2026 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
CYBERSECURITY TECHNICAL SESSION
AUGUST 11-13, 2026 - NOVI, MICHIGAN

COUNTERFEIT AVOIDANCE AND QUALITY ASSURANCE: SUPPLY CHAIN SCREENING OF COTS MICROELECTRONICS IN TACTICAL SYSTEM

Carlos R. Aguayo Gonzalez, PhD[1], Ken Roberson[2]

[1]PFP Cybersecurity, Vienna, VA
[2]NCS Technologies, Manassas, VA

ABSTRACT

This paper details the successful scaling demonstration of a comprehensive supply chain screening process for commercial off-the-shelf (COTS) motherboard subassemblies used in tactical servers for naval applications. Our approach leverages Power Fingerprinting (PFP) technology, which uses unintended analog emissions and machine learning to provide independent, non-destructive, and scalable integrity assessment of microelectronics. The primary goal of the effort was to demonstrate the effectiveness and scalability of the PFP screening process without disrupting or delaying the manufacturing workflow. The screening successfully detected hardware and firmware modifications and identified two cases of abnormal behavior: unusual BIOS power reset and elevated CPU sensor readings on two motherboard subassemblies. Following our quality control forensic analysis, we determined the root cause of these anomalies and their potential impact on the host platform.

1. INTRODUCTION

The introduction of modern IT technologies into weapon systems and platforms promises significant cost reductions and increased flexibility and scalability. Techniques such as virtualization remove reliance on specific hardware and enables the use of COTS components. The underlying hardware platform is often considered beyond the reach of cyber attacks. Unfortunately, server hardware platforms have several components and firmware that can be used as attack vectors in a complex global untrusted supply chain. Supply chain attacks can be extremely difficult to detect using traditional measures. Traditional supply chain approaches, such as destructive physical inspection and provenance and traceability analysis, including cryptographic signatures, provide only partial resolution for microelectronics. They are limited in scalability, do not directly validate the physical component itself, and are often infeasible to apply across deployed platforms. Integrity assessment approaches based on unintended analog emissions—with artificial intelligence and machine learning (AI/ML)—have been developed and demonstrated to provide an independent,

non-destructive, and scalable integrity assessment of microelectronics components and microsystems. Power Fingerprinting (PFP) is one of these approaches which directly measures the physical characteristics of chips, boards, subassemblies, and systems to verify the integrity of actual hardware and firmware beyond traditional supply chain documentation or signatures. The PFP technology uses a physical sensor to capture fine-grained side-channel signals, which contain tiny patterns that emerge during operation and which are unique to the hardware and firmware in the target device. PFP has already been demonstrated for technological feasibility and operational utility in military-context pilots.

This paper presents the results of a scaling demonstration of a comprehensive supply chain integrity assessment screening using PFP technology of COTS motherboard subassembly hardware and firmware components during the manufacture of tactical servers for naval applications. This integrity assessment screening process is designed to prevent tampered, counterfeit, or substandard components from entering the supply chain. It safeguards the stability, performance, and life expectancy of mission-critical systems, ensuring they remain uncompromised. The ultimate goal of this effort is to demonstrate scalability and effectiveness of the integrity screening approach and to ensure it does not disrupt or delay the manufacturing process.

2. BACKGROUND AND RELATED WORK

2.1. Supply Chain Risk in COTS Microelectronics

Defense and tactical platforms increasingly rely on commercial off-the-shelf (COTS) microelectronics to reduce cost and accelerate deployment. These components are sourced and assembled through complex global supply chains that introduce risk from counterfeit parts, unauthorized hardware modifications, malicious or altered firmware, and latent manufacturing defects. For mission-critical systems, such compromises can affect reliability, performance, and operational safety[1].

Traditional acceptance testing and quality control processes are not designed to provide continuous or scalable assurance of microelectronics integrity at manufacturing time. As a result, there is a need for screening approaches that can be applied in production environments to identify compromised or anomalous hardware without delaying manufacturing workflows.

2.2. Limitations of Existing Assurance Techniques

Current microelectronics assurance practices rely on supplier vetting, documentation review [2], visual inspection, electrical testing, and functional validation. While effective for detecting gross defects and ensuring nominal functionality, these methods have limited sensitivity to subtle hardware modifications, firmware alterations, or configuration drift that does not immediately affect functional outputs [3].

Advanced techniques such as destructive physical analysis and reverse engineering provide high confidence but are inherently incompatible with production screening due to cost, time, and the destructive nature of the

analysis [4]. As a result, they are typically applied only to small sample sets or forensic investigations rather than broad manufacturing deployments.

2.3. Power Fingerprinting Integrity Assessment

Power Fingerprinting (PFP) is a non-intrusive integrity assessment technique for critical systems for detecting unauthorized modifications across the full execution stack, including hardware, firmware, and software [5] [6]. Operating through an independent physical sensing device, PFP introduces negligible overhead on the target platform, is agnostic to the operating environment, and is applicable to modern, legacy, and resource-constrained systems. This enables detection of integrity violations arising from malicious software, firmware manipulation, hardware tampering, or counterfeit components introduced through untrusted supply chains.

PFP performs fine-grained anomaly detection by analyzing unintended side-channel emissions captured during operation. These emissions contain distinctive patterns that reflect the combined behavior of the platform's hardware and software. A central element of PFP is the establishment of reference baselines that characterize the expected range of side-channel behavior for known-good devices, including normal inter-device variability. Once established, these baselines enable scalable manufacturing-time screening and ongoing integrity assessment to prevent compromised or substandard components from entering mission-critical systems (See Figure 1).

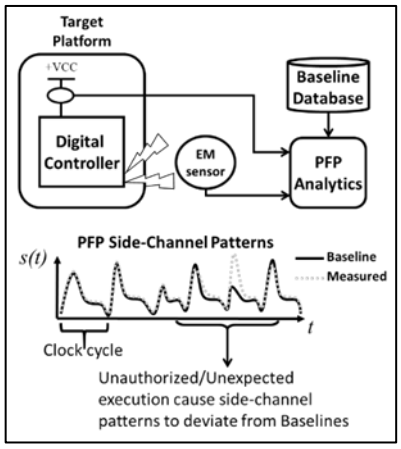

Figure 1: Recommended layout options for text boxes containing figures, tables or code listings.

3. METHODOLOGY

3.1. Target Platform: Motherboard Subassemblies

For this scaling demonstration, we target Submarine Warfare Federated Tactical Systems (SWFTS) motherboard subassemblies, based on Supermicro X12SPW-TF motherboard and 3rd Gen Intel Xeon Scalable processor (LGA-4189) with up to 40 cores [7]. The motherboards are optimized for high-performance, high-end computing platforms that address the needs of next generation server applications and are currently used in production of tactical systems, at full volume scales. The motherboards boot a BMC (Baseboard Management Controller) from ASPEED which provides essential out-of-band management capabilities. This effort focused on characterizing unintended analog emissions associated with the following key components within the motherboard subassembly:

- BMC Flash
- BMC
- BIOS Flash
- CPU

These components were selected due to their critical role in system initialization, management, and operation, as well as their historical relevance to supply-chain, firmware, and hardware-based integrity threats. The location of the target components

relative to the motherboard subassembly is shown in Figure 2.

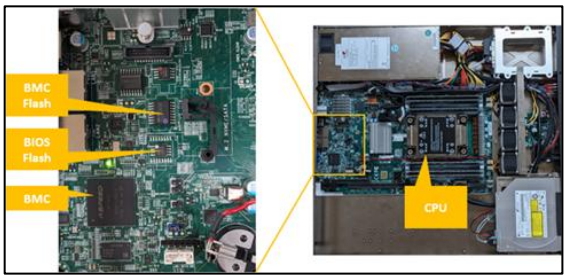

Figure 2: Target components from target motherboard.

3.2. Sensing modalities and Data Collection

The PFP solution collects unintended analog emissions using COTS sensors and digitizers. We focus on the near magnetic field in direct close proximity to the target components. We use a custom version of the Beehive Electronics 100A EMC Probe [8], which is magnetic field probe ideal for locating the sources of EMC emissions. The sensors are strategically placed using a 3D-printed harness, shown in Figure 3. that accurately and consistently positions the

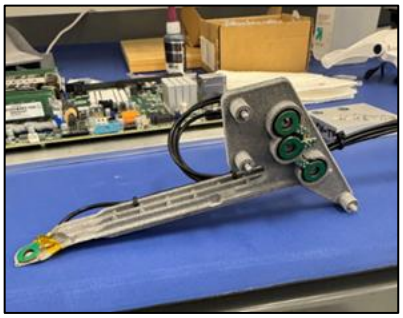

Figure 3: 3D printed sensor harness for accurate and consistency sensor placement.

highly sensitive EM sensors on the key components.

We developed a dedicated test fixture, shown in Figure 4, to provide controlled power, cooling, and signaling required to exercise target motherboards in a repeatable and automated manner. The fixture functions as a stand-alone screening station, delivering regulated power and maintaining stable thermal conditions through integrated active cooling to allow the safe execution of multiple boot cycles. Precision machining enables consistent accurate placement, while integrated alignment and retention features for the sensor harness ensure consistent sensor positioning, cable routing, and strain relief across repeated insertions.

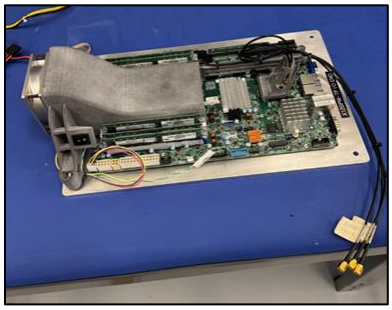

Figure 4: Test fixture for PFP Screening.

To digitize and capture the unintended analog emissions collected by the sensors from the various components within the Supermicro motherboard, we employed a suite of software-defined radios (SDRs). These SDRs collect the signals from the strategically positioned sensors to capture the near-field electromagnetic emissions from different components, as shown in Figure 5.

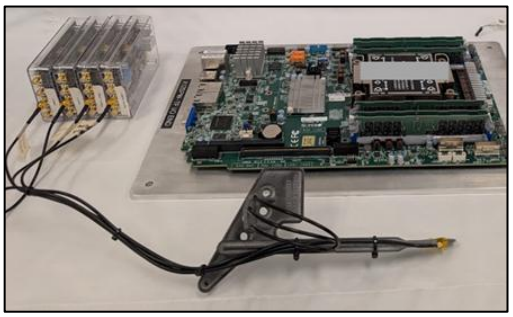

Figure 5: SDR Collector for EMI sensors in the harness.

3.3. Analytic Tools: PFP Siglytics Platform

Emissions data collected from the different sensors on the target components in the motherboards is analyzed using PFP's Siglytics platform, a sophisticated toolkit developed to extract discriminatory features from side-channels, manage side channel data, and uses powerful machine learning algorithms to determine normal patterns and detect anomalies. Leveraging over a decade of research and development, Siglytics' advanced algorithms and signal processing techniques enabled us to identify subtle variations in the collected side-channel data, such as changes in frequency, amplitude, or shape, which could be indicative of hardware or firmware tampering.

3.4. Integration into manufacturing process

1) Platform Enrollment and Baseline Definition

For each target platform, the PFP process begins with an enrollment phase that establishes the analytical and operational foundation for subsequent screening. Enrollment encompasses the activities required to identify and refine data collection and analysis parameters needed to achieve the desired detection performance. These activities include exploratory platform characterization, sensor selection and placement, configuration of data acquisition settings, and definition of analysis parameters that together enable reliable and repeatable integrity assessment for the specific motherboard design.

Beyond analytical setup, the enrollment phase prepares the system for scalable and automated screening. This includes development and validation of automation scripts, definition of standardized execution procedures, and end-to-end verification of the collection and analysis pipeline. The outputs of enrollment are designed to be directly transferable to production screening workflows, ensuring consistent application of PFP across manufacturing environments without additional platform-specific tuning.

Following completion of the enrollment process, an initial sample of 30 production motherboards is used to establish benchmark baselines for full-scale PFP screening. Data is collected from all boards using the sensor configuration, data acquisition settings, and analysis parameters defined during enrollment. The resulting dataset is used to train the PFP models, identify natural clustering within the population, characterize the expected emanation behavior of the platform, and quantify normal inter-device variability. These baselines are then incorporated into the PFP analysis tools, which are configured to use them as references for automated production screening of subsequent motherboards.

2) Production Screening

The screening process is executed by a technician on bare motherboards after they have had the CPU kit and the memory installed. Before initiating PFP screening, motherboards are outfitted with the production BMC and BIOS firmware versions. The technician places the motherboards on a test harness that provides power and cooling and installs the sensor harness. During screening, motherboards undergo multiple reset cycles, which are managed via automated IPMI (Intelligent Platform Management Interface) scripting to guarantee uniform test conditions, reducing variability and enhancing result reliability.

There are two screening stages: an initial test where sensor emanations are compared against predefined baselines (shown in **Error! Reference source not found.**), and a secondary analysis that compares screened motherboards against one another. Once a

motherboard clears the screening, it is passed to production for server assembly.

Figure 6: PFP screening results from a test motherboard showing a PASS assessment on all key components.

3) Handling Anomalies

If a motherboard displays abnormal behavior at either stage, it is sent to the Quality Control (QC) station, which corroborates abnormal behaviors and executes a predetermined forensic process when necessary. This forensic process is aimed at distinguishing between hardware and firmware issues, identifying the affected component, pinpointing the likely cause of anomalies, and determining when additional verification by a third party is needed.

3.5. Screening Results

We successfully screened thirty additional production motherboards as part of this scaling implementation for a total of 60 motherboards, with plans to expand to full production scale. As part of the screening, we introduced controlled changes to evaluate the ability of the process to detect modifications. Very importantly, we identified two cases of abnormal behavior: unusual BIOS reset and elevated CPU sensor readings on two motherboards.

1) Controlled Changes Validation: FW tamper emulation

To evaluate the effectiveness of our proposed approach in detecting tampering, we introduced various modifications to the different target components in the Supermicro motherboard. We perform a 1-2-1 test, in which the target device is measured three times with different firmware, with the first and third states being the same firmware version, and the second state being a different firmware version. In practical terms, this test collects one baseline reference from the device, then compares it against a collection with different firmware and a collection with the same firmware. In a 1-2-1 test, the PFP Siglytics™ analytics tool is expected to discriminate State 2, but match states 1 & 3.

For the validation tests we use the following configurations:

- State 1: Original Firmware
  - BMC: 01.04.13 - BIOS: 2.1
- State 2: Alternative Firmware
  - BMC: 01.01.45 - BIOS: 1.5
- State 3: Original Firmware again
  - BMC: 01.04.13 - BIOS: 2.1

Furthermore, in order to quantitatively determine whether different emanation features distributions can be considered a match against one another, we perform the two-sample Kolmogorov-Smirnov (KS) Test, to assess whether the two sample distributions are likely drawn from the same underlying population or if they are significantly different. The following sections include the results of the KS Test and the cumulative distribution functions (CDFs) for comparing the Original FW used as a reference against the Alternative firmware change (FAIL) and the second Original collection in the 1-2-1 test (PASS). The evaluation results also include plots from the PFP analytic tools depicting the Variance of Means (VOM) error, which represents the relative distance in the feature space between the different changes, indicating the ability of the tools to detect each change. The following figures show the validation results

for BMC Flash (Figure 7), BMC (Figure 8), BIOS Flash (Figure 9), and CPU (Figure 10).

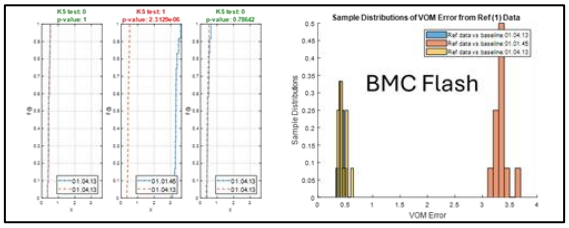

Figure 7: BMC Flash KS test results using Original FW version 01.04.13 as reference. Alternative FW version 01.01.45 correctly fails to match the reference, while Original FW correctly matches. Sample distributions, shown on the right, exhibit clear separation between original and alternative FW cases.

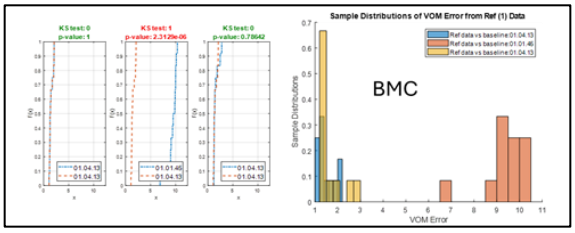

Figure 8: BMC KS test results using Original FW version 01.04.13 as reference. Alternative FW version 01.01.45 correctly fails to match the reference, while Original FW correctly matches. Sample distributions, shown on the right, exhibit clear separation between original and alternative FW cases.

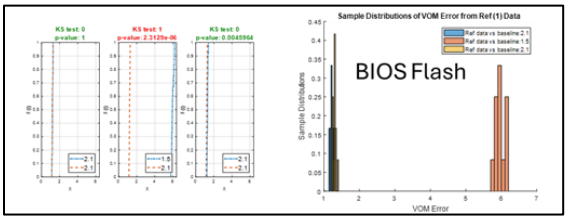

Figure 9: BIOS Flash KS test results using Original FW version 2.1 as reference. Alternative FW version 1.5 correctly fails to match the reference, while Original FW correctly matches. Sample distributions, shown on the right, exhibit clear separation between original and alternative FW cases.

The successful evaluation tests validate the parameters identified during the enrollment process and confirm the ability of the PFP tools to reliably detect modifications to the target system. The observed results demonstrate that the selected data collection and analysis settings provide sufficient sensitivity to identify deviations from expected behavior, supporting their suitability for use in production screening and integrity assessment workflows.

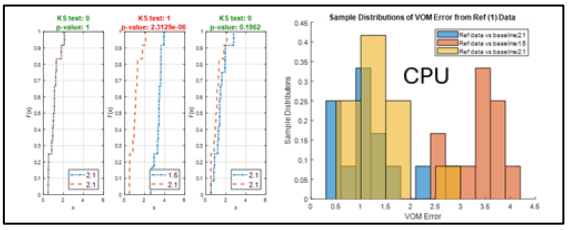

Figure 10: CPU KS test results using Original FW version 2.1 as reference. Alternative FW version 1.5 correctly fails to match the reference, while Original FW correctly matches. Sample distributions, shown on the right, exhibit clear separation between original and alternative FW cases.

2) Production Screening Findings: Abnormal Reset Behavior

During enrollment process, we observed abnormal BIOS reset behavior, which sporadically caused the boards to shut down and then power up, instead of restart. The abnormal behavior, shown in Figure 11, was observed in all test motherboards evaluated.

The abnormal reset behavior was only observed when production firmware was loaded on the motherboards, which is not the latest OEM release. The abnormal behavior is also captured in the system' s Maintenance Event Log, which show additional entries when the abnormal behavior happens, including a "Warning ... [MEL-0205] The user attempted to get the host FW user password", followed by a final successful reset event. Since the issue has been addressed in the latest firmware, and the firmware gets replaced in late integration stages, it was considered safe to proceed. We identified a workaround by modifying the automation scripts to perform a full power off and a power on instead of a soft reset.

Figure 11: Abnormal reset behavior in which the motherboards would shut down and then restart instead of reset.

3) Production Screening Findings: Non-conforming Units

In the second abnormal behavior case, two motherboards exhibited unusually high amplitudes in the CPU sensor readings compared to others. These abnormalities, shown in Figure 12 could be indicative of issues such as unauthorized modifications, quality deficiencies, or tampering, which pose a significant threat to both the operational life and reliability.

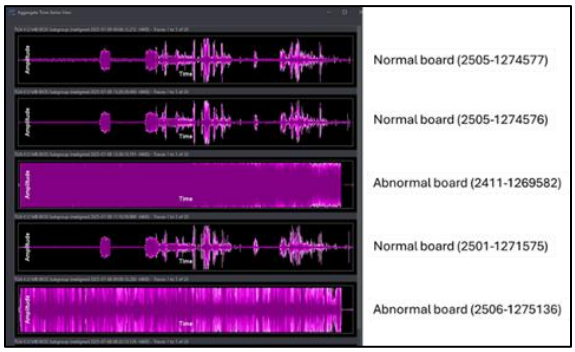

Figure 12: CPU sensor aggregate time-domain series plot showing differences on the emanations of two anomalous boards.

After verifying the consistency of these abnormalities, we implemented the Quality Control (QC) process's forensic analysis procedure to determine their root cause and assess the impact on the host platform. As part of our forensic procedure, which includes visual inspections and targeted tests with specialized equipment, we were able to determine that the abnormal behavior had a hardware origin, specifically the CPUs, rather than the motherboard or firmware components, and we were able to identify the most probable cause of these anomalies.

As part of the forensic procedure, we performed additional spectral analysis. The normal CPU had a large, wide spectral "bump" at a frequency which skipped the PFP Target Spectral region, as shown in Figure 13.

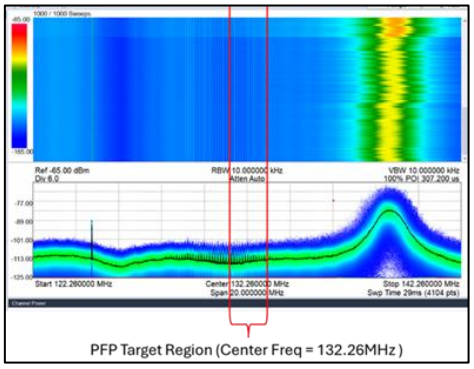

Figure 13: Spectral features from a normal CPU showing the interference away from the PFP target region.

In the two suspect CPUs, however, the "bump" did caused interference in the spectrum band of interest, as shown in Figure 14. Also, the interference was not static and seemed to be shifting around in frequency back and forth in random manner, although contained to ~3 or 4 MHz. The spectral characteristics in the abnormal CPUs had a close resemblance to those of voltage converters, which indicated the package power distribution network (PDN) as the source of the interference.

We performed a thermal pull test while monitoring the behavior of the spectral bump as the processor booted. The shifting of the

center frequency as the temperature increases confirmed that the abnormal spectral artifacts are driven by package PDN resonance being excited via broadband switching.

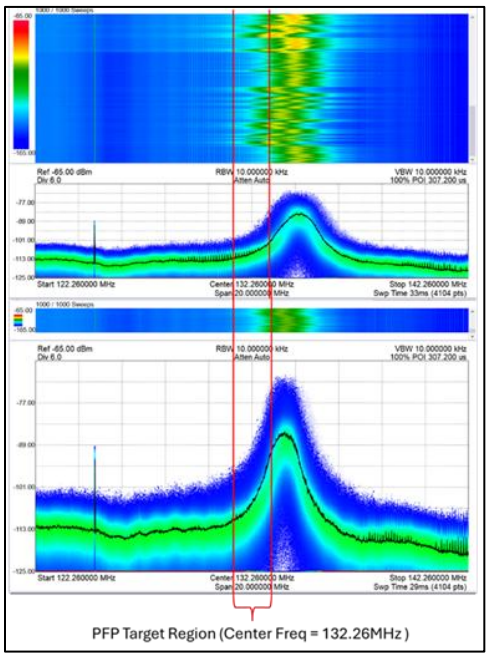

Figure 14: Spectral features from the suspect CPUs showing the interference encroaching the PFP target region.

The anomalous behavior was deemed not-malicious. The frequency shift in the resonance may not be inherently harmful yet clarified that the impedance of the Power Delivery Network (PDN) was different in the suspect CPUs, likely due to variance of the in-package capacitors which shifted the resonance characteristics outside of the range previously evaluated by PFP. Large impedance changes in a PDN, however, can cause power integrity/stability issues that can impact operation due to voltage drop under specific switching loads. The processors were removed from production for further testing.

4. CONCLUSIONS

We presented the results of a comprehensive supply chain integrity assessment scaling deployment of PFP technology on COTS motherboard hardware and firmware components during the manufacture of tactical servers. We successfully achieved the ultimate goal of this scaling implementation which is to demonstrate scalability and effectiveness of the integrity screening approach while ensuring it does not disrupt or delay manufacturing.

The implementation targeted Supermicro motherboard subassemblies which are COTS platforms commonly used in the manufacture of tactical systems. The screening process targeted unintended analog emissions from key motherboard components: BMC, BMC Flash, BIOS Flash, and CPU. We used PFP's Siglytics tools to analyze the emanations data, establish a reference baseline using machine learning, and to detect deviations.

The effectiveness of the screening approach was validated by detecting controlled hardware and firmware modifications introduced into the different. These modifications emulate firmware tampering of the BIOS and BMC and hardware modifications. During production motherboard subassemblies screening, we uncovered: abnormal BIOS reset behavior and unusually high amplitudes in the CPU sensor readings in two motherboard subassemblies. By implementing our Quality Control (QC) process's forensic analysis procedure we were able to determine the root cause and assess the impact on the host platform.

This successful implementation showed the ability of the integrity assessment screening process to prevent tampered, counterfeit, or substandard components from entering the supply chain. Furthermore, it safeguards the stability, performance, and life expectancy of

mission-critical systems, ensuring they remain uncompromised, without disrupting their production schedule.

5. REFERENCES

[1]M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2]GOMACTech. "Paper Submission." [Online]. Available: https://www.gomactech.net/paper_submission.html (access Dec. 5, 2023).

[3]V. J. Patel and N. G. Usechak, "Information Markings Guidance: Markings for GOMACTech Papers," Government Microcircuit Applications & Critical Technology Conference, December 2023.

[4]G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*.

[5]J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[6] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.