International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Infrastructure Hardening for Ot Networks: From Traditional Segmentation to Future-Proof Trusted Architectures

Mohammed Shoukatuddin[1], Mohammed Aqheel[2], Mohammed Afzal[3]
[1]Senior Specialist – OT Network & Cybersecurity, Ma'aden Aluminum Company, Saudi Arabia
[2]Senior IT Specialist, Ma'aden Aluminum Company, Saudi Arabia
[3]Specialist I – Systems Administration, Saudi Arabian Mining Company (Ma'aden), Saudi Arabia

ABSTRACT - Operational Technology (OT) networks operate critical industrial processes and must deliver safety and availability over long asset lifecycles. However, IT–OT convergence, Industrial IoT (IIoT) expansion, and remote operations have increased exposure to malware, ransomware, and targeted attacks. This paper proposes a practical hardening approach that combines (i) structured network segregation aligned with the Purdue reference hierarchy and IEC 62443 zones-and-conduits, and (ii) hardware-rooted security using Trusted Platform Modules (TPMs) and Trusted Execution Environments (TEEs) to anchor device identity and integrity. We compare legacy air-gapped designs, current segmented architectures, and a future hybrid model that incorporates Zero Trust principles, micro-segmentation, continuous attestation, and centralized monitoring. Our contribution is an integrated architecture and implementation guidance for brownfield OT environments, including controlled conduits, secure remote access, device attestation, cryptographic agility, and measurable detection-and-response. We further discuss Industry 4.0 and Industry 5.0 considerations—mass connectivity, cyber-physical safety, human-centric operations, sustainability, and resilience—and show how they influence security requirements and design choices. The analysis indicates that combining segmentation with hardware-backed trust reduces lateral movement, limits blast radius, and increases assurance that critical endpoints remain in a known-good state, enabling safer operations in increasingly connected industrial ecosystems.

***Keywords*— OT cybersecurity; network segmentation; Purdue model; IEC 62443; zones and conduits; TPM; secure enclaves; Zero Trust; Industry 4.0; Industry 5.0; infrastructure hardening.**

I. INTRODUCTION

Industrial control and automation networks were historically engineered for deterministic control and maximum availability, often under the assumption of physical isolation. In many plants, the control domain was separated from the enterprise domain by design, and security controls were minimal because the environment was considered trusted. As organizations adopted advanced analytics, centralized operations, and remote vendor support, IT and OT systems began to converge. IIoT sensors, edge gateways, and cloud services increased connectivity, but also expanded the attack surface. Consequently, threats traditionally associated with IT (phishing-driven ransomware, credential theft, supply-chain compromise) now routinely impact OT, with consequences that can include safety hazards, environmental incidents, and extended downtime.

Two levers consistently deliver the highest security value with minimal disruption to industrial processes: (1) segmentation to contain an intrusion and prevent uncontrolled lateral movement; and (2) endpoint integrity controls to reduce the chance that a compromised workstation or server can pivot into controllers and safety systems. Segmentation reduces risk by limiting reachability; hardware-rooted integrity reduces risk by enforcing a verifiable chain of trust at devices.

This paper targets practitioners and researchers. The goal is to translate established models (Purdue, IEC 62443) and modern hardware security (TPM/TEE) into reference architectures that can be adopted incrementally in brownfield environments. We emphasize operational realism: control systems must remain available, latency must be predictable, and safety must never be compromised by security controls.

II. BACKGROUND AND RELATED WORK

The Purdue Enterprise Reference Architecture (PERA) is commonly used to describe OT systems as hierarchical levels, from physical process (Level 0) through control (Levels 1–2), operations (Level 3), and business/enterprise services (Levels 4–5). The Purdue model helps planners decide where to place functions and where to enforce separation, but it is not a security standard by itself. IEC 62443 complements Purdue by defining security zones (groups of assets with similar security requirements) and conduits (managed communication paths with explicit controls). Together, they provide a practical structure for segmentation that is compatible with long-lived industrial environments.

Hardware-rooted security is a parallel track that addresses endpoint trust. TPMs provide secure key storage, secure/measured boot, and remote attestation. TEEs or secure enclaves isolate sensitive operations from the rest of the system. Research has explored enclaves for privacy-preserving analytics and partitioned computation, while

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

other work has integrated hardware security modules into embedded TLS stacks. In OT, these mechanisms are valuable because patch cycles are slow and legacy systems are common.

Industry 5.0 literature highlights new cybersecurity pressures: human–machine collaboration, increased sensitivity of human-related data, and a stronger requirement for resilience and sustainability. The practical implication is that OT security must evolve from static perimeter thinking to continuous verification and safety-aware response.

III. TRADITIONAL OT ARCHITECTURE (LEGACY BASELINE)

Traditional OT security relied on isolation, proprietary protocols, and implicit trust. Many plants operated flat control networks where engineering stations, operator HMIs, SCADA servers, and controllers shared the same trust domain. The air-gap assumption reduced exposure to remote attackers, but it did not address insiders, infected maintenance laptops, or supply-chain compromise. When malicious code enters such an environment, the absence of internal boundaries makes lateral movement easy.

Legacy constraints amplify risk. Controllers are often difficult to patch, cannot run modern endpoint protection, and use protocols without authentication or encryption. Continuous process plants cannot tolerate unplanned downtime, which limits intrusive scanning and aggressive change. Therefore, in the legacy baseline, security is commonly retrofitted with an availability-first mindset.

Figure 1 depicts the typical situation: a coarse boundary between enterprise and OT, and limited internal segmentation inside the OT domain. Many brownfield environments still resemble this design, especially where connectivity has been added informally over time.

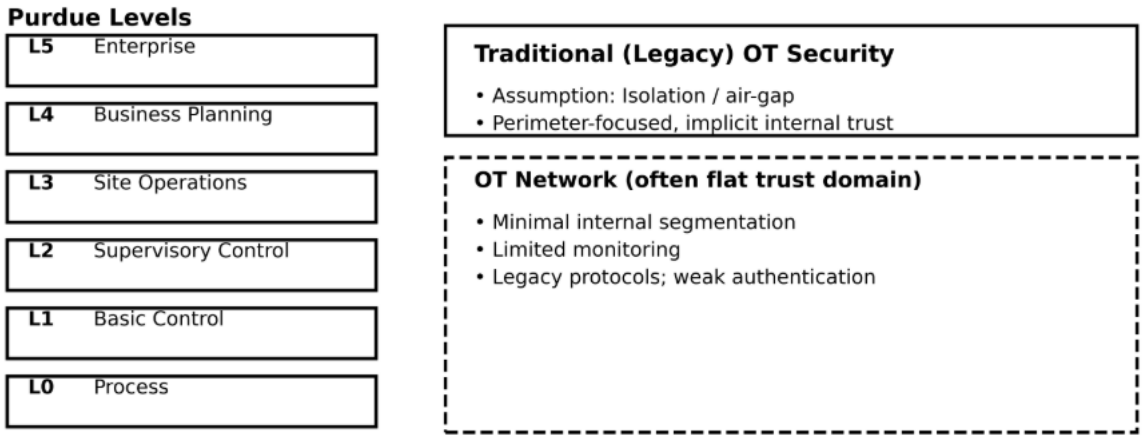

Fig. 1. Traditional Purdue reference view and typical legacy OT security posture (air-gap/implicit trust).

IV. CURRENT OT ARCHITECTURE (SEGMENTATION + HARDWARE TRUST)

Current best practice adopts structured segmentation using Purdue and IEC 62443 zoning. A common pattern is an OT demilitarized zone (DMZ) that separates enterprise IT from site operations. Services that must bridge IT and OT—historians, remote access brokers, patch staging, and file transfer—are placed in the DMZ and are tightly controlled. Inside the plant, the network is further segmented into zones for operations, supervisory systems, and cell/area control networks. Firewalls and allowlists restrict traffic to necessary flows, and passive monitoring tools observe industrial protocols without disrupting operations.

Hardware-based trust strengthens endpoint security. TPM-enabled secure boot ensures that a controller or gateway starts from a known-good firmware image. Remote attestation allows a verifier to confirm that a device remains in an expected state. TEEs protect secrets and sensitive logic at runtime by isolating them from the general-purpose operating system. This is valuable in OT where patching may be infrequent.

Figure 2 shows a reference segmentation architecture with an OT DMZ and controlled conduits. Figure 3 shows a device trust architecture combining TPM and TEE and linking it to attestation and monitoring services. Figure 5 adds a practical secure remote-access pattern that avoids direct IT-to-OT connectivity, which is a common weakness in real plants.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

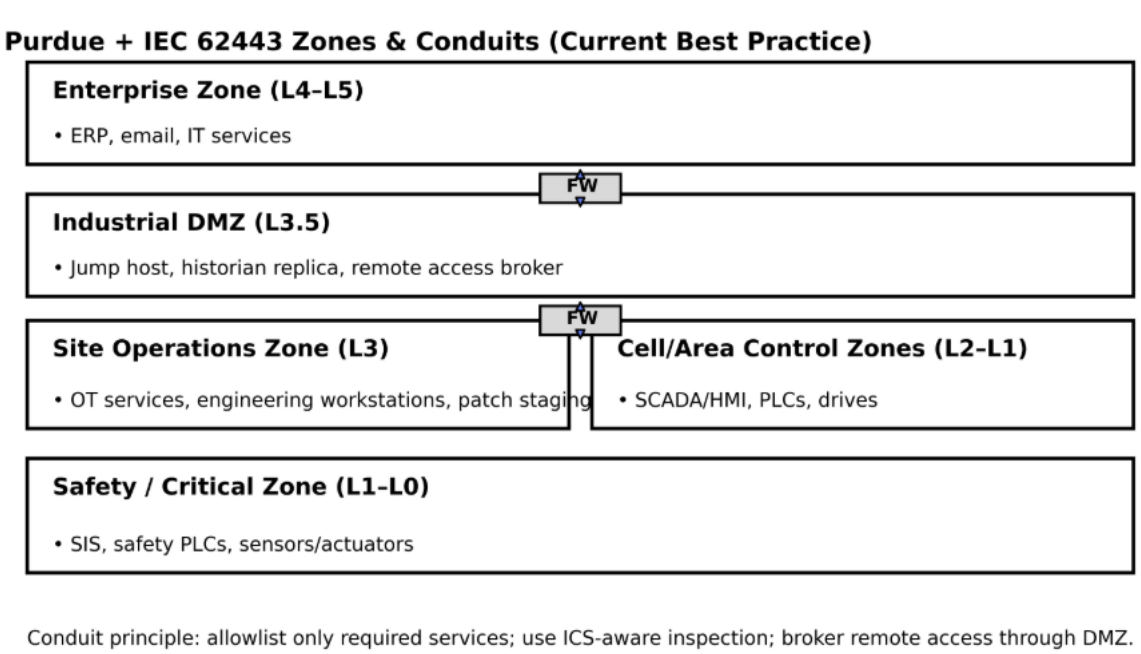

Fig. 2. Current Purdue-aligned segmentation with IEC 62443 zones and controlled conduits including an OT DMZ.

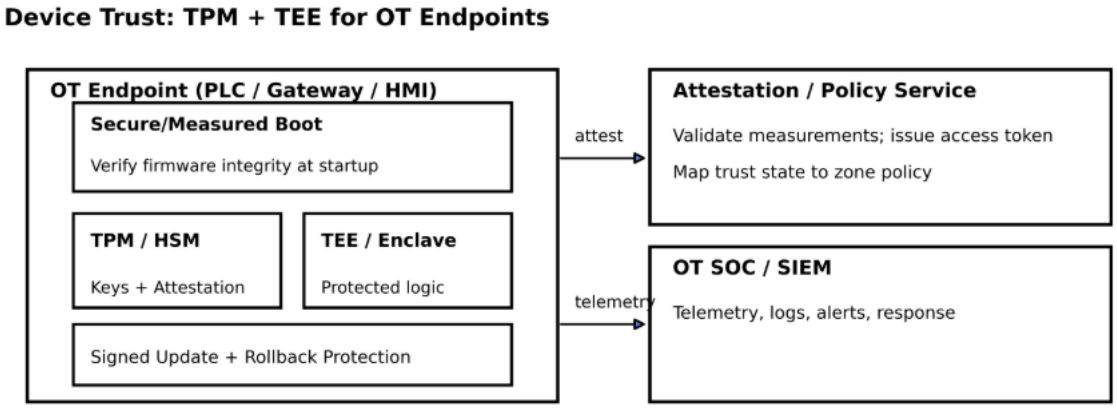

Fig. 3. Hardware-rooted device trust using TPM/HSM and TEE, integrated with attestation and monitoring services.

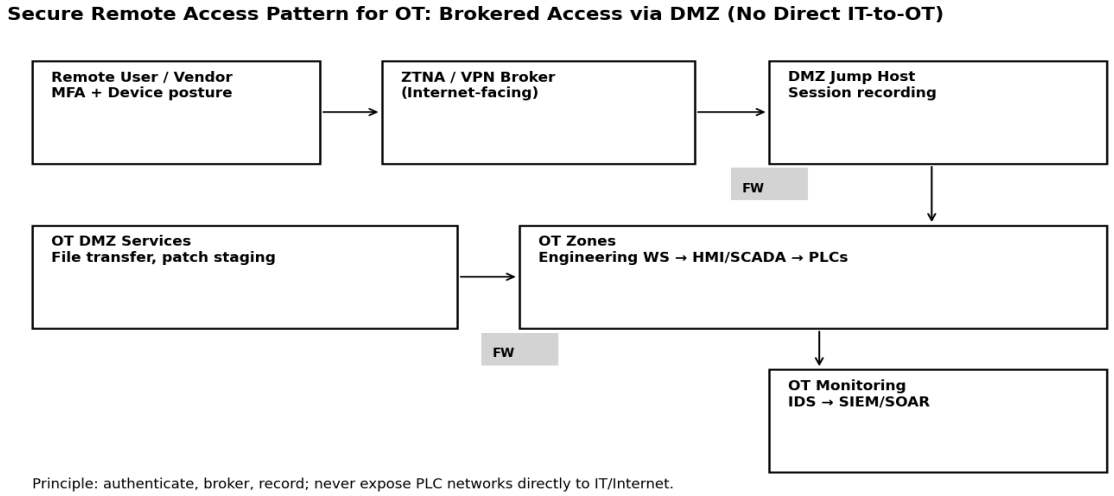

Fig. 4. Brokered secure remote access pattern for OT using ZTNA/VPN broker and DMZ jump host (no direct IT-to-OT).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

V. PROPOSED FUTURE-PROOF ARCHITECTURE (HYBRID ZERO TRUST OT)

While current best practices reduce risk, they are often static. Firewall rules and VLAN boundaries may not adapt quickly to operational change or threat conditions. Future OT environments will be more dynamic due to IIoT scale, edge analytics, and cross-site operations. Therefore, we propose a hybrid architecture that applies Zero Trust principles to OT while keeping the operational realism of Purdue segmentation.

A. Threat model and assumptions: The architecture assumes adversaries may enter through enterprise compromise, remote access misuse, supply-chain/firmware tampering, or infected maintenance assets. It also assumes partial failures: a workstation or server can be compromised even with good hygiene. Therefore, the system is designed to contain intrusions and to continuously verify that critical endpoints remain trusted. Operational constraints are assumed: latency-sensitive control traffic must not be disrupted, and safety functions must remain deterministic.

B. Architecture overview: The design introduces an identity and policy plane that continuously authenticates users and devices and authorizes only the minimum required access for limited time windows. Device identity is anchored in hardware (TPM/secure element) and device health is proven via attestation. A segmentation and transport plane implements micro-segmentation where feasible, using identity-based policies instead of only IP-based rules. Finally, trustworthy endpoints and edge systems implement secure boot, signed updates, TEEs for sensitive code paths, and strong telemetry to the monitoring plane.

C. Hardening methodology: (1) Build asset inventory and communications baselines; (2) define zones by consequence and function; (3) enforce conduits using allowlists and protocol-aware inspection; (4) standardize remote access through brokered pathways with MFA and recording; (5) deploy monitoring and response playbooks; and (6) progressively enable hardware-rooted identity, attestation, and micro-segmentation. This staged approach provides measurable risk reduction at each step.

Figure 4 summarizes the future hybrid model and the interaction between policy, segmentation, endpoint trust, cloud/digital twin, and SOC automation.

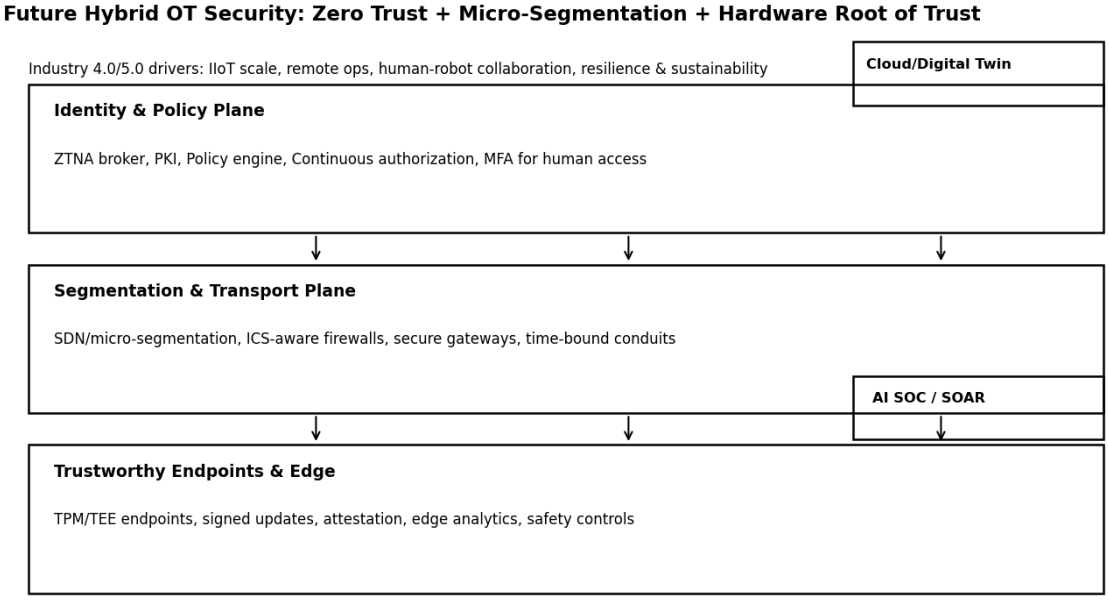

Fig. 5. Future hybrid OT security model: Zero Trust policy plane, micro-segmentation, and hardware-rooted endpoints.

VI. COMPARATIVE ANALYSIS

This section compares architectures across time and across frameworks. Table 1 compares traditional, current, and future-proof approaches. Table 2 compares Purdue, IEC 62443 zones-and-conduits, and a Zero Trust hybrid model. Table 3 contrasts Industry 4.0 and Industry 5.0 security drivers. Table 4 maps key control families to practical OT implementations and shows which part of the proposed architecture provides the control.

The central conclusion is that segmentation remains necessary but not sufficient. As connectivity increases, security must shift from implicit trust to explicit verification and from static boundaries to adaptive controls. Hardware-rooted trust provides a stable anchor for such verification, especially where patching is constrained.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

TABLE 1. Comparison of Traditional, Current, and Future-Proof OT Security

Aspect	Traditional OT	Current OT	Future-Proof OT
Security model	Implicit trust; perimeter/air-gap	Defense-in-depth; zones & conduits	Zero Trust; continuous verification
Segmentation	Physical separation; flat OT	Purdue + IEC 62443 zoning; DMZ	Micro-segmentation; policy-driven conduits
Device integrity	Minimal	Secure boot + TPM on key assets	TPM/TEE on endpoints; attestation everywhere
Monitoring	Limited	Central logging + OT IDS	AI-assisted analytics + automated response
Resilience	Low; high impact if breached	Improved containment and recovery	Graceful degradation; rapid recovery

TABLE 2. Purdue vs. IEC 62443 vs. Zero Trust Hybrid OT Models

Dimension	Purdue Model Focus	IEC 62443 Zones & Conduits	Zero Trust Hybrid OT
Core idea	Hierarchy of functions/levels	Risk-based zones + controlled conduits	Identity-driven access; verify continuously
Strength	Simple placement guidance	Formal security levels; design requirements	Adapts to change; reduces implicit trust
Typical controls	Layer boundaries; DMZ pattern	Industrial firewalls; allowlists; segmentation	ZTNA; attestation-based access; micro-segmentation
Key gap	Not a security standard	Often implemented statically	Requires OT-safe tuning and governance
Best use	Initial segmentation blueprint	Detailed architecture and compliance	Future-ready operations at scale

TABLE 3. Industry 4.0 vs. Industry 5.0 Security Requirements and OT Implications

Security driver	Industry 4.0 implication	Industry 5.0 implication
Connectivity	IIoT and IT–OT convergence expands entry points	Adds human-machine interfaces and new data sources
Safety	Cyber incidents disrupt production and quality	Incidents can directly endanger humans (cobots, wearables)
Data sensitivity	Process/IP data requires protection	Personal and well-being data increases privacy requirements
Resilience	Downtime costs; ransomware risk	Resilience is a core pillar; recovery is essential
Sustainability	Optimization and efficiency goals	Security must protect green transition and sustainable operations

TABLE 4. Control Families and Where They Fit in the Proposed OT Hardening Architecture

Control family	Practical OT implementation	Where it sits in the architecture
Asset & identity	Inventory, unique device identity, credential hygiene	Policy plane + CMDB/asset registry
Access control	Brokered remote access, MFA, least privilege, session recording	ZTNA/VPN broker + DMZ jump host
Network segregation	Zones, conduits, allowlists, ICS-aware firewalls	Segmentation/transport plane
Endpoint integrity	Secure/measured boot, signed updates, rollback protection	TPM/secure element + endpoint management
Runtime protection	TEE/enclave for secrets and critical logic	Trustworthy endpoints
Monitoring & response	Passive OT IDS, SIEM correlation, safe containment playbooks	SOC/SOAR + OT sensors

VII. INDUSTRY 4.0/5.0 DISCUSSION AND FUTURE TRENDS

Industry 4.0 introduced smart manufacturing, cyber-physical systems, and large-scale connectivity between OT and IT. Security implications include more entry points (IIoT devices, remote access paths), more complex supply chains, and higher ransomware impact. Industry 5.0 builds on Industry 4.0 but shifts focus toward human-centric operations, sustainability, and resilience. This evolution increases the importance of protecting human safety and privacy in addition to operational continuity. Human–robot collaboration and wearable/assistive technologies introduce new interfaces that must be strongly authenticated and protected against manipulation.

Three trends are likely to shape OT hardening. First, identity-based access and Zero Trust controls will increasingly replace shared credentials and flat trust models. Second, attestation and hardware-backed identity will become more common in industrial endpoints due to supply-chain risk and the need to trust telemetry and commands. Third, cryptographic agility (including post-quantum readiness) will become a planning requirement because OT lifecycles are long and cryptographic assumptions can change.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Practically, these trends reinforce the need for a unified architecture where controls are consistent across enterprise, DMZ, operations, and cell/area zones, and where safety is explicitly considered in incident response.

VIII. IMPLEMENTATION GUIDANCE FOR BROWNFIELD OT

Brownfield sites contain legacy controllers and vendor systems that cannot be replaced quickly. The proposed architecture can still be implemented using compensating controls. First, define zones based on function and consequence (safety, control, monitoring, engineering, and enterprise integration). Second, implement conduits using industrial firewalls and secure gateways, and use allowlists for protocols and endpoints. Third, standardize remote access through a DMZ jump host with multi-factor authentication and session recording (Figure 5).

For device trust, start where the technology is available: gateways, servers, and workstations can enforce secure boot and store keys in TPMs. For legacy controllers, place a hardened gateway in front of the device to terminate secure channels, provide protocol-aware filtering, and create a ‘protective shell’ around the legacy asset. For critical safety areas, consider one-way gateways (data diodes) where monitoring data must flow out but control commands must not flow in.

Operationalize monitoring: collect logs from firewalls, servers, and engineering workstations; deploy passive OT network sensors for protocol anomaly detection; integrate alerts into the SOC; and test response playbooks that preserve safety (isolation, manual mode, safe shutdown where required).

IX. FUTURE-PROOFING RECOMMENDATIONS

1) Cryptographic agility: design key and certificate management so algorithms can be replaced without replacing devices; ensure firmware update mechanisms can deliver crypto changes.

2) Hardware-anchored identity and attestation: standardize TPM/secure-element usage for new procurements; enable measured boot and attestation for critical assets; integrate attestation results into access decisions.

3) Adaptive segmentation: move toward identity-based micro-segmentation; apply deny-by-default conduits; grant time-bound access for maintenance.

4) Continuous monitoring and response: baseline control traffic; use OT-aware analytics; automate safe containment actions with human oversight.

5) Safety-security co-engineering: validate security controls against process safety requirements; ensure response actions do not create unsafe states.

These recommendations improve lifecycle durability and reduce dependence on static boundaries, enabling OT systems to remain resilient as threats and technologies evolve.

X. CONCLUSION

OT infrastructure hardening is most effective when network segregation limits blast radius and hardware-level security anchors trust at endpoints. Traditional reliance on isolation and implicit trust does not meet the needs of connected Industry 4.0/5.0 environments. Current best practices—Purdue segmentation, IEC 62443 zoning, DMZs, and hardware-backed secure boot—provide a strong baseline. To future-proof OT, organizations should evolve toward a hybrid model incorporating Zero Trust principles, micro-segmentation, continuous attestation, and AI-enabled monitoring and response.

The reference architectures and graphics in this paper provide an actionable blueprint for staged adoption in brownfield plants. By starting with zoning and conduits and progressively adding hardware trust and adaptive policy, organizations can reduce risk while maintaining availability and safety.

REFERENCES

[1] M. Bhole, W. Kastner, and T. Sauter, "A Model Based Framework for Testing Safety and Security in Operational Technology Environments," Proc. IEEE ETFA, 2022.

[2] J. I. Choi et al., "A Hybrid Approach to Secure Function Evaluation using SGX," Proc. ACM AsiaCCS, 2019.

[3] T. Elgamal and K. Nahrstedt, "Serdab: An IoT Framework for Partitioning Neural Networks Computation across Multiple Enclaves," Proc. IEEE/ACM CCGRID, 2020.

[4] L. Fiolhais and L. Sousa, "QR TPM in Programmable Low-Power Devices," arXiv:2309.17414, 2023.

[5] D. Jha et al., "Trusted Platform Module-Based Privacy in the Public Cloud: Challenges and Future Perspective," IT Professional, 2022.

[6] O. Kehret, A. Walz, and A. Sikora, "Integration of Hardware Security Modules into a Deeply Embedded TLS Stack," International Journal of Computers, 2016.

[7] S. Saha et al., "Integrating Hardware Security into a Blockchain-Based Transactive Energy Platform," Proc. IEEE NAPS, 2020.

[8] H. Son et al., "ASM: Augmented Security Module for Commercial IoT Devices," Tehnicki Vjesnik – Technical Gazette, 2024.

[9] S. Ugwuanyi and J. Irvine, "Industrial and Consumer Internet of Things: Cyber Security Considerations, Threat Landscape, and Countermeasure Opportunities," Proc. IEEE SmartNets, 2021.

[10] K. Stouffer et al., "Guide to Operational Technology (OT) Security," NIST SP 800-82 Rev. 3, 2023.

[11] ISA/IEC 62443 series, "Security for Industrial Automation and Control Systems" (Zones and Conduits), 2020.

[12] M. Breque, L. De Nul, and A. Petridis, "Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry," European Commission, 2021.

[13] R. Kour et al., "Cybersecurity for Industry 5.0: trends and gaps," Frontiers in Computer Science, 2024.

[14] B. Santos et al., "Cybersecurity in Industry 5.0: Open Challenges and Future Directions," arXiv:2410.09538, 2024.