How Technology Advancements Are Accelerating the Proliferation of Counterfeit Electronic Components

A white paper on the convergence of compute-driven competition, supply volatility, and AI-enabled counterfeiting

By Michael Schwarm, Chief Growth Officer, SMT Corp.

January 15th, 2026

Executive Summary

Counterfeit electronic components are a systemic and accelerating risk to defense, safety critical, and critical infrastructure supply chains driven by the convergence of rapid computing innovation, shrinking hardware lifecycles, and AI-assisted counterfeit capability. As compute performance becomes a core competitive differentiator across industries—from cloud infrastructure to financial systems and defense—organizations are refreshing high-value assets at unprecedented speed. This accelerates the flow of reclaimed parts into the market and increases the attractiveness of unauthorized sourcing channels.

At the same time, global semiconductor supply chains remain vulnerable to demand spikes and lead time disruptions. When organizations face urgent production schedules and allocation risk, they often turn to independent distributors and electronic component brokers outside authorized channels. That shift creates the opportunity counterfeit operations need: weak traceability, inconsistent provenance, and high incentives to substitute or remark parts.

The threat is amplified by technological progress on the counterfeiters' side. Automation and AI-assisted design tools are reducing the cost of producing convincing fakes—not only physical parts, but also the packaging, test reports, and certifications that accompany them. Modern counterfeit operations increasingly optimize for passing basic tests and inspections, including elements of SAE AS6171 [1] testing, while still failing under long-term stress conditions such as thermal cycling, humidity, and parametric drift.

This white paper explains the key dynamics driving the proliferation of counterfeit electronic components, highlights the supply channels most associated with infiltration, and provides a prevention-oriented strategy for organizations that require trustworthy component integrity.

Core Thesis: Why Counterfeit Risk Is Rising Now

Rapid advancements in computing technology intensify competition in markets where compute performance is a differentiator. As firms compete on performance-per-dollar and latency-per-watt, they refresh data center and

high-tech hardware faster. This accelerates turnover and expands the pipeline of reclaimed and decommissioned parts.

These trends produce a cascading effect:

· Faster refresh cycles increase reclaimed parts volume

· More reclaimed parts enter broker networks [2]

· Demand volatility and lead-time pressure push buyers into weaker traceability channels

· AI tools lower the cost and increase the quality of counterfeits [3]

· Shorter product lifecycles increase electronic component obsolescence, forcing reliance on gray markets

· Higher chip value increases the economic incentive for counterfeiting [4]

The result is a broadening risk across global electronics supply chains.

Market Pressure: Compute-Driven Competition Is Fueling Hardware Turnover

Across industries, computing capability has become a strategic differentiator. This is most visible in hyperscale cloud and AI expansion, but it extends to finance, telecom, healthcare research, and defense.

Examples of industries driving accelerated refresh cycles:

· Cloud & hyperscale providers

· Telecom, 5G & network backbone providers

· Semiconductor, electronics & hardware manufacturers

· High-frequency trading and financial market infrastructure

· Government & defense contractors

· Universities & HPC labs

· Healthcare networks and medical research organizations

· Energy, utilities & smart infrastructure

As an example, AWS is investing about $11 billion to build a large-scale data center campus in northern Indiana in the United States, describing it as the largest planned capital investment in Indiana's history [5]. The campus is intended to expand AWS's cloud infrastructure capacity and support compute-intensive workloads, including generative AI.

Figure: Construction work takes place on an $11 billion Amazon Web Services [6] data center campus photographed using a drone on Tuesday, Dec. 17, 2024, in New Carlisle MICHAEL CLUBB/SOUTH BEND TRIBUNE

The Reclaimed Parts Pipeline: Asset Turnover Expands "Harvest-and-Resell" Supply

Modern counterfeiting isn't only about manufacturing fake chips. In many cases, it's about repackaging real parts sourced from used systems.

How reclaimed parts become counterfeit:

1) Decommissioned equipment enters liquidation, e-waste, or broker channels

2) High-value components are extracted (memory, processors, power devices, networking silicon)

3) Parts are cleaned, resurfaced, re-marked, and repackaged

4) Components are resold as “new,” “unused,” or “factory sealed”

Photo of e-waste ready for component harvesting. Source: SMT Corp.

Demand Surges and Lead-Time Pressure Drive Buyers to Weak-Traceability Channels

When demand spikes occur—particularly for constrained components such as memory, microcontrollers, or power management ICs—lead times expand and allocation becomes uncertain. Under schedule pressure, OEMs and contract manufacturers increasingly turn to independent distributors, electronic component brokers, online marketplaces, and secondary and surplus inventory channels.

Many of these channels are not inherently fraudulent. However, they often have weaker traceability than authorized distribution and create opportunities for counterfeit insertion, including refurbished-as-new parts, date code/lot code relabeling, outright clones or look-alike parts, substitution, and documentation laundering.

The key driver is urgency: when the cost of delay exceeds the cost of uncertainty, buyers accept supply that brings increased risk.

AI and Automation: Lowering the Barrier to Counterfeit Manufacturing and Documentation

The most important accelerant in the next decade is not only demand—but capability.

AI-assisted design and automation tools enable faster cloning and counterfeiting by reducing the time required to replicate labels, packaging, and documentation; generate plausible test reports and certificates; mimic or clone electronic components; build functional look-alikes; and scale operations across many part types. AI also improves the

quality of the deception layer—counterfeit operations can now produce supporting materials that appear legitimate to procurement teams and pass superficial validation.

Note: This chart is an illustrative (0–100) index showing the industry's accelerating adoption and capability of AI-assisted EDA/design automation from 2000–2030. The curve is anchored to public milestones such as the shift from early ML in EDA to production reinforcement-learning design-space optimization (e.g., Synopsys DSO.ai) [7], broader commercial deployment of AI optimization platforms (e.g., Cadence Cerebrus in 2021) [8], and the emergence of generative/agentic EDA systems. The "iteration speedup" line reflects the growing potential of these tools to shorten closure loops, automate flow tuning, and enable faster reuse/replication ("cloning") of proven design blocks and implementation recipes. Values represent relative trend progression, not a single measured market statistic.

Faster Semiconductor Iteration Increases Obsolescence and EOL-Driven Gray Market Demand

Advances in semiconductor design tooling accelerate product cycles. As new nodes and architectures emerge faster, components reach end-of-life (EOL) sooner, driving reduced availability through authorized channels, increased reliance on aftermarket suppliers, surging pricing for legacy components, and higher incentives for remarking and substitution.

This creates a long tail of risk: industries with extended lifecycle requirements—industrial controls, aerospace, defense, medical, energy —often need parts long after commercial markets have moved on. That disconnect forces procurement into high-risk channels. Electronic component obsolescence becomes a structural driver of counterfeit exposure.

The Economics: Modern Chips Are Expensive, Scarce, and Highly Incentivized

Electronic parts counterfeiters follow margin.

Semiconductors are more valuable than ever — especially in AI, networking, and power. Scarcity and lead-time volatility increase price dispersion between authorized and unauthorized channels. When the cost of authentic supply rises sharply, opportunistic profits are pursued, and the market becomes saturated with counterfeits.

Major Sources of Counterfeit Electronic Components

Counterfeit electronic components originate from multiple sources, including:

· Electronic waste (e-waste) and used equipment harvesting

· Decommissioned industrial/telecom/military equipment

· Excess inventory, liquidation, and distressed supply

· Unauthorized production and factory overbuild

· Rejected/failed production lots diverted instead of scrapped

· Obsolete parts demand and EOL-driven gray markets

· Clone/look-alike component manufacturing

· Documentation forgery and traceability laundering

· Returned goods and RMA streams

· Online marketplaces and small traders

The most difficult risks are hybrid: authentic reclaimed parts relabeled as new, with forged documentation that appears plausible.

Why Testing Alone Isn’t Enough (Even SAE AS6171 Testing)

Industry-standard testing remains critical—but it is no longer sufficient alone because counterfeit operations increasingly optimize for test-passing behavior.

Counterfeit and reworked parts often pass basic electrical tests, superficial visual inspection, simple functional checks, limited sampling-based QA, and even certain elements of SAE AS6171 testing depending on depth and scope [9]. But they may fail under thermal cycling, long-term stress, humidity/corrosion exposure, and parametric drift over time. [10]

This supports a central conclusion: counterfeit defense must emphasize higher levels of testing, prevention, and supply-chain controls as much as basic testing and inspection.

Recommendations: How to Reduce Counterfeit Risk in a High-Velocity Tech Era

Strengthen supply-chain controls and sourcing strategy

• Use authorized channels and require traceability evidence and chain-of-custody documentation wherever possible

• Maintain pre-approved lists of independent distributors and brokers OR use trusted independent distributors that are SAE AS6081 [11] accredited and have expertise in sourcing from broker markets

• Implement a risk-based procurement gate for urgent buys

Build proactive obsolescence and lifecycle planning

• Anticipate EOL risk early and lock supply before scarcity

• Qualify alternates before shortages occur

• Align last-time-buy procurement with strategic inventory management

• Avoid emergency procurement whenever possible

Make verification multi-layered

• Combine advanced testing methods as defined by AS6171 High Risk Level 2 [9] including spectroscopy and electrical parameter testing along with basic physical, materials, and mechanical inspections defined by AS6171 Moderate Risk Level 2

• Improve inspection & test regime sophistication

• Use risk scoring by component type and source

• Track anomalies by lot, supplier, and geography

Address documentation forgery and traceability laundering

• Validate certificates and test reports through direct confirmation when possible

• Use digital chain-of-custody records

• Flag mismatched formatting, metadata inconsistencies, and serial anomalies

Align incentives internally

• Ensure procurement teams are not primarily rewarded for cost savings and/or locating immediate inventory.

• Encourage early escalation of constrained component risks

• Create interdepartmental objectives to reduce the risk of counterfeits as measurable KPIs

Conclusion

The proliferation of counterfeit electronic components is being fueled by structural shifts in the technology economy: faster compute-driven competition, more aggressive hardware turnover, volatile demand and lead-time pressure, AI-assisted design and automation, higher chip value and scarcity, and accelerating electronic component obsolescence.

Organizations that rely only on testing will remain exposed—because counterfeit operations are increasingly optimized to pass inspections. The next era of component integrity must be built around prevention, traceability, and control of sourcing pathways, supported by advanced verification as one layer of a broader risk mitigation strategy.

About SMT Corp.

With locations in the United States and United Kingdom, SMT Corp. helps customers execute the key best-practice recommendations for managing supply-chain risk and part availability, especially in today's constrained and fast-changing semiconductor ecosystem. As an SAE AS6081-accredited Independent Distributor, SMT brings proven expertise in responsible sourcing through the broker/independent market, including supplier qualification, documentation review, and market intelligence to secure hard-to-find components while protecting quality and continuity. When parts lack full traceability, SMT is uniquely positioned to support rigorous component testing and verification as an accredited SAE AS6171 (High Risk Level 2)–accredited and DLA-accredited provider for testing electronic components without traceability—helping customers mitigate counterfeit, performance, and reliability risks. SMT also delivers inventory management strategies tailored to EOL and obsolete components, guiding last-time-buy decisions, buffer stocking, and demand planning to prevent production disruption. Across the entire bill of materials, SMT provides a comprehensive risk assessment and BOM support service—identifying lifecycle, compliance, allocation, and substitution risks and recommending mitigation options—so customers can make faster, better-informed decisions and keep products shipping with confidence.

AI-Assisted Research & Drafting Notice

Portions of this white paper—including select background research synthesis, drafting support, and the creation/organization of certain charts and visualizations—were produced with the assistance of AI tools. The thesis, core ideas, topic selection, structural outline, conclusions, and final editorial decisions are solely attributable to the author.

Citations & References

1. SAE International. (SAE AS6171). Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. SAE AS6171 Standard

2. ERAI 2024 Annual Report. ERAI Annual Report

3. AI Driving U.S. Counterfeit Crisis, New Study Finds – Part 1. SOCPUB Article

4. Recent Price Trends in the Semiconductor Industry: U.S. Bureau of Labor Statistics Price Trends

5. State of Indiana (Governor's Office). (2024). Gov. Holcomb announces Amazon Web Services plans to invest $11B to create a new data center campus in northern Indiana. Indiana Events

6. Amazon. (2024). AWS plans $11 billion Indiana investment. About Amazon

7. Synopsys. (n.d.). DSO.ai: AI-driven design applications. Synopsys

8. Cadence. (n.d.). Cadence Cerebrus AI Studio white paper (notes Cerebrus released in 2021). Cadence

9. Analysis of Standards-Based Counterfeit Microelectronics Detection Methods: IEEE Paper

10. N. Williams, N. Tuzzio, T. Sharpe, "Comparison of Known Good and Clone Device Electrical Performance for Counterfeit Detection," DMSMS 2017

11. SAE International. (2012; rev. 2023). SAE AS6081: Fraudulent/Counterfeit Electronic Parts—Avoidance, Detection, Mitigation, and Disposition—Distributors. SAE AS6081 Standard