Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Mitigating Supply Chain Malware Risks in Operational Technology: Challenges and Solutions for the Oil and Gas Industry

Suchismita Chatterjee

Suchi5978@gmail.com
Tx, USA

Abstract

The oil and gas industry, a cornerstone of critical infrastructure, faces an escalating threat landscape due to supply chain malware targeting Operational Technology (OT). These attacks exploit vulnerabilities introduced by third-party vendors and the convergence of legacy OT systems with modern IT networks, posing significant risks to industrial processes, national energy resilience, and environmental safety. This article examines the unique risks in OT systems, highlighting cascading operational, financial, and environmental consequences. Grounded in NERC CIP-013 standards, it proposes mitigation strategies such as supply chain mapping, sandbox testing, Zero Trust Architecture (ZTA), robust vendor audits, and cybersecurity-integrated project management practices. By analyzing high- impact scenarios and lessons learned, it provides actionable insights to empower stakeholders in safeguarding critical infrastructure.

Keywords: Supply Chain Malware, Oil and Gas Industry, NERC Compliance, NERC CIP-013, Operational Technology, Vendor Risk Management, Cybersecurity Mitigation, Zero Trust Architecture (ZTA), Supply Chain Security

I. INTRODUCTION

The oil and gas industry underpins global economic stability by providing essential energy for transportation, manufacturing, and daily life. Operational Technology (OT) systems are integral to monitoring and controlling industrial processes. However, the convergence of legacy OT systems with modern Information Technology (IT) networks has amplified cyber- security vulnerabilities, particularly in supply chain malware risks introduced via compromised third-party vendors or in- secure software updates. The reliance on OT for critical operations makes the sector a prime target for sophisticated cyberattacks.

Supply chain malware infiltrates OT systems through com- promised vendors, spreading across interconnected networks. Recognizing these risks, the U.S. government introduced initiatives like Executive Order 13800 [1] to bolster energy infrastructure resilience. The sector's increasing adoption of IoT devices, smart meters, and automation has further expanded the attack surface.

High-profile incidents, such as the 2017 Triton attack targeting safety instrumented systems (SIS) in a petrochemical facility, underscore the severe risks. TRITON malware modified in-memory firmware,

compromising critical safety functions and threatening operational continuity, safety, and environmental integrity [2]. This marked the first malware designed to directly target industrial safety systems.

Despite awareness and the implementation of standards like NERC CIP-013 [3], legacy systems and vendor dependencies remain critical vulnerabilities. This article addresses the challenges of mitigating supply chain malware risks in OT environments within the oil and gas sector. It explores NERC CIP-013 standards, proposes actionable strategies, and emphasizes integrating cybersecurity into project management. Additionally, it examines frameworks and their applications to equip stakeholders with tools to strengthen resilience against evolving cyber threats.

II. Background and Context

A. *Critical Infrastructure Role of Oil and Gas Industry*

The oil and gas sector are critical to global economic stability, supplying resources for transportation, manufacturing, and daily operations. However, its reliance on digital technologies and legacy OT systems, designed for longevity rather than security, exposes it to significant cybersecurity risks. The 2019 Norsk Hydro ransomware attack, which affected 170 sites in 40 countries, underscored this vulnerability [4].

Cyberattacks on the sector can lead to catastrophic out- comes, including equipment failures, production delays, and environmental damage. Legacy OT systems, lacking modern security protocols, are prime targets. To mitigate these risks, the Department of Homeland Security (DHS) advocates a defense-in-depth strategy, segmenting enterprise architectures into security zones to enhance IT/OT collaboration and safe- guard critical assets [5].

B. *Integration of OT and IT in the Oil and Gas Sector*

The integration of OT and IT systems has revolutionized the oil and gas industry by enabling advanced analytics, predictive maintenance, and real-time decision-making. However, this convergence expands the attack surface, exposing critical infrastructure to sophisticated cyber threats. Legacy OT systems, often lacking modern security features, create vulnerabilities when integrated with IT networks [6]. Moreover, the reliance on third-party vendors for hardware, software, and services increases the risk of supply chain malware infiltration.

Practical implementation of IT/OT integration includes technologies such as distributed sensor networks, mobile connectivity, and artificial intelligence, which enable real-time monitoring and predictive maintenance [7]. However, the integration of legacy OT systems with modern IT environments is fraught with complexity, often leaving critical vulnerabilities unaddressed.

C. *Integration of OT and IT in the Oil and Gas Sector*

The integration of OT and IT systems has revolutionized the oil and gas industry by enabling advanced analytics, predictive maintenance, and real-time decision-making. However, this convergence expands the attack surface, exposing critical infrastructure to sophisticated cyber threats. Legacy OT systems, often lacking modern security features, create vulnerabilities when integrated with IT networks [6]. Moreover, the reliance on third-party vendors for hardware, software, and services increases the risk of supply chain malware infiltration.

Practical implementation of IT/OT integration includes technologies such as distributed sensor networks, mobile connectivity, and artificial intelligence, which enable real-time monitoring and predictive maintenance [7]. However, the integration of legacy OT systems with modern IT environments is fraught with complexity, often leaving critical vulnerabilities unaddressed.

D. Supply Chain Malware Risks and NERC Compliance

Supply chain malware is a significant threat to the oil and gas sector, often infiltrating OT systems through compromised third-party vendors or insecure software. For instance, the 2015 Ukraine power grid attack highlighted how malware introduced through vendor systems could disrupt operations and cause widespread damage [8]. Another example is the 2020 SolarWinds attack, where compromised software updates infiltrated numerous critical infrastructure networks, illustrating the severe impact of supply chain vulnerabilities [9].

The NERC CIP-013 standard mandates rigorous risk management practices to address these threats, including vendor security assessments, contractual obligations for cybersecurity, and improved supply chain transparency. Compliance with these standards not only mitigates risks but also supports organizational resilience against regulatory penalties. Non- compliance with these standards can result in penalties ranging from $500,000 to $1 million per day [10], emphasizing the need for stringent adherence.

By adopting NERC CIP-013-aligned strategies, such as sup- ply chain mapping, sandbox testing, and real-time monitoring, the oil and gas sector can enhance its cybersecurity posture while minimizing vulnerabilities associated with third-party dependencies.

To contextualize the growing cyber threat in the oil and gas industry, Figure 1 presents a temporal analysis of cyber incidents from 2015 to 2020. The diagram highlights the frequency and diversity of cyberattacks targeting OT systems, demonstrating how the threat landscape has evolved over time [11], [12], [13], [14], [15].

- **Dominance of Malware and Ransomware:** Malware consistently shows high occurrence, reflecting its adapt- ability and persistent threat to systems. Ransomware incidents have notable spikes in 2017 and 2020, aligning with high-profile global attacks.
- **Emerging Threats:** Advanced Persistent Threats (APTs) and SCADA/System attacks signify targeted and sophis-

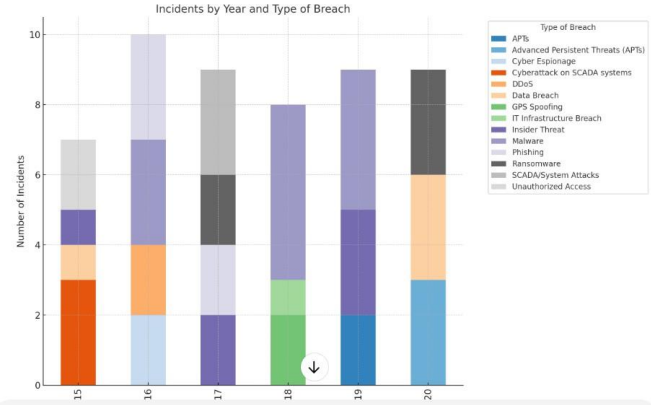

Fig. 1. Temporal analysis of cyber incidents by type and year

ticated breaches, emphasizing vulnerabilities in critical infrastructure.

- **Persistent Insider Threats:** Insider threats maintain a consistent presence, underscoring the critical need for robust internal security measures.
- **Preventative Gaps:** The recurrence of breaches despite advanced solutions suggests gaps in proactive measures, integration of AI-driven detection, and real-time monitoring.

The Trend analysis reveals malware and ransomware as persistent threats, highlighting vulnerabilities in critical infrastructure. These insights guide defenses and future research on emerging risks and mitigation.

E. *1.3 Objectives*

- Identify and analyze supply chain risks in OT systems: Focus on how legacy OT systems and third-party vendors introduce vulnerabilities to the oil and gas sector, increasing exposure to supply chain malware.
- Propose NERC CIP-aligned mitigation strategies: Develop actionable strategies based on NERC CIP-013 standards to address and mitigate supply chain malware risks in OT environments.
- Outline steps for integrating cybersecurity in project management: Provide practical steps for embedding cybersecurity into project management processes, ensuring security is integral to OT system upgrades and vendor management.

III. THREAT LANDSCAPE: LEGACY EQUIPMENT AND CROWN JEWEL ASSETS

The oil and gas industry faces unique cybersecurity challenges, particularly in the context of legacy equipment and crown jewel assets [26]. These vulnerabilities make the sector a prime target for cybercriminals. This section explores the anatomy of supply chain malware attacks, real-world examples of their impact, and the unique vulnerabilities faced by the sector due to outdated systems and external dependencies.

A. *Anatomy of a Supply Chain Attack*

Supply chain malware is a major cybersecurity threat to the oil and gas sector, exploiting vulnerabilities from third- party vendors through compromised software updates, insecure hardware, or weak development practices. Legacy OT systems, built for longevity rather than cybersecurity, are especially at risk [17].

The 2017 NotPetya ransomware attack, launched via a com- promised vendor update, disrupted operations across critical sectors. This demonstrated how a single supply chain breach can propagate through interconnected OT systems, corrupting data, disabling safety systems, and causing significant damage [18].

In the oil and gas sector, malware targets industrial control systems (ICS), programmable logic controllers (PLCs), and SCADA systems, disrupting remote monitoring and forcing manual shutdowns that endanger safety and operational continuity.

B. *High-Impact Scenarios*

Cyber incidents in the oil and gas sector can rapidly escalate, causing widespread operational and financial disruptions. For example, malware infiltrating a pipeline's SCADA system could disable remote monitoring and control, forcing manual shutdowns. Such incidents can result in substantial downtime, fuel shortages, safety hazards, and environmental damage, while cascading through the supply chain to impact contractors, regulators, and logistics providers.

A refinery's OT system is equally vulnerable; a cyberattack could compromise process controls, leading to catastrophic outcomes such as chemical spills, equipment failures, or explosions. These disruptions not only threaten local communities but also significantly impact supply chain stability and economic activity.

The financial implications are profound. The 2017 Maersk attack, though outside the oil and gas sector, caused $300 million in damages, demonstrating the cascading effects of supply chain disruptions [19]. These scenarios underscore the urgent need for robust cybersecurity strategies to secure OT environments.

C. *Unique Vulnerabilities in the Oil and Gas Industry*

1) *Legacy OT Systems:* Many Operational Technology (OT) systems in the oil and gas sector were designed decades ago and lack modern cybersecurity features. As these legacy systems are integrated with contemporary IT networks, they introduce additional vulnerabilities. These older systems are often incompatible with modern cybersecurity tools, leaving critical infrastructure exposed to evolving cyber threats [5].

2) *Vendor Dependencies:* The heavy reliance on third-party vendors for hardware, software, and services significantly increases the risk of cyberattacks. Vendors may not always follow stringent cybersecurity practices, providing an entry point for malware through compromised components or insecure software updates [20]. Consequently, organizations must take a proactive stance to ensure their vendors meet rigorous security standards.

3) *Crown Jewel Assets:* Critical assets, often referred to as "crown jewel" assets, such as drilling rigs, pipelines, and refineries, are prime targets for cybercriminals. These high-value assets are vital to national security and economic stability, making them frequent targets for cyberattacks [26]. Protecting these assets requires advanced security measures, including real-time threat detection, machine-learning-based intrusion detection systems, and strict access control protocols.

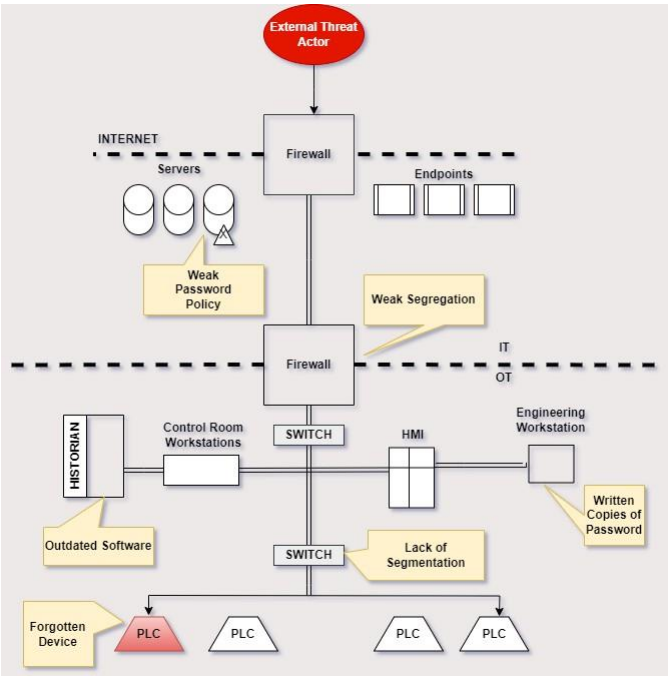

Fig. 2. Illustration of IT/OT vulnerabilities in legacy equipment and crown jewel assets

The diagram in Figure 2 highlights critical vulnerabilities within Industrial Control Systems (ICS) in the oil and gas sector, emphasizing the susceptibility of legacy equipment and crown jewel assets. These vulnerabilities, often exploited by supply chain malware, present significant risks to operational technology (OT) environments:

- **Weak Password Policies:** Inadequate password management on IT servers creates exploitable entry points for malware from compromised supply chain actors.
- **Insufficient Network Segregation:** Poorly defined IT/OT boundaries enable malware to target high-value assets like PLCs, HMIs, and engineering workstations.
- **Outdated Software:** Legacy equipment, often running unsupported or unpatched software, becomes a prime target for supply chain malware.
- **Human Factor Vulnerabilities:** Storing written pass- words and other mismanagement practices facilitate unauthorized access to critical systems.
- **Forgotten Devices:** Unmonitored OT devices act as silent entry points for sophisticated malware from compromised supply chain components.
- **Lack of Segmentation:** Poor network segmentation of critical OT assets like PLCs increases the risk of operational disruptions from malware.
- **Relevance to Supply Chain Malware Risks:** Legacy equipment and crown jewel assets are highly susceptible to supply chain malware. Such malware exploits outdated systems, weak network segmentation, and OT vulnerabilities, directly threatening operational resilience in the oil and gas sector.
- **Research Significance:** Proactive mitigation strategies are crucial to securing legacy systems, enforcing IT/OT segregation, and protecting crown jewel assets from supply chain malware. These measures ensure the safety and continuity of critical operational processes in the oil and gas industry.

4) A Proactive Approach: Addressing these vulnerabilities effectively requires a multi-faceted approach. Technical solutions like network segmentation and machine-learning- based intrusion detection systems help limit the exposure of critical OT systems to attacks. Complementing these technical defenses, organizational practices such as vendor audits and personnel training ensure that the entire supply chain is secure and that the workforce is prepared to recognize and respond to emerging cyber threats.

IV. Risk Assessment and Interdependencies

A. *Framework for Identifying Vulnerabilities*

Effective risk management in the oil and gas industry requires a structured methodology to identify and mitigate vulnerabilities in OT systems. A comprehensive framework should involve both *technical* and *organizational* assessments. Below is a recommended approach for identifying vulnerabilities and prioritizing risks:

- **Asset Identification and Risk Mapping**: The first step is to identify critical assets such as SCADA systems, PLCs, and pipeline control units. Mapping interdependencies across these assets helps in understanding how a breach in one part of the supply chain could impact other systems [22].
- **Vulnerability Scanning and Penetration Testing**: Con- ducting regular vulnerability scans on OT systems and performing penetration tests helps in identifying known vulnerabilities. It also provides an opportunity to simu- late real-world cyber-attacks, assessing how resilient the systems are to evolving threats.
- **Risk Scoring and Prioritization**: Tools like the *Risk Management Framework (RMF)* by NIST and *OWASP IoT Top 10* provide methodologies for scoring and prioritizing risks based on likelihood and impact. For example, assessing the risks associated with legacy equipment versus newer devices ensures that vulnerabilities are effectively managed across the asset lifecycle.
- **Vendor Security Assessment**: The *Vendor Risk Management Framework (VRMF)* should be used to assess third-party vendors, ensuring their security practices are in line with industry standards, such as NIST or IEC 62443. This is critical to mitigate risks from vulnerable third-party systems entering OT networks [23].

TABLE I

Frameworks and Tools for OT Vulnerability Assessment

Framework/Tool	Purpose	Use Case in OT Systems
Risk Management Framework (RMF)	Comprehensive risk essment (NIST 800-37).	Evaluates vulnerabilities in OT and IT systems.
NIST Cybersecurity Framework (CSF)	Guides cybersecurity risk management (E.O. 13636, 13800).	Prepares OT environments for incident response and recovery.
Cybersecurity	Maturity assessment	Identifies gaps in OT

Capability Maturity Model (C2M2)	of cybersecurity practices.	security programs.
Vendor Risk Management Framework (VRMF)	Evaluates third-party vendor security practices.	Mitigates supply chain and vendor-related vulnerabilities.
Distributed Energy Resource Cybersecurity Framework (DERCF)	Tailored for energy OT environments.	Secures distributed energy resources (DERs) in OT networks.
OWASP IoT Top 10	Highlights common vulnerabilities in IoT.	Prioritizes risks in connected OT devices.

- **Incident Response Planning**: Frameworks such as the *NIST Cybersecurity Framework (CSF)* should be adapted to the OT environment, focusing on incident detection, response, and recovery. OT systems require specific protocols and procedures to ensure rapid recovery in case of a security breach [23].

This methodology ensures that vulnerabilities are identified early, and resources are allocated to address the most critical risks first.

B. *Interdependencies in Risk Mitigation*

The interconnectedness between *Operational Technology (OT)* and *Information Technology (IT)* systems poses unique challenges for risk mitigation. As OT systems become more integrated with IT systems, any vulnerabilities in one domain may quickly affect the other, resulting in cyber-physical risks.

1) **OT and IT System Interdependence**: Oil and gas companies increasingly use *IT/OT convergence* to im- prove operational efficiency. While IT systems handle data processing, analytics, and communications, OT systems manage critical control functions (e.g., automated drilling). Cyber-attacks targeting IT infrastructure can thus exploit weaknesses in OT systems, and vice versa. For instance, ransomware targeting IT networks can disrupt OT operations, potentially leading to catastrophic failures in pipeline controls or refinery operations.
2) **Cross-Departmental Collaboration**: Effective risk mitigation requires a *collaborative approach* between departments such as *procurement*, *legal*, and *security*. Procurement teams must ensure that vendor contracts include robust cybersecurity clauses, such as adherence to NIST or IEC standards, and that OT assets are rigorously tested before deployment. The *legal team* must be involved in setting up the appropriate terms for cybersecurity compliance, liability, and incident response. Meanwhile, the *security team* needs to ensure that security policies address both IT and OT systems.
3) **Role of Regulatory Bodies**: Regulatory frameworks, such as those set by *NERC (North American Electric Reliability Corporation)*, provide essential guidance for securing OT systems. NERC's *CIP-013* standard focuses on *Supply Chain Cybersecurity*, compelling organizations to assess the cybersecurity practices of vendors supplying OT components.

Similarly, the *EU Agency for Cybersecurity (ENISA)* provides guidelines on securing OT systems [23], especially in critical sectors such as oil and gas, where infrastructure safety is paramount. These regulatory standards help create a baseline for securing OT systems across the supply chain and establishing *best practices* for vendor management, incident response, and resilience.

4) **Vendor Security and Third-Party Risk Management**: The *MITRE ATT&CK Framework for ICS* provides actionable insights into attack vectors targeting OT and IT systems, enabling oil and gas organizations to address vulnerabilities arising from vendor relationships. By conducting *third-party risk assessments*, companies can ensure vendors and contractors comply with cybersecurity standards, mitigating risks to the OT ecosystem [24]. The *Industroyer* and *Triton* attacks demonstrate how IT infrastructure can be exploited to compromise control systems. Techniques like *Remote System Discovery* (T1018) and *Network Service Scanning* (T1046) identified critical targets. Although ICS-specific actions such as issuing *Unauthorized Command Messages* (T855) to control substation switches fall outside ATT&CK for Enterprise, these are now captured within ATT&CK for ICS, reflecting the unique requirements of industrial environments [25].

V. MITIGATION STRATEGIES

This section discusses key strategies for mitigating risks associated with legacy systems and crown jewel assets in OT environments.

A. *Technical Measures*

- **Legacy Equipment Management:** To mitigate risks as- sociated with legacy systems, strategies such as isolation or gradual upgrading should be implemented. Techniques like network segmentation, sandboxing, and Zero Trust architectures can be applied to secure these systems without disrupting operations.
- **Protection of Crown Jewel Assets:** Critical assets in key operational processes need advanced threat detection and monitoring. These assets should be isolated in segmented network zones with restricted access for authorized personnel only. In critical infrastructure like the Oil and Gas (O&G) sector, Operational Data Networks (ODN) and Utility Data Networks (UDN) are considered crown jewels. Protection strategies must cover physical infrastructure, including secure hosting, safety measures for servers, and robust environmental monitoring systems. For example, weather monitoring for oil and gas pipelines in Alaska is essential. Ensuring physical security requires fortified infrastructure, proper fencing, and adherence to safety protocols [26].

B. *Organizational Measures*

- **Vendor Security and Audits:** Conduct regular cybersecurity audits to ensure vendors adhere to standards, particularly those managing legacy systems, strengthening supply chain security.
- **Personnel Training:** Train personnel to identify threats to legacy systems and crown jewel assets, focusing on their unique vulnerabilities in OT environments.
- **Compliance with Industry Standards:** Adopt frame- works like NERC CIP-013 and NIST CSF to manage risks associated with legacy systems and ensure compliance with vendor risk management and supply chain transparency.

C. *Network and Physical Infrastructure Resilience*

In OT environments, securing both network and physical infrastructure is crucial for operational

continuity. This includes ensuring network availability for critical systems, especially in remote oil and gas facilities. Oil pipelines require robust physical security, including fencing, building resilience, and continuous monitoring to prevent disruptions from external factors like extreme weather [5]. Securing physical servers hosting critical infrastructure is vital for long-term operational success.

VI. Case Studies and Simulations

A. *Hypothetical Attack Scenario*

A supply chain malware attack targets legacy systems and crown jewel assets within OT environments. Malware exploits outdated vendor systems, bypassing weak security protocols, and spreads to critical infrastructure like pipeline control systems. This scenario highlights the vulnerabilities of legacy systems, insufficient vendor security, and the lack of proper network segmentation in safeguarding critical OT assets.

B. *Lessons Learned*

Key lessons from real-world breaches emphasize the need for:

- **Legacy System Modernization**: Isolate or upgrade out- dated systems to reduce vulnerabilities.
- **Vendor Risk Management**: Enforce strict cybersecurity practices with third-party vendors.
- **Access Control and Segmentation**: Implement robust access controls and network segmentation to contain threats.
- **Proactive Monitoring**: Continuous monitoring and incident response plans are essential to detect and mitigate attacks.

These steps are critical for securing OT environments and preventing supply chain vulnerabilities.

VII. Conclusion

This paper presents a structured approach for mitigating the risks associated with legacy systems and crown jewel assets in OT environments. By implementing the proposed technical and organizational measures, organizations can significantly reduce their exposure to supply chain threats. Overcoming the challenges associated with legacy systems, vendor resistance, and regulatory compliance is essential for securing critical infrastructure in an increasingly complex threat landscape.

References

1. Executive Order 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” The White House, May 11, 2017. [Online]. Available: https://www.cio.gov/tags/eo-13800/
2. Fortinet, ”The Evolution of Cyber Threats in OT Environments,” Fortinet, 2020. [Online]. Available: https://www.fortinet.com/blog/ industry-trends/evolution-of-cyber-threats-in-ot-environments.
3. NERC, ”CIP-013: Cybersecurity Risk Management,” North American Electric Reliability Corporation, 2020. [Online]. Available: https://www. nerc.com/Pages/default.aspx.
4. Norsk Hydro, *Norsk Hydro ransomware attack*, 2019, Industrial Cyber. [Online]. Available: https://industrialcyber.co/news/ norsk-hydro-ransomware-attack/.
5. Lamba, ”Protecting ‘cybersecurity & resiliency’ of nation’s critical infrastructure–energy, oil &

gas," *International Journal of Current Research*, vol. 10, pp. 76865–76876, 2018.
6. Murray, M. N. Johnstone, and C. Valli, *The convergence of IT and OT in critical infrastructure*, 2017.
7. The Essential Guide, *What Is IT/OT Convergence?*, 2021. [Online]. Available: https://industrialcyber.co/analyst-corner/ the-essential-guide-to-it-ot-convergence/.
8. Defense Use Case, *Analysis of the cyber attack on the Ukrainian power grid*, Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, no. 1-29, pp. 3, 2016, Washington, DC.
9. Third Party Trust, *NERC CIP-013 Requirements and CIP-013-1 Implementation Guidance*, 2020. [On- line].Available:https://www.thirdpartytrust.com/blog/ nerc-cip-013-1-cyber-supply-chain-risk-management/.
10. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *CSO Online*. [Online]. Available: https://www.csoonline.com/article/3250875/inside-the-cunning- unprecedented-hack-of-ukraines-power-grid.html.
11. "Triton Attackers Accidentally Caused Operational Disruption," *Se- curity Week*. [Online]. Available: https://www.securityweek.com/triton- attackers-accidentally-caused-operational-disruption-report.
12. "Dragonfly Energy Sector Cyber Attacks," *Symantec Blog*. [Online]. Available: https://www.symantec.com/blogs/threat- intelligence/dragonfly-energy-sector-cyber-attacks.
13. "Saudi Aramco Cyberattack," *Reuters*. [Online]. Avail- able: https://www.reuters.com/article/us-saudi-aramco-cyber- idUSKBN24Z0Y8.
14. "Cyberattack on Energy Transfer," *Reuters*. [Online]. Available: https://www.reuters.com/article/us-energy-transfer-cyber-natgas- idUSKBN1HP2M7.
15. Booth, A. Dhingra, S. Heiligtag, M. Nayfeh, and D. Wallance, "Critical infrastructure companies and the global cybersecurity threat," *McKinsey & Company*, vol. 11, 2019.
16. T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electronics*, vol. 9, no. 11, pp. 1864, 2020.
17. T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Computer Communications*, vol. 155, pp. 1–8, 2020.
18. Oruc, "Claims of state-sponsored cyberattack in the maritime indus- try," in *Conference Proceedings of INEC*, 2020.
19. Z. Al-Balushi and C. M. Durugbo, "Management strategies for supply risk dependencies: empirical evidence from the Gulf region," *Interna- tional Journal of Physical Distribution & Logistics Management*, vol. 50, no. 4, pp. 457–481, 2020.
20. Booth, A. Dhingra, S. Heiligtag, M. Nayfeh, and D. Wallance, "Critical infrastructure companies and the global cybersecurity threat," *McKinsey & Company*, vol. 11, 2019.
21. R. Baudoin, "Deploying the industrial internet in oil & gas: Chal- lenges and opportunities," in *SPE Intelligent Energy International Con- ference and Exhibition*, 2016, pp. SPE–181107.
20. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, "Cyber-attacks on the oil & gas sector: A survey on incident assessment and at- tack patterns," *IEEE Access*, vol. 8, pp. 128440-128475, 2020, doi: 10.1109/ACCESS.2020.3007960.

21. Avanzini and A. Spessa, ”Cybersecurity verification approach for the oil & gas industry,” in *Offshore Mediterranean Conference and Exhibition*, 2019, pp. OMC–2019.
22. O. Alexander, M. Belisle, and J. Steele, ”MITRE ATT&CK for industrial control systems: Design and philosophy,” *The MITRE Corporation*, Bedford, MA, USA, vol. 29, 2020.
23. Booth, A. Dhingra, S. Heiligtag, M. Nayfeh, and D. Wallance, ”Critical infrastructure companies and the global cybersecurity threat,” *McKinsey & Company*, vol. 11, 2019.