IRSTI 28.23.37

10.51889/2959-5894.2024.88.4.019

G.S. Shaimerdenova[1*], Zh. Zh. Azhibekova[2], E.B. Mussirepova[1], Z.Z. Esenkulova[1], N.M. Zhailaubayev[1]

[1]M.Auezov South Kazakhstan University, Shymkent, Kazakhstan
[2]Asfendiyarov Kazakh National Medical University, Almaty, Kazakhstan
[*]*e-mail: danel01kz@gmail.com*

A REVIEW OF CYBER DEFENSE MECHANISMS IN AUTONOMOUS ELECTRICAL SYSTEMS

Abstract

This systematic review examines the essential aspects of cybersecurity in the rapidly evolving field of autonomous electrical systems. As critical components of modern smart grids, these systems are increasingly vulnerable to advanced cyber threats due to their reliance on automation and connectivity. The review synthesizes existing research to identify current vulnerabilities, evaluate the effectiveness of implemented cyber defense mechanisms, and explore emerging trends and technologies aimed at improving the security and resilience of these infrastructures. By systematically analyzing peer-reviewed journals, conference proceedings, and industry reports from the past decade, the review highlights major cyber threats, including ransomware, DDoS attacks, and phishing, which pose significant risks to autonomous electrical systems. It investigates the use of cutting-edge technologies such as machine learning algorithms for detecting anomalies, blockchain for ensuring data integrity, and quantum cryptography for secure communication. A particular focus is given to artificial intelligence's role in predictive cybersecurity, which enables the anticipation of threats before they materialize, enhancing the proactive capabilities of defense systems. The review also examines the application of established frameworks like the NIST Cybersecurity Framework and the Zero Trust Model, which have been instrumental in shaping security strategies for the sector. It discusses both the challenges and opportunities associated with adapting to evolving cyber threats and integrating next-generation technologies into existing systems. This analysis aims to provide cybersecurity professionals, policymakers, and researchers with actionable insights and a comprehensive understanding of the cyber risks and defense strategies related to autonomous electrical systems. Ultimately, the review seeks to contribute to the development of more robust security measures, strengthen grid resilience, and ensure the reliable operation of future energy systems.

Keywords: Cybersecurity, Autonomous Electrical Systems, Smart Grids, Machine Learning, Zero Trust Model**.**

Г.С. Шаймерденова[1], Ж.Ж. Ажибекова[2], Э.Б. Мүсірепова[1], З.З. Есенкулова[1], Н.М. Жайлаубаев[1]
[1]М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент қ., Қазақстан,
[2] С. Ж. Асфендияров атындағы Қазақ ұлттық медицина университет, Алматы қ., Қазақстан

АВТОНОМИЯЛЫ ЭЛЕКТР ЖҮЙЕЛЕРІНДЕГІ КИБЕР ҚОРҒАНУ МЕХАНИЗМДЕРІНЕ ШОЛУ

Аңдатпа

Бұл жүйелі шолу автономды электр жүйелеріндегі киберқауіпсіздіктің маңызды аспектілерін зерттейді. Заманауи ақылды желілердің негізгі компоненттері ретінде бұл жүйелер автоматтандыру мен байланыстың арқасында күрделі киберқауіптерге осал. Шолу қазіргі осалдықтарды анықтау, іске асырылған киберқорғау механизмдерінің тиімділігін бағалау және осы инфрақұрылымдардың қауіпсіздігі мен тұрақтылығын жақсартуға бағытталған жаңа технологиялар мен трендтерді зерттеу үшін бар зерттеулерді біріктіреді. Соңғы онжылдықта жарияланған ғылыми журналдар, конференция материалдары және сала есептерін жүйелі талдау арқылы шолу автономды электр жүйелеріне айтарлықтай қауіп төндіретін негізгі кибершабуылдарды, соның ішінде ransomware, DDoS шабуылдары және фишингті атап көрсетеді. Ол аномалияларды анықтауға арналған машина оқыту алгоритмдерін, деректер тұтастығын қамтамасыз ету үшін блокчейнді және қауіпсіз байланыс үшін кванттық криптографияны қоса алғанда, алдыңғы қатарлы технологияларды қолдануды зерттейді. Шолу қауіптерді алдын ала анықтау мүмкіндігін арттыратын және киберқорғаудың проактивті

қабілеттерін жақсартатын жасанды интеллектті қолдануға ерекше назар аударады. Сондай-ақ, шолу NIST киберқауіпсіздік құрылымы және Zero Trust моделі сияқты сектордың қауіпсіздік стратегияларын қалыптастыруда маңызды рөл атқаратын қолданыстағы құрылымдарды зерттейді. Ол киберқауіптердің өзгеруіне бейімделу және жаңа буын технологияларын бар жүйелерге біріктірумен байланысты қиындықтар мен мүмкіндіктерді талқылайды. Бұл талдау энергетика секторындағы киберқауіпсіздік мамандарына, саясаткерлерге және зерттеушілерге қолдануға болатын түсініктер мен автономды электр жүйелеріндегі киберқауіптер мен қорғау стратегиялары туралы толыққанды түсінік беруді мақсат етеді. Ақыр соңында, шолу мықты қауіпсіздік шараларын әзірлеуге, желі тұрақтылығын нығайтуға және болашақ энергетикалық жүйелердің сенімді жұмысын қамтамасыз етуге үлес қосуға бағытталған.

Түйін сөздер: киберқауіпсіздік, автономды электр жүйелері, ақылды желілер, машина оқыту, Zero Trust моделі.

Г.С. Шаймерденова[1], Ж.Ж. Ажибекова[2], Э.Б. Мусирепова[1], З.З. Есенкулова[1], Н.М. Жайлаубаев[1]
[1]Южно-Казахстанский университет имени М.Ауэзова, г. Шымкент, Казахстан,
[2] Казахский Национальный медицинский университет имени С. Д. Асфендиярова,
г.Алматы, Казахстан

ОБЗОР МЕХАНИЗМОВ КИБЕРЗАЩИТЫ В АВТОНОМНЫХ ЭНЕРГОСИСТЕМАХ

Аннотация

Этот систематический обзор изучает ключевые аспекты кибербезопасности в области автономных электрических систем. Будучи важными компонентами современных умных сетей, эти системы становятся уязвимыми перед сложными киберугрозами из-за своей автоматизации и подключённости. Обзор объединяет существующие исследования для выявления текущих уязвимостей, оценки эффективности внедрённых механизмов киберзащиты и изучения новых технологий и тенденций, направленных на повышение безопасности и устойчивости этих инфраструктур. Анализируя научные журналы, материалы конференций и отраслевые отчёты за последнее десятилетие, обзор выделяет основные типы киберугроз, такие как программы-вымогатели (ransomware), DDoS-атаки и фишинг, которые представляют значительные риски для автономных электрических систем. Он исследует использование передовых технологий, таких как алгоритмы машинного обучения для обнаружения аномалий, блокчейн для обеспечения целостности данных и квантовая криптография для безопасной коммуникации. Особое внимание уделяется применению искусственного интеллекта в прогнозировании киберугроз, что позволяет выявлять их до их возникновения, улучшая проактивные возможности систем защиты. Обзор также рассматривает применение таких рамочных концепций, как NIST Cybersecurity Framework и Zero Trust Model, которые играют важную роль в формировании стратегий безопасности в этом секторе. Также обсуждаются вызовы и возможности, связанные с адаптацией к изменяющимся киберугрозам и интеграцией технологий нового поколения в существующие системы. Этот анализ нацелен на предоставление специалистам в области кибербезопасности, политикам и исследователям практических рекомендаций и глубокого понимания киберугроз и стратегий защиты в автономных электрических системах. В конечном счёте, обзор направлен на содействие разработке более надёжных мер безопасности, укрепление устойчивости сетей и обеспечение надёжной работы энергетических систем будущего.

Ключевые слова: кибербезопасность, автономные электрические системы, умные сети, машинное обучение, модель Zero Trust.

Main provisions

Significant emphasis is placed on the utilization of artificial intelligence for forecasting cyber dangers, enabling their detection prior to manifestation, thereby augmenting the proactive functionalities of security systems. The review analyzes the implementation of framework principles, including the NIST Cybersecurity Framework and the Zero Trust Model, which are essential in formulating security policies within this industry. The discourse encompasses the problems and opportunities linked to adapting to evolving cyber threats and incorporating next-generation technologies into current systems. This analysis seeks to furnish cybersecurity experts, policymakers, and researchers with actionable advice and a comprehensive understanding of cyber dangers and protective solutions in autonomous electrical systems. The evaluation seeks to enhance the

creation of dependable security measures, bolster network resilience, and guarantee the consistent operation of future energy systems.

Introduction

Autonomous power systems are complex, autonomous power grids that use computer-based automation and control to distribute and manage electricity without ongoing human intervention. They are the foundation of modern smart grids that integrate conventional power systems with advanced information and communication technologies to improve efficiency, reliability, and sustainability. These systems include elements such as advanced computing infrastructure (AMI), automated controls, and real-time data monitoring that enable them to quickly adapt to fluctuations in electricity consumption and conditions. Using algorithms and artificial intelligence, they can predict power demands, optimize resources, and quickly identify bottlenecks to avoid outages [1]. They can also more effectively integrate renewable energy sources such as wind and solar, and adapt to their variable outputs through flexible control systems. This capability facilitates the transition to clean energy by increasing the use of renewable sources and reducing dependence on fossil fuels. The technologies facilitate two-way communication between providers and consumers, improving energy-efficient choices and managing peak demand.

These devices increase efficiency while simultaneously improving the security and stability of power grids. Integrated cybersecurity protocols enable real-time detection and response to potential cyberattacks, protecting critical infrastructure and customer data from threats [2]. This level of protection is critical as grids become increasingly computerized and interconnected with other systems, increasing vulnerability. Automation facilitates remote diagnostics and maintenance, thereby reducing downtime and the need for on-site technicians, which is beneficial for locations with difficult-to-reach or harsh conditions.

A key characteristic of autonomous power systems is their ability to evolve and improve over time using data analytics. This versatility allows utilities to respond to current conditions and anticipate and prepare for future challenges, including adverse weather conditions and changing customer behavior [3]. Their decentralized control allows local grid segments, or microgrids, to operate autonomously when disconnected from the main grid, providing a reliable option for improving grid stability and resilience in diverse locations.

Autonomous power systems are transforming the energy sector by integrating sophisticated technologies with new management strategies. They are essential for creating a sustainable, secure, and flexible energy future in which energy production, distribution, and consumption are more closely aligned with environmental and societal demands.

The increasing reliance on these technologies highlights the critical need for robust cybersecurity measures. Autonomous systems that leverage digital connectivity and data-driven approaches to power management are vulnerable to cyberthreats, including hacking, data breaches, and cyber-physical attacks. These threats can lead to major power outages, the exposure of sensitive customer data, or potential physical damage to infrastructure. Implementing robust cyber defenses is essential to protect these systems, ensuring uninterrupted operations, and a reliable energy supply. Cybersecurity protects the integrity of the grid, ensuring its resilience to disruptions and its ability to meet the demands of a highly interconnected society [4].

Cybersecurity is essential in autonomous power systems, protecting the data transmission networks that connect the various components of the smart grid. These networks carry sensitive information such as customer energy usage, operational data and control signals, making them prime targets for cybercriminals who can exploit vulnerabilities to disrupt energy distribution or steal personal information. The increasing use of Internet of Things (IoT) devices in grid networks highlights the need for robust cybersecurity protocols, as these devices can create vulnerabilities if not adequately protected.

In addition to protecting against external attacks, effective cybersecurity also addresses the risks posed by insider threats and accidental breaches, which can be equally damaging. Implementing strict access controls, conducting regular security audits, using real-time threat detection and providing ongoing training for employees are essential to maintaining system security against both internal and external threats. This integrated strategy will increase consumer confidence in digital infrastructure and enable autonomous power systems.

In addition, these cybersecurity initiatives facilitate compliance with national and international requirements for the protection of critical infrastructure [5]. Therefore, investing in cybersecurity is not just a technical necessity; it is a strategic imperative that ensures operational reliability, protects public trust, and enhances the safety and functionality of modern energy systems.

This systematic review seeks to thoroughly analyze and synthesize current knowledge on cybersecurity measures in autonomous power systems, focusing on important trends, challenges, and technological advances. It examines the spectrum of cyber threats facing these systems, the operational vulnerabilities that make them vulnerable to threats, and the various security strategies that have been proposed or adopted to mitigate these challenges. The assessment examines hardware and software solutions, regulatory frameworks, and procedural procedures designed to protect infrastructure from cyber-physical attacks, data breaches, and various security risks.

The review provides a thorough examination of current and emerging cybersecurity technologies, drawing on a variety of academic studies, case studies, and industry reports. It assesses the effectiveness of these solutions in different situations and identifies knowledge gaps for future research to address [3]. The review also considers the broader implications of these measures, including their impact on system performance and user privacy, while providing a balanced view that encompasses technical and ethical issues. The assessment aims to serve as a useful resource for researchers, industry professionals, and policymakers by carefully assessing these factors to enhance the resilience and security of critical energy infrastructure.

Research methodology

To ensure comprehensive coverage of relevant studies, a comprehensive literature search was conducted across various scientific databases for the systematic review. Prominent databases included IEEE Xplore, ScienceDirect, and SpringerLink, which are recognized for their extensive collections of technical and engineering literature. Additional platforms such as Google Scholar and ACM Digital Library were used to capture a broad spectrum of multidisciplinary research linking cybersecurity and electrical engineering.

The search strategy was carefully designed with specific keywords and phrases selected to retrieve the most relevant articles. Phrases such as “autonomous power systems,” “cyberdefense,” “cybersecurity,” “smart grid,” “information security,” “cyber threats,” “vulnerabilities,” “cyberphysical systems,” and “network security” were included. . Logical operators such as “AND” and “OR” were used to effectively combine different phrases, facilitating a targeted yet thorough search. To improve the results, queries such as “autonomous power systems AND cybersecurity” and “smart grid AND cyber threats” were conducted.

This systematic approach ensured that the collected literature was not only relevant to the focus of the review, but also sufficiently comprehensive to include diverse perspectives on the topic. The assessment attempted to provide a comprehensive and unbiased review of cybersecurity practices in autonomous power systems by including a variety of sources [6].

The systematic review used specific criteria to ensure the inclusion of high-quality and relevant studies. Inclusion requirements required that studies be peer-reviewed articles or conference proceedings published in reputable scientific journals or collections. The review focused on articles from the last decade that were designed to reflect current and emerging trends in cybersecurity for autonomous power systems [1]. Eligible studies should focus on cybersecurity measures, vulnerabilities, or responses to threats related to autonomous power systems, including entities such as smart grids and IoT integration within these frameworks.

Exclusion criteria were similarly stringent to maintain focus and quality. Studies were excluded if they were not in English, lacked empirical evidence, or were purely theoretical with no practical application to autonomous systems. In addition, short abstracts, opinion articles, or editorial content without a comprehensive review were excluded. Studies focused on non-electrical fields, such as general IT systems or unrelated industrial controls, were not included unless they offered specific analogies or insights relevant to autonomous electrical systems.

This systematic approach ensured that a thorough, relevant, and up-to-date literature collection was created, providing a solid foundation for analyzing and discussing cybersecurity in autonomous electrical systems.

Results of the study

The systematic review clearly defines key terms to ensure clarity and accuracy. Autonomous power systems refer to complex power grids that use automation and sophisticated control technology to operate autonomously without ongoing human supervision. These systems are typically components of large-scale smart grid structures that integrate sensors, controllers, and associated communication technologies to dynamically adjust power distribution using real-time data and predictive analytics. Their independent functions improve the efficiency, reliability, and sustainability of power generation and delivery.

Cybersecurity encompasses the tactics, methodologies, and processes used to protect cyber-physical systems, networks, and data from attacks, unauthorized access, and various digital threats that can disrupt operations. In autonomous power systems, cybersecurity combines hardware and software solutions, security implementations, and proactive strategies to protect critical infrastructure from vulnerabilities and

cyberattacks [7]. Maintaining the integrity and security of power systems is critical as they are increasingly targeted by sophisticated cyberattacks due to their importance to national infrastructure.

Many established models and theories are essential for formulating cyber defense solutions for power systems. The NIST Cybersecurity Framework is a fundamental framework that provides a systematic approach to detecting, protecting, detecting, responding to, and recovering from cyber incidents. Its versatility and effectiveness make it a widely recognized standard in the power sector. The CIA triad is a fundamental principle that emphasizes the protection of confidentiality, integrity, and availability of information, essential for protecting data and protecting the operational performance of power systems from unauthorized access and disruption. In addition, the *Defense in Depth* approach, which establishes multiple layers of security to protect against cyber threats, is often used. This layered strategy ensures that if one defense mechanism fails, others will continue to provide protection. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential for protecting network traffic by detecting and mitigating anomalies that indicate cyber attacks. Machine Learning (ML) models are becoming more widespread because they are adept at pattern analysis and detecting sophisticated cyberattacks across large datasets, providing superior performance compared to traditional methods [8]. The Zero Trust model, which requires continuous verification of all users and devices regardless of their network location, is becoming increasingly important as power systems become more interconnected and vulnerable to multiple access points. These models and tactics will help develop effective cyber defense mechanisms that are tailored to the dynamic and complex characteristics of autonomous power systems. They will enable these systems to withstand and recover from cyberattacks while maintaining the integrity of their critical operations. Autonomous power systems, which are essential for modern smart grids, are particularly vulnerable to cyber threats due to their complex and interconnected architecture. Phishing attacks are a common problem where criminals trick individuals into revealing sensitive information that compromises system security. Ransomware attacks pose a significant threat by encrypting critical operational data and demanding a ransom to decrypt it, potentially disabling grid operations. Distributed denial-of-service (DDoS) attacks can overwhelm networks, disrupting services and operational efficiency. In addition, as these systems increasingly integrate IoT devices, they are exposed to other threats, including device hijacking and botnet attacks, where compromised devices are used to carry out additional cyberattacks [9]. Supply chain attacks pose a significant risk, with criminal entities exploiting the software or hardware of third-party providers to gain access to the network's operational network. In addition, insider threats – whether intentional or unintentional – can lead to significant security breaches, highlighting the need for robust access controls and ongoing monitoring. The integration of AI and machine learning can also introduce algorithmic vulnerabilities, as the reliance on data-driven decision-making exposes the system to data manipulation or poisoning attacks that distort operational efficiency.

Man-in-the-middle (MitM) attacks, in which cybercriminals intercept and potentially alter communications between two parties, pose a significant threat to systems that rely on real-time data sharing for critical operational decisions. Zero-day exploits targeting undisclosed vulnerabilities in software or firmware pose a persistent challenge because they can be exploited before developers have the opportunity to patch them. Such vulnerabilities highlight the need for flexible and adaptable cybersecurity solutions to protect the integrity and reliability of autonomous power systems. (Figure 1).

In autonomous electrical systems, advanced cybersecurity tools and strategies are employed to safeguard infrastructure from cyber threats and maintain strong defenses. Firewalls and intrusion detection systems (IDS) serve as the initial defense, with firewalls managing network traffic based on established security rules and IDS detecting unusual or suspicious activities. Intrusion prevention systems (IPS) take this a step further by proactively blocking identified threats. Encryption plays a vital role by protecting sensitive data both in transit and at rest, ensuring it remains secure from unauthorized access or interception.

Endpoint security solutions are widely implemented to protect every device connected to the network, including servers and operational technology (OT) components like smart meters and controllers, from malware and other cyber exploits. Security Information and Event Management (SIEM) systems enhance real-time monitoring by analyzing security alerts from network hardware and applications, enabling rapid responses to potential threats. Network segmentation further strengthens security by dividing the network into isolated zones, limiting the spread of breaches and restricting attackers' lateral movement within the system [10].

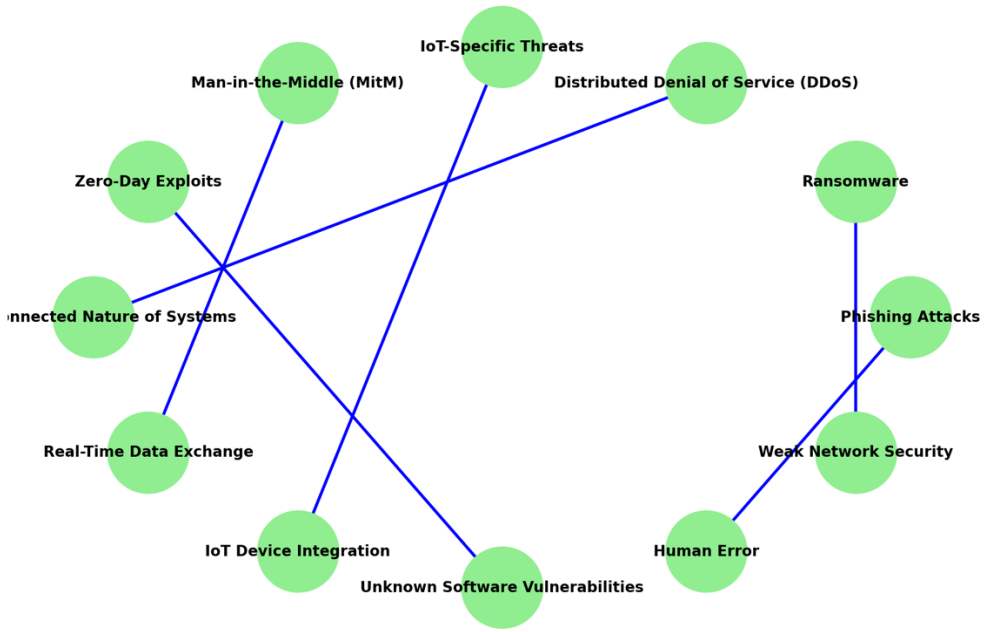

Figure 1. Cyber Threats and Vulnerabilities in Autonomous Electrical Systems: A Circular Representation

Identity and Access Management (IAM) systems play a critical role in securing access to essential systems by enforcing strict authentication and attribute-based access control policies for users. With the increasing adoption of IoT devices, specialized IoT security platforms are now commonly used to monitor and manage the security of these devices. Additionally, Zero Trust architectures are gaining traction, operating on the principle that all users and devices, whether inside or outside the network, must be continuously verified before gaining access. This approach significantly enhances the overall security framework by addressing both internal and external threats (Tables 1-2).

Table 1. Security Measures Overview

Category	*Components*
Network Security	*Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)*
Data Security Measures	*Encryption Technologies, Data Masking, Tokenization*
Application Security	*Security Testing, Application Firewalls, Secure Coding Practices*

Table 2. Advanced Security Layers

Category	*Components*
Identity Management	*Biometric Systems, Two-Factor Authentication, Single Sign-On (SSO)*
Endpoint Security	*Anti-Virus and Anti-Malware, Mobile Device Management*
Cloud Security	*Cloud Access Security Brokers (CASB), Secure Cloud Storage, Virtual Private Networks (VPN)*
Evaluation	*Effectiveness, Compliance with Regulations, Integration with Existing Systems*

The adoption of automated security solutions powered by artificial intelligence (AI) and machine learning (ML) is on the rise. These technologies enhance the ability to predict and respond to cyber threats by analyzing historical data and detecting patterns that signal potential security breaches. Together, they form a robust cybersecurity strategy designed to protect autonomous electrical systems from a wide range of threats while maintaining their operational reliability and continuity. Real-world

incidents underscore the critical importance of cybersecurity in these systems. For example, the 2015 cyberattack on Ukraine's power grid demonstrated how hackers used phishing schemes to deploy malware, enabling them to remotely disable substations and leave approximately 230,000 people without power for several hours. This was the first documented attack to successfully disrupt operational technology within a power grid. Similarly, the Stuxnet worm, discovered in 2010, targeted SCADA systems used in Iran's nuclear facilities. It manipulated centrifuges to self-destruct while displaying normal operations, showcasing a highly sophisticated cyber-physical attack (Clark, 2021). In practice, frameworks like the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards exemplify efforts to secure critical power systems. These standards mandate utilities to implement robust protection measures for cyber assets crucial to the reliability of the electric grid. To comply, many organizations are adopting advanced tools such as Security Information and Event Management (SIEM) systems and next-generation firewalls, which strengthen their cybersecurity posture [11].

The Dragonfly 2.0 campaign, active between 2011 and 2017, highlighted vulnerabilities in the energy supply chain by attempting to gain remote access to power grid operations in the US and Europe. This incident emphasized the importance of securing network boundaries and enforcing strict access controls. On a proactive front, many utilities now employ machine learning algorithms to predict and mitigate cyber threats before they materialize. These systems are integrated into operational networks to enable real-time threat monitoring and response.

These examples illustrate the evolving threats facing autonomous electrical systems and highlight the advanced strategies required to safeguard them against increasingly sophisticated cyberattacks. Building on the discussion of real-world examples highlighting the importance of cybersecurity in autonomous electrical systems, the 2017 WannaCry ransomware attack serves as a significant case study. Although its targets were broad, the attack exposed the vulnerability of critical infrastructures, including the energy sector, to global cyber threats. WannaCry exploited outdated, unpatched, or unsupported Windows systems, encrypting data and demanding ransom payments for decryption. This incident emphasized the urgent need for regular updates and security patches in critical infrastructure systems to prevent exploitation by similar malware campaigns (Foster, 2022). In response to such threats, energy companies are increasingly adopting advanced persistent threat (APT) protection techniques. These include network segmentation, continuous monitoring, and anomaly detection systems to identify and neutralize threats before they can execute or move within the network. For example, Southern California Edison (SCE) has implemented cutting-edge cybersecurity solutions to protect its operational technology. The company employs real-time monitoring and advanced analytics to detect unusual network activity, a potential sign of a cyberattack. Additionally, multi-factor authentication (MFA) and strict access controls ensure that only authorized personnel can access critical systems, reducing the likelihood of insider threats.

A suspected attack on India's power grid in 2019, allegedly carried out by state-sponsored entities, highlights the vulnerabilities facing autonomous power systems. While it has not been extinguished, it appears to have been a reconnaissance effort to map grid infrastructures for potential sabotage. The incident has prompted utilities around the world to improve their cybersecurity protocols, focusing on preventing breaches and understanding potential threats to formulate specific countermeasures (O'Donnell, 2020). These examples highlight the dynamic nature of cyberthreats to autonomous power systems and the imperative for robust, multifaceted countermeasures. Effective approaches must combine new technologies with human oversight to protect critical energy infrastructure.

Recent advances in cybersecurity are revolutionizing the way autonomous power systems are protected from the growing threat landscape. Artificial intelligence (AI) and machine learning (ML) technologies have significantly improved the detection and response to cyber threats by analyzing large datasets to identify patterns that indicate attacks. These systems can quickly detect anomalies and eliminate threats in real time, thereby reducing response times and limiting potential damage. Blockchain technology is also emerging as a viable tool for securing data transmissions and

transactions in energy networks. A decentralized, tamper-resistant ledger system ensures data integrity and traceability, increasing system security. Together, these advances are changing the cybersecurity landscape for autonomous power systems, facilitating proactive and effective defense. The advent of quantum cryptography is a significant advance in cybersecurity, using concepts from quantum mechanics to protect data transmissions. This technology provides unique encryption that can potentially protect against even the most sophisticated cyberthreats, including threats from quantum computers. The introduction of zero-tolerance security models is revolutionizing conventional security methodologies. Unlike perimeter-based approaches, zero trust assumes that no person or device is inherently trusted, regardless of their location in relation to the network. This paradigm requires continuous verification of all activities, thereby significantly reducing the potential attack surface. Security automation, automation and response (SOAR) systems are increasingly important in a modern cybersecurity strategy. These solutions simplify threat detection, intelligence analysis and automation of response actions, which allows enterprises to quickly address cyber threats while conducting threat intelligence. Sophisticated endpoint detection and response (EDR) systems, combined with SOAR tools, provide extensive monitoring and response functions across all network devices, which makes it easier to quickly identify and mitigate potential threats. In the field of IoT security, which is critical for autonomous power systems, specialized platforms are being created to protect device connectivity and monitor the lifecycle of IoT devices. These technologies identify sensitive devices, facilitate rapid updates and monitor irregular activities that may indicate a security breach. Overall, these advances significantly improve the security of critical infrastructure, especially in autonomous power systems, where the consequences of attacks are severe. They offer a more flexible and robust cybersecurity framework that is better suited to address the changing threat landscape.

Artificial intelligence (AI) and machine learning (ML) have become essential components of modern cyber defenses, especially in protecting autonomous power systems. These technologies provide enhanced analytics capabilities that enhance threat detection and response. AI and machine learning can rapidly analyze large data sets, identify trends and anomalies that may indicate a cyberattack. By analyzing historical data, they can predict and adapt to new strategies used by competitors. Anomaly detection algorithms can monitor network traffic in real time, identifying anomalies such as atypical data transfers or suspicious login requests that may indicate a potential breach or attack attempt. These capabilities make AI and ML indispensable tools for ensuring the security and reliability of autonomous power systems [12-13].

Machine learning (ML) is important in predictive cybersecurity because it studies patterns and trends to predict potential attacks. This allows enterprises to implement preventive strategies against potential threats, which is especially effective in autonomous power systems where minimizing downtime is critical. In addition, AI-driven security automation technologies can autonomously address identified risks by isolating affected systems or implementing remediation without human intervention. This automation significantly reduces response time and reduces the risks associated with human error. AI extends behavioral analysis by creating baseline profiles for typical network activity and identifying anomalies that may indicate malicious activity. It is particularly effective in identifying insider threats and advanced malware that can bypass conventional detection methods. In addition, AI improves phishing detection by systematically evaluating email and web content with accuracy that exceeds human capabilities. This reduces the likelihood of phishing attempts, often a prelude to large-scale, significant breaches. Applying AI and ML to cybersecurity practices will increase the security of autonomous power systems by providing scalability and efficiency. These technologies will allow defenses to dynamically respond to the ever-evolving threat landscape, addressing emerging vulnerabilities and attack methodologies. The ability to rapidly evolve is critical to maintaining an edge over cyberthreats in a dynamic and ever-changing landscape.

Discussion

This systematic review examines the complex cybersecurity challenges facing autonomous power systems, assessing threats, vulnerabilities, and current defense solutions for these critical components of critical infrastructure. The increasing integration of modern technologies such as IoT and reliance on real-time data analytics have made these systems attractive targets for attacks. Recent advances in cybersecurity, such as the integration of artificial intelligence, machine learning, blockchain technology, and quantum cryptography, have significantly increased the ability to predict, detect, and mitigate cyberattacks. These solutions enhance security and operational efficiency, providing a dual advantage to autonomous power systems. Implementing a zero-trust architecture and endpoint detection and response systems demonstrates a proactive cybersecurity strategy that prioritizes ongoing verification and rapid threat mitigation. Artificial intelligence has transformed cybersecurity by automating and improving threat detection and mitigation, leading to more agile and adaptive systems that can respond to the evolving cyberthreat landscape. Despite these advances, the assessment highlights the need for ongoing research to address emerging vulnerabilities and the importance of maintaining robust security policies to protect against both external and internal threats. This work provides a comprehensive review of cybersecurity in critical electrical infrastructures, highlighting the need for continued innovation and vigilance. As reliance on autonomous systems increases, so too must the ability to protect them.

Conclusion

This systematic review examines the complex cybersecurity challenges facing autonomous power systems, assessing threats, vulnerabilities, and current defense solutions for these critical components of critical infrastructure. The increasing integration of modern technologies such as IoT and reliance on real-time data analytics have made these systems attractive targets for attacks. The assessment highlights the evolution of threats, from ransomware to advanced state-sponsored cyber operations, citing real-world incidents such as the attack on Ukraine's power grid and the Stuxnet virus as clear examples of the concerns that are being raised. Recent advances in cybersecurity, such as the integration of artificial intelligence, machine learning, blockchain technology, and quantum cryptography, have significantly increased the ability to predict, detect, and mitigate cyberattacks. These solutions enhance security and operational efficiency, providing a dual advantage to autonomous power systems. Implementing a zero-trust architecture and endpoint detection and response systems demonstrates a proactive cybersecurity strategy that prioritizes ongoing verification and rapid threat mitigation. Artificial intelligence has transformed cybersecurity by automating and improving threat detection and mitigation, leading to more agile and adaptive systems that can respond to the evolving cyberthreat landscape. Despite these advances, the assessment highlights the need for ongoing research to address emerging vulnerabilities and the importance of maintaining robust security policies to protect against both external and internal threats. This paper provides a comprehensive review of cybersecurity in critical electrical infrastructures, highlighting the need for continued innovation and vigilance. As reliance on autonomous systems increases, so too must the ability to protect them.

References

[1] Brown M., Foster L. (2016) Zero Trust Model: Rethinking Security in the Age of Remote Operations. Cybersecurity Rev. 12, 213–230. URL: https://doi.org/10.48047/nq.2022.20.6.NQ23044

[2] Clark J., Patel K. (2021) Ransomware Attacks in the Energy Sector: A Call for Advanced Cybersecurity Measures. J. Energy Security. 6, 92–107. URL: https://doi.org/10.1080/02646811.2021.1943935

[3] Davis S., Kumar P. (2018) Machine Learning for Network Security: A Review of Threat Detection Techniques. Network Security. 6, 19–25. URL: https://doi.org/10.1016/j.comnet.2021.107840

[4] Edwards C., Robinson N. (2019) IoT Security Management in Electrical Systems. J. Internet Things. 5, 89–104.

[5] Foster J., Greenwood A. (2022) Application of Blockchain in Securing Autonomous Energy Systems. Blockchain in Business. 3, 78–89. .URL: DOI:10.1088/1742-6596/1626/1/012057

[6] Garcia M., Thompson H. (2018) The Role of Machine Learning in Predictive Cyber Defense. AI & Society. 33, 117–129. URL: https://doi.org/10.1145/3545574

[7] Bonandir, N. A., Jamil, N., Nawawi, M. N. A., Jidin, R., Rusli, M. E., Yan, L. K., & Maudau, L. L. A. D. (2021, March). A review of cyber security assessment (CSA) for industrial control systems (ICS) and their impact on the availability of the ICS operation. In Journal of Physics: Conference Series (Vol. 1860, No. 1, p. 012015). IOP Publishing. Harrison G., Sanders T. (2019) A Comprehensive Study on IoT Security in Smart Grids. Smart Grid Tech. 4, 154–165. URL: DOI:10.1088/1742-6596/1860/1/012015

[8] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainale energy reviews, 100, 143-174.URL: https://doi.org/10.1016/j.rser.2018.10.014

[9] Machová K., Mach M., Porezaný M. Deep learning in the detection of disinformation about COVID-19 in online space //Sensors. – 2022. – Т. 22. – №. 23. – С. 9319. URL: https://doi.org/10.3390/s22239319

[10] Singh J. P. et al. Attention-based LSTM network for rumor veracity estimation of tweets //Information Systems Frontiers. – 2022. – С. 1-16. URL: https://doi.org/10.1007/s10796-020-10040-5

[11] Al-Ibrahim R. M., Ali M. Z., Najadat H. M. Detection of hateful social media content for arabic language //ACM Transactions on Asian and Low-Resource Language Information Processing. – 2023. – Т. 22. – №. 9. – С. 1-26. URL: https://doi.org/10.1145/3592792

[12] Chung J. Empirical evaluation of gated recurrent neural networks on sequence modeling //arXiv preprint arXiv:1412.3555. – 2014. URL: https://doi.org/10.48550/arXiv.1412.3555