**Trading Static for Dynamic Power.** The simulation results reveal a clear power consumption tradeoff. The memristor-loaded amplifier's primary advantage is a 69.2 % reduction in leakage power, as the memristor's high off-state resistance effectively gates leakage current during idle periods. This makes the design highly suitable for applications where static power is a dominant concern. However, this static power benefit is coupled with a 10–12 % increase in average power during operation. This higher dynamic power is a direct consequence of the circuit's enhanced performance, as its faster response and higher gain require larger transient currents, effectively trading static power efficiency for improved speed [3, 6].

Speed vs. Signal Integrity.

The proposed design improves speed at the cost of signal fidelity. While sensing delay is reduced by up to 7.3 % due to higher gain from the memristive loads, this enhancement degrades signal integrity. The maximum output voltage swing is cut by 22.5 % due to an inherent voltage drop across the memristor. More critically, output noise increases by 52.5 %, as the stochastic physical process within the memristor introduces intrinsic noise that the amplifier's higher gain then magnifies. Therefore, the desirable speed improvement and detrimental noise increase are fundamentally linked in this design [4].

**Discussion and Conclusion.** The memristor-loaded sense amplifier is not a universal improvement over CMOS but a specialized design with clear tradeoffs. Its primary advantage is a 69.2 % reduction in leakage power, making it ideal for low-duty-cycle applications like IoT devices where static power is the main concern. However, it is poorly suited for high-performance computing due to increased dynamic power and degraded noise margins. In conclusion, integrating memristors requires a co-design paradigm, matching the device's unique properties to specific application needs. Future research should focus on mitigating its dynamic power and noise penalties while retaining its static power benefits.

**References**

1. Williams, R. How We Found The Missing Memristor / R. Williams // IEEE Spectrum. – 2008. – Vol. 45, № 12. – P. 28–35.

2. Ho, Y. Nonvolatile memristor memory: Device characteristics and design implications / Y. Ho, G. Huang, P. Li // Proceedings of IEEE/ACM International Conference on Computer Aided Design (ICCAD). – 2009. – P. 485–490.

3. Shin, S. Memristor-based fine resolution programmable resistance and its applications / S. Shin, K. Kim, S. Kang // 2009 International Conference on Communications, Circuits and Systems. – 2009. – P. 948–951.

4. Wang, N. On the design of MOS dynamic sense amplifiers / N. Wang // IEEE Transactions on Circuits and Systems. – 1982. – Vol. 29, № 7. – P. 467–477.

5. Wicht, B. Yield and speed optimization of a latch-type voltage sense amplifier / B. Wicht, T. Nirschl, D. Schmitt-Landsiedel // IEEE Journal of Solid-State Circuits. – 2004. – Vol. 39, № 7. – P. 1148–1158.

6. Wicht, B. Current sense amplifiers for embedded SRAM in high-performance system-on-a-chip designs / B. Wicht. – Heidelberg: Springer Verlag, 2002. – 198 p.

*UDC 681*

## THE SILICON SHIELD: A SYNERGISTIC, HARDWARE-ANCHORED ARCHITECTURE FOR NEXT-GENERATION CYBER RESILIENCE

**Musiiwa P. B.[1], Rushambwa M. C.[1], Gwamuri J.[1], Kanhukamwe Q. C.[1], Tyavlovsky A.[2], Svistun A. I.[2]**

*[1]Harare Institute of technology, Harare, Zimbabwe*
*[2]Belarusian National Technical University, Minsk, Belarus*

**Abstract.** The escalating sophistication of cyber threats, which now routinely target the hardware layer, has rendered traditional software-only security models insufficient.1 This paper challenges the long-held assumption that hardware constitutes an inherently trusted foundation, a premise invalidated by the rise of physical, side-channel, and supply chain attacks. It introduces the "Silicon Shield," an integrated, hardware-first security architecture designed to establish genuine cyber resilience from the ground up. This framework is built upon a triad of complementary security primitives: a Hardware Root of Trust (RoT) to ensure boot-time integrity, Trusted Execution Environments (TEEs) to protect data-in-use from compromised privileged software, and Physical Unclonable Functions (PUFs) to generate inherent, unclonable device identities. This paper posits that a holistic, secure-by-design approach, anchored in the immutable properties of silicon, is the only viable path toward building trustworthy computing systems in an increasingly hostile digital landscape.

**Keywords:** Silicon Shield, hardware cyber threats.

*Address for correspondence: Peter Bukelani Musiiwa, BE277 Belvedere Harare, Zimbabwe*
*e-mail: pbmusiiwa@hit.ac.zw*

**Introduction: Shifting the Security Paradigm.** For decades, cybersecurity has mistakenly assumed hardware is secure [1]. This flawed, software-focused approach is failing because adversaries now attack the silicon directly. A new hardware-based philosophy, the "Silicon Shield," [2] argues that true security must be rooted in the hardware itself [3]. This layered defense strategy combines three pillars: a Hardware Root of Trust, Trusted Execution Environments (TEEs) for isolated processing, and Physical Unclonable Functions (PUFs) for unique device identity. As increasingly sophisticated attackers exploit hardware

vulnerabilities with attacks like Spectre, building security from the silicon up is no longer optional but essential for creating a defensible system. The Modern Hardware Threat Landscape

Hardware security is threatened by physical, supply chain, and microarchitectural attacks. Physical attacks include monitoring power consumption or inducing faults to extract secret data [2, 4]. Supply chain threats involve inserting malicious "Hardware Trojans" or creating counterfeit components [3, 4]. Microarchitectural exploits, like Spectre and Meltdown, abuse processor features to leak information, while firmware attacks can install persistent rootkits. A Multi-Primitive Framework Silicon Shield's unified defense is built on three core hardware security primitives, each tackling a different security dimension for strength beyond any single technology.

**Hardware Root of Trust (RoT).** This is the system's foundational trust anchor. It uses technologies like TPM and Secure Boot to verify that all software, from firmware to the operating system, is authentic and untampered during startup, creating an unbroken "chain of trust" [3, 5].

**Trusted Execution Environments (TEEs).** TEEs protect data while it's in use by creating isolated, hardware-encrypted memory areas (like Intel SGX enclaves) [6]. This shield sensitive code and data from a compromised operating system, enabling confidential computing [7].

**Physical Unclonable Functions (PUFs).** A PUF acts as a chip's unique, unclonable fingerprint derived from microscopic manufacturing variations [7, 8]. It generates cryptographic keys on demand without ever storing them in memory, making it highly resistant to physical tampering and ideal for secure device authentication [8, 9].

**An Integrated Defense-in-Depth Strategy.** The strength of the Silicon Shield lies in the synergistic integration of its primitives, creating a mutually reinforcing, layered defense [10, 12]. In a practical implementation, a PUF generates a unique root key at power-on to bind a TPM's identity to the silicon. The TPM then anchors a Secure Boot process, creating a chain of trust, and can later attest to a TEE enclave's integrity, proving to a remote party that the secure environment is running on an authentic, untampered device [13, 15]. This layered approach ensures a compromise at one level does not lead to total system failure. The table shows that no single primitive is foolproof, but together they form a strong defense. TEEs guard against OS compromise but offer limited side-channel protection, while PUFs prevent cloning but don’t secure runtime execution. The Silicon Shield’s strength lies in layering complementary protections

Table 1 – Mapping Hardware Threats to Mitigation Primitives

| Threat Category | Hardware Root of Trust (TPM/Secure Boot) | Trusted Execution Environment (TEE) | Physical Unclonable Function (PUF) |
|---|---|---|---|
| Firmware Rootkits & Boot-time Malware | Primary Mitigation | Secondary Mitigation (Protects runtime) | – |
| Software-based Key Theft (from memory) | Secondary Mitigation (Key Wrapping) | Primary Mitigation (Protects data-in-use) | Primary Mitigation (Key is not stored) |
| Side-Channel Attacks (e. g., Power, Cache) | Limited | Partial Mitigation (Ongoing Research) | Limited |
| Hardware Trojans (in supply chain) | Limited (Attestation may fail) | Partial Mitigation (Can isolate Trojan) | Primary Mitigation (Authentication fails) |
| Physical Cloning / IP Theft | Limited | Secondary Mitigation (Code is encrypted) | Primary Mitigation (Physically unclonable) |
| OS/Hypervisor Compromise | Limited | Primary Mitigation (Isolation from OS) | – |
| Fault Injection Attacks | Limited | Partial Mitigation (Can detect anomalies) | Partial Mitigation (Tampering disrupts PUF) |

**Future-Proofing the Shield.** To remain effective, the Silicon Shield architecture must evolve to address emerging threats like quantum computing and increasing semiconductor complexity. To counter the "harvest now, decrypt later" danger posed by quantum computers, hardware Roots of Trust must be crypto-agile, ready to adopt Post-Quantum Cryptography (PQC) standards [14] As chip complexity makes detecting hardware Trojans intractable, AI/ML offers a solution by analyzing a chip's side-channel emissions for anomalies and identifying suspicious logic during the design phase, shifting verification from reactive to proactive [15].

**Conclusion.** The evolution of cyber threats has shattered the paradigm of software-only security and the assumption of a trusted hardware base, as attacks now target fundamental layers from firmware to the silicon itself, demanding a secure-by-design philosophy anchored in hardware. This paper presented the "Silicon Shield," a blueprint integrating a Hardware Root of Trust, Trusted Execution Environments, and Physical Unclonable Functions to create a robust, multi-layered defense. This synergistic strategy, where security primitives mutually reinforce one another, is essential for addressing future challenges like post-quantum cryptography and building the next generation of resilient, trustworthy systems.

**References**

1. Modern Hardware Security: A Review of Attacks and Countermeasures / O. Oleksenko [et al.] // ACM Computing Surveys. – 2025. – Vol. 58, № 3. – P. 1–38.

2. IOActive. Threat Brief: Low-level Hardware Attacks / IOActive Labs. – Seattle: IOActive, 2023. – 24 p.

3. Introduction to Hardware Security / M. Rostami [et al.] // Electronics. – 2015. – Vol. 4, № 4. – P. 763–784.

4. National Institute of Standards and Technology (NIST). IR 8517: Hardware Security Failure Scenarios – Potential Weaknesses in Hardware Design. – Gaithersburg: NIST, 2024. – 89 p.

5. National Institute of Standards and Technology (NIST). IR 8517: Hardware Security Failure Scenarios – Potential Hardware Weaknesses. – Gaithersburg: NIST, 2025. – 94 p.

6. Help Net Security. NIST report on hardware security risks reveals 98 failure scenarios. – 2024. – URL: https://www.helpnetsecurity.com/2024/05/22/nist-hardware-security-failure-scenarios/ (date of access: 15.11.2024).

7. Weis, S. Protecting Data In-Use from Firmware and Physical Attacks / S. Weis. – MIT Lincoln Laboratory, 2014. – 45 p.

8. Hardware-Based Cyber Threats: Attack Vectors and Defence Techniques / A. Kumar [et al.] // Journal of Hardware and Systems Security. – 2019. – № 2. – P. 112–129.

9. IEEE Micro Special Issue for Security / Guest eds.: R. Avizienis, T. Knight // IEEE Micro. – 2019. – № 4. – 120 p.

10. Hasselbach, D. Intel SGX Explained / D. Hasselbach. – Intel Corporation, 2020. – 32 p.

11. SEFCOM. TrustZone Explained: Architectural Features and Use / SEFCOM Research Group. – Arizona State University, 2016. – 28 p.

12. UKRISE. Security in the Era of Global Semiconductor Initiatives / UKRISE Task Force. – London: UK Government.

*UDC 681*

## IMPLEMENTATION OF ANDON IN A SEED PROCESSING PLANT FOR ENHANCED OPERATIONAL SUSTAINABILITY

**Mushiri T., Chikuruwo M. N. H., Dhliwayo S., Munjoma K., Chipfurwe Makoni B., Chikonobaya A., Chirere E., Jaya C., Mugutso I., Makomo J., Makumbe T., Mberi R., Njenje T., Hwendere C., Ranganai M., Maranga T., Sithole R., Chitiyo N., Borerwe A., Chita T.**

*Scientific and Industrial Research and Development Centre, Harare, Zimbabwe*

**Abstract.** This study implemented a low-cost, open-source Andon system at a seed processing plant in Zimbabwe to address chronic inefficiencies from manual fault monitoring. The system integrated ESP32 microcontrollers, MQTT protocol, Node-RED, and stack lights. Results showed a 42 % reduction in downtime, a 22 % increase in throughput, and 80 % of critical faults resolved within 8 minutes. The framework demonstrates how techno-localism and open-source ecosystems can foster sustainable, locally maintainable automation for agro-processing SMEs.

**Keywords:** Andon System, Operational Sustainability, Seed Processing, Open-Source, Techno-Localism.

*Address for correspondence: Scientific and Industrial Research and Development Centre, Zimbabwe, Harare, e-mail: achikonobaya@sirdc.ac.zw.*

**Introduction.** Seed processing plants are critical for food security, yet many in developing nations suffer from significant operational inefficiencies. Manual fault reporting leads to prolonged equipment downtime, reduced throughput, and compromised quality. This research addresses these challenges by adapting the lean manufacturing Andon principle a visual management tool for immediate fault signaling to a low-resource context. The study aims to enhance operational sustainability at the Scientific and Industrial Research and Development Centre (SIRDC) seed plant through a locally built, low-cost digital Andon system, contributing to the techno-localism discourse.

**Methodology.** The implementation followed a structured, four-stage methodology. First, Process Analysis mapped the seed cleaning, grading, treatment, and packaging lines to identify critical fault points. Second, the System Architecture was designed using a distributed IoT model. The field layer used ESP32 microcontrollers with manual call buttons on six key machines. The communication layer employed the MQTT protocol. A Raspberry Pi served as the central server, running Node RED for application logic, a SQLite database for data persistence, and a supervisory dashboard. Third, Hardware Implementation involved installing tri-colour stack lights and wiring them to the control system. Finally, Software Development created Node RED flows to manage MQTT communication, business logic, and the real-time dashboard for remote monitoring and alerts.

Results and Discussion. The system was successfully deployed and evaluated over several months. Key performance metrics showed substantial improvement, as summarized in Table 1.

Table 1 – Key Performance Indicators (KPIs) Before and After Implementation

| KPI | Before Implementation | After Implementation | Improvement |
|---|---|---|---|
| Average Downtime | Baseline | –42 % | Significant |
| Processing Throughput | Baseline | +22 % | Significant |
| Fault Resolution (< 8min) | Low | 80 % | Drastic |
| Quality Reject Rate | Baseline | –17 % | Notable |

Figure 1 – SIRDC Seed Plant after the implementation of the Andon System