International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry

Suchismita Chatterjee

M.S.-University of North Texas| Cyber Security Product Specialist

Abstract

The increasing complexity of Advanced Persistent Threats (APTs) poses significant risks to the security of Supervisory Control and Data Acquisition (SCADA) systems, particularly within critical infrastructure sectors like oil and gas. These systems are essential for operational continuity and safety, making them prime targets for cyber attackers seeking to disrupt services. As such, it is crucial to implement robust cybersecurity risk management frameworks, in alignment with guidelines from the North American Electric Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST). This paper investigates vulnerabilities within SCADA systems, evaluates the effectiveness of existing regulatory frameworks, and explores strategies to enhance resilience against APTs. By analyzing the interplay between regulatory compliance and technological advancements, the article aims to provide valuable insights for strengthening the security of critical infrastructure in the face of escalating cyber threats.

Keywords: —Advanced Persistent Threats (APTs), SCADA Systems, Oil and Gas Industry, Critical Infrastructure, NERC Guidelines, Risk Management, AWS Lambda, Cybersecurity.

1. Introduction

Advanced Persistent Threats (APTs) pose a significant and evolving risk to SCADA (Supervisory Control and Data Acquisition) systems, especially in critical sectors like the oil and gas industry, where operational continuity is paramount. APTs are characterized by their stealth, persistence, and sophisticated attack methods, making them particularly dangerous to SCADA systems that control and monitor essential infrastructure. The convergence of Information Technology (IT) and Operational Technology (OT) within these systems has increased their vulnerability, exposing previously isolated systems to a wider range of attack vectors.

The rising complexity of cyber threats demands comprehensive risk management strategies that address both technical vulnerabilities and human factors. While frameworks such as those from the North American Electric Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST) provide foundational guidelines for enhancing cybersecurity, the dynamic nature of APTs requires continuous adaptation to ensure the protection of critical infrastructure. This article investigates the current state of SCADA system cybersecurity within the oil and gas industry, focusing on the risks posed by APTs. It examines existing vulnerabilities, explores how current industry practices align with established cybersecurity frameworks like NERC and NIST, and identifies the challenges in fortifying these systems

against increasingly sophisticated threats. The paper further highlights the need for a dynamic risk management approach that evolves with the threat landscape, ensuring the resilience of SCADA systems and safeguarding critical infrastructure against emerging APT techniques.

II. CHALLENGES IN SECURING SCADA SYSTEMS

The increasing complexity of SCADA systems, particularly in the oil and gas industry, presents significant challenges in managing cybersecurity risks. Remote management capabilities exacerbate these issues, as they rely on potentially less secure communication channels and devices, increasing the likelihood of cyberattacks that could disrupt operations and tarnish reputations. Addressing these vulnerabilities requires a comprehensive strategy encompassing robust security measures, continuous monitoring, and regular training to strengthen cybersecurity resilience in this critical sector.

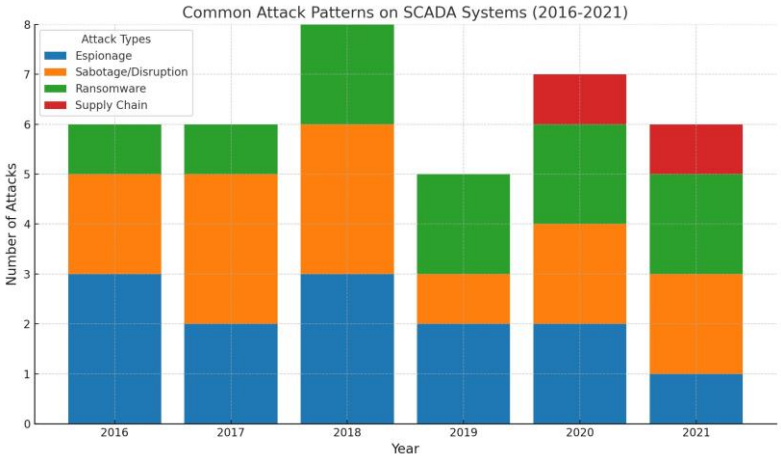

Fig. 1. Common APT Attack Patterns on SCADA Systems (2016-2021). The visualization highlights the evolution of threats, showcasing the consistent rise in espionage and sabotage attacks, alongside the growing prominence of ransomware and supply chain breaches in later years.

Figure 1 illustrates the trends in Advanced Persistent Threats (APTs) targeting SCADA systems [1] between 2016 and 2021. The data categorizes attacks into espionage, sabotage/disruption, ransomware, and supply chain incidents. Espionage and sabotage remain the predominant threats, emphasizing the critical need for enhanced security measures in SCADA environments [2]. The rise of ransomware and the emergence of supply chain attacks in later years further underscore the evolving nature of APTs and their increasing sophistication. These patterns highlight the pressing need for a robust risk management framework tailored to the oil and gas industry.

A. Complexity of SCADA Architecture and Nature of Advanced Persistent Threats

- The complicated structure of SCADA systems exposes serious weaknesses to APTs, especially in the oil and gas industry. The complex, layered setup of SCADA systems, which includes linked elements from field tools to enterprise networks, offers many entry points for possible cyber attackers. APTs take advantage of these weaknesses to break into essential infrastructure, often carrying out long-term spying before launching targeted attacks meant to disrupt systems or steal data. Recent studies show that merging Operational Technology (OT) with information technology (IT) heightens the vulnerabilities in these systems [3], making strong cybersecurity measures necessary that blend technical protections with regulatory compliance as outlined by groups like NERC and NIST. Adding managed services, such as thorough threat management and vulnerability checks, is critical to

strengthening SCADA systems against these advanced threats, ensuring the operational reliability of essential infrastructure in the oil and gas sector.

B. Regulatory and Compliance Constraints

- In the oil and gas sector, securing SCADA systems requires compliance with regulatory frameworks such as NERC and NIST, which serve as both a legal requirement and a strategic defense against APTs [4]. The evolving nature of APTs demands that compliance strategies not only meet current standards but also anticipate future risks. Organizations must proactively integrate compliance into their cybersecurity posture, ensuring adaptability to emerging threats.

Key considerations for effective compliance integration include:

- Real-Time Compliance Management: Compliance protocols must evolve in real-time to address new vulnerabilities. Automation and AI-driven systems can streamline updates, ensuring continuous alignment with evolving standards.

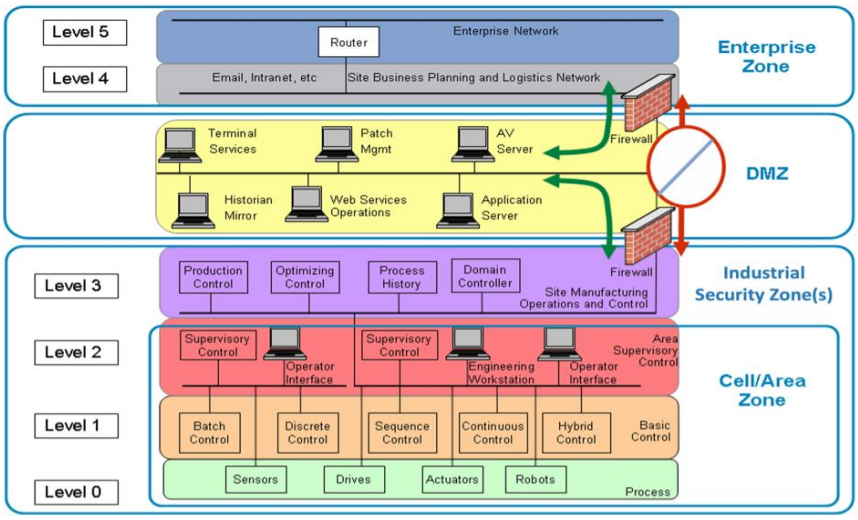

Fig. 2. Layered Network Architecture of Industrial Control Systems. The image illustrates a multi-layered network architecture diagram, depicting various levels of an industrial control system. The architecture is divided into several zones: the Enterprise Zone at the top level, which includes router and networking elements; a Demilitarized Zone (DMZ) featuring firewalls and services such as an AV server and application server; and multiple levels (0-5) that encompass different operational controls and interfaces, including sensor and actuator control, supervisory control, and production control. This hierarchical structure indicates the separation of network functions and security protocols necessary to ensure efficient operations within industrial environments while maintaining cybersecurity across the different zones.

- Dynamic Risk Assessment Models: Risk management frameworks must adapt to the rapid emergence of new attack vectors. Regular reassessment of security controls ensures vulnerabilities are promptly addressed.
- Cross-Jurisdictional Collaboration: Global compliance requires collaboration across regions, ensuring organizations meet both local and international standards while enhancing collective cybersecurity resilience.
- Embedding Compliance in Cybersecurity Culture: Compliance must be ingrained within organizational culture. Ongoing training and awareness programs ensure the workforce remains aligned with regulatory shifts and security best practices.

III. RISK MANAGEMENT FRAMEWORK FOR APTS

Developing a comprehensive Risk Management Framework tailored to APTs is essential for protecting critical infrastructure within the oil and gas sector. This framework must incorporate standards from both NERC and NIST, emphasizing active risk assessment and incident response planning. NERC guidelines advocate for systematic identification of vulnerabilities, evaluation of potential cyber threat impacts, and the implementation of robust protective controls specifically targeting APTs [17]. Concurrently, NIST's cybersecurity framework underscores the necessity of continuous monitoring and dynamic risk management to counter evolving threats.

By integrating regulatory approaches, the framework enhances the resilience of SCADA systems against sophisticated threats, ensuring both operational continuity and the protection of national security.

A. Risk Identification and Assessment

Effective risk identification and assessment are fundamental to defending SCADA systems in the oil and gas industry from APTs. A structured approach is required to evaluate both physical and cyber vulnerabilities in SCADA components—such as Supervisory Control Servers, Remote Terminal Units (RTUs), and communication networks [6]. The following steps outline how risk identification can be effectively conducted:

- Vulnerability Mapping: Use threat modeling tools to identify and categorize vulnerabilities within SCADA components. This includes assessing weak points in communication protocols (e.g., Modbus, DNP3) and legacy systems often targeted by APTs.
- Attack Surface Analysis: Conduct an in-depth analysis of the SCADA architecture, focusing on the attack surface. This involves evaluating the exposure of SCADA systems to both internal and external threats, including internet-facing components and remote access points.
- Risk Scoring: Implement risk scoring models based on the likelihood and potential impact of identified threats. This model should consider the interdependencies of SCADA components, highlighting critical vulnerabilities with high cascading risks.
- Simulated Attack Scenarios: Perform regular red team exercises and penetration testing to simulate APT scenarios. This helps in identifying potential gaps in detection, response mechanisms, and system resilience.
- Asset and Dependency Mapping: Identify all critical assets and their dependencies within the SCADA system [7]. Understanding how each component (e.g., PLCs, field devices) interacts with others enables accurate risk assessment and prioritization.

These techniques enable organizations to identify vulnerabilities, prioritize risk mitigation, and enhance SCADA system security, preventing APT attacks and safeguarding critical infrastructure.

B. Proactive Defense Strategies

Proactive identification and assessment of risks in SCADA systems is critical to prevent APTs in critical oil and gas infrastructure.

- AI-powered anomaly detection enables early identification of threats by analyzing operational data for deviations such as abnormal network activity or unauthorized control commands.
- Zero-trust architecture strengthens defenses by enforcing strict access controls and continuously verifying internal and external communications, limiting lateral movement after a breach.
- Regular vulnerability assessments using automated scanners identify system weaknesses and outdated software, enabling timely remediation to reduce APT risks [8].

C. Incident Response Planning

A well-defined incident response framework ensures rapid identification, containment, and recovery from cyber threats while maintaining the integrity of critical operations [9]. Key steps in incident response include:

- Preparation: Establish a specialized incident response team (IRT) with expertise in SCADA architecture, including RTUs, PLCs, and HMIs. Regularly update asset inventories and define clear thresholds for activating the IRT to minimize response time.
- Detection and Analysis: Deploy advanced anomaly detection tools tailored for SCADA traffic, integrating threat intelligence feeds to identify potential APT indicators. Machine learning-based anomaly detection can enhance early threat recognition, such as unusual communication patterns between SCADA components.
- Containment and Eradication: Implement network segmentation and real-time threat mitigation measures to isolate compromised SCADA components, ensuring minimal disruption. Automate threat neutralization through predefined kill chain protocols to maintain service continuity.
- Recovery and Post-Incident Review: Develop detailed recovery procedures from secure, validated backups. Post-incident, conduct a thorough analysis of the attack vector, assess vulnerabilities, and refine the response plan to address identified weaknesses.

Incident response success hinges on seamless coordination between technical and operational teams. Regular APT simulation exercises improve response times and resilience. This approach fortifies SCADA defenses, reduces APT impact, and ensures operational continuity.

IV. TECHNOLOGICAL ENABLERS FOR MITIGATION

Adopting advanced technologies is essential to strengthen SCADA system security in the oil and gas sector, protecting against persistent APTs through a multi-layered defense strategy.

A. AWS Lambda in SCADA Security

AWS Lambda automates real-time security responses within SCADA environments. By triggering predefined actions on detecting anomalies (e.g., unauthorized access), Lambda enables rapid mitigation. Its seamless integration with monitoring systems ensures **dynamic incident response**, minimizing response time without adding infrastructure complexity [10].

B. Adaptive Network Segmentation

Adaptive network segmentation uses AI to analyze traffic in real-time and dynamically isolate compromised zones. This approach prevents lateral movement of APTs by instantly adjusting security policies, offering containment without manual intervention. It is key to defending critical SCADA components from evolving threats [16].

C. AI-Driven Intrusion Detection Systems (IDS)

AI-powered IDS systems enhance traditional detection methods by continuously learning from attack patterns, improving the accuracy of identifying **APT-related anomalies**. This reduces false positives and enhances proactive monitoring, enabling real-time identification of advanced attacks before significant damage occurs [12].

D. Zero-Trust Architecture for SCADA Systems

Zero-Trust Architecture (ZTA) assumes no inherent trust and continuously verifies identities, devices, and network traffic. By enforcing strict access control, ZTA limits exposure to APTs and minimizes lateral movement [13], providing robust defense against insider threats and unauthorized access.

E. Blockchain for Data Integrity

Blockchain ensures the integrity of SCADA system data by creating an immutable ledger. Any unauthorized change to control data or operational logs is instantly detected, providing real-time assurance of data authenticity, and preventing APTs from tampering with critical information [22].

F. Secure Communication Protocols and Threat Intelligence

Using encrypted communication protocols ensures the confidentiality and integrity of SCADA data in transit, mitigating risks of eavesdropping or tampering [23]. Integrated threat intelligence platforms enable real-time analysis of cyber threats, empowering SCADA systems to adapt to evolving attack tactics and proactively prevent APTs.

V. INTERDEPENDENCIES AND COLLABORATIVE APPROACHES

Addressing APTs in SCADA systems for critical oil and gas infrastructure requires a unified approach that integrates technological, regulatory, and operational efforts across multiple stakeholders. Collaborative strategies enhance the agility and depth of defense mechanisms against sophisticated cyber threats [22].

- Real-time Threat Intelligence Sharing: Continuous exchange of actionable threat data across sectors accelerates APT detection and response, minimizing attack impact and ensuring synchronized defense.
- Coordinated Incident Response: Centralized Security Operations Centers (SOCs) enable swift, unified mitigation, ensuring seamless collaboration between operators, regulators, and security teams for efficient APT management.
- Regulatory Synergy: Close coordination between industry regulators and private sectors enables dynamic policy evolution. Real-time updates to frameworks like NERC and NIST ensure timely adaptation to emerging APT tactics.
- Supply Chain Integration: Collaborative risk management across the supply chain ensures rapid identification and containment of vulnerabilities, preventing lateral movement of APTs through interconnected systems.
- Blockchain for Compliance and Transparency: Blockchain enhances trust and accountability in SCADA systems, ensuring data integrity and strengthening compliance with evolving regulatory standards.

These collaborative frameworks ensure SCADA systems remain resilient, adaptive, and secure, safeguarding critical infrastructure from evolving cyber threats.

VI. PROJECT MANAGEMENT FOR CYBERSECURITY IMPLEMENTATION

Effective project management is essential to securing SCADA systems in the oil and gas industry. A structured, risk-based approach ensures that cybersecurity plans are tailored to the unique vulnerabilities of SCADA systems. By leveraging artificial intelligence (AI) for threat detection, project managers can enhance incident response capabilities, enabling proactive identification and neutralization of APTs before they cause damage [17]. Implementing real-time monitoring and adaptive security measures helps in dynamically countering emerging threats and minimizing system downtime.

A. Role of Project Management Teams and Measuring Success

Project management teams play a crucial role in addressing cybersecurity challenges in SCADA systems by integrating risk management with operational goals. They do this by creating a collaborative environment where cybersecurity strategies align with organizational priorities. Using methodologies like the Balanced Scorecard, they measure success through specific, quantifiable cybersecurity metrics that

track vulnerability reduction and incident response effectiveness [18]. Continuous communication with stakeholders ensures a responsive approach to threat mitigation, adapting to evolving cyber risks and ensuring sustained resilience against APTs.

B. Practical Applications for APT Mitigation

Innovative cybersecurity strategies such as network segmentation and AI-powered anomaly detection are vital for mitigating APTs in SCADA systems. Network segmentation isolates critical systems, limiting the spread of attacks and reducing the impact on essential operations. AI-driven detection tools continuously learn and adapt, identifying attack patterns that may go unnoticed by traditional systems. Additionally, dynamic incident response frameworks ensure that potential threats are swiftly contained, limiting their ability to disrupt system functions [23]. These strategies, supported by regular security drills and vulnerability assessments, offer robust defense mechanisms against sophisticated cyber threats.

C. Collaboration Between IT and OT Security Teams

Collaboration between IT and OT security teams is essential for effective cybersecurity implementation. By sharing threat intelligence and expertise, these teams ensure that both operational technology (OT) and information technology (IT) systems are protected in a unified manner. Joint risk assessments allow for identifying cross-domain vulnerabilities, while integrated security policies and tools enable seamless protection of SCADA systems from evolving APT tactics. This collaboration fosters a proactive security posture, ensuring that all layers of the infrastructure remain resilient against advanced attacks.

VII. TECHNICAL ILLUSTRATIONS AND DATA ANALYSIS

Technical illustrations and data analysis serve as pivotal tools for uncovering vulnerabilities and fortifying SCADA systems against Advanced Persistent Threats (APTs). By employing precise diagnostic and analytical methodologies, stakeholders can translate complex operational risks into actionable insights. This section delves into targeted approaches to visualize and address vulnerabilities within SCADA components.

A. Dynamic Vulnerability Mapping for SCADA Systems

Dynamic vulnerability mapping leverages real-time data and predictive analytics to identify weak points in SCADA systems. This method involves:

- Data Aggregation: Continuous monitoring of PLCs, RTUs, and HMIs to collect operational data, flagging anomalous behaviors linked to potential APT activities.
- Heatmap Generation: Using AI-driven tools to create visual overlays that rank system vulnerabilities based on exploitation probability, enabling teams to focus on high-risk zones.
- Temporal Analysis: Tracking vulnerability shifts over time, aiding in proactive patching and configuration hardening.

This approach provides actionable insights by aligning real-time vulnerabilities with evolving APT strategies, reducing the attack surface [18].

B. Incident Trends and Root Cause Analysis

Understanding incident trends is critical for mitigating future risks. A robust root cause analysis (RCA) can be implemented through:

- Causal Loop Diagrams: Highlight interdependencies among SCADA components to identify cascading failure patterns exploited by APTs.
- Forensic Analysis: Utilize network traffic logs and event sequences to pinpoint the exact ingress vector of previous attacks.

- Mitigation Simulation: Simulate hypothetical APT scenarios using digital twins to evaluate the effectiveness of existing defenses, enabling refined response plans [14].
- These techniques not only address current vulnerabilities but also adapt defenses for emerging threat vectors.

C. Comparative Analysis of SCADA Security Enhancements

A comparative analysis of SCADA-specific security strategies reveals the operational efficacy of various methodologies:

- Protocol-Specific Firewalls: Enhance security at communication layers by deploying application-aware firewalls tailored to protocols such as Modbus and DNP3.
- Deception Technologies: Deploy decoy nodes within SCADA networks to mislead attackers, capture threat intelligence, and delay APT progression.
- AI-Powered Threat Modeling: Continuously train AI models on simulated APT behaviors to identify patterns and auto-recommend countermeasures for system operators.
- These innovations deliver scalable and adaptive defenses, ensuring robust risk management across SCADA operations [17].

VIII. CONCLUSION AND FUTURE WORK

The dynamic threat landscape targeting SCADA systems in critical infrastructure demands innovative and adaptive cybersecurity measures. This article has provided a detailed exploration of advanced technical strategies to enhance the resilience of SCADA systems, particularly in the oil and gas sector. By integrating real-time diagnostics, advanced analytics, and proactive defense mechanisms, organizations can achieve a robust cybersecurity posture.

A. Key Conclusions

- Strategic Vulnerability Management: Real-time vulnerability mapping, coupled with predictive analytics, empowers organizations to preemptively address weaknesses and minimize attack surfaces.
- Data-Driven Incident Response: The integration of root cause analysis and simulation-driven evaluations facilitates targeted mitigation strategies, reducing response times and operational disruption.
- Adaptive Defense Mechanisms: Techniques such as deception technologies, protocol-specific firewalls, and AI-powered threat modeling provide scalable solutions to counter evolving Advanced Persistent Threats (APTs).
- Focus on Interoperability and Integration: Bridging IT-OT communication gaps through unified frameworks ensures cohesive threat detection and response across SCADA networks.

B. Future Directions

The rapid evolution of cyber threats requires a sustained focus on emerging technologies and collaborative frameworks [15]. Future work should explore:

- AI-Enhanced Detection Systems: Leveraging deep learning models to identify and respond to novel attack patterns with near-zero latency.
- Blockchain for Secure Transactions: Utilizing blockchain technology to ensure data integrity and secure communications across SCADA systems.
- Quantum-Resilient Encryption: Investigating the integration of quantum cryptographic techniques to safeguard critical infrastructure against next-generation cyberattacks.

- Cross-Sector Intelligence Sharing: Establishing collaborative platforms for real-time threat intelligence exchange between industries and regulatory bodies to mitigate sector-wide risks.
- Continuous Workforce Upskilling: Developing tailored training programs for SCADA operators and cybersecurity teams to ensure effective implementation of advanced risk management strategies.

By embracing these directions, the oil and gas sector—and other critical industries—can foster resilient, future-ready SCADA systems capable of withstanding increasingly sophisticated cyber threats. This ongoing commitment to innovation and collaboration will be pivotal in safeguarding essential infrastructure and maintaining operational continuity in a digitally connected world.

REFERENCES

1. X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, ”APT Attack Analysis in SCADA Systems,” *MATEC Web Conf.*, vol. 173, p. 01010, 2018. [Online]. Available: https://doi.org/10.1051/matecconf/201817301010
2. I. Stellios, P. Kotzanikolaou, and M. Psarakis, ”Advanced persistent threats and zero-day exploits in industrial Internet of Things,” *Security and Privacy Trends in the Industrial Internet of Things*, pp. 47-68, 2019, Springer.
3. N. Tariq, M. Asim, and F. A. Khan, ”Securing SCADA-based critical infrastructures: Challenges and open issues,” *Procedia Computer Science*, vol. 155, pp. 612-617, 2019, Elsevier.
4. D. Upadhyay and S. Sampalli, ”SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations,” *Computers & Security*, vol. 89, p. 101666, 2020, Elsevier.
5. S. S. Fortunato, ”Risk management in ICS/SCADA systems to enhance security within the energy sector,” M.S. thesis, Utica College, 2020.
6. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, ”A review of cyber security risk assessment methods for SCADA systems,” *Computers & Security*, vol. 56, pp. 1-27, 2016, Elsevier.
7. A. M. Elhady, H. M. El-Bakry, and A. Abou Elfetouh, ”Comprehensive risk identification model for SCADA systems,” *Security and Communication Networks*, vol. 2019, no. 1, p. 3914283, 2019, Wiley Online Library.
8. J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, ”Current cyber-defense trends in industrial control systems,” *Computers & Security*, vol. 87, p. 101561, 2019, Elsevier.
9. L. Rosa, T. Cruz, P. Simoes, E. Monteiro, and L. Lev, ”Attacking˜ SCADA systems: A practical perspective,” in *Proc. 2017 IFIP/IEEE Symp. Integrated Network and Service Management (IM)*, 2017, pp. 741746, IEEE.
10. A. Mishra, T. Reichherzer, E. Kalaimannan, N. Wilde, and R. Ramirez, ”Trade-offs involved in the choice of cloud service configurations when building secure, scalable, and efficient Internet-of-Things networks,” *Int. J. Distrib. Sensor Networks*, vol. 16, no. 2, p. 1550147720908199, 2020, SAGE Publications.
11. S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, ”Harnessing artificial intelligence capabilities to improve cybersecurity,” *IEEE Access*, vol. 8, pp. 23817-23837, 2020.
12. G. Sharkov, ”A System-of-Systems approach to cyber security and resilience,” *Information & Security*, vol. 37, pp. 69-94, 2017.

13. S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, ”A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions,” *J. Supercomput.*, vol. 75, pp. 4543-4574, 2019.
14. S. S. Fortunato, ”Risk management in ICS/SCADA systems to enhance security within the energy sector,” M.S. thesis, Utica College, Utica, NY, USA, 2020.
15. S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, ”A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions,” *The Journal of Supercomputing*, vol. 75, pp. 4543–4574, 2019.
16. K. Coffey, L. Maglaras, R. Smith, H. Janicke, M. A. Ferrag, A. Derhab, M. Mukherjee, S. Rallis, and A. Yousaf, "Vulnerability assessment of cybersecurity for SCADA systems," in Cybersecurity in Critical Infrastructure Protection, 2018, ISBN: 978-3-319-92624-7
17. G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, ”Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns,” *IEEE Access*, vol. 8, pp. 128440–128475, 2020.
18. S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, ”A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions,” *The Journal of Supercomputing*, vol. 75, pp. 4543–4574, 2019.