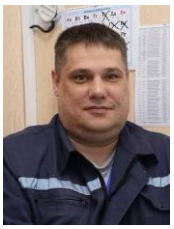
DOI: 10.18372/2225-5036.31.20706

ENERGY CRITICAL INFRASTRUCTURE UNDER ATTACK: INCIDENT ANALYSIS AND IMPLICATIONS FOR ICS/SCADA RESILIENCE

Oleksandr Dobrynchuk[1,2], Viktoriia Lukashenko[2]

[1]Khmelnytskyi Nuclear Power Plant, Ukraine
[2]State University "Kyiv Aviation Institute", Ukraine



DOBRYNCHUK Oleksandr
Year and place of birth: 1985, Dovzhky, Khmelnytskyi oblast, Ukraine
Education: National University of Water and Environmental Engineering, 2007
Position: [1]Head of the Laboratory for Special and Neutron Measurements, [2]Junior Researcher
Research Interests: critical infrastructure, energy security, ICS/SCADA resilience
Publications: 3 research papers, 1 book chapter, and 3 conference proceedings
E-mail: dobrynchuk.oleksandr@khnpp.atom.gov.ua
Orcid: 0009-0002-2877-844X

LUKASHENKO Viktoriia, D.Sc., Professor
Year and place of birth: 1982, Kyiv, Ukraine
Education: National Aviation University, 2005
Position: Head of R&D Department State University «Kyiv Aviation Institute»
Research Interests: computer networks that are tolerant to delays in control information
Publications: more than 70 works including monographs, papers and conference proceedings
E-mail: viktoriia.lukashenko@kai.edu.ua
Orcid: 0009-0009-0458-2590

Abstract. *Energy sector critical infrastructure has been increasingly targeted by cyber, physical, and hybrid attacks that exploit vulnerabilities in monitoring and control systems. This paper analyzes major security incidents affecting energy facilities over the past 10-15 years, with a particular focus on attacks that compromise measurement data, telemetry, and situational awareness. Based on incident analysis, the study identifies common attack patterns and resilience gaps and discusses their implications for the secure operation of energy systems. The paper concludes with practical recommendations for strengthening cyber resilience through measurement-aware monitoring, improved detection, and resilient recovery mechanisms in energy critical infrastructure.*
Keywords: *critical infrastructure, energy sector, ICS/SCADA, resilience, incident, attack, security, practical recommendations, power grid.*

1. Introduction

Energy critical infrastructure has become one of the primary targets of cyber, physical, and hybrid attacks due to its strategic importance for national security, economic stability, and societal functioning. The growing digitalization of energy systems, including the integration of industrial control systems, smart grids, and remote monitoring technologies, has significantly expanded the attack surface and increased system interdependencies. Recent incidents demonstrate that attacks on energy infrastructure are no longer isolated technical events but systemic disruptions capable of cascading across sectors, affecting telecommunications, transportation, healthcare, and defense. In the context of prolonged geopolitical instability and hybrid warfare, energy systems are increasingly exploited as instruments of strategic pressure, emphasizing the urgent need to move beyond traditional cybersecurity toward comprehensive cyber resilience. Analyzing real-world incidents enables the identification of recurring attack patterns, systemic vulnerabilities, and resilience gaps that cannot be revealed through theoretical models alone. Therefore, this study is highly relevant as it provides an evidence-based assessment of attacks on energy critical infrastructure and derives practical implications for strengthening cyber resilience, continuity of operations, and adaptive defense mechanisms in complex and adversarial environments.

The purpose of this study is to systematically analyze attacks and security incidents affecting energy sector critical infrastructure in order to identify prevalent attack patterns, systemic vulnerabilities, and their implications for cyber resilience.

The study aims to examine how different types of incidents (cyber, physical, and hybrid) impact the continuity and stability of energy systems, and to assess the adequacy of existing protection and response mechanisms. Based on the incident analysis, the research seeks to formulate practical recommendations for enhancing cyber resilience, including improvements in detection, response, recovery, and adaptive defense strategies for energy critical infrastructure operating under high-threat and crisis conditions.

2. Incident analysis and implications

Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents is discussed in [1]. Critical infrastructures and industrial organizations are increasingly integrating modern Information Technology (IT) components into their traditionally isolated Operational Technology (OT) environments. As OT systems become increasingly interconnected, they have also become high-value targets

for a diverse range of adversaries. However, the inherent complexity and legacy nature of these systems often hinder the timely deployment of modern cybersecurity controls. This convergence of factors has contributed to some of the most severe cybersecurity incidents in recent years. This paper presents a comprehensive and up-to-date survey of major threats and attacks targeting Industrial Control Systems (ICS) and critical infrastructures, as well as the communication protocols and devices used within them. The analysis reveals that threats against critical infrastructure are escalating, fueled by the widespread availability of off-the-shelf attack tools and techniques.

Moreover, design and implementation flaws in OT-specific network protocols and devices can enable adversaries to compromise or disrupt physical processes. The study provides a detailed categorization of threats and vulnerabilities (Fig. 1), offering a holistic understanding of the evolving risk landscape in industrial and critical infrastructure systems. To the best of the knowledge, this is the first exhaustive and detailed survey addressing these issues in such depth.

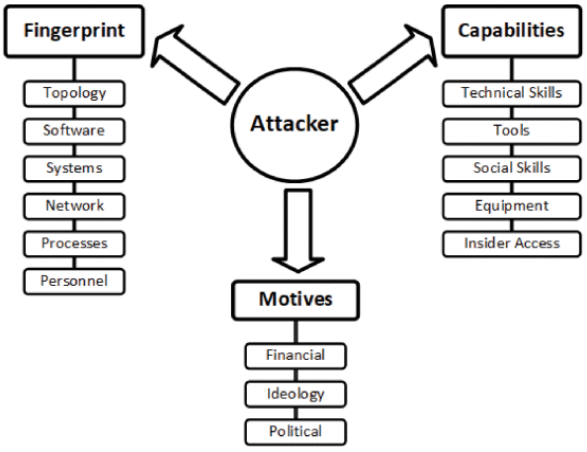


Fig. 1. Taxonomy of characteristics of CI attackers based on three main criteria

In [2], the analysis of machine learning methods in EtherCAT-based anomaly detection is investigated. The widespread adoption of Ethernet-based protocols in ICS has exposed supervisory control and data acquisition (SCADA) systems to cyberattacks traditionally associated with IT environments. The familiarity and ubiquity of Ethernet and TCP/IP protocols, combined with the growing number of successful attacks against them, have significantly increased cybersecurity risks for ICS.

These vulnerabilities are further exacerbated by the lack of encryption, authentication, and authorization mechanisms, as many industrial communication protocols were originally designed with performance, not security, in mind. High-profile incidents such as Stuxnet, Triton, Havex, Dragonfly, BlackEnergy, and the Ukraine power grid attack demonstrate the severe impact of protocol-level weaknesses in communications between PLCs, I/O units, HMIs, and engineering stations. To address this challenge, this paper evaluates machine learning (ML) techniques for anomaly detection in EtherCAT-based ICS networks—a topic that has received little prior attention. An EtherCAT-based water-level control system testbed (Fig. 2,3) was developed to generate 16 events across four categories, forming a dataset for ML evaluation.

Fig.2. Water level control automation components [2]

Experimental results show that k-nearest neighbors (k-NN) and support vector machines with genetic algorithms (SVM-GA) outperform 16 other models in detecting anomalies and classifying attack types. The proposed methods demonstrate strong applicability in EtherCAT environments, and the generated dataset offers a valuable resource for future ICS cybersecurity research, where real-world data remains scarce due to operational constraints in critical infrastructure.

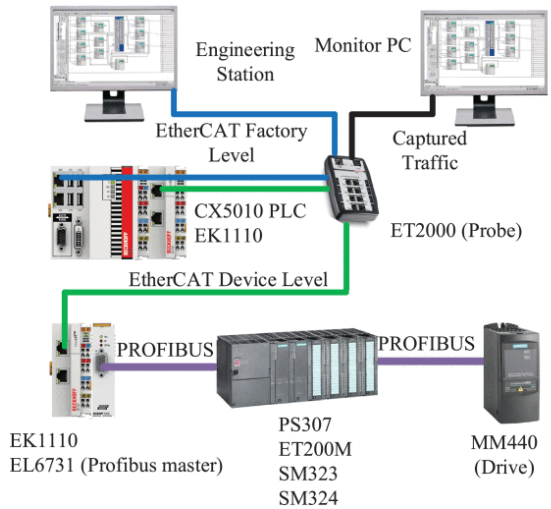


Fig.3. Testbed control devices [2]

In [3] a story of two industroyers is described. Authors analyze two malware families that were used in attempts to induce power outages in Ukraine. To study their behavior and potential impact, authors designed and implemented a novel sandbox (Fig.4) that emulates realistic substation environments – replicating networks, devices, and operational characteristics – allowing safe execution and in-depth observation of malware targeting power-grid equipment.

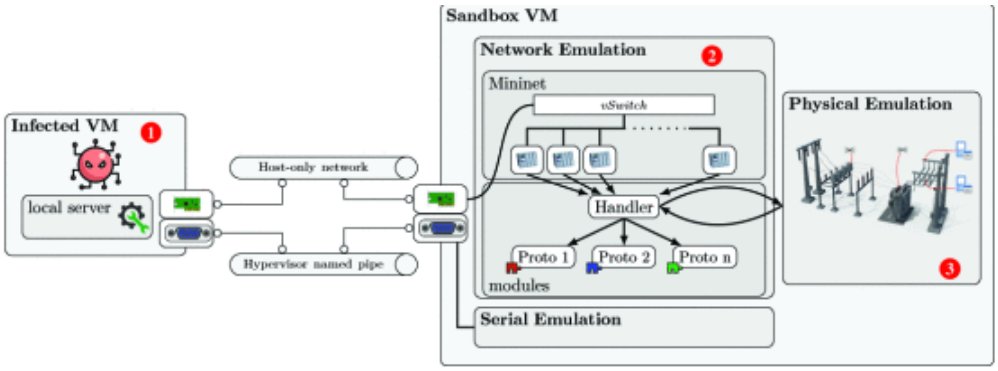


Fig. 4. Sandbox architecture [3]

Using this testbed, authors reconstructed the attackers' sequences of actions against substation components and evaluated the consequences of similar future campaigns on different targets (Fig.5). The Authors' investigation revealed previously undocumented malware behaviors, including a detailed algorithm for the MMS-protocol payload, and demonstrated how variations in attack targets and execution sequences lead to distinct physical effects. These findings deepen understanding of destructive ICS malware, improve the capability to attribute and mitigate such threats, and provide a validated experimental platform for future research into grid-focused cyberattacks.

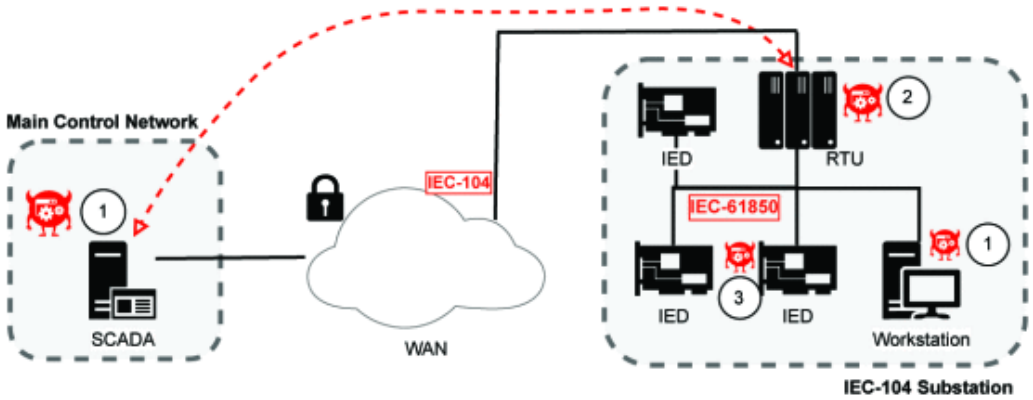


Fig. 5. Attack surfaces [3]

A Hydro-Quebec Use Case is investigated in [4]. Hydro-Québec (HQ) (Fig.6) is a vertically integrated utility responsible for the generation, transmission, and distribution of most of the electricity in the province of Québec. Its power grid features a unique architecture, characterized by large hydroelectric power plants located in the far north and a 735 kV transmission network that delivers electricity over thousands of kilometers to the southern load centers. This configuration has led HQ to develop specialized monitoring tools for calculating *stability limits*—boundaries determined by nonlinear phenomena such as angular, frequency, and voltage stability. However, integrating these nonlinear stability constraints into HQ's existing generation planning and operational frameworks – largely based on mixed-integer linear programming (MILP) – has presented significant challenges. This paper discusses these challenges and describes the methodologies developed to incorporate stability limits into HQ's reserve monitoring and unit commitment tools. The insights gained contribute to improving operational reliability and optimizing system performance within complex large-scale power grids.

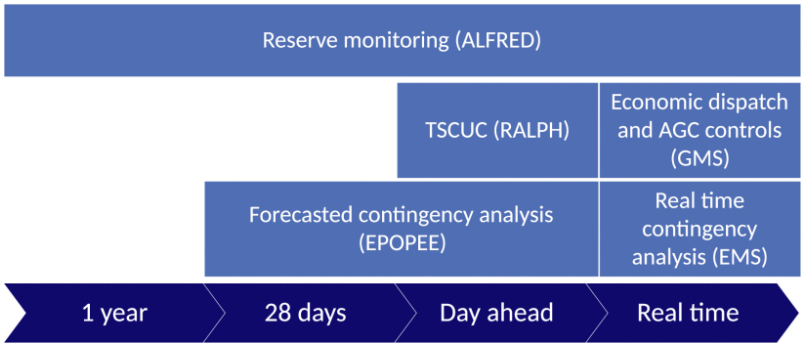


Fig. 6. Operation planning at HQ overview [4]

In [5] Convolutional Variational Autoencoder for Anomaly Detection in On-Load Tap Changers is reviewed. Transformer outages have a major impact on the reliability and cost efficiency of power systems, with studies showing that approximately 30% of transformer failures are attributed to faults in on-load tap changers (OLTCs)—critical components for voltage regulation. Continuous condition monitoring of OLTCs is therefore vital to enhance transformer reliability. This paper presents a vibro-acoustic signal analysis-based monitoring system used to assess OLTC health. Operational since 2016, the system continuously records vibration signals, temperature, and other parameters from paired OLTC units, utilizing three single-phase autotransformers in the Hydro-Québec network. To detect anomalies, a convolutional variational autoencoder (CVAE) is trained individually for each transformer family, mapping signal envelopes into a two-dimensional latent space for visual analysis. The decoder reconstructs inputs from the latent space, and anomaly thresholds are determined using reconstruction errors. Optimal thresholds yield intra-family anomaly detection rates of 4%, 5%, and 2%, and inter-family rates of 99%, 99%, and 100%, respectively. These results demonstrate the high accuracy and robustness of the proposed approach for distinguishing between transformer families and detecting emerging anomalies in OLTC operation, supporting proactive maintenance and improved grid reliability.

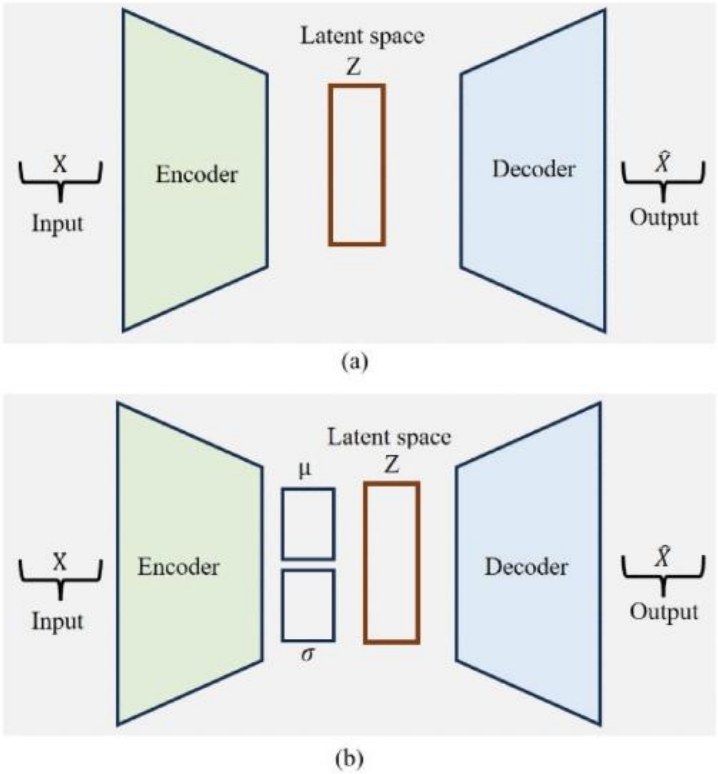


Fig. 7. The architecture of an autoencoder (a) and a variational autoencoder (b) [5]

The article [6] highlights that malware such as Stuxnet can compromise critical physical infrastructures controlled by software, indicating that cyber threats may directly endanger human lives. Stuxnet (Fig. 8) differs from conventional malware in several key aspects. Unlike typical malware, which seeks to infect as many systems as possible, Stuxnet specifically targets ICS and activates its payload only under narrowly defined operational conditions. Furthermore, Stuxnet exhibits exceptional size and complexity compared to earlier malware, incorporating four distinct zero-day exploits to achieve its objectives. This sophistication marks a pivotal shift in the nature of cyberattack, from digital disruption to the potential manipulation of physical systems, underscoring the growing convergence of cybersecurity and safety in critical infrastructure environments.

Table 1. Stuxnet's novel characteristics.

Aspect	Stuxnet	Common malware
Targeting	Extremely selective	Indiscriminate
Type of target	Industrial control systems	Computers
Size	500 Kbytes	Less than 1 Mbyte
Probable initial infection vector	Removable flash drive	Internet and other networks
Exploits	Four zero-days	Possibly one zero-day

Fig. 8. Stuxnet's novel characteristics [6]

Cybersecurity in power grids is showed in [7] Growing volatility in power transmission and distribution networks compels grid operators to increasingly rely on advanced communication infrastructures for monitoring and control. However, this expanded interconnectivity significantly enlarges the cyber-attack surface, exposing power grids to heightened security risks. Recent incidents have demonstrated that cyberattacks can cause widespread and prolonged blackouts, underscoring the urgency of resilient cybersecurity strategies. This paper analyzes the communication infrastructure of modern power grids to identify fundamental cybersecurity challenges and the resulting attack vectors and scenarios that threaten grid stability. To address these challenges, authors propose a defense-in-depth strategy encompassing four complementary dimensions (Fig.9): device and application security, network security, physical security, and organizational policies, procedures, and awareness. For each dimension, authors synthesize and evaluate state-of-the-art solutions while highlighting research opportunities to further enhance the cybersecurity posture of interconnected power systems.

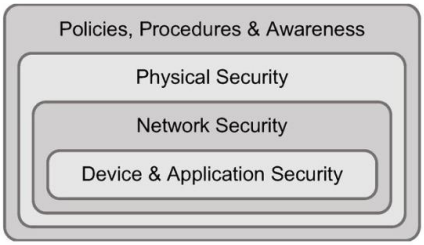


Fig. 9. Principle of defense-in-depth, providing security for interconnected powergrids needs [7]

In [8] a comprehensive review on cyber-attacks in power systems is discussed. Advancements in communication and information technologies are driving the transformation of traditional energy grids into integrated, intelligent platforms. The Internet of Things (IoT) plays a central role in this modernization by enabling smart grid functionalities and facilitating two-way communication between utilities and end-users. However, the increasing reliance on IoT-based communication systems introduces significant cybersecurity vulnerabilities (Fig.10). Critical information exchanges between interconnected devices are particularly attractive targets for cyber attackers, who seek to compromise data integrity, confidentiality, and authenticity—often with financial motives. Ensuring data security and privacy throughout communication and distribution processes is therefore essential. This review provides a comprehensive investigation of potential cyber threats and mitigation strategies in IoT-enabled smart grids. It examines recent advances in detection and prevention methods leveraging blockchain, cryptography, and advanced computational tools, with particular emphasis on smart meter security, end-user privacy, and electricity theft prevention. The operational and economic impacts of cyberattacks on power systems and deregulated energy markets are also analyzed. Drawing upon more than 135 research studies, this paper focuses on distribution-side cyberattacks, exploring their impact, detection mechanisms, protection strategies, and identifying future research directions in cybersecurity for smart grids.

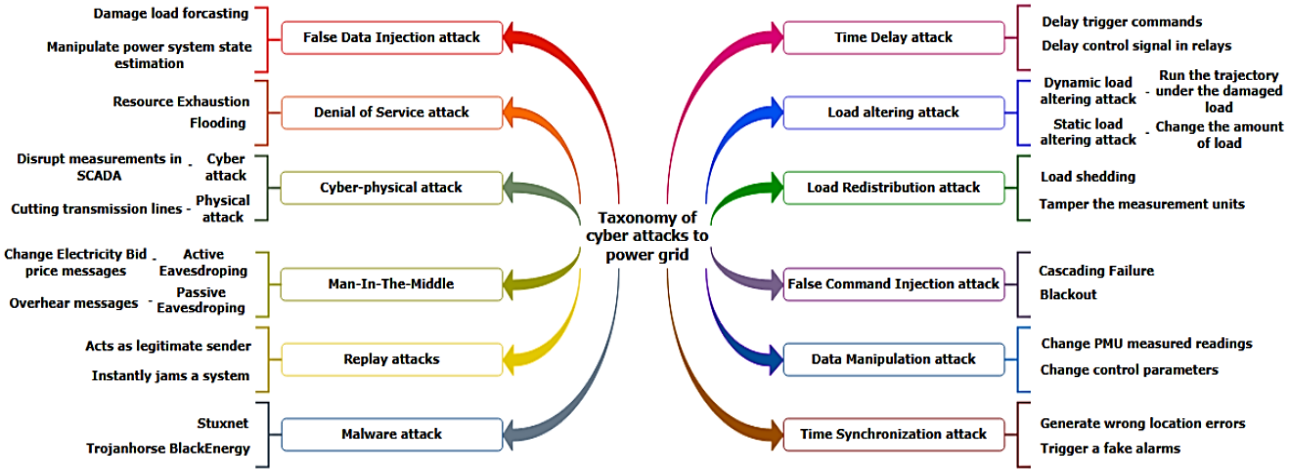


Fig. 10. Possible Cyber-attacks Impact on Power systems [8]

A Review of Colonial Pipeline Ransomware Attack is prepared in [9]. In April 2021, a ransomware attack targeted Colonial Pipeline, one of the largest fuel pipeline operators in the United States (Fig. 11). The incident was attributed to the hacking group DarkSide, which exploited design flaws in the company's network infrastructure. Extensive analysis revealed that the attackers gained unauthorized access through an unused VPN account. In an effort to restore operations, Colonial Pipeline paid a ransom to the attackers—an action that inadvertently incentivized similar attacks across critical sectors. This paper provides a detailed examination of the Colonial Pipeline attack, drawing on publicly available data to reconstruct the attack methodology and sequence of events. The analysis then examines the broader implications of the incident for the company, the United States, and global energy markets. Furthermore, the paper outlines defense strategies and preventive measures that could have mitigated the attack's success, offering insights into how organizations can enhance resilience against future ransomware threats. The study concludes with key lessons learned from this high-profile cybersecurity event.

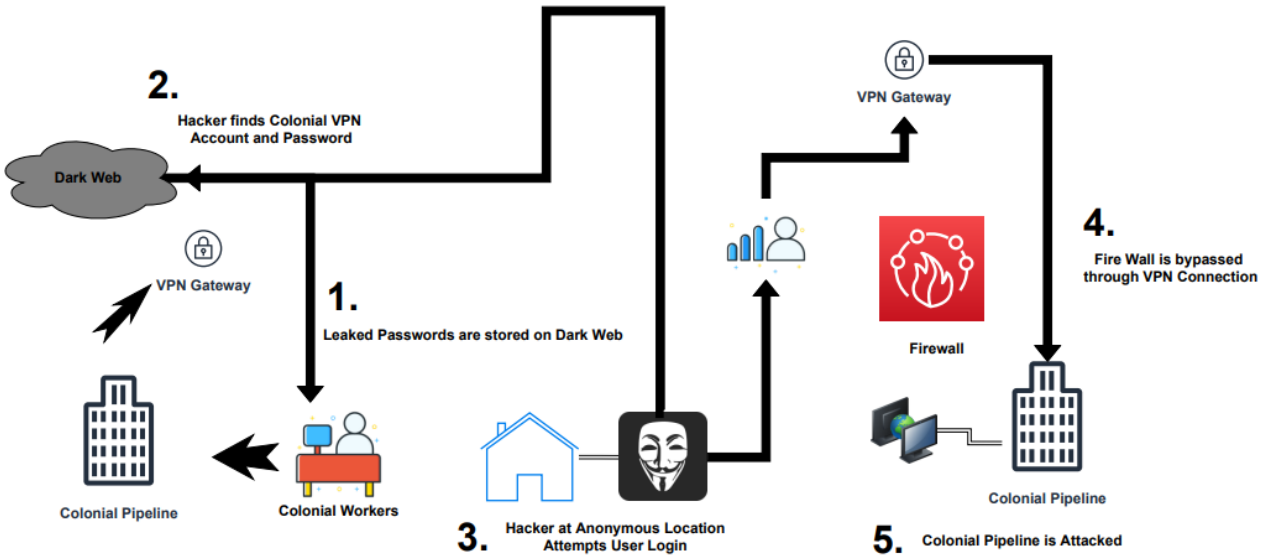


Fig. 11. Process of Access to Colonial Pipeline Infrastructure [9]

In [10] a study of the colonial pipeline incident is shown. The Colonial Pipeline ransomware attack marked a watershed moment in critical infrastructure cybersecurity, revealing significant vulnerabilities in industrial control systems with wide-ranging national security implications. This analysis traces the attack from initial compromise to system recovery, highlighting its unprecedented disruption of fuel distribution across the Eastern United States. The study examines technical, operational, and strategic lessons, emphasizing the need for robust security controls, comprehensive incident response procedures, and effective collaboration between the public and private sectors. By exploring the policy implications and subsequent regulatory measures, this research provides actionable insights for safeguarding critical infrastructure against evolving cyber threats (Fig. 12) and offers recommendations to strengthen organizational cybersecurity posture and resilience.

Security Component	Vulnerable Systems (%)	Number of Affected Systems	Security Risk Level
Remote Access Endpoints	76	189	High
Network Traffic Monitoring	84	142	Critical
VPN Sessions	47	324	Medium
Intrusion Detection	84	2846	Critical
Access Control Mechanisms	100	17	Critical

Fig. 12. Colonial Pipeline Cyberattack Security Vulnerabilities Assessment (2021) [10]

Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in Smart Grid. The is investigated in [11]. BlackEnergy malware, targeting critical infrastructures, has evolved from a simple DDoS platform into a sophisticated plug-in–based threat, featuring a persistent core with modular components for DDoS, spamming, information theft, remote access, and boot-sector attacks. BlackEnergy has been implicated in multiple high-profile cyber-physical attacks, including the December 2015 incident involving the Ukrainian power grid. This paper examines the evolution of BlackEnergy and its cyberattack capabilities, presenting a fundamental attack model for targeting ICS. In particular, the study focuses on threats to synchrophasor-based systems, which are essential for real-time monitoring and control in smart grids. Various BlackEnergy-based attack scenarios are explored, exploiting vulnerabilities in two widely used synchrophasor communication standards: IEEE C37.118 and IEC 61850-90-5. The analysis includes reconnaissance, DDoS, man-in-the-middle, and replay/reflection attacks. The paper further investigates strategies for detecting and preventing BlackEnergy-driven cyber-physical attacks, providing recommendations to enhance the security and resilience of smart grid systems.

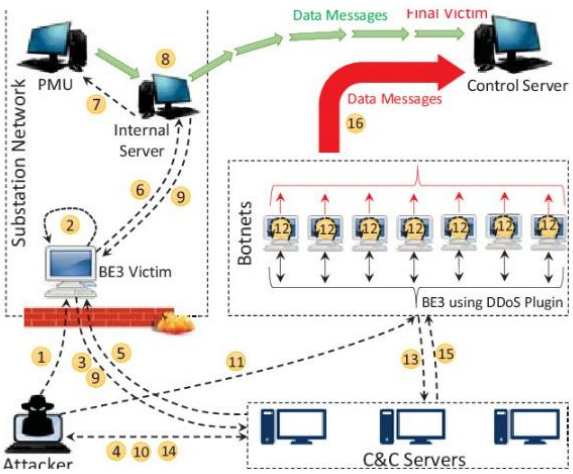


Fig. 13. DDoS attack based on two-stage interim attacks utilizing BlackEnergy plugins for credential theft and DDoS [11]

Cybersecurity Challenges in Smart Grid Systems is investigated in [12]. The transformation of traditional power grids into Smart Grids (SG) addresses challenges such as unidirectional information flow, rising energy demand, energy inefficiency, and issues related to availability and security. This evolution is driven by the IoT, whose integration with power systems promises future SGs that are more efficient, reliable, and adaptive. However, the increased connectivity and reliance on IoT technologies introduce significant cybersecurity risks that threaten the continuous operation of SG. This paper presents a comprehensive survey of cybersecurity challenges faced by IoT devices in SG environments. It begins by outlining SG architecture (Fig. 14) and IoT applications, followed by an analysis of security objectives, requirements, and threats.

Cyberattacks are classified and evaluated based on the Confidentiality, Integrity, and Availability (so-called CIA model) principles and emerging sophisticated threats. The paper further reviews current security solutions, protocols, and standards, as well as emerging approaches leveraging artificial intelligence, blockchain, and Software-Defined Networking (SDN) to enhance resilience. Finally, it provides recommendations for future research to strengthen cybersecurity in SG and ensure the robust deployment of IoT-enabled power systems.

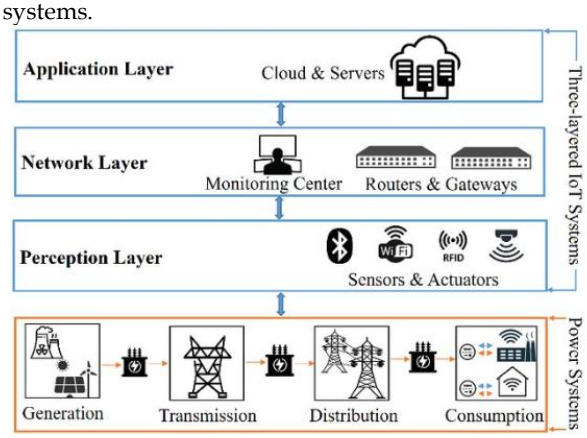


Fig. 14. Three-layered architecture for SG [12]

In [13], exploiting the temporal behavior of state transitions for intrusion detection in ICS/SCADA is described. ICS are essential for monitoring and managing physical processes, but their security has become a major concern due to the potential for cyber-attacks to cause severe real-world damage. While much of the existing research focuses on defending ICS through traditional IT security measures, comparatively fewer studies address the detection of attacks that directly manipulate the physical process. Such detection methods are known as *process-aware* intrusion detection systems (IDS). In this paper, the authors present a time-based process-aware IDS designed to identify cyber-attacks by exploiting the inherent regularity and temporal characteristics of physical processes. The proposed system learns the temporal behavior of process variables and leverages this model to detect anomalies indicative of attacks (Fig. 15). Authors assess its performance using a public SCADA dataset as well as a simulated SCADA system developed for this research. Given results demonstrate that the proposed IDS can detect attacks that are overlooked by existing process-aware systems, which disregard temporal properties.

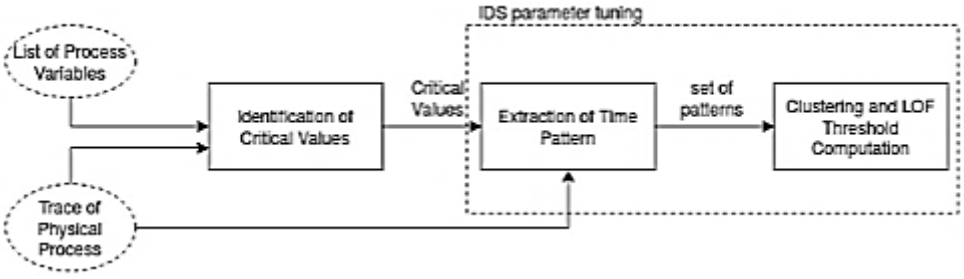


Fig. 15. Learning phase steps [13]

Recent progress in anomaly detection in Energy Applications is discussed in [14]. In recent years, anomaly detection has become a highly active research area across various domains and applications. From a data analysis perspective, anomalies are data points that deviate from normal patterns, representing atypical or abnormal events within a dataset. The significance of detecting such anomalies lies in their ability to reveal potentially harmful or undesirable conditions related to the underlying physical processes, which may have serious implications for people, the environment, infrastructure, or information systems (Fig. 16). This review provides a comprehensive overview of recent advancements in anomaly detection within the energy sector—a field undergoing profound digital transformation. A total of 52 studies are examined, with the majority focusing on

renewable energy generation, building energy consumption, and energy storage. Notably, many approaches employ AI-based ensemble methods, often integrating deep learning models to enhance detection performance. Nonetheless, several underexplored areas and research gaps remain, particularly concerning specific energy applications such as critical infrastructures and electric vehicle (EV) charging systems. Furthermore, ongoing challenges persist in methodological aspects, including explainability and practical applicability of deep learning-based anomaly detection. Emerging concepts and potential directions for future research are also discussed.

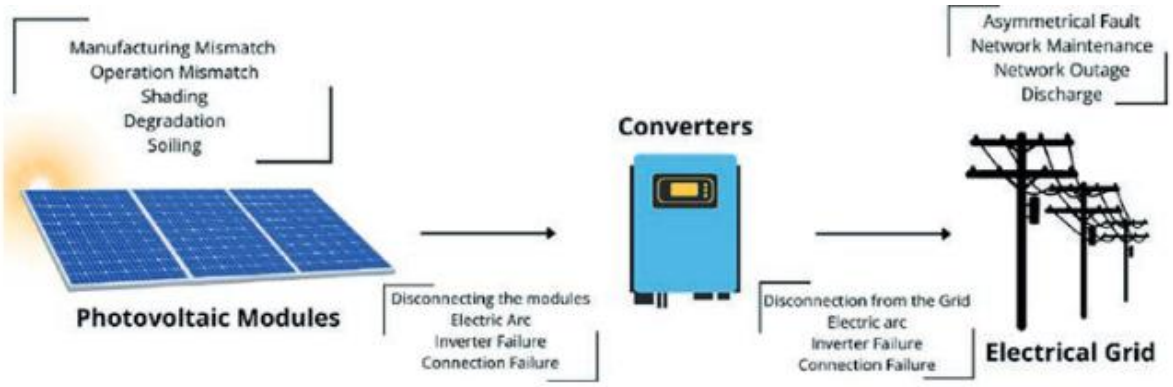


Fig. 16. Various problems that can cause anomalies in PV systems [14]

Real-world case studies for a process-aware IDS is discussed in [15]. The transition toward sustainable energy increasingly depends on resilient communication infrastructures that enable the monitoring, control, and optimization of energy distribution. SCADA networks (Fig.17) play a central role in these operations by transmitting sensor data and control commands. However, integrating modern communication technologies into aging infrastructure introduces new cybersecurity vulnerabilities, including false data injection and man-in-the-middle attacks. While recent advances in IDS for SCADA networks demonstrate promise in identifying such domain-specific threats, most evaluations remain limited to simulated environments due to the critical nature of real-world systems. This paper presents two real-world case studies using actual grid data, in which a process-aware IDS is customized for specific network topologies. The proposed approach effectively detects various cyber-attacks, including those targeting key assets such as transformers. This study represents a significant step toward practical deployment, underscoring the importance of transitioning from simulation-based testing to real-world validation to ensure the security and reliability of critical grid infrastructures.

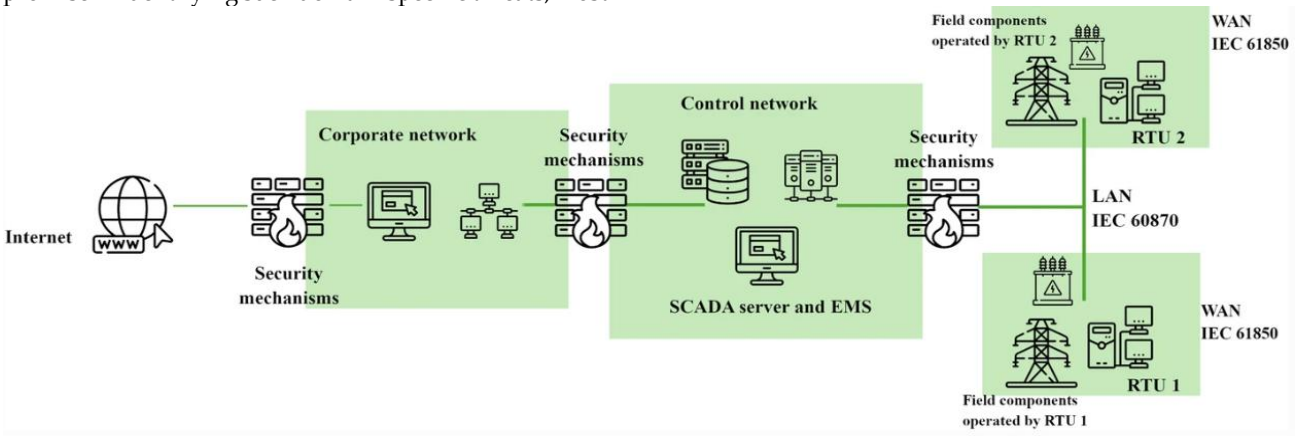


Fig. 17. Networked SCADA architecture (control network) in the context of a corporate network and field components [15]

In [16] different cyber-attacks on energy infrastructure is investigated. Advanced Persistent Threats (APTs) are stealthy, multi-stage cyberattacks executed over extended periods and often tailored to specific targets. Characterized by their "low and slow" approach, APTs typically remain undetected until their impact becomes evident. Energy infrastructures—such as power grids, oil and gas facilities, and offshore wind installations—form the backbone of modern digital societies. A successful APT (Fig. 18) attack on these systems could lead to widespread power outages, disrupting financial services, banking, and other critical digital functions.

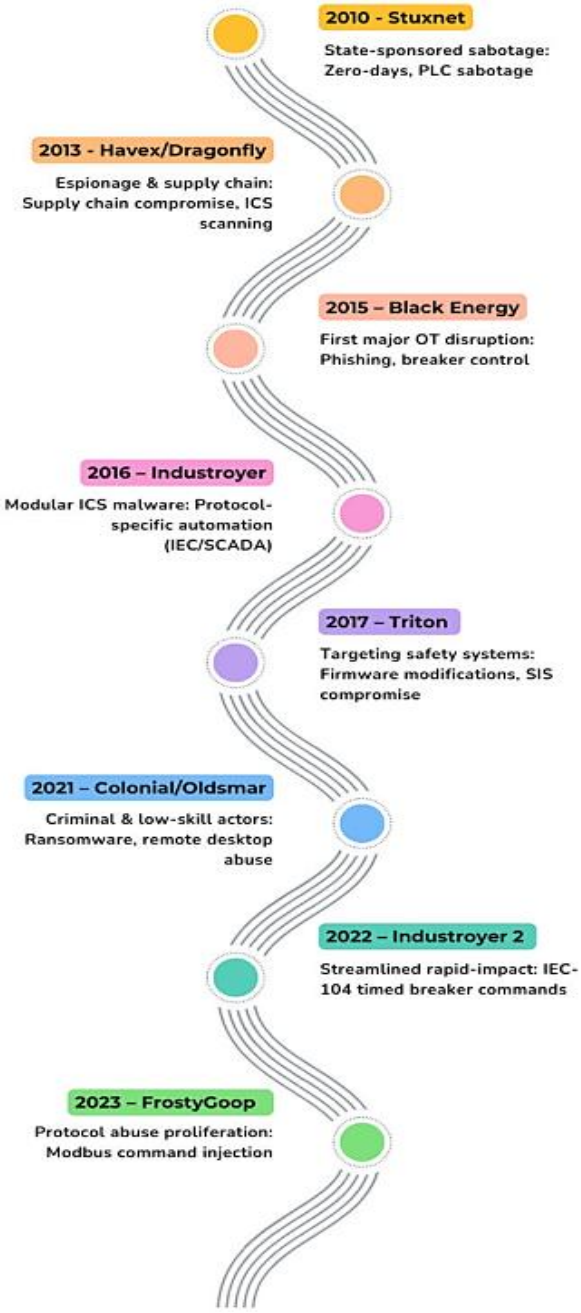


Fig. 18. Evolution of Cyberattacks [16]

The resulting loss of electricity could escalate into life-threatening situations and digital chaos, where essential services like digital payments and identification become unavailable, and even point-of-sale systems depend on limited emergency power. Notable examples include the Triton malware (2017), which targeted the safety systems of a Saudi petrochemical plant, and Industroyer2 (2022), which attempted to disrupt a Ukrainian energy provider. This paper integrates insights from cybersecurity and energy system engineering to analyze APTs targeting critical energy infrastructures. It emphasizes the technical mechanisms of such threats while exploring their potential societal and economic consequences, highlighting the urgent need for enhanced detection, resilience, and response strategies in the energy sector.

Destabilizing Power Grid and Energy Market by Cyberattacks on Smart Inverters is investigated in [17]. Cyberattacks on smart inverters and distributed photovoltaic (PV) systems have emerged as a pressing concern due to recently disclosed vulnerabilities and documented attack incidents. The long operational lifespan of inverter devices, limited user awareness of cybersecurity practices, and the absence of comprehensive cyber regulations further heighten the risk. This raises a critical question: Can large-scale cyberattacks on smart inverters trigger widespread instability in power grids and energy markets (Fig.19)?

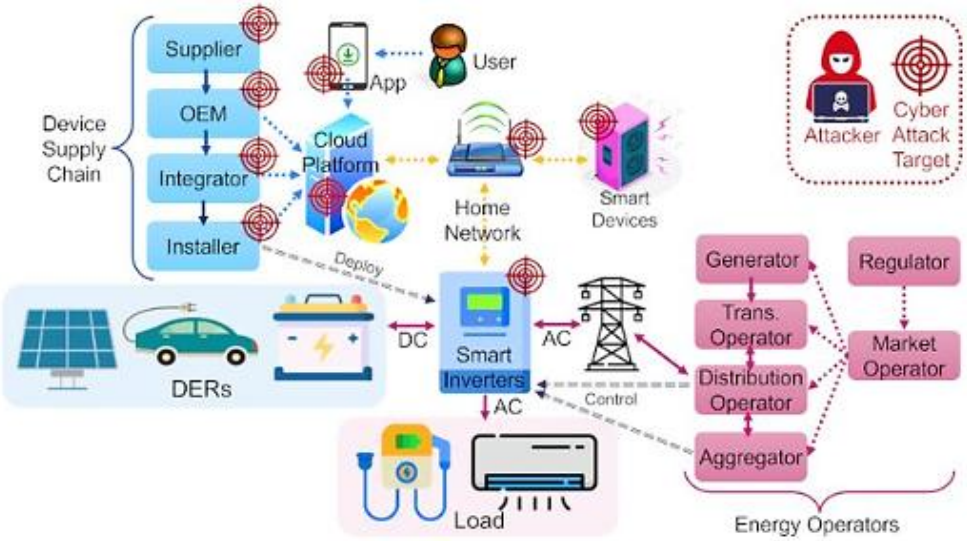


Fig. 19. An illustration of the systems and parties interacting with a smart inverter [17]

This paper provides a realistic assessment of the plausibility and potential impacts of such attacks (Fig. 20). Using Australian electricity market data and insights from practical contingency mechanisms, the authors conduct an in-depth analysis to evaluate grid resilience under adversarial conditions. Authors' findings indicate that (1) while cyberattacks on smart inverters can disrupt grid operations, significant impacts require coordinated and carefully orchestrated efforts, and (2) existing grid security measures are sufficient for handling accidental contingencies but remain inadequate against intelligent, well-planned adversarial attacks. Moreover, the analysis reveals that even a relatively small proportion of compromised distributed PV units could generate a concerted and destabilizing effect on the grid. These results highlight the urgent need for robust defense strategies and regulatory frameworks to safeguard power systems with high levels of distributed PV integration.

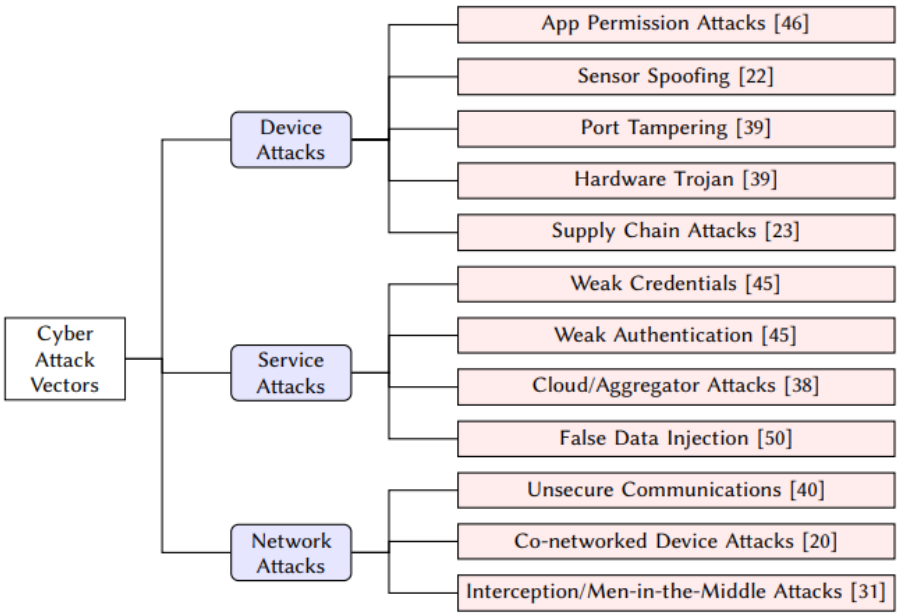


Fig. 20. Taxonomy of cyber attack vectors on smart inverters [17]

Attacks on the Siemens S7 Protocol using an industrial control system testbed (Fig. 21) is described in paper [18]. The stability of critical infrastructure relies on a secure and resilient energy supply, emphasizing the growing importance of cybersecurity in SG as they increasingly integrate renewable energy sources. Unlike conventional power plants, modern renewable facilities are geographically distributed and remotely controlled, expanding the attack surface and necessitating enhanced protection against cyber threats to maintain operational availability. However, testing such threats on real power plants poses significant risks, including service disruptions and financial losses. To address this challenge, authors developed a Hardware-in-the-Loop (HIL) testbed that simulates three renewable energy plants, providing a safe, flexible, and cost-efficient environment for studying the effects of cyberattacks.

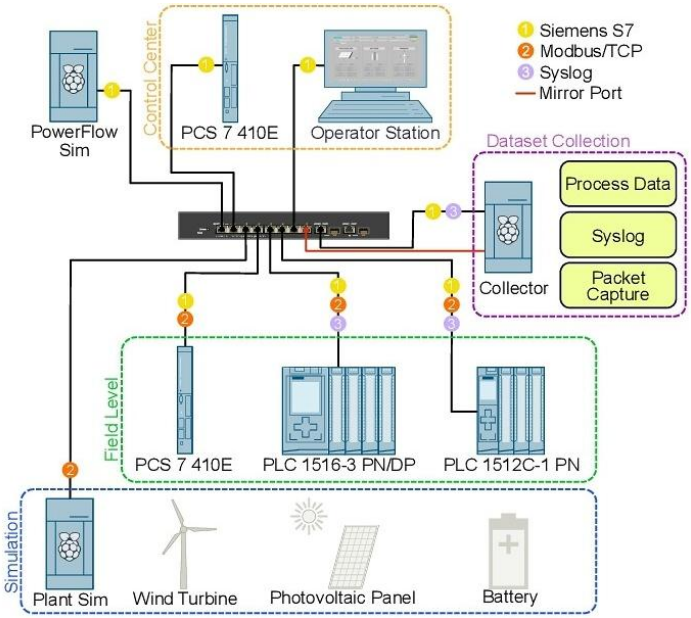


Fig. 21. Architecture of testbed including data collection and conversion to dataset [18]

The proposed testbed architecture enables the emulation of unsafe operational states under attack conditions. Authors further advance the field by demonstrating a novel S7 (Fig. 22) data modification attack, a technique seldom explored in prior research. Additionally, authors present a comprehensive dataset for Smart Grid cybersecurity and employ it to establish a baseline ML-based IDS. This work provides practical tools and insights for enhancing the cyber-resilience of modern energy infrastructures.

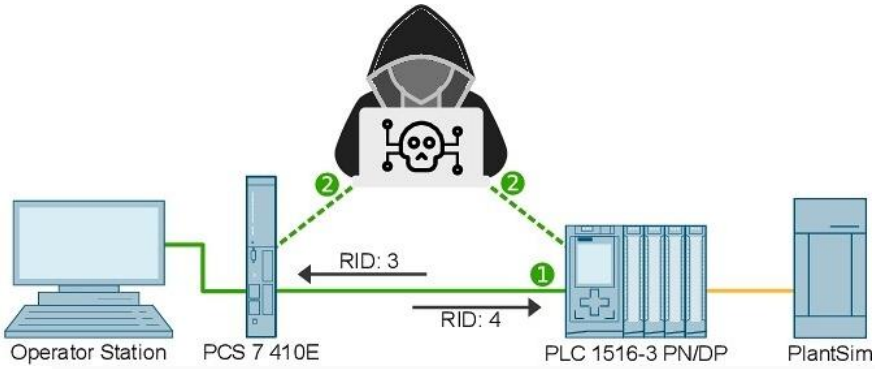


Fig. 22. Data modification attack on S7 protocol between a PLCs and Process Control System [18]

Who controls the power grid? The possible answer in article [19]. The power grid is a critical infrastructure whose importance continues to grow with increasing electrification (Fig.23). Failures within the grid, depending on their scale, can cause severe societal and economic disruptions. Understanding the vulnerabilities inherent in this complex system is therefore essential, as cyberattacks targeting the power grid have the potential to inflict damage on both national and global levels. The emergence of smart grid technologies has further expanded the attack surface, providing adversaries with multiple points of entry. Quantifying the number of compromised devices required to destabilize the grid is a key factor in assessing its security. This paper emphasizes the importance of identifying weaknesses within power grid control systems, analyzing potential attack vectors, and developing robust protection mechanisms. Authors' findings reveal a concerning reality: even adversaries with limited control over grid-connected technologies can significantly affect system stability, particularly by influencing the frequency containment reserve — a critical component of grid balance. By highlighting these potential vulnerabilities, this study enhances the understanding of the multi-layered threats that compromise the resilience and reliability of modern power grids.

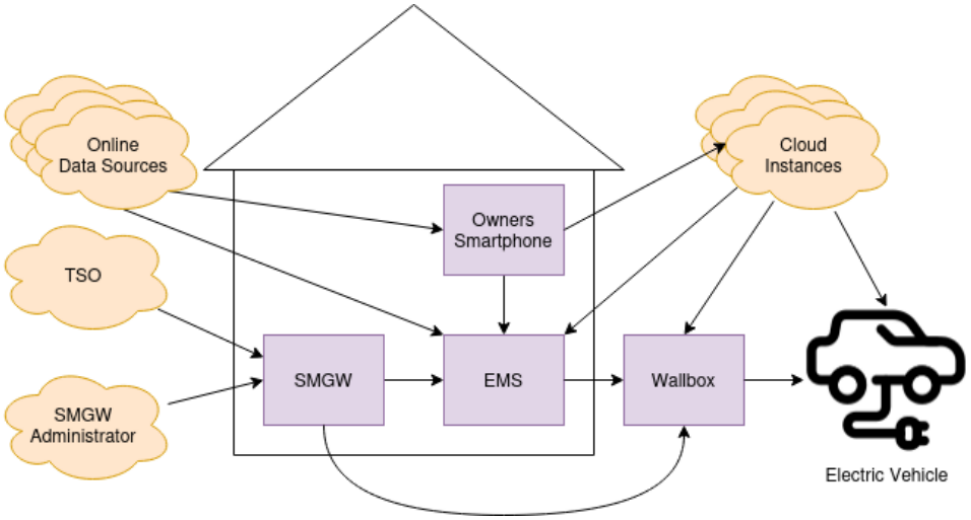


Fig. 23. Influences on Electric Vehicles [19]

In [20] deep reinforcement learning for autonomous grid operation and attack detection is prepared. As modern power grids evolve, IT has become essential for ensuring reliable and efficient operations. While IT enhances operators' situational awareness and responsiveness, it simultaneously expands the cyberattack surface — evident from incidents such as BlackEnergy and CrashOverride. To safeguard grid reliability, power systems must not only withstand ongoing attacks but also promptly detect and respond to them. To address these challenges, authors propose DRAGON (Fig.24) — a Deep Reinforcement Learning framework for Autonomous Grid Operation and attack detectiON. DRAGON is designed to (i) autonomously learn strategies for maintaining stable grid operations and (ii) detect cyberattacks in real time. Authors implement and evaluate DRAGON on the IEEE 14-bus power transmission system under multiple attack scenarios. Experimental results demonstrate that DRAGON sustains safe grid operations 225.5% longer than a state-of-the-art autonomous grid operator. Moreover, its detection component achieves a 92.9% true positive rate, 11.4% false positive rate, and reduces the false negative rate by 63.1% compared to a recent benchmark method. These results highlight DRAGON's effectiveness in enhancing both the resilience and situational awareness of modern smart grids under adversarial conditions.

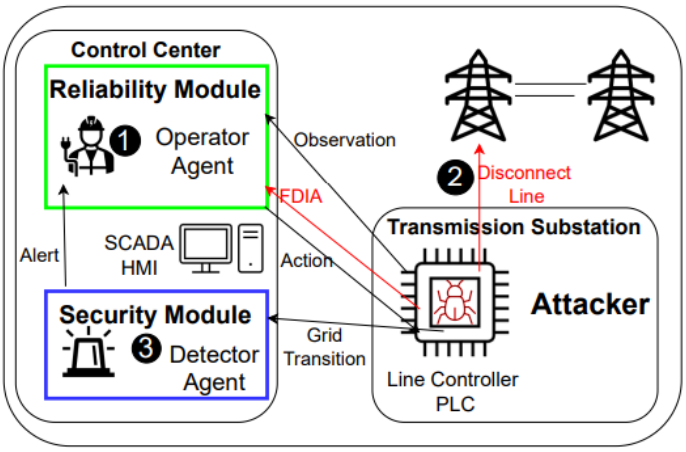


Fig. 24. Overview of DRAGON's operation and detection problem definitions [20]

Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks is investigated in [21]. The SG is a complex cyber-physical ecosystem that integrates communication, computation, and control technologies to enable reliable power system operations. However, its interconnected nature exposes it to sophisticated cyber threats, including advanced persistent threats (APTs) and coordinated attacks, as demonstrated by Ukrainian power grid incident. This article reviews smart grid security through the lens of situational awareness (SA) and collaborative defense (Fig.25). A threat modeling framework is proposed to characterize cyber-physical attacks and assess their impact on control and power systems. Existing defense mechanisms, such as IDS, moving target defense (MTD), and co-simulation approaches, are examined in terms of their effectiveness in enhancing grid resilience. The review also highlights the human factor in maintaining situational awareness during cyber incidents. Finally, key research gaps and future directions are identified to strengthen the detection, defense, and overall cyber-resilience of modern smart grids.

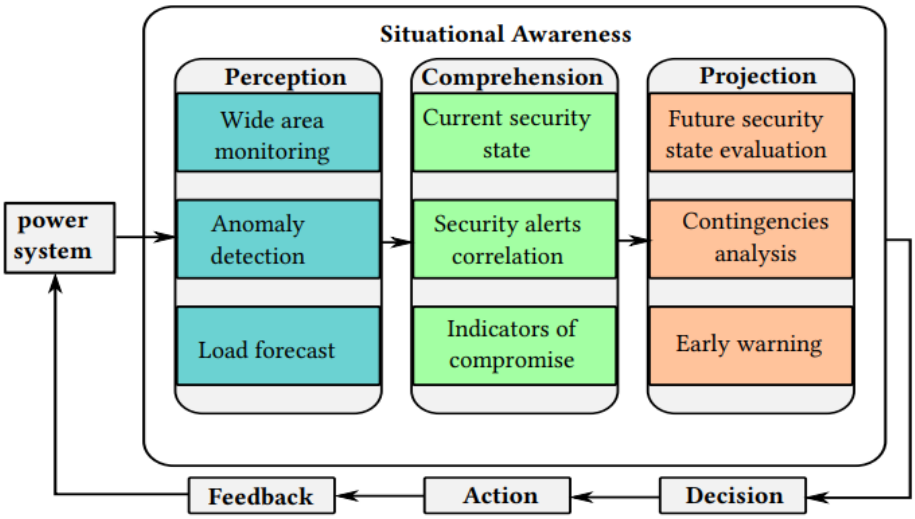


Fig. 25. Situational awareness framework for smart grid [21]

The report [22] analyzes the series of cyber and physical attacks targeting Ukraine's electric grid and examines the lessons they offer for improving the resilience of U.S. critical infrastructure. Since 2015, Ukraine has faced repeated assaults on its power system—most notably through advanced malware such as BlackEnergy, Industroyer, and coordinated missile strikes—highlighting the interdependence of cyber and physical threats in modern energy networks (Fig.26). The study outlines how Ukraine's grid operators have maintained operational continuity through rapid system restoration, EU grid interconnection, manual overrides of automated systems, equipment stockpiling, and robust international technical assistance. By comparing Ukraine's response with U.S. infrastructure frameworks, the report underscores the need for comprehensive digital supply chain risk management, real-time situational awareness, and resilience-by-design approaches across operational technology environments. The findings emphasize that proactive coordination among government agencies, private utilities, and international partners is essential to strengthen preparedness against evolving hybrid threats targeting the power sector.

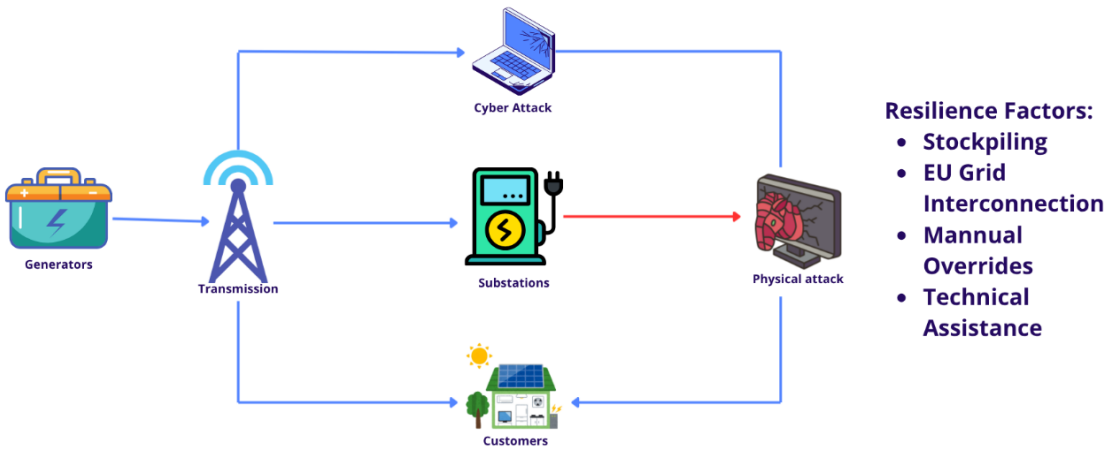


Fig. 26. Attack on Ukraine's Electric Grid [22]

The report [23] provides an overview of the California Public Utilities Commission's (CPUC) investigation into the physical security of electric distribution assets (Fig.27), initiated following the April 2013 Metcalf substation sniper attack. The incident underscored the vulnerability of critical electric infrastructure to both physical and cyber threats, prompting the passage of SB 699 (Hill, 2014) and the subsequent CPUC Rulemaking R.15-06-009. The study identifies three key focus areas: (1) prioritizing critical electrical facilities and developing appropriate security measures, (2) improving protocols for sharing sensitive information between utilities and regulators, and (3) evaluating the adequacy of existing incident reporting requirements. While California's investor-owned utilities (IOUs) have enhanced physical security through infrastructure hardening, surveillance, and improved access control, the report emphasizes that most incidents still involve opportunistic crimes, such as theft and vandalism, rather than coordinated attacks. The CPUC recommends a risk-based approach to security planning, continued collaboration between utilities and state agencies, data sharing through DOE and DHS programs, and the integration of resilience and physical protection measures into long-term infrastructure design. These efforts aim to balance preventive investments with network resiliency, ensuring a reliable, secure, and adaptable electric grid for California.

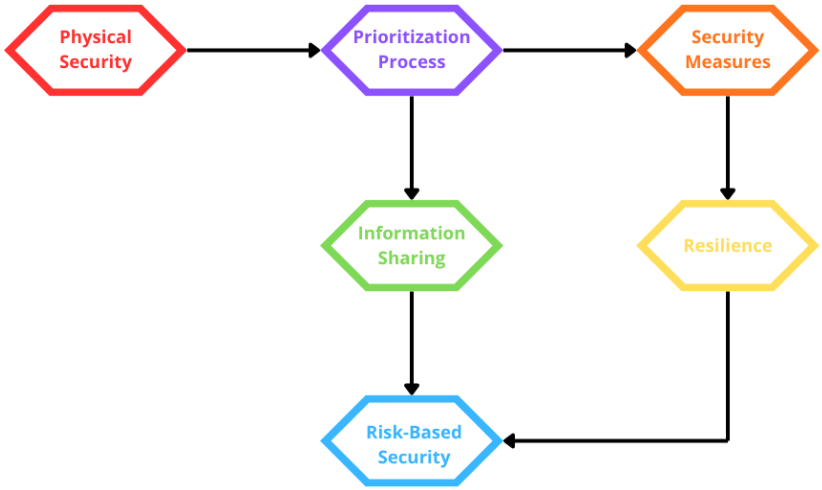


Fig. 27. Physical Security of Electric Distribution Assets [23]

Vulnerability assessment of Industrial Control Systems for Colonial Pipeline and WannaCry Ransomware is investigated in [24]. ICS enable a high degree of automation, enhancing efficiency and reducing operational costs across sectors such as manufacturing, energy, and utilities. However, the increasing convergence of OT and IT has made ICS environments more vulnerable to cyberattacks. This paper examines common vulnerabilities in ICS, including insecure communication protocols, weak authentication, outdated software, and poor network configurations. Exploiting these weaknesses allows attackers to gain unauthorized access, disrupt operations, and inflict physical damage. To mitigate such risks, this study highlights key security measures such as network segmentation, strong authentication and encryption, regular system updates and patching, continuous monitoring, and comprehensive vulnerability assessments. Implementing these measures is essential for strengthening the cybersecurity posture of ICS environments and ensuring the reliability of critical industrial processes.

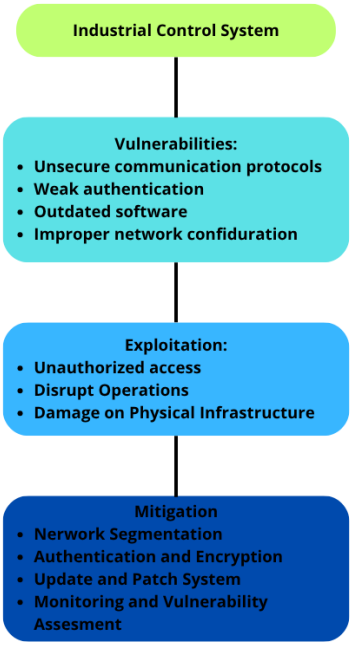


Fig. 28. Vulnerabilities, Exploitation, Mitigation of ICS [24]

In [25] Industroyer cyber-attacks on Ukraine's critical infrastructure is investigated. The threat of cyberattacks on power grids persists continuously, extending beyond periods of armed conflict. This article examines the most sophisticated cyber incidents targeting Ukraine's energy infrastructure during the ongoing conflict. It provides a concise overview of key events and analyzes the characteristics of Industroyer2 (Fig. 29) and its predecessor, the malware families used in these attacks. The study also considers the potential actors behind these operations and outlines possible future developments in cyber warfare targeting critical infrastructure. Finally, it proposes strategic measures to prevent similar attacks, emphasizing the importance of safeguarding both civilian and military energy systems against evolving cyber threats.

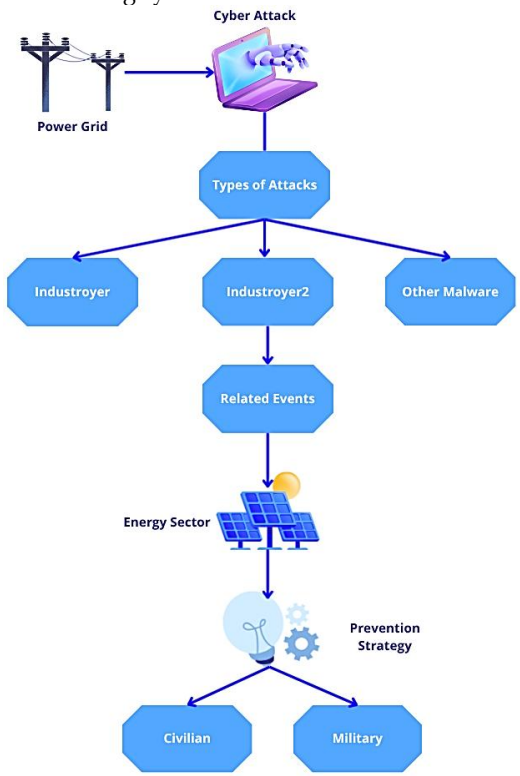


Fig. 29. The impact of Industroyer2 [25]

Cybersecurity Challenges in the Power Sector is discussed in [26]. Cybersecurity in the power sector has become a critical priority as cyberattacks on electrical grids and substations continue to escalate. This paper presents a comprehensive analysis of major cyber incidents in the energy sector, focusing on advanced malware such as BlackEnergy and Industroyer, which have disrupted power systems in Ukraine and other regions. These incidents expose vulnerabilities in ICS protocols—particularly IEC 61850—and illustrate how adversaries can exploit them to manipulate control operations and trigger large-scale outages (Fig.30). Moreover, state-sponsored campaigns such as RedEcho and TAG-38 highlight the growing link between geopolitical tensions and cyber operations targeting critical infrastructure. The study examines various attack vectors, including spear-phishing, malware injection, and Denial-of-Service (DoS) attacks, to assess their impact on grid stability and security. The findings emphasize the urgent need for robust cybersecurity measures, including adherence to IEC 62351 standards and the deployment of advanced IDS to strengthen energy network resilience against evolving threats.

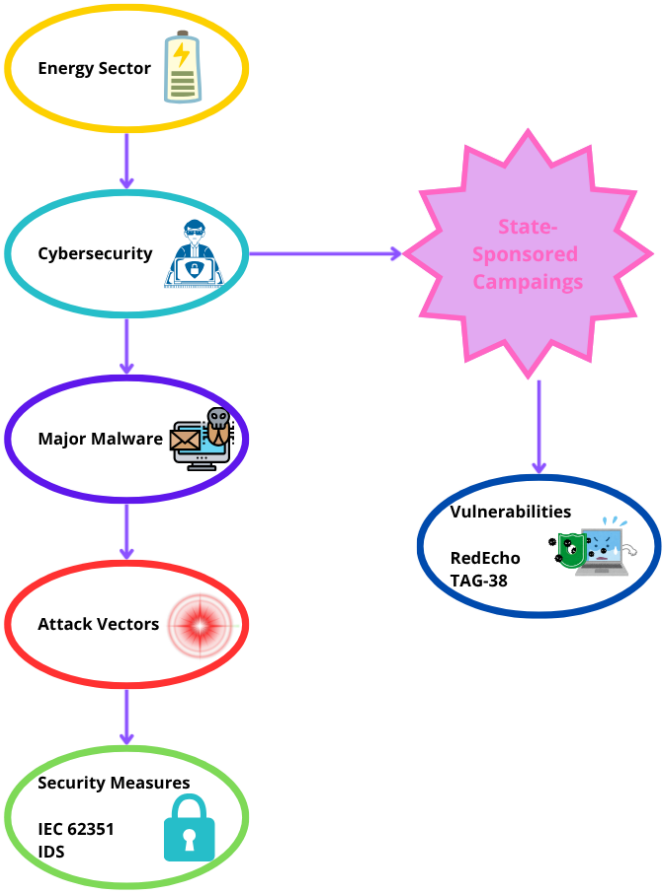


Fig. 30. Cybersecurity Structure in the Power Sector: Attack Vectors, Threat Actors, and Defense Measures [26]

In [27] the theme Towards Cross-Physical-Domain Threat Inference for Industrial Control System Defense Adaptation is analysed. Safety-critical ICS have become prime targets for Advanced Persistent Threats (APTs), as demonstrated by incidents such as Stuxnet, the Ukraine power grid attacks, and recent U.S. water treatment facility intrusions (Fig. 31). These sophisticated campaigns exploit common sensor and actuator abstractions shared across diverse ICS environments. Although frameworks like MITRE ATT&CK for ICS effectively classify attacker Tactics, Techniques, and Procedures (TTPs), they lack the capability to assess the physical impact of cyberattacks on OT. To address this limitation, authors propose OTThreat, a novel ontology that extends the Semantic Sensor Network (SSN) framework by integrating cyber-attack abstractions with the safety properties they compromise. This approach enables the mapping of analogous physical processes across distinct ICS domains, supporting the transfer of existing mitigations to novel threat scenarios. Authors implement and validate a proof-of-concept threat inference framework across three ICS use cases (spanning water treatment and oil processing systems) to demonstrate how threat assessments and mitigation strategies can be systematically adapted across heterogeneous physical domains.

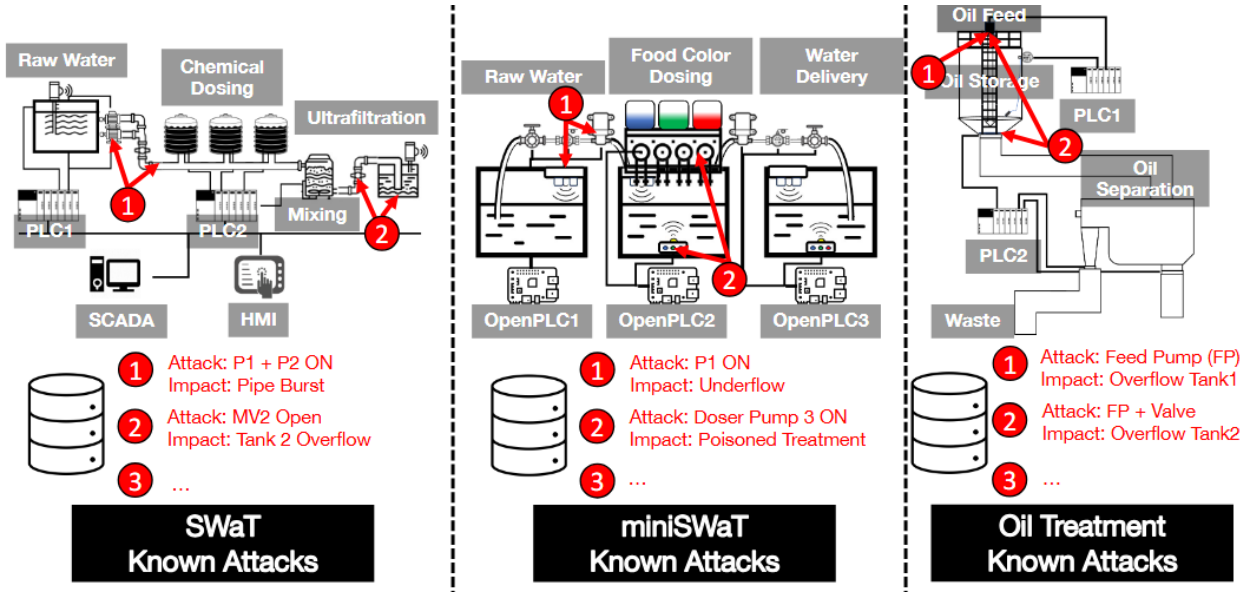


Fig. 31. Overview of three use case ICSs, highlighting cross-domain threats and commonalities [27]

3. Practical Recommendations

Based on the analysis of attacks and incidents affecting energy sector critical infrastructure [1-27], the following recommendations focus on strengthening cyber resilience through governance, architecture, detection, and recovery measures that can be realistically implemented by energy operators.

1) First, energy operators should establish dedicated OT/ICS cybersecurity governance, clearly separating responsibilities between IT, operational technology, security, and engineering teams. Risk management approaches must be tailored specifically to OT environments, prioritizing safety, availability, and the cascading cross-sector impacts, rather than relying solely on traditional IT confidentiality metrics. Asset criticality mapping and identification of single points of failure should serve as the foundation for resilience planning.

2) Second, reducing the attack surface of energy infrastructure requires strict network segmentation and zoning between corporate IT, DMZ, control centers, and field-level OT systems. Remote access for vendors and maintenance personnel should be centrally managed, time-limited, and continuously monitored, with multi-factor authentication and session recording. Control centers and dispatch systems must be treated as high-value assets and protected through isolation, privileged access management, and application whitelisting.

3) Third, effective resilience depends on early detection and situational awareness within OT environments. Energy operators should deploy passive OT-aware monitoring capable of identifying abnormal control commands and protocol misuse, and integrate OT telemetry into centralized SIEM and SOC workflows. Threat intelligence relevant to the energy sector should be systematically incorporated to anticipate emerging attack techniques.

4) Fourth, vulnerability and configuration management in OT systems should be risk-driven and operationally safe. Continuous asset inventory, controlled patching through predefined maintenance windows, and the use of hardened baseline configurations are crucial in preventing unintended disruptions to industrial processes.

5) Finally, resilience against destructive and large-scale attacks requires robust recovery and continuity capabilities. Energy organizations should maintain offline and immutable backups of critical OT configurations and control systems, regularly test restoration procedures, and prepare for degraded or manual modes of operation. Cyber incident response plans must be aligned with physical security and crisis communication procedures to ensure coordinated response under hybrid threat conditions.

These measures collectively enable a shift from reactive cybersecurity toward sustainable cyber resilience for energy critical infrastructure operating in high-threat and crisis environments.

Conclusions and future research directions

This study shows that over the past 10-15 years attacks on energy sector critical infrastructure have increasingly focused on compromising measurement and monitoring processes, including sensor data, telemetry, and state estimation, rather than isolated IT components. Loss or manipulation of measurement integrity directly undermines situational awareness, automated control, and emergency response, leading to cascading failures across energy systems. The findings confirm that cyber resilience in energy infrastructure depends on continuous, measurement-aware security that enables early detection of anomalies, correlation of data deviations with cyber and physical events, and rapid operational recovery in OT/ICS environments.

Future research should prioritize resilient monitoring of energy system measurements under adversarial conditions, with emphasis on real-time anomaly detection using AI/ML combined with physical

process models and state estimation. Key directions include secure sensor fusion, validation of distributed measurements, protection against false data injection, and the integration of measurement monitoring into adaptive control, digital twins, and self-healing resilience frameworks for energy critical infrastructure.

References

[1]. G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," in *IEEE Access*, vol. 9, pp. 165295-165325, 2021, doi: 10.1109/ACCESS.2021.3133348.

[2]. K. O. Akpinar and I. Ozcelik, "Analysis of Machine Learning Methods in EtherCAT-Based Anomaly Detection," in *IEEE Access*, vol. 7, pp. 184365-184374, 2019, doi: 10.1109/ACCESS.2019.2960497

[3]. L. Salazar *et al*., "A Tale of Two Industroyers: It was the Season of Darkness," *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2024, pp. 312-330, doi: 10.1109/SP54263.2024.00162.

[4]. A. Besner *et al*., "Generation Planning and Operation Under Power Stability Constraints: A Hydro-Quebec Use Case," in *IEEE Transactions on Power Systems*, vol. 40, no. 5, pp. 4006-4018, Sept. 2025, doi: 10.1109/TPWRS.2025.3528864.

[5]. F. Dabaghi-Zarandi, H. Ezzaidi, M. Gauvin, P. Picher, I. Fofana and V. Behjat, "Convolutional Variational Autoencoder for Anomaly Detection in On-Load Tap Changers," in *IEEE Access*, vol. 13, pp. 50838-50848, 2025, doi: 10.1109/ACCESS.2025.3550097

[6]. T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," in *Computer*, vol. 44, no. 4, pp. 91-93, April 2011, doi: 10.1109/MC.2011.115.

[7]. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. https://doi.org/10.3390/s21186225

[8]. N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," in *IEEE Access*, vol. 12, pp. 18147-18167, 2024, doi: 10.1109/ACCESS.2024.3361039.

[9]. J. Beerman, D. Berent, Z. Falter and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India, 2023, pp. 8-15, doi: 10.1109/CCGridW59191.2023.00017.

[10]. Bellamkonda, Srikanth. (2024). Ransomware Attacks On Critical Infrastructure: A Study Of The Colonial Pipeline Incident. International Journal of Research in Computer Applications and Information Technology. 7. 1423-1433. 10.5281/zenodo.14191113.

[11]. Khan, Rafiullah & Maynard, Peter & Mclaughlin, Kieran & Laverty, David & Sezer, Sakir. (2016). Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. 10.14236/ewic/ICS2016.7.

[12]. Amanlou, Sanaz & Hasan, Mohammad Kamrul & Mokhtar, Umi & Malik, Khalid & Islam, Shayla & Khan, Sheroz & Khan, M. & Khan, Muhammad. (2025). Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations. IEEE Open Journal of the Communications Society. 10.1109/OJCOMS.2025.3545153.

[13]. Ndonda, Gorby & Sadre, Ramin. (2022). Exploiting the Temporal Behavior of State Transitions for Intrusion Detection in ICS/SCADA. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3213080.

[14]. Pérez, Joan & Chávez, Mayra & Prieto, Miguel & Martínez, Luis. (2025). Recent Progress of Anomaly Detection in Energy Applications: A Systematic Literature Review. 10.5772/intechopen.1012028.

[15]. Menzel, V., Hurink, J. & Remke, A. Real-world case studies for a process-aware IDS. *Energy Inform* **8**, 86 (2025). https://doi.org/10.1186/s42162-025-00545-1

[16]. Abraham, D.; Houmb, S.H.; Erdodi, L. Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation. *Appl. Sci.* **2025**, *15*, 9233. https://doi.org/10.3390/app15179233

[17]. Hui, Xiangyu & Karumba, Samuel & Chau, Sid & Ahmed, Mohiuddin. (2025). Destabilizing Power Grid and Energy Market by Cyberattacks on Smart Inverters. 10.48550/arXiv.2505.14175.

[18]. Nicolai Kellerer, Gustavo Sánchez, Hermenegildo Alberto, Veit Hagenmeyer, and Ghada Elbez. 2025. Attacks on the Siemens S7 Protocol Using an Industrial Control System Testbed. In Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems (E-Energy '25). Association for Computing Machinery, New York, NY, USA, 770–779. https://doi.org/10.1145/3679240.3734645

[19]. Niklas Goerke, Alexandra Märtz, and Ingmar Baumgart. 2024. Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability. In Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems (e-Energy '24). Association for Computing Machinery, New York, NY, USA, 46–54. https://doi.org/10.1145/3632775.3661943

[20]. Matthew Landen, Keywhan Chung, Moses Ike, Sarah Mackay, Jean-Paul Watson, and Wenke Lee. 2022. DRAGON: Deep Reinforcement Learning for Autonomous Grid Operation and Attack Detection. In Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC '22). Association for Computing Machinery, New York, NY, USA, 13–27. https://doi.org/10.1145/3564625.3567969

[21]. Muhammad Nouman Nafees, Neetesh Saxena, Alvaro Cardenas, Santiago Grijalva, and Pete Burnap. 2023. Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. ACM Comput. Surv. 55, 10, Article 215 (October 2023), 36 pages. https://doi.org/10.1145/3565570

[22]. "Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience." *Congress.gov*, Library of Congress, 16 October 2025, https://www.congress.gov/crs-product/R48067.

[23]. California Public Utilities Commission, *Physical Security Executive Summary: Rulemaking R.15-06-009 – Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electric Corporations,* Safety and Enforcement Division, Risk Assessment and Safety Advisory Section, Jan. 2018.

[24]. M. Musluoglu, N. Kunicina and J. Caiko, "Vulnerability Assessment of Industrial Control Systems for Colonial Pipeline and WannaCry Ransomware," *2024 IEEE 65th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, Riga, Latvia, 2024, pp. 1-7, doi: 10.1109/RTUCON62997.2024.10830848.

[25]. P. Kozak, I. Klaban and T. Šlajs, "Industroyer cyber-attacks on Ukraine's critical infrastructure," *2023*

International Conference on Military Technologies (ICMT), Brno, Czech Republic, 2023, pp. 1-6, doi: 10.1109/ICMT58149.2023.10171308.

[26]. R. Štefko, K. Eliáš, K. Glajc, A. Hyseni, F. Margita and J. Šimčák, "Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations," *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Stará Lesná, Slovakia, 2025, pp. 000459-000464, doi: 10.1109/SAMI63904.2025.10883298.

[27]. Jainta Paul, Lawrence Ponce, Mu Zhang, and Luis Garcia. 2024. Towards Cross-Physical-Domain Threat Inference for Industrial Control System Defense Adaptation. In Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security (RICSS '24). Association for Computing Machinery, New York, NY, USA, 57–64. https://doi.org/10.1145/3689930.3695210

Добринчук О., Лукашенко В. Загрози критичній енергетичній інфраструктурі: аналіз інцидентів та наслідки для стійкості ICS/SCADA

Критична інфраструктура енергетичного сектору все частіше стає об'єктом кібернетичних, фізичних та гібридних атак, які використовують вразливості систем моніторингу та контролю. У цій статті аналізуються основні інциденти безпеки, що вплинули на енергетичні об'єкти протягом останніх 10-15 років, з особливим акцентом на атаках, що ставлять під загрозу дані вимірювань, телеметрію та ситуаційну обізнаність. На основі аналізу інцидентів у дослідженні визначено типові схеми атак та прогалини в стійкості, а також обговорено їх наслідки для безпечної експлуатації енергетичних систем. Наприкінці статті наводяться практичні рекомендації щодо посилення кіберстійкості за допомогою моніторингу з урахуванням вимірювань, вдосконалення виявлення та механізмів відновлення стійкості в критичній інфраструктурі енергетики.

***Ключові слова**: критична інфраструктура, енергетичний сектор, ICS/SCADA, стійкість, інцидент, атака, безпека, практичні рекомендації, енергомережа.*

Добринчук Олександр Анатолійович, керівник лабораторії спеціальних та нейтронних вимірювань, Хмельницька атомна електростанція.
Dobrynchuk Oleksandr, Head of the Laboratory for Special and Neutron Measurements, Khmelnytskyi Nuclear Power Plant.

Лукашенко Вікторія Вікторівна, доктор технічних наук, професор, начальник Науково-дослідної частики Державного університету «Київський авіаційний інститут».
Lukashenko Viktoriia, D.Sc., Professor, Head of R&D Department State University «Kyiv Aviation Institute».