BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2025 • Vol. **83**, pp. 58-62
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.83.25.04

Challenges of Smart Microgrids Cybersecurity

Radoslav Yoshinov

Institute of Mathematics and Informatics at Bulgarian Academy of Sciences
Email: yoshinov@cc.bas.bg

The recently published monograph "*Microgrids and Cybersecurity*" deals with very important and current problems related to the security aspects of microgrids. It consists of 9 chapters and begins with an introduction to the brief description of microgrids.

"Microgrids are defined as small, low- or medium-voltage power systems with a decentralized group of power sources and loads that can operate connected to or isolated from the main power grid. To ensure proper control, microgrids rely on information and communication technologies."

In today's world, society is becoming increasingly digitalized, and critical infrastructure is exposed to increased exposure to cyber threats. Modern economies also run on electricity, and without it they grind to a halt. One emerging solution is microgrids, which offer access to reliable power and constant electrical resilience for both businesses and governments.

Chapter 1 explains why microgrids can be considered a plan for the extended protection of critical infrastructure. Microgrids ensure that facilities and operations remain functional, but can also help stabilize the grid during periods of

grid stress. With their ability to operate independently of the main grid, microgrids can not only provide continuous protection against cyber threats, but also offer a flexible and efficient solution for the evolving energy landscape. The main components of a typical microgrid are shown in Fig. 1.

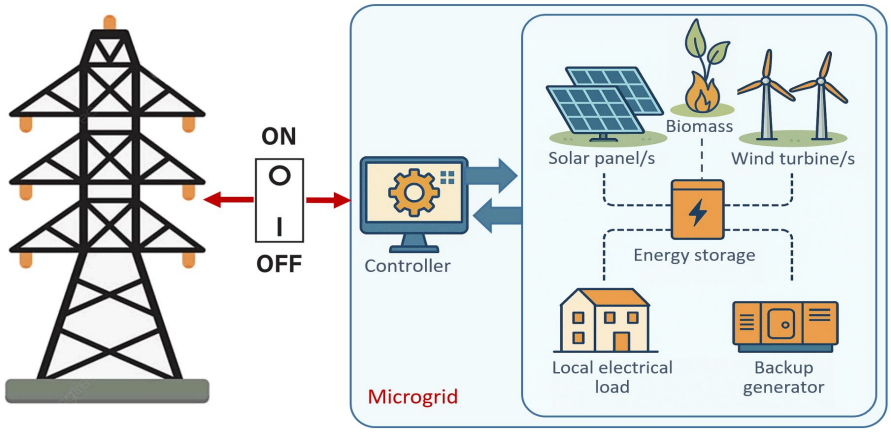

Fig. 1. Components of a typical microgrid [1]

Chapter 2 provides a classification of the different forms of cyberattacks against microgrids. A comprehensive understanding of the transmission channels in microgrids is necessary for accurate and effective detection of cyberattacks. Cyberattacks can lead to system intrusion, rendering the machine unable to execute desired commands. Six types of cyberattacks are described [2]. This chapter ends with 16 references.

Chapter 3 refers to the architectures and mathematical basis of the data exchange structure in microgrids. To analyze the effects of cyberattacks, it is important to model data exchange architectures in microgrids. Here, the different network topologies are described: centralized, decentralized/hierarchical, and distributed [3]. A comparison of some basic characteristics of microgrids using centralized and decentralized control structures is presented. In addition, the mathematical foundation of multi-agent systems is presented, which can be used to express the connections between vertices and edges in a data exchange structure in a microgrid [4, 5]. This chapter ends with 11 references.

Chapter 4 introduces communications in the microgrid infrastructure. The communication infrastructure is responsible for ensuring interoperability within a defined time horizon, taking into account the confidentiality, integrity, availability and authenticity of the exchanged information [6]. This makes smart microgrids vulnerable to cyberattacks. Attackers try to disrupt the microgrid operations by

manipulating the transmitted data or attacking the physical system. Special attention is paid to the paradigm of software-defined networking in a microgrid, which encompasses both security and control applications [7, 8]. This chapter is based on 26 references.

Chapter 5 refers to protocols and standards in smart microgrid infrastructure. This section presents a systematic review of standards, challenges, and solutions for cyber resilience of renewable smart microgrids, focusing on communication technologies, standards, and protocols [9]. There are 43 references to this chapter.

Chapter 6 focuses on smart microgrid cybersecurity. The communication infrastructure and associated devices embedded with sensors, software, and network connectivity that enable data collection and exchange expose renewable smart microgrids to significant cyber threats. Cybercriminals use various methods to target renewable smart microgrids, including data manipulation, compromise of smart electronic devices, communication hijacking, malware injection, and physical system attacks. The roadmap for attacking renewable smart microgrids is presented, types of attacks on embedded devices and their consequences are described, and some strategies for preventing malware infection are presented [10]. Possible attacks on communication and protocols are described, consequences of cyberattacks on protocols are analysed, and some solutions for preventing cyberattacks are presented [11, 12]. The number of references in this chapter is 19.

Chapter 7 discusses cyber vulnerabilities of renewable energy sources, protective measures and microgrid operation modes. Modern energy systems rely on complex networks of smart meters, sensors and automated control systems. Renewable energy sources are a vital part of renewable smart microgrids and are the main target of cyberattacks. Cyber vulnerabilities of photovoltaic system, wind power plant, and energy storage sources are analysed in detail [13, 14]. The operating conditions of microgrids and microgrid operation modes are presented, as well as protective measures to counter cyberattacks. The number of references in this chapter is 39.

Chapter 8 presents testing, assessment, and risk analysis in smart grids. In modern smart grids, managed by advanced computing and networking technologies, health monitoring relies on secure cyber-physical connectivity. It is difficult to assess the cybersecurity risk of smart grids due to the huge variety of information and communication technologies that can be used to achieve a wide range of tasks. Vulnerability assessment and risk analysis are two related but distinct processes that are often used in the field of cybersecurity to identify potential threats and vulnerabilities in computer systems, networks, and other digital assets. Therefore, researchers around the world are making enormous

efforts to study microgrids and to build testbeds and demonstration sites [15, 16]. The number of references in this chapter is 30.

Chapter 9 addresses current solutions for ensuring cybersecurity of microgrids such as machine learning. In ensuring cybersecurity of microgrids in the context of the increasing digitalization of energy systems, machine learning plays an important role, providing new methods for detection, prevention and response measures. Classifications of intrusion detection systems are presented [17], as well as some global solutions for protection against cyberattacks [10, 18, 19]. The number of references in this chapter is 44.

Cyberattacks on energy infrastructure can disrupt power supply, cause financial losses, and even pose a threat to national security. Therefore, effective microgrids that combine physical and cyber systems require reliable and efficient monitoring and administration. Microgrid cybersecurity research provides various aspects for securing and verifying various measures to ensure the normal operation of the microgrid.

The monograph presents challenges and solutions for protecting smart microgrids from cyberattacks that can be used by both specialists in the field and a wide range of readers interested in modern solutions for protecting smart microgrids.

References

1. Borissova, D.: Microgrids and Cybersecurity. Obrazovanie i Poznanie, 138 pages, ISBN 978-619-7515-57-2 (2025).
2. Ahmed, I., El-Rifaie, A.M., Akhtar, F., Ahmad, H., Alaas, Z., Ahmed, M.M.R.: Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. Energy Strategy Reviews, 58, 101654, (2025), https://doi.org/10.1016/j.esr.2025.101654.
3. Marzal, S., Salas, R., González-Medina, R., Garcerá, G., Figueres, E.: Current challenges and future trends in the field of communication architectures for microgrids. Renewable and Sustainable Energy Reviews, 82, Part 3, 3610-3622, (2018), https://doi.org/10.1016/j.rser.2017.10.101.
4. Basit, A., Tufail, M., Hong, K.-S., Rehan, M., Ahmed, I.: Event-triggered distributed exponential H∞ observers design for discrete-time nonlinear systems over wireless sensor networks. In: 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, pp. 1730-1735, (2022), https://doi.org/10.23919/ASCC56756.2022.9828291.
5. Ahmed, I., Rehan, M., Hong, K. -S., Basit, A.: Event-triggered leaderless robust consensus control of nonlinear multi-agents under disturbances. In: 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, pp. 1736-1741, (2022), https://doi.org/10.23919/ASCC56756.2022.9828087.
6. Marzal, S., Salas, R., Gonzalez-Medina, R., Garcera, G., Figueres, E.: Current challenges and future trends in the field of communication architectures for microgrids. Renewable and Sustainable Energy Reviews, 82, Part 3, 3610-3622, (2018), https://doi.org/10.1016/j.rser.2017.10.101.

7. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and research trends in microgrids cybersecurity. Applied Sciences, 11(16), 7363, (2021), https://doi.org/10.3390/app11167363.
8. Piedrahita, A.F.M.; Gaur, V.; Giraldo, J.; Cardenas, A.A.; Rueda, S.J. Leveraging software-defined networking for incident response in industrial control systems. IEEE Software, 35(1), 44-50, (2018), https://doi.org/10.1109/MS.2017.4541054.
9. Information security, cybersecurity and privacy protection — Information security management systems — Requirements, (Edition 3, 2022), https://www.iso.org/standard/27001.
10. Rouhani, S.H., Su, C.-L., Mobayen, S., Razmjooy, N., Elsisi, M.: Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. Energy, 309, 133081, (2024), https://doi.org/10.1016/j.energy.2024.133081.
11. Kang, B. et al.: Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, Luxembourg, pp. 1-8, (2015), https://doi.org/10.1109/ETFA.2015.7301457.
12. Rajkumar, V.S., Tealane, M., Stefanov, A., Presekal, A., Palensky, P.: Cyber attacks on power system automation and protection and impact analysis. In IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, pp. 247-254, (2020), https://doi.org/10.1109/ISGT-Europe47291.2020.9248840.
13. Tuyen, N.D., Quan, N.S., Linh, V.B., Van Tuyen, V., Fujita, G.: A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. IEEE Access, 10, 35846-35875, (2022), https://doi.org/10.1109/ACCESS.2022.3163551.
14. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., Ghadimi, N.: A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, Part A, 108975, (2023), https://doi.org/10.1016/j.epsr.2022.108975.
15. Hossain, E., Kabalci, E., Bayindir, R., Perez, R.: Microgrid testbeds around the world: State of art. Energy Conversion and Management, 86, 132-153, (2014), https://doi.org/10.1016/j.enconman.2014.05.012.
16. Wanik, M.Z.C., Krama, A., Jabbar, A.A., Sanfilippo, A., Satar, S.: Development of microgrid testbed for real desert environment testing and evaluation: project experience. In 22nd Wind and Solar Integration Workshop (WIW 2023), Copenhagen, Denmark, pp. 295-301, (2023), https://doi.org/10.1049/icp.2023.2751.
17. Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., Van der Vyver, C., Ahuja, R.: Intrusion detection and prevention systems: An updated review. Advances in Intelligent Systems and Computing, 1042, 685-696, (2020), https://doi.org/10.1007/978-981-32-9949-8_48.
18. Ustun, T.S., Hussain, S.M.S., Yavuz, L., Onen, A.: Artificial intelligence based intrusion detection system for IEC 61850 sampled values under symmetric and asymmetric faults. IEEE Access, 9, 56486-56495, (2021), https://doi.org/10.1109/Access.2021.3071141.
19. Mukherjee, D.: Detection of data-driven blind cyber-attacks on smart grid: A deep learning approach. Sustainable Cities and Society, 92, 104475, (2023), https://doi.org/10.1016/j.scs.2023.104475.