine, and unadulterated components are allowed into a product. This is why Cybord and Siemens Software worked together to bring this solution to market. Now both EMS and OEMs can have full transparency over the components they use, moving the supply chain state of mind from "100% trust" to "100% validation."

With a comprehensive traceability program in place, collaboration with suppliers is enhanced by the knowledge that 100% of components are checked.

RESOURCES

1. Barbara Jorgensen, "Component Makers Don't Expect a Q2 Recovery from Covid-19," *EPSNews,* https://epsnews.com/2020/03/11/component-makers-dont-expect-a-q2-recovery-from-covid-19/, March 11, 2020
2. *Siemens Dynamo + Cybord Collaboration,* https://www.youtube.com/watch?v=JMAVLH0VCnE
3. *How to Detect Defective Parts and Achieve Unprecedented Components Traceability with Predictive Analytics,* Siemens white paper, https://www.plm.automation.siemens.com/global/en/resource/defective-parts-detection-for-pcb-assembly-with-predictive-analytics/105382

Tovi Yadin is an Innovation Solutions Manager at Siemens Digital Industries Software. Tovi is passionate about leveraging advanced technologies such as AI and ML to optimize manufacturing and make the world a better place. She brings extensive expertise in electronic manufacturing processes and a strong business and technical background to her current role, where she focuses on smart manufacturing and Industry 4.0, promoting Siemens data-driven manufacturing initiative.