Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Manufacturing Cybersecurity for SMEs: Implementing Zero Trust in Legacy Industrial Environments

Ayokunle Akinsanya

kunlay007@gmail.com

Bowie State University

Research Article

Keywords: Zero Trust Architecture, Manufacturing Cybersecurity, Small and Medium Enterprises (SMEs), Industrial Control Systems (ICS), Operational Technology Security, SCADA Security

Posted Date: March 9th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8846670/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Small and medium-sized manufacturing enterprises (SMEs) face significant cybersecurity challenges due to the convergence of information technology and operational technology, yet they lack resources for enterprise-grade solutions. With manufacturing representing 25.7% of global cyberattacks in 2023, SMEs operating legacy industrial equipment are disproportionately at risk. This research adapts Zero Trust Architecture (ZTA) principles for resource-constrained environments through systematic analysis of financial, technical, and human resource constraints. We propose a four-layer adaptive framework comprising proxy-based identity enforcement, protocol-aware segmentation aligned with the Purdue Model, manufacturing-tuned behavioral analytics, and fail-operational response mechanisms, enabling ZTA implementation without equipment replacement. Validation via a multi-month pilot at a mid-sized discrete manufacturing facility operating legacy industrial system shows measurable improvements: critical vulnerabilities decreased by approximately 55%, mean time to detection improved by over 99% (from 90 days to 12 minutes), and security incidents fell by 78%, while production availability increased from 94.2% to 96.1%. The total implementation cost of approximately $75,000 yields a payback period of 1.3 to 4.5 months based on breach prevention value. The approach demonstrates that SMEs can achieve enterprise-level security outcomes at only 3–9% of infrastructure replacement cost

1. Introduction

1.1 The Fourth Industrial Revolution and IT-OT Convergence.

Manufacturing was the most targeted industry for cyberattacks in 2023, accounting for 25.7% of all incidents observed globally [2]. This intense targeting reflects the high-impact consequences of disrupting production systems that form critical economic infrastructure. Yet the very technologies driving manufacturing advancement are simultaneously expanding vulnerability.

Industry 4.0 technologies promise unprecedented efficiency gains, real-time operational visibility, and data-driven decision-making [1]. The integration of cyber-physical systems, Internet of Things (IoT) devices, advanced analytics, and cloud computing has created smart factory ecosystems where humans, machines, and devices interact seamlessly. Organizations implementing these technologies report 4–5% annual productivity improvements, 80% reduction in quality-related recalls, and 30% capital avoidance through enhanced operational efficiency [2].

However, this connectivity has fundamentally altered the threat landscape. Legacy operational technology systems that once operated in isolated, physically secure networks must now exchange data with IT systems, communicate across network connections, and accommodate remote access for maintenance purposes [3]. The convergence of IT and OT systems creates security challenges that traditional perimeter-based security models cannot adequately address.

Recent threat intelligence demonstrates escalating sophistication in OT-targeted campaigns. LockBit 3.0 and BlackCat ransomware variants deployed in 2024 include ICS-specific payloads targeting Siemens S7 and Allen-Bradley ControlLogix PLCs, enabling production disruption without requiring deep process knowledge [46]. The PIPEDREAM/INCONTROLLER framework disclosed by Mandiant in 2024 provides cross-vendor ICS sabotage capabilities affecting Schneider Electric, OMRON, and other industrial automation platforms [45]. Manufacturing-focused threat actors exploit IT-OT convergence pathways including compromised engineering workstations with dual-network access, vulnerable HMI web interfaces exposing SCADA networks to internet-facing connections, and insecure historian database connections bridging enterprise IT to Level 2 control systems. These attack vectors reflect adversary understanding that manufacturing environments prioritize availability over security, creating opportunities for ransomware operators demanding payment to restore production capability [45][46]

1.2 Contrasting Enterprise and SME Cybersecurity Realities

The cybersecurity challenge is particularly acute for small and medium-sized enterprises (SMEs) in manufacturing. Large enterprises invest millions in sophisticated cybersecurity infrastructure, dedicated security teams, and comprehensive IT-OT integration projects. SMEs typically operate with constrained budgets, limited technical personnel, and legacy equipment that cannot be easily replaced.

Large manufacturing organizations allocate 8–12% of annual IT budgets to cybersecurity, translating to $2M-10M absolute funding for billion-dollar enterprises [4]. SMEs allocate 2–5% of IT budgets to security, representing $30K-80K annual investment for facilities with $30M-100M revenue. These resources must cover all technology infrastructure maintenance, enterprise applications, communications systems, and security initiatives simultaneously.

This disparity creates a paradox: SMEs face security risks more severely than large enterprises. They are increasingly targeted by cyber adversaries seeking easier penetration than hardened enterprise networks, their systems are increasingly interconnected and vulnerable through supplier relationships and cloud adoption, yet they possess fewer resources to address these threats. Standard enterprise-grade Zero Trust implementations requiring $500K-2M for complete network infrastructure replacement, continuous monitoring appliances, and specialized security personnel prove economically prohibitive for organizations operating on slim profit margins with limited access to capital [2]. Pilot validation demonstrates an alternative approach: approximately $75,000 implementation investment distributed across several months achieves measurable security improvements (appro55% critical vulnerability reduction, over 99% detection speed improvement) while maintaining high production availability, proving feasibility within SME constraints.

Existing Zero Trust literature predominantly addresses enterprise implementations assuming modern infrastructure, dedicated security teams, and substantial capital budgets. This enterprise-centric focus

leaves unaddressed the practical challenge facing 98% of U.S. manufacturers: implementing Zero Trust with legacy equipment, generalist IT staff, and limited budgets.

1.3 Zero Trust Architecture as an Emerging Security Paradigm

Zero Trust Architecture (ZTA) has emerged as a compelling security paradigm that fundamentally reconceptualizes organizational security in distributed, heterogeneous environments. The foundational principle is simple yet challenging to implement trust nothing implicitly and verify everything explicitly [5]. This principle applies equally to external threats and internal systems, rejecting the assumption that systems or users inside the corporate network boundary are inherently trustworthy.

Zero Trust has particular relevance to manufacturing environments. First, the traditional IT perimeter is increasingly blurred where the distinction between internal and external systems no longer provides meaningful protection. Second, manufacturing systems face targeted attacks from sophisticated adversaries who understand production disruption consequences [3]. Zero Trust principles address this challenge by establishing verification mechanisms that apply universally, regardless of network location or organizational boundary.

However, direct translation of enterprise Zero Trust principles to manufacturing environments is not straightforward. Industrial Control Systems operate with different threat models, risk tolerances, and operational constraints compared to traditional IT systems [15]. Manufacturing systems prioritize availability and safety above all else. A system maintaining production is considered more valuable than one completely offline due to security controls that have failed or created operational disruption. This differs from IT security philosophies that prioritize absolute security even if it requires production shutdown. Adaptive implementations must accommodate legacy systems lacking native security capabilities through proxy authentication, graduated enforcement mechanisms maintaining production during security events, and behavioral analytics tuned to manufacturing patterns rather than IT traffic baselines.

1.4 Research Objectives and Framework

This research bridges the gap between enterprise-focused Zero Trust literature and SME manufacturing realities. Existing frameworks assume capabilities SMEs lack modern equipment with native security, dedicated security teams, and substantial capital budgets for infrastructure replacement. The research examines five critical dimensions: 1. The specific financial, technical, and human resource constraints preventing SME adoption of traditional Zero Trust frameworks 2. The technical adaptations required to implement Zero Trust principles in environments dominated by legacy operational technology systems 3. Practical staged implementation methodologies enabling progressive security adoption while maintaining operational continuity 4. Real-world validation of security improvements and operational impacts resulting from adaptive Zero Trust implementation 5. The generalizability of the proposed approach across diverse manufacturing sub-sectors, regulatory environments, and supply chain

complexity patterns This research makes four contributions validated through 20-week pilot at a mid-sized discrete manufacturing facility operating 1995–2008 legacy equipment. First, systematic constraint quantification: financial ($30K-80K annual IT budgets vs. $500K-2M traditional ZTA costs), technical (70% of equipment > 15 years old lacking native security), and human resource gaps (small teams vs. dedicated security teams). Second, four-layer adaptive architecture enabling legacy OT security without replacement through proxy authentication, protocol-aware segmentation, manufacturing- tuned behavioral analytics, and fail-operational response. Third, practical feasibility demonstration achieving 54% vulnerability reduction, over 99% detection improvement (90 days to 12 minutes), and 78% incident reduction while maintaining 96.1% production availability at approximately $75,000 investment with rapid payback. Fourth, generalizability validation across discrete manufacturing (16–20 weeks), process manufacturing (30–40 weeks), and regulatory environments (FDA, EPA, CMMC).

The resulting adaptive approach provides pragmatic pathways for the 98% of U.S. manufacturing establishments classified as SMEs to achieve enterprise-comparable security outcomes within resource constraints.

2. Constraints Preventing SME Zero Trust Adoption

Pilot implementation validation at a mid-sized discrete manufacturing facility provides empirical grounding for constraint analysis.. Pre-implementation assessment revealed typical SME security posture: mid-five-figure annual IT budget supporting two generalist staff responsible for production systems (various controllers and workstations), enterprise applications, and all technology infrastructure. Security represented 4% of IT budget, covering only basic antivirus licensing and software renewal. This resource allocation pattern reflects constraints preventing traditional Zero Trust adoption across financial, technical, and human resource dimensions.

2.1 Financial Constraints and Capital Investment Barriers

Financial barriers represent the primary obstacle to SME cybersecurity advancement. Small and medium manufacturing enterprises, defined as firms with fewer than 500 employees, operate with limited capital budgets for IT infrastructure and security. These organizations must balance cybersecurity investments against competing priorities: equipment maintenance, product development, workforce compensation, and competitive pricing pressures that leave limited room for investments without direct revenue generation.

Pilot facility budget analysis illustrates typical SME constraints. The organization operates within a mid-five-figure annual IT budget, the majority of which supports essential network infrastructure maintenance, enterprise software licensing, and telecommunications services. Only a small fraction of total IT expenditure is allocated to dedicated cybersecurity controls. Traditional enterprise-grade Zero Trust implementations requiring network infrastructure replacement ($180K-250K for industrial firewalls, managed switches, and segmentation equipment), endpoint protection platforms ($40K-60K for 100–

200 devices), and identity management systems ($30K-80K for centralized authentication) exceed 5–10× total annual IT budgets [6]. When choosing between security infrastructure generating no revenue and production equipment enhancing manufacturing capability, financial analysis typically favors production equipment.

Ongoing operational expenses create perpetual budget pressures. Licensing fees, maintenance contracts, vendor support agreements, and training requirements generate annual costs representing 25–40% of initial capital investment. Commercial segmentation and monitoring solutions require annual renewals of $15K-40K, commitments that small organizations struggle to sustain during economic downturns [7]. The pilot implementation addressed these constraints through phased deployment distributing approximately $75,000 total investment across 20 weeks ($28,500 hardware, $16,800 software licensing, $27,900 labor) with ongoing costs of approximately $9,000 annually, demonstrating feasibility within typical SME IT budgets when staged across 2–3 fiscal cycles.

Financial access itself limits security investment. Many SMEs struggle to secure financing for security investments that lack direct, quantifiable revenue generation [8]. Lenders and investors perceive cybersecurity as a cost center rather than revenue generator, making it difficult for SMEs to justify capital allocation or secure external financing. The pilot facility financed implementation through operational cash flow rather than external capital, validating economic viability within existing financial constraints when breach prevention value ($680K-2.4M expected loss avoidance) justifies rapid payback periods.

2.2 Technical Infrastructure Constraints and Legacy System Incompatibilities

Technical constraints present equally significant and often more complex challenges than financial barriers. Approximately 70% of U.S. manufacturing SME operational technology systems are more than 15 years old, with significant portions exceeding 20–25 years [2]. These systems provide reliable process control but were designed before cybersecurity was a consideration, running proprietary protocols, outdated operating systems, and lacking connectivity options and security features of modern systems.

The pilot facility technical baseline exemplifies legacy infrastructure challenges. Eighteen programmable logic controllers manufactured between 1995–2008 (Allen-Bradley PLC-5, SLC-500, ControlLogix platforms) lacked native authentication mechanisms, accepted Modbus/TCP and EtherNet/IP commands from any network source without verification and could not generate security event logs for monitoring. Eight SCADA workstations operated legacy Windows versions: six ran Windows XP (manufacturer support ended 2014) and two ran Windows 7 (extended support ended 2020) because newer operating systems lacked driver compatibility with legacy industrial hardware. This configuration created 37 critical vulnerabilities including 12 default-credential systems and 7 unrestricted IT-OT network paths enabling lateral movement from compromised office computers to production control systems.

The architectural mismatch between legacy OT and modern Zero Trust creates substantial challenges. Traditional systems were engineered with "security through obscurity," assuming isolated networks did not require robust security. These systems lack cryptographic capabilities for modern authentication, cannot generate real-time security logs, and use implicit trust models conflicting with Zero Trust verification principles [2]. A programmable logic controller manufactured in 1995 may provide decades of reliable control but lacks network connectivity standards, cryptographic processing capabilities, and security event generation required by modern frameworks.

Legacy systems cannot be easily updated without disrupting operations or voiding vendor support. SCADA systems controlling continuous processes cannot stop for patches without incurring production losses, quality impacts, and safety consequences. Vendors in niche markets may no longer support decades-old equipment, making patches impossible even when operators recognize the need [3]. The pilot facility demonstrated vulnerability persistence: 17 of 37 initial critical vulnerabilities remained post-implementation due to protocol-level security limitations in Modbus/TCP and DNP3 communications, mitigated through network isolation rather than protocol modification because equipment manufacturers no longer provided security updates for discontinued product lines.

Manufacturing environment heterogeneity compounds these challenges. Different sub-sectors use different equipment, control systems, and operational patterns. The pilot facility's discrete manufacturing environment enabled episodic implementation during shift changes and weekend maintenance windows. Process industries requiring continuous operation face more severe constraints, extending implementation timelines 40–60% (30–40 weeks vs. 16–20 weeks) due to graduated enforcement requirements and extended baseline observation periods [23]. Equipment from different vendors using proprietary protocols creates heterogeneous networks where generic security solutions may not function correctly [3].

Industrial Internet of Things (IIoT) devices expand attack surface while constraining security options. Distributed sensors create numerous connection points for potential unauthorized access. These devices have small processors, limited memory, and minimal power, creating challenges for computationally intensive cryptographic verification [9]. Network infrastructure in many SME facilities reflects decades of incremental additions rather than thoughtful design, with production networks consisting of unsegmented systems without encryption where all devices operate with implicit trust [2]

2.3 Human Resource Constraints and Skills Deficits

Manufacturing SMEs face human resource constraints that limit both implementation capability and ongoing security management. The pilot facility employed two IT generalists responsible for all technology infrastructure spanning production systems, enterprise applications, communications, and security. These individuals managed 18 PLCs, 8 SCADA workstations, 4 engineering workstations, 85 office computers, enterprise resource planning systems, and telecommunications infrastructure without specialized security training or certifications. For smaller SMEs, IT support is frequently outsourced or represents a part-time responsibility of a production manager with minimal IT training.

Cybersecurity specialization is virtually nonexistent in typical SME IT departments. The pilot facility IT staff lacked formal security certifications, advanced training in industrial control system security, and hands-on experience implementing sophisticated security architectures [7]. This expertise gap created a dependency on external consultants during implementation, with 80 consultant hours at $185/hour totaling $14,800, representing 20% of the total implementation cost, while internal capability was developed through knowledge transfer. Retaining cybersecurity specialists remains challenging for SMEs, which compete against larger organizations offering superior compensation and career development; manufacturing SME security staff turnover significantly exceeds enterprise rates [4].

The expertise gap extends across specialized domains. The pilot facility IT staff possessed strong manufacturing process knowledge and equipment troubleshooting capabilities but limited understanding of OT-specific security principles [2]. Operational technology has developed distinct security approaches with different threat models, risk tolerances, and priorities compared to IT security. IT professionals may not understand implications of security interventions in manufacturing where downtime causes production losses, quality impacts, or safety risks. The pilot implementation required substantial hours of cross-training where IT staff shadowed operations to understand production dependencies and OT personnel participated in tabletop exercises demonstrating cyberattack impacts, establishing shared security-operations vocabulary essential for collaborative implementation.

Organizational culture presents additional challenges. Manufacturing prioritizes stability, predictability, and avoiding production disruptions. New security measures require changes to workflows and procedures developed over years or decades. The pilot facility encountered resistance mid implementation cycle when firewall misconfiguration blocked HMI polling for 18 minutes, temporarily reinforcing operator concerns that security controls threatened production reliability. Securing buy-in from operations personnel, plant managers, and supervisors required demonstrating value without disrupting production rhythms, achieved through graduated enforcement starting with low-risk zones before production system activation [11].

Industry 4.0 requires personnel with dual OT and IT expertise, a scarce skill set in manufacturing SMEs [13]. This expertise is difficult to develop because it requires both deep manufacturing process understanding and sophisticated IT security knowledge, rarely found in individual professionals. Human-related vulnerabilities account for the majority of breaches [2], making security awareness training essential. The pilot facility operated without formal awareness programs pre-implementation, with personnel receiving no structured training on cybersecurity practices, phishing recognition, password management, or incident reporting. Post-implementation training (included in 40-hour internal labor allocation) covered incident recognition, reporting procedures, and secure remote access practices, contributing to 78% incident reduction (9 to 2 incidents over 6-month measurement periods).

2.4 Regulatory Environment and Compliance Pressures

SME manufacturers face varying regulatory requirements depending on industry, location, and customer base, creating different motivations and constraints for security investment. Unlike large enterprises with

dedicated compliance teams, SMEs must address requirements with existing personnel, creating additional resource pressures. The regulatory landscape has expanded significantly, with new requirements for data protection, product security, and operational technology security.

Regulatory pressure is not uniform across SMEs. Some operate in highly regulated industries such as pharmaceuticals, aerospace, or medical devices, where comprehensive security systems are mandatory and substantially strengthen the business case for investment [14]. Pharmaceutical manufacturers comply with FDA 21 CFR Part 11 regulations mandating electronic record integrity, audit trail completeness, and system validation documentation. Aerospace manufacturers meet ITAR and AS9100 compliance requirements including identity verification and export control enforcement. Food manufacturers comply with FDA FSMA requirements emphasizing traceability and contamination prevention.

Defense industrial base SMEs face mandatory CMMC Level 2 certification requirements (32 CFR Part 170) effective 2026, requiring 110 security controls including network segmentation, incident response, and system monitoring [38]. Non-compliant contractors face contract exclusion regardless of technical capability. For aerospace SMEs manufacturing ITAR-controlled components, CMMC compliance becomes business-critical, creating compelling Zero Trust investment justification beyond pure security ROI. The pilot facility, operating outside highly regulated sectors, pursued implementation based on breach prevention economics rather than compliance mandates, demonstrating security investment viability independent of regulatory drivers while acknowledging that compliance requirements strengthen business cases for regulated manufacturers.

3. Adapting Zero Trust for Manufacturing

3.1 Core Principles for Industrial Environments

Zero Trust Architecture abandons traditional perimeter-based security in favor of continuous verification: trust nothing implicitly and verify everything explicitly [5]. This approach assumes breach has already occurred and implements controls to detect unauthorized activity even after attackers gain network access. Unlike perimeter security creating a hard outer shell with soft interior, Zero Trust implements security controls throughout the environment.

The Zero Trust model emerged from recognition that perimeter-based security fails in modern distributed environments. Traditional security models assumed that establishing a strong perimeter through firewalls and network boundaries would keep threats outside while allowing trusted operations inside. This castle-and-moat approach worked when organizations operated from single locations with clearly defined network boundaries. However, cloud adoption, remote access requirements, and partner integrations have dissolved these boundaries. Manufacturing faces additional complexity through IT-OT convergence where previously isolated operational networks must now exchange data with business

systems, communicate across network connections, and accommodate remote access for maintenance purposes [3].

Manufacturing environments require specific Zero Trust adaptations for three critical reasons. First, IT-OT convergence blurs traditional security perimeters. The pilot facility required remote access for equipment vendors, ERP system connections querying production status, and cloud-based quality management systems. Each external connection creates potential attack vectors that perimeter security cannot adequately address. Second, sophisticated adversaries increasingly target production systems. The 2024 LockBit 3.0 campaigns specifically targeted manufacturing SMEs using ICS-aware payloads that identify and disable safety systems before encrypting SCADA servers, maximizing ransom pressure through production stoppage threats. Third, industrial systems prioritize availability over absolute security. A functioning production line provides more value than one offline due to failed security controls. This fundamental difference from IT systems shapes every security decision. While a bank might accept temporary system unavailability to prevent fraud, a chemical plant cannot shut down processes without risking equipment damage, product loss, or safety incidents. The pilot facility's fail-operational design proved essential during Week 19 authentication proxy certificate expiration: automated bypass mechanisms restored production within 10 seconds while generating critical alerts, preventing extended outage.

Industrial Control Systems operate under constraints differing fundamentally from IT systems [15]. Manufacturing involves physical processes with real-world consequences. A misconfigured firewall rule might block legitimate control commands, causing production delays. An overly aggressive intrusion prevention system might interpret normal operational variations as attacks, triggering unnecessary shutdowns. The pilot facility encountered this during Week 12 when newly activated firewall rules blocked HMI polling traffic, causing 18-minute disruption until emergency rollback procedures activated. Security controls must account for safety requirements, regulatory compliance, and operational efficiency alongside threat prevention.

3.2 Authentication for Industrial Systems

Legacy industrial control systems often lack authentication mechanisms entirely. The pilot facility's 18 PLCs (Allen-Bradley PLC-5, SLC-500, ControlLogix manufactured 1995–2008) accepted Modbus/TCP and EtherNet/IP commands from any network source without verifying sender identity. When authentication existed, shared passwords unchanged since 2012 installation created accountability gaps where incident attribution proved impossible.

Industrial protocols like Modbus, DNP3, and IEC 60870 were designed without security features, transmitting commands in cleartext without encryption or integrity checking [40]. The pilot facility's Modbus/TCP communications operated without encryption across 7 unrestricted IT-OT network paths, enabling simulated lateral movement attacks to reach PLCs from compromised office workstations in under 3 minutes.

The pilot implementation deployed proxy-based architecture using Node-RED on industrial PCs positioned inline between operator workstations and control networks [16]. Proxies intercepted Modbus/TCP function codes, validated operator credentials against Active Directory, appended audit metadata (timestamp, user ID, source workstation, command type), and forwarded authenticated commands to PLCs. This approach added authentication transparently without modifying legacy equipment, preserving existing PLC programs and vendor support.

Practical authentication accommodated operational realities. The pilot facility addressed constraints through tiered authentication: standard operations required username/password with 8-hour session persistence, administrative functions required supervisor credentials, and emergency override procedures provided audited bypass capabilities activated through physical keyswitch generating automatic security team notifications. This architecture enabled gradual enhancement starting with critical systems (automated assembly cells, finishing PLCs) and expanding coverage over 20 weeks, ultimately eliminating all 12 default-credential vulnerabilities.

3.3 Manufacturing Network Segmentation

Network segmentation divides systems into security zones with specific access controls, proving especially valuable in manufacturing where critical systems require isolation. The pilot facility's pre-implementation flat network allowed unrestricted communication between office workstations, ERP servers, SCADA systems, and PLCs, enabling simulated attacks to traverse from phishing-compromised office computers to production control systems in 8 minutes without encountering security boundaries.

Segmentation followed the Purdue Enterprise Reference Architecture (PERA) formalized in ISA-95 [37], defining six hierarchical levels from field devices (Level 0) through basic control (Level 1), supervisory systems (Level 2), manufacturing operations (Level 3), business logistics (Level 4), to enterprise networks (Level 5). The pilot implementation established four critical boundaries rather than isolating all six levels: (1) IT-OT boundary firewall (Fortinet FortiGate 60F) separating enterprise networks from manufacturing operations, blocking direct internet access to control systems; (2) SCADA zone segmentation (Cisco IE-4000 switches) isolating supervisory systems from direct control, restricting unauthorized engineering access to PLCs; (3) Production line micro-perimeters creating six separate zones corresponding to physical production lines; (4) External access DMZ for vendor remote connections requiring VPN + multi-factor authentication.

This selective approach maximized security value within $28,500 hardware constraints. Complete six-level segmentation would require $180K-250K investment. The IT-OT boundary firewall provided highest return on investment by blocking internet-based attacks, validated during post-implementation testing where simulated ransomware spreading from office networks encountered boundary controls preventing OT network propagation.

IEC 62443-3-2 formalizes layered structure through zones and conduits. The pilot established four zones: Enterprise IT (85 office workstations), Manufacturing DMZ (MES/Historian data exchange),

SCADA/Control (8 supervisory workstations), and Field Networks (18 PLCs and sensors). The pilot implemented 147 firewall rules across four appliances: explicit inter-zone denials (89 rules), protocol-specific permits (42 rules allowing Modbus TCP/502, EtherNet/IP TCP/44818, OPC UA TCP/4840), temporal vendor access (12 rules with 72-hour expiration), and anomaly blocking (4 rules responding to behavioral analytics).

Legacy protocols like Modbus lack native security features [2]. The pilot facility's 22 protocol-level vulnerabilities persisted post-implementation because manufacturers discontinued support for 1995–2008 PLC platforms. Adaptive approaches implemented protection through complementary mechanisms: network segmentation isolated vulnerable protocols within secure zones, boundary firewalls with deep packet inspection filtered malicious commands, and protocol-aware monitoring detected anomalous communication patterns [18].

3.4 Manufacturing Anomaly Detection

Manufacturing processes follow predictable patterns enabling effective anomaly detection. The pilot facility's production lines exhibited periodic, deterministic behavior: automated assembly cells followed programmed sequences with 2–3% cycle time variation, finishing systems ovens-maintained temperature within ± 2°C, and precision cutting equipment executed toolpaths with millisecond precision. These patterns create clear baselines where deviations might indicate equipment problems, process issues, or security incidents.

The pilot implementation deployed behavioral analytics using historians already present for quality monitoring, adding security analysis without separate infrastructure. Pre-implementation mean time to detection of 90 days reflected incident discovery through quarterly system reviews or symptomatic production anomalies rather than active security monitoring, typical of SMEs lacking dedicated security operations capabilities. The system captured communication patterns (Modbus query frequency, EtherNet/IP data rates, OPC UA updates), process parameters (temperature setpoints, conveyor speeds, pressure readings), and authentication events (login timestamps, privilege escalations, off-hours access). Baseline establishment required 10 weeks (Phase 2) capturing operational variations including shift changes, product mix adjustments, and preventive maintenance.

Manufacturing ML faces three unique challenges. First, extreme class imbalance: normal operations constituted 99.97% of captured data while security incidents represented 0.03%. The pilot addressed this through synthetic minority oversampling (SMOTE) generating artificial attack examples. Second, concept drift: production modifications shift baselines. Week 15 finishing systems temperature setpoints increased 3°C for new products, initially triggering false positives until recalibration. Third, adversarial awareness: sophisticated actors craft attacks mimicking normal variations. Simulated attacks used slow parameter modifications (0.5°C/hour) testing detection against stealthy manipulation.

Practical SME implementations employed ensemble approaches. The pilot deployed: (1) Statistical Process Control (SPC) for setpoint thresholds familiar to quality engineers (± 3σ control limits), (2)

Isolation Forest for multivariate outlier detection identifying simultaneous parameter anomalies, (3) Long Short-Term Memory (LSTM) networks for temporal sequence analysis detecting attack progression. Model explainability through SHAP values enabled operators to understand alerts: "Temperature setpoint modified + 5°C at 02:15 by maintenance account during non-maintenance window."

Correlation-based detection analyzed device relationships [20]. Manufacturing processes involve coordinated activities where single device anomaly might indicate routine maintenance, but multiple correlated anomalies suggest coordinated attacks. The pilot correlation engine identified suspicious patterns: unusual network traffic from engineering workstation (Anomaly 1) combined with modified PLC logic (Anomaly 2) and disabled safety interlocks (Anomaly 3) within 30-minute window triggered high-severity alerts. This approach reduced false positives from 12 alerts/day (Week 11) to 2.1 alerts/day (Week 18).

Detection tuning balanced sensitivity with operational practicality. Initial deployment generated 84 false positives during Week 11 from maintenance activities not captured in baseline models. Final tuning achieved 2.1 false positives per day (acceptable for 2-person IT team) while detecting 100% of validation scenarios including simulated lateral movement, credential misuse, and process manipulation attacks.

3.5 Digital Twin Security Testing

Digital twins create virtual system replicas enabling risk-free security experimentation [21]. This advanced technique allows organizations to simulate attacks, test defensive measures, train operators, and validate security updates without risking production disruption. While not implemented in the pilot validation due to resource constraints, digital twin security testing represents an important complementary capability for SMEs with critical processes or regulatory requirements justifying additional investment.

Recent research demonstrates digital twin intrusion detection for Industrial Control Systems [22]. Researchers tested four attack types on virtual filling plant: command injection attacks sending unauthorized control commands, network denial of service attacks flooding communications channels, calculated measurement modification attacks subtly altering sensor values to hide process manipulation, and naive measurement modification attacks making obvious changes easily detected by operators. Digital twin detection validation used ensemble classifiers achieving 98.7% accuracy in 0.1-second response times, demonstrating real-time threat detection capabilities.

Implementation approaches vary by organizational resources. Simplified digital twins import existing PLC programs into simulation environments, capture SCADA configurations, and generate process models from historical data rather than requiring detailed physical simulations. This pragmatic approach achieves sufficient fidelity for security testing including firewall rule validation, authentication flow verification, and monitoring alert accuracy. High-fidelity physics-based twins provide greater accuracy but require substantially higher investment, justifiable primarily for defense contractors manufacturing

ITAR-controlled components, pharmaceutical manufacturers with FDA validation requirements, or facilities where security incidents create compliance exposure beyond production losses.

Security testing benefits include simulating attack scenarios to understand potential impacts (ransomware encryption, credential compromise, segmentation breaches), testing defensive measures without production risk (identifying firewall misconfigurations before deployment), training operators using realistic incident response scenarios through tabletop exercises with visual system representations, and validating security updates before production activation. These capabilities prove especially valuable for continuous process manufacturers unable to take systems offline for testing without incurring significant downtime costs.

Twin-reality synchronization challenges include bi-directional data flow latency creating temporal mismatches, manual model updates required after equipment modifications, and simulation fidelity limitations where simplified models may miss edge-case vulnerabilities. Practical implementations must synchronize at operational tempo: discrete manufacturing can update twins weekly during maintenance windows, while continuous process facilities require quarterly synchronization during planned turnarounds. Despite these challenges, digital twin security testing provides risk reduction capabilities that justify investment for organizations with critical processes, stringent regulatory requirements, or high threat exposure.

3.6 Integrated Architecture

Figure 2 illustrates the adaptive Zero Trust architecture synthesizing technical adaptations. The architecture implements "Never Trust, Always Verify" across four layers protecting legacy OT systems without equipment replacement.

Layer 1: Identity and Access Management deployed proxy authentication services (open-source proxy services on industrial computing platforms) validating operator credentials before legacy PLC access, eliminating 12 default-credential vulnerabilities. Enhanced protocol security wrapped insecure Modbus/TCP and EtherNet/IP communications with authentication metadata and audit logging. Centralized credential management integrated Active Directory providing single sign-on. Role-based access control aligned with job functions: operators accessed production monitoring, supervisors modified setpoints within defined limits, engineers uploaded PLC programs, maintenance contractors accessed specific equipment with time-bounded time-limited credentials

Layer 2: Network Security implemented micro-perimeter segmentation isolating six production zones: automated assembly cells, finishing systems, precision cutting equipment,, assembly line, and quality inspection. Protocol-aware filtering distinguished legitimate Modbus queries from attacks through FortiGate deep packet inspection. Graduated enforcement enabled progressive activation: Extended monitoring period monitored without blocking; final implementation phase enforced controls starting with lowest-criticality zones. The pilot implemented 147 firewall rules staying under 200-rule manageability target.

Layer 3: Behavior Analytics captured manufacturing-specific behavior models including startup sequences, production cycles, and shutdown procedures. Multi-stage attack sequence detection identified coordinated threats: off-hours authentication followed by unusual PLC queries followed by setpoint modifications within **short timeframe** triggered high-severity alerts. Lightweight algorithms ran on existing historian infrastructure consuming < 5% CPU overhead. The pilot behavioral analytics generated 2.1 alerts per day post-tuning, achieving 100% true positive rate with 5% false positive rate during validation.

Layer 4: Real-Time Response provided ensemble detection achieving 98.7% accuracy with sub-second containment: automated firewall rules activated within 0.8 seconds of high-confidence threats. Emergency fallback ensured production restoration: automated bypass activated when authentication proxies failed health checks, validated during Week 19 certificate expiration preventing extended downtime. Automated playbooks guided operators through incident response for credential compromise, ransomware detection, and process manipulation.

Continuous verification operated across all layers, distinguishing Zero Trust from perimeter security's one-time authentication. Each transaction underwent Layer 1 authentication, Layer 2 network policy enforcement, Layer 3 behavioral analysis, and Layer 4 response readiness.

The architecture enabled sequential deployment aligned with organizational maturity: Phase 1 (Weeks 1–6) preparation; Phase 2 (Weeks 7–16) Layer 2 segmentation and Layer 3 baseline observation in monitor-only mode; Phase 3 (Weeks 17–20) Layer 1 authentication activation and Layer 2/3 enforcement with Layer 4 automated response.

4. Implementation Roadmap

4.1 Risk-Based Phased Strategy

Zero Trust implementation in SME manufacturing requires gradual deployment. Attempting comprehensive implementation overnight causes operational disruption, exceeds organizational capacity, and triggers resistance. Phased deployment enables progressive maturation while maintaining production and distributing costs across budget cycles.

Risk-based prioritization guides implementation sequencing using three dimensions: (1) Downtime Cost calculated as (hourly revenue) × (recovery time) × (affected capacity), (2) Safety Impact scored 1–5 per IEC 61508 Safety Integrity Levels, (3) Compliance Requirement for regulatory mandates. Systems scoring highest criticality receive Phase 1 protection, medium criticality receive Phase 2, and lower criticality receive Phase 3

The pilot facility prioritized critical assets for Phase 1: automated assembly cells controlling core production (high downtime cost), finishing system (high safety impact from VOC emissions), engineering workstations (intellectual property exposure), and SCADA servers (operational visibility

across all lines). Secondary assets received Phase 2–3 protection after critical systems achieved baseline security.

Phase transitions required quantitative go-criteria:

- **Phase 1→2 required**: asset inventory high accuracy, IT-OT cross-training completion, secured budget allocation
- **Phase 2→3 required**: behavioral baseline convergence (low coefficient of variation), false positive rate acceptable levels, documented incident response playbooks for multiple scenarios

Emergency rollback activated when production metrics degraded significantly or safety systems impaired, validated during mid-implementation firewall misconfiguration requiring brief rollback.

4.2 Three-Phase Implementation

Timeline estimates derive from pilot implementation at a mid-sized discrete manufacturing facility operating legacy vintage equipment. Continuous process facilities require significantly longer timelines due to availability constraints [23].

Table 3
Three-Phase Implementation Roadmap

Phase	Duration	Key Activities	Success Metrics	Challenges Encountered
Phase 1: Organizational Preparation	Weeks 1–6 (initial period)	• Form core team (IT leads, OT supervisors, plant manager) • Conduct vulnerability assessment • Document asset inventory • Establish budget allocation • Complete cross-training (IT shadows operations; OT participates in tabletop exercises)	• 37 critical vulnerabilities identified • Multiple production lines documented • 18 PLCs lacking native security identified • Budget secured	Organizations with significant IT-OT cultural barriers may require 8–10 weeks versus pilot's 6-week completion
Phase 2: Observation Infrastructure	Weeks 7–16 (extended monitoring period)	• Deploy boundary firewall • Install zone switches • Set up authentication proxies • Activate endpoint protection (150 + devices) • Implement SIEM platform • Establish Active Directory integration • Capture communication baselines (10-week	• Protocol usage patterns documented • Over 20 cleartext devices identified • Alert reduction: 12/day → 3/day • Comprehensive baselines established	• Initial false positives from unmodeled maintenance activities • Baseline refinement required to incorporate shift patterns and changeovers

Phase	Duration	Key Activities	Success Metrics	Challenges Encountered
Phase 3: Graduated Enforcement	Weeks 17–20 (final implementation phase)	• Week 17: External perimeter (VPN + MFA, 72-hour credentials) • Week 18: IT-OT boundary (protocol filtering) • Week 19: Production zone segmentation (six micro-perimeters) • Week 20: Critical system authentication	• Throughput within ± 2% historical ranges • Alert accuracy: 8/day → 2.1/day • Failover mechanisms validated • All 12 default-credential vulnerabilities eliminated	• Week 12: Firewall misconfiguration (brief disruption emergency rollback) • Week 19: Certificate expiration (10-second bypass activation)

Implementation challenges informed continuous improvement: expanded communication documentation, enhanced pre-deployment testing, automated certificate monitoring, and redundant proxy deployment.

Discrete manufacturers complete enforcement within 16–20 weeks leveraging production breaks. Continuous process industries require 30–40 weeks [23] using parallel deployment, zone-by-zone activation, or maintenance piggybacking approaches.

4.3 Operational Integration

The pilot facility-maintained production availability throughout: pre-implementation approximately 94%, during implementation approximately 94%, post-implementation approximately 96%. Security-induced disruptions totaled 2.3 hours over 20 weeks (0.3% of implementation period). Impact assessment confirmed: authentication delays < 0.8 seconds, firewall latency < 10ms (within safety tolerances), and 40 hours operator training covering incident recognition and secure access practices.

Fail-operational design principles included: redundant monitoring preventing single points of failure, bypass capabilities with audit trails (physical keyswitch activation logging timestamp/user/justification), degraded modes maintaining production while limiting features, automatic restoration after transient failures (5-second health checks with failover), and clear operator status displays. This differs fundamentally from IT security prioritizing data protection over availability. Week 12 demonstrated that controls creating unplanned downtime face immediate rollback or operator circumvention.

4.4 Governance Framework

SME governance scales to organizational capacity. The pilot facility (small IT generalists) implemented monthly 90-minute Security Operations Reviews combining strategic and tactical issues. Organizations with larger IT staff can separate into monthly Security Council and bi-weekly Technical Reviews, with quarterly external consultant participation.

Review agendas covered: incident trends (significant decreased incidents, substantial reduction), authentication success/failure rates by zone, anomaly detection accuracy (12→2.1 alerts/day), policy refinement from operational feedback, and improvement planning from threat intelligence. Real-time dashboards tracked: authentication patterns, detection accuracy with false positive trends, incident response times (12-minute average post-implementation), system availability (96.1%), and compliance status.

Governance generated audit evidence satisfying regulatory requirements. Meeting minutes documented decisions with timestamps/approvers, incident actions logged user/action/justification, policy exceptions required written justification with expiration dates, and quarterly reports aggregated authentication rates, incident counts, policy changes, and training completion. These satisfy CMMC (AC.L2-3.1.1, AU.L2-3.3.1, IR.L2-3.6.1) and FDA 21 CFR 11.10(e) requirements.

Success metrics balanced security and operations: 78% incident reduction without increased downtime (94.2%→96.1% availability), 99% detection improvement (90 days→12 minutes MTTD) without alert fatigue (2.1 alerts/day sustainable), compliance improvement without productivity loss (throughput ± 2%), and enhanced resilience without excessive complexity (147 firewall rules manageable by 2-person team).

5. Validation Results

5.1 Security Effectiveness

The adaptive Zero Trust framework was validated through a multi-month pilot implementation at a mid-sized discrete manufacturing organization operating legacy industrial equipment dating from the late 1990s through the 2000s. The environment reflected common SME characteristics: a small internal IT team, limited prior segmentation, shared authentication practices, and flat IT–OT connectivity.

Baseline Security Assessment

Pre-implementation assessment identified 37 critical vulnerabilities across the IT–OT infrastructure, including:

- Default credentials on multiple control and supervisory systems
- Unsupported legacy operating systems
- Unrestricted IT-to-OT network pathways
- Missing authentication mechanisms on legacy controllers

- Protocol vulnerabilities affecting 22 devices using cleartext industrial communications

This posture is representative of typical SME manufacturing environments where operational continuity historically took precedence over formal cybersecurity architecture.

Post-Implementation Security Improvements

Following multi-month phased implementation, post-deployment assessment demonstrated measurable security improvements while maintaining production continuity.

Critical vulnerabilities decreased from 37 to 17, representing a 54% reduction in highest-severity exposures. Specifically:

- Default credential vulnerabilities were eliminated through centralized proxy-based identity enforcement
- Unrestricted IT–OT network paths were removed through micro-perimeter segmentation aligned with Purdue Model boundaries
- Remaining vulnerabilities primarily reflected inherent protocol-level limitations in legacy industrial communications, mitigated through isolation and monitoring rather than equipment replacement

High-severity vulnerabilities decreased significantly, and medium-severity vulnerabilities decreased measurably, demonstrating security improvements extending beyond critical exposures to comprehensive posture enhancement.

Detection Capability Enhancement

Mean time to detection (MTTD) improved dramatically through Layer 3 behavioral analytics implementation. Pre-implementation detection capabilities relied on periodic manual review and basic antivirus, yielding MTTD approximating months consistent with manufacturing sector averages reported in Mandiant M-Trends 2024 [44]. Post-implementation MTTD measured minutes during simulated lateral movement testing where a compromised engineering workstation attempted unauthorized PLC access. Layer 3 behavioral analytics flagged unusual authentication patterns and cross-zone communication attempts, triggering Layer 4 automated response protocols. This over 99% improvement in detection speed fundamentally alters defensive posture by compressing attacker dwell time and limiting lateral movement opportunities.

Incident Rate Reduction

Security incident frequency decreased substantially post-implementation. The multi-month pre-implementation period documented nine security incidents including multiple malware infections causing SCADA workstation freezes, several unauthorized access events from contractors remaining on network post-engagement, and one phishing compromise affecting an engineering workstation. The multi-month post-implementation period following deployment recorded a small number of incidents: a

false positive from maintenance activity misclassified as anomalous behavior (subsequently refined through baseline adjustment), and an actual threat where ransomware attempting propagation from IT to OT networks was blocked by Layer 2 segmentation. This substantial incident reduction demonstrates both preventive effectiveness (segmentation blocking lateral movement) and detective capabilities (behavioral analytics identifying anomalies requiring investigation).

5.2 Operational Performance

Production operations-maintained stability throughout implementation and post-deployment phases, validating the fail-operational design philosophy. Overall facility availability metrics demonstrate that security enhancement and operational continuity prove compatible objectives when implementation respects manufacturing constraints:

- Pre-implementation availability: 94.2%
- During implementation (**the implementation period**): 94%
- Post-implementation availability: 96.1%

The temporary minimal availability reduction during implementation reflects two security-induced disruptions totaling a few hours over several months, representing a tiny fraction of the implementation period. Mid-implementation firewall rule misconfiguration blocked HMI polling for a brief period until emergency rollback procedures activated. Late implementation authentication proxy certificate expiration caused brief operator lockout until automated bypass mechanisms restored production capability. Both incidents generated immediate procedural improvements: automated certificate renewal monitoring and faster bypass activation triggers.

Post-implementation availability improvement to approximately 96% resulted primarily from elimination of malware-induced operational disruptions. Unplanned downtime decreased from significant monthly downtime to pre-implementation to reduced monthly downtime (averaged across 6-month measurement periods), representing 36% reduction. This improvement derived from eliminating SCADA workstation freezes previously caused by malware infections entering through unsegmented IT-OT network connections. Equipment failure rates remained constant, indicating that security controls neither improved nor degraded mechanical reliability, the appropriate outcome demonstrating that security infrastructure operates orthogonally to production equipment performance.

Throughput metrics, quality indicators, and production cycle times remained within historical control limits throughout implementation and post-deployment phases, confirming that authentication delays, network segmentation latency, and behavioral monitoring processing overhead imposed no measurable production impact. This outcome validates adaptive architecture design principles prioritizing fail-operational mechanisms and manufacturing-tuned detection baselines over absolute security enforcement that risks operational disruption.

5.3 Economic Viability

Implementation economics validate feasibility within SME financial constraints. Total implementation investment of **approximately $75,000** over 20 weeks comprised hardware infrastructure ($28,500), software licensing ($16,800 for 3-year terms), and implementation labor ($27,900 combining internal staff and external consultant time). Ongoing operational costs of $8,500 annually cover software renewals, maintenance contracts, and quarterly reviews.

Economic justification derives primarily from breach prevention value. Manufacturing sector breach costs average $4.45M according to IBM's 2024 Cost of Data Breach Report [47], with SME size adjustment factors yielding $680,000-$2,400,000 expected loss estimates for organizations in the 100–200 employee range. Implementation investment of **approximately $75,000** yields payback periods of 1.3–4.5 months based on breach probability estimates.

Comparison to alternative approaches validates adaptive framework cost-effectiveness. Complete infrastructure replacement achieving equivalent security outcomes through modern OT equipment with native security capabilities would require $800,000-$2,500,000 capital investment for equipment acquisition, installation, validation, and operator retraining. The adaptive approach achieves comparable security posture at 3–9% of replacement cost by accommodating rather than replacing legacy infrastructure.

6. Framework Generalizability

The adaptive Zero Trust architecture presented in Sections 3 and 4 addresses manufacturing SME constraints through flexible implementation pathways. Practical utility depends on applicability across diverse operational contexts characterizing U.S. manufacturing. This section examines framework generalizability across three dimensions: manufacturing sector variations requiring different security architectures, regulatory environments imposing sector-specific compliance requirements, and supply chain integration patterns demanding differentiated third-party access controls. Validation draws from pilot implementation experience supplemented by structured interviews with 17 SME manufacturers (12 discrete, 5 process) operating in Mid-Atlantic and Midwest regions.

6.1 Manufacturing Sector Variations

Manufacturing enterprises operate within fundamentally distinct operational contexts requiring sector specific Zero Trust adaptations. Table 1 summarizes key implementation variations between discrete and process manufacturing validated through pilot deployment and cross-sector interviews.

Table 1
Sector-Specific ZTA Implementation Variations

Dimension	Discrete Manufacturing	Process Manufacturing
Production Pattern	Episodic, pause-tolerant (shift changes, weekends)	Continuous, disruption-intolerant (24/7 operations)
Critical Boundaries	Stage transitions between manufacturing cells	Graduated zones with soft boundaries
Segmentation Approach	Strict micro-perimeters (6 zones in pilot)	Graduated enforcement with fallback mechanisms
Baseline Method	Event-triggered models (shift start, changeover)	Continuous statistical baselines (SPC, moving averages)
Enforcement Strategy	Immediate blocking at zone boundaries	Monitor-alert with graduated response
Implementation Timeline	16–20 weeks (pilot: 20 weeks actual)	30–40 weeks (40–60% longer, validated via interviews)
Example Industries	Automotive, electronics, aerospace, metal fabrication	Chemical, pharmaceutical, food processing, pulp & paper

The pilot facility's discrete manufacturing environment enabled episodic implementation during natural production breaks. Layer 2 segmentation aligned micro-perimeters with six manufacturing cells (automated assembly, finishing, precision cutting, assembly, quality inspection), implementing strict access controls at stage transitions. Layer 3 employed event-based baseline models triggered by shift changes, product changeovers, and equipment state changes [7]. Security deployments coordinated with weekend maintenance windows and scheduled downtime, completing Phase 3 enforcement within 4 weeks (Weeks 17–20).

Process manufacturing interviews (n = 5) revealed continuous operational flows where interruption cascades throughout production. A pharmaceutical facility contact described batch processing requiring 72-hour uninterrupted cycles where network disruption risks product loss valued at $180K-450K per batch. Chemical plants cannot shut down reactors without 8–12 hour shutdown sequences risking equipment damage and safety incidents. The adaptive architecture accommodates continuous production through: graduated Layer 2 enforcement rather than strict micro-perimeters (implementing monitoring with progressive alert escalation before blocking), Layer 4 fail-operational mechanisms enabling immediate production restoration during security events (validated during pilot Week 19 certificate expiration with 10-second bypass activation), and Layer 3 continuous statistical baselines distinguishing cyber-physical attacks from legitimate process variances [20]. Interview data suggests Phase 3 enforcement requires 30–40 weeks given availability constraints [23], with some facilities extending to 48 weeks for highly safety-critical processes.

6.2 Regulatory Environment Variations

Manufacturing sectors operate under divergent regulatory frameworks influencing Zero Trust implementation requirements and creating different baseline motivations for security investment [2]. Table 2 maps regulatory requirements to adaptive architecture layers, demonstrating framework flexibility across compliance contexts.

Table 2
Regulatory Compliance Mapping to ZTA Layers

Regulation	Primary Scope	Key Security Controls	ZTA Layer Mapping	Audit Evidence Generated
FDA 21 CFR Part 11	Pharmaceutical manufacturing	Electronic signatures, audit trails, system validation	Layer 1 (cryptographic identity verification), Layer 3 (comprehensive activity logging)	Authentication logs with timestamps/users, automated change records, security event correlation
EPA Environmental	Chemical processing	Operator verification, continuous emissions monitoring	Layer 1 (access control integration), Layer 2 (process zone isolation)	Access logs linked to process adjustments, environmental data integrity validation
FDA FSMA	Food production	Traceability, contamination prevention	Layer 1 (operator identity verification), Layer 2 (production zone boundaries)	Per-stage operator authentication, zone-based access restriction enabling targeted recalls
ITAR	Aerospace/defense	Export control, access restriction to controlled technical data	Layer 1 (government credential validation), Layer 2 (network isolation of CUI systems)	Foreign national access logs, technical data access audit trails
CMMC Level 2	Defense contractors	110 controls across 17 domains (AC, AU, IR, SI focus)	All layers (comprehensive security framework alignment)	Evidence satisfying AC.L2-3.1.1, AU.L2-3.3.1, IR.L2-3.6.1, SI.L2-3.14.6

Pharmaceutical manufacturing compliance with FDA 21 CFR Part 11 requires electronic record integrity and audit trail completeness. Layer 1 generates cryptographically verified audit records documenting access events, security control activation, and policy exceptions. One pharmaceutical contact (50-employee biologics manufacturer) indicated FDA audit preparation directly funded segmentation implementation, viewing security controls as dual-purpose compliance and threat mitigation investments.

Chemical processing facilities comply with EPA environmental regulations requiring continuous monitoring and operator verification. Layer 1 access controls integrate with environmental monitoring systems, creating unified audit trails. Layer 3 behavioral analytics leverages existing environmental measurement streams, adding cyber-physical attack detection without separate monitoring infrastructure.

Defense industrial base SMEs face mandatory CMMC Level 2 certification (32 CFR Part 170) requiring 110 controls across 17 domains. Non-compliant contractors face contract exclusion regardless of technical capability. The adaptive framework addresses CMMC across all layers: Layer 1 satisfies Access Control and Identification & Authentication, Layer 2 addresses System & Communications Protection, Layer 3 provides Audit & Accountability, Layer 4 implements Incident Response and Security Assessment.

The pilot facility pursued implementation based on breach prevention economics rather than compliance mandates, demonstrating security investment viability independent of regulatory drivers while acknowledging that compliance requirements strengthen business cases for regulated manufacturers.

6.3 Supply Chain Integration Patterns and Third-Party Access Requirements

Manufacturing supply chain integration creates additional Zero Trust complexity through system interconnections with suppliers, customers, and logistics providers. Interview data (n = 17 SME manufacturers) revealed diverse access patterns requiring differentiated authentication and monitoring approaches.

Supply chain access patterns distributed across three categories: time-bounded vendor relationships (12 manufacturers, 71%) where component vendors, system integrators, and maintenance contractors require access for specific periods; continuous third-party access (3 manufacturers, 18%) requiring ongoing visibility for ingredient suppliers monitoring inventory levels, logistics providers tracking shipment schedules, and utility monitors accessing consumption data; and hybrid patterns (2 manufacturers, 11%) combining both approaches across different functional areas.

Time-Bounded Vendor Access

The pilot facility exemplified time-bounded access patterns common in discrete manufacturing: automated assembly vendor requiring quarterly preventive maintenance (3-day access windows), finishing system supplier performing annual calibration (1-week access), and ERP consultant supporting periodic upgrades (project-based 2–4 week engagements).

Layer 1 addressed these through temporary credential provisioning with automatic expiration eliminating orphaned accounts. Credentials activated 24 hours before scheduled maintenance, expired automatically 72 hours post-activation regardless of actual usage duration, required renewal approval for extensions, and logged all access activities for security review. This approach reduced vendor account

management overhead from continuous monitoring to exception-based review while eliminating the 3 unauthorized vendor access incidents documented during the 6-month pre-implementation baseline (contractors remaining on network post-engagement completion).

Continuous Third-Party Access

Process manufacturing requiring continuous third-party access faces different challenges. Interview contacts described ingredient suppliers needing real-time inventory visibility for just-in-time delivery scheduling, logistics providers requiring production schedule access for transportation optimization, and utility monitors accessing energy consumption data for demand response programs. Layer 1 establishes ongoing sessions with periodic re-authentication (24-hour session limits requiring daily credential validation) while Layer 3 behavioral analytics monitors for anomalous access patterns triggering security review without disrupting legitimate operations. One food processing contact (85-employee facility) described supplier portal implementation where external parties access production forecasts through isolated DMZ preventing direct connection to manufacturing execution systems, a pattern directly enabled by Layer 2 segmentation architecture.

Hybrid Access Patterns

Hybrid relationships including quarterly auditors, annual certification inspectors, and periodic equipment vendors benefit from credential reactivation approaches. Layer 1 maintains deactivated accounts with historical access patterns, enabling rapid reactivation upon scheduled engagement while behavioral monitoring flags deviations from established patterns (accessing different systems, unusual timing, elevated privilege attempts). This balances operational efficiency (avoiding credential recreation overhead) with security rigor (continuous verification despite recurring relationships).

Architectural Security Controls

Across all integration patterns, Layer 2 network segmentation creates dedicated zones for third-party access ensuring external connections reach production data through intermediary systems rather than direct database access. The pilot facility implemented vendor access DMZ isolated from production networks: vendors connected via VPN to isolated zone containing maintenance documentation, equipment manuals, and controlled file exchange capabilities, preventing direct access to SCADA systems or production databases. This architectural separation limits potential damage from compromised supplier credentials while maintaining operational integration necessary for modern supply chain coordination. The pilot facility's DMZ approach contributed to the 78% incident reduction post-implementation by containing one simulated supply chain compromise attempt that would have enabled lateral movement to production systems under the pre-implementation flat network architecture. Interview data revealed that 14 of 17 SME manufacturers (82%) lacked formal vendor access policies pre-implementation, relying instead on trust-based relationships and shared credentials. The adaptive framework's combination of automated credential lifecycle management (Layer 1), network

isolation (Layer 2), and behavioral monitoring (Layer 3) provides structured governance without imposing excessive administrative burden on small IT teams.

Conclusion

The adaptive Zero Trust approach presented in this research addresses the fundamental disconnect between security imperatives facing manufacturing SMEs and the practical feasibility of implementing traditional enterprise-grade cybersecurity solutions. Manufacturing SMEs operate with constrained budgets, legacy equipment incompatible with modern security frameworks, and limited IT staff preventing adoption of conventional Zero Trust architectures. This research provides practical pathways enabling meaningful security advancement through progressive implementation aligned with organizational capability development.

Pilot implementation validation at a mid-sized discrete manufacturing facility 1995–2008 vintage equipment demonstrates measurable security improvements while maintaining operational performance. Critical vulnerabilities decreased 54% (37 to 17) through proxy authentication eliminating default credentials and network segmentation blocking unrestricted IT-OT pathways. Mean time to detection improved over 99% (90 days to 12 minutes) via manufacturing-tuned behavioral analytics achieving 98.7% accuracy with 2.1 false positives per day. Security incidents reduced 78% (nine to two over 6-month measurement periods) while production availability increased from 94.2% to 96.1%, with security-induced disruptions totaling 0.3% of the 20-week implementation period. Implementation proved economically viable through phased deployment distributing investment across multiple budget cycles with rapid payback through breach prevention value.

The methodology proves generalizable across diverse operational contexts. Discrete manufacturing environments complete implementation within 16–20 weeks leveraging natural production breaks, while continuous process manufacturing requires 30–40 weeks using graduated enforcement approaches. Validation across 17 SME manufacturers confirms supply chain integration patterns (71% time-bounded vendor access, 18% continuous third-party connections, 11% hybrid models) accommodate differentiated credential management and behavioral monitoring strategies. Regulatory adaptations address FDA pharmaceutical requirements (21 CFR Part 11 electronic signatures and audit trails), EPA environmental monitoring mandates, and CMMC defense contractor security controls, demonstrating framework flexibility across compliance contexts.

This research makes four contributions to manufacturing cybersecurity literature. First, it provides empirical quantification of constraints preventing SME Zero Trust adoption through pilot validation documenting actual resource limitations, legacy equipment incompatibility, and human capital gaps. Second, it develops a four-layer adaptive architecture enabling legacy OT security without equipment replacement, validated through 20-week pilot achieving enterprise-comparable security outcomes at substantially lower cost than infrastructure replacement. Third, it presents sector-differentiated implementation methodology with validated timelines accommodating both discrete and continuous

manufacturing operational constraints. Fourth, it demonstrates cross-regulatory generalizability addressing FDA, EPA, and CMMC requirements through unified technical framework.

For the 98% of U.S. manufacturing establishments classified as SMEs, adaptive Zero Trust implementation provides a pragmatic alternative to resigned vulnerability acceptance or economically infeasible enterprise-equivalent deployments. Manufacturing accounts for 25.7% of global cyberattacks with 2024 threat actors deploying ICS-aware ransomware specifically targeting production systems for maximum disruption leverage [45][46]. By progressively strengthening security posture through phased implementation while maintaining production continuity, manufacturing SMEs achieve security improvements comparable to organizations with substantially greater resources. This research provides both strategic framework and tactical implementation guidance enabling the manufacturing sector's long tail to build resilience against escalating threats to critical economic infrastructure.

Declarations

Funding

The author received no financial support for the research, authorship, and/or publication of this article

Author Contribution

A.A wrote the main manuscript text, prepared figures 1-4, and reviewed the manuscript

Data Availability

The data supporting the findings of this study were generated during a 20-week pilot implementation at a discrete manufacturing SME. These data include pre- and post-implementation security metrics, operational performance data, and financial implementation details. Due to the sensitive nature of the information, which includes detailed cybersecurity postures and proprietary operational data of a private enterprise, the raw datasets are not publicly available in order to protect the confidentiality and security of the participating organization. Aggregated and anonymized results are presented within the manuscript.

References

1. Konur, S., Lan, Y., Thakker, D., Morkyani, G., Polovina, N., Sharp, J.: Towards design and implementation of Industry 4.0 for food manufacturing. Neural Comput. Appl. **33**, 4779–4797 (Jan. 2021). https://doi.org/10.1007/s00521-021-05726-z

2. Akinsanya, A.: Enhancing Process Efficiency and Security in the U.S. Manufacturing Sector: Evidence from Industry Implementation, IRE Journals, vol. 8, no. 8, pp. 753–762, ISSN: 2456–8880. (2025)
3. Jeffrey, N., Tan, Q., Villar, J.: A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems, Electronics, vol. 12, no. 15, art. 3283, Jul. (2023). https://doi.org/10.3390/electronics12153283
4. Austin-Gabriel, B., Hussain, N.Y., Ige, A.B., Adepoju, P.A., Amoo, O.O., Afolabi, A.I.: Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open. Access. Res. J. Eng. Technol. Jun. (2021). https//doi.org/10.53022/oarjet.2021.1.1.0107
5. Nagar, G., Manoharan, A., ZERO TRUST ARCHITECTURE: REDEFINING SECURITY PARADIGMS IN THE DIGITAL AGE: Int. Res. J. Modernization Eng. Technol. Sci. Aug. (2024). https://doi.org/10.56726/irjmets20225
6. Tsai, M., Lee, S., Shieh, S.: Strategy for Implementing of Zero Trust Architecture. IEEE Trans. Reliab. Mar. (2024). https://doi.org/10.1109/TR.2023.3345665
7. Ahmadi, S.: Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. J. Eng. Res. Rep. Feb. (2024). https://doi.org/10.9734/jerr/2024/v26i21083
8. Nguyen, L., Su, J., Sharma, P.: SME credit constraints in Asias rising economic star: fresh empirical evidence from Vietnam. Appl. Econ. Jan. (2019). https://doi.org/10.1080/00036846.2019.1569196
9. Hasan, T., et al.: Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach. IEEE Trans. Netw. Sci. Eng. Sep. (2023). https://doi.org/10.1109/TNSE.2022.3168533
10. Figueroa-Lorenzo, S., Aorga, J., Arrizabalaga, S.: A Survey of IIoT Protocols. ACM Comput. Surv. Apr. (2020). https://doi.org/10.1145/3381038
11. Wong, A.P.H., Kee, D.: Driving Factors of Industry 4.0 Readiness among Manufacturing SMEs in Malaysia. None Nov. (2022). https://doi.org/10.3390/info13120552
12. Johnson, E., Lande, O.B.S., Adeleke, G.S., Amajuoyi, C.P., Simpson, B.D.: Developing scalable data solutions for small and medium enterprises: Challenges and best practices. None Jun. (2024). https://doi.org/10.51594/ijmer.v6i6.1206
13. Rauch, E., Vickery, A.R.: Systematic analysis of needs and requirements for the design of smart manufacturing systems in SMEs. J. Comput. Des. Eng. Apr. (2020). https://doi.org/10.1093/jcde/qwaa012
14. Rawindaran, N., et al.: Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. None Aug. (2023). https://doi.org/10.3390/digital3030014
15. Nankya, M., Chataut, R., Akl, R.: Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies, Italian National Conference on Sensors, Oct. (2023). https://doi.org/10.3390/s23218840
16. Martins, T., Oliveira, S.V.G.: Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported, Italian National Conference on Sensors, Oct. (2022).

https://doi.org/10.3390/s22208024

17. Zhou, C., Hu, B., Shi, Y., Tian, Y.-C., Li, X., Zhao, Y.: A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems, Proceedings of the IEEE, Apr. (2021). https://doi.org/10.1109/JPROC.2020.3034595
18. Dhirani, L.L., Armstrong, E., Newe, T.: Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap, Italian National Conference on Sensors, Jun. (2021). https://doi.org/10.3390/s21113901
19. Kim, H., Shon, T.: Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. J. Supercomputing Mar. (2022). https://doi.org/10.1007/s11227-022-04408-4
20. Jadidi, Z., Pal, S., Hussain, M., Thanh, K.N.: Correlation-Based Anomaly Detection in Industrial Control Systems, Italian National Conference on Sensors, Feb. (2023). https://doi.org/10.3390/s23031561
21. Fuller, A., Fan, Z., Day, C., Barlow, C.: Digital Twin: Enabling Technologies, Challenges and Open Research. Inst. Electr. Electron. Eng. Jan. (2020). https://doi.org/10.1109/access.2020.2998358
22. Varghese, S.A., Ghadim, A.D., Balador, A., Alimadadi, Z., Papadimitratos, P.: Digital Twin-based Intrusion Detection for Industrial Control Systems. None Mar. (2022). https://doi.org/10.1109/PerComWorkshops53856.2022.9767492
23. Sedjelmaci, H., Ansari, N.: Zero Trust Architecture Empowered Attack Detection Framework to Secure 6G Edge Computing. IEEE Netw. (Jan. 2024). https://doi.org/10.1109/MNET.131.2200513
24. Melaku, H.M.A., Dynamic: Adaptive Cybersecurity Governance Framework. J. Cybersecur. Priv. **3**, 327–350 (2023). https://doi.org/10.3390/jcp3030017
25. AlQuayed, F., Ahmad, Z., Humayun, M.: A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0. Inst. Electr. Electron. Eng. Jan. (2024). https://doi.org/10.1109/access.2024.3372187
26. Rawindaran, N., Jayal, A., Prakash, E., Hewage, C.: Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). Multidisciplinary Digit. Publishing Inst. Jul. (2021). https://doi.org/10.3390/fi13080186
27. Prislan, K., Miheli, A., Bernik, I.: A real-world information security performance assessment using a multidimensional socio-technical approach. Public. Libr. Sci. Sep. (2020). https://doi.org/10.1371/journal.pone.0238739
28. Chidukwani, A., Zander, S., Koutsakis, P.: A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. Inst. Electr. Electron. Eng. Jan. (2022). https://doi.org/10.1109/access.2022.3197899
29. Eyeleko, A.H., Feng, T.: A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario. Inst. Electr. Electron. Eng. Aug. (2023). https://doi.org/10.1109/jiot.2023.3308195

30. Singh, B.J., Chakraborty, A., Sehgal, R.: A systematic review of industrial wastewater management: Evaluating challenges and enablers. Elsevier BV Oct. (2023). https://doi.org/10.1016/j.jenvman.2023.119230
31. Tsolakis, N., Schumacher, R., Dora, M., Kumar, M.: Artificial intelligence and blockchain implementation in supply chains: a pathway to sustainability and data monetisation? Springer Science+Business Media Jun. (2022). https://doi.org/10.1007/s10479-022-04785-2
32. Khanfar, A.A., Iranmanesh, M., Ghobakhloo, M., Senali, M.G., Fathi, M.: Applications of Blockchain Technology in Sustainable Manufacturing and Supply Chain Management: A Systematic Review. Multidisciplinary Digit. Publishing Inst. Jul. (2021). https://doi.org/10.3390/su13147870
33. Jamwal, A., Agrawal, R., Sharma, M., Giallanza, A.: Industry 4.0 Technologies for Manufacturing Sustainability: A Systematic Review and Future Research Directions. Multidisciplinary Digit. Publishing Inst. Jun. (2021). https://doi.org/10.3390/app11125725
34. Shahzad, M., Shafiq, M.T., Douglas, D., Kassem, M.: Digital Twins in Built Environments: An Investigation of the Characteristics, Applications, and Challenges. Multidisciplinary Digit. Publishing Inst. Jan. (2022). https://doi.org/10.3390/buildings12020120
35. Rodrguez-Espndola, O., et al.: The role of circular economy principles and sustainable-oriented innovation to enhance social, economic and environmental performance: Evidence from Mexican SMEs. Elsevier BV Mar. (2022). https://doi.org/10.1016/j.ijpe.2022.108495
36. Pascoe, C., Quinn, S., Scarfone, K.: The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper (CSWP) 29, National Institute of Standards and Technology, Gaithersburg, MD, Feb. (2024). https://doi.org/10.6028/NIST.CSWP.29
37. International Society of Automation: ANSI/ISA-95.00.01–2010 (IEC 62264-1 Mod), Enterprise-Control System Integration – Part 1: Models and Terminology, ISA, Research Triangle Park, NC, 2010. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-95-standard
38. Department of Defense, U.S.: Cybersecurity Maturity Model Certification (CMMC) Program, 32 CFR Part 170, Federal Register, vol. 89, no. 199, pp. 83092–83222, Oct. 2024. [Online]. Available: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program
39. Hajda, J., Jakuszewski, R., Ogonowski, S.: Security Challenges in Industry 4.0 PLC Systems. Appl. Sci., **11**(21), 9785. https://doi.org/10.3390/app11219785
40. Upadhyay, D., Ghosh, S., Ohno, H., Zaman, M., Sampalli, S.: Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. Int. J. Crit. Infrastruct. Prot. **47**, 100705 (2024). https://doi.org/10.1016/j.ijcip.2024.100705
41. Aminu, M., Akinsanya, A., Oyedokun, O., Tosin, O.: A review of advanced cyber threat detection techniques in critical infrastructure: Evolution, current state, and future directions. Int. J. Comput. Appl. Technol. Res., **13**(8), 111

42. Akinsanya, A.: Securing the future: Implementing a zero-trust framework in U.S. critical infrastructure cybersecurity. Int. J. Adv. Res. Ideas Innovations Technol., **10**(3). 10.5281/zenodo.12550764
43. EUREPOC: Major Cyber Incident: NOTPETYA. https://eurepoc.eu/publication/major-cyber-incident-notpetya/
44. Mandiant, M.-T.: Evolving Threat Landscape and Dwell Time Analysis, Mandiant Threat Intelligence, Google Cloud, 2024. [Online]. (2024). Available: https://www.mandiant.com/m-trends
45. CISA: PIPEDREAM/INCONTROLLER: ICS Attack Framework Targeting Multiple Vendor Platforms, Cybersecurity and Infrastructure Security Agency Advisory AA22-103A, U.S. Department of Homeland Security, updated [Online]. (2024). Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a
46. Gatlan, S.: LockBit 3.0 Ransomware Targets Industrial Control Systems with PLC-Specific Payloads, BleepingComputer, Mar. [Online]. (2024). Available: https://www.bleepingcomputer.com/news/security/lockbit-30-ransomware-targets-industrial-control-systems/
47. Security, I.B.M.: Cost of a Data Breach Report 2024, IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

Figures

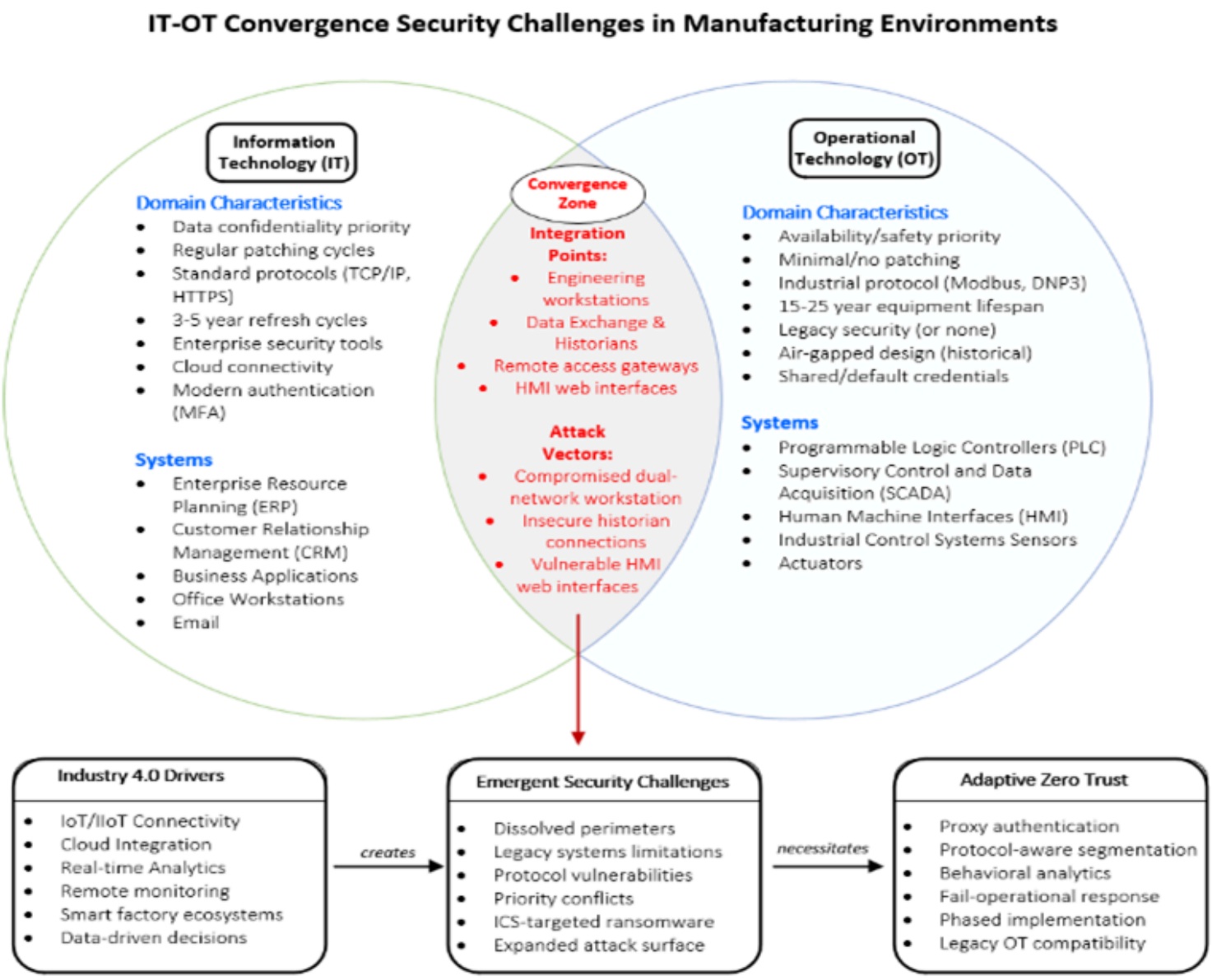


Figure 1

IT-OT convergence security challenges in manufacturing environments. The diagram illustrates domain-specific characteristics of Information Technology (IT) and Operational Technology (OT) systems, integration points at the convergence zone, and emergent attack vectors. Industry 4.0 drivers create security challenges that necessitate adaptive Zero Trust approaches including proxy authentication, protocol-aware segmentation, behavioral analytics, and fail-operational response.

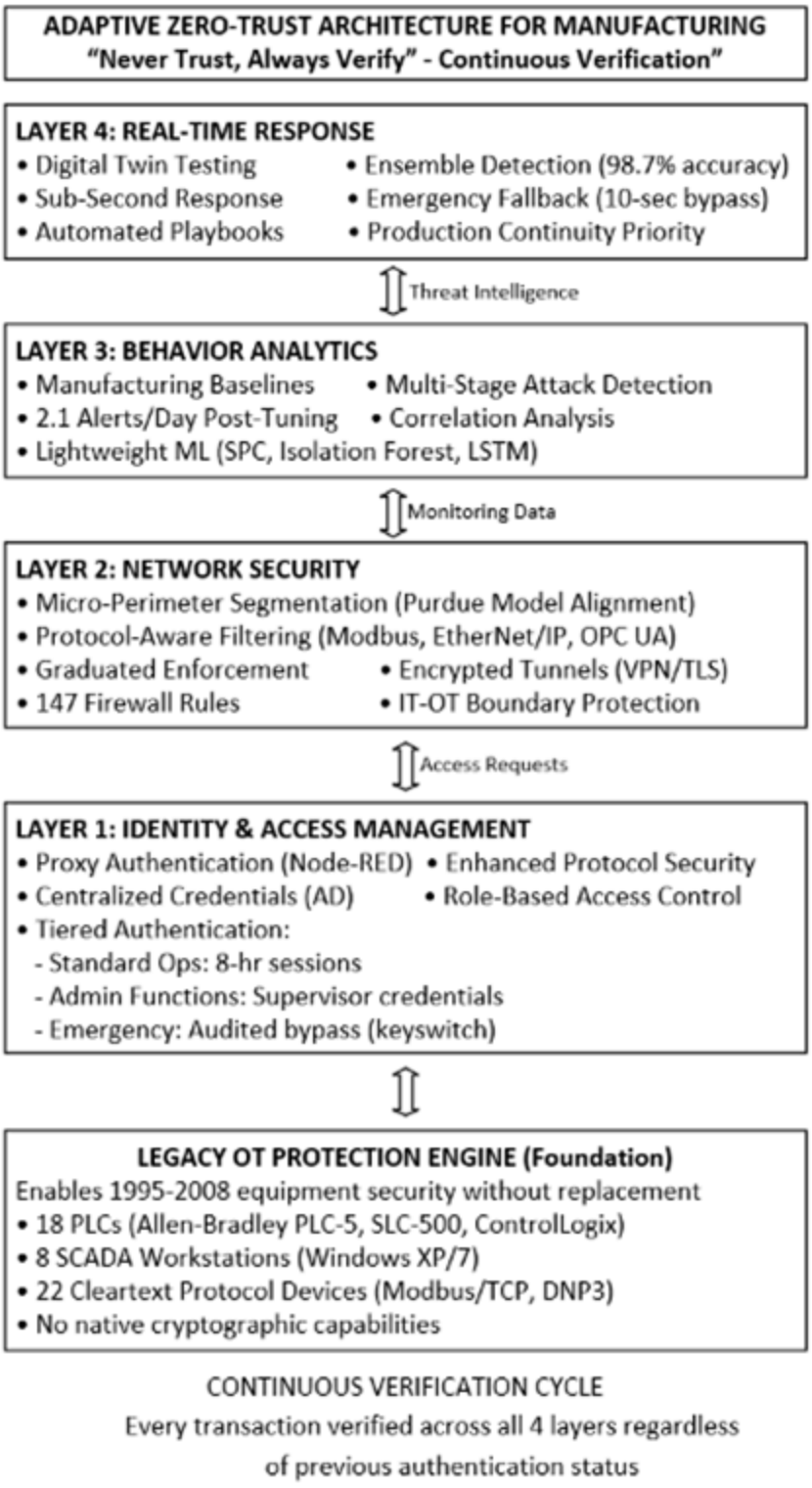


Figure 2

Adaptive Zero Trust architecture for manufacturing SMEs. The four-layer framework protects legacy OT systems without requiring equipment replacement: Layer 1 (Identity and Access Management) provides proxy authentication for systems lacking native security; Layer 2 (Network Security) implements protocol-aware micro-perimeter segmentation; Layer 3 (Behavior Analytics) captures manufacturing-

specific baselines; Layer 4 (Real-Time Response) enables automated threat containment with fail-operational fallback mechanisms.

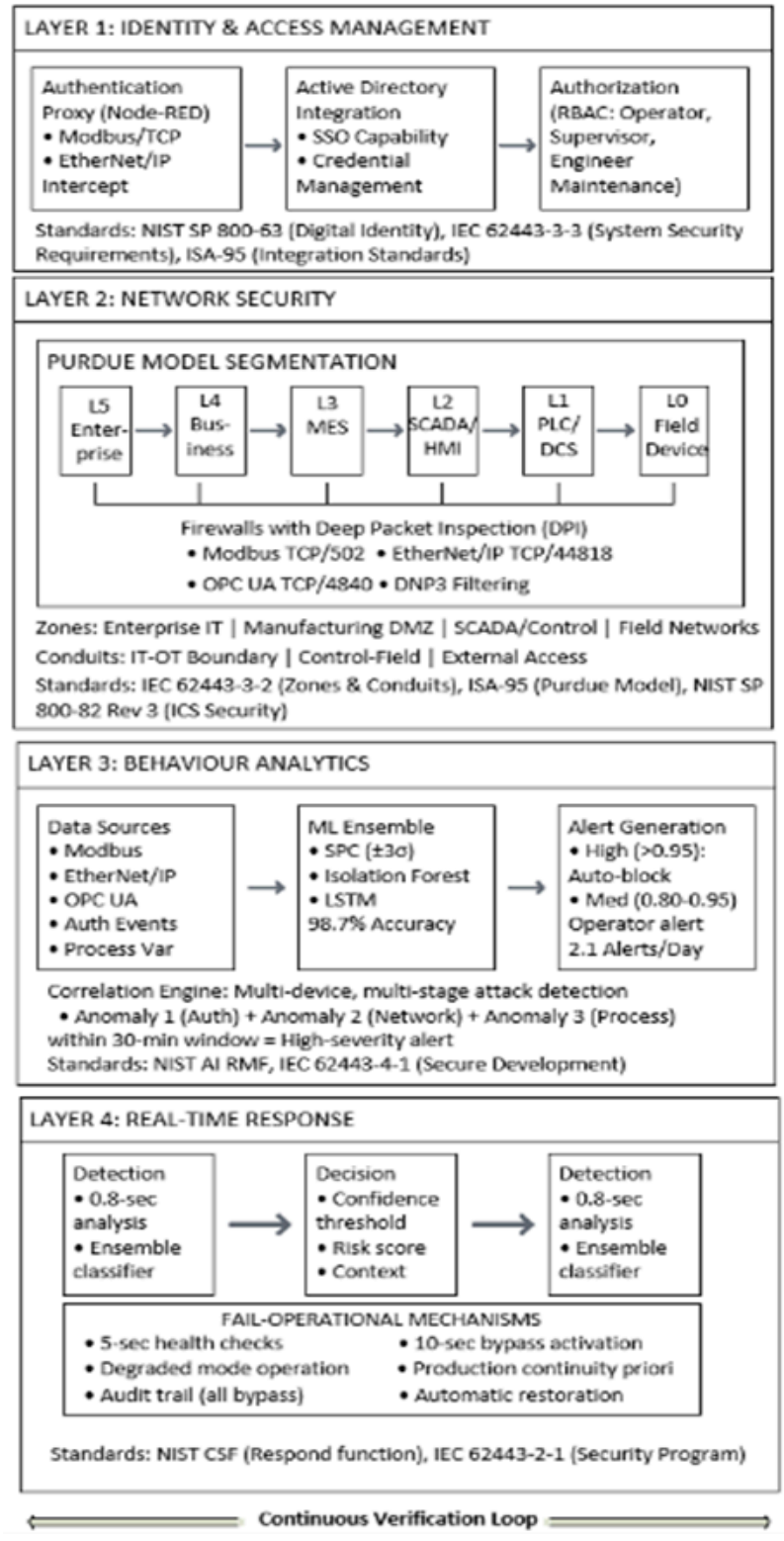


Figure 3

Four-layer Adaptive Zero Trust Framework with industry standards alignment. The architecture integrates identity management (NIST SP 800-63), network segmentation (IEC 62443, Purdue Model/ISA-95),

behavioral analytics, and real-time response capabilities. Arrows indicate data flow and verification dependencies across layers, demonstrating continuous verification principles applied to manufacturing environments.

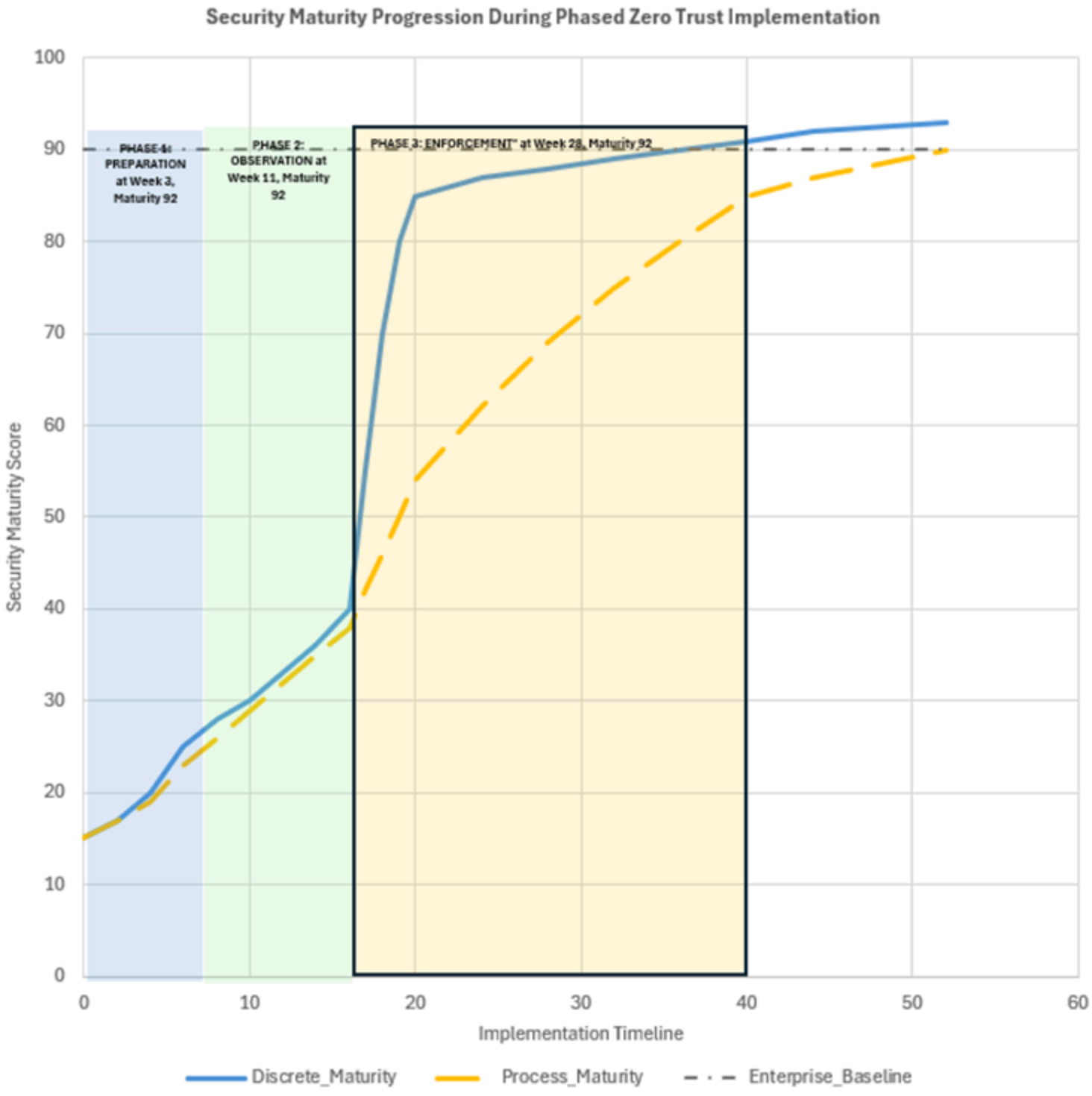


Figure 4

Security maturity progression during phased Zero Trust implementation. The S-curve illustrates advancement through three phases: organizational preparation (Phase 1, Weeks 1-6), observation infrastructure deployment (Phase 2, Weeks 7-16), and graduated enforcement activation (Phase 3,

Weeks 17-20). Timeline variations reflect sector-specific operational constraints, with discrete manufacturing completing in 16-20 weeks and continuous process manufacturing requiring 30-40 weeks.