CYBERATTACKS ON RENEWABLE ENERGIES: "HOW HACKERS ARE THREATENING THE ENERGY TRANSITION AND WHICH TECHNOLOGIES CAN PROTECT US"

Prof. Dr. Raphael Röttinger
Ulm, GERMANY

INTRODUCTION

The energy sector is undergoing progressive digitalisation. This development opens up new opportunities, but there are also significant risks. For example, the increased use of digital technologies in renewable energy systems means increased vulnerability to cyberattacks (Chowdhury & Gkioulos, 2021, p. 2). This vulnerability destabilises not only efficiency, but also the energy supply itself. The cyber attack, which became known as "Dragonfly", shows that the human factor also plays an important role. Therefore, not only technical measures must be taken, but also those that train and sensitise human resources in order to reduce errors. (Chowdhury & Gkioulos, 2021, p. 3).

The aim of this paper is to demonstrate the relevance of cyber security measures within renewable energy systems. To this end, organisational measures such as training measures are presented. Such measures serve to shield systems and increase their resilience to attacks. The technological dependence of renewable energy sources leads to an increase in the complexity of security requirements. These dangers overshadow many of the advantages of renewable energies (Gellings, 2010, p. 57).

In addition, new technologies such as intelligent networks, which are being integrated into this sector, create further challenges that need to be overcome. The operation of these systems must be stable and secure in the long term, which requires the development of technical and organisational solutions.

Method

This paper is based on a comprehensive literature review aimed at identifying the main security risks for renewable energy systems and developing solution strategies. Particular attention was paid to research that deals with cyber security measures such as firewalls, intrusion detection systems (IDS) and educational aspects.

Theory

Cybersecurity plays a major role in networked energy systems that are increasingly reliant on digital technologies (Johnson, 2015, p. 292). In order to understand these challenges, the fundamental changes in renewable energy systems and their digital transformation are examined in more detail below (Asif, 2022, p. 50).

Overview of renewable energy systems and their digital transformation

Renewable energy systems utilise inexhaustible natural resources such as sun, wind, water, geothermal energy and biomass, which, unlike fossil fuels, are quickly renewed. Photovoltaic systems and solar thermal convert solar energy into electricity, while wind turbines and hydroelectric power stations utilise the kinetic energy of wind and water. Geothermal energy extracts heat from the earth's interior, and biomass includes organic materials for energy production. These sources reduce greenhouse gas emissions and secure the energy supply in the long term (Al Qubeissi et al., 2020, p. 7-23).

The sharp increase in the efficiency and reliability of energy supply systems associated with renewable energy sources is leading to a progressive digital transformation in this sector. The implementation of smart grids and decentralised energy systems plays a key role in this sector. The digitalisation of energy systems is being driven significantly by the use of distributed energy resources (DERs), virtual power plants (VPPs) and peer-to-peer (P2P) solutions (Asif, 2022, p. 50).

In this context, however, it must be pointed out that digitalisation comes with both advantages and new problems. On the one hand, digitalisation promotes security of supply, but on the other hand, it also creates new targets for cyber attacks (Johnson, 2015, p. 292). In particular, data flows in networked systems - for example VPPs and P2P trading platforms - harbour considerable potential dangers. This is due to the large number of potential access points for potential attackers.

The complexity of these networked infrastructures requires the continuous development of security strategies to ensure the resilience of systems against cyber threats (Johnson, 2015, p. 292; Asif, 2022, p. 50).

The ongoing digital transformation in the field of renewable energy systems is being driven to a large extent by the use of modern technologies such as the Internet of Things (IoT). The term "Internet of Things" (IoT) refers to the networking of physical devices that can collect and exchange data. The aim is to make the operation of energy systems more efficient (Macaulay & Singer, 2010, p. 274).

Definition and importance of cybersecurity in the energy sector

The International Telecommunication Union (ITU) defines cybersecurity as the totality of all measures, concepts and technologies that serve to protect the cyber environment and the assets of organisations and users. These assets include not only the connected computing devices, personnel and infrastructure, but also a variety of other factors such as applications, services, telecommunication systems and all information transmitted and/or stored in the cyber environment. (Johnson, 2015, p. 222).

Ensuring cyber security is a critical factor for the energy sector, as it plays a key role as an essential infrastructure and is therefore highly vulnerable to cyber attacks. Due to the large number of components that are used in the electricity sector and are interconnected, there is a complex network of relationships that influence each other. In this context, the following aspects in particular must be taken into account: the production, transmission and distribution of electricity and the interfaces between these areas. The increased risk of cyberattacks at these interfaces results from the fact that disruptions at these neuralgic points can cause large-scale power outages, which would massively jeopardise the security of supply (Johnson, 2015, p. 46).

With the transformation to decentralised, digitally networked energy systems, vulnerability to cyber security attacks continues to increase. Power generation and distribution are increasingly being managed and controlled via IT systems, which increases vulnerability to cyberattacks. The use of protective measures such as data encryption and IDS is necessary to ensure the confidentiality, authenticity and integrity of data as well as the availability of IT systems (Asif, 2022, p. 65-66).

Security challenges in networked energy systems (e.g. in SCADA systems)

Within networked energy systems such as the Supervisory Control and Data Acquisition (SCADA) system, monitoring and controlling the infrastructure plays a crucial role. A major problem with such systems is their particular vulnerability to cyber attacks, as adequate protection against such attacks cannot yet be guaranteed. This is due to the fact that SCADA systems were originally designed for use in isolated environments without an internet connection. However, in the course of digital transformation and networking with other IT systems, new vulnerabilities have emerged as these systems do not have any integrated security measures such as encryption or IDS in their original architecture (Johnson, 2015, p. 47).

In the scientific literature, advanced security measures such as firewalls, encryption techniques and real-time monitoring are recommended as solutions to protect SCADA systems from cyber threats (Asif, 2022, p. 65; Johnson, 2015, p. 47). Another problem is that a large number of older SCADA systems cannot be easily updated to modern security standards without compromising operations. This makes the introduction of comprehensive security measures considerably more difficult. Internal threats such as disgruntled employees can also pose a threat to SCADA systems. These people could manipulate the system through targeted acts of sabotage. It is therefore not enough to simply secure these systems technically; security at the organisational level is also necessary. Regular employee training and awareness-raising measures are crucial to minimise the risk of human error (Asif, 2022, p. 65).

Discussion

The following chapter discusses the main problem areas and risks involved in implementing security strategies in decentralised and digitalised energy systems. In addition to the challenges, current solution approaches are also discussed, which are intended to help protect the systems. Finally, an outlook is given on future developments in which artificial intelligence (AI) and machine learning (ML) will play a central role.

Challenges in the implementation of safety strategies in renewable energy systems

As outlined above, systems such as wind turbines, photovoltaics and smart grids are becoming increasingly complex and interconnected. At the same time, the implementation of standardised security strategies to protect specific infrastructures is also becoming increasingly complex. This represents an obstacle to the application of security strategies to these systems.

Decentralised structures and their impact on security

The decentralised structure of natural, renewable energy systems is one of their most important characteristics. This characteristic is due to the fact that the systems often comprise a large number of geographically distributed units. The implementation of security strategies is therefore the most significant challenge. In contrast to centralised power supply systems, the control and monitoring of security solutions in decentralised structures proves to be more difficult, as central control of the security systems is not possible (Luo & Hong, 2012, p. 47). Consequently, the degree of complexity in taking the necessary protective measures is significantly higher, as each of these decentralised units can potentially be the target of a cyber attack.

The management of distributed units is hindered by a variety of factors, which leads to limited enforceability of uniform security standards in this decentralised structure. The use of different security solutions by individual users who do not have specific security policies increases the risk of incompatibilities and the danger of introducing potential vulnerabilities into the system (Johnson, 2015, p. 102).

Lack of standardisation

A key problem for renewable energy systems is the lack of standardisation of cybersecurity solutions, which impairs the effectiveness and efficiency of cybersecurity in the context of energy supply networks. International guidelines and standards exist, such as the NIST-800-82 and NERC-CIP standards, but these are not aligned with the specifics of renewable energy systems. The NIST-800-82 standard provides guidelines for the security of industrial control systems (ICS), including SCADA systems, which are used in many critical infrastructures (Stouffer, Falco, & Scarfone, 2023), while the NERC-CIP standard aims to ensure the security of energy supply systems by establishing minimum requirements for the protection of critical infrastructure in the energy sector (Macaulay & Singer, 2011, p. 24).

Furthermore, the inconsistent implementation of pre-standards is problematic and leads to a weakening of global cyber security in the energy sector. In the United States, for example, binding standards for process controls have often not been established in the past, even in sensitive infrastructures. (Macaulay & Singer, 2011, p. 24).

As explained above, insufficient standardisation is an obstacle to the integration of new technological developments into established energy systems. An exemplary scenario is the connection of smart grids to traditional energy systems. Compatibility problems manifest themselves in this process, as older systems were generally not designed for the integration of modern technologies such as cloud computing and the Internet of Things (IoT) (Ernst & Young Global Limited, 2024, p. 12).

Furthermore, while technologies such as AI, big data and the IoT have brought fundamental advances in the optimisation of energy systems, they have also increased security risks, especially when integrating traditional systems into modern digital infrastructures (Lai, et al., 2024, p. 47).

Organisational and human challenges

Analyses of safety incidents in renewable energy systems reveal that a significant proportion of these events can be attributed to human error. In particular, inadequately trained personnel contribute significantly to the vulnerability of the systems (Chowdhury & Gkioulos, 2021, p. 3). In practice, however, the human and organisational factor is often disregarded when implementing cybersecurity strategies. Insufficient preparation of employees for security requirements is a major cause of this. There are often insufficient or in-depth training and awareness programmes for the workforce, which gives potential attackers easy access (Chowdhury & Gkioulos, 2021, p. 3).

The most common methods attackers use to access critical systems include phishing attacks and other forms of social manipulation, such as spear phishing and social engineering. These attacks are often successful because humans are the weakest point in the security network. (Chowdhury & Gkioulos, 2021, p. 3).

For companies in the renewable energy sector, continuous investment in training programmes is an indispensable measure to strengthen the resilience of their employees (Chowdhury & Gkioulos, 2021, p. 2).

Technological complexity and new threats

The progressive implementation of digital technologies such as the Internet of Things (IoT) and networked sensors in renewable energy supply systems is associated with a number of challenges. While these technologies offer advantages in terms of efficiency and automation, they significantly increase the attack surface for potential cyberattacks (Macaulay & Singer, 2010, p. 230). The large number of connected devices leads to an increase in attack surfaces for cyber criminals, as many IoT devices have inadequate security measures . This makes IoT devices in renewable energy systems an attractive target for attacks, especially when these devices are integrated into critical infrastructures such as SCADA systems (Macaulay & Singer, 2010, p. 304).

The integration of SCADA systems harbours a major risk as they are used to monitor and control energy generation and distribution. In addition, the modernisation of SCADA systems has been neglected in recent years, which increases their vulnerability to attacks as they do not meet the requirements of modern cyber security (Macaulay & Singer, 2010, p. 232).

Recent cyberattacks, including the attack on Deutsche Windtechnik in 2022, in which control of almost 2,000 wind turbines was lost for more than a day, highlight the urgent need for increased security measures (Ernst & Young Global Limited, 2024, p. 9).

Lack of cooperation between stakeholders

A major obstacle to the development of effective security strategies in the energy sector is the lack of cooperation between the various players, particularly between the energy industry and cybersecurity providers. However, co-operation between these two sectors is essential in order to develop comprehensive security solutions, such as the establishment of uniform security standards that are tailored to the complex challenges of smart grids and networked energy systems (Sorebo & Echols, 2012, p. 122).

The fact that numerous organisations and companies do not have common standards and communication protocols proves to be particularly problematic. This results in isolated implementation of security measures without effective coordination between the players involved. Increased co-operation between the energy sector and cybersecurity providers is important to strengthen cybersecurity in the energy sector. (Sorebo & Echols, 2012, p. 162). The key players include government institutions, which set the regulatory framework, as well as companies and specialised security service providers.

The government plays a central role by issuing regulations that define the minimum requirements for cyber security. The practical implementation of these measures is the responsibility of companies and security service providers. (Sorebo & Echols, 2012, p. 122).

Analysis of current solution approaches: Firewalls, Intrusion Detection Systems IDS, encryption techniques

In view of the increasing threats posed by cyber attacks on renewable energy systems, technical solutions such as IDS and encryption have been developed to secure data integrity and system control. These measures strengthen the resilience of critical infrastructures both preventively and reactively.

Firewalls

The use of firewalls is the primary line of defence against attacks on networked energy systems. Their purpose is to prevent unauthorised access to these systems. Intelligent firewalls are extremely relevant in this context (Macaulay & Singer, 2011, p. 230).

Intrusion Detection Systems (IDS)

Intrusion detection systems play an important role in real-time detection in the context of recognising attacks. The functionality of IDS includes the efficient detection of anomalies and the targeted response based on this. This can include, for example, blocking malicious activities or sending alerts to security personnel. In the literature, IDSs are divided into two categories: signature-based systems, which are based on known attack patterns, and anomalous systems, which recognise and react to unusual activities (Lai et al., 2024, p. 10).

By using reinforcement learning (RL) and ML, modern IDS are able to react flexibly to changing network conditions. It is also possible to recognise network activities and complex attack patterns using autoencoders (AE) and one-class support vector machines (OCSVM) (Lai et al., 2024, p. 10).

Another advantage of RL-based IDS is the ability to not only make decisions in real time, but also to adapt the system itself to changing grid situations. The use of deep Q networks (DQN) is proving to be particularly helpful in decentralised renewable energy systems. The networks ensure responsiveness so that potential threats can be identified and averted before they jeopardise critical infrastructure (Lai et al., 2024, p. 12).

In addition, automated risk assessments generated by ML and recurring patterns enable a standardised and timely evaluation of threats. This increases the effectiveness of countermeasures, closes potential security gaps and prevents potential attacks (Macaulay & Singer, 2011, p. 230). However, the integration of IDS into existing security infrastructures remains a major challenge, as sufficient network integration and networking between the systems has not yet been achieved (Macaulay & Singer, 2011, p. 230).

Encryption techniques

Ensuring integrity is an important point in the communication channels of networked energy systems, as secure communication can only be guaranteed by ensuring the confidentiality of data. This is particularly relevant for SCADA systems (Supervisory Control and Data Acquisition), which are used to monitor and control renewable energy systems. These systems rely on effective encryption mechanisms to protect against manipulation and unauthorised access to data (Johnson, 2015, p. 47; Asif, 2022, p. 65).

However, modern SCADA protocols such as Modbus TCP and DNP3 often lack sufficient encryption and authentication mechanisms, making them particularly vulnerable to cyberattacks. Modbus, for example, does not have built-in security mechanisms such as encryption or authentication, so additional measures such as secure tunnels or advanced encryption are required. DNP3, on the other hand, includes basic security features, such as authentication and data integrity checks, which enable more secure communication. However, in many cases, additional security measures are required to ensure complete protection. These vulnerabilities are particularly prevalent in cloud-based environments where SCADA systems are operated. Attackers can easily access sensitive information such as IP addresses and credentials (Ernst & Young Global Limited, 2024, pp. 8-9; Zahran & Zahra, 2023, p. 1747).

In addition to traditional methods of encryption, the use of quantum-safe cryptographic techniques is becoming increasingly important to counter the potential threats posed by quantum computers. Quantum computers use the laws of quantum mechanics to perform complex calculations such as factoring large numbers more efficiently. This poses a threat to conventional encryption techniques such as Rivest-Shamir-Adleman (RSA), as quantum computers could break them in a short space of time. The development of quantum-resistant encryption methods such as post-quantum cryptography is therefore highly relevant for the cyber security of networked energy systems (Ernst & Young Global Limited, 2024, p. 17; Hey, 1998, p. 5).

An innovative approach to securing cloud-based SCADA systems is the use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This technology enables fine-grained access control over encrypted data by taking both static and dynamic user attributes into account. With CP-ABE, access to data can be granularly controlled so that only users with the appropriate attributes are granted access to the information (Ernst & Young Global Limited, 2024, p. 14; Doshi & Patel, 2022, p. 5).

Future developments: The role of AI and machine learning (in outlook)

The use of technologies such as AI and ML will increasingly characterise cyber security in renewable energy systems and therefore play a decisive role in their future design. In particular, innovative technologies such as RL, deep learning (DL) and neural networks have the ability to identify threats with greater speed and combat them effectively through the automated initiation of countermeasures. RL models are able to proactively detect threats by analysing network anomalies in real time and reacting to them through self-learning mechanisms. Deep learning and neural networks can also efficiently process large amounts of data and recognise patterns in cyberattacks that would remain invisible to traditional systems (Lai, et al. 2024, p. 14). It can therefore be assumed that such technologies will continue to play a key role in cyber security in the future.

Conclusion

Ensuring the cyber security of energy systems presents those responsible with an increasingly complex task, the relevance of which continues to increase with the ongoing digitalisation and networking of these systems and the management of which is therefore a high priority. The increasing digitalisation and networking of energy systems is accompanied by an increased vulnerability to cyber attacks, which can have a potentially serious impact on security of supply. The analysis of current solutions, which include firewalls, IDS, encryption techniques, SCADA security measures, PRE and CP-ABE, shows that these technologies fulfil a fundamental function in the defence against threats. However, further optimisation can be achieved through the use of AI and ML, which is why these two aspects are of great importance.

AI-supported IDS in particular offer a dynamic and adaptive solution that enables anomalies to be recognised and responded to in real time. The use of these technologies increases the effectiveness of security strategies and contributes to their improvement. However, the standardisation of security strategies remains a major challenge. To overcome this challenge, not only technical but also organisational measures are required. These include regular and comprehensive staff training. At the same time, standardised security protocols and guidelines must be implemented.

I Bibliography

Al Qubeissi, M., El-kharouf, A., & Soyhan, H. S. (Eds.). (2020). *Renewable Energy: Resources, Challenges, and Applications*. IntechOpen.

Asif, M. (2022). *Handbook of Energy and Environmental Security*. Charlotte Cockle.

Chowdhury, N., & Gkioulos, V. (2021). Cybersecurity training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361. doi:10.1016/j.cosrev.2021.100361

Doshi, N., & Patel, R. (2022). An improved approach in CP-ABE with proxy re-encryption. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 2, 100042.

Ernst & Young Global Limited. (2024). *Cyber attacks in the energy industry: Enhancing resilience against cyber threats.* https://assets.ey.com/content/dam/ey-sites/ey-com/en_ae/topics/government-and-public-sector/ey-ae-cyber-attacks-in-the-06-2024.pdf

Gellings, C. W. (2010). *The Smart Grid: Enabling Energy Efficiency and Demand Response*. The Fairmont Press, Inc.

Hey, T. (1998). *Quantum Computing: An Introduction*. University of Southampton.

Johnson, T. A. (2015). *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. CRC Press.

Lai, Y.-C., Sudyana, D., Lin, Y.-D., Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2024). Task assignment and capacity allocation for ML-based intrusion detection as a service in a multi-tier architecture. *Journal of Network and Computer Applications*, 229, 103936.

Luo, F. L., & Hong, Y. (2012). *Renewable energy systems: advanced conversion technologies and applications.* CRC Press.

Macaulay, T., & Singer, B. L. (2011). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.

Sorebo, G. N., & Echols, M. C. (2012). *Smart grid security: an end-to-end view of security in the new electrical grid.* CRC Press.

Stouffer, K., Falco, J., & Scarfone, K. (2023). *Guide to Industrial Control Systems (ICS) Security: NIST Special Publication* 800-82, Revision 2, Tech. rep, National Institute of Standards and Technology.

Zahran, B., & Zahra, F. A. (2023). IT/OT Convergence Protocols: DNP3, Ethernet/IP, and Modbus. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE),* (pp. 1-5).