Central Power Research Institute

Vol. 20(1)/17-25, June 2024
ISSN (Print) : 0973-0338
DOI : 10.33686/pwj.v20i1.1163

Power Research

Cyber Security Analysis of a Power Distribution System Using Vulnerability Assessment and Penetration Testing Tools

R. K. Nidhi[1*], M. Pradish[2] and M. N. Suneetha[1]

[1]University Visvesvaraya College of Engineering, Bengaluru - 560001, Karnataka, India; nidhi.arkay98@gmail.com

[2]Smart Grid Research Laboratory, Central Power Research Institute, Bengaluru - 560080, Karnataka, India

Abstract

The cyber security analysis on a power distribution system, utilizing Vulnerability Assessment and Penetration Testing (VAPT) tools, emphasizes the critical need to evaluate and mitigate cyber security risks for the reliability, integrity, and resilience of these systems. The growing threat landscape faced by interconnected and digitally reliant power distribution systems is discussed, highlighting the severe consequences of potential cyber-attacks. VAPT tools offer an effective approach to identifying vulnerabilities and assessing the security posture. Vulnerability assessment targets weaknesses in software, hardware, and network infrastructure, while penetration testing actively exploits vulnerabilities to gauge system resilience. The analysis aims to identify potential vulnerabilities, evaluate the system's response to attacks, and provide recommendations for improving overall security. Proactively addressing vulnerabilities and enhancing cyber security defences ensures uninterrupted electricity delivery, safeguards critical infrastructure, and protects against cyber threats in an interconnected world.

Keywords: Cyber Security, Intelligent Electronic Devices, Penetration Testing, Power Distribution System, Vulnerability Assessment

1. Introduction

In our increasingly interconnected world, critical infrastructure systems like power distribution networks have become prime targets for cyberattacks. A successful breach of these systems could lead to widespread power outages, disrupt essential services, and even pose a threat to national security. To address these growing concerns, it is imperative to proactively evaluate and enhance the cyber security of power distribution systems. This paper focuses on assessing and fortifying the security of a power distribution network by employing comprehensive vulnerability assessment and penetration testing techniques.

Power distribution systems are the backbone of modern societies, ensuring the reliable supply of electricity to homes, businesses, and critical infrastructure. However, the increased reliance on digital technologies, automation, and networked communication has made these systems vulnerable to cyber threats. The potential risks range from unauthorized access to the power grid, data breaches, and physical damage to equipment, ultimately jeopardizing the availability and integrity of the electricity supply.

The traditional power systems have undergone immense technological reforms that have transformed the conventional power grids into large, advanced, interconnected and complex cyber-physical systems.

These are equipped with modern pieces of equipment like distributed generators, digital relays, Phasor Measurement Units (PMUs)[1], and other Intelligent Electronic Devices (IEDs).

These integrate diverse critical control components, and a single component failure can cause severe impact on the power grid, ranging from medium scale to large

**Author for correspondence*

© Power Research

scale blackout and significantly damaging the assets and power equipment such as transmission lines, transformers, generators, protective relays, etc. and cause a threat to human life.

The sensors-based technologies and highly integrated nature of cyber-physical control systems having various critical infrastructures are targets of various synthetic attacks. These attacks are expected to increase soon, and their prevention, mitigation, and detailed vulnerability assessment are essential to improve the power grid's resiliency against such possible attacks.

The primary objectives of this project are as follows:

Vulnerability assessment: Identify vulnerabilities by conducting a thorough vulnerability assessment of the power distribution system to pinpoint potential weaknesses in its cybersecurity posture. This step involves analyzing the network architecture, hardware, and software components for known vulnerabilities.

Penetration testing: Performing controlled penetration testing to simulate cyberattacks and evaluate the system's resilience against real-world threats. This includes testing the system's ability to detect and respond to intrusions[2].

Risk assessment: Evaluate the impact and likelihood of potential cyber threats on the power distribution network, helping prioritize security measures based on risk severity.

2. Cyber Security in Power System

The increasing digitization and interconnection of power systems make cybersecurity critically important. Power systems heavily rely on information technology and Operational Technology (OT) for optimal performance and reliable energy delivery. OT systems, crucial in managing power generation and distribution, are classified as critical infrastructure, with any compromise posing severe consequences, including disruptions in power supply and potential threats to national security. Cyberattacks on OT systems can lead to malfunctions, equipment failures, and power outages, impacting industries, businesses, and individuals.

Protecting sensitive data in OT systems is essential to prevent unauthorized access and manipulation. Financially, cyberattacks on power systems incur substantial costs for recovery, equipment repair, and economic losses during downtime. Given the close link between the power sector and national security, successful cyberattacks can be used as tools for coercion or disruption, posing a threat to a nation's overall security and stability. The multifaceted importance of cybersecurity in power systems encompasses safety, reliability, financial stability, national security, and public trust, requiring ongoing adaptation to address emerging threats and vulnerabilities as technology evolves[3]. Figure 1 shows the types of cyber attacks.

The power sector is increasingly vulnerable to various cyber threats that can lead to disruptions in power generation, transmission, and distribution. The types of cyber attacks targeting the power sector include Advanced Persistent Threats (APTs), ransomware attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, insider threats, phishing and social engineering attacks, malware attacks, supply chain attacks, zero-day exploits, physical attacks facilitated by cyber means, Man-in-the-Middle (MitM) attacks, USB-based attacks, and exploitation of Human-Computer Interface (HCI) vulnerabilities.



Figure 1. Types and impacts of cyber-attacks on power systems.

The power sector is increasingly vulnerable to various cyber threats that can lead to disruptions in power generation, transmission, and distribution. The types of cyber attacks targeting the power sector include APTs, ransomware attacks, DoS and DDoS attacks, insider threats, phishing and social engineering attacks, malware attacks, supply chain attacks, zero-day exploits, physical attacks facilitated by cyber means, MitM attacks, USB-based attacks, and exploitation of HCI vulnerabilities. Cyber attacks on OT systems in the power sector can have severe physical consequences, manipulating control systems to damage power generation or distribution equipment, and posing a significant threat to the reliability and safety of the

entire power infrastructure. This has public, economic, and data security implications. Power outages can disrupt essential public services, healthcare, and communication, highlighting the importance of securing OT systems to prevent malicious actors from causing public inconvenience.

Economically, any disruption in the power sector due to a cyber-attack can result in significant losses, including downtime costs, equipment damage, and emergency response expenses. OT systems in the power sector handle sensitive data, making data security crucial to prevent unauthorized access, manipulation, or theft.

To protect against these threats, the power sector requires a comprehensive cybersecurity strategy, involving regular vulnerability assessments, penetration testing, employee training, and robust security controls[3]. Collaboration with cybersecurity experts, information-sharing initiatives, and adherence to industry standards and regulations are essential for safeguarding critical infrastructure in the power sector. A well-defined and periodically updated cybersecurity policy is crucial for staying abreast of global best practices and statutory requirements.

3. Vulnerable Equipment of Power Systems

OT systems in the power sector, comprising interconnected equipment vital for electrical power generation, transmission, and distribution, are susceptible to significant risks due to vulnerabilities. Notably, processing and communicable-capable equipment, as well as control and monitoring software, pose threats. Examples of vulnerable equipment include Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), Human-Machine Interfaces (HMIs), communication networks, smart grid components, power plant control systems, Energy Management Systems (EMS), historian systems, electronic protection relays, and control servers and workstations.

Exploiting vulnerabilities in these components can lead to unauthorized access, data manipulation, disruptions, and potential damage to the power network. Regular vulnerability assessments, penetration testing, and adherence to security best practices are crucial for identifying and addressing vulnerabilities in OT systems within the power sector. Given the dynamic risk landscape, staying informed about the latest threats and complying with industry cybersecurity standards and regulations are essential for maintaining the security and reliability of power infrastructure. The importance of having an updated cybersecurity policy followed diligently at all organizational levels, is emphasized for enhanced protection.

4. Vulnerability Assessment

Vulnerability assessment is a critical aspect of cybersecurity, involving the identification and evaluation of weaknesses in computer systems, networks, applications, and both Information Technology (IT) and OT infrastructure[4]. The primary goal is to proactively discover and mitigate potential security risks before they can be exploited by malicious actors. Various tools automate the scanning, analysis, and reporting process, aiding organizations in maintaining a robust security posture. The assessments utilize automated tools to scan networks, systems, and applications, identifying known software flaws, misconfigurations, and security weaknesses.

Data collected during scanning is then analyzed to assess the severity of vulnerabilities, with risk scores assigned based on factors like exploitability and potential impact[5]. The generated reports provide actionable insights for remediation, aiding organizations in prioritizing and addressing vulnerabilities based on their impact on security. Figure 2 shows the testing setup for RTU.

Vulnerability assessments contribute to public safety by safeguarding assets and preventing potential risks posed by cyber incidents. As operational technology systems in the power sector become targets for evolving cyber threats, vulnerability assessments aid organizations in staying ahead of potential risks, implementing protective measures and developing resilience strategies[6]. These assessments also ensure compliance with regulatory guidelines and standards, as many regulatory bodies mandate cybersecurity practices for critical infrastructure.



Figure 2. Testing setup for vulnerability assessment of an RTU.

A thorough vulnerability assessment of the protection relay, remote terminal unit, smart meters, merging unit, feeder protection system, line distance protection system, and overcurrent relay was performed using the Tenable Nessus tool[a]. Few critical, medium and low severity vulnerabilities were discovered in all the devices which are further discussed in the results section of this paper. Figure 3 shows the smart meters testing setup.



Figure 3. Smart meter test setup.

To address these vulnerabilities, it is crucial to implement robust cyber security measures, including secure communication protocols, access controls, regular software updates and patch management, intrusion detection systems, and continuous monitoring. Additionally, industry standards and best practices, such as those outlined by organizations like the International Electrotechnical Commission (IEC) and The Indian Computer Emergency Response Team (CERT-In), should be followed to enhance the overall cyber security posture of power systems.

5. Penetration Testing

Penetration testing is a crucial cybersecurity methodology for assessing and strengthening the resilience of power distribution system equipment against potential cyber threats. It involves simulated attacks and comprehensive assessments to identify vulnerabilities, evaluate security controls, and ensure the robustness of defence mechanisms. The primary objective in power distribution cyber security assessment is to assess the security posture of equipment and control systems by simulating real-world cyber threats. This systematic evaluation aims to uncover weaknesses in network architecture, communication protocols, embedded systems, and other components.

In the context of OT, penetration testing is paramount in today's interconnected industrial landscape. OT, encompassing hardware and software for monitoring and controlling physical processes, is susceptible to cyber threats. Performing live penetration tests on vulnerable OT equipment can be challenging due to potential service interruptions, so tests are often conducted offline, during maintenance, or in a sandbox environment.

The importance of penetration testing for OT equipment lies in, identifying vulnerabilities, security validation, mitigating risks, ensuring resilience, compliance and regulations, preventing unplanned downtime, protecting intellectual property, incident response readiness, supply chain security, increasing cybersecurity awareness and adapting to evolving threats.

The penetration testing was performed on some of the operational technology equipment such as the remote terminal unit, relay and smart meter using the Metasploit tool[b]. Considering the previous vulnerability assessment findings, penetration testing was carried out and the following observations were recorded,

Remote terminal unit: It was observed that the tool was able to identify the name and make of the RTU but was unable to exploit the system even after several login attempts as it was password protected.

Smart meters: The penetration testing of smart meters was carried out and the results show that the devices were unexploitable as there is a password-protected software present which denied the exploitation.

Relay: The penetration testing of the relay was carried out and the results show that the device was not suitable for any type of exploit.

Penetration testing is a proactive and strategic approach to securing operational technology equipment, safeguarding critical industrial processes, and ensuring the continuity of essential services in an increasingly interconnected and digitized industrial landscape.

6. Power Distribution System

A power distribution system is a vital element of electrical infrastructure, ensuring efficient electricity supply from generation sources to end-users. Modern systems, equipped with a substation automation system, employ advanced technologies for enhanced control, monitoring, and automation within substations. SAS includes Intelligent Electronic Devices (IEDs), communication networks, and control applications, optimizing substation operations and improving reliability.

The system enables quick fault detection and response, reducing downtime, streamlining operations, and providing

insights into system performance. While SAS enhances the efficiency and adaptability of power grids, robust cybersecurity measures are crucial to safeguard against potential cyber threats.

Simulated scenarios in MATLAB Simulink[c] illustrate the consequences of cyber-attacks on a power distribution station, including current transformer ratio manipulation, circuit breaker malfunctions, power theft, and fault detection issues[7]. The work underscores the importance of cybersecurity in maintaining the reliability and intelligence of modern power distribution systems.

The simulated power distribution system consists of a 25KV line, 4 transformers, 7 feeder buses and 4 areas to which the power is being supplied. Area 1 consists of load 1, load 7 and load 8 with circuit breakers CB7 and CB8. In area 2, a single load with a three-phase fault is present. The areas 3 and 4 consist of two loads and two circuit breakers each. There are a few circuit breakers that are present between the areas and the transmission line to isolate the part where the fault has occurred and maintain balance in the network. When the fault F2 is acting in area 3 the CB8 opens and with F3, CB9 opens, in case both the faults are occurring at the same instance the CB5 opens and isolates area 3. The same operation is seen in Area 4 as well. Figure 4 shows the simulated power distribution system.

Three scenarios are considered for the simulation which include fault distance detection, power theft and current transformer manipulation.

7. Fault Theft Scenario

In the fault detection scenario, the travelling wave method is utilized. It is a technique used in power systems to identify and locate faults in transmission lines. This method relies on the analysis of electromagnetic waves that propagate along the power transmission lines when a fault occurs.

When a fault, such as a short circuit, occurs on a power line, it generates travelling waves that propagate along the transmission line in both directions from the fault location[8]. These waves carry information about the fault, including its location and type. With the analysis of the time of travelling waves to reach the endpoints of the lines, the exact location of the fault is calculated. Figure 6 shows the subsystem of the Simulink model with the fault detection model.

8. Power Theft Scenario

The power distribution system simulation was developed to study the power theft scenario where unregistered loads get connected during the time of fault and draw power from the grid. In this scenario, it is considered loads L1, L2, L3, L4, L5, L6 as registered loads and loads L7 and L8 as unregistered loads. From 0 to 1 seconds, the system operates with normal operating conditions. The fault F1 is activated at time t = 1 seconds and ends at 1.2 seconds. Simultaneously, the circuit breakers CB12 and CB13 close at t = 1.2 seconds and the unregistered loads L7 and L8 are connected to the grid and draw excess power.

The voltage and current flowing through the lines are considered and the active and reactive power is measured.

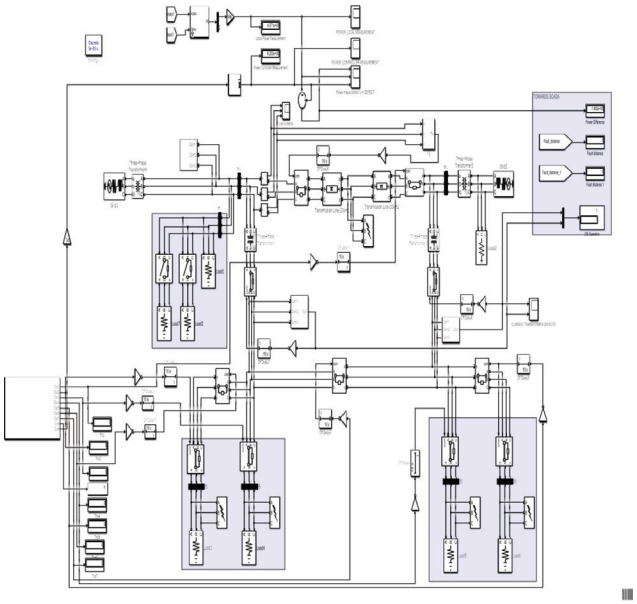


Figure 4. Primary distribution station Simulink model.

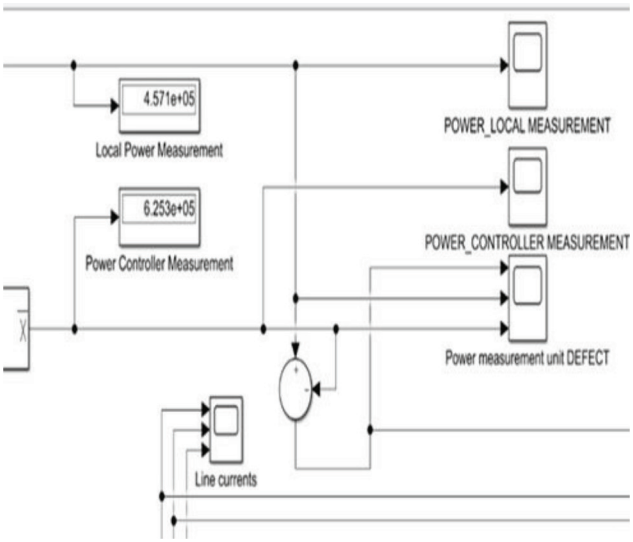


Figure 5. Difference in power measurement.

A fault environment is simulated with delays to the circuit breakers and an error in the reading is recorded in the local power measurement block. From Figure 5 it is observed that the local power measurement blocks responsible for displaying the data of power drawn by the registered loads recorded a value of 457.1KW. The controller power measurement records the actual power being drawn from the grid and recorded a value of 625.3KW. A difference of 168.2 KW is observed. This scenario represents a case of power theft and error in the measurement of power.

9. Current Transformer Manipulation

The current transformers are typically used to measure the amount of current passing through a power distribution station with the use of their current transformer ratios. In this scenario, we have connected a gain to the current transformers which acts after t = 4 seconds to t = 8 seconds. The gain leads to increasing the current measurement value more than the threshold and the circuit breakers treat it as overcurrent and open to isolate the areas. The sudden opening of circuit breakers or improper operation of circuit breakers could lead to a sudden fall or surge in the currents and voltages in the network. This scenario is known as the current transformer ratio manipulation.

10. Results and Discussions

The results of vulnerability assessments in power distribution equipment provide valuable insights into the potential risks and weaknesses within the infrastructure. These assessments encompass a comprehensive evaluation of the security posture, resilience, and reliability of power distribution systems. The assessment results guide the development of targeted risk mitigation strategies, allowing for the implementation of security measures, resilience enhancements, and the optimization of resource allocation.

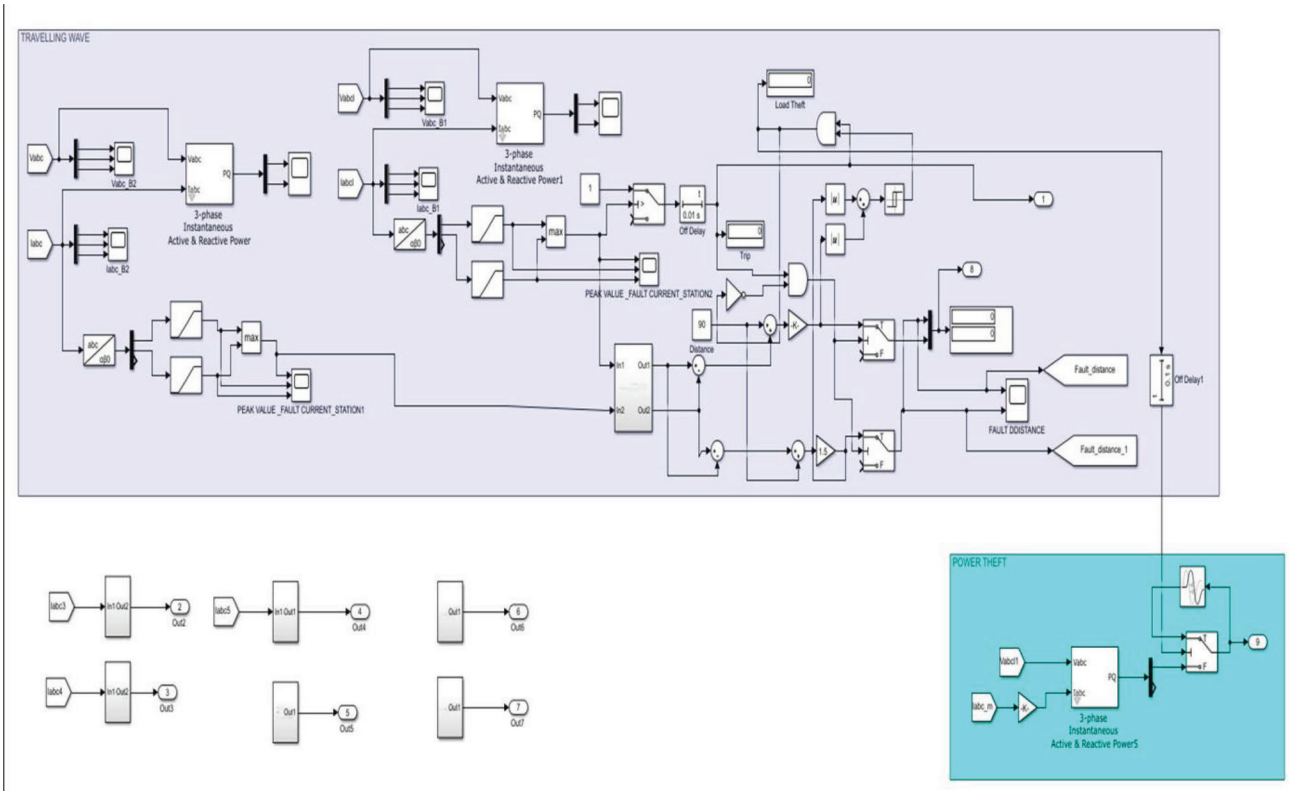


Figure 6. Subsystem of Simulink model with fault detection model.

The findings aid in emergency preparedness by informing response plans to address identified vulnerabilities. Overall, these assessments play a crucial role in maintaining a secure, reliable, and resilient power infrastructure, ensuring public

safety and compliance with industry standards. Regular assessments contribute to continuous improvement and adaptation to evolving threats in the dynamic landscape of power distribution. Table 1 displays vulnerability assessment results, associated risks, and possible solutions.

Penetration testing on power distribution equipment provided a thorough cybersecurity resilience examination, simulating real-world cyberattacks to uncover vulnerabilities and evaluate existing security measures. The tests focused on relay, RTU, and smart meters, revealing that all three were secure, with the RTU being password-protected and resistant to exploitation.

The results contribute significantly to enhancing overall cybersecurity strategy, ensuring the integrity and reliability of critical infrastructure amid evolving cyber threats. Regular penetration testing is vital for maintaining a proactive and adaptive cybersecurity approach, aligning with industry best practices and compliance requirements in the dynamic landscape of power distribution systems. Figure 7 shows the results of the penetration testing on the relay.

The simulation of a power distribution system was carried out with possible cyber-attack scenarios and the results are as follows.

The fault distance detection was done using the travelling wave method which is based on transient wave propagation created during the time of disturbances. It was observed that the fault occurred at 45 km on the transmission line in buses B1 and B2 between time t = 1s to t = 1.2s. Figure 8 shows the graphical representation of the fault distance located.

The second scenario simulated was power theft where unregistered loads were connected to the system during the time of fault and drew excess power from the system without being noticed. The local power measurement, controller power measurements, and their difference are recorded as 457.1KW, 625.3KW and 168.2KW respectively and are given in Figure 10. 168.2KW of power is lost due to the unregistered loads.

Table 1. Vulnerability assessment results

Sl. No.	Name of Vulnerability	Equipment	Type of Cyber Attack	Risk Level	Solution
1	ICCP/COTP protocol vulnerability	Protection relay Overcurrent relay Merging unit Feeder protection system Line distance protection system	Zero Day Exploits	Medium	Either limit traffic to this port to authorized hosts or upgrade to Secure ICCP, which protects the basic protocol with SSL / TLS encryption and digital certificates.
2	Unencrypted telnet server	RTU	Man in the middle attack	Medium	Use encrypting the telnet server or using a signed certificate for logins
3	Firewall detection	Smart meters	Secured	Zero	Proactive defence against cyber threats exists
4	Untrusted SSL certificate	Overcurrent relay Merging unit	Man in the middle attack	Medium	Purchase or generate a proper SSL Certificate
5	VxWorks multiple vulnerabilities	Feeder protection system Line distance protection system	Zero- day exploits	Critical	Patch update from the device development team
6	Secure Shell (SSH)	Feeder protection system Line distance protection system	Man in the middle attack or Phishing attack	High	Use of Secure Shell which is a cryptographic network protocol used for secure communication over an unsecured network
7	Wind River VxWorks	Feeder protection system Line distance protection system	Zero- day exploits	Critical	Patch update resistant to denial-of-service attacks
8	Simple network management protocol Agent default community name	Overcurrent relay	Data exploits	High	Disable the SNMP service on the remote host if it is not in use or administrators should implement access restrictions and monitoring for this service.

The current transformer ratio was manipulated and due to that the reading of the currents was wrongly signalled as overcurrent after t = 4s the circuit breakers operation was disrupted, and the circuit breakers opened. The sudden opening of circuit breakers leads to an imbalance in the network, if it is continued for a longer period then there may be a blackout or physical damage to the power system. Figure 9 shows a graphical representation of the circuit breaker.

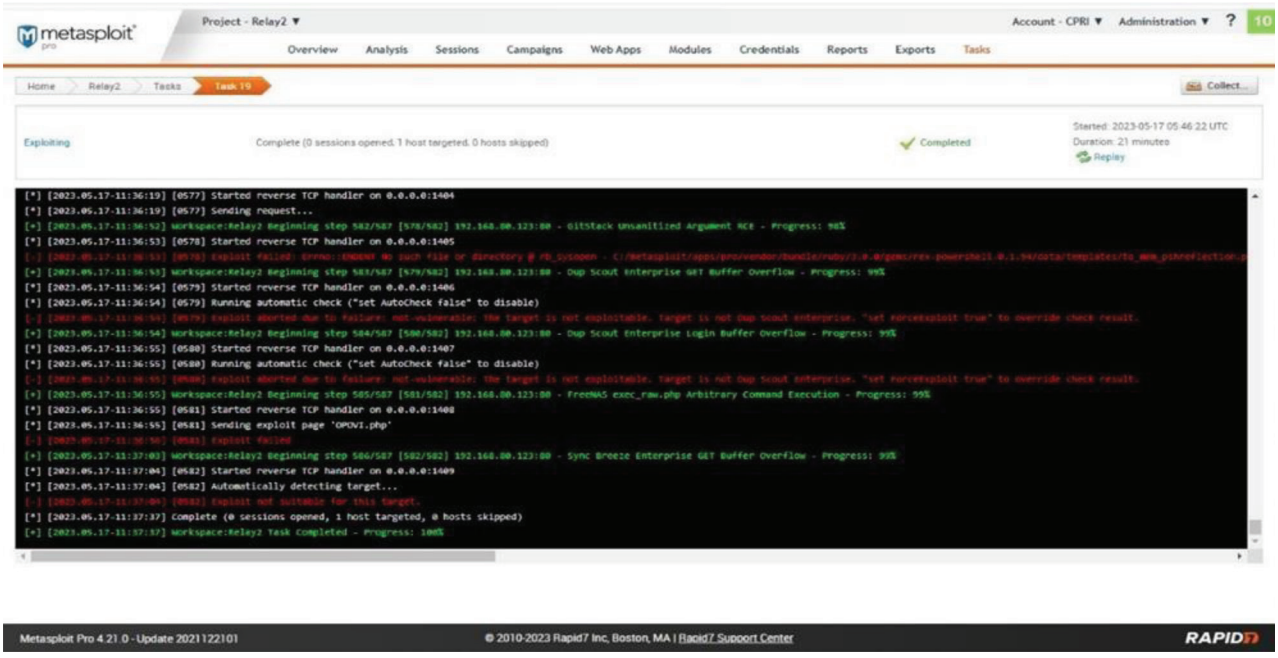


Figure 7. Penetration testing results of the relay.

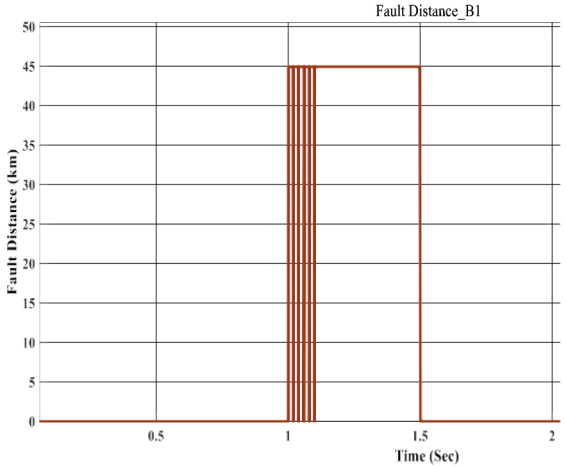


Figure 8. Fault Distance Detection at B1.

The simulation scenarios gave insights into the possible consequences that may be faced in case of a cyber-attack that may fall under the man-in-the-middle attack or zero-day exploits or data manipulation where the attacker could send false data of current and voltage readings leading to improper operation of the protection devices and hence causing imbalance in the distribution network.

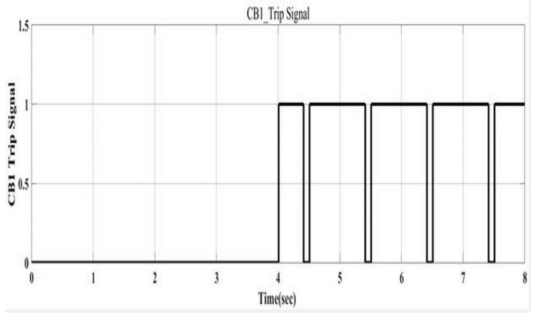
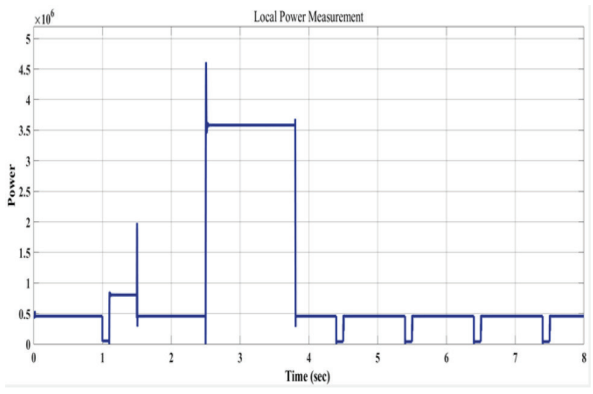


Figure 9. Trip signals of the circuit breaker.



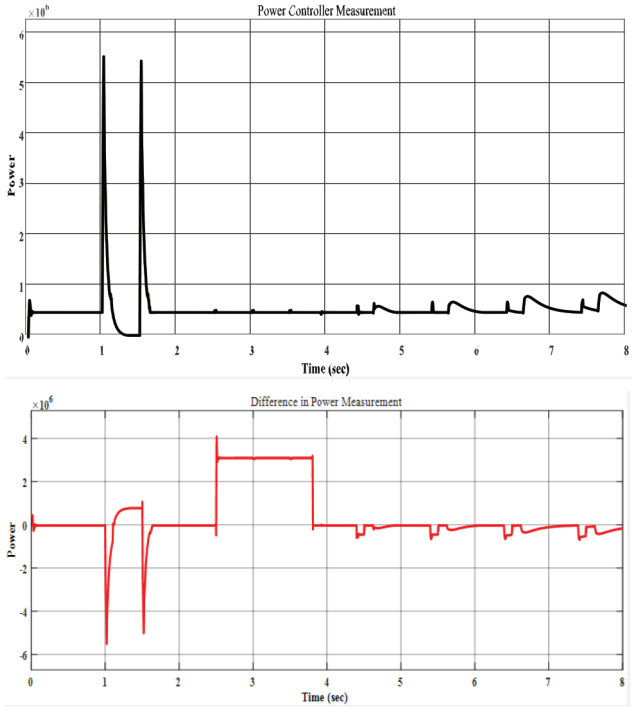


Figure 10. Power measurement result.

11. Conclusion

The study highlights the critical importance of cybersecurity in power system infrastructure by examining vulnerabilities and risks in various components like relays, RTUs, smart meters, and protection systems. Through vulnerability assessment and penetration testing, weaknesses in individual components were identified, contributing to an enhanced understanding of the overall cybersecurity landscape. The analysis of reported vulnerabilities led to the identification of response actions, emphasizing the role of cybersecurity in ensuring power system resilience against evolving threats. The simulation of cyber-attack scenarios underscored the consequences and informed the development of strategies to enhance the network's resilience. The significance of proactive cybersecurity measures for safeguarding critical infrastructure and contributing to ongoing efforts to ensure the robustness and reliability of power systems in the face of evolving cyber threats is discussed.

12. Future Scope

The future research recommendations emphasize the need for real-time monitoring, adaptive defence mechanisms, and specialized intrusion detection systems to address evolving cyber risks in power systems. Standardized response protocols and incident management strategies tailored to power systems are suggested for significant contributions. The human element in cybersecurity resilience can be strengthened through effective training programs and awareness campaigns. Ongoing research is proposed to focus on the adaptation and optimization of simulation environments, incorporating the latest cyber-attack scenarios and fault models for the continuous improvement of resilience strategies in securing power systems in the digital age.

13. References

1. De S, Sodhi R. A PMU assisted cyber-attack resilient framework against power systems structural vulnerabilities. J Electr Power Syst Res. 2022.
2. Sun C-C, Sebastian DJ, Hahn A, Liu C-C. Intrusion detection for cyber security of smart meters. IEEE Trans Smart Grid. 2020.
3. Oyewole PA, Jayaweera D. Power system security with the cyber-physical power system. IEEE Access. 2020; 8. https://doi.org/10.1109/ACCESS.2020.3028222
4. Nayak J, Al-Anbagi I. Vulnerability assessment and defence strategy to site distributed generation in smart grid. IET Smart Grid. 2022. https://doi.org/10.1049/stg2.12059
5. Hemmati M, Palahalli MH, Gajani GS, Gruoss G. Impact and vulnerability analysis of IEC61850 in smart grids using multiple HIL real-time testbeds. IEEE Access. 2022; 10. https://doi.org/10.1109/ACCESS.2022.3209698
6. Negi R, Kumar P, Ghosh S, Shukla SK, Gahlot A. Vulnerability assessment and mitigation for industrial critical infrastructures with cyber-physical test bed. International Conference on Industrial Cyber-Physical Systems. IEEE. 2019. https://doi.org/10.1109/ICPHYS.2019.8780291
7. Wang X, Fidge C, Nourbakhsh G, Foo E. Anomaly detection for insider attacks from untrusted intelligent electronic devices in substation automation systems. IEEE Access. 2022; 10. https://doi.org/10.1109/ACCESS.2022.3142022
8. Zheng X, Nadeem MH, Tai N, Habib S, Wang B, Yu M, *et al.* A transient current protection and fault location scheme for MMC-HVDC transmission network. Int J Electr Power Energy Syst. 2020. https://doi.org/10.1016/j.ijepes.2020.106348

Software Tools

a. Tenable NESSUS Software.
b. Rapid 7 Metasploit Software.
c. MATLAB Simulink Software.