REDUCING THE VULNERABILITY IN MICROGRID POWER SYSTEMS

[1]Yusupov Ziyodulla, [2]Yaghoubi Elaheh, [3]Yaghoubi Elnaz, [4]Valisher Soyibjonov

[1,2,3] Department of Electrical-Electronics Engineering of Karabuk University, Karabuk, Türkiye

[4] Department of Electrical Machines, Tashkent State Technical University named after Islam Karimov

https://doi.org/10.5281/zenodo.7954885

Abstract. *One of the world's biggest obsessions is cyberattacks on electric power systems. The power system is a critical infrastructure that supplies electricity to homes, businesses, and industries. Any disruption to this system can seriously affect the economy and people's daily lives. Finding the system's vulnerability points may be the solution to preventing cyberattacks. There are numerous signs that a cyberattack has occurred. The study highlights the importance of finding vulnerability points in power systems to prevent cyberattacks and proposes a method based on network planning indicators to reduce the number of cyberattacks by implementing microgrids. At first, this paper uses the Newton-Raphson algorithm to analyse IEEE 33-bus network planning indicators to identify vulnerable points in the power system. Then, it applies microgrids to various system components to show that implementing microgrids can reduce the number of cyberattacks on the power system and increase resilience to cyber threats.*

Keywords*: cyberattack, Microgrid, distributed generation, power system, Newton Raphson*

1. Introduction

Globally, there is a lot of anxiety about cyber-attacks on the electrical infrastructure. Cyber-attacks on the power system can take various forms, such as Malware attacks, Denial-of-service (DoS) attacks, Phishing attacks, Man-in-the-middle (MitM) attacks, and Physical attacks [1]. These attacks can cause power outages, equipment damage, and even physical harm to people. Therefore, it is crucial to identify the vulnerable parts in a power system to ensure its secure and stable operation. The goal of vulnerability analysis is to identify the transmission lines vulnerable to small changes in their conductive qualities that could cause severe grid disturbances, including voltage decreases, or necessitate the shedding of load at demand nodes to resume practical operation [2]. Cyber-attacks can happen on transmission lines, generators, and transformers [3-8]. Hence, power flow analysis and configuration of power systems play a critical role in identifying potential cyber-attacks on electric power systems [9]. Power flow analysis is a computational method used to model and analyze the flow of electricity through the power system [10]. It provides information about the system's voltage, current, and power flows, which can be used to identify potential vulnerabilities. There are two types of modeling for vulnerability analysis problems, including DC power flow models and AC power flow models [2, 11]. The linearized DC power model's precision drops under strong disturbances, and the model may greatly overestimate both active and apparent power. As a result, while the simplicity and ease of computation of DC models are appealing, making decisions according to such linearized models may not be appropriate for analyzing power systems that are operating under abnormal conditions. Therefore, using the AC power flow is reasonable. There are many methods for AC power flow analysis, including backwards-forward [12], Gauss-Seidel [13], Newton Raphson [14] and so on. One of the popular methods for analyzing AC power flow is Newton Raphson method. The advantages of using the Newton-Raphson method for power flow analysis include its ability to handle radial and meshed networks and fast convergence rate [15]. Moreover, the configuration of a power system can affect the system's susceptibility to cyberattacks. Different power system configurations can have varying degrees of vulnerability to cyberattacks, depending on the type and placement of control systems, communication networks, and security measures [16]. Proper planning and design, as well as robust security measures, can help to mitigate these risks and ensure the reliability and resilience of the power system.

Additionally, the incorporation of microgrids (MGs) in electricity generation has increased due to their ability to provide a local energy supply and improve grid resilience. A microgrid is a small-scale power system that can operate independently or in connection with the main grid, using a combination of distributed energy resources such as solar panels, wind turbines, and energy storage systems [17]. Using microgrids in power systems can provide a valuable defense against cyberattacks while offering other benefits such as improved reliability, resiliency, and local energy supply. Microgrids can be designed with advanced control and communication systems that are more secure than those used in traditional grid infrastructure [18]. For example, microgrids can incorporate encryption, authentication, and other security measures to protect against cyber threats [19]. However, it is important to ensure that microgrids are designed and operated with robust cybersecurity measures to prevent potential vulnerabilities.

In this research, optimization models for power system microgrid vulnerability analysis are proposed. This model considers attacks including the failure of generators and transmission lines and is based on the AC power flow equations.

2. Methodology

Vulnerability points in a power grid can provide access points for cyber-attacks, and identifying these vulnerabilities is important for ensuring the security and reliability of the grid [20]. There are various indicators for detecting cyber-attacks. In general, stability analyses of power systems can be categorized as either static or dynamic. In this investigation, a network planning indicator is utilized as a form of static stability analysis to identify vulnerable points in the network. The network planning indicator, which considers the balance between energy production and consumption, can be useful for identifying potential points of failure in the power grid. The network planning indicator highlights that balancing production and energy consumption is necessary to avoid harm to the power system. Failure to achieve this balance can lead to network shutdown or collapse. The primary factors considered in the proposed strategy of study are generator outages and transmission line outages between buses. It means the power generation rate is not equal to the rate of power demand ($P_{\text{manufactured}} \neq P_{\text{requested}}$). In other words, from a mathematical point of view, power flow equations will not be solved or converged, as shown in Figures 1 and 2.

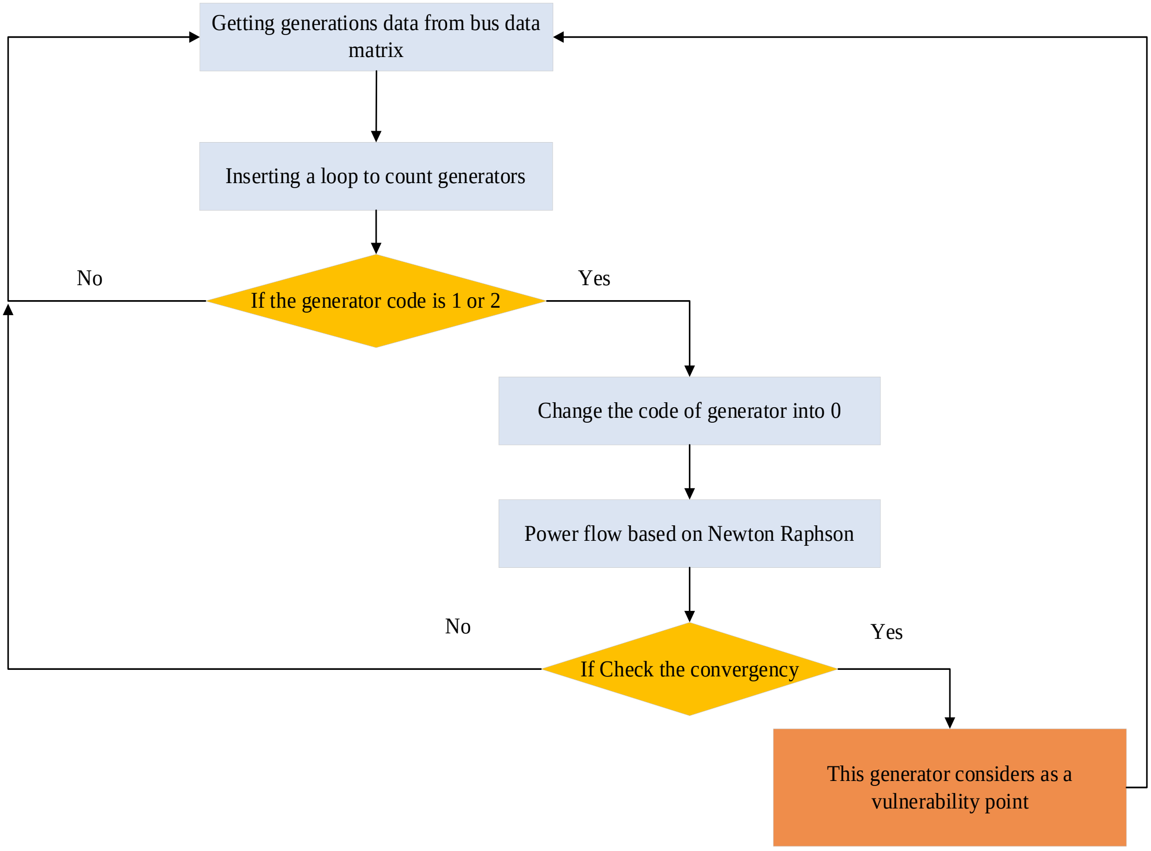
Getting generations data from bus data matrix
Inserting a loop to count generators
No
If the generator code is 1 or 2
Yes
Change the code of generator into 0
Power flow based on Newton Raphson
No
If Check the convergency
Yes
This generator considers as a vulnerability point

Figure 1. Algorithm for calculating the generation outage

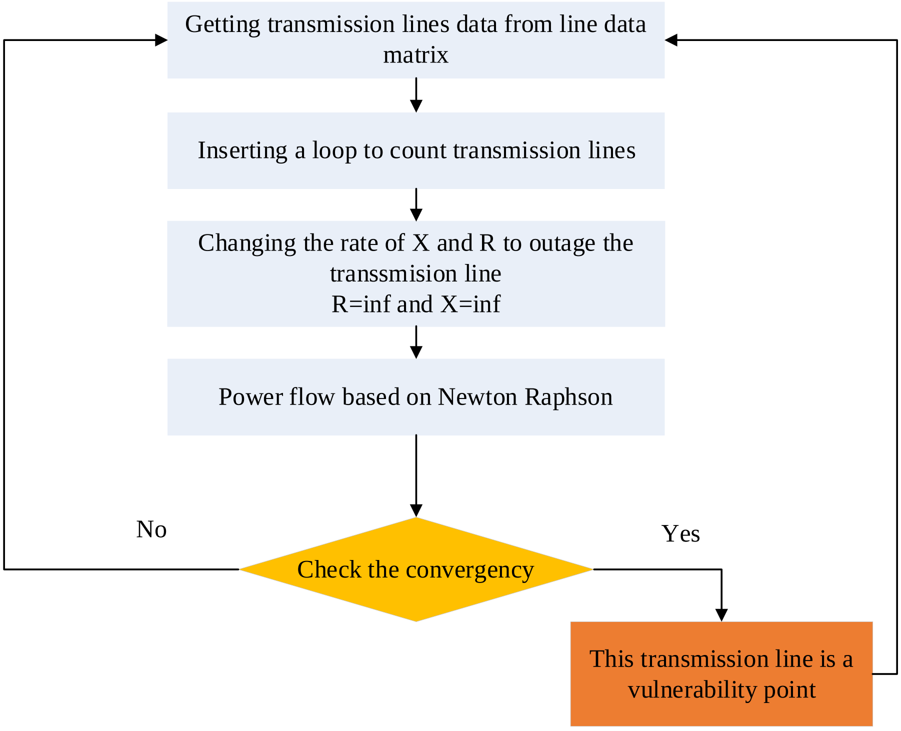
Getting transmission lines data from line data matrix
Inserting a loop to count transmission lines
Changing the rate of X and R to outage the transsmision line
R=inf and X=inf
Power flow based on Newton Raphson
No
Check the convergency
Yes
This transmission line is a vulnerability point

Figure 2. Algorithm for calculating the transmission line outage.

2.1 Power flow analyzing

For the power flow equation to converge, the power produced must match the amount consumed, as shown in equation 1.

$$P_{\text{manufactured}} = P_{\text{requested}} \tag{1}$$

To achieve this balance, we rely on the following equations.

$$P_i = \sum(V_i * V_j /* cos(\theta_i - \theta_j)) + V_i^2/X_i \tag{2}$$

$$Q_i = \sum(V_i * V_j /X_{ij} * sin(\theta_i - \theta_j)) - V_i^2/X_i \tag{3}$$

where:

P_i and Q_i are the active and reactive power injection at bus i , respectively

V_i and V_j – the magnitude of voltage in *i* and *j* buses, respectively

θ_i and θ_j – the voltage phase angles in bus *i* and *j*, respectively

X_i is the impedance of the line or branch at bus *i*

X_{ij} is the impedance of the line or branch between buses *i* and *j*, respectively

$cos(\theta_i - \theta_j)$ is the cosine of the phase angle difference between bus *i* and bus *j*

$sin(\theta_i - \theta_j)$ is the sine of the phase angle difference between bus *i* and bus *j*.

Equations (4) to (8) represent the foundational equations utilized in the Newton-Raphson method to iteratively solve for a system's unknown variables, such as power flow or voltage magnitude. This matrix can be used to model the behavior of power systems and identify potential vulnerabilities. A matrix of partial derivatives of the nonlinear equations with respect to the unidentified variables makes up the Jacobian matrix. It is calculated at each iteration of the method and is used to approximate the nonlinear equations by a set of linear equations as shown in equation (9) [15, 21].

$$f(x) = c \tag{4}$$

$$x^{(k+1)} = x^k + \Delta x^k \tag{5}$$

$$\Delta x^k = \frac{\Delta c^k}{\left(\frac{\partial f}{\partial x}\right)^k} \tag{6}$$

$$J = \left(\frac{\partial f}{\partial x}\right) \tag{7}$$

$$\Delta c^{(k+1)} = c - f(x^k) \tag{8}$$

$$J^k = \begin{bmatrix} \left(\frac{\partial f_1}{\partial x_1}\right)^k & \left(\frac{\partial f_1}{\partial x_2}\right)^k & \cdots & \left(\frac{\partial f_1}{\partial x_n}\right)^k \\ \left(\frac{\partial f_2}{\partial x_1}\right)^k & \left(\frac{\partial f_2}{\partial x_2}\right)^k & \cdots & \left(\frac{\partial f_2}{\partial x_n}\right)^k \\ \left(\frac{\partial f_3}{\partial x_1}\right)^k & \left(\frac{\partial f_3}{\partial x_2}\right)^k & \cdots & \left(\frac{\partial f_3}{\partial x_n}\right)^k \\ \vdots & \vdots & \vdots & \vdots \\ \left(\frac{\partial f_n}{\partial x_1}\right)^k & \left(\frac{\partial f_n}{\partial x_2}\right)^k & \cdots & \left(\frac{\partial f_n}{\partial x_n}\right)^k \end{bmatrix} \tag{9}$$

Since the equations converge as much as possible in Newton Raphson's method, the maximum iteration is one of the factors that affects the Jacobian matrix to the power system's vulnerability point. The maximum iteration in this study is 20.

2.2. Microgrids

Microgrids can reduce power system vulnerability by reducing reliance on centralized power generation and transmission infrastructure. Microgrids can help to prevent cascading failures and blackouts that can occur when large portions of the power grid are affected [22]. Distributed energy resources (DERs) are a critical component of microgrids, providing localized power sources that can operate independently or in conjunction with the larger power grid. [23]. Hence, in this study, three microgrids are considered in different parts of IEEE 33-buses including PV panels, wind turbines, diesel generators, microturbines as shown in Figure 3.

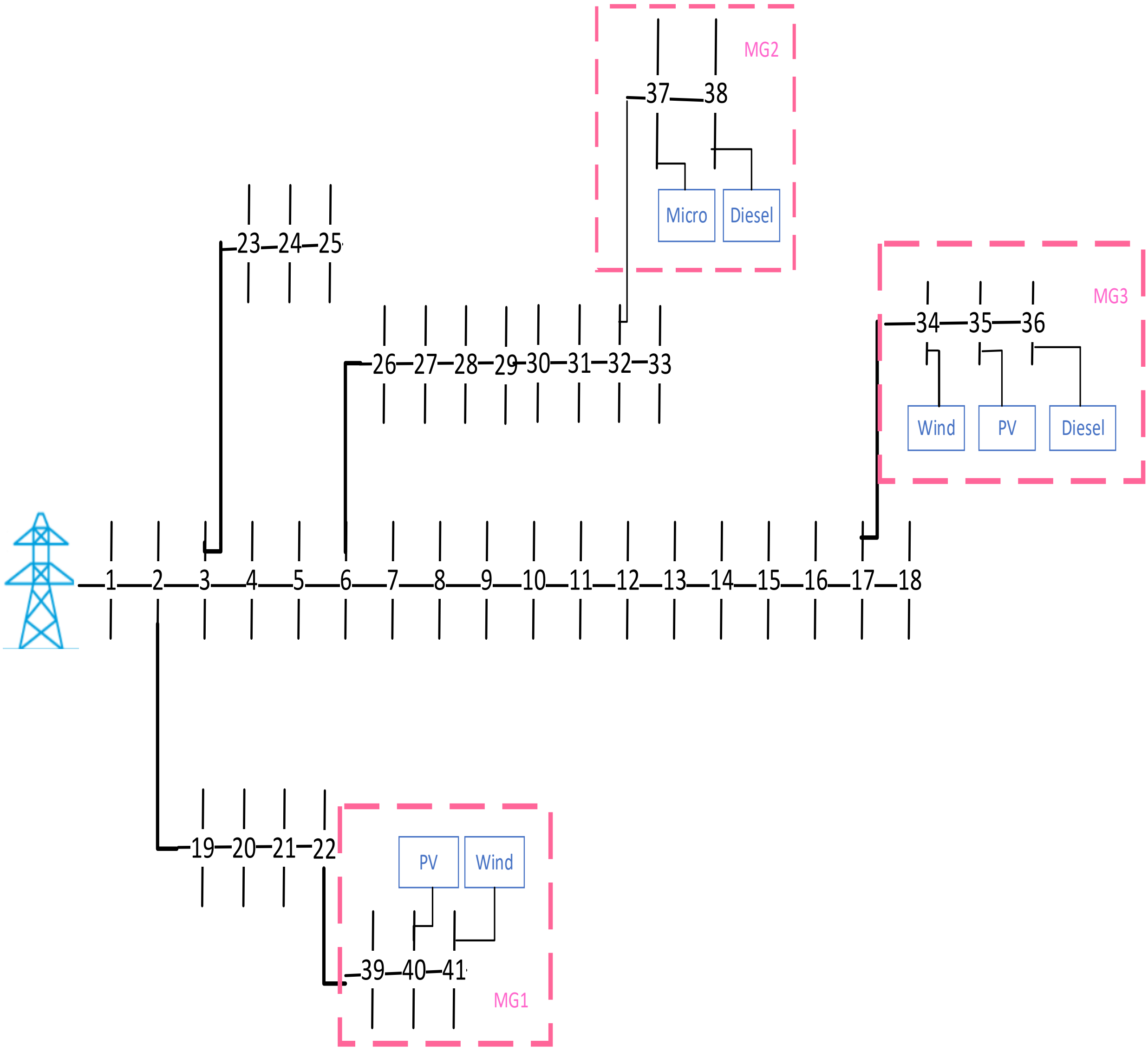

Figure 3. Three different decentralized microgrids in IEEE33 bus

2.2.1. Modeling of Distributed Generation

To perform an accurate analysis, it is essential to calculate the rate of power generation for each DG involved in the system. The power output of photovoltaic arrays is determined by the temperature of the cells and the intensity of the solar radiation at the maximum power point. The following equation can express this relationship:

$$P_{PV}(t) = \left[P_{PV,STC} \times \frac{G_T(t)}{1000} \times [1 - \gamma(T_j - 25)]\right] \times N_{PVs} \times N_{PVp} \quad (10)$$

The equation (10) includes the following variables:

P_{PV}: Generator output power at the maximum power point (kW)

$P_{PV,STC}$: Nominal PV power at the maximum power point and standard conditions

G_T: Radiation amount in standard conditions; it is considered 1000(W/m2).

γ: Temperature coefficient

T_j: The temperature of the solar cells; is considered 25°C.

N_{PVs}: Number of series modules; it is considered 75.

N_{PVp}: Number of parallel modules; is considered 1.

The power output of wind turbines depends on the wind speed, which can fluctuate on a range of timescales from instantaneous to seasonal. The following equation is applied to simulate the real power generated by the wind turbine:

$$P_{wt}(\nu) = \begin{cases} 0 & if \nu < V_{ci} \\ P_R(A + B\nu + C\nu^2) & if\ V_{ci} < \nu < V_r \\ P_R & if\ V_r < \nu < V_{co} \\ 0 & if\ V_{co} < \nu \end{cases} \tag{11}$$

V_{ci}: Lower cutoff speed; it is considered 8(m/s)
V_r: Nominal speed of the wind turbine; it is considered 13(m/s)
V_{co}: Upper cutoff speed; it is considered 14(m/s)
P_R: Nominal power of the wind turbine; it is considered 200(KW)
A, B, and C: Coefficients related to the wind turbine; are 0.2, 0.02, and 0.003, respectively. These coefficients depend on the wind turbine's specific design and operating conditions and are typically determined through testing or simulation.
100 kW are assumed for other DGs, including diesels, microturbine.

3. Result and discussion

The outage rates for generations and transmission lines are calculated in the IEEE 33-bus system without microgrids to compare better. Since bus 1 is the main generation in the IEEE 33-bus, based on the presented contingency analysis, if the generation outage happens, all the power systems will be gone. First, the outage rates for generations and transmission lines are calculated in the IEEE 33-bus system without microgrids to compare better. Since bus 1 is the main generation in the IEEE 33-bus, based on the presented contingency analysis, if the generation outage happens, all the power systems will be gone. Also, the number of transmission line outages in this condition is shown in Table 1. Figure 4 depicts the vulnerability points of this condition. According to the results, 26 transmission lines outages and one generation outage occurred in this system.

Table 1.

The contingency of Line outage in IEEE 33-bus without MGs

Sending node	Receiving node	Sending node	Receiving node
1	2	2	19
2	3	19	20
3	4	3	23
4	5	23	24
5	6	6	26
6	7	26	27
7	8	27	28
8	9	28	29
9	10	29	30
10	11	30	31
11	12	31	32
12	13		
13	14		
14	15		
15	16		

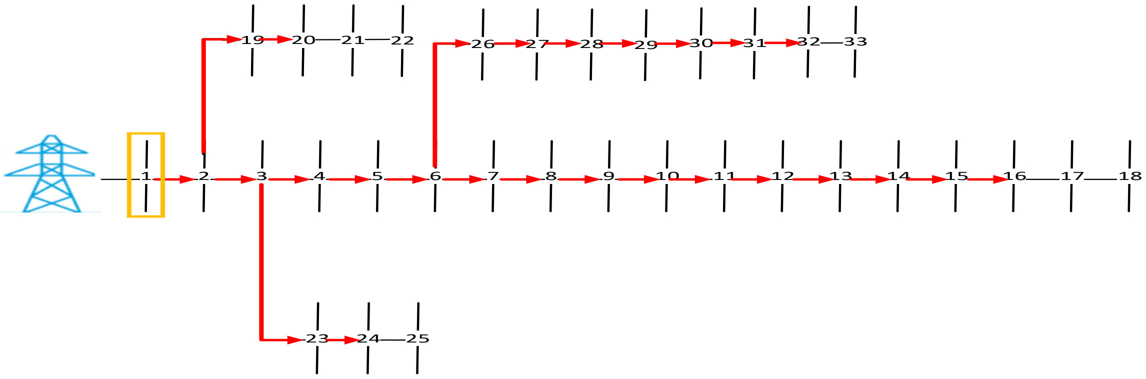

Figure 4. The vulnerability points of IEEE 33-bus without MGs

In the subsequent step, microgrids are incorporated into the system, and the outage rates of generators and transmission lines are computed. Initially, we assume that all distributed generations (DGs) function as PV buses and do not consider any voltage/frequency (VF) control buses for the microgrids in island mode. In this approach, the number of transmission line outages is 11 (Table 2). Moreover, the outage of bus 1, as a primary generator, substantially impacts the system. Figure 5 is presented to clarify this situation.

Table 2.

The contingency of **l**ine outage in IEEE 33-bus with MGs

Sending node	**Receiving node**
1	2
4	5
8	9
19	20
21	22
3	23
23	24
6	26
27	28
28	29
31	32

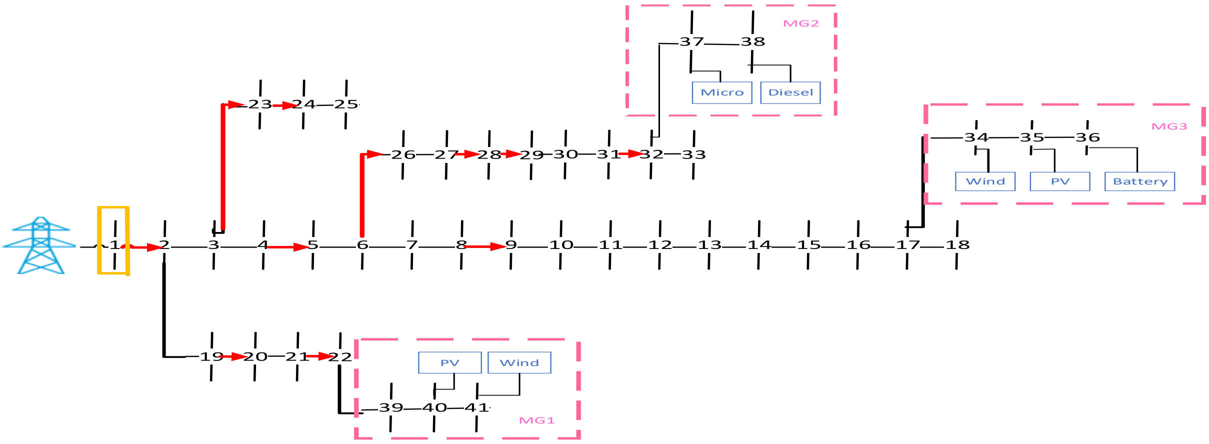

Figure 5. The vulnerability points of IEEE 33-bus with MGs when DGs in PV Bus mode

Assigning one of the DGs in each microgrid as a VF bus is a critical step in controlling the frequency and voltage of the microgrids while operating in island mode. In our study, we designate the DGs in 41, 38, and 35 as VF buses for their microgrids and then perform the system calculations. This approach reduces transmission line outages, as the number decreases to 2, as shown in Table 3. While this strategy considering VF buses for increased control in island mode and outage control of generators can improve the reliability of a power grid, it is critical to emphasize that the slack bus (bus 1) still poses a significant vulnerability to the system. The slack bus sets the system's voltage magnitude and phase angle reference. Any disturbances or outages at this point can ripple throughout the system, potentially causing instability and blackouts. Figure 6 provides a visual representation of this strategy.

Table 3.

The contingency of Line outage in IEEE 33-bus with MGs when one of DGs in VF Bus mode

Sending node	Receiving node
3	23
23	24

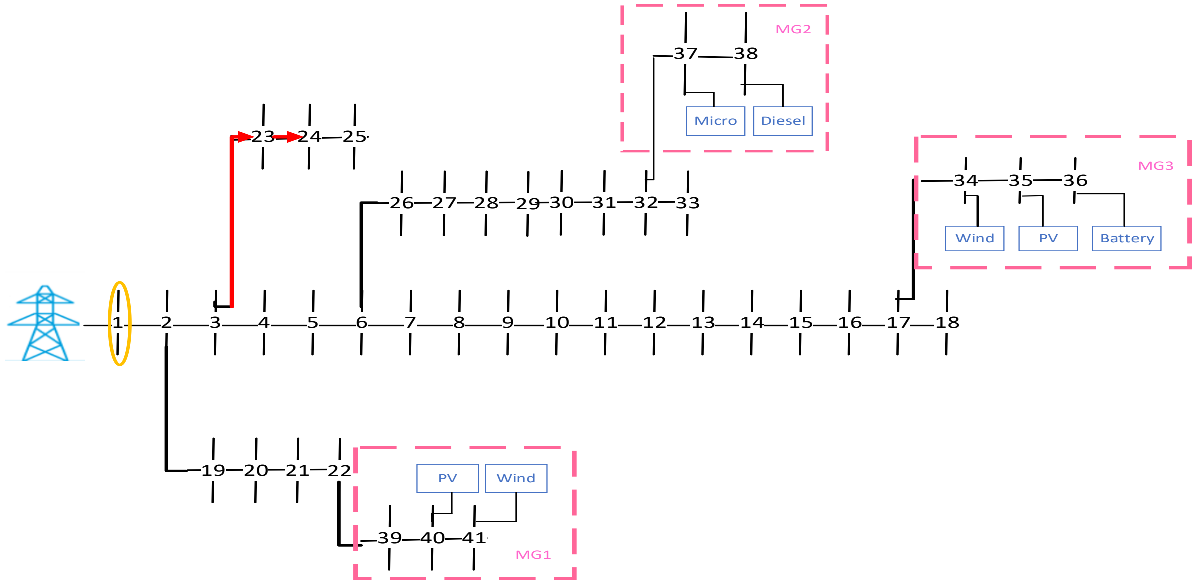

Figure 6. The vulnerability points of IEEE 33-bus with MGs while one of DGs in VF bus mode

4. Conclusion

This study recommends a method that utilizes network planning indicators as a static index to identify vulnerable points in the power system. Specifically, the Newton-Raphson method analyses IEEE 33-bus network planning indicators to identify these points.

To decrease the frequency of cyberattacks on the electrical system and improve resilience to cyberthreats, the paper investigates the efficacy of integrating microgrids in various system components. Introducing microgrids makes the system more decentralized, making it more difficult for attackers to target specific power system components. To demonstrate the effectiveness of microgrids in reducing power system vulnerability to cyber-attacks, DGs contributed to the microgrids using both PV and VF bus modes. The analysis of the results indicated that adding DGs in PV bus mode reduced the number of transmission line outages. While for each MG considering one DG in VF bus mode has a higher efficiency in decreasing the outages of transmission lines. Although incorporating VF buses to improve control in island mode and generator outage management can enhance power system reliability; it is crucial to recognize that the slack bus (bus 1) remains a vulnerable point for the system. As the slack bus sets the voltage magnitude and phase angle reference for the entire system, any disruptions or outages at this point can trigger instability and even lead to blackouts throughout the system. This finding highlights the potential for microgrids to enhance power system resilience and reduce the impact of cyber-attacks by increasing the control and stability of the system. By implementing appropriate control strategies, such as incorporating DGs in VF and PV bus modes, power system operators can enhance system security and minimize the impact of cyber-attacks.

REFERENCES

1. Ocaka, D. O. Briain, S. Davy, and K. Barrett, “Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review,” Multidiscip. Perspect. Cybersecurity Res. Pract. Educ., p. 35, 2022.
2. T. Kim, S. J. Wright, D. Bienstock, and S. Harnett, “Analyzing vulnerability of power systems with continuous optimization formulations,” IEEE Trans. Netw. Sci. Eng., vol. 3, no. 3, pp. 132–146, 2016.
3. J. Salmeron, K. Wood, and R. Baldick, “Analysis of electric grid security under terrorist threat,” IEEE Trans. power Syst., vol. 19, no. 2, pp. 905–912, 2004.
4. L. Motto, J. M. Arroyo, and F. D. Galiana, “A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat,” IEEE Trans. Power Syst., vol. 20, no. 3, pp. 1357–1365, 2005.
5. Z. X. Huang, P. L. So, A. M. Y. M. Ghias, and L. H. Koh, “Analysis of Cyber-Physical Attack in Transmission Systems,” 2021 IEEE 6th Int. Conf. Comput. Commun. Autom. ICCCA 2021, no. 1, pp. 720–724, 2021, doi: 10.1109/ICCCA52192.2021.9666239.
6. J. Salmeron, K. Wood, and R. Baldick, “Worst-case interdiction analysis of large-scale electric power grids,” IEEE Trans. power Syst., vol. 24, no. 1, pp. 96–104, 2009.
7. V. Donde, V. López, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, “Severe multiple contingency screening in electric power systems,” IEEE Trans. Power Syst., vol. 23, no. 2, pp. 406–417, 2008.
8. J. M. Arroyo, “Bilevel programming applied to power system vulnerability analysis under multiple contingencies,” IET Gener. Transm. Distrib., vol. 4, no. 2, pp. 178–190, 2010.
9. K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, “Power flow cyber attacks and perturbation-based defense,” in 2012 IEEE third international conference on smart grid communications (SmartGridComm), 2012, pp. 342–347.
10. P. S. Kundur and O. P. Malik, Power system stability and control. McGraw-Hill Education, 2022.
11. Coffrin, P. Van Hentenryck, and R. Bent, “Accurate load and generation scheduling for linearized DC models with contingencies,” in 2012 IEEE Power and Energy Society General Meeting, 2012, pp. 1–8.
12. J. A. M. Rupa and S. Ganesh, “Power flow analysis for radial distribution system using backward/forward sweep method,” Int. J. Electr. Comput. Electron. Commun. Eng., vol. 8, no. 10, pp. 1540–1544, 2014.
13. M. Eltamaly and A. N. A. Elghaffar, “Load flow analysis by gauss-seidel method; a survey,” Int J Mech Electr Comput Technol (IJMEC), PISSN, pp. 2411–6173, 2017.

14. W. F. Tinney and C. E. Hart, “Power flow solution by Newton’s method,” IEEE Trans. Power Appar. Syst., no. 11, pp. 1449–1460, 1967.
15. S. Akram and Q. U. Ann, “Newton raphson method,” Int. J. Sci. Eng. Res., vol. 6, no. 7, pp. 1748–1752, 2015.
16. U. Case, “Analysis of the cyber attack on the Ukrainian power grid,” Electr. Inf. Shar. Anal. Cent., vol. 388, pp. 1–29, 2016.
17. M. Elweddad, M.T. Guneser, Z. Yusupov, “Energy management and optimization of microgrid system using particle swarm optimization algorithm“, AIP Conference Proceedings 2686, 2022.
18. Issa and Z. Yusupov, "Development of a mas based distributed intelligent control and fault control strategy for microgrid", Polyteknik Dergisi, vol. 24, no. 1, pp. 161-173, 2021.
19. Mohan, G. Brainard, H. Khurana, and S. Fischer, “A cyber security architecture for microgrid deployments,” in Critical Infrastructure Protection IX: 9th IFIP 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, 2015, Revised Selected Papers 9, 2015, pp. 245–259.
20. U. Shahzad, “Vulnerability assessment in power systems: a review,” J. Electr. Eng. Electron. Control Comput. Sci., vol. 7, no. 4, pp. 17–24, 2021.
21. V. V. Mehtre and P. T. Jahngir, “Analysis of Newton Raphson Method,” 2019.
22. O. Egbue, D. Naidu, and P. Peterson, “The role of microgrids in enhancing macrogrid resilience,” 2016 Int. Conf. Smart Grid Clean Energy Technol. ICSGCE 2016, pp. 125–129, 2017, doi: 10.1109/ICSGCE.2016.7876038.
23. K. Twaisan and N. Bar, “Integrated Distributed Energy Resources (DER) and Microgrids: Modeling and Optimization of DERs,” Electron., vol. 11, no. 18, 2022, doi: 10.3390/electronics11182816.