The Hidden Price Tag: Quantifying the True Cost of Counterfeit Electronics

Daniel DiMase[1], Joshua Paulsen[2], Ujjwal Guin[2], Steve Walters[1], Zachary A. Collier[3], Jeremy Muldavin[4], Paula George[5], Grant Meyer[6]

[1]Aerocyonics, Inc., East Greenwich, RI 02818, USA
[2]Auburn University, Auburn, AL 36849, USA
[3]Radford University, Radford, VA 24142, USA
[4]Cadence Design Systems, San Jose, CA 95134, USA
[5]U.S. Department of Defense (Retired), Alexandria, VA, USA
[6]NDIA Electronics Division Chair, Arlington, VA 22201, USA

Emails: daniel.dimase@aerocyonics.com, jap0131@auburn.edu, ujjwal.guin@auburn.edu, steve.walters@aerocyonics.com, zcollier@radford.edu, muldavin@cadence.com, glutenfreie@yahoo.com, william.r.haselrick@lmco.com, grant.d.meyer@lmco.com

***Abstract*—The growing threat of counterfeit microelectronics continues to intensify despite advancements in detection and avoidance techniques over the last decade. The widespread infiltration of recycled and fraudulent components into the semiconductor supply chain poses significant risks, including reduced system reliability, safety concerns, degraded performance, shortened operational lifetimes, and increased vulnerability to security breaches. As modern electronic systems increasingly support mission-critical applications and essential infrastructure, the presence of counterfeit microelectronics can lead to unexpected failures, operational disruptions, and potentially severe economic and security consequences. This paper analyzes why the financial impact of counterfeit microelectronics on defense and other high-reliability systems is systematically underestimated, and how targeted investments can better control risk and cost. It first situates counterfeit parts as a national security and readiness issue driven by long-lifecycle systems' reliance on secondary markets and the limitations of documentation-based assurance. The paper then develops a cost-mechanics framework showing how timing of detection, uncertainty, legal processes, and program-level remediation cause costs to escalate nonlinearly once system integrity is questioned. A modeled Defense Logistics Agency case demonstrates how approximately $1.8 million in procurement can generate an estimated $9.6–$17.9 million in downstream investigation, testing, legal, and Diminishing Manufacturing Sources and Material Shortages (DMSMS) related costs. Drawing on recent inter-laboratory evaluations of SAE AS6171 counterfeit detection standard workflows, the paper shows that improper interpretation and lack of evidence traceability, not just test execution, dominate cost drivers. It concludes that traceability-centered decision infrastructure and risk-informed test selection offer a pragmatic path to earlier detection, bounded investigation scope, and measurable cost avoidance.**

***Index Terms*—Counterfeit electronics, cybersecurity, traceability, reliability, cost-mechanics.**

I. Introduction

The growing threat of counterfeit microelectronics continues to intensify despite advancements in detection and avoidance techniques over the last decade, allowing recycled and fraudulent components to infiltrate the semiconductor supply chain and degrade reliability, performance, and security. As electronic systems increasingly support mission-critical applications and critical infrastructure, counterfeit microelectronics can lead to unexpected failures with significant economic and security consequences [1]–[3].

Counterfeit microelectronics remain a persistent challenge for defense and other high-reliability systems, not because the threat is poorly understood, but because its true cost is often underestimated. While counterfeit incidents may appear infrequent and procurement values modest, the downstream consequences—investigation, remediation, legal action, and program disruption—can escalate rapidly once system integrity is called into question. The same uncertainty-driven cost escalation applies to counterfeit electronic assemblies embedded in critical infrastructure, including networked devices whose provenance and configuration are foundational to cybersecurity [4]. This paper examines how and why those costs accrue and identifies targeted investments that can materially reduce both risk and cost.

Congressional attention over the past decade has established counterfeits as a national security and readiness concern, particularly as long-lifecycle systems increasingly rely on secondary markets to sustain obsolete components [5]. In response, the defense community has developed standards and testing protocols, most notably SAE International standard AS6171 [6]–[9], which have significantly improved the ability to identify suspect parts. However, experience has shown that standards and testing alone are insufficient to control cost when counterfeit exposure is discovered late or when uncertainty cannot be bounded.

Unlike routine quality issues, counterfeit exposure triggers a shift from component-level assessment to system-level assurance. Costs escalate nonlinearly as the investigation scope expands, uncertainty grows, and remediation actions propagate across lots, assemblies, and programs. Timing of detection,

false-positive testing outcomes (i.e., incorrect classification of an authentic part as counterfeit) and false-negative testing outcomes (i.e., failure to identify a counterfeit part), weak traceability, and legal considerations all contribute to this escalation, making procurement value a poor indicator of total exposure. This escalation dynamic is increasingly relevant for networked electronics, such as counterfeit networking equipment, where authenticity concerns include cybersecurity assurance and potential data-exposure consequences in addition to reliability and performance.

This paper examines why current mitigation approaches struggle to contain these costs and the shortfalls associated with documentation-based traceability, which is vulnerable to falsification and fragmentation [10]. We also describe insights from recent government-sponsored inter-laboratory evaluations that show that while laboratories generally execute prescribed test methods competently, significant variability persists in how findings are interpreted, categorized, and used to support disposition decisions.

The paper contributes to the literature on risk analysis and systems engineering by highlighting implications for risk management: augmenting existing standards and limiting indiscriminately expanded testing can reduce both the cost and consequences of counterfeit microelectronics. This requires targeted investment in a traceability-centered decision infrastructure (analytic marketplace) that strengthens how existing methods are selected, applied, interpreted, and documented. Treating traceability as a risk-reduction and cost-avoidance mechanism—rather than a compliance artifact—enables earlier detection, bounds investigation scope, and supports more defensible decisions under cost and schedule pressure. A strong tie between physical evidence (provenance) and identity of authentic parts, defects, and test artifacts may further reduce false positive identifications while streamlining a triage approach to additional testing and validation. Together, these efforts provide a practical path to demonstrating measurable improvements in consistency, efficiency, and avoidance cost, while enabling a shift in counterfeit mitigation from reactive remediation to proactive, data-driven risk management.

II. Background: Counterfeit Microelectronics as a Systemic Risk

2.1. Congressional Focus and Standardization: Concerns about counterfeit microelectronics in defense and high-reliability systems are not new. For over a decade, government agencies, industry, and standards organizations have acknowledged that counterfeit parts represent a persistent threat to system reliability, safety, and mission assurance. What has evolved over time is not the existence of the problem, but a growing recognition that counterfeit exposure carries systemic consequences that extend far beyond individual components or suppliers.

Early congressional attention to counterfeit electronics highlighted the national security implications of compromised supply chains, particularly as defense systems became increasingly dependent on commercial-off-the-shelf (COTS) components and globalized manufacturing. [11] Testimony before Congress underscored that counterfeit incidents were not isolated quality escapes, but events capable of disrupting programs, delaying fielding, and imposing substantial remediation costs. These hearings helped establish counterfeit microelectronics as a readiness and assurance issue rather than a narrow procurement concern.

Despite this attention, structural factors have continued to increase exposure. Defense systems are designed for long service lives, often spanning decades, while the commercial electronics market operates on rapid innovation cycles. This mismatch between supply and demand results in obsolescence issues [12]. As original manufacturers discontinue parts, programs are increasingly forced to rely on secondary markets to sustain legacy systems. These markets, while essential, introduce additional risk due to limited visibility into provenance, variable documentation quality, and the presence of bad actors willing to exploit demand for obsolete components.

In response, the defense community has developed standards, policies, and testing protocols intended to reduce counterfeit risk. Among these, AS6171 has become a cornerstone for counterfeit detection, providing structured methods for inspection, testing, and analysis of suspect parts [6]–[9]. These standards have significantly improved the ability to identify anomalies and defects that may indicate counterfeiting activity. However, as experience has accumulated, it has become clear that standards and testing alone cannot fully address the problem, particularly when applied late in the lifecycle or without strong traceability and decision support.

2.2. Systemic Risk: A critical challenge is that counterfeit mitigation has often been treated as a compliance activity rather than a risk-management function. Programs focus on satisfying documentation and testing requirements, but less attention is paid to how information flows across organizations, how uncertainty is managed, or how decisions are made under cost and schedule pressure. As a result, counterfeit exposure is frequently discovered only after parts have been integrated or fielded, at which point options are limited, and costs escalate rapidly.

Another complicating factor is that counterfeit incidents are relatively infrequent compared to routine procurement activities, but their consequences are disproportionate. This mismatch makes it difficult for organizations to justify preventive investment using traditional cost-benefit analyses based solely on procurement value or failure rates. Additionally, counterfeit risk is difficult to quantify within the supply chain, given the fact that in some cases, counterfeits may appear indistinguishable from their authentic counterparts, as is typically the case in overproduction [13]. Without a clear understanding of how costs accumulate once counterfeit risk is identified, decision-makers may underestimate exposure and over-rely on reactive mitigation.

Taken together, these factors have created an environment in which counterfeit microelectronics remain a persistent, systemic risk. While awareness is high and technical capa-

bilities continue to improve, the underlying cost drivers – late detection, uncertainty, and limited traceability – have not been fully addressed. This context is essential for understanding why counterfeit-related costs escalate as they do, and why targeted investments in traceability and decision support represent a logical next step in managing both risk and cost. More broadly, public reporting on supply-chain compromises of communication devices has reinforced the idea that adversarial manipulation of electronics can produce consequences beyond traditional quality escapes, strengthening the case for provenance that supports rapid bounding of exposure and restoration of trust [14].

This paper is positioned within the topic of security economics, which seeks to apply economic concepts and modeling techniques to cybersecurity problems [15]. The field addresses questions like how much an organization should invest in cybersecurity [16] and how financial instruments like cyber insurance can be effectively utilized [17], [18]. These methodological frameworks have been more recently applied to hardware security. For example, a number of cost modeling methodologies for electronics obsolescence, maintenance, inventory management, and other applications have been developed [19]. Game theory has been utilized for Trojan detection [20] and intellectual property theft avoidance [13]. Cost-benefit and risk reduction metrics have also been studied in the context of hardware security [21]. While this is an emerging field, more research is needed on quantifying the costs of counterfeits and counterfeit reduction countermeasures to support risk-informed and economical decisions.

III. Cost Mechanics of Counterfeit Microelectronics

3.1. Cost Mechanics: The cost of counterfeit microelectronics is often misunderstood because it does not scale linearly with the value of the affected parts. Unlike conventional quality issues, where defects are typically isolated, corrected, and absorbed within routine processes, counterfeit exposure triggers a cascade of investigative, technical, legal, and programmatic activities that expand in scope as uncertainty increases. The magnitude of escalation is driven not only by uncertainty but also by application criticality; incidents involving mission-essential or safety-critical systems attract significantly greater investigative and remediation effort than those confined to lower-consequence applications. Understanding these cost mechanics is essential for interpreting the estimates presented in Section 4 and for identifying where targeted risk-reduction investments can have the greatest impact.

A defining characteristic of counterfeit-related costs is that they are driven less by the intrinsic value of the component and more by the effort required to establish confidence in system integrity. Once a part is suspected of being counterfeit, the immediate question is no longer whether the part meets form, fit, and function, but whether the system into which it may have been introduced can be trusted. This shift in framing—from component quality to system assurance—fundamentally changes the cost structure. This shift is even more pronounced for networked electronics. When the suspect device is part of communications or security infrastructure, the assurance question expands beyond form, fit, and function to include cybersecurity posture: whether hardware and firmware provenance can be trusted, whether configurations and entitlements are legitimate, and whether the device can be safely relied upon in a privileged network role. As a result, downstream cost may include not only testing and replacement, but also security assessment, forensic review, credential and key rotation, configuration rebuild, and broader "trust restoration" actions to bound potential exposure [4], [22]. Activities that were previously scoped to individual items expand to include lots, assemblies, suppliers, and, in some cases, entire programs.

One of the primary drivers of cost escalation is the timing of detection. When suspect material is identified early, such as during an incoming inspection, the investigation scope can often be limited to a set of parts or transactions. As detection occurs later in the lifecycle—during integration, qualification, or after fielding—the number of potential impact points increases dramatically. Late discovery necessitates broader testing, expanded record reviews, and more extensive remediation, even when only a small number of parts are ultimately affected. In this way, time acts as a cost multiplier, amplifying both labor and disruption. This is consistent with observations from other fields, such as software engineering, where it can be as much as 150 times as expensive to fix faulty software in the operations phase as it is during the requirements phase [23].

False-positive and false-negative outcomes further compound this effect. A false positive, in which authentic parts are incorrectly classified as counterfeit, can trigger unnecessary redesigns, substitutions, or Diminishing Manufacturing Sources and Material Shortages (DMSMS) actions. These responses consume engineering resources, delay schedules, and introduce new qualification costs, even though no counterfeit threat ultimately existed. Conversely, a false negative, in which counterfeit parts are misclassified as authentic, allows risk to propagate downstream. When such escapes are later discovered, they often require extensive investigation and remediation to determine where else similar parts may reside. Both outcomes are costly, but for different reasons: false positives waste resources proactively, while false negatives defer and magnify cost reactively.

Table I highlights the specific average costs associated with each DMSMS solution, organized from least costly to most costly. Each cost is based on resolving the issue on a per-case basis, with the relative increase over the lowest-cost solution also listed. Even when the number of suspect parts is limited, the actions required to restore confidence—requalification, revalidation, redesign, or substitution—can affect entire systems or fleets. These impacts are especially pronounced in long-lifecycle systems, where redesigns must account for legacy interfaces, certification requirements, and operational constraints, such that relatively small counterfeit exposures can generate disproportionately large organizational costs. These

TABLE I: AVERAGE COSTS ASSOCIATED WITH IMPLEMENTING EACH DMSMS RESOLUTION ALTERNATIVE.

Resolution Alternative	Average FY24 Dollars [24]	Δ Change	Frequency of Occurrence [25]
Approved Item	$1,258	1X	34%
Life Of Need (LON) Buy	$6,399	5X	15%
Simple Substitute	$15,379	12X	33%
Complex Substitute	$31,068	25X	9%
Extension of production of support	$31,143	25X	2%
Repair, refurbishment, or reclamation	$79,492	63X	1%
Development of a new source	$322,098	256X	3%
Design refreshment	$938,476	746X	
Redesign - Next Higher Assembly (NHA)	$1,336,220	1,063X	3%
Redevelop the item	$2,043,388	1,625X	
Redesign - complex/system replacement	$12,578,942	10,002X	1%
Frequency Weighted Cost per Issue: $186,216			

relative cost increases, Δ Change, demonstrate that as the resolution complexity increases, the cost increases exponentially. This leads to an overall high frequency-weighted cost per issue, with the least often used solutions raising the average significantly due to their relatively high costs when compared to the most frequently used solutions. This weighted average was calculated by multiplying the average cost per resolution by its relative frequency of occurrence and then totaling those values together. A false positive report will lead to, on average, $186,216 being spent per issue to resolve the falsely identified counterfeit parts.

Another important cost driver is uncertainty. In counterfeit investigations, uncertainty expands the scope. When evidence linking suspect parts to specific suppliers, lots, or transactions is weak, organizations are forced to assume worst-case scenarios. This leads to broader part sweeps, additional testing, and prolonged investigation timelines. Conversely, when traceability and evidence are strong, uncertainty can be reduced, allowing the investigation scope to narrow quickly. The difference between these two states—high uncertainty versus bounded confidence—often determines whether costs remain manageable or escalate dramatically.

Legal and compliance considerations also play a significant role in cost accumulation. Counterfeit cases that involve intentional fraud require coordination with law enforcement, legal review, and, in some cases, prosecution. These activities introduce costs that are largely independent of the number of affected parts and are instead driven by the complexity and duration of the case. Once initiated, such processes are difficult to curtail, further decoupling total cost from original procurement value.

These dynamics become most visible when costs are aggregated beyond a single incident and examined at the organizational level. While Table I presents the frequency-weighted average cost to resolve a single counterfeit instance using established DMSMS resolution pathways, Table II scales this framework to illustrate organization-level exposure when multiple National Stock Numbers (NSNs) are affected. Rather than reflecting per-device cost, Table II applies the same resolution cost structure across 598 impacted NSNs and weights those outcomes by historical resolution frequency. Specifically, the average cost for each resolution option was multiplied by 598 NSNs to estimate the cost if all NSNs were resolved using that option, and those totals were then weighted by the relative frequency of occurrence for the respective resolution. The weighted costs for each resolution were summed, with the exception of redesign resolutions, which are not applicable to this example and whose high costs and low frequency would have substantially skewed the total. Overall, this produced an estimated total of $12,163,009, while still assuming that the most expensive redesign resolutions would not be required [26].

Taken together, these mechanisms explain why counterfeit-related costs tend to escalate nonlinearly and why initial procurement value is a poor indicator of total exposure. Costs are driven by timing, uncertainty, scope expansion, and the need to reestablish trust in systems, rather than by the price of the parts themselves. This cost structure provides the conceptual foundation for the modeled estimates presented in Section 4 and underscores the importance of investments that reduce uncertainty, enable earlier detection, and bound the scope of the investigation. Improvements in traceability and decision support directly target these cost drivers, offering a practical path to reducing both the likelihood and severity of high-cost counterfeit events.

3.2. MDA Example: Congressional testimony from the Missile Defense Agency (MDA) reinforces this escalation dynamic. In November 2011, Lieutenant General Patrick J. O'Reilly, then Director of MDA, testified before the U.S. Senate Armed Services Committee that counterfeit electronic components discovered within ballistic missile defense systems resulted in approximately $4 million in remediation costs, including an estimated $3 million to remove and replace suspect parts from a THAAD mission computer. Importantly, these costs were not driven by the procurement value of the components themselves, but by the engineering effort, system-level validation, and mission assurance activities required to restore confidence in operational hardware. This testimony provides a real-world defense program example of how counterfeit exposure can generate multi-million-dollar impacts disproportionate to the original component value, consistent with the nonlinear cost mechanics described in this paper [27].

IV. EMPIRICAL EVIDENCE: ESTIMATED COST AND CONSEQUENCES OF A COUNTERFEIT MICROELECTRONICS CASE

4.1. Case Overview: The true cost of counterfeit microelectronics is often poorly understood because it is rarely captured at the point of procurement. Instead, costs accumulate over time as suspect material is investigated, tested, remediated, and, in some cases, prosecuted. To illustrate how these costs

TABLE II: POTENTIAL PROGRAM COSTS OF SUSPECT PARTS.

Resolution Option	Average FY24 Dollars [25]	Frequency of Occurrence [24]	Cost if all the Same Resolution	Weighted Cost
Approved Item	$1,258	34%	$752,284	$255,777
Life Of Need (LON) Buy	$6,399	15%	$3,828,802	$573,990
Simple Substitute	$15,379	33%	$9,196,642	$3,034,892
Complex Substitute	$31,068	9%	$18,578,664	$1,672,080
Extension of production of support	$31,143	2%	$18,623,514	$372,470
Repair, refurbishment, or reclamation	$79,492	1%	$47,536,216	$475,362
Development of a new source	$322,098	3%	$192,614,604	$5,778,438
Design refreshment	$938,476	-	$561,208,648	-
Redesign - Next Higher Assembly (NHA)	$1,336,220	3%	$799,059,560	$23,971,787
Redevelop the item	$2,043,388	-	$1,221,946,024	-
Redesign - complex/system replacement	$12,578,942	1%	$7,522,207,316	$75,222,073
Weighted Total Cost Per Case				**$20,339**
Total Weighted Cost For All 598 NSN's				**$12,163,009**

can escalate in practice, this section examines a counterfeit case investigated by the Defense Logistics Agency (DLA), using a structured cost-estimation model developed jointly by DLA and Aerocyonics to estimate downstream cost impacts associated with investigation, remediation, and program disruption [26].

Between 2012 and 2015, DLA investigated a multi-year counterfeit and fraud scheme involving electronic components supplied into defense systems. The scheme was characterized by deliberate efforts to obscure traceability, including the creation of multiple shell companies and CAGE codes, the use of family members and unwitting associates, and the procurement of electronic parts from unvetted online marketplaces. As scrutiny increased, additional supplier identities were introduced, complicating detection and containment efforts. Throughout the investigation, suspect material was treated conservatively until authenticity could be established through testing and legal adjudication. The case resulted in federal prosecution and sentencing in the Southern District of Ohio, as publicly documented by the U.S. Department of Justice [28].

Over the course of the investigation, the scope of impact expanded substantially. In total, the scheme affected 891 purchase orders, 730 contracts, and 598 National Stock Numbers (NSNs) across multiple programs and systems. The original value of the contracts associated with these procurements totaled approximately $1.8 million. While this figure represents the baseline procurement exposure, it captures only a small fraction of the potential costs associated with managing counterfeit risk once suspect material is identified [26].

4.2. Cost framework: Using a structured, assumption-driven cost framework, the analysis evaluated the types of costs that typically accrue as counterfeit investigations expand beyond initial receipt inspection. These included estimated labor and resource burdens associated with supply chain and logistics activities such as contracting, item management, depot operations, transportation, and storage. Technical evaluation costs were modeled to account for test coordination, laboratory labor, counterfeit screening, and engagement with original equipment manufacturers and end users. These activities are necessary not only to identify suspect parts, but also to bound the scope of potential impact and prevent further propagation.

The cost model also incorporated estimated legal and law-enforcement activities required to resolve cases involving intentional fraud. These included sustained involvement by special agents, financial investigators, inter-agency partners, and federal prosecutors, as well as multi-year case management and court proceedings. In addition, remediation activities were modeled to account for hardware replacement or rework, requalification and validation efforts, and program-level disruption associated with restoring confidence in system integrity. Consistent with historical Missile Defense Agency testimony to Congress, the remediation assumptions used in this analysis were conservative and included only a single field escape.

When aggregated, the estimated total cost impact associated with this single counterfeit case was calculated to be approximately $9.65 million (see Table III), based on high-level assumptions regarding labor rates, investigation scope, remediation activities, and legal proceedings. This estimate reflects the combined government and industry burden across supply chain operations, technical evaluation, legal action, and remediation. Even under these conservative assumptions, the estimated cost exceeded the original contract value by more than a factor of five.

The analysis further explored organizational-level impacts by applying weighted assumptions for Diminishing Manufacturing Sources and Material Shortages (DMSMS) resolution pathways across the 598 affected NSNs. When potential substitutions, redesigns, requalification activities, and associated organizational disruption were incorporated, the estimated total cost impact increased to approximately $17.9 million and is shown in Table IV. At this scale, the original procurement value represented less than eleven percent of the modeled total cost.

It is important to emphasize that these figures represent

TABLE III: SUPPLY CHAIN, LEGAL-LAW ENFORCEMENT, AND REMEDIATION COST.

Cost Items	Government	Industry
Supply Chain Costs		
Procurement		
Contracting Specialist	$ 59,800	$ 11,960
Material Planner	$ 29,900	$ 5,980
Item Manager	$ 29,900	$ 5,980
Product Specialist	$ 29,900	$ 5,980
Technical Evaluations		
Test Coordinator	$ 25,000	$ 5,000
Lab Personnel	$ 7,000	
Lab Testing	$ 15,000	$ 41,860
OEM/End User	$ 2,800	
Depot/Warehousing		
Depot Foreperson	$ 59,800	$ 11,960
DLA	$ 25,000	
Storage (30% of Material Cost)	$ 539,222	$ 172,551
Total Supply Chain Cost	**$ 823,322**	**$ 261,271**
Legal Costs		
Special Agent - Gov	$ 100,000	
Other Agencies - Gov	$ 75,000	
Other Legal Cost - Industry		$ 166,400
Cross Functional Team Meetings	$ 51,840	$ 51,840
Federal Court / Prosecution	$ 2,019,248	$ 403,850
Total Legal Costs	**$ 2,246,088**	**$ 622,090**
Warfighter Costs		
Remediation	$ 2,700,000	$ 1,200,000
Original Value of Contracts	$ 1,797,405	
Subtotal	**$ 7,566,815**	**$ 2,083,361**
Total Cost	**$ 9,650,176**	

TABLE IV: FINAL COST WRAP UP.

Cost Type	Government	Industry
Supply Chain	$ 823,322	$ 261,271
Remediation	$ 2,700,000	$ 1,200,000
Legal	$ 2,246,088	$ 622,090
Program Level Costs	$ 12,163,009	-
Subtotal	**$ 17,932,419**	**$ 2,083,361**
Total	**$ 20,015,780**	

order-of-magnitude estimates, not audited accounting totals. The cost model intentionally relied on conservative, high-level assumptions to bound the scope of potential impacts and to illustrate how counterfeit exposure can drive cost escalation well beyond initial procurement value. Actual costs will vary by program, system, and detection point; however, the structure of the escalation—and the dominance of downstream investigation, remediation, and program disruption costs—remains consistent.

4.3. Key Observations: Several observations emerge from this estimated case analysis. First, the majority of the cost is incurred after counterfeit exposure is identified, not at the point of procurement. Second, documentation-based traceability alone is insufficient to prevent or rapidly contain counterfeit activity, allowing investigation scope and associated cost to grow over time. Public prosecutions involving large-scale trafficking of counterfeit Cisco-branded networking equipment show a similar pattern: when documentation and provenance cannot be reconciled with the physical device and its operational role, investigation scope expands, and the cost of re-establishing trust can quickly dominate the response [4]. Third, once counterfeit risk is confirmed, cost escalation is nonlinear, driven primarily by investigation breadth, legal requirements, and program-level remediation rather than the value of the parts themselves.

This modeled case demonstrates that counterfeit microelectronics represent a systemic cost risk rather than a localized quality issue. Late detection and limited traceability amplify financial, operational, and readiness impacts well beyond the value of the original components. The cost structure illustrated here provides essential context for understanding why improvements in early detection, evidence traceability, and decision support are central to reducing both the frequency and severity of future counterfeit-related losses.

V. LIMITATIONS OF CURRENT COUNTERFEIT MITIGATION APPROACHES

5.1. Persistent Risk: Despite increased awareness, improved standards, and expanded testing capabilities, counterfeit microelectronics continue to impose significant cost and risk. This persistence is not due to a lack of effort or technical competence, but rather to structural limitations in how counterfeit mitigation is currently implemented across the supply chain. These limitations constrain the effectiveness of existing approaches and help explain why costs escalate even when standards and testing are applied.

A central limitation is the reliance on documentation-based traceability as a primary control mechanism. Certificates of conformance, chain-of-custody records, and supplier declarations remain foundational elements of procurement assurance. However, documentation is inherently vulnerable to falsification, misrepresentation, and fragmentation across organizations. When documentation is disconnected from physical parts and supporting test evidence, it provides limited protection against intentional fraud and does little to bound the investigation scope once counterfeit risk is suspected. As a result, documentation that initially supported procurement decisions often becomes insufficient during investigations, leading to broader and more costly corrective actions. Public prosecutions involving counterfeit networking equipment illustrate how this documentation gap can scale into enterprise-level consequences when provenance cannot be bounded quickly and confidently [4], [29].

5.2. Cisco Example: For example, the U.S. Attorney's Office (District of New Jersey) publicly described a multi-year scheme in which tens of thousands of low-quality, modified computer networking devices were imported and sold with counterfeit Cisco labels, packaging, and documentation to falsely appear "new" and "genuine," including sales that reached government and military environments; the principal was sentenced to 78 months in prison. Charging materials characterized the trafficking scheme as involving an estimated retail value of over $1 billion, and sentencing materials report that the operation generated over $100 million in revenue; under the plea agreement, the defendant also agreed to pay restitution of $100 million to Cisco (with other victim restitution to be determined by the court). Critically, prosecutors described

frequent device failures and malfunctions that caused significant damage to users' networks and operations—sometimes costing users tens of thousands of dollars—highlighting that a "counterfeit device" can impose direct operational and remediation costs well beyond the purchase transaction. In cost-mechanics terms, counterfeit networking equipment is especially troubling because it is not merely a functional substitute: it can occupy a privileged position in a system's security architecture. Even in the absence of a confirmed exploit, uncertainty regarding hardware and firmware provenance can trigger security-driven remediation—inventorying deployments, bounding exposure, validating configurations, and restoring confidence in the integrity of the protected network—thereby amplifying the scope of investigation and downstream costs beyond traditional "test and replace" models [22].

Although the Cisco prosecution involves counterfeit networking equipment, the underlying cost mechanism is broadly applicable. Any connected system—whether a sensor, embedded controller, medical device, server, chip, or software-enabled application—both produces and consumes data that other systems rely upon for decisions. When counterfeit exposure cannot be quickly linked to traceable evidence, organizations must assume greater uncertainty across the data supply chain (identity, provenance, configuration, firmware/software baseline, and downstream dependencies). The resulting response shifts from a discrete "replace the item" action to a focus on trust restoration across interconnected assets and datasets, driving nonlinear growth in investigation scope, labor, downtime, and remediation costs.

The enterprise cost of "bounding exposure" is visible in public operational alerts as well. The U.S. Department of Energy issued an Operating Experience Level 3 (OE-3) notice to raise awareness of suspect/counterfeit and fraudulent Cisco networking equipment that may have been procured across the DOE enterprise—underscoring that even determining where suspect equipment resides, what it touches, and what must be validated or replaced can impose material labor, downtime, and replacement-planning costs [30]. This same uncertainty mechanism drives cost escalation in microelectronics and electronic systems: when documentation cannot be linked to traceable physical evidence and defensible disposition rationale, organizations compensate with broader testing, wider sweeps, and more disruptive remediation to restore confidence.

5.3. The Limits of Testing: Testing, while essential, is also constrained by how and when it is applied. Standards such as AS6171 provide robust methods for identifying anomalies and defects associated with counterfeit activity, thereby significantly improving detection capability. However, testing is often employed reactively, triggered by suspicion or failure rather than used as part of a proactive, risk-informed strategy. While some companies test material when they acquire parts with unknown pedigree, many organizations rely on a paper trail of traceability, which is easily falsified. When testing occurs late in the lifecycle—after integration or fielding—the cost of both false positives and false negatives increases substantially. Moreover, testing alone cannot resolve uncertainty if results are difficult to interpret consistently or cannot be clearly linked to traceable evidence. From a total cost of quality perspective, focusing only on appraisal activities (i.e., testing) is inadequate, as investment should also be made in prevention activities [31].

Another limitation lies in the absence of decision-support infrastructure. Counterfeit mitigation decisions are frequently made under cost, schedule, and information constraints, yet laboratories and program offices lack tools to quantify trade-offs between testing depth, confidence, turnaround time, and cost. In the absence of such tools, decision-makers often default to conservative approaches that expand the scope of testing and investigation to manage uncertainty. While understandable, this tendency contributes directly to the nonlinear cost escalation described earlier, particularly when investigations span multiple suppliers, lots, or systems.

Variability across organizations further complicates mitigation efforts. Laboratories differ in expertise, interpretation practices, and evidence documentation, even when applying the same standards. Program offices and supply chain organizations likewise vary in risk tolerance and response strategies [32]. Without mechanisms to normalize evidence expectations and interpretation, these differences translate into inconsistent outcomes and expanded coordination effort. Over time, this variability erodes confidence and reinforces reliance on broad, resource-intensive mitigation actions. Risk-based approaches must therefore balance risk assessment on one hand, and decision support on the other [33].

Finally, current approaches offer limited feedback mechanisms to drive systemic improvement. Lessons learned from investigations, testing outcomes, and remediation efforts are rarely captured in a form that informs future decisions or the refinement of standards. As a result, similar issues recur across programs and over time, and investments in mitigation yield diminishing returns. Without closing this feedback loop, organizations remain locked in a reactive cycle that addresses individual incidents but does not materially reduce long-term exposure.

Taken together, these limitations explain why counterfeit mitigation, as currently practiced, often fails to control cost even when standards and testing are applied diligently. The challenge is not the absence of tools, but the lack of integration among documentation, testing, evidence, and decision-making. Addressing this gap requires a shift from compliance-oriented controls toward traceability-centered risk management, a transition explored in the following section through insights from recent inter-laboratory evaluations.

VI. Findings from Recent Inter-Laboratory Evaluations: Why Targeted Investment Is Required

6.1. Study Methodology: While documented case studies illustrate the magnitude of counterfeit-related costs, understanding why those costs recur requires examination of how

counterfeit risk is assessed and managed in practice. To that end, a recent government-sponsored, multi-laboratory round-robin evaluation was conducted to assess the effectiveness, consistency, and cost drivers associated with AS6171-based counterfeit detection workflows. The observations summarized here reflect generalizable patterns that are consistent with earlier industry inter-laboratory studies (see Fig. 1) and align directly with the cost escalation mechanisms documented in Section 4 [34].

In the round-robin evaluation, identical sets of suspect or known counterfeit electronic components were distributed to multiple participating laboratories for independent analysis, along with a control set of authentic components. Each laboratory examined the parts using the inspection and analytical methods available within its facility and documented the observed defects, test results, and final disposition regarding counterfeit determination. The results from all laboratories were then compiled and compared to assess variability in defect detection, interpretation, and final classification outcomes, including both false-positive and false-negative determinations. Earlier inter-laboratory studies conducted by Honeywell followed a similar structure using a defined testing statement of work, while the later government-sponsored evaluation aligned laboratory activities with the procedures defined in AS6171. Together, these evaluations provide a consistent framework for examining how differences in testing execution and interpretation contribute to variability in counterfeit detection outcomes.

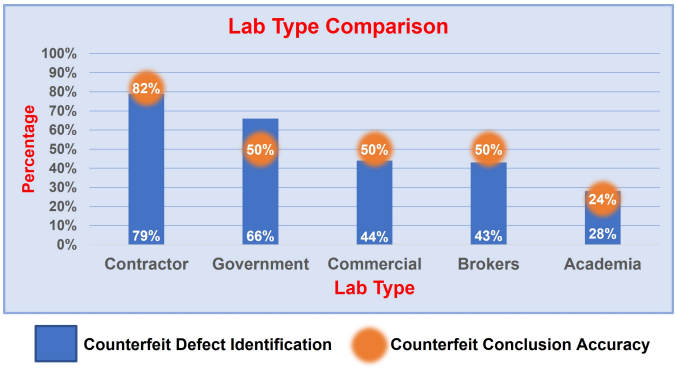

Fig. 1: Comparison of lab defect detection and counterfeit accuracy [35].

6.2. Study Results: A central observation from the latest evaluation was that interpretation, rather than defect detection, remains the primary limiting factor in counterfeit risk assessment. Across participating laboratories, test execution was generally competent and consistent with AS6171 requirements. Laboratories were typically able to identify observable defects when executing prescribed test methods. However, significant variability emerged in how those observations were interpreted, attributed to root cause, and mapped to counterfeit classifications. As a result, identical or near-identical findings often led to different final dispositions depending on the laboratory performing the assessment. This interpretive divergence, rather than deficiencies in test execution, was the dominant contributor to false-positive and false-negative outcomes.

Comparison with inter-laboratory evaluations conducted approximately a decade earlier indicates that performance remains inconsistent across evaluation years, with substantial variability persisting in false-positive and false-negative rates (see Fig. 2). While laboratories have advanced their technical capabilities and expanded test offerings, the fundamental challenge of consistently translating observations into defensible conclusions persists. In practice, laboratories continue to perform well at identifying what is visible, but struggle to consistently answer the more consequential question of why a defect is present and what it implies for authenticity and risk. The persistence of this gap suggests that incremental improvements in tools or procedures alone are insufficient to address the underlying issue.

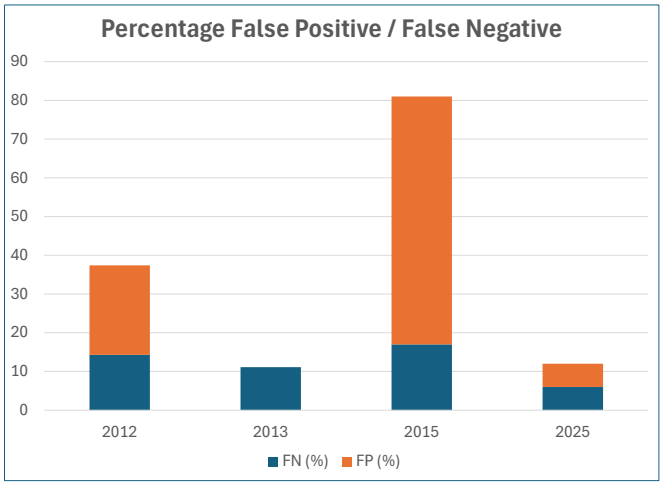

Fig. 2: False-positive and false-negative rates across inter-laboratory evaluations (2012–2025). Data derived from Honeywell round-robin presentations [34], [35] and subsequent inter-laboratory evaluations conducted with support from the U.S. Department of War Trusted & Assured Microelectronics (T&AM) Program [36].

The greatest divergence in outcomes was observed in test methods and workflows where procedural and interpretive guidance is least prescriptive. In such cases, laboratories exercised broad discretion in execution details, acceptance criteria, and interpretation of results. Even when underlying observations were similar, differences in how evidence was weighed and contextualized led to materially different conclusions. This lack of procedural and interpretive constraint limits repeatability and undermines confidence in results, particularly for higher-consequence parts and applications.

A related and recurring issue was inconsistency in defect categorization and evidence substantiation. Laboratories frequently documented observations without explicitly mapping findings into the AS6171 defect taxonomy [3] or clearly articulating how specific evidence supported a counterfeit determination. Similar defects were described using differ-

ent terminology, and supporting evidence varied widely in completeness and quality. These inconsistencies complicate comparison across laboratories, hinder effective peer review, and expand the scope of downstream investigation. In effect, a weak linkage between observations, taxonomy, and evidence increases both uncertainty and cost, directly contributing to the escalation mechanisms documented in the DLA case study.

6.3. Study Implications: The evaluation also reinforced the limitations of documentation-based traceability as a standalone control. While documentation is a necessary component of supply chain assurance, it is insufficient when disconnected from physical evidence and test results. Documentation can be falsified, misinterpreted, or incomplete, and without a stronger linkage between traceability records, observed defects, and physical parts, investigations tend to broaden rather than converge. As the scope expands, so do labor, testing, legal, and programmatic costs.

Importantly, the evaluation identified approaches that demonstrably improved consistency, confidence, and efficiency when applied. Where available, the use of golden samples, known-good comparative baselines, and detailed manufacturer reference data significantly improved laboratories' ability to distinguish manufacturing variation from counterfeit indicators. These reference points reduced reliance on subjective judgment and strengthened the evidentiary basis for conclusions, without requiring changes to AS6171 itself. Similarly, early application of objective, metric-based image analysis showed strong promise in standardizing how inspectors perceive surface features, markings, textures, and geometries. When used to augment, rather than replace, existing AS6171 workflows, such analytics improved triage efficiency and helped focus expert attention where risk was highest.

Despite these positive indicators, the evaluation made clear that isolated or lab-specific improvements do not scale or persist. Personnel turnover erodes institutional knowledge, local practices diverge over time, and the absence of standardized evidence expectations limits cross-organizational consistency. Moreover, without decision-support infrastructure to quantify cost-versus-coverage tradeoffs, laboratories and program offices are often forced to choose between over-testing and under-assurance, both of which drive unnecessary cost. The lack of a formal feedback loop between observed variability and standards refinement further limits systemic improvement.

Taken together, these findings lead to a clear conclusion. The dominant drivers of counterfeit-related cost are not the absence of standards or testing capability, but the lack of scalable decision support, consistent evidence traceability, and optimized application of existing methods. Addressing these gaps requires targeted investment focused on strengthening how AS6171 workflows are selected, executed, interpreted, and documented, rather than expanding testing indiscriminately. These observations directly inform the recommended next steps outlined in Section 7, which focus on funding a traceability-centered proof of concept designed to reduce both cost and risk while improving consistency and confidence in counterfeit mitigation outcomes.

VII. Implications for Traceability and Risk Reduction

7.1. Supply Chain Traceability: The cost escalation illustrated in Section 4 and the recurring failure modes described in Section 6 point to a common conclusion: counterfeit microelectronics are not primarily a problem of insufficient testing or missing standards, but of how existing tools, data, and evidence are applied across the supply chain. The dominant cost drivers arise when suspect material is discovered late, when the investigation scope cannot be bounded, and when decision-making relies on subjective interpretation rather than traceable, auditable evidence. Addressing these issues requires targeted investment focused on traceability and decision support rather than broader or more indiscriminate testing.

A central implication of this analysis is that traceability should be treated as a risk-reduction and cost-avoidance mechanism, not merely as a compliance requirement. Traceability is linked to improved risk-awareness and improved consumer trust and confidence [37]. When traceability is limited to documentation that is disconnected from physical parts and test evidence, investigations tend to expand rather than converge. For networked devices, that evidentiary thread must also extend to software/firmware provenance and configuration baselines, because counterfeit substitution can create cybersecurity assurance burdens that further expand investigation scope and cost. Conversely, when traceability links procurement records, physical artifacts, test results, and disposition rationale into a coherent evidentiary thread, programs are better positioned to isolate affected material quickly, limit downstream impact, and avoid unnecessary remediation. Funding a traceability-focused proof of concept provides an opportunity to demonstrate this effect in a controlled, measurable way.

Such a proof of concept should focus on integrating traceability with how counterfeit risk decisions are actually made. Rather than attempting to replace existing standards or laboratory expertise, the objective is to strengthen the decision infrastructure that surrounds AS6171 workflows. This includes improving how test plans are selected based on risk and consequence, how evidence is captured and substantiated, and how findings are interpreted consistently across laboratories and programs. By doing so, traceability becomes an enabling function that supports earlier detection, narrower investigation scope, and more defensible disposition decisions. This type of analytic service could be offered as part of a larger traceability system in an analytics marketplace where trusted third party providers could offer services, standardized analytics, and remediation recommendations through the same evidence (provenance) traceability capability described above.

Another implication is the need to move from static, checklist-driven testing toward a more optimized application of existing methods. As observed in recent inter-laboratory evaluations, laboratories often face a tradeoff between cost, turnaround time, and confidence, yet lack tools to quantify

those tradeoffs explicitly. Investments that enable cost-versus-coverage optimization—grounded in empirical performance data—can reduce unnecessary testing while preserving or improving risk coverage. When coupled with traceability, such optimization helps ensure that testing effort is commensurate with consequence, rather than applied uniformly regardless of risk.

7.2. From Data to Decision Making: The findings also highlight the importance of strengthening evidence consistency and interpretability. Variability in defect categorization, evidence substantiation, and disposition rationale drives both technical disagreement and cost escalation. Targeted investment in standardized evidence capture, clearer mapping to established defect taxonomies, and explainable analytic support can reduce subjectivity without diminishing the role of expert judgment. Importantly, these improvements enhance auditability and confidence, which are critical when counterfeit determinations have legal, contractual, and operational implications.

From a risk-reduction perspective, these investments directly address the mechanisms that lead to high downstream costs. Earlier and more confident detection reduces the likelihood of field escapes. Better evidence traceability limits the need for broad lot sweeps and extended investigations. More consistent interpretation reduces false positives that drive unnecessary redesigns and DMSMS actions. Taken together, these effects reduce both the frequency and severity of high-cost counterfeit events.

Finally, the analysis underscores that the cost of inaction is not neutral. As systems age, supply chains become more complex, and adversarial activity continues to evolve, the likelihood of counterfeit exposure persists. Without improved traceability and decision support, programs will continue to rely on reactive responses that incur substantial investigation and remediation costs, even when initial procurement values are modest. In this context, funding targeted traceability and risk-reduction activities represents a pragmatic investment in cost avoidance and mission assurance rather than an expansion of compliance burden.

In summary, the implications of this work are clear. Reducing the cost and consequences of counterfeit microelectronics does not require reinventing standards or dramatically expanding testing. It requires focused investment in a traceability-centered decision infrastructure that strengthens how existing methods are applied, interpreted, and trusted. A well-scoped proof of concept provides a low-risk path to empirically demonstrate these benefits and inform broader adoption through measurable reductions in cost, variability, and risk.

VIII. Conclusion

Counterfeit microelectronics continue to pose a persistent challenge for defense and other high-reliability systems, not because the problem is poorly understood, but because its true cost is often underestimated. As this paper has shown, the financial and operational consequences of counterfeit exposure are driven less by the value of the affected components and more by the uncertainty, scope expansion, and programmatic disruption that follow once trust in system integrity is called into question.

The cost mechanics associated with counterfeit incidents explain why relatively modest procurements can escalate into multi-million-dollar impacts. Late detection, weak linkage between evidence and physical parts, and inconsistent interpretation of test results all contribute to expanded investigations and costly remediation. These mechanisms are not hypothetical; they are reflected in modeled case analyses and reinforced by observed patterns in inter-laboratory evaluations. Together, they demonstrate that counterfeit-related costs are systemic and nonlinear, and that traditional procurement metrics provide little insight into true exposure. Although this paper focuses on counterfeit electronics, similar cost escalation dynamics, safety implications, and mission consequences occur across other counterfeit materiel categories; Appendix A provides illustrative examples.

Importantly, the findings presented here indicate that reducing the cost and consequences of counterfeit microelectronics does not require abandoning existing standards or dramatically expanding testing. Rather, meaningful risk reduction can be achieved by strengthening the application of current tools and methods. Investments that improve traceability, support consistent interpretation, and enable earlier, more confident decision-making directly target the drivers of cost escalation. By reducing uncertainty and bounding the investigation scope, such investments offer a practical path to cost avoidance and improved mission assurance.

The implications for policy and acquisition are clear. Treating traceability primarily as a documentation artifact for compliance rather than as decision infrastructure leaves organizations dependent on reactive responses that are both expensive and disruptive. In contrast, targeted, traceability-centered investments—such as a focused proof of concept—provide an opportunity to demonstrate measurable reductions in variability, cost, and risk using existing workflows and standards. Even under conservative assumptions, the potential return on such investments is significant when compared to the modeled costs of unmanaged counterfeit exposure.

In closing, counterfeit microelectronics should be understood not as an occasional anomaly, but as an enduring risk that demands a more deliberate and data-informed response. By shifting the focus from reactive remediation to proactive risk reduction through improved traceability and decision support, organizations can better protect system integrity, control costs, and sustain confidence in the supply chains that underpin critical missions.

Appendix A
Costs Related to Non-Electronic Counterfeits (i.e., Mechanical/Materials)

Over the years, there have been many other counterfeits that have had very serious effects on Government Programs,

industry, and the general public, costing millions of dollars and, in some instances, lives.

Counterfeit Fasteners: Counterfeit fasteners (fasteners masquerading as legitimate but failing to meet required specifications) pose extreme dangers in military applications, aviation/aerospace, construction, the energy sector, and more. Counterfeit fasteners may look genuine, but they often lack the mechanical strength, traceability, and consistency necessary for mission-critical operations. Their presence jeopardizes both equipment functionality and personnel safety. Manufacturers of counterfeit fasteners often take low-grade steel and stamp it with head markings that indicate a much higher strength or grade.

In the 1980s, an influx of counterfeit Grade 8 and Grade 5 bolts infiltrated into the US from foreign sources. This problem continued for years, sadly culminating in the crash of Partnair Flight 394, which cost the lives of 55 people because of three counterfeit bolts. That led to the U.S. Fastener Quality Act (updated three times), which has reduced the number of incidences of counterfeit fasteners in the United States.

To assist the Government and industry entities in detecting/avoiding counterfeit fasteners, the SAE G-21H Committee (Counterfeit Fastener Prevention) drafted and published AS 6832 "Counterfeit Materiel, Assuring Acquisition of Authentic and Conforming Fasteners".

Counterfeit Refrigerant: In late 2010, the refrigeration compressors on two refrigerated shipping containers (called reefers) violently exploded in Vietnam and Brazil, killing the three men repairing them. At the same time, another reefer serviced at the same location as the first two was found at the Port of Los Angeles smoking and spewing foam, requiring a total evacuation of that area. The United States Government immediately stopped all reefers from entering the U.S. while awaiting test results. It was determined that the explosions resulted from the refrigeration units on the reefers being charged with counterfeit refrigerant.

What is counterfeit refrigerant made of, and why is it bad? Just about any compressed gas can be used to counterfeit refrigerant, but some are harder to detect and more damaging. Use of counterfeit refrigerant will damage/contaminate equipment, increase operating/maintenance costs, damage the environment, and possibly cause fires, explosions, and deaths. Counterfeiters use mixes of old refrigerants like R-12 and R-22; ammonia; flammables such as propane, ethane, and/or butane; or dangerous substances such as R-40 (methyl chloride). R-40 is an old refrigerant that was phased out years ago, but is still readily available and cheap, used in the plastics industry. This gas is highly flammable, poisonous, carcinogenic, and toxic, has no real discernible smell, and when inhaled, can make personnel high. It is also extremely corrosive – it eats plastic and aluminum. The problems really happen when R-40 eats aluminum because of a by-product called Trimethylaluminium (TMA). TMA is a clear liquid that will end up at the bottom of a compressor, where it is impossible to safely remove. It is pyrophoric (spontaneously combusts in the presence of oxygen), and when exposed to certain other chemicals and to common fire suppressants such as water, CO2, or halon, it will violently explode.

Legislative obsolescence is the term used to describe what happens to the availability of certain refrigerants because of the limits set by the United Nations – the Montreal Protocol limits the use and availability of ozone-depleting substances, and the Kyoto Protocol seeks to reduce the onset of global warming by reducing greenhouse gases. In other words, some countries can no longer manufacture or import certain refrigerants, which are still in demand for existing older equipment. Other countries may not be able to buy or sell certain new refrigerants.

Currently, the threat of counterfeit refrigerant has increased significantly in the United States, due to adding R-22 to the list of refrigerants that can no longer be manufactured or sold as new. R-22 is still in very high demand for home air conditioning, but it is becoming more difficult to obtain, which makes it a bigger target for counterfeiting. There have been a number of seizures of counterfeit refrigerant in the U.S. recently. There are now warnings posted online that if you or your company have purchased, sold, or used counterfeit refrigerants, you are at risk of investigation by the Environmental Protection Agency, the Internal Revenue Service, and even the United States Customs Service if you imported the product. The problem of counterfeit refrigerant outside of the U.S. continues to grow as well. There are over 1.3 million reefers being used worldwide, and it is estimated that 10-15% of the world's fleet is contaminated with counterfeit refrigerant. The European Union (EU) introduced the phase-down mechanism to gradually reduce the consumption of high Global Warming Potential refrigerants, like R134a, which, until recently, was the most common air conditioning refrigerant used by the world's vehicle manufacturers. That higher demand for R-134a is increasing the desirability for counterfeiting it as well.

To assist Government and industry entities to detect/avoid counterfeit refrigerant, the SAE G-21R Committee (Counterfeit Refrigerant Prevention) drafted and published AS6886 "Counterfeit Materiel: Assuring Acquisition and Use of Authentic and Conforming Refrigerant".

ACKNOWLEDGMENT

Portions of the inter-laboratory proficiency data summarized in Fig. 2 were developed with support from the U.S. Department of War under the Trusted & Assured Microelectronics (T&AM) Program [36]. The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the U.S. Government.

REFERENCES

[1] M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer International Publishing, 2015.

[2] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[3] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[4] U.S. Department of Justice, Office of Public Affairs, "CEO of Dozens of Companies and Entities Charged in Scheme to Traffic an Estimated $1 Billion in Fraudulent and Counterfeit Cisco Networking Equipment," 2022. Press Release, July 8, 2022, https://www.justice.gov/archives/opa/pr/ceo-dozens-companies-and-entities-charged-scheme-traffic-estimated-1-billion-fraudulent-and.

[5] U.S. Senate Armed Services Committee, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," 2012. Press Release, U.S. Senate, https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts.

[6] SAE G-19A Test Laboratory Standards Development Committee, "Test methods standard; general requirements, suspect/counterfeit, electrical, electronic, and electromechanical parts," 2016, https://www.sae.org/standards/content/as6171.

[7] SAE G-19A Test Laboratory Standards Development Committee, "AS6171/1: Suspect/Counterfeit Test Evaluation Method," 2016, https://saemobilus.sae.org/content/as6171/1.

[8] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[9] Z. Collier, S. Walters, D. DiMase, J. Keisler, and I. Linkov, "A Semi-Quantitative Risk Assessment Standard for Counterfeit Electronics Detection," *SAE International Journal of Aerospace*, vol. 7, no. 1, pp. 171–181, 2014.

[10] D. DiMase, Z. Collier, J. Carlson, R. Gray Jr., and I. Linkov, "Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems," *Risk Analysis*, vol. 36, no. 10, pp. 1834–1843, 2016.

[11] U.S. Senate Committee on Armed Services, "The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain." Senate Hearing, 112th Congress, 2nd Session, 2011. S. Hrg. 112-340. Available: https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf.

[12] P. Sandborn, "Design for Obsolescence Risk Management," *Procedia CIRP*, vol. 11, pp. 15–22, 2013.

[13] Z. Collier, D. Henderson, and J. Kopf, "Protecting Intellectual Property in Low Trust Environments: Game Theoretic Modelling of Overproduction in Contract Manufacturing," *International Journal of Intellectual Property Management*, vol. 14, no. 5, pp. 444–458, 2024.

[14] U.S. Department of Energy, Office of Environment, Health, Safety and Security, "Operating Experience Level 3 (OE-3) 2022-01: Suspect/Counterfeit and Fraudulent Networking Products," 2022. Web page, Oct. 14, 2022, https://www.energy.gov/ehss/articles/operating-experience-level-3-2022-01-suspectcounterfeit-and-fraudulent-networking.

[15] R. Anderson and T. Moore, "The Economics of Information Security," *Science*, vol. 314, pp. 610–613, 2006.

[16] L. Gordon and M. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information System Security*, vol. 5, no. 4, pp. 438–457, 2012.

[17] S. Shackelford, "Should Your Firm Invest in Cyber Risk Insurance?," *Business Horizons*, vol. 55, pp. 349–356, 2012.

[18] G. D'Anna and Z. Collier, *Cybersecurity for Entrepreneurs*. SAE International, 2023.

[19] P. Sandborn, *Cost Analysis of Electronic Systems*. World Scientific, 2016.

[20] J. Graf, W. Batchelor, S. Harper, R. Marlow, E. Carlisle IV, and P. Athanas, "A Practical Application of Game Theory to Optimize Selection of Hardware Trojan Detection Strategies," *Journal of Hardware Systems Security*, vol. 4, no. 2, pp. 98–119, 2020.

[21] Z. Collier, B. Briglia, T. Finkelston, M. Manasco, D. Slutzky, and J. Lambert, "On Metrics and Prioritization of Investments in Hardware Security," *Systems Engineering*, vol. 26, pp. 425–437, 2023.

[22] U.S. Department of Justice, U.S. Attorney's Office, District of New Jersey, "CEO of Dozens of Companies Sentenced to 78 Months in Prison for Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment," 2024. Press Release, May 2, 2024, https://www.justice.gov/usao-nj/pr/ceo-dozens-companies-sentenced-78-months-prison-massive-scheme-traffic-fraudulent-and.

[23] M. Olama and J. Nutaro, "Secure it now or secure it later: The benefits of addressing cybersecurity from the outset." Proceedings of SPIE, 2013.

[24] U.S. Department of Commerce, Bureau of Industry and Security, "Diminishing Manufacturing Sources and Material Shortages (DMSMS): Cost Metrics." Bureau of Industry and Security, U.S. Department of Commerce, February 2015. Available: https://www.bis.gov/media/documents/dmsms-cost-metrics-report-2015-final.pdf.

[25] Defense Standardization Program Office, "Diminishing Manufacturing Sources and Material Shortages (DMSMS): A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program (SD-22)." Defense Standardization Program Office, Department of Defense, December 2025. Working Draft—FY24. Available via ASSIST, http://assist.dla.mil.

[26] S. Foster and S. Walters, "A Proficiency Scheme for Counterfeit Part Testing Effectiveness," 2022. Presented at the Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, Surface Mount Technology Association (SMTA), CALCE/SMTA Symposium on Counterfeit Parts and Materials (SCEP) 2022. Listed in SCEP 2022 Proceedings. Available: https://web.calce.umd.edu/symposiums/SCEP2022_Proceedings.html.

[27] U.S. Senate Armed Services Committee, "Hearing on Counterfeit Electronic Parts in Defense Systems: Testimony of Lieutenant General Patrick J. O'Reilly, USA, Director, Missile Defense Agency," Nov. 2011. Written testimony, Nov. 8, 2011. Available: https://www.armed-services.senate.gov/download/2011/11/08/patrick-oreilly-testimony-110811.

[28] U.S. Department of Justice, U.S. Attorney's Office, Southern District of Ohio, "Business Manager Sentenced to Prison for Crimes Involving More Than $2 Million in Department of Defense Contracts." Press Release, Jan. 2019.

[29] U.S. Department of Justice, U.S. Attorney's Office, District of New Jersey, "CEO of Dozens of Companies and Entities in Florida and New Jersey Admits Role in Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment," 2023. Press Release, June 6, 2023, https://www.justice.gov/usao-nj/pr/ceo-dozens-companies-and-entities-florida-and-new-jersey-admits-role-massive-scheme.

[30] The Straits Times (via Reuters), "Hack of Hezbollah devices exposes dark corners of Asia supply chains," 2024. News article, Sept. 20, 2024, https://www.straitstimes.com/asia/hack-of-hezbollah-devices-exposes-dark-corners-of-asia-supply-chains.

[31] G. Cokins, "Measuring the Cost of Quality for Management," *Quality Progress*, vol. 39, no. 9, pp. 45–51, 2006.

[32] H. Miller and C. Griffy-Brown, "Developing a Framework and Methodology for Assessing Cyber Risk for Business Leaders," *Journal of Applied Business and Economics*, vol. 20, no. 3, pp. 34–50, 2018.

[33] I. Linkov, E. Anklam, Z. Collier, D. DiMase, and O. Renn, "Risk-Based Standards: Integrating Top-Down and Bottom-Up Approaches," *Environment Systems and Decisions*, vol. 34, pp. 134–137, 2014.

[34] S. Walters, "Round Robin Testing/Results." Presentation (Honeywell) at the 7th Annual NASA Supply Chain Quality Assurance Conference, NASA Goddard Space Flight Center, Greenbelt, MD, 2014. Honeywell International, Inc.

[35] S. Walters, "2015 Counterfeit Avoidance Round Robin Test Results." Presentation (Honeywell) at a CHASE (Center for Hardware Assurance, Security and Engineering) event, University of Connecticut, 2015. Event program not publicly archived; citation is to the presentation materials.

[36] Office of the Under Secretary of War for Research and Engineering, "Trusted & Assured Microelectronics." Program web page, 2026. Available: https://www.cto.mil/tam/.

[37] G. Razak, L. 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.