

Intelligent Network Security Models for Connected Engineering Infrastructure

Michał Lewandowski

Professor, Poznan University of Applied Sciences, Poland

Abstract

The rapid integration of Internet of Things devices, industrial control systems, cloud platforms, intelligent sensors, robotics, and data-driven engineering applications has transformed conventional engineering infrastructure into highly connected cyber-physical environments. Although connectivity improves operational efficiency, remote monitoring, automation, and predictive decision-making, it also expands the network attack surface and introduces complex cybersecurity risks. Traditional security approaches based primarily on static rules and perimeter protection are increasingly inadequate for dynamic engineering environments in which devices, users, applications, and data continuously interact. This paper examines intelligent network security models designed for connected engineering infrastructure, with particular emphasis on adaptive threat detection, behavioral analysis, artificial intelligence, access control, network segmentation, and real-time response. A conceptual and analytical research methodology is adopted to identify the major security requirements of connected engineering systems and map them to intelligent security mechanisms.

The study develops a layered security model integrating continuous monitoring, machine-learning-based anomaly detection, identity-aware access control, secure communication, network segmentation, and automated incident response. The analysis indicates that intelligent security models can improve the ability of engineering infrastructures to detect abnormal network behavior, identify emerging threats, and respond to security incidents more rapidly than conventional rule-based approaches. The framework is particularly applicable to smart manufacturing, industrial automation, energy systems, intelligent transportation, infrastructure monitoring, and connected engineering facilities. However, intelligent security implementation introduces challenges involving false positives, adversarial machine learning, data privacy, computational requirements, interoperability, legacy systems, and the explainability of automated decisions. The study concludes that effective protection of connected engineering infrastructure requires a multi-layered and adaptive security architecture rather than dependence on a single security mechanism. Intelligent network security should continuously evaluate system behavior, device identity, communication patterns, and operational context while maintaining appropriate human oversight. The proposed model provides a conceptual foundation for developing resilient engineering networks capable of supporting secure digital transformation.

Keywords: Intelligent network security; Connected engineering infrastructure; Cybersecurity; Machine learning; Anomaly detection; Industrial networks; Intrusion detection; Critical infrastructure; Network monitoring; Cyber-physical systems.

1. Introduction

The increasing convergence of engineering systems and digital technologies has created highly interconnected infrastructures in which physical processes depend extensively on communication networks and computational platforms. Industrial equipment, sensors, programmable controllers, robotic systems, engineering workstations, cloud services, and monitoring applications increasingly exchange information in real time. This connectivity supports automation, predictive maintenance, remote supervision, and data-driven optimization. However, it also creates additional pathways through which unauthorized users, malicious software, compromised devices, and network-based attacks can affect engineering operations.

Connected engineering infrastructure differs from conventional information technology environments because cyber incidents can have direct physical consequences. A compromised industrial controller, for example, may influence machinery behavior, production parameters, energy distribution, or safety systems. Similarly, unauthorized access to engineering networks can expose sensitive design information, operational configurations, and maintenance records. Consequently, cybersecurity mechanisms must protect not only digital information but also the availability, integrity, and safe operation of physical engineering processes.

Traditional network security approaches often rely on predefined signatures, static access rules, firewalls, and perimeter-based controls. Although these mechanisms remain important, they may be insufficient for modern engineering networks characterized by dynamic device populations, heterogeneous protocols, distributed architectures, and rapidly changing communication patterns. Intelligent security models address these limitations by applying machine learning, behavioral analytics, contextual monitoring, and automated response mechanisms to identify deviations from normal system behavior.

Artificial intelligence and machine learning provide opportunities to analyze large volumes of network information generated by connected engineering environments. Instead of depending exclusively on previously identified attack signatures, intelligent systems can establish behavioral baselines and detect anomalous activities. These capabilities can support early identification of unusual communication, unauthorized device interactions, abnormal traffic patterns, and suspicious access behavior. However, intelligent models must be carefully designed because inaccurate classifications may disrupt legitimate engineering operations.

This paper investigates intelligent network security models for connected engineering infrastructure and proposes a layered conceptual framework that combines network monitoring, machine-learning-based anomaly detection, identity-aware access control, segmentation, secure communication, and automated response. The study considers the technical and operational requirements of engineering environments and evaluates how intelligent security mechanisms can strengthen resilience against evolving cyber threats.

2. Objectives

2.1 Enhancing Threat Detection and Network Visibility

The first objective is to examine how intelligent technologies can improve threat detection within connected engineering networks. Modern infrastructure generates large quantities of communication and operational data that can be analyzed to identify unusual behavior. Machine-learning models can evaluate traffic patterns, device interactions, authentication events, and system states to establish

behavioral baselines. Deviations from these baselines can provide indicators of potentially malicious activity that may not be detected effectively through conventional signature-based mechanisms.

The objective also includes improving network visibility across heterogeneous engineering environments. Connected infrastructure may contain legacy controllers, modern IoT devices, cloud platforms, engineering workstations, and specialized communication protocols. Intelligent monitoring can correlate information from these different sources and create a more comprehensive view of network behavior. Such visibility can support earlier identification of security weaknesses, unauthorized connections, abnormal device behavior, and potential attack propagation.

2.2 Developing Adaptive and Resilient Security Models

The second objective is to develop a conceptual security model capable of adapting to changing engineering network conditions. Static security policies may become less effective as new devices, applications, and communication relationships are introduced. An intelligent model should continuously evaluate identity, behavior, context, and network conditions to determine appropriate security responses. Adaptive mechanisms can dynamically modify access decisions, isolate suspicious devices, and prioritize security events according to operational risk.

The objective further considers resilience and continuity of engineering operations. Security controls should prevent or contain cyber threats without unnecessarily interrupting legitimate industrial processes. The proposed model therefore combines automated detection and response with human oversight. This approach enables intelligent systems to perform rapid security actions while allowing engineering and cybersecurity personnel to validate high-impact decisions and maintain operational control.

3. Literature Review

3.1 Cybersecurity in Connected Engineering Systems

The growth of cyber-physical systems and industrial Internet of Things technologies has increased the interdependence between engineering processes and digital networks. Research on industrial cybersecurity has emphasized the importance of protecting control systems against unauthorized access, malware, denial-of-service attacks, manipulation of operational data, and communication-based threats.

Connected engineering environments require security approaches that recognize the relationship between cyber events and physical processes. Traditional IT security models often prioritize information confidentiality, whereas engineering infrastructure must additionally protect process integrity, safety, and availability. Security mechanisms must therefore operate within operational technology environments where system downtime can have significant economic and safety consequences.

3.2 Intelligent Intrusion Detection

Intrusion detection systems traditionally identify malicious behavior using known signatures or predefined rules. Signature-based systems are effective for known threats but may struggle with previously unseen attacks. Intelligent intrusion detection models address this limitation by applying statistical learning, machine learning, deep learning, and behavioral analytics to network data.

Machine-learning approaches can classify network traffic, detect anomalies, and identify deviations from established behavioral patterns. Supervised learning models can distinguish known attack categories when labeled datasets are available, while unsupervised and semi-supervised

approaches can identify previously unknown anomalies. However, model performance depends heavily on data quality, feature selection, training methodology, and environmental changes.

3.3 Zero-Trust and Identity-Centric Security

Zero-trust security principles have become increasingly relevant to connected engineering infrastructure because network location alone cannot reliably establish trust. Devices and users may require continuous verification before accessing sensitive resources. Identity-aware security can combine authentication, authorization, device health, contextual information, and behavioral indicators to determine whether a connection should be permitted.

Within engineering environments, zero-trust principles can be implemented through micro-segmentation, least-privilege access, multi-factor authentication, continuous monitoring, and policy-based authorization. These mechanisms reduce the potential impact of compromised credentials or devices by limiting the resources available to each authenticated entity.

3.4 Artificial Intelligence for Cybersecurity

Artificial intelligence can support cybersecurity through automated classification, anomaly detection, threat prioritization, and response optimization. Deep-learning architectures can process complex network patterns, while ensemble models can combine multiple detection mechanisms. AI-based security systems can also assist security personnel by prioritizing alerts and reducing the workload associated with high-volume network monitoring.

Despite these benefits, AI introduces new security challenges. Attackers may attempt to manipulate training datasets, evade detection models, or generate adversarial inputs designed to cause incorrect classifications. Consequently, intelligent cybersecurity systems require continuous validation, model monitoring, secure data pipelines, and mechanisms for detecting model degradation.

4. Methodology

4.1 Research Design

This study employs a conceptual and analytical research design to investigate intelligent security mechanisms applicable to connected engineering infrastructure. The research identifies the principal cybersecurity requirements of interconnected engineering systems and examines how artificial intelligence, machine learning, network analytics, access control, and automated response mechanisms can address these requirements. The approach focuses on system-level integration rather than evaluating one specific cybersecurity product or algorithm.

The conceptual analysis considers the complete security lifecycle, including asset identification, network observation, anomaly detection, risk assessment, access control, incident response, and recovery. Engineering infrastructure is treated as a cyber-physical environment in which network events may affect physical processes. Consequently, security decisions are evaluated according to both cybersecurity risk and potential operational consequences.

4.2 Intelligent Threat Detection

The second methodological component examines intelligent detection mechanisms. Network traffic, authentication records, device behavior, protocol interactions, and system events are considered potential data sources for machine-learning-based security analysis. Behavioral profiles can be developed to

represent expected communication patterns for individual devices or operational zones. Deviations from established profiles can subsequently be assigned risk scores.

The methodology also considers a combination of supervised and unsupervised learning. Supervised models can identify known attack categories when sufficient labeled data are available, whereas unsupervised models can identify previously unseen anomalies. Combining multiple detection approaches can improve resilience against evolving threats. Nevertheless, detection outputs should be validated against operational context to reduce false positives that could unnecessarily disrupt engineering activities.

4.3 Security Model Components

The proposed model incorporates the following key components:

- **Continuous network monitoring:** Collects traffic and system events across connected engineering infrastructure.
- **Asset and identity management:** Maintains information about authorized users, devices, and applications.
- **Behavioral analytics:** Establishes normal communication and operational patterns.
- **Machine-learning detection:** Identifies anomalous and potentially malicious activities.
- **Network segmentation:** Limits lateral movement between engineering zones.
- **Risk-based access control:** Adjusts permissions according to identity, context, and security status.
- **Automated response:** Isolates or restricts suspicious entities when predefined risk thresholds are reached.
- **Human oversight:** Enables cybersecurity and engineering personnel to validate critical decisions.
- **Recovery mechanisms:** Support restoration of affected systems after security incidents.

These components are designed to operate as an integrated security architecture. The model emphasizes continuous assessment rather than one-time authentication or perimeter protection.

4.4 Framework Development

The final methodological stage develops a layered intelligent network security framework. The first layer establishes asset visibility and identity management. The second layer collects network and operational telemetry. The third layer applies intelligent analytics to identify abnormal behavior. The fourth layer performs contextual risk assessment and determines whether an event requires intervention. The fifth layer executes security responses such as access restriction, device isolation, or traffic filtering.

The framework also includes a feedback mechanism through which security outcomes are evaluated and detection models are periodically updated. This feedback is important because engineering environments evolve as equipment, software, network configurations, and operational processes change. A continuously maintained model can therefore remain more relevant than a static security configuration. Human review remains integrated into the architecture for high-risk decisions and model governance.

5. Analysis

5.1 Layered Intelligent Security Architecture

A connected engineering environment requires multiple security layers because no single mechanism can adequately address all attack scenarios. The proposed architecture begins with asset and identity management, ensuring that devices and users are known before network activity is evaluated.

Continuous monitoring then collects information about traffic, authentication, device interactions, and operational events.

The intelligent analytics layer processes this information to identify deviations from expected behavior. Detected events are evaluated according to contextual risk, considering factors such as device importance, communication destination, time, historical behavior, and operational state. High-risk activities can trigger automated containment mechanisms, while uncertain events can be forwarded to security personnel for review.

Table 1: Layers of the Proposed Intelligent Network Security Model

Security Layer	Main Function	Expected Security Contribution
Asset Identification	Identifies connected devices and systems	Improves infrastructure visibility
Identity Management	Verifies users and devices	Reduces unauthorized access
Network Monitoring	Collects traffic and event data	Enables continuous observation
Behavioral Analytics	Establishes normal activity patterns	Detects deviations
AI/ML Detection	Classifies suspicious activities	Improves threat identification
Risk Assessment	Evaluates contextual severity	Prioritizes security events
Network Segmentation	Separates critical zones	Limits attack propagation
Automated Response	Applies predefined containment actions	Reduces response time
Human Oversight	Reviews high-impact decisions	Prevents inappropriate automation
Recovery	Restores affected resources	Supports operational resilience

Interpretation: The layered architecture demonstrates that intelligent network security depends on coordinated security functions. Asset identification and identity management establish a trustworthy foundation, while monitoring and behavioral analytics provide the information required for intelligent detection. Network segmentation limits the consequences of compromised devices, and automated response reduces the time required to contain threats.

Human oversight remains important because engineering operations can be sensitive to unnecessary intervention. The combination of these layers therefore provides a more resilient approach than relying exclusively on firewalls, antivirus systems, or individual intrusion detection tools.

5.2 Intelligent Detection and Risk Prioritization

Machine-learning-based detection can improve the identification of abnormal activities in engineering networks by analyzing multiple variables simultaneously. For example, a device that normally communicates with a limited set of controllers may generate a high-risk event if it suddenly establishes connections with unfamiliar systems. Similarly, unusual authentication times, traffic volumes, protocol usage, or command sequences may indicate compromise.

Risk prioritization is essential because not every anomaly represents a cyberattack. Engineering systems naturally generate unusual events during maintenance, commissioning, upgrades, or process changes. Intelligent security models should therefore combine anomaly scores with contextual information before initiating disruptive responses. This approach can reduce false positives and enable security teams to focus on events with the greatest potential operational impact.

5.3 Security Performance and Operational Resilience

The effectiveness of an intelligent security model can be evaluated using indicators such as detection accuracy, false-positive rate, response time, attack containment, system availability, and recovery performance. Security systems that detect threats accurately but generate excessive false alarms may reduce operational effectiveness. Conversely, systems with very restrictive thresholds may overlook subtle attacks.

Table 2: Key Evaluation Indicators for Intelligent Engineering Network Security

Indicator	Purpose	Desired Outcome
Detection Accuracy	Measures correct threat identification	High identification reliability
False-Positive Rate	Measures incorrect alerts	Minimal unnecessary intervention
Detection Latency	Measures time to identify threats	Rapid detection
Response Time	Measures time to initiate containment	Fast incident response
Attack Containment	Measures spread prevention	Limited network impact
System Availability	Measures operational continuity	High availability
Model Adaptability	Measures response to changing behavior	Continuous effectiveness
Explainability	Supports understanding of AI decisions	Improved trust
Recovery Time	Measures restoration speed	Rapid service recovery
Scalability	Measures performance as infrastructure grows	Sustainable expansion

Interpretation: The evaluation indicators show that intelligent cybersecurity performance should not be measured solely through detection accuracy. Response speed, false-positive rates, attack containment, availability, explainability, and recovery are equally important in engineering environments. A highly accurate model may still be unsuitable if it produces delayed responses or disrupts critical processes through excessive false alarms. A balanced evaluation approach should therefore consider security effectiveness and operational continuity simultaneously.

6. Discussion

6.1 Advantages of Intelligent Network Security

Intelligent network security models provide several advantages for connected engineering infrastructure. Continuous monitoring enables organizations to maintain greater visibility of device behavior and communication patterns. Machine-learning techniques can identify subtle deviations that may not match predefined attack signatures. This can strengthen the ability of engineering organizations to detect emerging threats before they develop into major operational incidents.

Another advantage is adaptive risk management. Instead of assigning permanent trust based only on network location, intelligent systems can evaluate identity, behavior, context, and current security conditions. A device that becomes compromised can therefore be subjected to additional verification or temporary isolation. Such adaptability is particularly useful in large engineering environments where devices and communication relationships change continuously.

6.2 Balancing Automation and Human Decision-Making

Automated cybersecurity response can significantly reduce incident response time. When a high-confidence threat is detected, the system can immediately restrict communication, isolate a device, or block suspicious traffic. Rapid containment can prevent attackers from moving laterally through connected engineering systems.

However, complete automation can introduce operational risks. A legitimate engineering activity may appear anomalous to a machine-learning model, and an automatic shutdown could interrupt critical operations. Human oversight should therefore remain part of high-impact security decisions. Intelligent systems should prioritize and recommend responses while allowing authorized personnel to intervene when operational context requires a different action.

6.3 Integration with Engineering Technologies

Intelligent network security can be integrated with IoT platforms, digital twins, industrial control systems, cloud infrastructure, robotics, and predictive-maintenance systems. These technologies generate extensive operational data that can improve security visibility. Conversely, security information can strengthen the reliability of connected engineering applications by identifying compromised devices and suspicious data sources.

The integration of security analytics with digital engineering platforms can also support context-aware threat detection. For example, security models can distinguish between normal maintenance traffic and unexpected communication during critical production periods. This contextual awareness can improve detection quality and reduce unnecessary intervention.

7. Challenges

One major challenge is the presence of heterogeneous devices and communication protocols. Connected engineering infrastructure may contain modern IoT devices alongside legacy controllers and specialized industrial equipment. Some legacy systems may have limited computational resources or lack modern authentication capabilities. Integrating intelligent security mechanisms without affecting operational performance therefore requires carefully designed monitoring and gateway architectures.

Another challenge is the quality and availability of cybersecurity data. Machine-learning systems require representative datasets for training and validation. Engineering networks may generate highly specialized traffic that differs from publicly available cybersecurity datasets. Inadequate training data can lead to poor detection performance and excessive false positives. Organizations therefore need secure mechanisms for collecting, labeling, and updating network-security datasets.

Adversarial attacks against AI models represent another significant concern. Attackers may deliberately manipulate network behavior or training information to evade detection. Model poisoning, adversarial inputs, and data manipulation can reduce the reliability of intelligent security systems. Robust training, anomaly-resistant learning, model validation, and continuous monitoring are therefore required.

A further challenge involves explainability. Engineering managers and cybersecurity personnel may hesitate to trust automated decisions when machine-learning models cannot clearly explain why an event was classified as malicious. Explainable AI techniques can help provide understandable evidence for security decisions. This is particularly important when automated responses could affect production processes, safety systems, or critical infrastructure availability.

8. Future Research

Future research should investigate adaptive machine-learning architectures capable of maintaining reliable detection performance as engineering networks evolve. Connected infrastructures frequently experience changes in devices, software, traffic patterns, and operational procedures, which can cause model drift. Research should therefore explore online learning, continual learning, federated learning, and automated model validation approaches. These techniques could enable intelligent security systems to update behavioral profiles without requiring complete retraining. Experimental studies using realistic industrial network environments would be valuable for evaluating the accuracy, stability, and computational requirements of adaptive models.

Another promising research direction is the integration of intelligent security with digital twins and engineering simulation environments. Digital twins can provide contextual information about expected physical and operational behavior, allowing cybersecurity systems to distinguish legitimate changes from suspicious activities. Future models could correlate network anomalies with physical-process states to improve threat classification. Such integration could enable security systems to identify attacks that appear normal at the network level but create abnormal physical consequences, strengthening protection of cyber-physical engineering systems.

Future studies should also examine collaborative and privacy-preserving cybersecurity architectures. Engineering organizations may be reluctant to share raw security data because it can reveal proprietary operational information. Federated learning and privacy-preserving analytics could allow multiple organizations to improve threat-detection models without directly exchanging sensitive datasets. Research should evaluate the effectiveness, communication requirements, governance

implications, and security of such approaches across engineering supply chains and interconnected industrial infrastructures.

9. Limitations

This study presents a conceptual intelligent network security model and does not include implementation within a live industrial engineering environment. Consequently, the proposed architecture has not been experimentally evaluated against real-time attacks, heterogeneous industrial protocols, or operational constraints. Performance indicators such as detection accuracy, response latency, computational overhead, and false-positive rates therefore require validation through future experimental studies.

Another limitation is that intelligent cybersecurity effectiveness depends heavily on the quality of available data. Engineering environments differ significantly in their network configurations, device populations, operational patterns, and security policies. A machine-learning model developed for one environment may not perform equally well in another. This limits the generalizability of results derived from theoretical analysis.

The proposed framework also assumes that appropriate identity management, monitoring infrastructure, and security governance are available. Organizations with outdated infrastructure may face substantial costs when implementing these capabilities. Furthermore, automated security responses can introduce operational risks if machine-learning models incorrectly classify legitimate engineering activities. Human validation and carefully defined response thresholds are therefore necessary before deployment in safety-critical environments.

10. Conclusion

Connected engineering infrastructure has created substantial opportunities for automation, remote management, intelligent monitoring, and data-driven decision-making, but it has simultaneously expanded the cybersecurity attack surface. Conventional perimeter-based and signature-oriented security mechanisms remain valuable but are increasingly insufficient for complex environments containing heterogeneous devices, industrial controllers, cloud platforms, and cyber-physical systems. Intelligent network security models provide a more adaptive approach by combining continuous monitoring, behavioral analytics, machine learning, identity-aware access control, network segmentation, and automated response.

The proposed framework demonstrates that effective engineering cybersecurity should operate through multiple coordinated layers. Asset identification and identity management establish visibility and accountability, while intelligent analytics detect abnormal behavior. Risk assessment adds operational context, segmentation limits attack propagation, and automated response supports rapid containment. At the same time, human oversight remains essential for high-impact decisions because engineering environments can be highly sensitive to unnecessary system intervention.

Overall, intelligent network security represents an important foundation for resilient connected engineering infrastructure. Future implementation should emphasize adaptive learning, explainable security decisions, interoperability with legacy systems, privacy-preserving analytics, and integration with digital twins and other engineering technologies. Rather than replacing established cybersecurity mechanisms, intelligent models should complement them through continuous analysis and context-aware protection. Properly designed and governed intelligent security architectures can enable engineering organizations to achieve stronger cyber resilience while maintaining the reliability, availability, and operational continuity required by modern connected infrastructure.

References

1. Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, 165, Article 106946. <https://doi.org/10.1016/j.comnet.2019.106946>
2. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 101, 1–12. <https://doi.org/10.1016/j.compind.2018.04.015>
3. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>
4. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831. <https://doi.org/10.1109/JIOT.2017.2703172>
5. Ijure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), 498–506. <https://doi.org/10.1016/j.cose.2006.03.008>
6. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys*, 54(11s), Article 229. <https://doi.org/10.1145/3510410>
7. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52–80. <https://doi.org/10.1016/j.ijcip.2015.02.002>
8. Knapp, E. D., & Langill, J. T. (2015). *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems* (2nd ed.). Syngress.
9. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5), 1039–1057. <https://doi.org/10.1109/JPROC.2015.2512234>
10. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>
11. National Institute of Standards and Technology. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82, Revision 3). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-82r3>
12. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
13. Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82, Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r1>
14. Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans*, 38(4), 853–865. <https://doi.org/10.1109/TSMCA.2008.923862>
15. Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. In 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (pp. 380–388). IEEE. <https://doi.org/10.1109/iThings/CPSCoM.2011.34>

16. Agrawal, N., & Kumar, R. (2022). Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. *ISA Transactions*, 130, 10–24. <https://doi.org/10.1016/j.isatra.2022.03.018>
17. Sun, Z., Chen, G., Ding, Y., & Yang, S.-H. (2024). Joint safety and security risk analysis in industrial cyber-physical systems: A survey. *IET Cyber-Physical Systems: Theory & Applications*, 9(4), 334–349. <https://doi.org/10.1049/cps2.12095>
18. Cyber-physical systems security: A systematic review. (2024). *Computers & Industrial Engineering*, 188, Article 109891. <https://doi.org/10.1016/j.cie.2024.109891>
19. A survey on security control and attack detection for industrial cyber-physical systems. (2018). *Neurocomputing*, 275, 1674–1683. <https://doi.org/10.1016/j.neucom.2017.10.009>
20. A survey on attack detection, estimation and control of industrial cyber-physical systems. (2021). *ISA Transactions*. <https://doi.org/10.1016/j.isatra.2021.02.012>