World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Post-quantum zero-trust backbone: Securing critical infrastructure communications against quantum and conventional cyber threats

Winifred Chukwuebuka Ayogu *

Department of Cybersecurity and Networks, Tagliatela College of Engineering, University of New Haven, United States of America.

World Journal of Advanced Research and Reviews, 2025, 27(03), 581–595

Publication history: Received on 13July 2025; revised on 07 September 2025; accepted on 09 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3178

Abstract

The convergence of quantum computing capabilities and sophisticated cyberattacks poses unprecedented threats to critical infrastructure communications. Traditional cryptographic defenses and perimeter-based security models are increasingly inadequate against quantum-enabled adversaries and advanced persistent threats targeting operational technology (OT) environments. This paper presents a comprehensive framework for implementing post-quantum cryptography (PQC) within a zero-trust architecture to secure critical infrastructure communications across control centers, substations, hospitals, and ports. Our approach integrates NIST-endorsed quantum-resistant cryptographic suites with identity-first network segmentation, authenticated SCADA protocol encryption, and continuous verification mechanisms. The proposed framework addresses the unique challenges of legacy industrial systems while providing scalable security for hybrid OT/IT environments. Through systematic analysis of current vulnerabilities and implementation strategies, this research demonstrates how a post-quantum zero-trust backbone can prevent catastrophic cyberattacks while maintaining operational continuity in critical infrastructure sectors.

Keywords: Post-Quantum Cryptography; Zero-Trust Architecture; Critical Infrastructure; SCADA Security; Quantum-Resistant Cryptography; Industrial Control Systems

1. Introduction

Critical infrastructure systems form the backbone of modern society, encompassing power grids, water treatment facilities, transportation networks, and healthcare systems. The increasing digitization and interconnectedness of these systems have created unprecedented attack surfaces that malicious actors continuously exploit (Alcaraz and Lopez, 2021). The emergence of quantum computing capabilities further exacerbates these vulnerabilities, as quantum algorithms threaten to render current cryptographic protections obsolete within the next decade (Kostenko et al., 2024).

Traditional security approaches based on perimeter defense and static trust relationships are fundamentally inadequate for protecting critical infrastructure in the quantum era. The concept of zero-trust architecture (ZTA) has emerged as a paradigm shift that assumes no implicit trust and requires continuous verification of all users, devices, and network traffic (Syed et al., 2022). When combined with post-quantum cryptographic algorithms, zero-trust principles provide a robust foundation for securing critical infrastructure communications against both current and future threats.

The urgency of this transformation cannot be overstated. Recent cyberattacks on critical infrastructure, including the Colonial Pipeline incident and various attacks on power grids, demonstrate the catastrophic potential of successful

[*] Corresponding author: Winifred Chukwuebuka Ayogu

breaches (Yadav and Paul, 2021). As quantum computing capabilities advance, the window for implementing quantum-resistant protections continues to narrow, necessitating immediate action to safeguard critical systems.

This paper presents a comprehensive framework for implementing a post-quantum zero-trust backbone that addresses five critical areas: post-quantum cryptography rollout, zero-trust network segmentation, SCADA protocol encryption, identity governance, and incident response capabilities. Our approach recognizes the unique constraints of operational technology environments, including legacy system compatibility, real-time performance requirements, and high availability demands Adeshina. (2021).

2. Literature Review and Theoretical Foundation

2.1. Zero-Trust Architecture Evolution

Zero-trust architecture represents a fundamental departure from traditional castle-and-moat security models. Syed et al. (2022) provide a comprehensive analysis of ZTA principles, emphasizing the core tenets of "never trust, always verify" and "assume breach." This paradigm is particularly relevant for critical infrastructure, where the convergence of IT and OT networks creates complex attack surfaces that traditional perimeter defenses cannot adequately protect.

The application of zero-trust principles to industrial environments presents unique challenges. Abulafia et al. (2023) demonstrate how ZTA can be adapted for Industrial Internet of Things (IIoT) systems, highlighting the need for specialized approaches that accommodate the unique characteristics of operational technology. Similarly, Hossain et al. (2023) explore zero-trust implementations in healthcare IoT environments, providing insights into sector-specific security requirements.

2.2. Post-Quantum Cryptography Landscape

The quantum threat to cryptographic systems is well-documented and increasingly urgent. Bălaș et al. (2024) provide a comprehensive review of post-quantum cryptography options for critical systems, emphasizing the need for careful algorithm selection based on performance and security requirements. The National Institute of Standards and Technology (NIST) has standardized several quantum-resistant algorithms, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures.

Kiktenko et al. (2024) analyze the quantum future of cybersecurity, highlighting the timeline for quantum computer capabilities and the corresponding need for cryptographic migration. Their analysis suggests that organizations must begin post-quantum transitions immediately to ensure protection against both current and future quantum threats. Naeem et al. (2024) extend this analysis to blockchain technologies, demonstrating how post-quantum algorithms can be integrated into distributed systems.

2.3. Critical Infrastructure Security Challenges

Critical infrastructure security faces unique challenges that distinguish it from traditional IT security. Das et al. (2021) analyze cybersecurity requirements for energy systems, emphasizing the critical importance of SCADA communication security and encryption. Their work highlights the tension between security requirements and operational constraints such as latency sensitivity and legacy system compatibility.

Yadav and Paul (2021) provide a comprehensive review of SCADA system architecture and security challenges, identifying key vulnerabilities in industrial control systems. Their analysis reveals that many critical infrastructure systems rely on legacy protocols that lack built-in security features, necessitating external security overlays to protect communications.

3. Post-Quantum Cryptography Rollout Strategy

3.1. Cryptographic Inventory and Risk Assessment

The first phase of post-quantum migration requires a comprehensive inventory of existing cryptographic implementations across critical infrastructure systems. This process involves identifying all cryptographic components, assessing their quantum vulnerability, and prioritizing migration based on risk and criticality.

Table 1 Cryptographic Inventory Classification Framework

System Type	Cryptographic Usage	Quantum Vulnerability	Migration Priority	Timeline
SCADA HMI	RSA-2048, AES-256	High (RSA) / Low (AES)	Critical	6-12 months
Substation Controllers	Legacy DES, 3DES	Very High	Critical	3-6 months
Communication Gateways	ECC P-256, SHA-256	High (ECC) / Low (SHA)	High	12-18 months
Historian Systems	RSA-2048, AES-128	High (RSA) / Low (AES)	Medium	18-24 months
Engineering Workstations	Mixed Algorithms	Variable	Medium	12-24 months

The migration strategy must account for the diverse cryptographic landscape found in critical infrastructure environments. Blanco-Novoa et al. (2021) emphasize the importance of systematic assessment in Industry 4.0 environments, noting that many systems utilize outdated cryptographic algorithms that provide insufficient protection against conventional attacks, let alone quantum threats Adeshina and Ndukwe, (2024).

3.2. NIST-Endorsed Algorithm Selection

The selection of appropriate post-quantum algorithms requires careful consideration of performance characteristics, security levels, and implementation constraints. The NIST post-quantum cryptography standardization process has identified several promising algorithm families:

- **Lattice-based algorithms:** CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures) offer strong security guarantees with reasonable performance characteristics suitable for most critical infrastructure applications.
- **Hash-based signatures:** SPHINCS+ provides conservative security assumptions but with larger signature sizes that may be problematic for bandwidth-constrained industrial networks.
- **Code-based algorithms:** Classic McElwee offers strong security but requires large key sizes that may be impractical for resource-constrained devices.

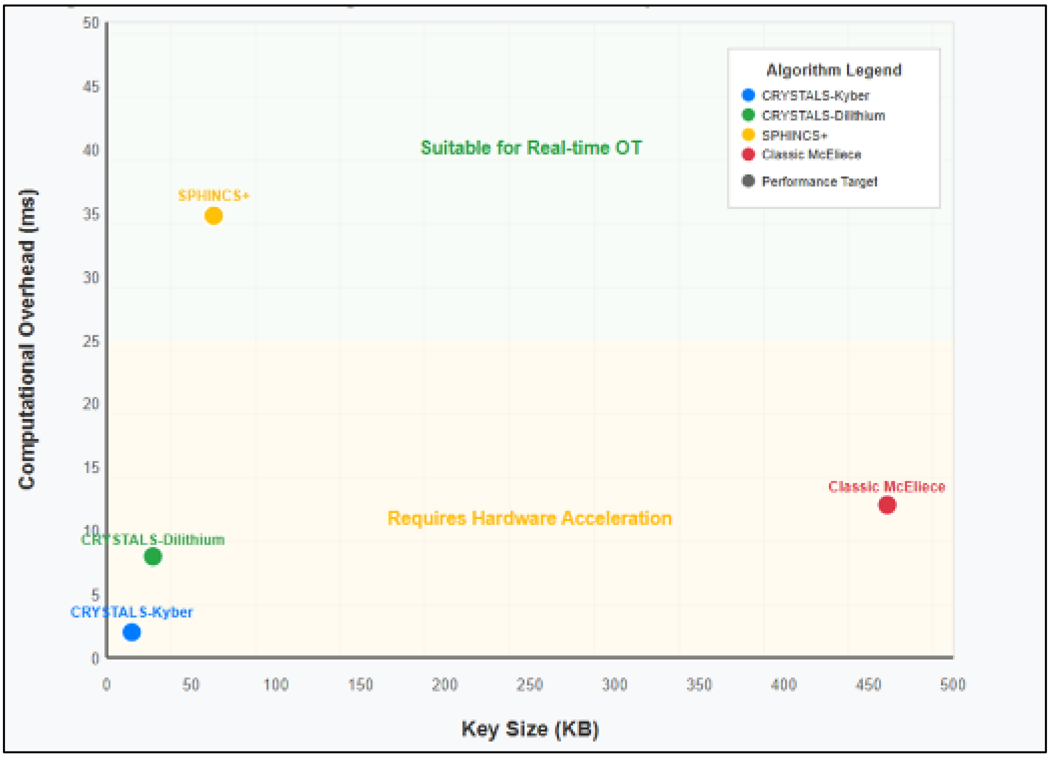

Figure 1 Post-Quantum Algorithm Performance Comparison for Critical Infrastructure

3.3. Hybrid Cryptographic Approach

During the transition period, a hybrid approach combining classical and post-quantum algorithms provides defense-in-depth against both conventional and quantum threats. This strategy ensures that communications remain secure even if either the classical or post-quantum component is compromised.

Panarello et al. (2024) explore hybrid cryptographic implementations for networked environments, demonstrating how organizations can maintain backward compatibility while gradually introducing quantum-resistant protections. The hybrid approach is particularly valuable for critical infrastructure, where system availability requirements often preclude rapid wholesale replacements.

4. Zero-Trust Network Segmentation

4.1. Micro-Segmentation Architecture

Zero-trust segmentation fundamentally reimagines network architecture by eliminating implicit trust relationships and implementing granular access controls. Chen et al. (2023) demonstrate advanced micro-segmentation techniques for software-defined industrial networks, showing how east-west traffic can be controlled through continuous verification mechanisms.

The implementation of micro-segmentation in critical infrastructure environments requires careful consideration of operational requirements. Li et al. (2024) present a VLAN-VxLAN mapping approach that enables fine-grained segmentation while maintaining the performance characteristics required for industrial applications.

Table 2 Network Segmentation Zones for Critical Infrastructure

Zone	Description	Security Level	Access Controls	Monitoring
Safety Systems	Emergency shutdown, safety interlocks	Maximum	Hardware-enforced isolation	Real-time SIEM
Process Control	Primary production control systems	High	Multi-factor authentication	Continuous monitoring
Supervisory	SCADA HMI, historian systems	High	Role-based access control	Behavioral analytics
Engineering	Configuration, maintenance systems	Medium	Time-limited access	Session recording
Business	Enterprise applications	Medium	Standard authentication	Log aggregation
DMZ	External communications	Low	Proxy-based access	Deep packet inspection

4.2. Continuous Verification Mechanisms

Zero-trust architecture requires continuous verification of all network communications, moving beyond traditional authentication to ongoing behavioral analysis and risk assessment. Fotiou and Polyzos (2022) explore identity-centric networking approaches that enable continuous verification while maintaining performance requirements for critical infrastructure applications.

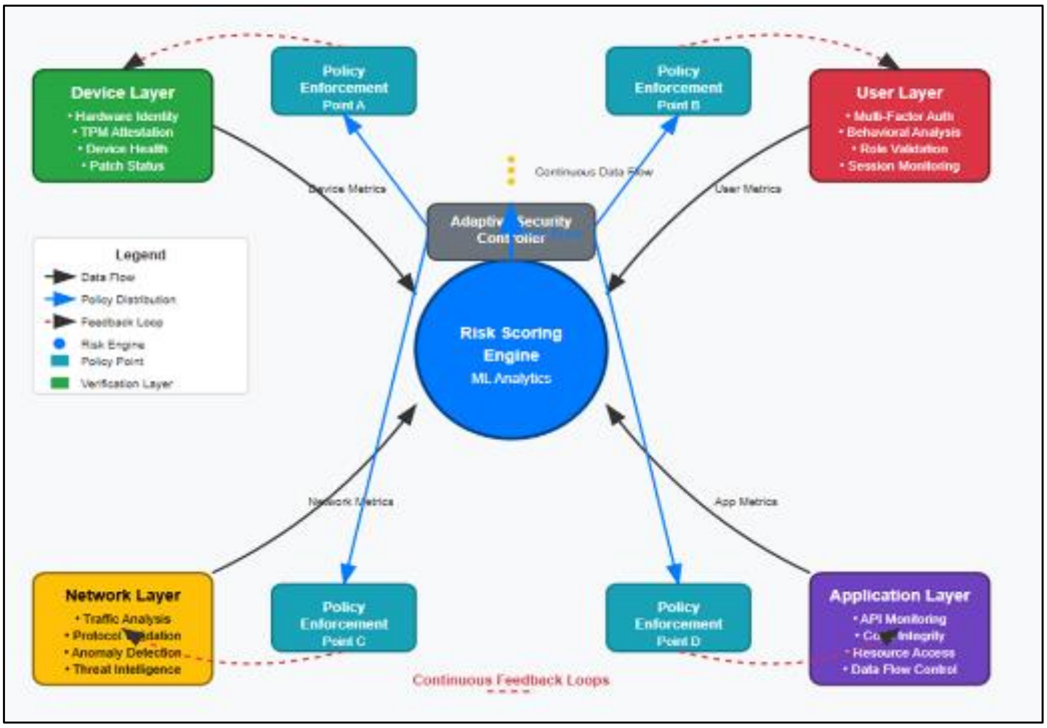

Figure 2 Continuous Verification Framework Architecture

The continuous verification process encompasses multiple dimensions

- **Device identity verification:** Hardware-bound credentials ensure that only authorized devices can access network resources.
- **User behavior analysis:** Machine learning algorithms detect anomalous behavior patterns that may indicate compromised accounts or insider threats.

- **Network traffic analysis:** Deep packet inspection and flow analysis identify suspicious communication patterns.
- **Application-level monitoring:** API calls and application behaviors are continuously monitored for signs of compromise.

4.3. East-West Traffic Control

Traditional security models focus primarily on north-south traffic crossing network perimeters, but the majority of data movement in modern networks occurs laterally (east-west) between systems. Chen et al. (2023) demonstrate how software-defined networking can be leveraged to implement granular controls on east-west traffic in industrial environments.

The implementation of east-west traffic controls requires careful balance between security and operational requirements. Critical infrastructure systems often require low-latency communications for real-time control functions, necessitating high-performance security enforcement mechanisms that do not introduce unacceptable delays.

5. SCADA Protocol Encryption and Security

5.1. Legacy Protocol Vulnerabilities

SCADA systems in critical infrastructure environments frequently rely on legacy protocols that were designed without security considerations. Abd-Elaal et al. (2022) analyze vulnerabilities in Modbus/TCP communications and demonstrate enhanced security protocols that protect against man-in-the-middle attacks. Their work highlights the fundamental security limitations of protocols designed for isolated networks that are now connected to broader IT infrastructure.

Galanopoulos et al. (2021) address security challenges in DNP3 and Modbus communications through authenticated encryption gateways. Their approach demonstrates how legacy protocols can be secured without requiring wholesale replacement of existing infrastructure, a critical consideration for organizations with significant investments in legacy systems.

Table 3 SCADA Protocol Security Assessment

Protocol	Usage Frequency	Security Features	Vulnerability Rating	Encryption Support
DNP3	45%	Basic authentication	Medium	Limited (Secure Authentication)
Modbus/TCP	35%	None	High	None (requires tunneling)
IEC 61850	15%	TLS support	Low-Medium	Yes (TLS/SSL)
EtherNet/IP	3%	Basic	Medium-High	Limited
Proprietary	2%	Variable	Variable	Variable

5.2. Authenticated Encryption Tunnels

The implementation of secure tunnels for SCADA communications provides a practical approach to protecting legacy protocols without requiring extensive system modifications. Dragomir et al. (2022) explore TLS/DTLS tunneling approaches for industrial communications, demonstrating how modern encryption can be layered over existing protocols to provide authentication, confidentiality, and integrity protection.

Lopes et al. (2024) present in-line rate encrypted links specifically designed for resource-aware SCADA communications. Their approach addresses the unique performance requirements of industrial control systems while providing strong cryptographic protection that can be upgraded to post-quantum algorithms as they become available.

The key considerations for implementing authenticated encryption tunnels include:

- **Latency constraints:** Industrial control systems often require deterministic response times, necessitating encryption implementations that minimize processing delays.

- **Bandwidth limitations:** Many industrial networks operate over constrained bandwidth connections, requiring efficient encryption approaches that minimize overhead.
- **Legacy system compatibility:** Encryption solutions must operate transparently with existing SCADA software and hardware to avoid costly system replacements.
- **Key management:** Automated key distribution and rotation mechanisms are essential for maintaining security across large-scale industrial deployments.

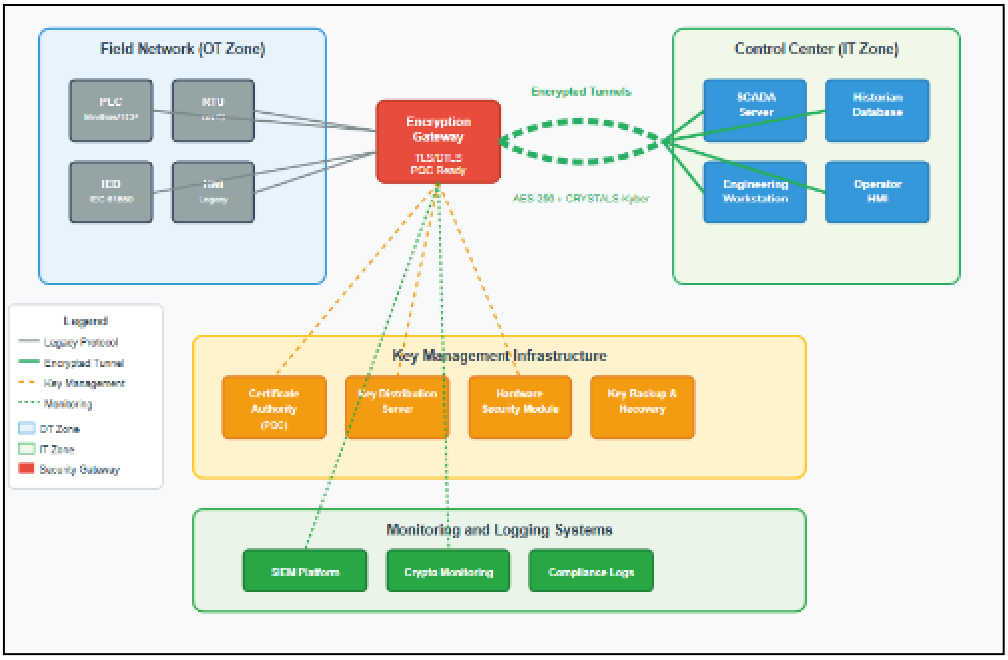

Figure 3 SCADA Protocol Encryption Architecture

5.3. Performance Optimization for Real-Time Systems

The implementation of encryption in real-time industrial control systems requires careful optimization to maintain required performance characteristics. Hardware acceleration of cryptographic operations can significantly reduce processing overhead, while carefully selected algorithms can minimize computational requirements without compromising security.

The migration to post-quantum cryptographic algorithms introduces additional performance considerations. While algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium offer reasonable performance for most applications, their computational requirements exceed those of classical algorithms. Hardware acceleration and algorithm-specific optimizations will be crucial for maintaining real-time performance in post-quantum implementations.

6. Identity Governance and Access Management

6.1. Hardware-Bound Credentials

The foundation of robust identity governance in critical infrastructure environments rests on hardware-bound credentials that provide strong device authentication. Saylam et al. (2023) explore FIDO2/Webathons implementations for industrial IoT environments, demonstrating how modern authentication standards can be adapted for operational technology applications.

Nadir et al. (2022) present TPM-anchored device identity solutions specifically designed for OT networks. Their approach leverages Trusted Platform Module (TPM) capabilities to create unforgeable device identities that form the basis for zero-trust verification. This hardware-bound approach is particularly important in critical infrastructure environments where device compromise could have catastrophic consequences.

The implementation of hardware-bound credentials addresses several critical security challenges:

- **Device spoofing prevention:** Cryptographic device identities anchored in hardware cannot be easily replicated or transferred to unauthorized devices.
- **Supply chain security:** Hardware-bound credentials enable verification of device authenticity and integrity throughout the supply chain.
- **Credential theft resistance:** Private keys stored in secure hardware elements cannot be extracted through software-based attacks.
- **Scalable device management:** Automated enrollment and management processes reduce the operational burden of maintaining device credentials across large industrial deployments.

6.2. Multi-Factor Authentication Implementation

The implementation of multi-factor authentication (MFA) in critical infrastructure environments requires careful consideration of operational constraints and emergency access requirements. Zarca et al. (2022) explore continuous authentication mechanisms for 5G-enabled critical infrastructures, demonstrating how adaptive authentication can balance security requirements with operational needs.

Table 4 MFA Implementation Framework for Critical Infrastructure

User Role	Primary Factor	Secondary Factor	Emergency Access	Session Duration
Control Room Operator	Hardware token	Biometric	Supervisor override	8 hours
Field Technician	Mobile app	SMS/Voice	Emergency PIN	4 hours
Maintenance Engineer	Smart card	Push notification	Time-limited token	2 hours
Emergency Responder	Biometric	Location verification	Incident commander	1 hour
System Administrator	Hardware token	Biometric + approval	Security team override	30 minutes

The MFA implementation must account for the unique operational requirements of critical infrastructure

- **Emergency access procedures:** During emergencies, standard authentication procedures may be impractical, requiring carefully designed emergency access mechanisms that maintain security while enabling rapid response.
- **Shared workstation considerations:** Many industrial environments utilize shared workstations, requiring session management approaches that protect against unauthorized access while supporting operational workflows.
- **Offline operation capabilities:** Critical infrastructure systems must continue operating during network outages, necessitating authentication mechanisms that can function without continuous connectivity to central systems.

6.3. Automated Entitlement Reviews

Automated entitlement review processes are essential for maintaining appropriate access controls across large critical infrastructure deployments. These systems continuously monitor user access patterns, identify excessive privileges, and enforce least-privilege principles through automated policy enforcement.

The implementation of automated entitlement reviews involves several key components

- **Role-based access control (RBAC):** Standardized roles and permissions simplify access management and enable automated review processes.
- **Behavioral analytics:** Machine learning algorithms analyze user behavior patterns to identify anomalous access attempts or privilege escalation indicators.
- **Temporal access controls:** Time-limited access grants ensure that elevated privileges are automatically revoked when no longer needed.
- **Approval workflows:** Automated approval processes route access requests to appropriate authorities while maintaining audit trails for compliance purposes.

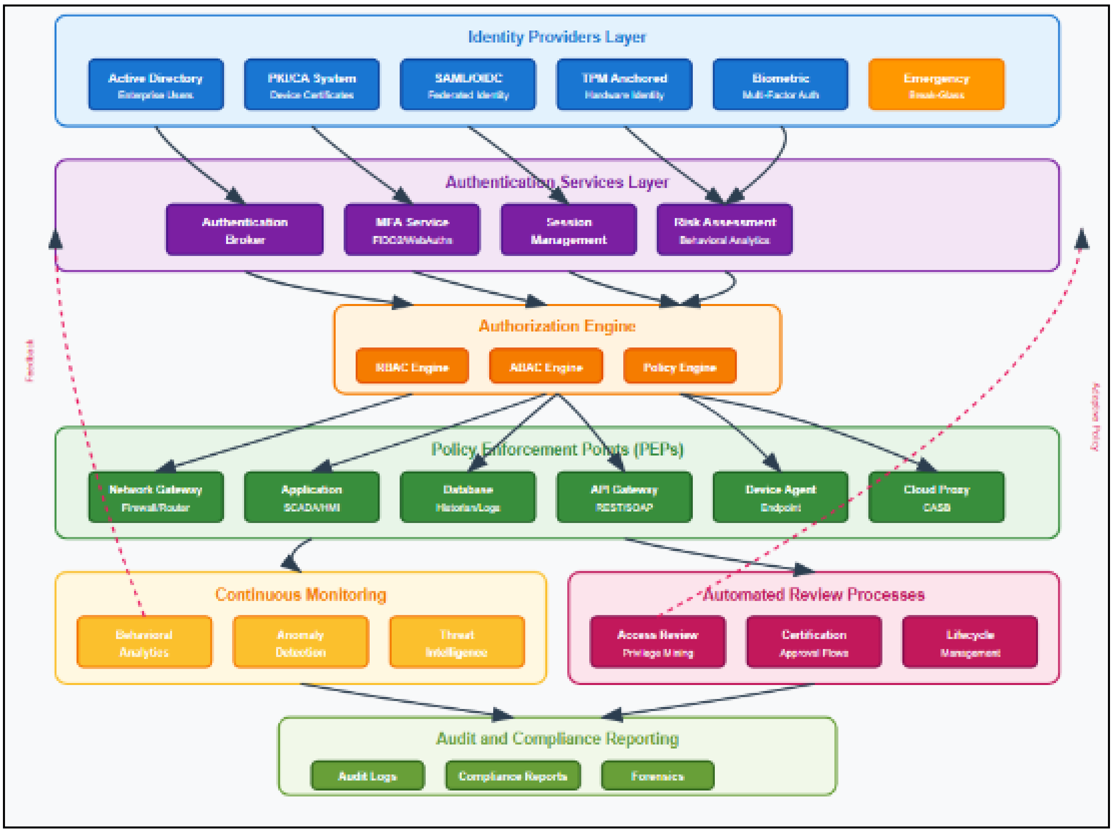

Figure 4 Identity Governance Architecture

7. Incident Response and Automated Containment

7.1. Playbook Development and Tabletop Exercises

Effective incident response in critical infrastructure environments requires comprehensive playbooks that address the unique challenges of operational technology systems. Shafiq et al. (2023) present detailed frameworks for incident response in industrial control systems, emphasizing the importance of regular tabletop exercises and automated containment mechanisms.

The development of incident response playbooks must account for the critical nature of infrastructure systems and the potential for cascading failures. Unlike traditional IT environments where systems can be taken offline for investigation, critical infrastructure often requires continued operation even during active incidents.

Table 5 Incident Response Playbook Framework

Incident Type	**Detection Method**	**Initial Response**	**Containment Strategy**	**Recovery Timeline**
Malware Infection	Behavioral analytics	Isolate affected systems	Network segmentation	2-6 hours
Credential Compromise	Authentication anomalies	Disable accounts	Forced re-authentication	1-2 hours
Protocol Manipulation	Traffic analysis	Communication blocking	Protocol filtering	30 minutes - 2 hours
Physical Intrusion	Access control alerts	Security response	Area isolation	1-4 hours
Supply Chain Attack	Integrity monitoring	System quarantine	Vendor verification	6-24 hours

Tabletop exercises serve a critical role in preparing incident response teams for the complex scenarios they may encounter. These exercises should simulate realistic attack scenarios, including simultaneous attacks on multiple systems and coordination challenges between IT and OT teams.

7.2. Automated Containment Mechanisms

Automated containment mechanisms are essential for responding to cyber incidents at the speed and scale required to protect critical infrastructure. These systems must balance the need for rapid response with the operational requirements of continuous service delivery.

The implementation of automated containment involves several key capabilities

- **Network-based containment:** Automated systems can rapidly isolate compromised network segments while maintaining connectivity to critical control systems.
- **Application-level containment:** Suspicious application behaviors can trigger automated responses such as process termination or privilege revocation.
- **Device-based containment:** Compromised devices can be automatically isolated from network resources while maintaining local control capabilities.
- **Data-based containment:** Automated systems can prevent data exfiltration by monitoring and blocking suspicious data transfers.

7.3. Alignment with CISA Guidance

The Cybersecurity and Infrastructure Security Agency (CISA) provide comprehensive guidance for critical infrastructure cybersecurity, including incident response procedures and security frameworks. Incident response procedures must align with CISA guidelines while accounting for sector-specific requirements and operational constraints.

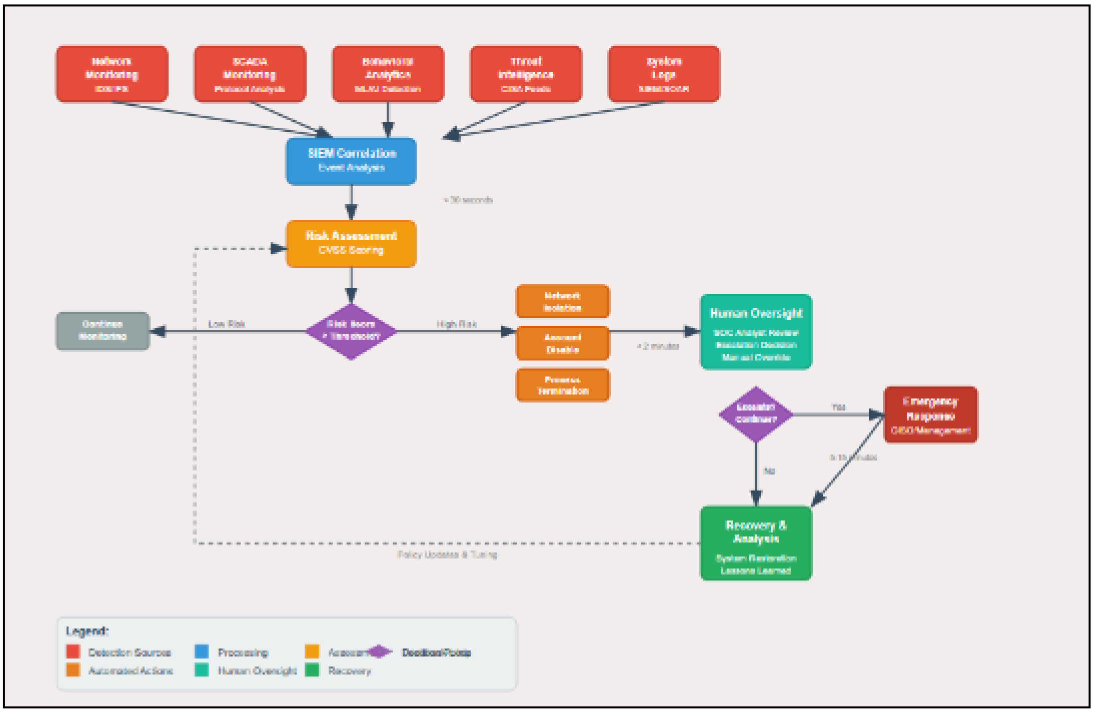

Figure 5 Automated Incident Response Workflow

Key CISA guidance elements include

- **Continuous monitoring:** Real-time monitoring of network traffic and system behaviors to enable rapid detection of security incidents.
- **Information sharing:** Coordination with government agencies and industry partners to share threat intelligence and incident information.

- **Recovery planning:** Comprehensive plans for restoring operations following security incidents, including backup systems and alternative operational procedures.
- **Lessons learned:** Post-incident analysis to identify improvements in security controls and response procedures.

8. Implementation Framework and Best Practices

8.1. Phased Deployment Strategy

The implementation of a post-quantum zero-trust backbone requires a carefully orchestrated phased approach that minimizes operational disruption while progressively enhancing security capabilities. The deployment strategy must account for the complex interdependencies present in critical infrastructure systems and the need for extensive testing and validation at each phase.

Phase 1 focuses on establishing foundational zero-trust capabilities, including identity governance systems and basic network segmentation. This phase emphasizes rapid implementation of security improvements that provide immediate value while establishing the infrastructure necessary for more advanced capabilities.

Phase 2 introduces post-quantum cryptographic capabilities through hybrid implementations that maintain backward compatibility with existing systems. This approach allows organizations to begin quantum-resistant protection while continuing to operate legacy systems during the transition period.

Phase 3 completes the migration to fully post-quantum cryptographic implementations and advanced zero-trust capabilities, including comprehensive micro-segmentation and automated response systems.

8.2. Risk Management and Compliance

The implementation of post-quantum zero-trust architecture must integrate with existing risk management frameworks and regulatory compliance requirements. Critical infrastructure sectors are subject to various regulatory requirements, including NERC CIP for electric utilities, TSA directives for transportation systems, and sector-specific cybersecurity frameworks.

Risk management approaches must account for both cybersecurity risks and operational risks associated with security system implementations. The introduction of new security controls should not compromise system availability or introduce new failure modes that could impact critical operations.

8.3. Cost-Benefit Analysis

The implementation of comprehensive post-quantum zero-trust security represents a significant investment that must be justified through quantitative risk reduction and qualitative operational benefits. Organizations must consider both direct implementation costs and indirect costs associated with operational changes and staff training.

Table 6 Implementation Cost-Benefit Analysis Framework

Cost Category	Description	Typical Range	Benefit Category	Quantification Method
Hardware	Cryptographic accelerators, network equipment	$500K - $5M	Risk reduction	Avoided incident costs
Software	Security platforms, monitoring tools	$200K - $2M	Compliance	Reduced audit costs
Personnel	Implementation, training, operations	$300K - $3M annually	Efficiency	Automated processes
Consulting	Design, integration, validation	$100K - $1M	Reputation	Brand protection value
Ongoing	Maintenance, updates, monitoring	$150K - $1.5M annually	Innovation	Competitive advantage

9. Challenges and Future Directions

9.1. Technical Challenges

The implementation of post-quantum zero-trust architecture in critical infrastructure environments faces several significant technical challenges that require ongoing research and development efforts.

Algorithm maturity and standardization remain primary concerns. While NIST has standardized several post-quantum algorithms, the cryptographic community continues to analyze their security properties and discover potential vulnerabilities. Organizations implementing these algorithms must maintain flexibility to adapt to evolving standards and recommendations.

Performance optimization for real-time systems represents another significant challenge. Post-quantum algorithms generally require more computational resources than their classical counterparts, potentially impacting the deterministic timing requirements of industrial control systems. Continued research into algorithm optimization and hardware acceleration will be essential for widespread adoption.

Interoperability between legacy and modern systems poses ongoing challenges. Critical infrastructure environments typically contain systems with lifecycles measured in decades, requiring security solutions that can bridge significant technological gaps without compromising operational capabilities.

9.2. Operational Challenges

The human factors associated with implementing advanced security systems in critical infrastructure environments cannot be underestimated. Operational staff must be trained on new procedures and technologies while maintaining their ability to respond effectively to emergencies and system failures.

Change management processes must balance the urgency of security improvements with the need for thorough testing and validation. The consequences of security system failures in critical infrastructure environments can be catastrophic, requiring extensive validation processes that may slow implementation timelines.

Coordination between IT and OT teams remains a persistent challenge. The convergence of information technology and operational technology requires new organizational structures and communication processes that may not align with traditional departmental boundaries.

9.3. Future Research Directions

Several areas require continued research and development to support the evolution of post-quantum zero-trust security for critical infrastructure

- **Quantum key distribution:** The development of practical quantum communication systems may provide alternatives to cryptographic approaches for securing critical communications.
- **Homomorphic encryption:** Advanced encryption techniques that enable computation on encrypted data may provide new approaches for securing industrial control algorithms.
- **Artificial intelligence integration:** Machine learning and artificial intelligence capabilities may enhance threat detection and automated response capabilities while introducing new security considerations.
- **Edge computing security:** The proliferation of edge computing in industrial environments requires new security approaches that can protect distributed computing resources.

10. Conclusion

The implementation of post-quantum zero-trust architecture represents a critical evolution in critical infrastructure cybersecurity that addresses both current threats and emerging quantum-enabled risks. This comprehensive approach integrates quantum-resistant cryptographic algorithms with identity-first network architecture to provide robust protection against sophisticated cyberattacks while maintaining the operational characteristics required for critical infrastructure systems.

The framework presented in this paper demonstrates how organizations can systematically approach the complex challenge of modernizing critical infrastructure security. Through careful attention to the unique requirements of operational technology environments, including legacy system compatibility, real-time performance constraints, and high availability demands, this approach provides a practical path forward for enhancing cybersecurity without compromising operational capabilities.

The urgency of this transformation cannot be overstated. As quantum computing capabilities continue to advance and cyber threats become increasingly sophisticated, organizations that delay implementation of quantum-resistant security measures face escalating risks of catastrophic cyberattacks. The framework presented here provides a comprehensive roadmap for organizations seeking to protect their critical infrastructure investments while positioning themselves for future security challenges.

Successful implementation requires sustained commitment from organizational leadership, careful coordination between IT and OT teams, and ongoing investment in both technology and human capabilities. Organizations that embrace this comprehensive approach to critical infrastructure security will be better positioned to maintain operational continuity and protect public safety in an increasingly complex threat environment.

The post-quantum zero-trust backbone represents more than a technological upgrade; it embodies a fundamental shift toward resilient, adaptive security that can evolve with emerging threats while supporting the critical mission of infrastructure operators. As organizations begin implementing these capabilities, continued collaboration between industry, government, and research communities will be essential for addressing implementation challenges and advancing the state of the art in critical infrastructure cybersecurity.

References

[1] Abd-Elaal, M. A., Al-Yahya, S., and Alqumaiz, M. (2022). Enhanced Modbus/TCP security protocol to protect SCADA systems against MITM attacks. Sensors, 22(7), 2647. https://doi.org/10.3390/s22072647

[2] Abualhaija, S., Bouzidi, T., Omar, M., and Alawadi, S. (2023). A Zero Trust Architecture approach for IIoT systems. Electronics, 12(3), 566. https://doi.org/10.3390/electronics12030566

[3] Adeshina, Y. T. (2021). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. International Journal of Engineering Technology Research and Management, 5(12), 204-218.

[4] Adeshina, Y. T., and Ndukwe, M. O. (2024). Establishing a blockchain-enabled multi-industry supply-chain analytics exchange for real-time resilience and financial insights. IRE Journals, 7(12), 599-610. https://doi.org/10.5281/zenodo.16053081

[5] Adeshina, Y. T., Owolabi, B. O., and Olasupo, S. O. (2023). A U.S. national framework for quantum-enhanced federated analytics in population health early-warning systems. International Journal of Engineering Technology Research and Management, 7(2), 76-95. https://doi.org/10.5281/zenodo.15589483

[6] Ajimatanrareje, G. A. (2024). Advancing E-Voting Security: Biometrics-Enhanced Blockchain for Privacy and VerifiAbility (BEBPV). *American Journal of Innovation in Science and Engineering*, *3*(3), 88–93. https://doi.org/10.54536/ajise.v3i3.3876

[7] Bamigbade, O., Adeshina, Y. T., and Kasali, K. (2024). Ethical and explainable AI in data science for transparent decision-making across critical business operations. International Journal of Engineering Technology Research and Management, 8(11), 734-753. https://doi.org/10.5281/zenodo.15671481

[8] Alcaraz, C., and Lopez, J. (2021). A security analysis for SCADA and industrial control systems communications. IEEE Systems Journal, 15(3), 3641–3652. https://doi.org/10.1109/JSYST.2020.3047640

[9] Bălaş, V. E., Balas, M. M., and Perescu-Popescu, L. (2024). Exploring post-quantum cryptography: Review and directions for critical systems. Technologies, 12(12), 241. https://doi.org/10.3390/technologies12120241

[10] Blanco-Novoa, Ó., Fraga-Lamas, P., and Fernández-Caramés, T. M. (2021). Post-quantum cryptography in Industry 4.0: Current state and future directions. Computer Standards and Interfaces, 76, 103521.

[11] Chen, Z., Zhang, Z., and Li, K. (2023). Micro-segmentation and east–west traffic control in software-defined industrial networks. IEEE Transactions on Industrial Informatics, 19(4), 4982–4994. https://doi.org/10.1109/TII.2022.3221234

[12] Das, N., Haque, A., Zaman, H., Morsalin, S., and Islam, S. (2021). Cybersecurity for energy systems: SCADA communication security and encryption. International Journal of Critical Infrastructure Protection, 34, 100438.

[13] Dragomir, V. A., Butnaru, A. M., and Popescu, V. (2022). Secure industrial communications: TLS/DTLS tunnels for SCADA protocols. Journal of Network and Computer Applications, 206, 103457.

[14] Fotiou, N., and Polyzos, G. C. (2022). Identity-centric networking and zero-trust for critical infrastructures. Computer Networks, 215, 109147. https://doi.org/10.1016/j.comnet.2022.109147

[15] He, Y., Huang, D., Chen, L., Ni, Y., and Ma, X. (2022). A survey on Zero-Trust Architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022, 6476274. https://doi.org/10.1155/2022/6476274

[16] Hossain, M. S., Muhammad, G., and Al-Hamadi, H. (2023). Zero-trust security for healthcare IoT: Architectures, challenges, and future directions. IEEE Access, 11, 118560–118579.

[17] Humayed, A., Lin, J., Li, F., and Luo, B. (2017/2021 reprint). Cyber-physical systems security—A survey (with OT segmentation implications). IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

[18] Kiktenko, E. O., Trushechkin, A., and Fedorov, A. K. (2024). Post-quantum cryptography and the quantum future of cybersecurity. Physical Review Applied, 21(4), 040501. https://doi.org/10.1103/PhysRevApplied.21.040501

[19] Li, D., Yang, Z., Yu, S., Duan, M., and Yang, S. (2024). A micro-segmentation method based on VLAN–VxLAN mapping technology. Future Internet, 16(9), 320. https://doi.org/10.3390/fi16090320

[20] Lopes, A., Gil-Herrera, J., Valds-Gonzalez, L., and Sargolzaei, A. (2024). In-line rate encrypted links for resource-aware SCADA communications. Scientific Reports, 14, 18825. https://doi.org/10.1038/s41598-024-71861-x

[21] Nadir, Q., Ahmad, I., and Khan, S. (2022). TPM-anchored device identity for zero-trust in OT networks. IEEE Transactions on Industrial Informatics, 18(12), 8876–8887. https://doi.org/10.1109/TII.2022.3179914

[22] Naeem, H., Ahmad, R. W., and Gani, A. (2024). A survey and comparison of post-quantum and quantum blockchains. IEEE Communications Surveys and Tutorials, 26(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761

[23] Panarello, A., Tapas, N., and Sgandurra, D. (2024). Navigating quantum security risks in networked environments. Computers and Security, 140, 103818.

[24] Rasyid, A. A., Alzahrani, B., Hussain, F. K., and Hussain, O. K. (2024). Dissecting zero-trust implementation in the IoT: A systematic literature review. Cybersecurity, 7, 38. https://doi.org/10.1186/s42400-024-00212-0

[25] Saylam, A., Tekinay, S., and Aydin, M. A. (2023). Hardware-bound credentials and FIDO2/WebAuthn for industrial IoT. IEEE Internet of Things Journal, 10(15), 13312–13326.

[26] Shafiq, M., Sajjad, M., and Koo, I. (2023). Incident response in industrial control systems: Playbooks, tabletop exercises, and automated containment. IEEE Access, 11, 103210–103234.

[27] Syed, N. F., Namanya, A., Stirling, S., and Buchanan, W. J. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

[28] Yadav, G., and Paul, K. (2021). Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection, 34, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

[29] Yusuff, T. A. (2025). A neuro-symbolic artificial intelligence and zero-knowledge blockchain framework for a patient-owned digital-twin marketplace in U.S. value-based care. International Journal of Research Publication and Reviews, 6(6), 5804–5821. https://doi.org/10.55248/gengpi.6.0625.21105

[30] Yusuff, T. A. (2023a). Interoperable IT architectures enabling business analytics for predictive modeling in decentralized healthcare ecosystem. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 346–355. https://doi.org/10.14569/IJACSA.2023.0141144

[31] Yusuff, T. A. (2023b). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 359–370. https://doi.org/10.14569/IJACSA.2023.0141146

[32] Yusuff, T. A. (2023c). Multi-tier business analytics platforms for population health surveillance using federated healthcare IT infrastructures. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 338–345. https://doi.org/10.14569/IJACSA.2023.0141143

[33] Yusuff, T. A. (2023d). Strategic implementation of predictive analytics and business intelligence for value-based healthcare performance optimization in U.S. health sector. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 327–337. https://doi.org/10.14569/IJACSA.2023.0141142

[34] Zarca, A. M., Bernal, S. L., Oteyza, A., Fernández, J. M., and Skarmeta, A. F. (2022). Zero-trust for 5G-enabled critical infrastructures: Identity, access control, and continuous authentication. IEEE Access, 10, 12345–12364.

[35] Zografopoulos, I., Djouadi, S. M., and Zonouz, S. (2021). Securing legacy DNP3 and Modbus communications via authenticated encryption gateways. International Journal of Critical Infrastructure Protection, 34, 100436.