From Quality Inspection to Hardware Security Verification

Eyal Weiss, Ph.D.
Cybord inc.
NY, USA
Eyal.w@cybord.ai

ABSTRACT
The integrity of electronic assemblies is increasingly threatened by counterfeit components, unauthorized modifications, malicious substitutions, and hardware-based cyberattacks. Traditional mitigation strategies rely primarily on supply-chain documentation, sample-based testing, regulatory compliance, and post-deployment security controls. These approaches provide limited visibility into the actual hardware incorporated into electronic systems.

This paper presents an AI-driven inspection framework that transforms manufacturing inspection infrastructure into a hardware security verification platform. The proposed approach combines bottom-side component inspection during placement with top-side inspection of assembled printed circuit boards to identify hardware tampering events including counterfeit devices, remarked components, unauthorized programming, component substitutions, unexpected additions, and assembly modifications.

The framework leverages large-scale manufacturing imagery and deep-learning models trained on billions of component observations collected from production environments. By correlating visual observations with manufacturing context including approved vendor lists, traceability records, and engineering definitions, the system generates evidence describing component authenticity, provenance, compliance, and assembly integrity.

Industrial examples demonstrate detection of multiple classes of hardware threats directly from production imagery. The results suggest that existing manufacturing inspection infrastructure can serve not only as a quality control mechanism but also as a practical cybersecurity control capable of identifying compromised hardware before deployment.

Key words: Hardware Security, Cyber Threats, Counterfeit Components, AOI, SMT Inspection, Artificial Intelligence, Hardware Assurance.

INTRODUCTION
Modern electronics manufacturing has become one of the world's most automated production environments. Every board, component, and manufacturing step generates digital information intended to improve quality, traceability, and productivity. Cybersecurity has traditionally focused on software vulnerabilities, network attacks, identity management, and system access control [1], [2]. In contrast, the physical hardware underlying modern electronic systems has received comparatively limited attention [3], [4], [5], [6], [7]. As a result, many security architectures implicitly assume that the deployed hardware corresponds to the intended design and that the electronic components incorporated into a system are authentic, authorized, and uncompromised.

Recent incidents involving counterfeit semiconductors, unauthorized component substitutions, malicious hardware modifications, and supply-chain attacks have challenged this assumption [8], [9]. Hardware-based attacks can introduce vulnerabilities before software is installed, bypass traditional security controls, and remain difficult to detect throughout the operational life of a product.

At the same time, modern electronics manufacturing environments generate enormous quantities of inspection data. Automated Optical Inspection (AOI) systems, placement machines, board scanners, and traceability platforms continuously capture detailed observations of electronic components and assemblies. These systems were originally designed to support quality assurance, process control, and process defect detection. However, they also provide a unique opportunity to verify the physical integrity of hardware before products leave the factory.

This paper explores the use of manufacturing inspection data as a security verification mechanism. Rather than treating

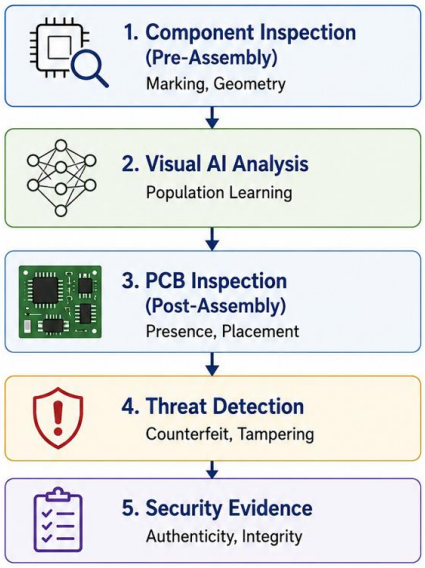


Figure 1. AI-based hardware verification framework integrating component-level and assembly-level inspection data.

inspection solely as a quality activity [10], [11], [12], [13], [14], the proposed framework leverages production imagery and artificial intelligence to identify hardware threats directly from the physical characteristics of electronic assemblies. As illustrated in Figure 1, hardware trust is established through multiple verification stages spanning the manufacturing lifecycle, from incoming material inspection to final system integration.

HARDWARE THREATS IN ELECTRONIC ASSEMBLIES

Hardware threats manifest in multiple forms throughout the electronics supply chain. Counterfeit devices represent one of the most widely recognized categories and may include cloned components, refurbished devices, remarked parts, or products manufactured outside authorized supply channels [15], [16], [17], [18], [19], [20]. Although such devices may initially appear functional, they often introduce reliability risks, hidden defects, or unknown origins.

Another important category involves component substitution. A component may be replaced with an alternative device that differs from the approved design, potentially altering system functionality, reliability, regulatory compliance, or security characteristics. Similar concerns arise when unexpected components are added to a design or when authorized components are removed during manufacturing or repair processes [21], [22], [23].

More sophisticated attacks may involve unauthorized programming or manipulation of programmable devices [11], [24]. Firmware modifications, configuration changes, and reprogramming events can introduce malicious functionality while preserving the outward appearance of the original hardware. In other cases, piggyback devices or covert modifications may be introduced to create hidden communication paths, monitoring capabilities, or backdoor access mechanisms [25], [26].

Although these threats differ technically, they share a common characteristic: they alter the physical state of the hardware. Consequently, they create observable evidence that may be detected through inspection and analysis of manufacturing imagery. Unlike software attacks, these threats become embedded in the physical product itself and therefore cannot be corrected through software updates alone.

AI-BASED HARDWARE VERIFICATION FRAMEWORK

The proposed framework is founded on the hypothesis that semiconductor manufacturing, package assembly, laser marking, plating, molding, and final test collectively produce stable physical signatures that remain observable throughout the component lifecycle [27], [28], [29]. Although these signatures are generated as a byproduct of manufacturing rather than for security purposes, they form statistically consistent visual populations that can be learned from large-scale manufacturing data. Hardware tampering, counterfeit production, unauthorized substitutions, and remarking disturb these populations, producing measurable deviations from expected manufacturing behavior.

Unlike conventional machine vision systems that detect predefined defects, the proposed framework models the statistical distribution of authentic manufacturing populations. Rather than learning individual attack classes, the system learns the normal variability of legitimate hardware. Counterfeit devices, unauthorized substitutions, remarked components, and modified hardware are subsequently detected as statistically significant deviations from these learned populations.

Inspection is performed at multiple stages throughout the manufacturing lifecycle (Figure 1). Component-level observations are first acquired during incoming inspection and placement using high-resolution bottom-side imagery. Figure 2 illustrates the proposed population-based learning architecture. Additional observations are collected after assembly using AOI systems and board scanners, allowing verification of component identity, placement, orientation, and assembly integrity. Acceptance verification compares the received product against the manufacturing baseline, providing evidence that the hardware has not changed between production and deployment.

Each inspected component is transformed into a manufacturing signature derived from complementary geometric, optical, semantic, and contextual descriptors. This

representation serves as the basis for population-level comparison and hardware assurance reasoning.

$$S = f(F_g, F_t, F_m, F_c);$$
$$A = g(S, C);$$

where S denotes the manufacturing signature extracted from the observed component, A denotes the resulting hardware assurance evidence, F_g represents geometric features including package dimensions, lead geometry, body shape, and pin configuration, F_t describes surface texture and optical reflectance characteristics, F_m represents semantic marking information including decoded text, logos, font morphology, and character layout, F_c represents component-specific manufacturing characteristics, and C denotes the manufacturing context. Throughout this paper, *manufacturing context* refers to the collection of engineering and production information associated with a component, including BOM definitions, AVL constraints, supplier information, procurement records, traceability data, production history, and inspection metadata. The resulting manufacturing signature is subsequently compared against learned populations and fused with manufacturing context, as illustrated in Figure 2.

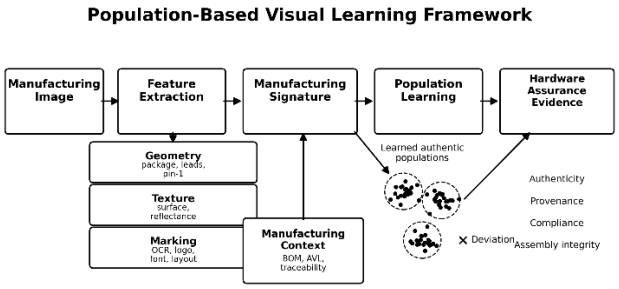


Figure 2. Population-based visual learning framework. Individual visual features extracted from manufacturing imagery are transformed into multidimensional embeddings and compared with learned populations of authentic components. Contextual manufacturing information is subsequently fused to generate hardware assurance evidence.

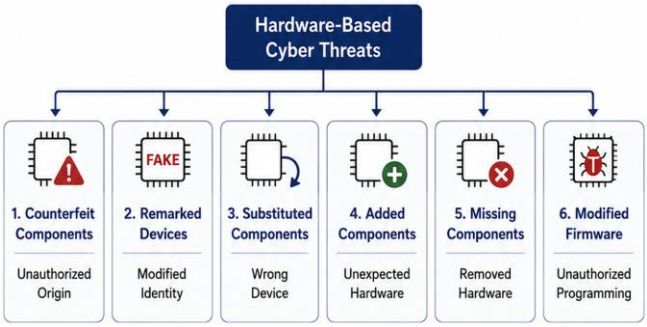


Figure 3. Representative hardware threat categories addressed by the proposed verification framework, spanning counterfeit devices, unauthorized modifications, substitutions, and firmware manipulation.

The framework combines multiple complementary population-based visual learning operating on independent visual and semantic representations. Dedicated models characterize package morphology, lead geometry, surface texture, optical reflectance, top-marking semantics, manufacturer logos, font morphology, and marking layout. Optical character recognition extracts textual information, while semantic interpretation resolves manufacturer-specific coding conventions. The resulting manufacturing signature is subsequently compared against learned authentic populations using statistical embedding models. Evidence generated by these independent models is fused to produce a unified hardware assurance assessment rather than relying on any single visual feature or classifier. Figure 2 summarizes the proposed population-based visual learning methodology.

Unlike traditional defect classification, the objective is not to recognize known defects but to model authentic manufacturing populations from which deviations become measurable indicators of hardware risk.

Population-based learning plays a central role in the proposed methodology. The training dataset consists of billions of component observations collected from production environments spanning multiple manufacturers, package families, date-code ranges, production facilities, and inspection systems. This diversity enables the learned representations to capture normal manufacturing variability while remaining sensitive to subtle deviations introduced by counterfeit production, remarking, unauthorized substitutions, refurbishment, or hardware modification.

The generated visual evidence is subsequently correlated with manufacturing context including engineering definitions, BOMs, approved vendor lists, traceability records, procurement information, and production history. This contextual reasoning transforms low-level visual observations into structured hardware assurance evidence describing provenance, authenticity, compliance, and assembly integrity. Instead of asking whether a specific defect is present, the framework evaluates whether the observed hardware remains statistically and contextually consistent with the product that was intended to be manufactured.

LARGE-SCALE MANUFACTURING DATASET

The proposed methodology was developed using a manufacturing dataset containing billions of component observations collected from high-volume electronics production. The dataset spans multiple AOI platforms, placement systems, package families, semiconductor manufacturers, illumination conditions, production facilities, and geographic regions. This diversity enables the learning process to model manufacturing variability itself rather than equipment-specific image characteristics.

The scale of the dataset is important because many hardware threats become observable only when evaluated relative to large populations of authentic devices. Population-based learning enables the method to distinguish normal manufacturing variability from anomalies associated with

counterfeit devices, unauthorized substitutions, and other forms of tampering.

INDUSTRIAL CASE STUDIES

Several industrial examples illustrate the application of the proposed framework to real-world hardware threats. Figure 4 presents an example of a remarked component identified through analysis of marking characteristics and population-level comparisons. Although the textual content appeared consistent with documentation, deviations in marking execution and physical appearance revealed evidence of modification.

Figure 5 presents an unauthorized component substitution identified through comparison between observed component identity and engineering requirements.

Figure 6 demonstrates assembly-level analysis in which an unexpected component was identified within an assembled board. Such observations may indicate manufacturing errors, unauthorized modifications, or undocumented design changes.

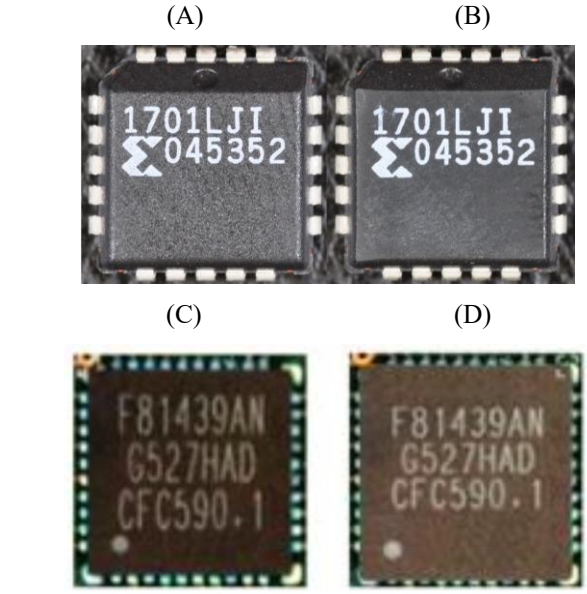


Figure 4. Example of a remarked component identified through visual analysis. (A) Authentic, (B) Black-topped, (C) Remarked, (D) Authentic.

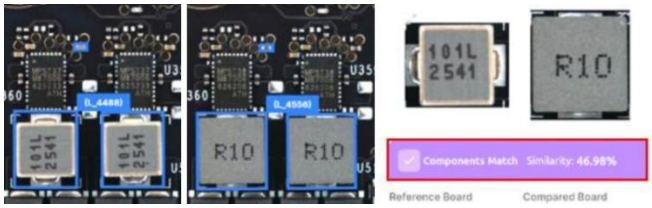


Figure 5. Unauthorized component substitution detected through comparison between the observed component identity and the engineering reference.



Figure 6. Detection of an unexpected component within an assembled PCB assembly. In the example an MLCC capacitor was mounted instead of a resistor.

Collectively, these examples demonstrate that multiple categories of hardware threats can be detected directly from manufacturing inspection data before products enter service.

DISCUSSION

Traditional manufacturing inspection systems were designed to identify defects, verify assembly quality, and support process control. The results presented in this work suggest that the same infrastructure can also function as a security sensor capable of detecting hardware-based cyber threats.

The proposed methodology does not replace conventional inspection or cybersecurity mechanisms. Instead, it introduces an additional evidence layer that directly links physical hardware observations with engineering intent. By continuously validating that the assembled hardware remains consistent with both manufacturing populations and engineering definitions, the framework extends hardware assurance beyond documentation and traceability alone.

Unlike sample-based testing approaches, manufacturing inspection enables verification at production scale. Every component and every assembly can be evaluated using the same inspection infrastructure already deployed within electronics manufacturing facilities. This capability provides a practical path toward continuous hardware verification without introducing significant disruption to existing manufacturing processes.

Unlike conventional quality inspection, which primarily evaluates manufacturing correctness, hardware security verification evaluates hardware trust. This distinction shifts inspection from identifying defects to establishing evidence regarding authenticity, provenance, compliance, and integrity throughout the manufacturing lifecycle.

The findings also highlight the importance of combining visual observations with manufacturing context. Hardware threats frequently become apparent only when observed physical characteristics are compared against approved designs, sourcing requirements, traceability information, and historical manufacturing populations.

CONCLUSION

This paper presented an AI-driven framework for detection of hardware-based cyber threats during electronics manufacturing. By combining component-level and assembly-level inspection data with deep-learning analysis and manufacturing context, the proposed approach

transforms traditional inspection infrastructure into a hardware security verification platform.

Industrial examples demonstrated detection of counterfeit devices, remarked components, unauthorized substitutions, and assembly-level modifications using production imagery collected from real manufacturing environments. The results indicate that manufacturing inspection infrastructure can provide a practical and scalable mechanism for identifying compromised hardware before deployment.

The presented results demonstrate that manufacturing imagery contains substantially more information than traditional quality inspection requires. When combined with population-based visual learning and manufacturing context, these observations become measurable hardware assurance evidence capable of identifying counterfeit devices, unauthorized substitutions, and hardware modifications at production scale.

The future of hardware security may not begin after deployment. It may begin on the manufacturing line, where trust can first be established from the hardware itself.

REFERENCES

[1] P. Kumar and S. Verma, "IMPROVING THE RESILIENCE OF CYBER SECURITY DATA CENTERS TO CYBER-PHYSICAL ATTACKS," *International Journal of Management Research and Reviews*, vol. 15, no. 1, pp. 14–22, 2025.

[2] J. M. Boyens, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," 2024. doi: 10.6028/NIST.SP.800-161r1-upd1.

[3] M. Tehranipoor, N. Pundir, N. Vashistha, and F. Farahmandi, *Hardware security primitives*. Springer, 2023.

[4] M. Kucera and M. Vetter, "FPGA-rootkits hiding malicious code inside the hardware," *Proceedings of the 5th International Workshop on Intelligent Solutions in Embedded Systems, WISES 07*, pp. 262–272, 2007, doi: 10.1109/WISES.2007.4408497.

[5] X. Wang *et al.*, "Malicious firmware detection with hardware performance counters," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 160–173, 2016.

[6] W. Zhao, S. R. Gurudu, S. Taheri, S. Ghosh, M. A. M. Sathiaseelan, and N. Asadizanjani, "PCB Component Detection Using Computer Vision for Hardware Assurance," *Big Data and Cognitive Computing*, vol. 6, no. 2, Jun. 2022, doi: 10.3390/bdcc6020039.

[7] J. Mishra and S. K. Sahay, "Modern Hardware Security: A Review of Attacks and Countermeasures," *arXiv preprint arXiv:2501.04394*, 2025.

[8] D. Mehta *et al.*, "The big hack explained: Detection and prevention of PCB supply chain implants," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 16, no. 4, pp. 1–25, 2020.

[9] V. A. Greiman, "Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure."

[10] E. Weiss, "Electronic component solderability assessment algorithm by deep external visual inspection," in *2020 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, IEEE, 2020, pp. 1–6.

[11] E. Weiss, "AI Detection of Body Defects and Corrosion on Leads in Electronic Components, and a study of their Occurrence," in *2022 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, IEEE, 2022, pp. 1–6.

[12] E. Weiss, "Preventing Corrosion-related Failures in Electronic Assembly: A Multi-case Study Analysis," *IEEE Trans. Compon. Packaging Manuf. Technol.*, May 2023, doi: 10.1109/TCPMT.2023.3285776.

[13] E. Weiss, "Revealing Hidden Defects in Electronic Components with an AI-Based Inspection Method: A Corrosion Case Study," *IEEE Trans. Compon. Packaging Manuf. Technol.*, 2023, doi: 10.1109/TCPMT.2023.3293005.

[14] E. Weiss, "Detecting Corrosion to Prevent Cracks in MLCCs with AI," *Journal of Failure Analysis and Prevention*, 2023, doi: 10.1007/s11668-023-01824-3.

[15] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit integrated circuits," in *Counterfeit Integrated Circuits*, Springer, 2015, pp. 15–36.

[16] M. M. Tehranipoor, U. Guin, and D. Forte, "Electrical Tests for Counterfeit Detection," in *Counterfeit Integrated Circuits*, Springer, 2015, pp. 95–107.

[17] S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, and D. Masouras, "A review and classification framework of traceability approaches for identifying product supply chain counterfeiting," *Sustainability*, vol. 14, no. 11, p. 6666, 2022.

[18] L. W. Kessler and T. Sharpe, "FAKED PARTS DETECTION The counterfeiting of electronics components and related parts is widespread. But newly developed methods promise now to help identify counterfeit plastic-encapsulated components using detection methods that cannot be tricked. PLUS: ," *Printed Circuit Design & Fab*, vol. 27, no. 6, p. 64, 2010.

[19] a S. Report, "counterfeit parts : increasing Awareness and Developing countermeasures Counterfeit Parts : Increasing Awareness and," *T*, no. March, 2011.

[20] Semiconductor Industry Association, "Winning the battle against counterfeit semiconductor products," no. August, 2013, [Online]. Available: https://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA Anti-Counterfeiting Whitepaper.pdf

[21] G. M. Razak, L. C. Hendry, and M. Stevenson, "Supply chain traceability: a review of the benefits and its relationship with supply chain resilience," *Production Planning and Control*, vol. 34, no. 11, pp.

1114–1134, 2023, doi: 10.1080/09537287.2021.1983661.
[22] C. E. Shearon, “IPC-1782 standard for traceability of critical items based on risk,” in *2018 Pan Pacific Microelectronics Symposium (Pan Pacific)*, IEEE, 2018, pp. 1–3.
[23] E. Weiss and Z. Efrat, “High Resolution Traceability,” 2023
[24] K. Yang, H. Wang, and L. Sun, “An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks,” *Comput. Ind.*, vol. 138, p. 103613, 2022.
[25] J. Mishra and S. K. Sahay, “Modern hardware security: A review of attacks and countermeasures,” *arXiv preprint arXiv:2501.04394*, 2025.
[26] L. F. Ribas Monteiro, Y. R. Rodrigues, and A. C. Zambroni de Souza, “Cybersecurity in Cyber–Physical Power Systems,” Jun. 01, 2023, *MDPI*. doi: 10.3390/en16124556.
[27] E. Weiss, “Counterfeit mitigation by in-line deep visula inspection,” SMTA. [Online]. Available: http://iconnect007.uberflip.com/i/1440051-smt007-jan2022/87?
[28] E. Weiss, “Electronic Components Provenance Assurance Through AI and Big Data in Assembly Processes,” *IEEE Trans. Compon. Packaging Manuf. Technol.*, pp. 1–1, 2024, doi: 10.1109/TCPMT.2024.3482467.
[29] E. Weiss, “Secure Hardware Assurance Using Visual AI on AOI Imaging of Electronic Assemblies,” *Journal of Hardware and Systems Security*, vol. 10, no. 1, p. 3, Dec. 2026, doi: 10.1007/s41635-026-00173-5.