Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ **Research Article**

Cybersecurity Threats to Energy Pipelines: How Endpoint Compromise Leads to Operational Disruption

Vilas Shewale
Independent Researcher, USA

ARTICLE INFO

Received: 31 Dec 2025
Revised: 03 Jan 2026

ABSTRACT

The energy pipeline infrastructure faces the threat of advanced cyber-attacks on the national critical infrastructure. Attackers target the vulnerabilities of the endpoints because they constitute the main entry points into the pipeline network. Phishing campaigns and social engineering tactics deceive personnel into executing malicious actions. Contractor devices and third-party connections introduce additional vulnerabilities beyond organizational security controls. Once initial access occurs through compromised endpoints, attackers conduct reconnaissance activities to map network architecture. Lateral movement progresses systematically from enterprise information technology environments toward operational technology systems. Credential harvesting enables authenticated access to jump servers, engineering workstations, and historian databases. Remote access solutions provide pathways for boundary traversal without triggering perimeter alerts. Behavioral analytics and endpoint detection platforms offer visibility into attacker techniques beyond signature-based detection. Application whitelisting constrains unauthorized executable deployment on critical systems. Privilege access management enforces least-privilege principles, limiting credential utility. Network segmentation through industrial demilitarized zones creates monitored chokepoints between enterprise and control system domains. Zero-trust frameworks require continuous authentication verification, eliminating implicit trust assumptions. Incident response planning must address operational continuity while maintaining safe pipeline states. There must be a level of coordination between security teams and operations teams to ensure the implications of physical processes are considered when taking these actions.

Keywords: Endpoint Security, Industrial Control Systems, Pipeline Cybersecurity, Lateral Movement, Operational Technology Protection, Critical Infrastructure Defense

I. INTRODUCTION

Energy pipeline infrastructure is the backbone of the fuel pipeline transport networks. Natural gas and oil products are conveyed using very long pipelines that stretch for thousands of miles. The pipelines link the energy production plants to the refineries and the storage tanks, and the consumers. Pipelines are a very strategic infrastructure that can easily be attacked by an enemy due to the effects it may have on fuel shortages and economic instability. Federal authorities have long recognized pipelines as critical assets requiring dedicated security attention [1].

Pipeline infrastructure faces threats from multiple adversary categories. Nation-state actors use infrastructure targeting to meet their strategic intentions. Criminals use the ransomware tool for financial motives through the deployment of the tool for extortion. Hacktivists focus on the energy domain to meet their ideological goals. Despite the varied motives, the attackers use the same modes in the attack process. Initial access typically occurs through endpoint compromise within corporate networks. Attackers then escalate privileges and move laterally toward operational systems [1].

The operational technology environment within pipeline facilities presents unique security challenges. Supervisory control and data acquisition systems are responsible for the measurement of pipe pressures, flow rates, and valve

positions. These controllers perform an automatic action to ensure safe operating conditions. Remote terminal units collect field data from sensors distributed along pipeline routes. Human-machine interfaces allow operators to visualize system status and issue commands. These components were engineered decades ago with reliability and safety as primary design objectives. Cybersecurity considerations received minimal attention during original system development [2].

Modern pipeline operations require connectivity between enterprise information technology and operational technology domains. To be beneficial, business systems must have access to operational data necessary for such tasks as scheduling, billing, and reporting mandated by government regulations. Remote monitoring capabilities make it possible to monitor geographically dispersed facilities from a central location. Vendor connections support equipment maintenance and software updates. Each connectivity pathway introduces potential attack vectors. The historical air gap separating corporate and industrial networks no longer exists in most pipeline environments [2].

Cyber attacks carried out against the energy and power industry follow known patterns. There is reconnaissance to find weak points of entry. There are phishing emails to trick personnel with authorized access to key systems." Compromised credentials enable authentication to remote access services. Malware establishes persistent footholds within enterprise networks. Attackers then enumerate network architecture to locate pathways toward operational systems. The progression from initial endpoint compromise to operational disruption can occur over weeks or months [2].

The consequences of successful cyber intrusion extend beyond data theft. Attackers gaining access to control systems can manipulate physical processes. Pipeline pressure manipulation risks equipment damage and safety incidents. Unauthorized valve operations can disrupt product flow across entire distribution networks. Even attacks limited to enterprise systems can force operational shutdowns. Operators may halt pipeline activities as a precautionary measure while investigating the intrusion scope. The intersection of cyber and physical domains elevates the stakes for pipeline security [1].

Protecting pipeline infrastructure requires understanding the complete attack lifecycle. Endpoint security serves as the first line of defense against initial compromise. Detection capabilities must identify lateral movement before attackers reach operational systems. Response procedures must account for both cyber and physical safety considerations.

II. RELATED WORK

Existing literature on industrial control system security has established a foundational understanding of vulnerabilities within critical infrastructure environments. Prior contributions have documented attack taxonomies targeting supervisory control and data acquisition systems. Scholars have examined network-based intrusion detection mechanisms for operational technology environments. Machine learning applications for anomaly detection in industrial settings have received considerable attention. However, existing frameworks often treat endpoint compromise and operational technology attacks as separate phenomena. The connection between initial access vectors and ultimate operational impact remains underexplored in current literature.

The present article addresses the gap by tracing the complete attack chain from endpoint compromise through lateral movement to operational disruption. The threat model with an endpoint as the target views vulnerabilities in workstations as essential in facilitating future attacks on industrial control systems. The overall security framework is an integration of behavioral analysis, application control, and privilege management. Network segmentation strategies utilizing industrial demilitarized zones receive detailed treatment within operational contexts. Zero-trust principles receive application specific to pipeline environments where information technology and operational technology convergence creates unique challenges. The incident response coordination model bridges cybersecurity and operations teams through unified command structures. The article synthesizes technical controls with organizational processes to present a holistic defensive posture for pipeline infrastructure protection against sophisticated adversaries.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ **Research Article**

III. ATTACK VECTORS TARGETING PIPELINE ENDPOINTS

A. Phishing and Social Engineering

Phishing is the foremost method of obtaining initial access in pipeline infrastructure. Tailored attacks aim at duping personnel with specific operations. Spear phishing attacks target individuals with high privileges for operational systems. Persons working within the energy industry find themselves targeted by an email that looks like the regulatory body, the supplier, or even the company's mail. This is all related, of its nature, including matters of regulatory audits, operational notifications, and even more. This is more successful since the attack is contextually relevant [3].

The level of technology used in phishing attacks is progressively increasing. The malicious file attachments look like common files such as spreadsheets, technology specifications, or policy notices. The macro-enabled files contain code execution when opened, creating first points of presence for these malicious programs. The executable payloads are disguised to look like common programs for installation or system functions. The harvesting pages mimic actual login pages for email, remote access, or operational applications. The stolen credentials enable attackers to leverage normal authentication functions [3].

Social engineering also encompasses non-electronic communication. Attackers do phone-based pretexting to gain personal data from vulnerable personnel. Another form is physical social engineering, where there is illegal facility entry by tailgating or impersonation.

The human element represents the most vulnerable component within pipeline security architectures. Technical controls cannot fully compensate for employee susceptibility to manipulation. Security awareness training addresses this gap but requires continuous reinforcement to remain effective [3].

The energy sector faces elevated targeting due to its critical infrastructure status. Monitoring and control systems within pipeline facilities present attractive objectives for sophisticated threat actors. Successful phishing attacks against operational personnel can yield credentials for SCADA systems and engineering workstations. The compromise of a single endpoint creates opportunities for deeper network penetration. Initial access through phishing frequently precedes lateral movement toward industrial control environments [3].

B. Contractor and Third-Party Device Risks

Pipeline operations require extensive third-party involvement for specialized functions. Contractors perform equipment maintenance, software updates, and system integration tasks. Vendor technicians connect directly to operational technology networks during service activities. These external parties operate outside the direct security governance of pipeline operators. The devices brought into facilities may lack adequate security configurations or current patch levels [4].

Industrial control system environments face unique challenges regarding third-party access. Legacy systems often require vendor-specific tools and software for maintenance procedures. Remote access capabilities enable contractors to perform support functions without physical presence. Each connection pathway represents a potential entry point for malicious actors. Compromised contractor credentials provide attackers with trusted access to sensitive networks [4].

The supply chain introduces additional risk vectors. Hardware and software components may contain embedded vulnerabilities or malicious code. Firmware updates from compromised vendor systems can propagate threats across multiple facilities. Machine learning approaches offer potential for detecting anomalous contractor behavior patterns. However, distinguishing legitimate maintenance activities from malicious actions presents significant classification challenges. The diversity of normal contractor operations complicates baseline establishment for anomaly detection systems [4].

Effective third-party risk management requires contractual security requirements, device inspection protocols, and network segmentation, limiting contractor access scope. Continuous monitoring of third-party sessions enables the detection of suspicious activities during authorized access windows.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ **Research Article**

Attack Category	Attack Method	Target	Impact
Phishing	Spear-phishing emails	Pipeline personnel	Credential theft and malware deployment
Phishing	Malicious attachments	Employee workstations	Backdoor establishment
Phishing	Credential harvesting pages	Authentication systems	Unauthorized network access
Social Engineering	Telephone pretexting	Operations staff	Sensitive information extraction
Social Engineering	Physical impersonation	Facility access points	Unauthorized facility entry
Third-Party Risk	Contractor device connection	Operational networks	Direct malware introduction
Third-Party Risk	Compromised vendor credentials	Remote access services	Trusted access exploitation
Supply Chain	Malicious firmware updates	Control system components	Widespread threat propagation

Table 1. Primary Attack Methods for Initial Pipeline Network Access [3, 4].

IV. LATERAL MOVEMENT FROM IT TO OT ENVIRONMENTS

Initial endpoint compromise within enterprise networks marks the beginning of a broader intrusion campaign. Attackers rarely achieve operational technology access through direct external attack. The pathway to industrial control systems traverses intermediate network zones and authentication boundaries. Lateral movement describes the systematic progression through interconnected systems toward high-value targets. Pipeline environments present attackers with multiple potential routes from corporate infrastructure to process control networks [5].

Reconnaissance activities follow a successful endpoint compromise. Adversaries enumerate network topology to understand system relationships and trust configurations. Active Directory analysis discloses user account information, group memberships, and administrative access. Scanning a network provides information about active hosts, open ports, and operational services on reachable subnetworks. Attackers map data flows between enterprise applications and operational systems. Historian servers storing process data often maintain connections to both IT and OT domains. These dual-homed systems represent attractive pivot points for boundary traversal [5].

Industrial control system architectures include multiple component categories susceptible to lateral movement exploitation. Programmable logic controllers execute automated control logic for physical processes. Remote terminal units aggregate field device data for transmission to central systems. Human-machine interfaces display operational status and accept operator commands. Supervisory control and data acquisition systems coordinate distributed control elements across geographic areas. Each component type presents distinct vulnerabilities and access requirements. Attackers study these architectures to identify the most efficient pathways toward process manipulation capabilities [5].

Credential harvesting enables authenticated access to protected systems. Memory extraction tools recover passwords and authentication tokens from compromised workstations. Pass-the-hash techniques allow lateral movement

without plaintext password knowledge. Kerberos ticket attacks facilitate domain-wide privilege escalation. Stolen credentials belonging to engineers or operators grant access to systems with direct OT connectivity. Jump servers intended to provide secure access become stepping stones for adversarial progression [6].

Remote access infrastructure presents significant lateral movement opportunities. Virtual private network services extend network connectivity to external locations. Remote desktop protocols enable graphical access to internal workstations. Industrial remote access solutions permit vendor maintenance activities. Each remote access pathway can be exploited using harvested credentials or session hijacking techniques. Attackers leveraging legitimate remote access tools generate traffic patterns resembling authorized activity. Traditional perimeter monitoring fails to detect this boundary-crossing behavior [6].

Engineering workstations occupy critical positions within pipeline network architectures. These systems host configuration software for programmable controllers and safety systems. Direct connections to process control networks enable programming and diagnostic functions. Compromise of an engineering workstation provides attackers with powerful capabilities. Malicious logic can be deployed to controllers governing pipeline operations. Configuration changes may disable safety interlocks or alter setpoint values. The engineering workstation represents the final lateral movement objective before physical process impact becomes achievable [6].

Honeypot deployments within IT-OT boundary zones enable detection of lateral movement attempts. Decoy systems mimicking historians, jump servers, and engineering workstations attract adversary attention. Interaction with honeypot resources generates high-fidelity alerts indicating active intrusion progression.

Movement Phase	Technique	Target System	Objective
Reconnaissance	Active Directory queries	Domain controllers	User and privilege enumeration
Reconnaissance	Network scanning	Enterprise infrastructure	Topology mapping
Reconnaissance	Data flow analysis	Historian servers	IT-OT boundary identification
Credential Access	Memory extraction	Compromised workstations	Password recovery
Credential Access	Pass-the-hash attacks	Authentication services	Lateral authentication
Credential Access	Kerberos ticket attacks	Domain infrastructure	Privilege escalation
Boundary Traversal	VPN credential exploitation	Remote access services	Network segment crossing
Boundary Traversal	Remote desktop hijacking	Jump servers	OT network access
Final Target	Engineering workstation compromise	Configuration software	Process control capability

Table 2. Adversary Progression Techniques Toward Operational Technology Systems [5, 6].

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ **Research Article**

IV. ENDPOINT DETECTION AND PREVENTION STRATEGIES

A. Behavioral Analytics and Threat Hunting

Conventional signature-based anti-virus software is not very effective against sophisticated attackers. Regarded malware is only a small part of the entire risk. This is because attackers regularly update their malware in order to get beyond its signature. This sort of malware is called polymorphic because its code structure alters with each attack. These are zero-day attacks, which work on an unknown vulnerability by the security providers. Behavioral analysis addresses these limitations through activity pattern monitoring rather than static signature matching [7].

Endpoint detection and response platforms provide comprehensive visibility into system activities. Process execution chains reveal parent-child relationships, indicating malicious spawning behavior. Network connection monitoring identifies unauthorized communication with external infrastructure. File system surveillance detects suspicious modifications to critical directories and registry locations. Memory analysis exposes fileless malware operating entirely within volatile storage. The aggregation of these telemetry sources enables the detection of attacker techniques independent of specific tool variants [7].

Industrial control system environments require specialized behavioral baselines. Normal operational patterns differ significantly from enterprise IT workloads. Engineering workstations exhibit distinct process execution profiles during maintenance windows. Human-machine interface systems maintain predictable communication patterns with downstream controllers. Deviations from established baselines warrant investigation regardless of whether known threat signatures exist. Machine learning algorithms assist in establishing and maintaining behavioral profiles across diverse endpoint populations [7].

Threat hunting represents proactive security operations beyond automated detection. Skilled analysts formulate hypotheses about potential adversary presence. Searches across endpoint telemetry seek evidence supporting or refuting these hypotheses. Pipeline-specific threat intelligence informs hunting activities with relevant indicators of compromise. Known attacker toolkits, command and control infrastructure, and tactical procedures guide investigation priorities. Effective threat hunting discovers intrusions that evade automated detection mechanisms [7].

B. Application Control and Privilege Management

Application whitelisting fundamentally constrains attacker capabilities on compromised endpoints. Only preapproved executables receive permission to run. Malicious payloads delivered through phishing fail to execute regardless of user interaction. Unauthorized tools required for reconnaissance and lateral movement cannot operate. The enforcement of application control transforms endpoint compromise from a foothold into a dead end [8].

Critical control system environments benefit particularly from strict application policies. Operational technology endpoints execute limited software sets for defined functions. The stability requirements of industrial systems align naturally with whitelist enforcement. Engineering workstations require broader application permissions but still benefit from controlled execution environments. Careful policy development balances security restrictions with operational functionality requirements [8].

Privilege management complements application control through access limitation. Least-privilege principles restrict user permissions to the minimum necessary levels. Administrative credentials receive protection through privileged access management solutions. Just-in-time privilege elevation grants temporary permissions for specific tasks. Credential vaulting prevents exposure of sensitive authentication material. Session recording creates audit trails documenting all privileged activities [8].

The combination of behavioral monitoring, application control, and privilege management creates defense in depth. Each layer addresses distinct attack phases and techniques. Adversaries must overcome multiple barriers to progress from initial access toward operational impact. Pipeline security architectures integrating these endpoint protections significantly increase attacker cost and detection probability.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ Research Article

Strategy Category	Security Control	Function	Defensive Benefit
Behavioral Analytics	Process execution monitoring	Track parent-child relationships	Malicious spawning detection
Behavioral Analytics	Network connection surveillance	Monitor external communications	Command and control identification
Behavioral Analytics	File system monitoring	Detect suspicious modifications	Malware activity detection
Behavioral Analytics	Memory analysis	Examine volatile storage	Fileless malware exposure
Threat Hunting	Hypothesis-driven investigation	Proactive adversary search	Pre-detection intrusion discovery
Threat Hunting	Threat intelligence integration	Apply known indicators	Targeted threat identification
Application Control	Executable whitelisting	Restrict program execution	Malware execution prevention
Privilege Management	Least-privilege enforcement	Limit user permissions	Lateral movement constraint
Privilege Management	Credential vaulting	Protect the authentication material	Credential theft prevention
Privilege Management	Session recording	Document privileged activities	Audit trail creation

Table 3. Detection and Prevention Mechanisms for Pipeline Endpoints [7, 8].

V. INTEGRATED DEFENSE FOR PIPELINE CONTINUITY

Pipeline cybersecurity demands architectural strategies extending beyond individual security tools. Point solutions addressing specific threats provide incomplete protection. Adversaries adapt techniques to circumvent isolated defensive measures. Integrated security architectures coordinate multiple protective layers into cohesive defensive frameworks. The interdependence of enterprise and operational technology systems requires unified approaches spanning both domains [9].

Network segmentation establishes foundational boundaries between system categories. Industrial demilitarized zones create buffer networks separating corporate infrastructure from process control environments. All traffic crossing these boundaries traverses designated inspection points. Firewalls enforce access control policies governing permitted communications. Intrusion detection systems monitor boundary traffic for malicious patterns. Protocol-aware inspection validates that industrial communications conform to expected formats. Unauthorized protocols or anomalous command sequences trigger alerts for security analyst review [9].

The Purdue Enterprise Reference Architecture provides a conceptual model for industrial network segmentation. Level zero contains physical process sensors and actuators. Level one encompasses basic control devices, including programmable logic controllers. Level two houses supervisory systems and human-machine interfaces. Level three

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ Research Article

contains site-level operations management functions. Levels four and five represent enterprise business systems. Each level maintains defined connectivity rules with adjacent levels. Direct connections spanning multiple levels violate architectural principles and create security vulnerabilities [9].

Zero-trust security models go against the conventional security models and approaches focused on network perimeter security. In conventional security models, there is an assumption made for internal network communications. This assumption proves dangerous when adversaries achieve internal positioning. Zero acceptance as true with frameworks requires non-stop verification, no matter the network location. Every access request undergoes authentication and authorization evaluation. Micro-segmentation limits lateral movement even within previously trusted zones. Identity-based access controls replace network-location-based trust decisions [9].

Incident response capabilities require pipeline-specific adaptations. Generic information technology response procedures may endanger physical processes. Isolating compromised systems can disrupt pipeline operations if executed without coordination. Response teams must understand interdependencies between cyber and physical systems. Actions protecting information assets must not create safety hazards or environmental risks. Pre-planned response playbooks address common scenarios with operationally safe procedures [10].

The convergence of information technology and operational technology creates organizational coordination challenges. IT security teams possess cybersecurity expertise but may lack industrial process knowledge. Operations personnel understand physical systems but may not recognize cyber threat indicators. Effective incident response requires collaboration between both groups. Joint training exercises build mutual understanding and establish communication protocols. Unified command structures prevent conflicting response actions during active incidents [10].

Pipeline infrastructure faces persistent threats from capable adversaries. Nation-states have demonstrated a willingness to target critical infrastructure for strategic purposes. Criminal organizations recognize the high-value extortion potential of operational disruption. The consequences of successful attacks extend beyond individual organizations to affect national energy security. Public safety implications elevate the stakes for pipeline cybersecurity beyond typical enterprise considerations [10].

-Ongoing process of security improvement helps to maintain protection efficacy. Assessment of vulnerabilities is used to detect gaps in protection that require remediation. Tests of penetration are applied to demonstrate control efficacy. Threat intelligence is used to ensure that protection measures cover contemporary adversary capacities. Security architecture needs to be responsive to changing threats.

Defense Layer	Component	Implementation	Security Function
Network Architecture	Industrial DMZ	Buffer network deployment	IT-OT traffic isolation
Network Architecture	Boundary firewalls	Access control enforcement	Communication restriction
Network Architecture	Protocol inspection	Deep packet analysis	Industrial protocol validation
Network Architecture	Purdue model implementation	Hierarchical segmentation	Level-based access control
Zero Trust	Continuous authentication	Ongoing verification	Implicit trust elimination
Zero Trust	Micro-segmentation	Granular network division	Lateral movement limitation

Zero Trust	Identity-based access	User verification controls	Location-independent security
Incident Response	Pipeline-specific playbooks	Pre-planned procedures	Operationally safe response
Incident Response	IT-OT team coordination	Joint command structures	Unified incident management
Incident Response	Joint training exercises	Cross-team preparation	Mutual understanding development

Table 4. Integrated Security Architecture Elements for Pipeline Protection [9, 10].

CONCLUSION

Energy pipeline infrastructures require holistic approaches to ensure their security, starting right from the stages of attack. Endpoint devices are the commonly used pathways by malicious actors wanting to attack pipeline networks. As such, phishing attacks, vulnerabilities involving devices used by contractors, and remote access serve as the main initial points used by attackers wanting to breach enterprise networks. The stages involving attack development, starting from enterprise network breaches, leading up to industrial control systems, follow predictable chains involving stealing authentication credentials, gaining privilege escalation, and executing systematic lateral movements. To ensure effective protective measure implementation, each step involved during attacks by malicious actors should receive similar attention. System behavior allows for the identification of attacks irrespective of the malware types used. Code execution, especially by untrusted applications, is prevented. The used authentication credentials cannot offer useful services during attacks, especially when dealing with network movements. Networks, as well as zero-trust methodologies, constitute certain structural barriers used for protecting industrial control systems. Demilitarized zones for industries ensure that all network-abundant traffic is inspected by using inspection points. There are required approaches involving incident response, especially through upholding necessary cybersecurity, as well as safety concerns. Energy is under constant attack by nationstates, gangs, and idealistic actors. As such, their impacts are limited to organizations, impacting energy safety, especially within the country.

REFERENCES

[1] Paul W. Parfomak, "Pipeline Security: An Overview of Federal Activities and Current Policy Issues," Congressional Research Service Reports, 2004. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA456883.pdf
[2] NAVEEN TATIPATRI AND S. L. ARUN, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," IEEE Access, 2023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10418207
[3] Mohammed Alghassab, "Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector," MDPI, 2022. [Online]. Available: https://www.mdpi.com/1996-1073/15/1/218
[4] Abigail M. Y. Koay et al., "Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges," Journal of Intelligent Information Systems, 2023. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10844-022-00753-1.pdf
[5] Mary Nankya et al., "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies," MDPI, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/21/8840
[6] Mohamed Mesbah et al., "Analysis of ICS and SCADA Systems Attacks Using Honeypots," MDPI, 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/7/241

[7] Keith Kirkpatrick, "Protecting Industrial Control Systems," Communications of the ACM, 2019. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3355377
[8] David Geer, "Security of Critical Control Systems Sparks Concern," IEEE Computer Society, 2006. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1580377
[9] Deval Bhamare et al., "Cybersecurity for Industrial Control Systems: A Survey," Computers and Security, Elsevier, 2019. [Online]. Available: https://arxiv.org/pdf/2002.04124
[10] Joel F. Brenner, "Eyes wide shut: The growing threat of cyber attacks on industrial control systems," Bulletin of the Atomic Scientists, 2013. [Online]. Available: https://journals.sagepub.com/doi/pdf/10.1177/0096340213501372