143 (2025) 205744

Contents lists available at ScienceDirect

Gas Science and Engineering

journal homepage: www.journals.elsevier.com/gas-science-and-engineering

Cybersecurity and cyber-attacks in the growing natural gas and hydrogen Industry: A systematic review of challenges and opportunities

Haoming Ma [a], Yang Lu [b,c,*], Zuhao Kou [d], Zhenqian Xue [e,**], Wei Yu [f,g], Kai Zhang [h,i,j,***], Peng Deng [e], Chaojie Di [e], Yuanrui Zhu [k], Hao Wang [k], Zhangxing Chen [l,e]

[a] School of Energy Resources, University of Wyoming, Laramie, WY, 82071, United States
[b] School of Robotics and Automation, Nanjing University, Suzhou, 215163, China
[c] School of Computing and Communications, Lancaster University, Lancaster, LA1 4YW, United Kingdom
[d] Department of Earth and Environmental Engineering, Columbia University, New York, 10027, United States
[e] Department of Chemical and Petroleum Engineering, University of Calgary, Calgary, AB, Canada, T2N 1N4
[f] Law School, Lancaster University, Lancaster, LA1 4YW, United Kingdom
[g] Beijing Zhonglun W&D (Suzhou) Law Firm, Suzhou, China
[h] Hubei Key Laboratory of Oil and Gas Exploration and Development Theory and Technology (China University of Geosciences), Wuhan, 430074, China
[i] Key Laboratory of Tectonics and Petroleum Resources (China University of Geosciences), Ministry of Education, Wuhan, 430074, China
[j] School of Earth Resources, China University of Geosciences (Wuhan), Wuhan, China
[k] Hildebrand Department of Petroleum and Geosystems Engineering, University of Texas at Austin, Austin, TX, 78712, United States
[l] Ningbo Institute of Digital Twin, Eastern Institute of Technology, Ningbo, China

ARTICLE INFO

Keywords:
Cybersecurity
Cyber-attack
Natural gas industry
Hydrogen economy

ABSTRACT

The natural gas and hydrogen industries are increasingly integral to the global transition toward a decarbonized energy future. With the integration of digital technologies such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Internet of Things (IoT) devices, and Artificial Intelligence (AI), these industries have enhanced operational efficiency and scalability. However, this digital evolution has concurrently expanded the cyber-attack surface, exposing critical infrastructure to sophisticated threats ranging from ransomware to advanced persistent threats (APTs). This review article summarizes the evolving cybersecurity landscape in the natural gas and hydrogen industries, emphasizing the vulnerabilities introduced by digital transformation and the rising frequencies of cyber intrusions. It investigates historical cyber-attacks, threat vectors, and their economic, operational, and environmental impacts. The article also discusses advanced security frameworks, the role of AI and machine learning in threat detection, and innovations such as blockchain and digital twins. Finally, forward-looking strategies and actionable recommendations are presented to foster cyber resilience in the context of the emerging hydrogen economy. This systematic review underscores the rising importance of integrating cybersecurity into energy system design, policy, and operations to safeguard infrastructure in a highly interconnected digital and renewable energy transition.

1. Introduction

The global energy sector is undergoing a profound transformation, driven by a growing demand for diversified low-carbon energy resources and the evolution of emerging artificial intelligence (AI) (IEA, 2024a, 2024d). Among the key players in this evolving energy landscape are the natural gas and hydrogen industries. Natural gas, often seen as a bridge fuel in the transition from fossil fuels to renewable energy, has long served as a reliable and efficient source of energy for heating, power generation, and industrial processes (IEA, 2024b). In particular, the low-emission gas is projected to reach nearly 400 billion cubic meters globally in 2050, representing a ten-fold increase as of today (IEA,

This article is part of a special issue entitled: Advancement in Gas Production and Storage published in Gas Science and Engineering.

* Corresponding author. School of Robotics and Automation, Nanjing University, Suzhou, 215163, China.
** Corresponding author. Department of Chemical and Petroleum Engineering, University of Calgary, Calgary, AB, Canada, T2N 1N4.
*** Corresponding author. Hubei Key Laboratory of Oil and Gas Exploration and Development Theory and Technology (China University of Geosciences), Wuhan, 430074, China.
E-mail addresses: luyang@nju.edu.cn (Y. Lu), zhenqian.xue@ucalgary.ca (Z. Xue), zhangkai91@cug.edu.cn (K. Zhang).

https://doi.org/10.1016/j.jgsce.2025.205744
Received 25 April 2025; Received in revised form 23 July 2025; Accepted 29 July 2025
Available online 30 July 2025
2949-9089/© 2025 Elsevier B.V. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

2024d). Meanwhile, hydrogen is emerging as a critical resource due to its potential to decarbonize the energy sector with the global investment of more than USD 3.5 billion in 2023 (IEA, 2024c; Ma et al., 2023). In parallel with the push toward sustainability, there has been a rapid integration of AI across all segments of the energy supply chain (IEA, 2024a). From the upstream exploration and production to transmission, distribution, and end-use, energy companies are increasingly adopting digital solutions to improve efficiency, reduce costs, and enhance operational flexibility (Ma et al., 2025; Ma et al., 2022; Xue et al., 2024). These include technologies such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Internet of Things (IoT) devices, and advanced analytics platforms powered by artificial intelligence (AI) and machine learning (ML) (Cárdenas et al., 2011; Ma et al., 2021, 2023, 2023a,b, 2025, 2025a) (see Table 1).

However, this digital evolution comes with a downside. As operational systems become more interconnected and reliant on digital infrastructure, they simultaneously become more vulnerable to cyber threats (Taherdoost, 2024). Unlike traditional safety and reliability risks that are often physical or environmental in nature, cybersecurity risks are dynamic, invisible, and potentially global in impact (Cremer et al., 2022). A single cyber-attack on a critical piece of energy infrastructure can lead to cascading failures, economic losses, and even environmental disasters. Historically, the energy sector has prioritized physical security and safety over cybersecurity. This legacy mindset has resulted in systems that are functionally robust but often lacking in basic security measures. Furthermore, many ICS and SCADA systems in use today were designed decades ago, with limited consideration for cybersecurity. When these legacy systems are connected to modern IT networks, they expose critical infrastructure to sophisticated cyber adversaries, including nation-state actors, hacktivists, and financially motivated cybercriminals.

The convergence of digitalization and energy decentralization presents both an opportunity and a challenge. On one hand, digital solutions can enhance grid stability, enable predictive maintenance, and facilitate real-time monitoring. On the other hand, the increasing complexity and interdependence of systems increase the attack surface and the likelihood of exploitation. In this context, cybersecurity is not merely a technical concern—it has become a cornerstone of energy system resilience and national security.

In the modern energy ecosystem, cybersecurity is as critical as the physical integrity of infrastructure. The natural gas and hydrogen sectors rely heavily on technologies that were never originally designed with cyber protection in mind. ICS and SCADA systems, which are central to monitoring and controlling complex industrial processes, were initially developed for isolated environments (Yadav and Paul, 2021). These systems were optimized for real-time performance and reliability, but not necessarily for confidentiality, authentication, or data integrity (Yadav and Paul, 2021).

With the increasing trend toward IT-OT (Information Technology–Operational Technology) convergence, these systems are now exposed to external networks and, by extension, to cyber threats. The growing deployment of IoT sensors and remote access interfaces compounds this vulnerability (El-Afifi et al., 2024). These endpoints can be exploited by attackers to gain a foothold into secure environments, leading to potentially catastrophic consequences (Doan et al., 2020). The importance of cybersecurity in these sectors is underscored by the growing frequency and sophistication of cyber-attacks targeting critical energy infrastructure (Ding et al., 2023). From ransomware attacks that paralyze operations to stealthy Advanced Persistent Threats (APTs) that dwell undetected within networks, the range and impact of cyber threats are escalating (Ding et al., 2023). In the case of hydrogen infrastructure, which often involves high-pressure storage and flammable gases, a successful cyber-attack could result in severe safety hazards, endangering human lives and causing significant environmental damage (Diaba et al., 2024; Vijayshankar et al., 2023).

Moreover, the implications of a cyber-attack go beyond the immediate operational impact. The reputational damage, regulatory penalties, and market disruptions that can follow a successful breach can have long-term consequences for energy providers (Diaba et al., 2024). In a sector where trust and reliability are paramount, even a single incident can erode public confidence and investor trust. From a strategic standpoint, cybersecurity is also a national security imperative (Vijayshankar et al., 2023). Natural gas and hydrogen infrastructure forms part of a country's critical energy assets. A coordinated cyber-attack on gas pipelines or hydrogen production plants could disrupt energy supply chains, affect industrial output, and compromise public safety (Vijayshankar et al., 2023). This reality has prompted governments and regulatory bodies to develop cybersecurity frameworks specifically tailored for the energy sector, emphasizing risk-based approaches, incident reporting, and resilience building.

The overarching goal of this review paper is to comprehensively examine the intersection between cybersecurity and the natural gas and hydrogen industries. The paper explores the multifaceted role of cybersecurity in protecting digital energy systems, the types of cyber-attacks that pose threats to these sectors, and the mechanisms through which such attacks are perpetrated. It also assesses the economic, operational, and environmental impacts of cyber incidents in these industries.

Specifically, this paper aims to.

- Provide an overview of how digital transformation is reshaping the operational landscape of the natural gas and hydrogen sectors.
- Identify and analyze common cybersecurity challenges and threat vectors in energy infrastructure.
- Review notable historical cyber-attacks that have impacted critical energy systems.
- Explore cybersecurity tools, frameworks, and technological innovations being adopted to mitigate cyber risks.
- Evaluate the current regulatory landscape and identify gaps in policies and standards.
- Discuss emerging trends such as AI-based threat detection, blockchain integration, and the use of digital twins.
- Offer insights into the future of cybersecurity in the context of the hydrogen economy.

Table 1
Top 5 Cyber-attacks in Natural Gas sector over the past 10 years.

Name	Year	Attacked Company & Continent	Segment(s)	Refs
Triton/TRISIS	2017	Petro Rabigh refinery (Schneider Electric Triconex SIS) – Saudi Arabia (Middle East)	Safety Instrumented Systems (SIS)	Di Pinto et al. (2018)
U.S. Pipeline Ransomware	2020	Unnamed U.S. natural-gas compression facility – North America	Pipelines (compression & control)	Beerman et al. (2023)
Colonial Pipeline (DarkSide)	2021	Colonial Pipeline Company – U.S. (North America)	Pipelines (fuel transport)	Beerman et al. (2023)
Canada Gas-Distribution Hack	2023	Canadian gas-distribution operator – North America	Distribution networks	Stergiopoulos et al. (2020)
CyberAv3ngers ICS Campaign	2023	Multiple oil & gas ICS operators (U.S., Israel, Ireland) – North America, Asia, Europe	PLCs, HMIs, SCADA	Beerman et al. (2023)

- Provide actionable recommendations for policymakers, industry stakeholders, and cybersecurity professionals.

By addressing these objectives, this review intends to contribute to a more robust understanding of cybersecurity as an integral part of modern energy strategies and infrastructure protection.

2. Overview of cybersecurity in the energy sector

2.1. Digital energy transformation

As Fig. 1 shows, the ongoing digital transformation within the energy sector represents a significant paradigm shift in the way energy is produced, transported, distributed, and consumed (Akberdina and Osmonova, 2021; Borowski, 2022; Ma et al., 2021; Ma et al., 2023; Maroufkhani et al., 2022). Digital technologies have introduced a new layer of intelligence and automation that enhances system efficiency, reduces operational costs, and enables better decision-making across the value chain (Maroufkhani et al., 2022). Beyond traditional physical infrastructures, digital solutions have gradually emerged within the natural gas and hydrogen sectors. This transformation is evident through the integration of advanced sensing technologies, real-time data analytics, cloud computing platforms, and remote-control capabilities (Maroufkhani et al., 2022). In contrast, conventional physical infrastructures have become increasingly vulnerable and outdated, further accelerating the shift towards widespread adoption of digital infrastructure in the energy industry.

One of the most prominent outcomes of digital transformation is the integration of the Industrial Internet of Things (IIoT), which facilitates real-time data collection from field assets such as compressors, storage tanks, pipeline networks, hydrogen refueling stations, and electrolysis units (Bhattacharjee and Nandi, 2019; Hossein Motlagh et al., 2020; Tabaa et al., 2020). These IIoT-enabled systems can predict equipment failures, detect anomalies, and optimize asset performance, ultimately improving the reliability and sustainability of energy supply chains. Furthermore, digital technologies are enabling predictive maintenance strategies, where machine learning algorithms analyze historical performance data to forecast failures and recommend proactive interventions (Ma et al., 2023; Xue et al., 2024, 2025; Xue et al., 2023a,b). In hydrogen infrastructure, where the reliability of high-pressure equipment is critical for safety, predictive maintenance can play a pivotal role in preventing catastrophic failures.

Similarly, digital twins—a virtual representation of physical assets—are becoming increasingly popular in these industries (Amaral et al., 2023; Jiang et al., 2021; Ismail et al., 2024; Kronberger et al., 2020; Ma et al., 2025; Nixon, 2020; Sleiti et al., 2022; Strielkowski et al., 2022; Yu et al., 2022). Digital twins allow engineers and operators to simulate real-world operations in a digital environment, test various operational scenarios, and identify vulnerabilities without disrupting actual systems. This helps in improving system reliability and facilitates advanced risk assessment, including cyber-risk analysis. Energy management systems (EMS), demand-side response platforms, and blockchain-enabled transaction mechanisms are also becoming integral components of modern energy architectures (Andoni et al., 2019; Borowski, 2021; El-Afifi et al., 2024; Lal and You, 2024; Lu et al., 2019; Ma et al., 2023). These tools allow for decentralized energy trading, transparent tracking of hydrogen supply chains, and improved coordination between producers, consumers, and grid operators.

However, this growing interconnectivity and reliance on digital systems have also expanded the cyber-attack surface. Systems that were once isolated and air-gapped are now part of broader digital ecosystems, exposing them to the same cyber threats that plague conventional IT systems. As a result, energy companies must shift their cybersecurity strategies from reactive defense to proactive threat anticipation and mitigation.

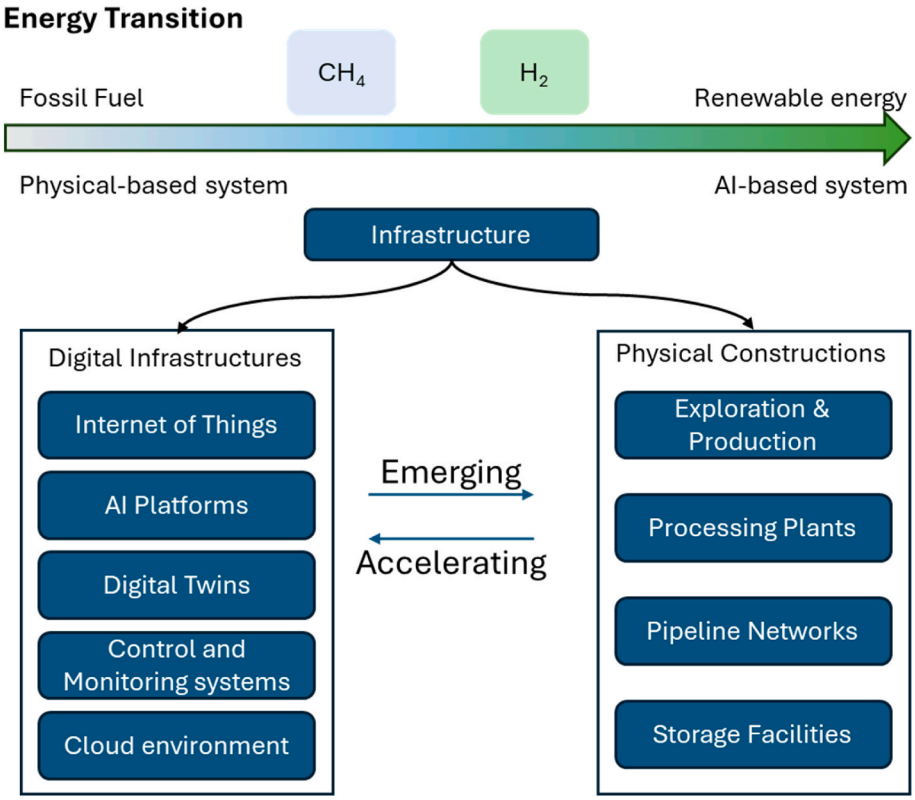

Fig. 1. Illustration of digital energy transition.

2.2. Cybersecurity challenges

The cybersecurity challenges in the energy sector are multifaceted and stem from a combination of technical, organizational, and strategic factors (Cremer et al., 2022; Diaba et al., 2024; Dragos, 2024a; Stergiopoulos et al., 2020; Yadav and Paul, 2021). A key issue is the legacy nature of many industrial systems. ICS and SCADA infrastructures—often decades old—were built with an emphasis on operational continuity, not cybersecurity. These systems operate on proprietary protocols and lack basic security features such as encryption, authentication, or secure update mechanisms. When these legacy systems are interconnected with corporate IT networks for data integration or remote access purposes, they become susceptible to cyber intrusions that exploit vulnerabilities in software, firmware, and human behaviors. For instance, attackers may use spear-phishing emails to compromise user credentials, which are then used to access control systems and disrupt operations.

Another challenge is the complexity of securing distributed and hybrid infrastructures. Modern energy systems span across multiple locations, integrate diverse technologies, and involve numerous stakeholders. Ensuring end-to-end security in such an environment requires holistic and scalable security architectures. Traditional perimeter-based security models are no longer adequate, prompting a shift toward zero-trust architectures that assume every access request is potentially malicious until verified. The challenge is further compounded by the lack of skilled cybersecurity professionals in the energy sector. The convergence of OT and IT requires expertise in both domains, yet such hybrid skillsets are in short supply globally. Many energy companies struggle to recruit and retain cybersecurity talent, which undermines their ability to respond effectively to evolving threats.

Moreover, insider threats pose a serious risk to critical infrastructure. Whether malicious or accidental, insider actions can lead to data breaches, system misconfigurations, and unauthorized access to sensitive assets. Organizations must implement strict access control policies, continuous monitoring systems, and robust training programs to mitigate these internal vulnerabilities. Supply chain security is another critical concern. Energy companies often rely on third-party vendors for hardware, software, and system maintenance. If these vendors are compromised, attackers can introduce malicious code or devices into the energy ecosystem. Ensuring vendor compliance with cybersecurity standards and conducting regular security audits are essential steps in addressing this risk.

Lastly, energy infrastructure is often a target for politically motivated cyber-attacks, particularly in times of geopolitical tension. Nation-state actors may target gas pipelines, hydrogen production facilities, or energy trading systems to disrupt national economies or exert political leverage. These attacks are typically sophisticated, stealthy, and persistent, requiring advanced threat intelligence capabilities to detect and neutralize.

2.3. Regulatory landscape

The regulatory landscape for cybersecurity in the energy sector is evolving rapidly, driven by the increasing recognition of cyber risks to national security and economic stability (Saxena et al., 2025). Several national and international frameworks have been developed to guide energy companies in implementing effective cybersecurity practices. In the United States, the NIST Cybersecurity Framework (CSF) provides a comprehensive approach to identifying, protecting, detecting, responding to, and recovering from cyber incidents (NIST, 2024a; 2024b). Although voluntary, this framework is widely adopted and often mandated for critical infrastructure operators. It promotes a risk-based approach and emphasizes continuous improvement. In Europe, the Network and Information Security Directive (NIS2) represents a significant regulatory advancement, requiring energy operators to adopt robust cybersecurity measures, report incidents, and undergo regular compliance assessments (European Commission, 2025). The European Union Agency for Cybersecurity (ENISA) supports these efforts by developing sector-specific guidelines and conducting threat assessments (ENISA, 2025). Globally, the ISO/IEC 27001 standard sets the benchmark for information security management systems (ISO/IEC27001, 2022). This standard helps organizations develop structured security policies, manage risks, and ensure continuous monitoring and review of security controls. Many energy companies seek ISO certification as part of their compliance strategies.

Despite these advancements, the regulatory landscape still faces several limitations. One key issue is the lack of harmonization across jurisdictions, which complicates compliance for multinational energy operators. Another concern is the pace of regulatory updates, which often lags behind the rapid evolution of cyber threats. There is a growing consensus on the need for more agile and adaptive regulatory frameworks that can respond to emerging risks in real time. Moreover, compliance should not be viewed merely as a checkbox activity but as an integral component of organizational culture. Regulators are increasingly encouraging outcome-based approaches that focus on cybersecurity effectiveness rather than prescriptive control lists. This shift requires companies to demonstrate not only technical compliance but also a strategic commitment to cyber resilience.

3. Cyber-attacks in the natural gas and hydrogen industry

3.1. Historical cyber-attacks

The natural gas and hydrogen sectors, as integral parts of the broader energy infrastructure, have not been immune to the growing wave of cyber-attacks that have affected critical industries worldwide. In fact, these sectors have increasingly become prime targets for cyber adversaries due to their strategic importance, legacy system vulnerabilities, and digital interconnectivity. One of the most significant and widely publicized incidents was the Colonial Pipeline ransomware attack in May 2021 (Beerman et al., 2023). A cybercriminal group known as DarkSide deployed ransomware that crippled one of the largest fuel pipeline operators in the United States, causing widespread fuel shortages across the East Coast. The attackers gained access through a compromised VPN account lacking multifactor authentication, encrypting vital business systems and forcing a temporary shutdown of pipeline operations. Although the attack targeted IT systems, the fear of lateral movement into operational technology (OT) networks prompted the shutdown, highlighting the interconnected nature of digital infrastructure and operational safety. Another prominent example is the 2012 Shamoon virus attack (Zhioua, 2013), which targeted Saudi Aramco, the world's largest oil company. The malware wiped data on over 30,000 workstations, disrupting internal communications and operations. While not directly related to natural gas or hydrogen systems, Shamoon serves as a cautionary tale of the impact malware can have on energy infrastructure. There have also been numerous stealthier intrusions, often attributed to nation-state actors, that have not resulted in immediate operational disruption but have involved surveillance, data exfiltration, or long-term system compromise. For instance, in 2014, a group known as Dragonfly (also called Energetic Bear) targeted energy firms in North America and Europe, including gas pipeline operators, using spear-phishing and watering hole attacks to collect sensitive information and map out critical control systems (Khan et al., 2023).

More recently, in 2023, cybersecurity researchers reported targeted attacks on hydrogen production and distribution networks in Europe, although most incidents have not been publicly disclosed in detail due to the sensitive nature of the infrastructure involved. For example, Fig. 2 highlights 905 ransomware incidents in 2023, and almost half of these were reported in North America (Dragos, 2024b). These attacks underline the emerging focus of cybercriminals and state-sponsored groups on the hydrogen sector as it scales toward commercial maturity. These case studies collectively illustrate that the threat is not hypothetical—it is

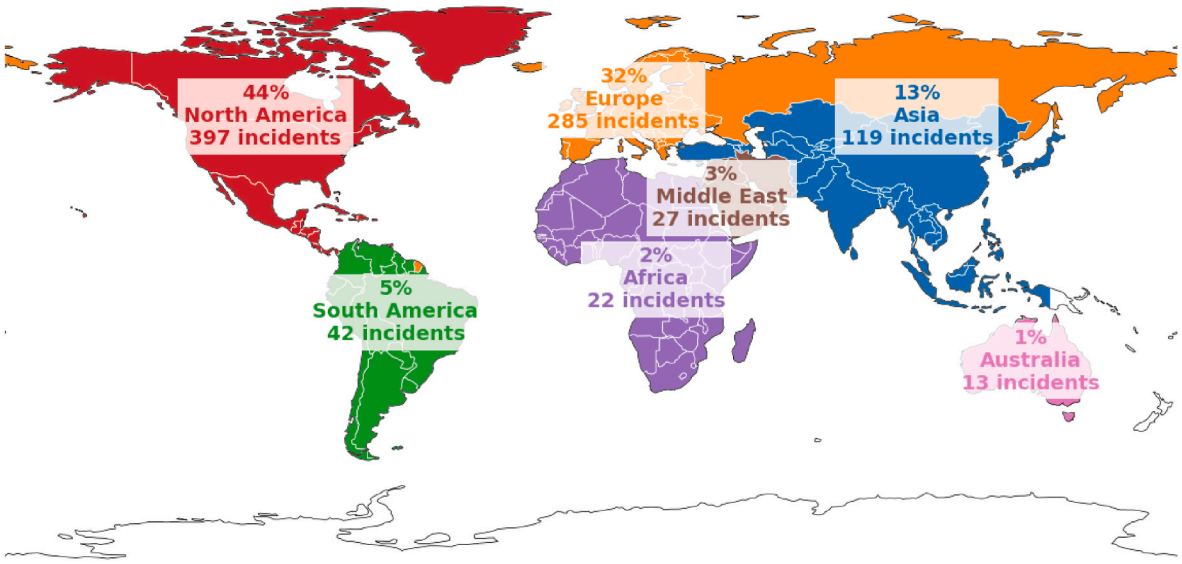

Fig. 2. Reported Ransomware Events Globally in 2023, data adapted from (Dragos, 2024b).

real, persistent, and evolving. Moreover, they demonstrate how even seemingly minor breaches in peripheral systems (such as IT networks or third-party vendors) can cascade into significant operational and security risks.

3.2. Common threat vectors

As Fig. 3 shows, there are eight common types of cyber threat vectors, whereas the ransomware is the most common reported type. Cyber adversaries employ a diverse arsenal of techniques to compromise systems in the natural gas and hydrogen industries. These attack vectors exploit both technological weaknesses and human vulnerabilities. Some of the most common and dangerous vectors include (Ding et al., 2023; NIST; 2024a; Saxena et al., 2025; Vijayshankar et al., 2023). Phishing and Spear-Phishing Attacks: These are among the most prevalent attack methods, involving deceptive emails designed to trick employees into clicking malicious links, downloading malware, or revealing login credentials. In targeted spear-phishing campaigns, attackers customize messages to appear highly authentic, impersonating trusted individuals or organizations (Mohamed et al., 2025).

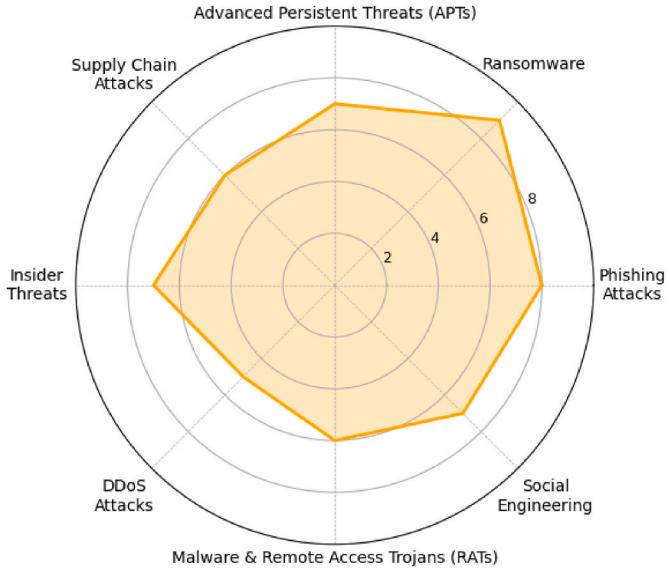

Fig. 3. Relative cyber-risk profile for the natural-gas and hydrogen value chains. Each axis shows a composite risk score from 0 (negligible) to 10 (very high), calculated by combining the historical frequency of each attack type with its average operational and safety impact reported in the literature.

Ransomware: Ransomware is malware that encrypts files or locks systems until a ransom is paid. It has increasingly been used against energy infrastructure due to its high potential for disruption and the likelihood of ransom payment. Variants such as Ryuk, DarkSide, and Conti have caused widespread outages in industrial sectors (Beerman et al., 2023).

Advanced Persistent Threats (APTs): APTs are sophisticated, stealthy, and prolonged attacks often carried out by nation-state actors. These threats involve a step-by-step compromise of networks, often starting with a low-privilege system and gradually escalating access. The goal is often espionage, sabotage, or preparation for future attacks (Jeun et al., 2012).

Supply Chain Attacks: Compromising a supplier's systems or software can provide an attacker with a backdoor into energy networks. The SolarWinds attack in 2020 is a notable example, in which attackers inserted malicious code into software updates that were distributed to numerous government and corporate networks.

Insider Threats: Employees or contractors with authorized access can intentionally or unintentionally cause security breaches. These threats are particularly difficult to detect and defend against, and can be amplified in environments where access controls and audit mechanisms are weak (Urciuoli et al., 2014).

Malware and Remote Access Trojans (RATs): These tools allow attackers to remotely control compromised systems. Once inside a network, malware can manipulate industrial processes, disable safety systems, or transmit sensitive data (Kovanen et al., 2018; Venkatachary et al., 2018).

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Although less common in industrial control environments, DoS attacks can flood network components or servers, rendering services unavailable and distracting cybersecurity teams from more sophisticated threats (Salim et al., 2020).

Each of these vectors poses unique challenges to detection, response, and mitigation. The sophistication of tools used by attackers continues to grow, often outpacing defensive capabilities in organizations that have not invested in modern cybersecurity measures.

3.3. Economic and operational impacts

The consequences of cyber-attacks in the natural gas and hydrogen

sectors can be catastrophic, not only from an operational standpoint but also in terms of economic losses, safety hazards, and reputational damage. These impacts are often multi-dimensional and can extend beyond the immediate aftermath of an incident.

Disruptions to pipeline monitoring systems, valve controls, or gas flow metering systems can halt operations, delay deliveries, and lead to cascading outages across dependent systems. In hydrogen production, disruption of electrolyzer controls or fuel dispensing systems can bring operations to a halt, affecting downstream users and supply contracts. Beyond direct revenue loss due to halted operations, companies may incur significant costs for forensic investigations, system recovery, legal liabilities, and ransom payments. The Colonial Pipeline attack, for example, involved a $4.4 million ransom and subsequent system overhaul costs. Energy companies are trusted custodians of public infrastructure. A successful cyber-attack can severely damage customer trust, brand reputation, and investor confidence—particularly if the incident is mishandled or perceived to be due to negligence. Governments and industry regulators may impose penalties or require mandatory audits in the aftermath of a cyber-attack, particularly if the company is found to be non-compliant with security regulations. This can further increase the financial and administrative burden on organizations. Perhaps the most alarming impact is the potential compromise of safety systems. Cyber-attacks that disable pressure relief valves, gas leak detection systems, or emergency shutdown mechanisms can lead to fires, explosions, or toxic releases. In hydrogen infrastructure, where containment and leak management are critical, such attacks pose a heightened risk. As both natural gas and hydrogen are increasingly integrated into regional and global supply networks, a cyber-attack on one facility or distribution node can ripple through the supply chain, affecting multiple stakeholders and economic sectors.

In summary, the costs of inadequate cybersecurity in the energy sector are not abstract—they are tangible, substantial, and growing. As threats become more sophisticated and targeted, the need for comprehensive and proactive cybersecurity strategies becomes increasingly urgent.

4. Challenges and barriers

While the importance of cybersecurity in the natural gas and hydrogen industries is well understood, implementing robust protective measures is fraught with technical, organizational, and regulatory challenges. These barriers hinder the adoption of advanced security practices and expose critical infrastructure to escalating threats. Rapid digital transformation, driven by advanced analytics, remote monitoring, and AI-enabled process control, has expanded the attack surface faster than protective technologies have matured. At the same time, threat actors have grown more sophisticated, shifting from opportunistic malware to coordinated campaigns that exploit zero-day vulnerabilities and supply-chain weaknesses. The energy transition itself introduces additional exposure: hydrogen blending, underground storage, and new power-to-gas facilities all carry distinct cybersecurity profiles that remain insufficiently characterized. These converging factors heighten risk and complicate defense strategies, demanding a holistic response that integrates technical innovation with organizational culture and supportive policy. These barriers hinder the adoption of advanced security practices and expose critical infrastructure to escalating threats. In this section, we discuss the key obstacles impeding progress toward a secure digital energy landscape.

4.1. Technical challenges

The technical complexity of securing critical energy infrastructure stems largely from the legacy nature of many operational systems and the increasing convergence of IT and OT environments. A major challenge is the prevalence of outdated ICS and SCADA systems (Gaiceanu et al., 2020). These systems often operate on proprietary protocols and are built for deterministic, real-time control rather than flexible or secure communication. Many lack basic security features such as user authentication, encryption, or patch management capabilities (Andoni et al., 2019). Updating or replacing these systems is a significant technical hurdle, as downtime may not be tolerable in continuous operations like gas pipeline monitoring or hydrogen production.

Furthermore, system heterogeneity is a persistent issue (Ding et al., 2023). In a typical energy facility, components from multiple vendors—often with incompatible security mechanisms—must work together. Integrating modern security solutions into such an environment requires extensive customization, testing, and often workarounds that may weaken overall security posture. Real-time requirements of OT systems also pose a challenge (El-Afifi et al., 2024). Unlike traditional IT systems where brief delays may be acceptable, energy systems demand immediate response to sensor inputs and actuator commands. Security solutions such as packet inspection, anomaly detection, or access control must be designed with minimal latency, otherwise they risk degrading system performance or causing control failures. Another barrier is the difficulty in testing security updates or changes in a live environment. Unlike office IT systems, many ICS and SCADA components cannot be rebooted or taken offline for routine updates without disrupting critical services. This often results in postponed or skipped security patches, leaving systems exposed to known vulnerabilities. Additionally, visibility across networks remains limited in many industrial environments. Operators often lack comprehensive tools to monitor all assets, detect anomalies, or map communication flows. This impairs their ability to identify early signs of compromise or assess the impact of an intrusion.

Lastly, interoperability with cloud platforms and remote access systems is increasingly common but often introduces additional risks (Markovic et al., 2013). Secure integration of cloud services, virtual private networks (VPNs), and third-party access tools requires sophisticated identity management and encryption strategies—capabilities not always readily available in traditional OT environments.

4.2. Organizational challenges

Beyond technical limitations, numerous organizational and cultural factors impede the implementation of effective cybersecurity programs in the natural gas and hydrogen industries (Dragos, 2024a, 2024b). One critical issue is the shortage of skilled cybersecurity professionals, particularly those with knowledge of both IT and OT systems. The hybrid expertise required to secure industrial environments is rare, and competition for qualified personnel is intense across sectors. This talent gap limits the ability of organizations to design, implement, and maintain advanced cybersecurity frameworks. Moreover, cybersecurity often competes with other operational priorities. In environments where safety, uptime, and production targets dominate management focus, cybersecurity is sometimes viewed as an auxiliary or compliance-driven function rather than a core business enabler. This mindset can lead to underfunded security teams, inadequate training programs, and reactive instead of proactive security practices.

Resistance to organizational change is another significant barrier. The adoption of new security protocols, technologies, or reporting systems often encounters pushback from operational teams who perceive them as disruptive or burdensome. This is particularly true in legacy-heavy organizations where manual procedures and informal practices are deeply embedded in daily workflows. There is also a tendency to treat cybersecurity as an IT problem, rather than a cross-functional challenge that requires collaboration across engineering, operations, legal, procurement, and executive leadership. Without clear ownership and cross-departmental coordination, security initiatives may become fragmented, poorly integrated, or insufficiently enforced. Communication gaps between IT and OT personnel further exacerbate the problem. These teams often operate with different priorities, terminologies, and decision-making processes. Building a common understanding and joint governance structure is essential for integrated cybersecurity risk

management. Finally, insufficient awareness and training at all organizational levels—especially among field operators and maintenance staff—leaves critical systems vulnerable to social engineering, insider threats, and accidental breaches. Regular training, simulations, and awareness campaigns are vital but are often neglected or underprioritized.

4.3. Policy and regulation gaps

While regulatory frameworks have evolved in recent years, there remain significant policy and compliance challenges that hamper the secure operation of gas and hydrogen infrastructure (Ekechukwu and Simpa, 2024; Krzykowski, 2021; Kumar et al., 2014; Saxena et al., 2025; Smith, 2018). One major concern is the lack of harmonized international cybersecurity standards. As energy supply chains increasingly cross borders, the disparity between national regulations creates compliance uncertainty and undermines collective security. A company operating across different jurisdictions may be subject to varying requirements on risk assessments, reporting timelines, audit criteria, and penalties, complicating implementation and oversight. Moreover, many existing regulations are reactive and prescriptive, focusing on static compliance checklists rather than encouraging continuous improvement or outcome-based security performance. In rapidly evolving threat landscapes, such frameworks risk becoming outdated and may fail to drive adaptive risk management practices.

In some regions, cybersecurity regulations do not adequately address the unique requirements of OT environments. While general data protection laws (e.g., GDPR) and IT security standards (e.g., ISO/IEC 27001) are widely enforced, sector-specific guidelines for ICS, SCADA, and hydrogen infrastructure are either underdeveloped or inconsistently applied (ISO/IEC27001, 2022). There is also ambiguity around liability and incident disclosure. Organizations often hesitate to report breaches due to fear of reputational damage or legal consequences, leading to underreporting and delayed threat intelligence sharing (Mishra et al., 2022). Clear rules on mandatory reporting, data anonymization, and legal protections for victims are essential to foster a more transparent and collaborative cybersecurity ecosystem. Another gap lies in funding and resource support for smaller operators. While large energy companies may have the resources to implement cutting-edge cybersecurity measures, smaller entities and municipal utilities often struggle to keep pace. Without financial incentives, technical assistance, or shared cybersecurity services, these actors may become the weakest links in the energy ecosystem. Finally, the pace of policy development often lags behind technological change. Emerging technologies like AI, blockchain, digital twins, and hydrogen-specific infrastructure are outpacing the ability of regulatory bodies to assess risks and update standards. A more agile and anticipatory policy approach is needed to keep pace with innovation and evolving threats.

5. Emerging trends and innovations

As cyber threats become more sophisticated and pervasive, the energy industry is responding with a wave of innovation in cybersecurity technologies, methodologies, and collaborative approaches as illustrated in Fig. 4. These innovations not only enhance the defensive posture of natural gas and hydrogen infrastructure but also offer proactive tools to anticipate, mitigate, and recover from cyber incidents. This section explores key trends that are shaping the future of cybersecurity in the energy sector.

5.1. Quantum computing and blockchain

Two of the most transformative technologies on the cybersecurity horizon are quantum computing and blockchain—each with significant implications for the energy sector(Ajagekar and You, 2019, 2022; Andoni et al., 2019; Bao et al., 2020; Giani and Eldredge, 2021; Khang et al., 2024; Olatunji et al., 2021; Paudel et al., 2022; Ricciardi Celsi and Ricciardi Celsi, 2024; Wang and Su, 2020). Quantum Computing presents both a challenge and an opportunity. On one hand, the development of quantum computers poses a threat to conventional encryption algorithms such as RSA and ECC (Elliptic Curve Cryptography), which underpin much of today's cybersecurity infrastructure. Once quantum computing reaches sufficient scale, it could potentially break these cryptographic systems within seconds, rendering traditional secure communications vulnerable. On the other hand, the energy sector is exploring quantum-resistant cryptographic protocols to prepare for the post-quantum era. These new cryptographic algorithms—based on lattice structures, hash functions, or code-based encryption—are being tested for secure communication in energy control systems. Quantum Key Distribution (QKD), which uses the principles of quantum mechanics to enable unhackable key exchanges, is also being considered for high-security applications in gas and hydrogen infrastructure.

Blockchain technology, originally developed to support cryptocurrencies, is being repurposed in the energy sector to enhance data integrity, transparency, and decentralized trust. In cybersecurity, blockchain offers tamper-proof logging systems, secure identity management, and immutable audit trails. For instance, blockchain can be used to record all system access attempts, firmware updates, or data transmissions in SCADA systems. This ensures that any unauthorized change or breach leaves an unalterable record, facilitating forensic analysis and accountability. In hydrogen supply chains, blockchain enables secure tracking of hydrogen provenance—from production to

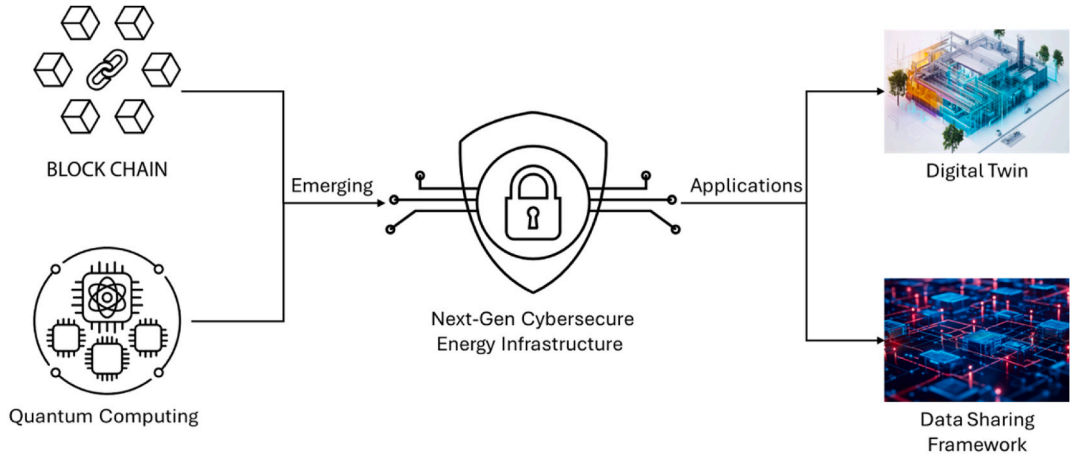

Fig. 4. Demonstration of emerging technological innovations and applications.

distribution—helping prevent fraud, data manipulation, and counterfeit documentation. Moreover, blockchain-based access control systems are being explored, where smart contracts automatically manage permissions based on predefined rules. These systems minimize human error, eliminate reliance on centralized authentication servers, and enhance resilience against insider threats.

While these technologies are still emerging and face scalability and integration challenges, they represent the next frontier in cybersecurity innovation for critical infrastructure.

5.2. Digital twins

Digital twins are rapidly becoming a cornerstone of modern industrial operations, offering advanced simulation and monitoring capabilities that enhance both operational efficiency and cybersecurity readiness (Borowski, 2021; Ismail et al., 2024; Jiang et al., 2021; Kronberger et al., 2020; Nixon, 2020; Sleiti et al., 2022; Strielkowski et al., 2022; Yu et al., 2022). A digital twin is a virtual replica of a physical asset, system, or process. It continuously receives data from real-world counterparts and mirrors their behavior in real-time, allowing operators to observe, analyze, and optimize performance without interacting directly with physical systems.

In the context of cybersecurity, digital twins offer several distinct advantages. First, digital twins provide a sandbox environment where new software patches, security updates, or architectural changes can be tested for vulnerabilities before deployment in live systems. Second, cybersecurity teams can simulate attack scenarios on the digital twin to assess system resilience, identify weak points, and refine response protocols—without risking disruption to operational systems. Third, digital twins allow AI systems to compare real-time operational data against baseline behavioral models. Discrepancies may indicate the presence of malicious activity, compromised devices, or abnormal data manipulation. Finally, digital twins can be used to reconstruct attack sequences, assess damage, and understand adversary tactics, techniques, and procedures (TTPs). This helps improve future defensive strategies and regulatory reporting. Last, digital twins can be used for immersive training simulations, enabling operators to experience cyber incident scenarios and learn best practices in a controlled environment.

In natural gas and hydrogen infrastructure, where systems are inherently high-risk due to explosive gas storage and high-pressure operations, digital twins offer critical safeguards. They allow for comprehensive stress testing of safety interlocks, fail-safe mechanisms, and emergency response systems under simulated cyber-attack conditions.

5.3. Collaboration and information sharing

Cybersecurity is no longer a challenge that individual organizations can tackle in isolation. The rise of collaborative cybersecurity models and information-sharing platforms is transforming how energy companies respond to threats and build collective resilience (Ekechukwu and Simpa, 2024; Fraccascia and Yazan, 2018; Liu et al., 2022; Mohamed, 2024; Sharkov, 2016; Tagarev and Yanakiev, 2020; Wallis and Dorey, 2023). One key development is the growth of Information Sharing and Analysis Centers (ISACs)—sector-specific consortia that collect, analyze, and disseminate cyber threat intelligence among member organizations. The Energy ISAC (E-ISAC), for example, supports utilities, pipeline operators, and hydrogen producers by providing threat alerts, vulnerability bulletins, and best practice guides. These shared resources accelerate response times and reduce duplication of effort across the industry. Similarly, government-industry partnerships are being strengthened through programs such as the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), which conducts joint exercises, shares threat indicators, and supports critical infrastructure operators with risk assessments and response planning. Public-private partnerships (PPPs) also play a vital role in coordinating cyber policy development, funding cybersecurity research, and fostering innovation. These partnerships help align industrial practices with national security priorities and ensure that emerging threats are addressed collectively.

Moreover, cross-border collaboration is becoming increasingly important as energy infrastructure and supply chains become more global. International cooperation on threat intelligence sharing, regulatory harmonization, and coordinated incident response is essential to address threats that transcend national boundaries. Emerging platforms are also using machine-readable threat intelligence formats, such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information), to automate the sharing of threat indicators between organizations. These standards facilitate faster and more accurate threat detection across diverse systems and geographies.

Finally, open-source cybersecurity communities and industry working groups are contributing to the development of free tools, shared vulnerability databases, and standardized practices that benefit the entire sector. Collaborative tools and intelligence sharing not only improve cyber readiness but also foster a culture of collective defense and mutual trust.

6. Future perspectives

As the natural gas and hydrogen sectors continue to evolve in response to decarbonization imperatives and digital transformation, so too must their cybersecurity strategies. The future will likely be characterized by increasingly complex, interconnected, and intelligent infrastructure, necessitating proactive and adaptive security mechanisms that go beyond traditional paradigms. Accelerated deployment of smart sensors, autonomous control systems, and cross-border data exchanges is blurring the once-distinct boundaries between information technology IT and OT, expanding the attack surface beyond what conventional perimeter defenses can protect. Simultaneously, policy instruments such as clean-hydrogen tax credits and carbon-intensity certification schemes are driving operators toward cloud-based analytics and third-party validation platforms, introducing new trust dependencies into mission-critical workflows. The growing interdependence of gas and hydrogen value chains—through blending, co-transport, and shared storage—means that a cyber incident in one domain can cascade rapidly into the other, amplifying systemic risk. These dynamics demand security-by-design principles, real-time situational awareness, and adaptive risk-management frameworks that evolve in lockstep with technological innovation. This section explores key forward-looking themes that are shaping the future of cybersecurity in these industries.

6.1. Evolving threat landscape

The cybersecurity threat landscape is undergoing a profound transformation, marked by increased sophistication, persistence, and scale of attacks. Cyber adversaries are no longer limited to individual hackers or loosely organized cybercriminal groups. Instead, state-sponsored threat actors, advanced organized cybercrime syndicates, and cyberterrorist organizations are leveraging powerful tools and resources to target critical infrastructure with strategic intent. Emerging technologies such as AI and ML, which are valuable tools for defenders, are equally being exploited by attackers. AI-powered malware, for instance, can evade traditional detection mechanisms by dynamically changing its behavior or adapting to defensive measures in real time. Similarly, deepfake technologies may soon be used in social engineering attacks, impersonating voice commands or digital identities to bypass security protocols.

Additionally, the expanding attack surface, driven by the proliferation of IoT devices, remote monitoring tools, and cloud-based platforms, introduces new vulnerabilities that require constant vigilance. Edge computing, while enhancing data processing efficiency, also

decentralizes security control, making consistent threat management more complex. Hybrid threats, where cyber-attacks are combined with physical sabotage, disinformation campaigns, or economic coercion, are expected to rise in frequency. These hybrid threats may be part of broader geopolitical strategies aimed at undermining energy security and public trust. In this context, cybersecurity must evolve from a static control model to a resilient, adaptive, and intelligence-driven approach. This involves continuous risk assessment, proactive threat hunting, and a shift from prevention-only models to rapid detection, containment, and recovery.

6.2. Cybersecurity in the hydrogen economy

The growing prominence of hydrogen as a cornerstone of the future clean energy economy introduces a new set of cybersecurity considerations. Unlike natural gas infrastructure, which benefits from decades of operational and security experience, hydrogen infrastructure is relatively nascent, and its unique characteristics necessitate customized protection strategies. Hydrogen systems involve specialized components such as electrolyzers, fuel cells, cryogenic storage tanks, high-pressure pipelines, and refueling stations. These assets have unique operational and safety requirements, which in turn influence their cybersecurity needs. For example, electrolyzers and hydrogen production plants often integrate advanced power electronics and smart control systems, which must be protected from manipulation that could cause unsafe voltage fluctuations or gas leakage. Hydrogen storage and transport systems, especially those operating at very high pressures, are highly sensitive to system integrity. A cyber-induced malfunction in valve control or pressure regulation systems could lead to catastrophic failures. Hydrogen refueling infrastructure, which includes digital payment interfaces and IoT-connected dispensers, must be secured not only from operational sabotage but also from financial fraud and data breaches.

Given the rapid expansion of hydrogen infrastructure—often funded through public-private partnerships or government subsidies—there is a pressing need to embed security-by-design principles from the outset. This includes secure system architectures, robust authentication protocols, encrypted data channels, and anomaly detection systems tailored to hydrogen-specific operational dynamics. Moreover, cyber risk assessments and impact modeling must become standard practice in hydrogen project planning, regulatory approval, and insurance underwriting. Tools such as digital twins can play a critical role in simulating cyber-attack scenarios and stress-testing infrastructure resilience. To ensure long-term security, the hydrogen economy must also invest in workforce development, cybersecurity standards, and cross-sector coordination mechanisms that reflect its unique infrastructure profile.

6.3. Research and innovation roadmap

Bridging the economic and policy gaps will require a coordinated programme of technical breakthroughs and economic-policy instruments that mature in parallel. On the technical front, future work should prioritise the deployment of zero-trust architectures that collapse the traditional IT/OT divide, subject every device to continuous authentication, and enforce least-privilege access in real time. Achieving this in latency-sensitive environments will depend on lightweight, AI-driven intrusion-detection models capable of running on embedded controllers and flagging anomalous process signals within sub-second windows. Complementary advances in quantum-resilient cryptography and software-defined networking can harden long-lived pipeline, compressor, and electrolyser assets against the inevitable arrival of post-quantum threats, while blockchain-backed event ledgers offer tamper-proof provenance for sensor data and maintenance logs. Digital-twin platforms should evolve from engineering simulators into full-spectrum cyber-range testbeds where operators rehearse attack scenarios, quantify cascading effects, and validate patch strategies before field deployment; coupling these twins to physics-based hydrogen safety models will be essential for high-pressure storage and refueling systems.

Economic research must proceed hand in hand with these technical innovations. Robust cost–benefit frameworks are needed to translate avoided downtime, safety incidents, and reputational losses into monetizable "cyber value at risk" metrics that can guide capital budgeting and justify security-by-design investments. Such metrics underpin performance-based cyber-insurance products that reward auditable risk reductions rather than mere compliance, thereby creating continuous improvement incentives for operators and service vendors alike. Public-private financing mechanisms, ranging from cybersecurity tax credits for small and medium-sized pipeline operators to co-funded hydrogen "living labs" that share threat-intelligence data, can lower adoption barriers and diffuse best practices across supply chains. Finally, regulatory sandboxes that allow controlled experimentation with adaptive security controls and dynamic compliance reporting will help policymakers keep pace with rapid technological change, while harmonized international standards can remove jurisdictional fragmentation and enable economies of scale in security tooling.

By interweaving these technical and economic threads, the roadmap offers a pragmatic path toward closing today's protection gaps and future-proofing the natural-gas and hydrogen sectors as they scale to meet global decarbonization goals.

7. Conclusions

The natural gas and hydrogen industries stand at a pivotal juncture in the global energy transition, serving as key enablers of decarbonization, energy diversification, and industrial transformation. As these sectors increasingly embrace digital technologies to optimize operations, reduce costs, and enhance sustainability, they also face a growing array of cybersecurity challenges that threaten the safety, reliability, and resilience of critical infrastructure.

This review has illustrated how digital transformation—though vital for modernization—significantly expands the cyber-attack surface. The convergence of OT and IT has introduced a complex ecosystem where legacy systems interact with smart sensors, cloud platforms, and remote interfaces. In this interconnected landscape, traditional perimeter defenses are insufficient, and proactive, layered cybersecurity strategies have become essential.

Historical cyber-attacks such as the Colonial Pipeline incident and the broader wave of ransomware and APT campaigns have demonstrated that energy infrastructure is not only vulnerable but also strategically attractive to malicious actors. The impacts of such attacks extend beyond operational downtime and financial losses—they can disrupt national economies, compromise environmental safety, and erode public trust in critical services. In response, the natural gas and hydrogen sectors must embrace a multifaceted cybersecurity approach grounded in risk management, resilience engineering, and continuous innovation. This includes adopting advanced security frameworks, leveraging AI and machine learning for threat detection, implementing zero-trust architectures, and investing in incident response and disaster recovery capabilities. Emerging technologies—such as quantum-resistant encryption, blockchain-integrated audit systems, and digital twins—offer promising avenues for strengthening defense mechanisms. However, their successful deployment requires foresight, investment, and multidisciplinary expertise.

Emerging safeguards, such as AI-driven anomaly detection, zero-trust architectures, blockchain-based audit trails, and quantum-resistant encryption, equip policymakers to move beyond static compliance checklists toward agile, performance-based regulations. By leveraging these innovations, regulators can mandate continuous monitoring, incentivize real-time information sharing, and align investment or tax-credit mechanisms with demonstrable cyber-resilience metrics. In this way, technical progress directly informs policy design, ensuring that governance frameworks keep pace with an evolving threat landscape.

Looking forward, the rise of the hydrogen economy brings both opportunities and responsibilities. As hydrogen infrastructure scales globally, it must not replicate the cybersecurity oversights of legacy energy systems. Instead, security-by-design principles, continuous threat modeling, and industry-wide knowledge sharing must become embedded in its development from inception. Because cybersecurity research focused on natural gas and hydrogen infrastructure is still in its early stage. This review therefore relies on a relatively small set of studies, supplemented by industry reports whose methodologies are not always transparent. The rapid evolution of technologies such as AI-based threat detection and next-generation hydrogen facilities means that some cited work may become outdated quickly. Proprietary or classified incident data also restrict the level of empirical validation available in the public domain. These constraints underscore the need for periodic updates, open data-sharing initiatives, and deeper cross-disciplinary collaboration to keep the knowledge base up to date and actionable.

In sum, cybersecurity is no longer a technical afterthought—it is a strategic cornerstone of modern energy systems. It must be integrated into every layer of infrastructure planning, system design, and operational execution. Through collaboration, innovation, and vigilance, the natural gas and hydrogen sectors can build the cyber resilience required to thrive in a dynamic, digitalized, and decarbonized world.

CRediT authorship contribution statement

Haoming Ma: Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Yang Lu:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Zuhao Kou:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Zhenqian Xue:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Wei Yu:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Kai Zhang:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Peng Deng:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Chaojie Di:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Yuanrui Zhu:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Hao Wang:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Zhangxing Chen:** Writing – review & editing, Writing – original draft, Conceptualization.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used AI language model ChatGPT-o3 by OpenAI in order to improve the grammar and readability. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Ajagekar, A., You, F., 2019. Quantum computing for energy systems optimization: challenges and opportunities. ENERGY 179, 76–89.

Ajagekar, A., You, F., 2022. Quantum computing and quantum artificial intelligence for renewable and sustainable energy: a emerging prospect towards climate neutrality. Renew. Sustain. Energy Rev. 165, 112493.

Akberdina, V., Osmonova, A., 2021. Digital Transformation of Energy Sector Companies. E3S Web of Conferences.

Amaral, J.V.S., dos Santos, C.H., Montevechi, J.A.B., de Queiroz, A.R., 2023. Energy digital twin applications: a review. Renew. Sustain. Energy Rev. 188. https://doi.org/10.1016/j.rser.2023.113891.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A., 2019. Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 100, 143–174. https://doi.org/10.1016/j.rser.2018.10.014.

Bao, J., He, D., Luo, M., Choo, K.-K.R., 2020. A survey of blockchain applications in the energy sector. IEEE Syst. J. 15 (3), 3370–3381.

Beerman, J., Berent, D., Falter, Z., Bhunia, S., 2023. A review of colonial pipeline ransomware attack. In: 2023 IEEE/ACM 23rd international symposium on cluster, cloud and internet computing workshops (CCGridW), Bangalore, India, pp. 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017.

Bhattacharjee, S., Nandi, C., 2019. Implementation of Industrial Internet of Things in the Renewable Energy Sector. *the Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0*, pp. 223–259.

Borowski, P.F., 2021. Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. Energies 14 (7), 1885.

Borowski, P.F., 2022. Digital transformation and prosumers activities in the energy sector. In: Intelligent Systems in Digital Transformation: Theory and Applications. Springer, pp. 129–150.

Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S., 2011. Attacks against process control systems: risk assessment, detection, and response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China. https://doi.org/10.1145/1966913.1966959.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap. Risk Insur. - Issues Pract. 47 (3), 698–736. https://doi.org/10.1057/s41288-022-00266-6.

Di Pinto, A., Dragoni, Y., Carcano, A., 2018. TRITON: the first ICS cyber attack on safety instrument systems. Proc. Black Hat USA 2018, 1–26.

Diaba, S.Y., Shafie-khah, M., Elmusrati, M., 2024. Cyber-physical attack and the future energy systems: a review. Energy Rep. 12, 2914–2932. https://doi.org/10.1016/j.egyr.2024.08.060.

Ding, S., Lu, S., Xu, Y., Korkali, M., Cao, Y., 2023. Review of cybersecurity for integrated energy systems with integration of cyber-physical systems. Energy Conversion and Economics 4 (5), 334–345.

Doan, Q.T., Kayes, A.S.M., Rahayu, W., Nguyen, K., 2020. Integration of IoT streaming data with efficient indexing and storage optimization. IEEE Access 8, 47456–47467. https://doi.org/10.1109/ACCESS.2020.2980006.

Dragos, 2024a. 5 CRITICAL CONTROLS FOR WORLD-CLASS OT CYBERSECURITY.

Dragos, 2024b. OT CYBERSECURITY THE 2023 YEAR IN REVIEW.

Ekechukwu, D.E., Simpa, P., 2024. The future of cybersecurity in renewable energy systems: a review, identifying challenges and proposing strategic solutions. Computer Science & IT Research Journal 5 (6), 1265–1299.

El-Afifi, M.I., Sedhom, B.E., Padmanaban, S., Eladl, A.A., 2024. A review of IoT-enabled smart energy hub systems: rising, applications, challenges, and future prospects. Renew. Energy Focus 51, 100634. https://doi.org/10.1016/j.ref.2024.100634.

ENISA, 2025. Cybersecurity of critical sectors - energy. Retrieved April 21 from. https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors.

European Commission, 2025. NIS2 directive: new rules on cybersecurity of network and information systems. Shaping Europe's digital future. Retrieved April 21 from. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Fraccascia, L., Yazan, D.M., 2018. The role of online information-sharing platforms on the performance of industrial symbiosis networks. Resour. Conserv. Recycl. 136, 473–485. https://doi.org/10.1016/j.resconrec.2018.03.009.

Gaiceanu, M., Stanculescu, M., Andrei, P.C., Solcanu, V., Gaiceanu, T., Andrei, H., 2020. Intrusion detection on ics and scada networks. Recent Developments on Industrial Control Systems Resilience, pp. 197–262.

Giani, A., Eldredge, Z., 2021. Quantum computing opportunities in renewable energy. SN Computer Science 2 (5), 393.

Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., Zakeri, B., 2020. Internet of things (IoT) and the energy sector. Energies 13 (2), 494.

IEA, 2024a. Energy and AI.

IEA, 2024b. Energy Technology Perspectives 2024.

IEA, 2024c. Global Hydrogen Review 2024.

IEA, 2024d. World Energy Outlook 2024.

Ismail, F.B., Al-Faiz, H., Hasini, H., Al-Bazi, A., Kazem, H.A., 2024. A comprehensive review of the dynamic applications of the digital twin technology across diverse energy sectors. Energy Strategy Rev. 52, 101334.

ISO/IEC27001, 2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. International Organization for Standardization/International Electrotechnical Commission, Geneva, 2022.

Jeun, I., Lee, Y., Won, D., 2012. A practical study on advanced persistent threats. In: Computer Applications for Security, Control and System Engineering: International

Conferences, SecTech, CA, CES 3 2012, Held in Conjunction with GST 2012, Jeju Island, Korea, November 28-December 2, 2012, pp. 144–152.
Jiang, Y., Yin, S., Li, K., Luo, H., Kaynak, O., 2021. Industrial applications of digital twins. Philosophical Transactions of the Royal Society A 379 (2207), 20200360.
Khan, F.B., Asad, A., Durad, H., Mohsin, S.M., Kazmi, S.N., 2023. Dragonfly cyber threats: a case study of malware attacks targeting power grids. Journal of Computing & Biomedical Informatics 4 (2), 172–185.
Khang, A., Hajimahmud, V.A., Ali, R.N., Alyar, A.V., Khalilov, M., Murad, B., Litvinova, E., 2024. Quantum computing in oil and gas exploration industry. In: The Quantum Evolution. CRC Press, pp. 373–385.
Kovanen, T., Nuojua, V., Lehto, M., 2018. Cyber threat landscape in energy sector. ICCWS 2018 13th International Conference on Cyber Warfare and Security.
Kronberger, P., Dabrowski, P., Chacon, J., Bangert, P., 2020. The digitalization journey of the brage digital twin. https://doi.org/10.2118/200728-MS.
Krzykowski, M., 2021. Legal aspects of cybersecurity in the energy sector—current state and latest proposals of legislative changes by the EU. Energies 14 (23), 7836.
Kumar, V.A., Pandey, K.K., Punia, D.K., 2014. Cyber security threats in the power sector: need for a domain specific regulatory framework in India. Energy Policy 65, 126–133.
Lal, A., You, F., 2024. Climate sustainability through a dynamic duo: green hydrogen and crypto driving energy transition and decarbonization. Proc. Natl. Acad. Sci. U. S. A. 121 (14), e2313911121. https://doi.org/10.1073/pnas.2313911121.
Liu, J., Huang, Z., Fan, M., Yang, J., Xiao, J., Wang, Y., 2022. Future energy infrastructure, energy platform and energy storage. Nano Energy 104, 107915. https://doi.org/10.1016/j.nanoen.2022.107915.
Lu, H., Huang, K., Azimi, M., Guo, L., 2019. Blockchain technology in the oil and gas industry: a review of applications, opportunities, challenges, and risks. IEEE Access 7, 41426–41444. https://doi.org/10.1109/access.2019.2907695.
Ma, H., Chen, S., Xue, D., Chen, Y., Chen, Z., 2021. Outlook for the coal industry and new coal production technologies. Advances in Geo-Energy Research 5 (2), 119–120. https://doi.org/10.46690/ager.2021.02.01.
Ma, H., Yang, Y., Zhang, Y., Li, Z., Zhang, K., Xue, Z., Zhan, J., Chen, Z., 2022. Optimized schemes of enhanced shale gas recovery by CO2-N2 mixtures associated with CO2 sequestration. Energy Convers. Manag. 268. https://doi.org/10.1016/j.enconman.2022.116062.
Ma, C.-Q., Lei, Y.-T., Ren, Y.-S., Chen, X.-Q., Wang, Y.-R., Narayan, S., 2023. Systematic analysis of the blockchain in the energy sector: trends, issues, and future directions. Telecommun. Policy. https://doi.org/10.1016/j.telpol.2023.102677.
Ma, H., Sun, Z., Xue, Z., Zhang, C., Chen, Z., 2023a. A systemic review of hydrogen supply chain in energy transition. Front. Energy. https://doi.org/10.1007/s11708-023-0861-0.
Ma, H., Yang, Y., Xue, Z., Chen, Z., 2023b. Comparative Machine Learning Frameworks for Forecasting CO2/CH4 Competitive Adsorption Ratios in Shale. SPE Western Regional Meeting.
Ma, H., Yang, Y., Xue, Z., Clarkson, C.R., Chen, Z., 2025. Transitioning from emission source to sink: economic and environmental trade-offs for CO2-enhanced coalbed methane recovery of mannville coal Canada. SCIENCE OF THE TOTAL ENVIRONMENT 966, 178721. https://doi.org/10.1016/j.scitotenv.2025.178721.
Ma, H., McCoy, S.T., Chen, Z., 2025a. Development and comparison of reduced-order models for CO2-enhanced oil recovery predictions. ENERGY 320. https://doi.org/10.1016/j.energy.2025.135313.
Markovic, D.S., Zivkovic, D., Branovic, I., Popovic, R., Cvetkovic, D., 2013. Smart power grid and cloud computing. Renew. Sustain. Energy Rev. 24, 566–577.
Maroufkhani, P., Desouza, K.C., Perrons, R.K., Iranmanesh, M., 2022. Digital transformation in the resource and energy sectors: a systematic review. Resour. Policy 76, 102622.
Mishra, A., Alzoubi, Y.I., Anwar, M.J., Gill, A.Q., 2022. Attributes impacting cybersecurity policy development: an evidence from seven nations. Comput. Secur. 120, 102820. https://doi.org/10.1016/j.cose.2022.102820.
Mohamed, N., 2024. Renewable energy in the age of AI: cybersecurity challenges and opportunities. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, pp. 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10724383.
Mohamed, N., Taherdoost, H., Khashan, O.A., 2025. A review of AI in spear phishing defense: detecting and thwarting. EAI 3rd international conference on smart technologies and innovation management: mtymex 2024. In: Cybersecurity Framework. NIST. Retrieved April 21 from.
NIST, 2024. The NIST Cybersecurity Framework (CSF) 2.0.
Nixon, J., 2020. Digitalization deployed: lessons learned from early adopters. https://doi.org/10.4043/30794-MS.
Olatunji, O.O., Adedeji, P.A., Madushele, N., 2021. Quantum computing in renewable energy exploration: status, opportunities, and challenges. Design, Analysis, and Applications of Renewable Energy Systems 549–572.
Paudel, H.P., Syamlal, M., Crawford, S.E., Lee, Y.-L., Shugayev, R.A., Lu, P., Ohodnicki, P.R., Mollot, D., Duan, Y., 2022. Quantum computing and simulations for energy applications: review and perspective. ACS Eng. Au 2 (3), 151–196.
Ricciardi Celsi, M., Ricciardi Celsi, L., 2024. Quantum computing as a game changer on the path towards a net-zero economy: a review of the main challenges in the energy domain. Energies 17 (5), 1039.
Salim, M.M., Rathore, S., Park, J.H., 2020. Distributed denial of service attacks and its defenses in IoT: a survey. J. Supercomput. 76, 5320–5363.
Saxena, S., Saxena, S., Tahilramani, N., Patel, U., Talreja, V.P., Patel, A., 2025. Enhancing cybersecurity in sustainable energy: regulatory compliance, challenges, and policy innovations. In: 2025 International Conference on Sustainable Energy Technologies and Computational Intelligence (SETCOM), Gandhinagar, India, pp. 1–6. https://doi.org/10.1109/SETCOM64758.2025.10932340.
Sharkov, G., 2016. From cybersecurity to collaborative resiliency. Proceedings of the 2016 ACM workshop on automated decision making for active cyber defense, pp. 3–9. https://doi.org/10.1145/2994475.2994484.
Sleiti, A.K., Kapat, J.S., Vesely, L., 2022. Digital twin in energy industry: proposed robust digital twin for power plant and other complex capital-intensive large engineering systems. Energy Rep. 8, 3704–3726.
Smith, D.C., 2018. In: Enhancing Cybersecurity in the Energy Sector: a Critical Priority, vol. 36. Taylor & Francis, pp. 373–380.
Stergiopoulos, G., Gritzalis, D.A., Limnaios, E., 2020. Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns. IEEE Access 8, 128440–128475. https://doi.org/10.1109/access.2020.3007960.
Strielkowski, W., Rausser, G., Kuzmin, E., 2022. Digital revolution in the energy sector: effects of using digital twin technology. In: Digital Transformation in Industry: Digital Twins and New Business Models. Springer, pp. 43–55.
Tabaa, M., Monteiro, F., Bensag, H., Dandache, A., 2020. Green industrial internet of things from a smart industry perspectives. Energy Rep. 6, 430–446.
Tagarev, T., Yanakiev, Y., 2020. Business models of collaborative networked organisations: implications for cybersecurity collaboration. In: 2020 IEEE 11th international conference on dependable systems, services and technologies (DESSERT), Kyiv, Ukraine, pp. 431–438. https://doi.org/10.1109/DESSERT50317.2020.9125011.
Taherdoost, H., 2024. Insights into cybercrime detection and response: a review of time factor. Information 15 (5), 273. https://www.mdpi.com/2078-2489/15/5/273.
Urciuoli, L., Mohanty, S., Hintsa, J., Gerine Boekesteijn, E., 2014. The resilience of energy supply chains: a multiple case study approach on oil and gas supply chains to Europe. Supply Chain Manag.: Int. J. 19 (1), 46–63.
Venkatachary, S.K., Prasad, J., Samikannu, R., 2018. Cybersecurity and cyber terrorism-in energy Sector–a review. Journal of Cyber Security Technology 2 (3–4), 111–130.
Vijayshankar, S., Chang, C.-Y., Utkarsh, K., Wald, D., Ding, F., Balamurugan, S.P., King, J., Macwan, R., 2023. Assessing the impact of cybersecurity attacks on energy systems. APPLIED ENERGY 345, 121297. https://doi.org/10.1016/j.apenergy.2023.121297.
Wallis, T., Dorey, P., 2023. Implementing partnerships in energy supply chain cybersecurity resilience. Energies 16 (4), 1868.
Wang, Q., Su, M., 2020. Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain. Computer Science Review 37, 100275.
Xue, Z., Yao, S., Ma, H., Zhang, C., Zhang, K., Chen, Z., 2023a. Thermo-economic optimization of an enhanced geothermal system (EGS) based on machine learning and differential evolution algorithms. Fuel 340. https://doi.org/10.1016/j.fuel.2023.127569.
Xue, Z., Zhang, K., Zhang, C., Ma, H., Chen, Z., 2023b. Comparative data-driven enhanced geothermal systems forecasting models: a case study of qiabuqia field in China. ENERGY 280. https://doi.org/10.1016/j.energy.2023.128255.
Xue, Z., Zhang, Y., Ma, H., Lu, Y., Zhang, K., Wei, Y., Yang, S., Wang, M., Chai, M., Sun, Z., Deng, P., Chen, Z., 2024. A combined neural network forecasting approach for CO2-Enhanced shale gas recovery. SPE J. 29 (8), 4459–4770. https://doi.org/10.2118/219774-pa.
Xue, Z., Wei, Z., Ma, H., Sun, Z., Lu, C., Chen, Z., 2025. Exploring the role of fracture networks in enhanced geothermal systems: insights from integrated thermal-hydraulic-mechanical-chemical and wellbore dynamics simulations. Renew. Sustain. Energy Rev. 215. https://doi.org/10.1016/j.rser.2025.115636.
Yadav, G., Paul, K., 2021. Architecture and security of SCADA systems: a review. International Journal of Critical Infrastructure Protection 34, 100433. https://doi.org/10.1016/j.ijcip.2021.100433.
Yu, W., Patros, P., Young, B., Klinac, E., Walmsley, T.G., 2022. Energy digital twin technology for industrial energy management: classification, challenges and future. Renew. Sustain. Energy Rev. 161, 112407.
Zhioua, S., 2013. The Middle east under malware attack dissecting cyber weapons. 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops.