Abstract

Authors: Ebtesam J. Alqahtani, Nouf J. Alqahtani, Prof. Mohammad H. Hammoudeh

Industrial Control Systems (ICS) form the backbone of critical infrastructure sectors. Their increasing interconnection with enterprise networks expanded the Operational Technology (OT) attack surface while maintaining strict real-time and safety constraints. Existing cybersecurity mechanisms relied primarily on perimeter-based defences and computationally secure cryptography, which introduced operational limitations and remained vulnerable to future quantum threats. A gap therefore existed for a defence architecture that preserved deterministic operation while enabling post-quantum resilience.

In this study, we experimentally validated a post-quantum cybersecurity defence mechanism called BlueSkyTec Technology (BST). The technology integrates Hardware-Rooted Cryptographic Identity (HRCI), and information-theoretically secure encryption within a unified identity-centric model. BST was selected as it represents a hardware-rooted, One-Time-Pad (OTP) based key-distribution architecture capable of meeting deterministic ICS timing constraints that conventional NIST standardised post-quantum algorithms cannot satisfy. Unlike zero-trust architectures, which address lateral movement at the network-policy level, BST provides cryptographic resilience against harvest-now-decrypt-later threats while maintaining microsecond-scale latency compatible with Programmable Logic Controllers (PLCs) cycles.

BST architecture consists of:

- The HRCI enabling device authentication bound to tamper-resistant hardware trust anchors
- The OTP encryption supported by quantum-derived entropy, providing information-theoretic confidentiality
- Identity-based communication enforcement in which each endpoint is authenticated using a HRCI derived from Physically Unclonable Function (PUF) or secure-element–bound key material
- Network policy permitting communication only among provisioned and verified HRCI identities, thereby enforcing an authorized identity space and implementing a zero-trust model across IT and OT boundaries

The architecture was evaluated within a simulated internet-connected ICS testbed representing modern critical infrastructure deployments. The environment comprised PLCs, a SCADA server, an engineering workstation, a Human Machine Interface (HMI), a historian server, and logically segmented IT and OT network zones, designed to replicate deterministic PLC and HMI communication cycles and UDP-based industrial traffic. Adversarial scenarios were derived from the MITRE ATT&CK for ICS framework to ensure realistic and reproducible threat coverage. Experimental evaluation considered both cybersecurity functional and non-functional performance. Functional performance included confidentiality, integrity, anti-tampering, and authentication. Non-functional metrics measured control-loop latency, throughput, environmental suitability, and interoperability.

Structured attack campaigns were designed to model realistic adversarial behaviours using controlled packet-level simulations. This included packet injection to emulate falsified or unexpected traffic patterns and unauthorized command attempts representing efforts to influence PLC behaviour without valid authentication. Additional scenarios assessed the system's ability to maintain confidentiality and authenticity of transmitted packets, ensuring that unverified identities could not access or impersonate trusted endpoints. Integrity experiment evaluated whether the system could detect and prevent unauthorised modification of packet contents during transmission. Finally, controlled tampering simulations were performed to verify that the defence mechanisms correctly identified and blocked attempts to alter, replay, or manipulate ICS traffic in alignment with MITRE ATT&CK for ICS techniques such as T0827 - Spoof Reporting Messages, T0820 - Manipulation of Control, and T0851 - Man-in-the-Middle.

Experimental results demonstrated comprehensive detection and prevention across evaluated attack scenarios. The HRCI mechanism prevented unauthorized lateral movement between IT and OT zones even when valid credentials were compromised because communication attempts lacking authenticated HRCI were automatically rejected at the policy enforcement layer. PLC logic integrity validation blocked malicious configuration uploads prior to execution, while the anomaly detection layer identified protocol and process deviations with high accuracy and negligible false positives. Across all adversarial scenarios executed within the simulated internet-connected ICS testbed,

the system consistently demonstrated strong functional and non-functional performance. Quantitatively, the system passed all confidentiality, integrity, authentication, and anti-tampering tests, correctly identifying and blocking attempts to alter, replay, or manipulate UDP-based industrial traffic. Non-functional performance also remained within operational limits; the latency stayed inside deterministic PLC–HMI timing requirements, throughput remained stable, and no measurable degradation in availability, environmental suitability, interoperability, or process-state stability was observed. Entropy analysis confirmed high-quality randomness, and key-uniqueness evaluation showed no statistical duplication across devices. The use of OTP-based encryption eliminated reliance on computational hardness assumptions, providing long-term resilience against anticipated quantum-era cryptanalytic threats.

Our key contributions are:

- Evaluate the BST architecture and its underlying security model
- Provide insights into the effectiveness of BST, deterministic security, and critically assess their suitability and limitations within ICS environments

Initial results demonstrated the feasibility of deploying post-quantum, identity-centric security mechanisms in safety-critical industrial environments. BST architecture proved to provide an effective ICS cybersecurity by addressing both present operational threats and emerging quantum risks while preserving system reliability and real-time performance.