https://doi.org/10.1051/itmconf/20257901005

# Securing the Convergence of IT and OT Networks in Cyber Physical System: Policy, Architecture and Implementation Challenges

*Rajiv* Raich[1*], *Anagha* Raich[2], and *Nandkishor* Kinhekar[1]

[1]Department of Electrical Engineering, Sardar Patel College of Engineering, Mumbai, India
[2]Depatment of Artificial Intelligence, SVKM's NMIMS, Mukesh Patel School of Technology Management & Engineering (MPSTME), Mumbai, India

**Abstract.** The integration of Information Technology (IT) and Operational Technology (OT) within Cyber-Physical Systems (CPS) is reshaping critical infrastructure, driving improvements in efficiency, automation, and agile decision-making. However, this integration introduces significant cybersecurity challenges due to fundamental differences in priorities, protocols, and governance models. While IT systems emphasize data confidentiality and rapid updates, OT systems prioritize availability, reliability, and safety—often relying on legacy infrastructure less-equipped to handle modern threats. This paper explores the multifaceted challenges in securing IT-OT convergence within CPS, with a particular focus on critical infrastructure sectors such as energy, water, transportation, and manufacturing. The policy and regulatory gaps that hinder unified security strategies are analysed. The architectural models that support secure interoperability are examined, and key implementation challenges including segmentation, legacy system integration, and threat modelling are identified. A literature review of contemporary frameworks and case studies reveals a fragmented approach to security, with a need for further standardization, governance harmonization, and real-time risk assessment tools. This paper outlines general guidelines and checkpoints aligned of existing frameworks for a layered, defense-in-depth strategy aligned with zero-trust principles, supported by policy recommendations and architectural guidelines tailored to critical infrastructure protection. The findings aim to assist policymakers, engineers, and security professionals in building resilient and adaptive CPS environments to mitigate evolving cyber threats.

## 1 Introduction

The rapid digital transformation of industrial environments has led to the Information Technology (IT) and Operational Technology (OT) convergence across Cyber-Physical Systems (CPS), particularly in vital infrastructure domains like energy, water, transportation, and manufacturing. Traditionally, IT systems have operated in corporate domains focused on data processing, communication, and cybersecurity, while OT systems have been designed to control and monitor physical processes with an emphasis on availability, safety, and real-time performance. Significant advantages, such as increased automation, remote monitoring, predictive maintenance, and increased operational efficiency, result from the convergence of these two disciplines. However, because IT and OT systems have different features, threat landscapes, and design philosophies, this integration also brings with it complicated cybersecurity threats. [1]

Critical infrastructures are particularly vulnerable to the implications of IT-OT convergence. Given that traditional OT systems, which were typically developed without cybersecurity as a core consideration, are increasingly connected to enterprise IT networks and the internet, the attack surface expands exponentially. This has been evidenced by numerous high-profile cyberattacks such as the Stuxnet worm, Colonial Pipeline breach, and Triton malware, which exploited weak links between IT and OT layers. Such incidents underscore the urgent need for robust, sector-specific cybersecurity strategies that bridge the policy, architecture, and implementation gaps between these domains.

Despite the growing awareness of these risks, current cybersecurity practices and regulatory frameworks often lacks in addressing the unique challenges posed by converged environments. Many organizations lack comprehensive policies tailored to hybrid IT-OT systems, while technical architectures frequently do not incorporate security-by-design principles for legacy OT assets. Additionally, implementation efforts are hampered by siloed operations, insufficient cross-domain expertise, and the absence of real-time monitoring and response mechanisms that span both IT and OT ecosystems.

This paper aims to investigate the policy, architectural, and implementation challenges in securing IT-OT convergence within CPS, with a specific focus on critical infrastructure systems. It provides a

* Corresponding author: raich.rajiv@gmail.com

comprehensive review of existing literature, highlights key gaps in current practices, and outlines general guidelines and checkpoints for a layered security framework grounded in defense-in-depth and zero-trust principles. By addressing both strategic and operational aspects, this study seeks to contribute to the development of resilient, adaptive, and secure CPS environments capable of withstanding evolving cyber threats.

The paper's sections are organized as follows:

- Section 2 provides a thorough literature analysis and emphasizes the particular security issues related to ICS and CPS in the context of IT and OT.
- Section 3 introduces the PERA and discusses its role in structuring secure CPS environments.
- Section 4 explores the security challenges and evolving threat landscape affecting converged IT/OT systems.
- Section 5 outlines key policy frameworks and governance models essential for securing CPS.
- Section 6 proposes secure architectural designs including segmentation, DMZ, and IDS.
- Section 7 discusses implementation challenges covering technical, organizational, and cost-related barriers.
- Section 8 provides a critical discussion on implications, limitations, and directions for future work.
- Finally, Section 9 concludes the paper with a summary of key findings and recommendations for building secure, resilient, and adaptive cyber-physical infrastructures.

## 2 Background / Literature review

Critical infrastructure sectors rely heavily on Industrial Control Systems (ICS) to function. In critical infrastructure sectors, the integration of IT and OT inside CPS has become both a technological requirement and a security challenge. Numerous studies and reports related to vulnerabilities, attack vectors, and security strategies applicable to OT have underscored the increasing complexity and vulnerability resulting from this convergence. [1]

### 2.1 Nature of ICS and unique security challenges

Traditional IT security solutions often fall short in ICS environments due to the latter's unique requirements for high availability, legacy equipment, and real-time performance. According to Maglaras et al. [2], ICS were originally designed for reliability and efficiency, not for cybersecurity. The integration of these systems with external networks has created new attack surfaces, which traditional security models are ill-equipped to handle.

Hajda et al. [3] emphasize that legacy protocols (e.g., Modbus, DNP3) commonly used in ICS lack basic encryption and authentication features. This makes them susceptible to various attacks such as spoofing, replay attacks, and man-in-the-middle intrusions.

### 2.2 Major threats and vulnerabilities

Recent literature highlights several high-profile incidents—such as Stuxnet, BlackEnergy, and the TRITON malware—as illustrative of the real-world impact of ICS vulnerabilities. Ara [4] identifies common vulnerabilities in SCADA systems, including weak authentication mechanisms, lack of proper segmentation, and insufficient monitoring.

Makrakis et al. [5] provide a comprehensive survey of attack vectors in ICS, including insider threats, supply chain attacks, and malware targeting PLCs. These attacks exploit both technical weaknesses and operational oversights.

From a threat perspective, Zografopoulos et al. [6] focus on CPS in energy infrastructure, identifying specific attack vectors such as network injection and false data injection. Similarly, Kumar and Vardhan [7] offer a comprehensive tutorial of OT-specific vulnerabilities and mitigation practices, detailing legacy system challenges and real-time threat detection requirements. Claroty [8] and TXOne Networks [9] reinforce these findings with global surveys showing that ransomware and third-party risks are escalating, particularly in unpatched or segmented OT environments.

### 2.3 Emerging security solutions

Multiple studies have proposed solutions tailored to the constraints of ICS environments. Umer et al. [10] explore the application of machine learning (ML) techniques for anomaly detection in ICS traffic, which can help identify zero-day threats without relying on predefined signatures.

Varghese et al. [11] introduces the concept of Digital Twins for ICS security—a virtual replica of physical systems that can simulate and predict behaviours, enabling advanced intrusion detection.

Emerging cybersecurity paradigms like Zero-Trust and defense-in-depth are examined in Lawal [12] and AlertEnterprise [13]. These papers stress the need for contextual identity, policy automation, and convergence of physical and cyber layers. Cryptographic advances are addressed in Mosteiro-Sanchez et al. [14] and Oliva del Moral et al. [15], which advocate for post-quantum cryptography and attribute-based encryption to secure Industrial IoT (IIoT) within CPS frameworks.

Surveys such as Ahmed and Zhou [16] and Sechi [17] contribute a broader academic perspective, discussing the integration of physical-aware security models and the role of cascading failure consequences. Armis [18] identifies five emerging priorities, such as integrated monitoring and AI-based threat hunting, which are increasingly vital due to rising OT asset connectivity.

Other researchers advocate for a defense-in-depth approach, involving layered security controls, segmentation of network, intrusion detection systems

(IDS), and strict access management. Frameworks such as IEC 62443 and NIST SP 800-82 provide structured guidelines for securing ICS environments. [19]

In terms of implementation, Fortinet [20] presents an OT security platform approach, integrating next-generation firewalls, virtual patching, and micro-segmentation to mitigate lateral movement of threats. RedSeal (a leader in network exposure management) highlights the challenge of legacy system exposure, proposing visibility and risk scoring mechanisms to support continuous compliance in hybrid IT-OT networks. Some researchers proposes firewall optimization algorithms to dynamically manage segmentation in power grid systems, while few others compared deployment strategies across water and power sectors, identifying bottlenecks in policy enforcement and technical execution.

### 2.4 Policy and human factors

Several studies point out the critical role of policy, training, and organizational culture. According to Kaspersky ICS-CERT, human error and lack of cybersecurity awareness are major contributors to ICS breaches. Regular training, incident response planning, and clear security policies are emphasized as necessary components of a holistic security strategy.

Foundational policy insights are provided by the NSTAC IT-OT Convergence Report and NIST SP 800-82r3, which outline the regulatory gaps and suggest architectural frameworks tailored to the unique needs of OT environments. They emphasize risk-based segmentation, asset inventory, and standardized protocols to harmonize security across IT and OT layers.

### 2.5 Summary

While considerable strides have been made in visibility and segmentation technologies, the literature consistently highlights enduring challenges in legacy OT integration, regulatory fragmentation, and organizational inertia. Therefore, a unified, risk-centric, and resilience-oriented approach remains critical to securing IT-OT convergence in critical infrastructure CPS environments.

Collectively, these works converge on key themes:

- The urgent need for standardized policy,
- Architectural adaptation for hybrid networks, and
- Implementation of intelligent and layered defenses.

## 3 Cyber-physical system architecture

The Purdue Enterprise Reference Architecture (PERA), or Purdue Model given in Figure 1, is a widely adopted framework for structuring ICS and CPS. It provides a hierarchical model that separates enterprise IT systems from OT systems, creating a structured framework for defense-in-depth and enabling better management, security, and integration.

### 3.1 Overview of the purdue model

The model is 7-layer framework and segments networks into zones based on function and security needs, with a DMZ (Demilitarized Zone) acting as a buffer between IT and OT networks. The model, while commonly presented with 6 levels, can be extended to 7 by including a DMZ (Level 3.5) between the IT and OT layers. This allows for controlled communication and protection of critical OT systems.

Here's a breakdown of the 7 layers, including the DMZ:

1. Level 0: Physical Process Zone: This is the bottommost level, containing the physical equipment and processes e.g. sensors, actuators, and machinery.
2. Level 1: Intelligent Devices Zone: This level includes devices like PLCs and DCS that directly manage the physical processes.
3. Level 2: Control Systems Zone: This level houses SCADA systems, which monitor and control the processes at a higher level.
4. Level 3: Manufacturing Operations Systems Zone: This zone includes systems like historians, alarm servers, and other systems that monitor and manage manufacturing operations.
5. Level 3.5: DMZ (Demilitarized Zone): This crucial level acts as a buffer between the IT and OT networks, filtering and regulating traffic to protect OT systems.
6. Level 4/5: Enterprise Zone/Network: This level includes corporate systems like Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) in Level 4 (Enterprise Zone) and the highest level, encompassing corporate IT systems like email and file storage in Level 5 (Enterprise Network)

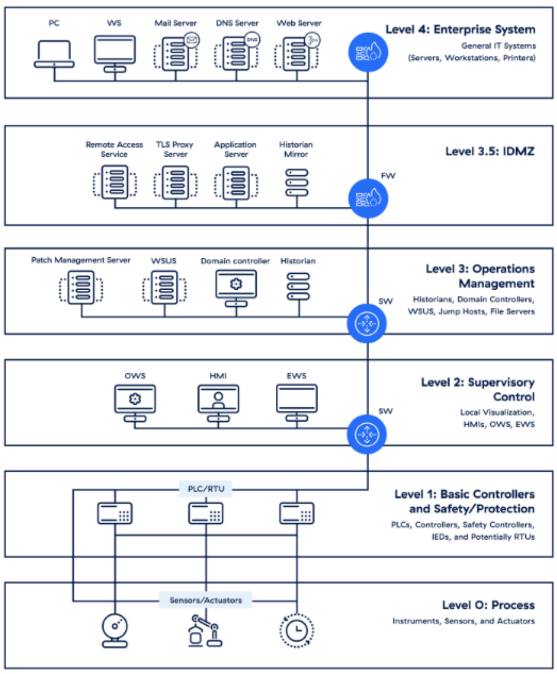


**Fig. 1.** Purdue model (image adapted from -zscaler.com).

The Purdue model, along with frameworks like NIST 800-82 and IEC 62443, enables a structured approach for securing ICS networks by isolating different parts of the organization's layers. The DMZ is a key component, ensuring controlled communication and protection of critical systems.

### 3.2 IT and OT convergence in the purdue model

Traditionally, IT (Levels 4–5) and OT (Levels 0–3) operated in silos. However, modern CPS demand seamless integration for real-time analytics, predictive maintenance, and adaptive control. This convergence introduces new challenges:

1. Data Flow: Real-time data from OT must be securely transmitted to IT systems for analysis and decision-making.
2. Security Zones: Each level must be segmented with firewalls and DMZs to prevent lateral movement of threats.
3. Protocol Bridging: Integration requires translation between IT protocols (e.g., TCP/IP, HTTPS) and OT protocols (e.g., Modbus, OPC UA).

## 4 Security challenges in IT/OT convergence

The IT and OT convergence increases the attack surface to large extent and needs to be analyzed and mitigated timely to avoid any untoward incidents. The CPS is further vulnerable to risks due to physical asset types and at times due to unmanned and unprotected location/zones to integrate physical processes with computing systems.

Understanding the distinctions between IT and OT cybersecurity is crucial for planning effective security strategies, especially as these domains increasingly converge in modern infrastructures like smart grids.

### 4.1 Threat landscape

The threat landscape and collaboration between attackers are exponentially increasing making all connected system much more vulnerable to threats.

1. Ransomware: These attacks have increasingly targeted industrial environments, encrypting critical OT systems and demanding payment for decryption. These attacks can hamper production lines, disrupt supply chains, and result in large financial losses. Notable examples include the Locker Goga and EKANS ransomware strains, which specifically target ICS environments.
2. Insider Threats: Insiders whether malicious or negligent—pose a unique risk due to their access to both IT and OT systems. A disgruntled employee or a contractor with elevated privileges can bypass security controls, manipulate process data, or disable safety systems.
3. Advanced Persistent Threats (APTs): APTs are long-term, targeted attacks often orchestrated by nation-state actors. These threats are particularly dangerous in CPS environments due to their stealthy nature and ability to remain undetected for extended periods. APTs often exploit IT/OT integration points to move laterally across networks.

### 4.2 Vulnerabilities in converged environments

1. Legacy Systems: Many OT systems were designed decades ago with little consideration for cybersecurity. These systems often run outdated software, lack encryption, and cannot be easily patched without disrupting operations.
2. Lack of Network Segmentation: Inadequate segmentation between IT and OT networks allows attackers to pivot from compromised IT systems into critical OT infrastructure. Flat network architectures are especially vulnerable to lateral movement.
3. Protocol Weaknesses: OT protocols such as Modbus, DNP3, and BACnet were not originally built with security considerations, often lacking essential safeguards such as authentication, encryption, and integrity verification. As a result, they are vulnerable to threats like spoofing, replay attacks, and man-in-the-middle exploits.

## 5 Policy and governance frameworks

Effective policy and governance frameworks are essential for securing the IT and OT networks convergence in Cyber-Physical Systems (CPS). These frameworks provide the foundation for implementing security controls, ensuring compliance, and managing risks across diverse technological domains.

### 5.1 Regulatory standards

Several international standards guide the development and enforcement of cybersecurity policies in CPS environments:

1. NIST Cybersecurity Framework (CSF): It is developed by the U.S. National Institute of Standards and Technology and provides a flexible, risk-based approach to managing cybersecurity. It includes five core functions: Identify, Protect, Detect, Respond, and Recover, which are applicable across both IT and OT domains.
2. IEC 62443: Developed by the International Electrotechnical Commission (IEC), to specifically addresses security for Industrial Automation and Control Systems (IACS). It defines roles, responsibilities, and technical requirements for securing OT environments, including system integrators and asset owners.
3. ISO/IEC-27001: This standard outlines requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It is widely used in IT environments and

increasingly adopted in OT settings to ensure consistent security governance.

### 5.2 Policy models

1. Role-Based Access Control (RBAC): RBAC restricts system access based on user roles and responsibilities. In CPS, it ensures that operators, engineers, and administrators have access only to the systems and data necessary for their tasks, reducing the risk of unauthorized actions.
2. Zero Trust Architecture (ZTA): Zero Trust assumes that no user or device is inherently trustworthy, even within the network perimeter. It enforces continuous verification, least privilege access, and micro-segmentation. ZTA is particularly effective in IT/OT environments where traditional perimeter-based security is insufficient.

### 5.3 Compliance challenges

Despite the availability of robust standards and models, organizations face several challenges in implementing and enforcing cybersecurity policies:

1. Interoperability Issues: IT and OT systems often use different protocols and platforms, making unified policy enforcement difficult.
2. Legacy Infrastructure: Many OT systems lack the capability to support modern security controls, such as encryption or authentication.
3. Cultural Divide: IT and OT teams may have differing priorities and risk perceptions, leading to inconsistent policy adoption.
4. Resource Constraints: Budget limitations and skill shortages can hinder the deployment of comprehensive governance frameworks.
5. Audit and Monitoring: Continuous compliance monitoring is complex due to the dynamic nature of CPS and the need for real-time operations.

## 6 Secure architecture design

Designing a secure architecture for CPS is critical to ensuring the confidentiality, integrity, and availability of both IT and OT environments. As these systems become increasingly interconnected, a layered and resilient security architecture becomes essential to defend against evolving cyber threats.

### 6.1 Segmentation strategies

#### *6.1.1 IT/OT Network Segmentation*

It is the foundational principle of secure CPS architecture. Dividing the network into distinct zones limits the spread of threats and enforce access control.

- Zoning: Separate IT and OT networks into different security zones.
- Conduits: Define controlled communication paths between zones.
- Access Control Lists (ACLs): Restrict traffic between segments based on roles and protocols.

#### *6.1.2 Demilitarized zones (DMZs)*

It acts as a buffer zone between IT and OT networks, hosting services that require access from both domains (e.g., data historians, remote access gateways).

- Dual Firewalls: One facing the IT network, the other facing the OT network.
- Proxy Servers: Mediate communication to prevent direct access.
- Data Diodes: Enforce unidirectional data flow for critical systems.

### 6.2 Security controls

#### *6.2.1 Firewalls*

Firewalls enforce perimeter security by filtering traffic based on predefined rules. In CPS, both traditional and industrial firewalls are used to protect control networks.

- Deep Packet Inspection (DPI): For protocol-aware filtering (e.g., Modbus, DNP3).
- Application Layer Gateways: For inspecting SCADA traffic.

#### *6.2.2 Intrusion detection and prevention systems (IDS/IPS)*

These IDS systems monitor network traffic for signs of malicious activity and can be classified as under:

- Signature-Based: Detect known threats using predefined patterns.
- Anomaly-Based: Detects irregularities from established behavioral norms, making them particularly effective in OT environments where network traffic tends to follow consistent patterns.

#### *6.2.3 Anomaly detection systems*

Machine learning-based systems can detect subtle anomalies in sensor data, control commands, or network behaviour, providing early warning of potential attacks.

### 6.3 Resilience mechanisms

#### *6.3.1 Redundancy*

Redundant systems ensure continued operation in case of hardware or software failure.

- Hot Standby Systems: Automatically take over if the primary system fails.
- Redundant Communication Paths: Prevent single points of failure in network infrastructure.

#### *6.3.2 Failover systems*

Failover mechanisms switch operations to backup systems during outages or attacks, minimizing downtime.

- Automated Failover: Triggered by system health checks or anomaly detection.
- Manual Override: Allows operators to intervene in critical situations.

#### *6.3.3 Incident response and recovery*

A well-defined incident response plan helps to minimize the impact of security breaches.

- Detection and Containment: Rapid identification and isolation of affected systems.
- Eradication and Recovery: Removal of threats and restoration of normal operations.
- Post-Incident Analysis: Lessons learned to improve future resilience.

## 7 Implementation challenges

Secure implementation of IT and OT presents a range of technical, organizational, and financial challenges. These challenges must be addressed holistically to ensure a resilient and scalable security posture.

### 7.1 Technical barriers

#### *7.1.1 Interoperability*

IT and OT systems often use different communication protocols, data formats, and hardware platforms. Integrating these systems securely requires:

- Protocol translation (e.g., Modbus to TCP/IP)
- Middleware solutions for data normalization
- Secure APIs for cross-domain communication

#### *7.1.2 Legacy systems*

Many OT environments rely on legacy equipment that lacks modern security features such as encryption, authentication, or patching capabilities. These systems are often mission-critical and cannot be easily replaced or taken offline for updates.

#### *7.1.3 Real-time constraints*

OT systems operate under strict real-time requirements. Security measures such as deep packet inspection or encryption can introduce latency, potentially disrupting time-sensitive operations like process control or safety mechanisms.

### 7.2 Organizational issues

#### *7.2.1 Skill gaps*

There is a shortage of professionals with expertise in both IT security and OT operations. This gap hinders the development and deployment of integrated security strategies.

- IT professionals may lack understanding of industrial protocols and safety requirements.
- OT engineers may be unfamiliar with cybersecurity principles and tools.

#### *7.2.2 Cultural differences*

IT and OT teams often have different priorities and risk tolerances:

- IT Focus: Data confidentiality, uptime, and patch management.
- OT Focus: Safety, availability, and deterministic performance.

Bridging this cultural divide requires cross-training, collaboration, and unified governance.

### 7.3 Cost and scalability

#### *7.3.1 Budget constraints*

Implementing comprehensive security solutions across both IT and OT domains can be costly. Expenses include:

- Hardware upgrades (e.g., secure PLCs, firewalls)
- Software licenses (e.g., IDS/IPS, SIEM)
- Training and staffing
- Organizations must balance security investments with operational budgets, often prioritizing short-term functionality over long-term resilience.

#### *7.3.2 Scalability of security solutions*

As CPS environments grow in complexity and scale, security solutions must adapt accordingly. Challenges include:

- Managing a growing number of endpoints and sensors
- Ensuring consistent policy enforcement across distributed sites
- Scaling monitoring and incident response capabilities

## 8 Discussion

The convergence of IT and OT networks in CPS represents a transformative shift in how industrial and critical infrastructure systems are designed, operated, and secured. This chapter reflects on the broader implications of the research, acknowledges its limitations, and outlines directions for future work.

### 8.1 Implications

#### *8.1.1 Industry impact*

The integration of IT and OT enables analytics based on real-time data, predictive maintenance, and increases operational efficiency [1]. However, it also introduces new vulnerabilities that require robust security architectures. Industries such as manufacturing, energy, transportation, and healthcare must adopt layered security strategies to protect against cyber threats without compromising operational continuity.

#### *8.1.2 Policy and governance*

The findings underscore the need for unified cybersecurity policies that bridge the gap between IT and OT domains. Regulatory frameworks like NIST, IEC 62443, and ISO/IEC 27001 must be adapted and enforced across sectors to ensure consistent security postures. Governments and industry bodies should collaborate to develop sector-specific guidelines and compliance mechanisms.

#### *8.1.3 Future CPS design*

Security must be embedded into the design phase of CPS rather than added as an afterthought. This includes secure-by-design hardware, protocol-aware firewalls, and AI-driven anomaly detection systems. Future CPS architectures should prioritize modularity, scalability, and resilience to adapt to evolving threats.

### 8.2 Limitations

While this research provides a comprehensive overview of secure CPS architecture, several limitations must be acknowledged:

1. Scope of Case Studies: The analysis focused on a limited number of high-profile incidents. Broader empirical studies across different industries could provide deeper insights.
2. Technology Assumptions: The proposed frameworks assume the availability of modern hardware and software, which may not be feasible in all legacy environments.
3. Simulation and Validation: Due to the conceptual nature of the work, proposed models and strategies are not validated through real-world deployment or simulation.

### 8.3 Future work

To build upon this research, the following areas are recommended for further exploration:

1. AI-Driven Security: Explore the use of machine learning for real-time threat detection and adaptive response in CPS environments.
2. Digital Twin Integration: Explore how digital twins can be used to simulate and test security architectures before deployment.
3. Cross-Domain Policy Enforcement: Develop frameworks for unified policy management across IT and OT systems, including automated compliance auditing.
4. Human Factors: Study the impact of organizational culture, training, and human error on the effectiveness of CPS security strategies.

## 9 Conclusion

This research explored the multifaceted challenges and solutions associated with securing the convergence of IT and OT in CPS. Key contributions include:

1. Architectural Insights: The use of the Purdue Model to structure CPS environments and highlight integration points between IT and OT.
2. Threat Analysis: A detailed examination of the evolving threat landscape, including ransomware, insider threats, and advanced persistent threats (APTs).
3. Security Frameworks: Evaluation of regulatory standards such as NIST, IEC 62443, and ISO/IEC 27001, along with policy models like Role-Based Access Control (RBAC) and Zero Trust Architecture (ZTA).
4. Design Strategies: Recommendations for secure architecture design, including segmentation, firewalls, IDS/IPS, and resilience mechanisms.
5. Implementation Challenges: Identification of technical, organizational, and financial barriers to secure IT/OT integration.

As CPS become increasingly central to critical infrastructure and industrial operations, the secure convergence of IT and OT is no longer optional—it is imperative. The complexity of these systems demands a holistic approach that combines technical controls, governance frameworks, and cross-disciplinary collaboration.

Security must be embedded into the design, deployment, and operation of CPS from the outset. Organizations must invest in not only technology but also in people and processes to build a culture of cybersecurity that spans both IT and OT domains.

Ultimately, the future of CPS depends on our ability to create architectures that are not only intelligent and efficient but also resilient and secure.

## Abbreviations

| Acronym | Meaning |
|---|---|
| ACL | Access Control Lists |
| ADMS | Advance Distribution Management System |
| APT | Advanced Persistent Threats |
| CERT | Cyber Emergency Response Team |
| CPS | Cyber Physical System |
| CRM | Customer Relationship Management |
| CSF | Cybersecurity Framework |
| DCS | Distributed Control System |
| DMZ | Demilitarized Zone |
| ERP | Enterprise Resource Planning |
| IACS | Industrial Automation and Control Systems |
| ICS | Industrial Control Systems |
| IDS | Intrusion Detection System |

| Acronym | Meaning |
|---|---|
| IEC | International Electrotechnical Commission |
| IIoT/IoT | (Industrial) Internet of Things |
| IPS | Intrusion Prevention System |
| ISA | Instrument Society of America |
| ISMS | Information Security Management System |
| IT | Informational Technology |
| NIST-SP | National Institute of Standards and Technology-Special Publications |
| NSTAC | National Security Telecommunications Advisory Committee (US) |
| OT | Operational Technology |
| PERA | Purdue Enterprise Reference Architecture |
| PLC | Programmable Logic Controller |
| RBAC | Role-Based Access Control |
| SCADA | Supervisory Control and Data Acquisition |
| ZTA | Zero Trust Architecture |

## References


1. A. Buja, Cybersecurity of Industrial Internet of Things (IIoT), 1st ed., CRC Press, Boca Raton, 2025.
2. L. Maglaras, H. Janicke, M.A. Ferrag, Combining security and reliability of critical infrastructures: The concept of securability. Appl. Sci. **12**, 10387 (2022). https://doi.org/10.3390/app122010387
3. J. Hajda, R. Jakuszewski, S. Ogonowski, Security challenges in industry 4.0 PLC systems. Appl. Sci. **11**, 9785 (2021). https://doi.org/10.3390/app11219785
4. A. Ara, Security in supervisory control and data acquisition (SCADA) based industrial control systems: Challenges and solutions, In IOP Conference Series: Earth and Environmental Science, IOP Publishing, Riyadh, Saudi Arabia, May 1 (2022), 012030
5. G.M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, J. Benjamin, Industrial and critical infrastructure security: Technical analysis of real-life security incidents. IEEE Access **9**, 165295-165325 (2021). https://doi.org/10.1109/ACCESS.2021.3133348
6. I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou, Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access **9**, 29775-29818 (2021). https://doi.org/10.48550/arXiv.2101.10198
7. S. Kumar, H. Vardhan, Cyber security of OT networks: A tutorial and overview. arXiv 2502.14017 (2025). https://doi.org/10.48550/arXiv.2502.14017
8. Claroty, The global state of CPS security 2024: Business impact of disruptions, Claroty, Survey Report, March 2024. https://web-assets.claroty.com/resource-downloads/cps-survey-business-disruptions.pdf
9. TXOne Networks, The Crisis of Convergence: OT/ICS Cybersecurity in 2023, Annual Report, 2023.
10. M.A. Umer, K.N. Junejo, M.T. Jilani, A.P. Mathur, Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. Int. J. Crit. Infrastruct. Prot. **38**, 100516 (2022). https://doi.org/10.1016/j.ijcip.2022.100516
11. S.A. Varghese, A.D. Ghadim, A. Balador, Z. Alimadadi, P. Papadimitratos, Digital Twin-based Intrusion Detection for Industrial Control Systems, In 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), IEEE, Pisa, Italy, May 06 (2022), 611-617
12. L. Qudus, Resilient systems: Building secure cyber-physical infrastructure for critical industries against emerging threats. Int. J. Res. Publ. Rev. **6**, 3330–3346 (2025). https://doi.org/10.55248/gengpi.6.0125.0514
13. Alert Enterprises, Cyber Physical Security Convergence, Alert Enterprises, 2024. [Online]. Available: https://alertenterprise.com/wp-content/uploads/2024/03/AE-Security-Convergence-White-Paper-FINAL-high-res-3.4.24-min.pdf
14. A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, A. Urbieta, Securing IIoT using defence-in-depth: Towards an end-to-end secure Industry 4.0. J. Manuf. Syst. **57**, 367-378 (2020). https://doi.org/10.1016/j.jmsy.2020.10.011
15. J.O. del Moral, A. deMarti iOlius, G. Vidal, P.M. Crespo, J.E. Martinez, Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. IEEE Internet Things J. **11**, 30217-30244 (2024). https://doi.org/10.1109/JIOT.2024.3410702
16. C.M. Ahmed, J. Zhou, Challenges and opportunities in CPS security: A physics-based perspective. arXiv: arXiv:2004.03178, (2020). doi: 10.48550/arXiv.2004.03178
17. F. Sechi, Critical Convergence for enhanced safety: A Literature Review on Integrated Cybersecurity Strategies for Information Technology and Operational Technology Systems within Critical Infrastructure, In Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2023), Research Publishing, Singapore (2023), 3414-3421
18. Armis, White Paper: Top 5 Emerging Security Priorities in OT and CPS Environments, Armis, 2025.
19. J. Edwards, Critical Security Controls for Effective Cyber Defense, 1st ed., vol. 1, Apress, Berkeley, CA, 2024. [Online]. Available: https://doi.org/10.1007/979-8-8688-0506-6
20. Fortinet, Securing Cyber-Physical Systems with the Fortinet OT Security Platform, Fortinet, 2024. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-ot-security-platform.pdf