AI-Driven Secure Electronics Manufacturing: Detecting Counterfeit and Hardware Tampering

Dr. Eyal Weiss
Cybord
eyal.w@cybord.ai

The increasing sophistication of hardware-based cyber threats poses significant risks to the aerospace and defense sectors, where electronic component integrity is paramount. Traditional anti-counterfeiting methods, such as supply chain documentation and sample-based testing, often fail to provide real-time, full-coverage verification. This session introduces an AI-driven automated inspection framework that enhances the detection of counterfeit components, unauthorized modifications, and hardware tampering during manufacturing and deployment.

By integrating high-resolution imaging with deep learning anomaly detection models, this approach systematically analyzes PCB assemblies at multiple stages. Bottom-side inspection during component placement identifies unauthorized firmware programming and counterfeit parts, while top-side verification ensures assembled boards remain unaltered. With a 99.3% detection accuracy, this AI-driven solution outperforms conventional X-ray imaging and manual verification, offering a scalable, real-time security layer for high-throughput production environments.

This session will present real-world case studies, demonstrating how AI-based verification enhances supply chain security and mitigates risks associated with counterfeit and tampered components as well as cyber threats. Attendees will gain insight into the latest advancements in AI-driven inspection technologies and their critical role in securing military and aerospace electronics against emerging hardware-based attacks.