IOCEN 2026 Conference
The 3rd International Online Conference on Energies
12–15 May 2026 | Online
MDPI

Securing Critical Energy Infrastructure: Cyber Risks, Challenges, and Defense Strategies in the Digital Era

Hirak Modi[1,3], Dr. Veera Gnaneswar Gude[1,2,4], Mohammad Marufuzzaman[5]

1. Purdue University Northwest Water Institute, Purdue University Northwest, Hammond, IN, USA
2. Mechanical and Civil engineering department, Purdue University Northwest, Hammond, IN, USA
3. Department of Computer Science, Purdue University Northwest, Hammond, IN, USA
4. School of Sustainability Engineering and Environmental Engineering, Purdue University, West Lafayette, IN, USA
5. Industrial and Systems Engineering, Mississippi State University, Mississippi State, MS, USA

INTRODUCTION & AIM

The energy sector has undergone rapid digital transformation, integrating cloud platforms, IoT devices, virtual power plants, and industrial control systems (ICS). While this digitalization improves efficiency and enables decarbonization, it dramatically expands the cyberattack surface. Reported cyberattacks on energy assets more than doubled between 2019 and 2023, with ransomware alone accounting for nearly 40% of all incidents. High-profile breaches, such as the Colonial Pipeline attack in 2021, have demonstrated that cyber incidents can trigger physical disruptions, economic losses exceeding USD 4 million per incident, and cascading effects on fuel supply chains.

Research Objective: To synthesize cybersecurity risks, technical mitigation strategies, and governance frameworks across four energy subsectors, oil & gas, electricity, nuclear, and renewable energy.

METHOD

A structured systematic literature review was conducted across Scopus, IEEE Xplore, Web of Science, and ScienceDirect (2019–2024). Sources were filtered using PRISMA guidelines. The study also integrates multi-criteria decision-making (MCDM) frameworks (TOPSIS, AHP) to rank cyber risks by impact and likelihood across subsectors. The five-layer cyber-physical architecture (Physical Infrastructure → OT Control → Communication & Cloud → Cyber Threats → Security & Resilience) from Figure 1 serves as the conceptual framework.

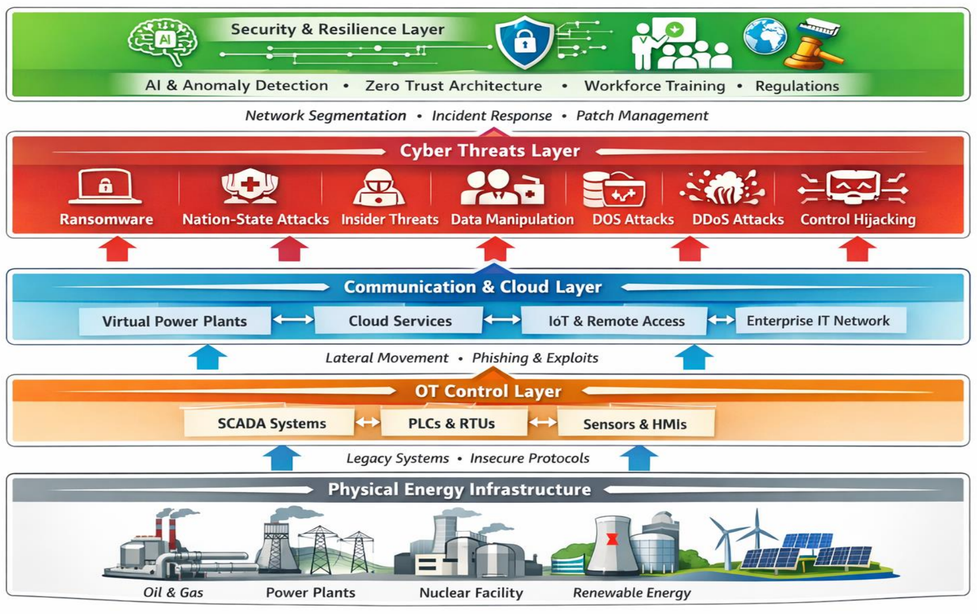

Figure 1: Cyber-Physical System Design for Secure Digitalized Energy Infrastructure

Key Findings

THREAT LANDSCAPE

Legacy ICS/SCADA systems remain the most systemic vulnerability, typically 15-30 years old and designed without security in mind.

IT/OT convergence has dramatically increased attack surface in electricity and renewables.

Ransomware attacks grew 355% from 2020 to 2025, rising from approximately 1,400 incidents to nearly 6,500 annually.

HMIs, SCADA systems, and PLCs accessed via public-facing internet with weak authentication are the most common entry points for attackers.

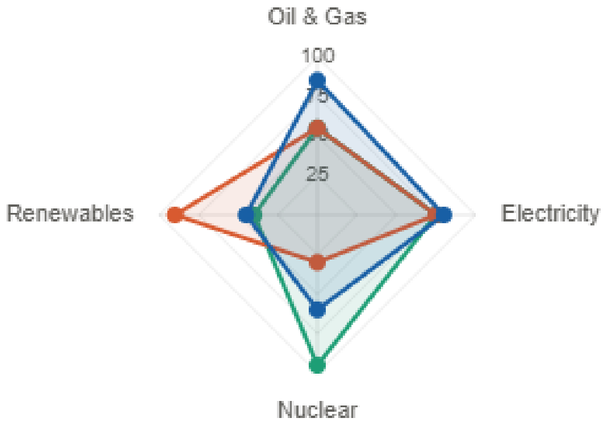

Figure 2: Vulnerability score by energy subsector

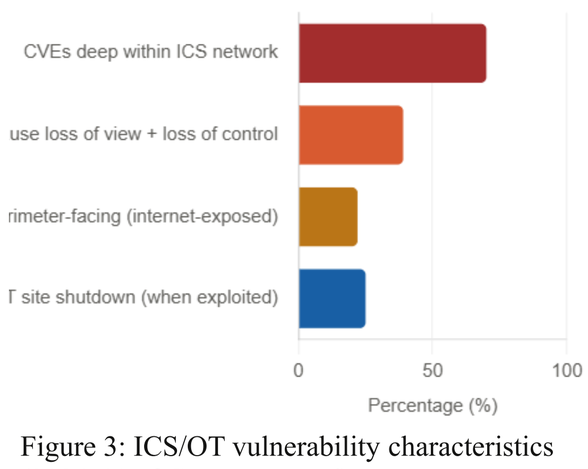

Figure 3: ICS/OT vulnerability characteristics (2024, % of CVEs assessed)

MITIGATION STRATEGIES

Table 1: Mitigation strategy effectiveness for energy OT/ICS environments

Mitigation Strategy	Threats Addressed	Effectiveness
AI/ML anomaly detection	Ransomware, APT, false data injection	98% detection rate; 70% response time (MDPI 2024); 94% of firms adopting
Zero Trust Architecture (ZTA)	Ransomware, APT, false data injection	Reduces attack surface by up to 60%; required by NIS2 & TSA directives (2024)
OT/IT network segmentation	Lateral movement, ransomware propagation	~70% of OT incidents originate in IT; proper segmentation prevents most propagation (Dragos 2024)
Patch & vulnerability management	Zero-day exploits, known CVEs	70% of 2024 ICS CVEs deep in network; 22% perimeter-facing; addressing latter has highest ROI (Dragos)
Edge-based IDS for distributed assets	IoT exploitation, VPP attacks, DDoS	Reduces detection latency from hours to seconds for distributed renewable assets
Cyber exercises & red teaming	Insider threat, social engineering, ICS Kill Chain	Tabletop exercises in electric sector rose 104% YoY 2023 (Dragos); reduces incident response time significantly
Supply chain security (SBOM)	Supply chain compromise, firmware backdoors	MOVEit/CLOP impacted 2,180+ victims; SBOM mandates reduce third-party risk exposure by ~40%

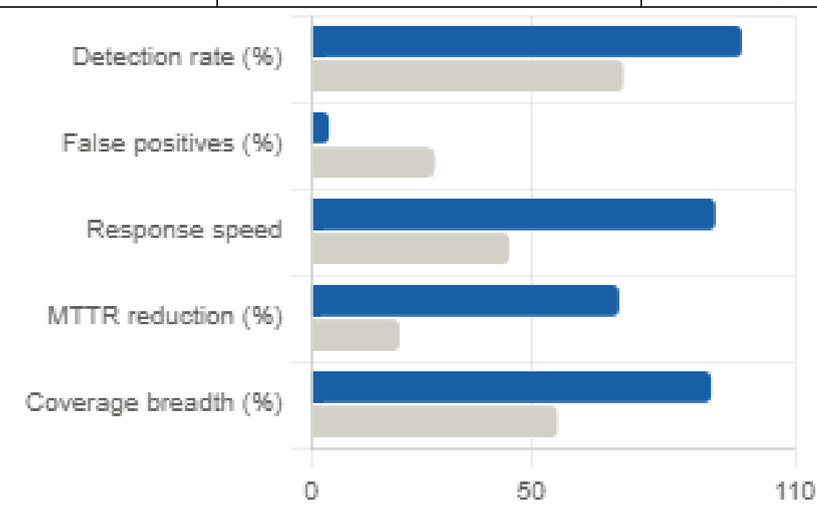

Figure 4: Mitigation effectiveness (AI-enhanced vs. traditional)

CONCLUSION

The rapid digitalization of energy infrastructure has created an expanding cyber-physical attack surface that adversaries, from ransomware operators to nation-state actors, are actively exploiting. This study confirms that **no single measure is sufficient**; resilience demands an integrated, adaptive response combining technical controls, organizational capacity, and harmonized policy.

FUTURE DIRECTIONS

1.Quantum-resilient cryptography for legacy ICS/SCADA protocols.
2.Autonomous AI incident response for OT, self-healing without disrupting physical processes.
3.Global binding standards for renewable energy cybersecurity.
4.Cross-sector real-time IoC sharing frameworks across energy subsectors.

REFERENCES

W. Villegas-Ch, J. C. García-Ortiz, and S. Luján-Mora, "*Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence,*" *Systems*, vol. 12, no. 5, p. 165, 2024. doi: 10.3390/systems12050165

T. M. Aljohani, "*Cyberattacks on Energy Infrastructures as Modern War Weapons, Part I: Analysis and Motives; Part II: Gaps, Standardization, and Mitigation,*" *IEEE Access*, 2024. doi: 10.1109/ACCESS.2024.3395032

Cloud Security Alliance, "*Zero Trust Guidance for Critical Infrastructure,*" CSA Technical Report, Zero Trust Working Group, Oct. 2024. cloudsecurityalliance.org