International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 1348-1357
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Converged SIEM Framework for Unified IT-OT Security Monitoring

Abhishek Suman*

Independent Researcher, USA
* **Corresponding Author Email:** asuman.text@gmail.com- **ORCID:** 0000-0002-5247-0050

Article Info:

DOI: 10.22399/ijcesen.5024
Received : 05 January 2026
Revised : 25 February 2026
Accepted : 01 March 2026

Keywords

Converged Siem Framework,
It-Ot Security Integration,
Cyber-Physical Systems Monitoring,
Industrial Control System Security,
Cross-Domain Threat Correlation

Abstract:

Critical infrastructure security has traditionally maintained a rigid separation between Information Technology and Operational Technology systems, creating dangerous blind spots that sophisticated threat actors increasingly exploit. This article presents a unified Security Information and Event Management framework that integrates telemetry from hardened endpoints, network firewalls, and industrial IoT sensors into a single correlation engine designed specifically for cyber-physical systems. The proposed architecture addresses the fundamental challenges of converged IT-OT security monitoring through three core pillars: standardized data ingestion accommodating heterogeneous protocols, normalized event processing establishing consistent taxonomies across domains, and cross-domain correlation logic capable of identifying sophisticated multi-stage attacks. By leveraging machine learning approaches, including convolutional neural networks and behavioral analytics, the framework enables the detection of subtle anomalies and previously unknown attack patterns while maintaining low false positive rates that minimize operational disruptions. The research demonstrates how automated asset discovery addresses the persistent challenge of shadow IT and unmanaged operational devices in dynamic industrial environments, while security orchestration and automated response capabilities streamline incident management workflows. Cross-domain context enrichment proves particularly valuable during incident response, revealing how digital compromises affect physical operations and ensuring that containment actions align with operational safety requirements. This converged approach provides comprehensive real-time visibility across the entire cyber-physical ecosystem, enabling security teams to detect threats that span both digital and physical realms, significantly reducing response times while accounting for the unique characteristics of operational technology environments, including deterministic timing requirements, legacy equipment constraints, and safety-critical operational continuity demands.

1. Introduction

The convergence of digital and physical infrastructure has fundamentally transformed the security landscape for critical operations. Traditional security architectures have maintained a rigid separation between information technology networks and operational technology systems, creating fragmented visibility that sophisticated threat actors increasingly exploit. According to research published in the framework for SCADA and Industrial Control Systems security, the expanding interconnection between corporate IT networks and operational control systems has introduced unprecedented vulnerabilities that were previously nonexistent when these environments operated in isolation [1]. This division becomes particularly problematic in modern environments where cloud computing intersects with industrial control systems, supervisory control and data acquisition platforms, and building management systems. The research emphasizes that as organizations pursue digital transformation initiatives, they inadvertently create pathways for cyber threats to propagate from enterprise networks into critical operational infrastructure, fundamentally altering the threat landscape facing industrial facilities [1].

The integration of these previously isolated domains demands a reimagined approach to security monitoring—one that recognizes the interdependencies between computational resources

and physical processes. Contemporary industrial environments now face sophisticated adversaries who understand that attacking operational technology through information technology entry points provides lucrative opportunities for disruption, espionage, and sabotage. The framework for SCADA and ICS security highlights that traditional security measures designed exclusively for either IT or OT environments prove inadequate when addressing threats that traverse both domains, necessitating integrated security architectures that provide unified visibility across the entire cyber-physical ecosystem [1]. Furthermore, a comprehensive analysis of programmable logic controller security reveals that these critical industrial devices face multiple attack vectors ranging from network-based exploitation to malicious firmware modification, with attackers leveraging weaknesses in authentication mechanisms, communication protocols, and configuration management processes [2].A unified security framework addresses this challenge by correlating telemetry streams from diverse sources into a cohesive threat detection system. This convergence enables security teams to identify attack patterns that span both digital and physical realms, revealing threats that would remain invisible within siloed monitoring approaches. The overview of programmable logic controller security demonstrates that modern PLCs, which serve as the foundational control elements in industrial automation, require security monitoring that extends beyond traditional IT security paradigms to encompass protocol-specific anomalies, unauthorized programming attempts, and manipulation of control logic [2]. The framework transforms disparate data points—ranging from network packet captures and authentication logs to industrial sensor readings and programmable logic controller state changes—into actionable intelligence, providing the comprehensive visibility necessary to protect critical infrastructure against evolving threat vectors. Research indicates that effective security monitoring must account for the unique characteristics of OT environments, including deterministic timing requirements, legacy protocol dependencies, and the critical nature of availability requirements that often supersede confidentiality concerns in operational contexts [1]. By establishing normalized correlation rules across both IT and OT domains, security operations centers can detect multi-stage attacks where initial compromise occurs through enterprise networks before pivoting to operational systems, enabling defenders to identify and contain threats before they achieve their ultimate objective of disrupting physical processes or compromising safety systems.

2. Architectural Foundation of Converged Security Monitoring

The foundation of unified security monitoring rests on three core architectural pillars: standardized data ingestion, normalized event processing, and cross-domain correlation logic. Data ingestion mechanisms must accommodate the heterogeneous nature of IT and OT telemetry sources, which often operate on different protocols and reporting intervals. Research on utilizing datasets from industrial control systems for cybersecurity purposes reveals that the complexity of collecting and standardizing telemetry from operational environments presents significant technical challenges, as these systems employ diverse communication protocols, proprietary data formats, and vendor-specific implementations that resist straightforward integration [3]. Endpoint security agents, network traffic analyzers, and industrial sensors each generate distinct data formats that require translation into a common schema. The study emphasizes that industrial control system datasets must capture not only network traffic and system logs but also process-specific variables such as sensor readings, actuator commands, and control logic execution states, which collectively provide the contextual information necessary for meaningful security analysis [3].Normalization processes establish consistent taxonomies for events across domains, mapping firewall alerts, sensor anomalies, and authentication failures into unified categories. This standardization enables correlation engines to identify relationships between seemingly unrelated events—such as unusual network traffic patterns preceding abnormal temperature readings from cooling systems. Comprehensive analysis of industrial control system security issues demonstrates that effective event normalization must account for the semantic differences between IT and OT environments, where identical events may carry fundamentally different security implications depending on operational context [4]. The architecture employs distributed processing to handle the volume and velocity of real-time telemetry while maintaining the low latency required for time-sensitive operational decisions. Research highlights that industrial control systems operate under strict timing constraints where delays in data processing or event correlation could compromise not only security detection capabilities but also the real-time performance characteristics essential for safe and reliable industrial operations [3].

3. Multi-Layer Telemetry Integration

Integration spans multiple layers of the technology stack, from physical sensor data through network communications to application-level activities. Industrial sensors monitor environmental conditions, equipment states, and process variables that indicate physical system behavior, generating continuous data streams that reflect the operational state of manufacturing processes, power generation systems, water treatment facilities, and other critical infrastructure applications. Network monitoring captures traffic patterns, protocol anomalies, and communication flows between operational systems, with particular emphasis on industrial protocols that often lack the security features inherent in modern information technology networks [4]. Endpoint telemetry provides visibility into host-level activities, including process execution, file modifications, and privilege escalations, enabling detection of unauthorized software installations, malicious configuration changes, or compromised engineering workstations that could be leveraged to manipulate control logic. The overview of industrial control system security issues underscores that layered security monitoring must address vulnerabilities at multiple levels, including inadequate access controls, insufficient network segmentation, weak authentication mechanisms, unpatched software vulnerabilities, and the inherent insecurity of legacy industrial protocols designed decades ago without consideration for cybersecurity threats [4]. This multi-layer approach creates comprehensive coverage across the entire cyber-physical ecosystem, ensuring that attack indicators manifesting at any technological layer can be correlated with events occurring simultaneously or sequentially at other layers, thereby revealing sophisticated multi-stage attacks that exploit the complex interdependencies characteristic of modern industrial automation architectures.

4. Detection Capabilities and Threat Correlation

The converged framework enables detection of sophisticated attack scenarios that exploit the interface between IT and OT systems. Threat actors increasingly target operational environments through IT network compromises, using legitimate credentials to move laterally into industrial networks. Comprehensive survey research on intrusion detection for industrial control systems reveals that attack methodologies targeting operational technology have evolved significantly, with adversaries employing sophisticated techniques that exploit the convergence of IT and OT networks to achieve objectives ranging from espionage and sabotage to financial extortion [5]. By correlating authentication events with subsequent operational commands, the system identifies suspicious progressions that indicate potential compromise. The survey emphasizes that traditional intrusion detection approaches developed for information technology environments often prove inadequate when applied to industrial control systems due to fundamental differences in network protocols, traffic patterns, and operational constraints, necessitating specialized detection mechanisms that account for the deterministic nature of industrial communications and the safety-critical requirements of operational technology [5].Cross-domain correlation reveals attack patterns such as reconnaissance activities followed by targeted manipulation of physical processes. When network scanning precedes unauthorized changes to programmable logic controller configurations, the unified view identifies this progression as a potential coordinated attack rather than isolated incidents. The framework detects temporal relationships between events, identifying sequences that suggest malicious intent even when individual actions appear benign. Research on intrusion detection methodologies highlights that effective threat correlation requires understanding the semantic relationships between network-level events and physical process behaviors, enabling security systems to recognize when seemingly normal network communications result in abnormal operational outcomes that indicate potential manipulation of control logic or process parameters [5]. The study identifies that detection systems must incorporate domain knowledge about industrial processes, control algorithms, and safety constraints to accurately distinguish between legitimate operational variations and malicious activities designed to disrupt production or compromise safety systems.

5. Behavioral Analytics and Anomaly Detection

Advanced analytics incorporate behavioral baselines for both digital and physical systems, enabling detection of subtle deviations that indicate emerging threats. Machine learning models establish normal operational patterns by analyzing historical telemetry, then flag anomalies that diverge from expected behavior. Comprehensive analysis of network anomaly detection techniques demonstrates that machine learning approaches, including neural networks, support vector machines, and ensemble methods, have demonstrated considerable effectiveness in identifying anomalous behaviors within complex

network environments [6]. This approach proves particularly valuable for detecting insider threats and slow-moving attacks that evade signature-based detection methods. The research indicates that anomaly detection systems must balance sensitivity against false positive rates, with statistical approaches providing mathematical frameworks for establishing threshold values that optimize detection accuracy while minimizing operational disruptions caused by spurious alerts [6]. Furthermore, the survey reveals that hybrid detection approaches combining multiple machine learning techniques typically outperform single-method implementations, as different algorithms exhibit complementary strengths in detecting various anomaly types. The study emphasizes that unsupervised learning methods prove particularly valuable in industrial control system environments where labeled attack datasets remain scarce, enabling detection of previously unknown attack patterns through identification of deviations from established behavioral norms without requiring extensive training datasets representing specific threat signatures [6].

6. Asset Discovery and Inventory Management

Automated asset discovery addresses a critical challenge in dynamic environments where devices connect and disconnect frequently. The framework passively monitors network traffic and system communications to identify active assets without requiring manual inventory processes. Research on programmable logic controller security emphasizes that comprehensive asset visibility represents a foundational requirement for industrial control system security, as organizations cannot effectively protect devices they do not know exist within their operational networks [7]. This continuous discovery proves especially valuable for identifying shadow IT resources and unmanaged operational devices that pose security risks. The study highlights that programmable logic controllers, which serve as the fundamental building blocks of industrial automation, often operate on networks with limited visibility and documentation, creating scenarios where unauthorized or forgotten devices remain connected to critical control networks for extended periods without detection [7]. Furthermore, the research indicates that manual asset inventory processes prove inadequate in modern industrial environments where temporary connections for maintenance activities, mobile engineering workstations, and remotely accessible support systems create constantly changing network topologies that resist static documentation approaches.Asset classification algorithms categorize discovered devices based on communication patterns, protocols, and behavioral characteristics. This automated categorization helps security teams prioritize protection efforts and identify critical systems requiring enhanced monitoring. Comprehensive research on detecting cyber attacks in industrial control systems using convolutional neural networks demonstrates that deep learning approaches can effectively distinguish between normal operational behaviors and anomalous activities that indicate potential security incidents, with experimental results showing detection accuracy of 99.46% when trained on comprehensive datasets encompassing diverse operational scenarios [8]. The dynamic inventory feeds directly into risk assessment processes, ensuring security controls adapt to evolving infrastructure configurations. The study reveals that convolutional neural networks, when applied to time-series data representing network traffic patterns and process variables, can automatically extract relevant features without requiring manual feature engineering, enabling the detection of subtle anomalies that might escape notice by traditional rule-based systems [8]. Research demonstrates that the deep learning model successfully identified multiple attack types, including denial of service, reconnaissance activities, command injection, and response injection attacks, with particularly strong performance in detecting attacks targeting Modbus protocol communications commonly employed in industrial automation systems. The experimental evaluation conducted using the Secure Water Treatment testbed dataset revealed that the convolutional neural network approach achieved superior detection performance compared to traditional machine learning methods such as support vector machines and artificial neural networks, while simultaneously maintaining low false positive rates of approximately 0.5% that minimize operational disruptions caused by spurious security alerts [8]. The study emphasizes that automated classification and anomaly detection capabilities enable security teams to rapidly identify and respond to threats within the compressed timeframes required by industrial operations, where delays in threat detection and response can result in physical damage to equipment, production interruptions, environmental releases, or safety incidents affecting personnel.

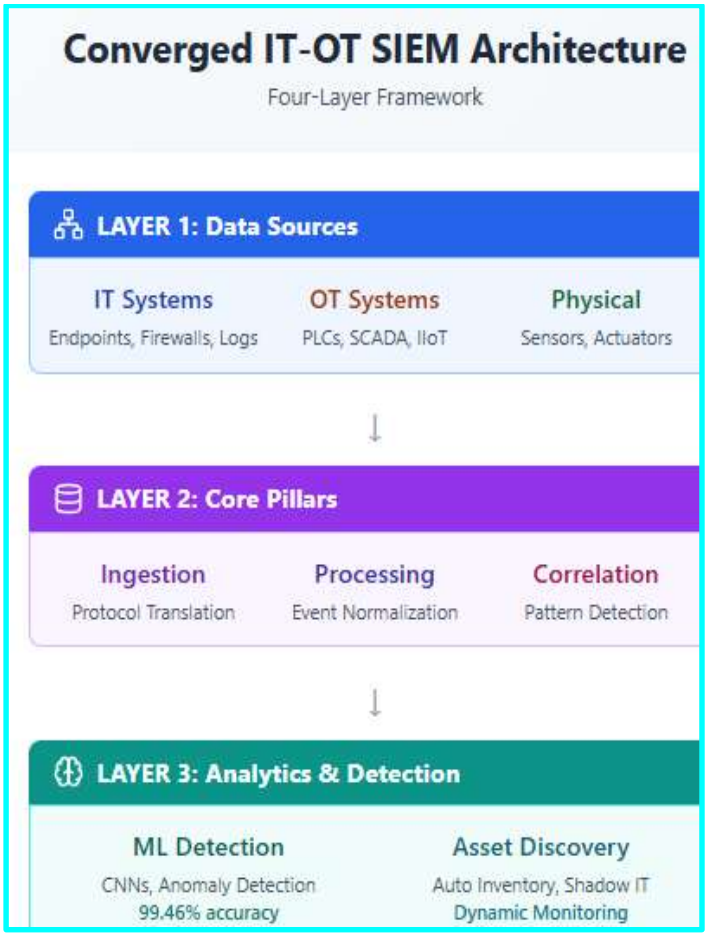
7. Incident Enrichment and Response Acceleration

Context enrichment significantly enhances incident response by aggregating relevant information from

multiple sources. When alerts trigger, the system automatically compiles associated events, asset information, vulnerability data, and threat intelligence into comprehensive incident packages. Research on security orchestration, automation, and response platforms demonstrates that these systems fundamentally transform incident management by automatically collecting, correlating, and contextualizing security alerts from diverse sources, enabling security operations centers to respond more rapidly and effectively to emerging threats [9]. This enrichment eliminates manual investigation steps, allowing responders to immediately assess scope and severity. The study emphasizes that security orchestration platforms integrate with multiple security tools, including security information and event management systems, intrusion detection systems, endpoint detection and response solutions, and threat intelligence platforms, to create unified workflows that streamline investigation processes and reduce the cognitive burden on security analysts [9]. Furthermore, research reveals that automated enrichment capabilities prove particularly valuable in addressing the persistent challenge of alert fatigue, where security teams become overwhelmed by the volume of alerts generated by modern security monitoring infrastructure, with automation enabling rapid filtering and prioritization of alerts based on contextual relevance and potential business impact.Cross-domain context proves particularly valuable during incident response, revealing how digital compromises affect physical operations or how physical tampering enables cyber attacks. Response workflows integrate with automation platforms to execute containment actions across both IT and OT environments, ensuring coordinated responses that prevent attack propagation. Comprehensive review of information security for industrial control systems highlights that effective incident response in operational technology environments requires specialized approaches that account for the unique characteristics of industrial systems, including real-time operational requirements, legacy equipment constraints, and the potential for cyber incidents to trigger physical consequences affecting safety and operational continuity [10]. The research emphasizes that industrial control systems face distinct security challenges compared to traditional information technology environments, with attack scenarios potentially resulting in equipment damage, production disruptions, environmental releases, or safety incidents that extend beyond the digital realm into physical operational impacts [10]. Studies indicate that incident response procedures for industrial environments must incorporate coordination mechanisms between cybersecurity personnel and operational staff who possess deep knowledge of industrial processes, control logic, and safety systems, ensuring that containment and recovery actions do not inadvertently create hazardous conditions or exacerbate operational disruptions. The review underscores that automated response capabilities in operational technology contexts require careful design to prevent unintended consequences, with validation mechanisms ensuring that automated containment actions, such as network isolation or system shutdown, align with operational safety requirements and do not create conditions more dangerous than the cyber threats they aim to mitigate [10]. Research demonstrates that organizations implementing structured incident response frameworks specifically tailored for industrial control systems achieve more effective threat containment while minimizing operational impacts, with documented procedures enabling rapid escalation, coordinated decision-making, and systematic recovery processes that restore normal operations while preserving forensic evidence necessary for post-incident analysis and regulatory compliance reporting.

Table 1: *Architectural Pillars of Converged IT-OT Security Monitoring Systems [3, 4]*

Architectural Pillar	Primary Function	Technical Challenge	Operational Requirement
Standardized Data Ingestion	Accommodate heterogeneous IT/OT telemetry sources	Diverse protocols, proprietary formats, vendor-specific implementations	Capture network traffic, system logs, and process-specific variables
Normalized Event Processing	Establish consistent taxonomies across domains	Semantic differences between IT and OT environments	Map firewall alerts, sensor anomalies, and authentication failures to unified categories
Cross-Domain Correlation Logic	Identify relationships between unrelated events	Volume and velocity of real-time telemetry	Maintain low latency for time-sensitive operational decisions
Distributed Processing	Handle real-time telemetry at scale	Strict timing constraints in industrial control systems	Preserve real-time performance for safe industrial operations



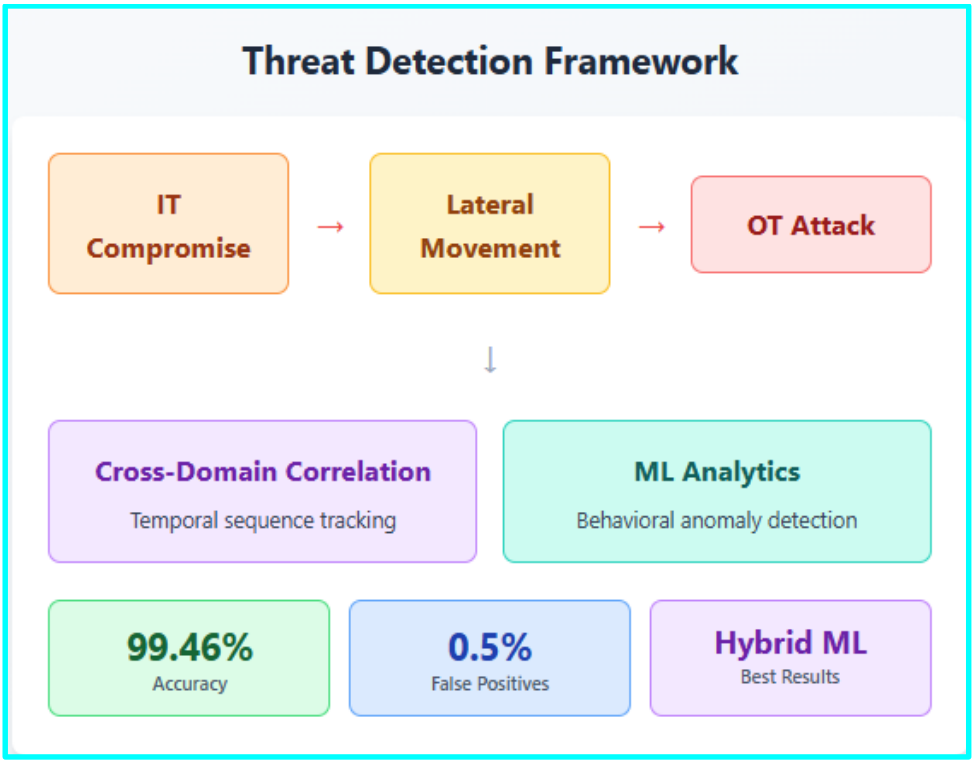


***Table 2**: Comparative Effectiveness of Machine Learning Techniques for ICS Anomaly Detection [5, 6]*

ML Technique	Detection Capability	Primary Advantage	Limitation Addressed	Application Context

Neural Networks	Identifies anomalous behaviors in complex networks	Effective pattern recognition	Signature-based detection gaps	Complex network environments
Support Vector Machines	Classifies normal vs. anomalous activities	Statistical classification strength	Unknown attack patterns	Industrial automation systems
Ensemble Methods	Superior performance across anomaly types	Complementary algorithm strengths	Single-method limitations	Multi-variant threat scenarios
Convolutional Neural Networks	Distinguishes normal from anomalous operations	Automatic feature extraction	Manual feature engineering requirements	Time-series network/process data
Unsupervised Learning	Detects unknown attack patterns	No labeled training data required	Scarce attack datasets	Industrial control systems
Hybrid Detection Approaches	Outperforms single implementations	Multiple technique synergy	Various anomaly type detection	Cross-domain ICS environments

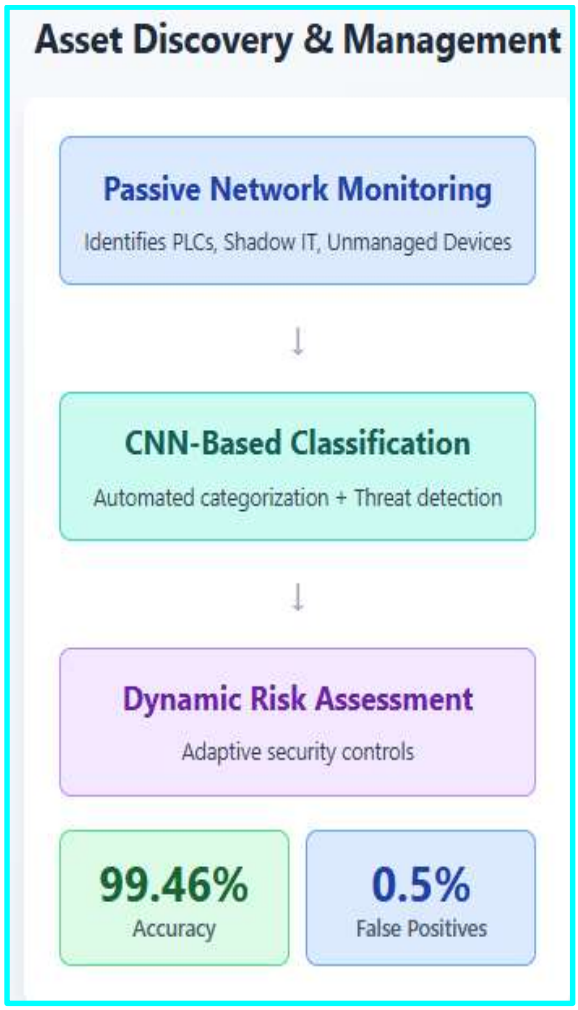


Table 3: *Automated Asset Discovery Solutions for Dynamic Industrial Control Environments [7, 8]*

Challenge	Traditional Approach Limitations	Automated Discovery Solution	Security Benefit
Frequently connecting/disconnecting devices	Manual inventory processes are inadequate	Passive network traffic monitoring	Continuous real-time asset visibility
Shadow IT resources	Limited visibility and documentation	System communications analysis	Identification of unmanaged operational devices

Unauthorized/forgotten devices	Static documentation approaches	Continuous discovery monitoring	Detection of devices on critical control networks
Temporary maintenance connections	Manual updates lag behind changes	Passive monitoring without manual updates	Captures transient device connections
Mobile engineering workstations	Documentation resistance	Network traffic pattern analysis	Tracks mobile and temporary systems
Remotely accessible support systems	Constantly changing topologies	Automated identification without inventory	Comprehensive remote access visibility

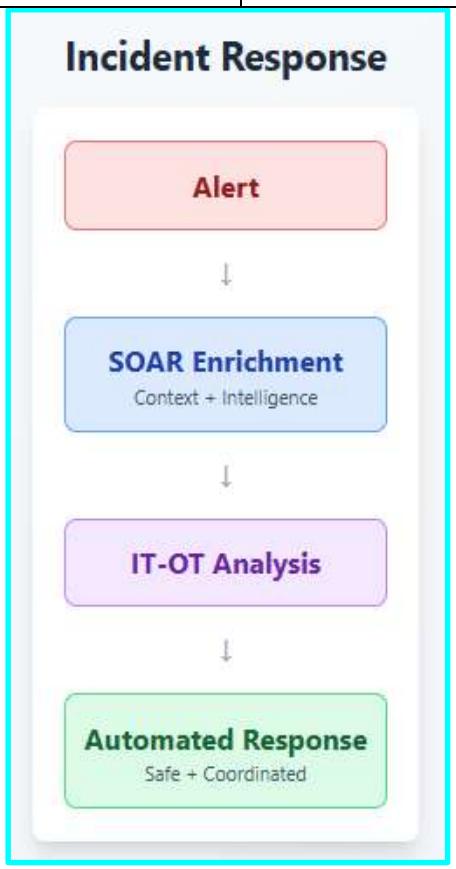


Table 4: *Specialized Incident Response Requirements for Industrial Control System Environments [9, 10]*

Response Requirement	**IT Environment Approach**	**OT Environment Constraint**	**Specialized Consideration**	**Safety/Operational Impact**
Containment Actions	Immediate isolation	Real-time operational requirements	Validation mechanisms needed	Production continuity preservation
Network Isolation	Standard response procedure	Legacy equipment constraints	Safety alignment verification	Prevention of hazardous conditions
System Shutdown	Automated execution	Physical consequence potential	Operational safety checks	Equipment damage prevention
Coordination Mechanisms	The IT security team focused	Cybersecurity-operational staff integration	Deep process knowledge required	Safety system protection
Recovery Procedures	Digital restoration priority	Physical operational impacts	Systematic recovery with forensics	Regulatory compliance maintenance
Threat Containment	Digital realm focus	Equipment, production, environmental, and safety consequences	Minimized operational disruption	Extended physical impact prevention

4. Conclusions

As such, unified security monitoring is a fundamental paradigm shift in critical infrastructure protection-one that tackles head-on the dangerous blind spots created by traditional separations of information technology and operational technology security architectures. The converged Security Information and Event Management framework presented in this research underlines that comprehensive threat detection across cyber-physical systems requires integrated approaches that correlate telemetry from diverse sources spanning physical sensors, network communications, and endpoint activities into cohesive intelligence. Building standardized data ingestion mechanisms, normalized event taxonomies, and cross-domain correlation logic that can identify temporal relationships between apparently unrelated events would provide the security operations center with the ability to identify complex multistage attacks threatening to compromise the interface between digital and physical infrastructure. Advanced machine learning techniques, including convolutional neural networks and behavioral analytics, enable the detection of subtle anomalies and hitherto unknown attack patterns while maintaining operational efficiency through low false positive rates. Automated asset discovery and classification capabilities address a critical challenge relative to maintaining comprehensive visibility in dynamic industrial environments where manual inventory processes are invariably inadequate. Security orchestration and automated response platforms further enhance incident management through the elimination of manual investigation steps, aggregation of contextual information sourced from multiple inputs, and the execution of coordinated containment actions across both IT and OT domains. The research emphasizes, however, that incident response in operational technology environments requires specialized approaches, inclusive of validation mechanisms that ensure that automated actions are consistent with safety requirements and do not lead to conditions more hazardous than those which they aim to mitigate. As infrastructure convergence accelerates and threat actors further develop sophisticated techniques, leveraging the seams between digital and physical systems, unified security monitoring becomes not simply advantageous but rather an imperative for ensuring operational resilience, protecting safety systems, and maintaining regulatory compliance across critical infrastructure sectors.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Jeyasingam Nivethan, "A Framework for SCADA/ICS Security," ResearchGate, December 2016. [Online]. Available: https://www.researchgate.net/publication/311607812_A_Framework_for_SCADAICS_Security

[2] Hui Cui et al., "An Overview of the Security of Programmable Logic Controllers in Industrial Control Systems," ResearchGate, May 2024. [Online]. Available: https://www.researchgate.net/publication/380800156_An_Overview_of_the_Security_of_Programmable_Logic_Controllers_in_Industrial_Control_Systems

[3] Qin Lin et al., "Using Datasets from Industrial Control Systems for Cyber Security Research and Education," ResearchGate, January 2020. [Online]. Available: https://www.researchgate.net/publication/338081179_Using_Datasets_from_Industrial_Control_Systems_for_Cyber_Security_Research_and_Education

[4] Lordes Ruiz et al., "Industrial Control System (ICS): The General Overview of the Security Issues and Countermeasures," ResearchGate, July 2021. [Online]. Available: https://www.researchgate.net/publication/353284100_Industrial_Control_System_ICS_The_General_Overview_of_the_Security_Issues_and_Countermeasures

[5] Yan Hu et al., "A Survey of Intrusion Detection on Industrial Control Systems," ResearchGate, August 2018. [Online]. Available: https://www.researchgate.net/publication/32707351

8_A_survey_of_intrusion_detection_on_industrial_control_systems

[6] Mohiuddin Ahmed et al., "A Survey of Network Anomaly Detection Techniques," January 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804515002891

[7] Haolan Lu et al., "Research on Programmable Logic Controller Security," ResearchGate, August 2019. [Online]. Available: https://www.researchgate.net/publication/335081417_Research_on_Programmable_Logic_Controller_Security

[8] Moshe Kravchik et al., "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks," ResearchGate, October 2018. [Online]. Available: https://www.researchgate.net/publication/328326814_Detecting_Cyber_Attacks_in_Industrial_Control_Systems_Using_Convolutional_Neural_Networks

[9] Robert A Bridges et al., "Security Orchestration, Automation and Response (SOAR): A Systematic Literature Review," Computers & Security, vol. 128, June 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404823001116

[10] Wang Mingqian et al., "Review on Information Security of Industrial Control Systems," ResearchGate, September 2019. [Online]. Available: https://www.researchgate.net/publication/368909327_REVIEW_ON_INFORMATION_SECURITY_OF_INDUSTRIAL_CONTROL_SYSTEMS