JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Enhancing Resilience and Cyber-Security in Power Systems through Advanced SCADA Applications: A Technical Review

[1]Rabiu B. Ahmad, [2]Abba Muhammad Adua, [3]I. I. Alabi, [3]A. I. Araga, [4]B. G. Danshehu, [5]Yau Alhaji Samaila, [2]Umar M. Jajere, [6]Wadzani Umaru

[1]Department of Aerospace Engineering, Faculty of Air Engineering, Air Force Institute of Technology, Kaduna, Nigeria.
[2]Dept. of Electrical/Electronics Engineering, Faculty of Engineering, Kebbi State University of Science &Technology, Aliero, P.M.B 1144, Kebbi State.
[3]Nigerian Defence Academic (NDA) Kaduna, Faculty of Engineering Technology, Department of Electrical/Electronics Engineering, Kaduna State
[4]Usmanu Danfodio University, Faculty of Engineering &Environmental Design, Department of Mechanical Engineering, Sokoto State
[5]Department of Electrical/Electronics Engineering, Faculty of Engineering, University of Maiduguri
[6]Department of Electrical/Electronics Engineering, Adamawa State Polytechnic, Yola, Nigeria

ABSTRACT

This literature review explores the crucial intersection of resilience and cyber-security within power systems, emphasizing the role of advanced Supervisory Control and Data Acquisition (SCADA) applications in fortifying these essential infrastructures. The paper delves into existing research to provide a comprehensive overview of the state-of-the-art advancements in enhancing the resilience of power systems against various threats, ranging from natural disasters to malicious cyber-attacks. The analysis encompasses key concepts such as threat detection, incident response, and recovery strategies, with a particular focus on how advanced SCADA applications contribute to bolstering the overall cyber-security posture. By synthesizing insights from diverse sources, this review aims to contribute valuable perspectives on the evolving landscape of power system protection and resilience, guiding future research directions and practical implementations for a more secure and robust energy infrastructure.

ARTICLE INFO

Article History
Received: March, 2023
Received in revised form: March, 2023
Accepted: April, 2023
Published online: June, 2023

KEYWORDS

Cyber-security, Power Systems Protection, Supervisory Control and Data Acquisition.

INTRODUCTION

The abbreviation SCADA stands for "Supervisory Control and Data Acquisition." It is a technology that allows real-time data acquisition and control for the management and oversight of a sizable distributed process from a central point known as the "control centre." It is highly helpful for managing and keeping an eye on electrical networks, such as TCNs [1]. Modern society's biggest marvel is electricity. There is nothing we can do in the world without power. The principal elements of the power system are the distribution networks, producing plants, and transmission lines. Thus, it necessitates an understanding of load fluxes, which is hard to achieve without meticulous planning, regulation, and overseeing [2]. Furthermore, the system must function in a way that minimizes losses and, consequently, manufacturing costs. Supervisory control and data acquisition are the two methods used by each process to monitor the many parameters in a substation. Each process will also have its specific systems for data acquisition and control [3].

SCADA

SCADA refers to the combination of telemetry and data acquisition. The Remote Terminal Unit (RTU) is used to gather data, which is then moved back to the central site for definitive rehashing and control. The data is then displayed on many operating screens or displays by the SCADA. Often dispersed over thousands of square kilometres, SCADA systems are highly distributed systems that are used to operate geographically dispersed

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

assets where centralized data acquisition and control are essential to system performance [4].

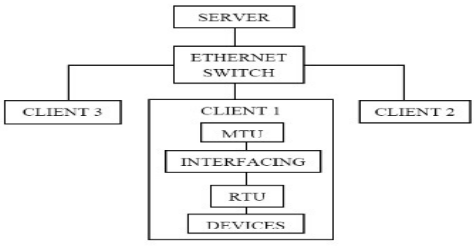

Figure 1.1: SCADA [3]

Physical components like switches, pumps, and other gadgets that can be managed by a Remote Telemetry Unit (RTU) are part of a SCADA's general design. The dual functions of the master computers are to give human operators easily readable information such as equipment status and meter readings, as well as to enable the operators to control field equipment through operator consoles that connect to the master computers via a network [5].

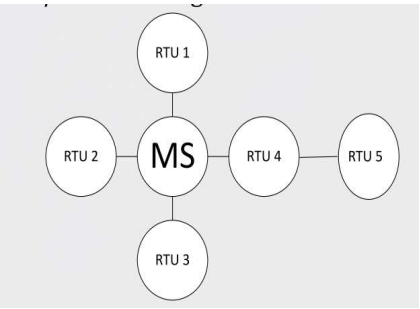

Figure 1.2: Star/In-line configuration topology of a SCADA system [6]

An Overview of the Importance of Resilience and Cyber-Security in Power Systems.

In the contemporary landscape of interconnected and digitized power systems, the significance of resilience and cyber-security cannot be overstated. Power systems serve as the backbone of modern societies, providing essential energy to support various sectors such as healthcare, transportation, communication, and industry. As these systems become increasingly reliant on advanced technologies and digital infrastructure, the vulnerabilities to cyber threats also escalate. This necessitates a comprehensive understanding of the importance of resilience and cyber-security to safeguard the reliability and functionality of power systems [7].

The implementation of a smart grid offers several benefits, including heightened automation in decision-making, closer integration of production and consumption, and greater digitization [8].

Critical Infrastructure Dependency:

Power systems are classified as critical infrastructure, forming the foundation for the functioning of other essential services. Any disruption in the power supply chain can have cascading effects on the entire societal infrastructure. Resilience measures ensure that power systems can withstand and recover from unforeseen events, both natural and human-induced, to maintain a continuous and reliable energy supply [9].

1. **Digital Transformation and Vulnerabilities:**

The ongoing digital transformation in power systems introduces new efficiencies and capabilities but also exposes them to cyber threats. The integration of smart grids, IoT devices, and communication networks enhances operational efficiency but concurrently creates potential entry points for malicious actors. Cyber-security measures are crucial to protect against unauthorized access, data breaches, and the manipulation of critical infrastructure [10].

2. **Risk of Cyber Attacks:**

Power systems are prime targets for cyber-attacks due to their economic and societal impact. Threat actors, ranging from state-sponsored entities to independent hackers, seek to exploit vulnerabilities in power infrastructure for financial gain, political motives, or even to create widespread disruption. Resilience planning involves anticipating and mitigating the impact of potential cyber-attacks to ensure a swift recovery [11].

3. **Ensuring Continuous Operation:**

Resilience in power systems involves strategies to minimize downtime and ensure

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

continuous operation, even in the face of adversity. This includes the development of redundant systems, backup power sources, and recovery plans that can be swiftly executed in the aftermath of an incident. Cyber-security measures act as a proactive defense mechanism to prevent disruptions and protect the integrity of power system operations [12].

4. Regulatory Compliance and Standards:

Governments and regulatory bodies recognize the critical importance of resilience and cyber-security in power systems. They have implemented standards and regulations to enforce cyber-security practices and ensure the resilience of power infrastructure [13].
Here's an overview of the importance of resilience and cyber-security in power systems:

A. Reliability and Continuity

Resilience in power systems ensures the ability to withstand and quickly recover from disruptions, whether caused by natural disasters, physical attacks, or cyber incidents. SCADA systems are critical components in various industries, including energy, manufacturing, water treatment, and transportation. The reliability of SCADA systems is crucial for ensuring the continuous and secure operation of industrial processes [14].

Here are key aspects related to the reliability and continuity of SCADA systems:

1. **Redundancy:** Reliable SCADA systems often incorporate redundancy at various levels, including hardware, software, and communication paths. Redundant components ensure that if one part of the system fails, another takes over seamlessly, minimizing downtime [15].
2. **Fault Tolerance:** SCADA systems are designed to be fault-tolerant, meaning they can continue to operate even in the presence of faults or failures. This involves the ability to detect and isolate faults, allowing the system to adapt and continue functioning [16].
3. **Cyber-security Measures:** Ensuring the cyber-security of SCADA systems is crucial for their reliability. Implementing robust security measures, such as firewalls, intrusion detection/prevention systems, and regular security audits, helps protect the system from cyber threats and unauthorized access [11].
4. **Regular Maintenance and Updates:** Scheduled maintenance and timely software updates are essential for the reliability of SCADA systems. This includes updating software patches, upgrading hardware components, and performing routine checks to identify and address potential issues before they become critical [14].
5. **Backup and Recovery Plans:** SCADA systems should have comprehensive backup and recovery plans in place. Regularly backing up critical data and configurations enables a quick recovery in the event of system failure, ensuring minimal disruption to operations [17].
6. **Physical Security:** Physical security measures are essential to protect the hardware components of SCADA systems from unauthorized access, tampering, or damage. Restricted access to SCADA control rooms and equipment locations is typically enforced [18].

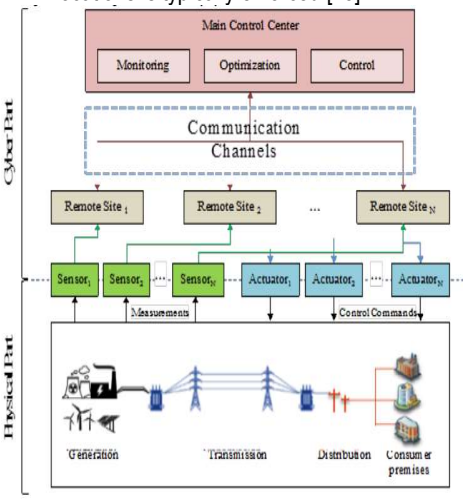

Figure 1.3: General architecture of a SCADA system [18]

Cyber-security measures protect power systems from intentional attacks or unintentional incidents that could compromise

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

the availability and reliability of electricity supply [7]. Securing power systems from intentional attacks or unintentional incidents is crucial to maintaining the availability and reliability of electricity supply [19]. Cyber-security measures play a vital role in safeguarding power infrastructure against various threats. Here are detailed measures to protect power systems:

1. **Network Segmentation:**
   i. Implement a robust network architecture with clear segmentation between corporate IT networks and operational technology (OT) networks [20].
   ii. Use firewalls and access controls to restrict unauthorized access between different network segments.
2. **Secure Communication Protocols:**
   i. Employ secure communication protocols, such as Transport Layer Security (TLS) and Advanced Encryption Standard (AES), to protect data in transit [21].
   ii. Ensure the integrity and authenticity of communication through the use of digital signatures and certificates.
3. **Access Control and Authentication:**
   i. Implement strong access controls and enforce the principle of least privilege to limit system access to authorized personnel only.
   ii. Utilize multi-factor authentication (MFA) to enhance user authentication and prevent unauthorized access.
4. Continuous Monitoring and Intrusion Detection:
   i. Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic for unusual patterns or malicious activities.
   ii. Implement continuous monitoring to promptly identify and respond to any anomalies or security incidents.
5. **Security Patching and Updates:**
   i. Regularly update and patch all software, firmware, and operating systems to address known vulnerabilities [16].
   ii. Establish a well-defined and tested process for applying security updates without

B. Critical Infrastructure Protection:

i. Power systems are considered critical infrastructure because they support the functioning of various sectors, including healthcare, communication, transportation, and finance. Any disruption can have cascading effects on the overall economy and society [22].
ii. Cyber-security measures are essential to protect critical infrastructure from malicious actors seeking to exploit vulnerabilities in the power grid for financial gain, political motives, or sabotage [16].

C. Preventing Cyber Attacks

i. Cyber threats to power systems include attacks on supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and other interconnected devices. These attacks can lead to disruptions in energy production, transmission, and distribution [23].
ii. Implementing robust cyber-security measures, such as firewalls, intrusion detection systems, and encryption, helps prevent unauthorized access and mitigate the risk of cyber-attacks.

D. Data Integrity and Confidentiality

1. Power systems rely on data from various sensors and devices for efficient operation and control. Ensuring the integrity and confidentiality of this data is crucial to maintaining the accuracy and reliability of the power grid [24].
2. Cyber-security measures protect against data manipulation, unauthorized access, and data breaches that could compromise the confidentiality of sensitive information.

E. Smart Grids and IoT Integration:

i. The integration of smart grids and the Internet of Things (IoT) brings new opportunities for enhancing the efficiency of power systems. However, it also introduces new vulnerabilities and potential entry points for cyber threats [18].
ii. Resilience planning and cyber-security protocols need to adapt to the evolving nature of power systems, taking into account the increased complexity of interconnected devices and systems [25].

F. Regulatory Compliance:

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

i. Many countries and regions have established regulations and standards to ensure the cyber-security of critical infrastructure, including power systems. Compliance with these regulations is essential for power operators to demonstrate a commitment to cyber-security best practices and protect against potential legal and financial consequences [26].

Role of SCADA Systems in Power Infrastructure.

SCADA systems play a pivotal role in modern power infrastructure, serving as the nerve centre that ensures the efficient and reliable operation of power generation, transmission, and distribution systems. As the demand for electricity continues to rise and the power grid becomes more complex, SCADA systems have become indispensable in monitoring, controlling, and optimizing the various components of the power network. One of the primary functions of SCADA systems is to monitor the entire power infrastructure in real-time. These systems collect data from sensors, remote terminal units (RTUs), and other devices distributed across the power grid..

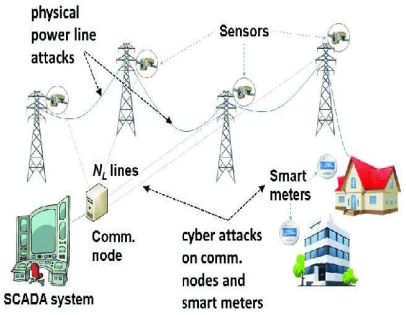

Figure 1.4: Smart power grid infrastructure. SCADA: supervisory control and data acquisition [27]

SCADA systems excel in their ability to detect faults and anomalies within the power grid. By continuously monitoring parameters such as voltage, current, and frequency, SCADA systems can promptly identify deviations from normal operating conditions. The rapid detection of faults enables operators to isolate and address issues swiftly, minimizing downtime and preventing potential cascading failures [22]. The reliability of power infrastructure is critical to meeting the demands of modern society.

Need for Advanced SCADA applications to address evolving cyber threats.

In today's dynamic technological landscape, the increasing prevalence of cyber threats poses a significant challenge to critical infrastructure systems. Supervisory Control and Data Acquisition (SCADA) applications, which form the backbone of industrial control systems, play a crucial role in monitoring and controlling essential processes across various sectors such as energy, water, and manufacturing [28]. As cyber threats continue to evolve in sophistication and frequency, there is a pressing need to highlight the importance of advanced SCADA applications in fortifying the resilience of these critical systems.

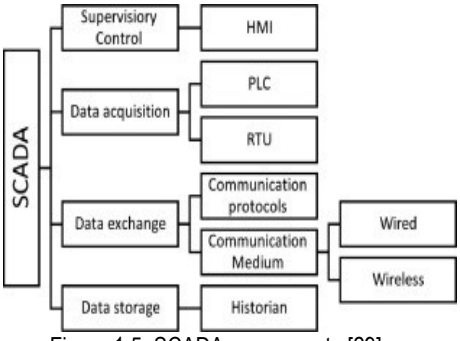

Figure 1.5. SCADA components [29].

Traditional SCADA systems were primarily designed with a focus on functionality and efficiency, often overlooking robust cyber-security measures. However, the escalating frequency and severity of cyber-attacks underscore the necessity for a paradigm shift in SCADA applications. Advanced SCADA systems integrate cutting-edge cyber-security protocols to proactively detect, prevent, and respond to cyber threats.

Problem Statement

The resilience and security of power systems are critical concerns in the modern era, where the increasing complexity and interconnectivity of electrical grids make them

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

vulnerable to a range of threats. SCADA) systems, while essential for the monitoring and control of power networks, are increasingly exposed to cyber-attacks and operational disruptions. These vulnerabilities pose significant risks to the stability and reliability of power systems, potentially leading to widespread outages and economic losses.

SCADA systems are integral to the operation of power systems, providing real-time data acquisition, monitoring, and control capabilities. However, the integration of SCADA systems with other network components and the rise of the Internet of Things (IoT) in the energy sector have expanded the attack surface for cyber threats. The inherent weaknesses in legacy SCADA systems, such as lack of encryption, inadequate authentication mechanisms, and insufficient intrusion detection, exacerbate these vulnerabilities. Consequently, enhancing the resilience and cyber-security of SCADA applications is imperative to safeguard the critical infrastructure of power systems.
infrastructure. Furthermore, the dynamic and evolving nature of cyber threats necessitates continuous updates and improvements to security protocols, making it a persistent challenge for power system operators.

Motivation and Contribution

The Power Grid is essential to the operation of many enterprises. Since there is very little margin for error in Power Grid service, vulnerability management and cyber-attack defence are critical. The management system that manages the Power Grid to prevent damage and service interruptions is called an Industrial management System (ICS). Cyber-security experts and ICS stakeholders are concerned, meanwhile, about recent hacks that have targeted ICS [7]s. Unidirectional firewalls, anti-virus/malware protection programs, and passive defence systems, such passive ICS Intrusion Detection Systems (IDS), have proven to be ineffective against malware attacks like BLACKENERGY3 and CRASH OVERRIDE. For instance, CRACHOVERRIDE sought to exploit simultaneous attacks at several locations.

Developing cyber resilience in the Power Grid requires an understanding of cyber-attacks. However, without prior knowledge of attacks, it can be challenging to comprehend how to create sufficient defence and detection systems [30]. The findings of conducting controlled attacks on the SCADA protocol are presented in this work, which makes use of a controlled experiment environment. IEC 60870-5-104, a SCADA protocol frequently used to send commands from the dispatch centre to the substation, is the one that has been attacked [29]. A Hardware-In-the-Loop (HIL) IEC 61850 Substation, sometimes referred to as a Digital Station, makes up the experiment environment [26].

REVIEW OF THE FUNDAMENTAL

SCADA systems are crucial in various industries for monitoring and controlling industrial processes. The primary purpose of SCADA is to gather, process, and analyse real-time data and provide control to efficiently manage equipment and conditions. The interface through which operators interact with the SCADA system [5]. It provides visualizations, alarms, and controls for efficient monitoring and management. SCADA systems use various communication protocols such as Modbus, DNP3, OPC, and others to facilitate data exchange between different components. SCADA systems find applications in industries like energy, water treatment, manufacturing, and transportation [31]. Remember that the specifics of SCADA systems can vary based on industry and application. This overview provides a general understanding of the fundamental concepts in SCADA [32].

The Application layer and Datalink layer security of the SCADA systems in the power utility industry were exploited by the author in [33]. They used IEC 60870- 5-101 for spoofing and non-repudiation attacks, and IEC 60870-5-104 for sniffing, data alteration, and replay assaults. They coordinated their attacks by taking advantage of the built-in weaknesses in security measures, such as a small checksum and constrained bandwidth. Ultimately, they suggested a study model with minimal requirements and checks to lessen these attacks; nevertheless, taking into account zero-

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

day attacks, merely putting in place minimal requirements and checks is insufficient to secure these communication protocols.

SCADA System Evolution

Initially, all SCADA systems relied on basic wiring topologies when they first came into being. However, more sophisticated wireless topologies have been included into SCADA as a result of significant technology advancements and growing concerns about the elevated costs of operation and maintenance. This circumstance led to the continual development of SCADA systems [34]. The integration of outdated SCADA components and topologies with contemporary technology components and topologies increased the security susceptibility of the systems. System security is then decreased by using several monitoring strategies and shifting data computation areas from physical devices to Web- or cloud-based systems.

Classical Wired-Based SCADA Systems

These stand-alone control and monitoring systems are centralized SCADA systems. Traditional wired-based monolithic SCADA systems relied more on the producer firm because they used producer-specific software instead of open-source software. A wide area network protocol was utilized for the communication between the remote terminal units (RTUs), even though the communication between the RTUs and the master terminal unit (MTU) was done over wires [14]. The typical architecture of wire-based, traditional SCADA systems is shown in Figure 2.1.

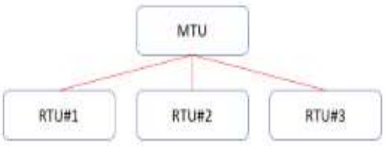

Figure 2.1: General architecture of wire-based classical SCADA system [34]

Distributed SCADA Systems

When opposed to traditional wired-based SCADA systems, the main advantage of dispersed SCADA systems was their first use of local area network (LAN) protocols. Nevertheless, producer-specific protocols and software—the primary flaw in previous generations of SCADA systems—remain in this generation as well. A typical distributed SCADA system architecture is seen in Figure 2.2.

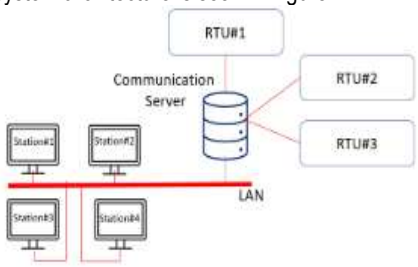

Figure 2.2: General architecture of distributed SCADA system [34]

Network-based SCADA Systems Compared

SCADA systems based on networks Utilizing open-source software and standard protocols, network-based SCADA systems offered revolutionary features when compared to first- and second-generation SCADA systems. The initial outlay, ongoing expenses, and maintenance expenses were all greatly decreased by this functionality. Being independent of the producer also improved redundancy and flexibility and made it easier for the system to grow in the future. Due to the fact that numerous SCADA components may be accessed via the Internet, the system is now more susceptible to cyber-attacks [26]. The fundamental architecture of network-based SCADA systems is shown in Figure 2.3.

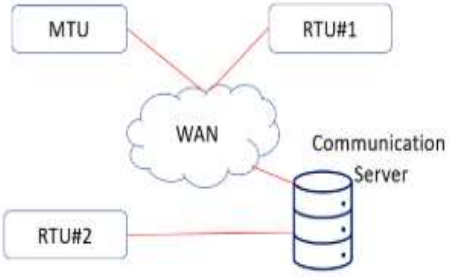

Figure 2.3: General architecture of network-based SCADA system [34]

IoT-Cloud Based SCADA Systems IoT-cloud-based

SCADA Systems Based on IoT and Cloud SCADA systems based on IoT clouds are

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

becoming commonplace. The primary cause of its popularity is the substantial ease with which SCADA system integration and maintenance are made possible by IoT-cloud-based SCADA systems. The cloud system is where all data storage and processing are done. IoT-cloud-based SCADA systems are more targeted for cyber-attacks than traditional SCADA systems [35]. The fundamental architecture of SCADA systems based on IoT clouds is shown in Figure 2.4. However, given their system's flexibility, redundancy, accessibility, and scalability as well as research in the field of cyber security, these systems will become increasingly prevalent in the energy and industrial sectors.

Resilience in Power Systems

This section delves into the concept of resilience in power systems, exploring the inherent vulnerabilities and potential disruptions that can impact the stability of the grid. It reviews existing literature on resilience metrics, methodologies, and strategies, highlighting the role of advanced SCADA applications in enhancing the adaptive capacity of power systems [31].

SCADA systems play a pivotal role in ensuring the reliable and efficient operation of power systems.

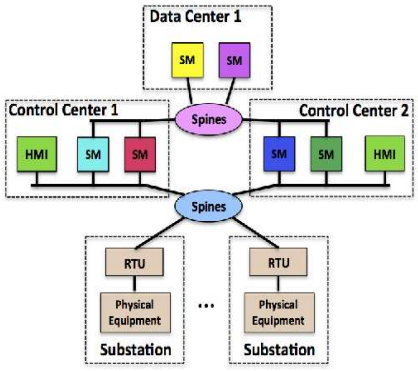

Figure 2.5. SCADA Architecture with 2 replicas in each of the two control centres and the single data centre [29]

One key element contributing to the resilience of SCADA in power systems is its capacity to provide real-time monitoring and control. SCADA enables operators to continuously observe the performance of various components within the power grid, allowing for swift identification and response to any anomalies or faults. This real-time awareness is crucial for preventing cascading failures and minimizing downtime, thereby enhancing the overall resilience of the power system [36].

Cyber-security Challenges in Power Systems

Addressing the escalating cyber-security threats to power systems is paramount in ensuring the reliability of energy supply. This section examines the current landscape of cyber-security challenges faced by power utilities, including attacks on SCADA systems [7].

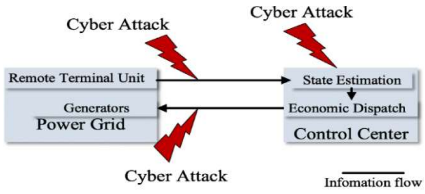

Figure 2.6: Cyber-attacks on a power system [37]

Industrial Control Systems (ICS) have been the target of numerous attacks; research has produced numerous summaries and in-depth forensic studies of these attacks. An extensive history and synopsis of industrial control system cyber events were given by the Idaho National Lab (INL) in 2018 [38], the example demonstrates how security is only as strong as its weakest point. What's more, the Power Grid, which still uses outdated methods, is becoming increasingly interconnected to form a hyper-connected Smart Grid.

Advanced SCADA Applications

This section provides an in-depth analysis of the state-of-the-art SCADA applications designed to enhance the resilience and cyber-security of power systems. It explores advancements in real-time monitoring, anomaly detection, intrusion prevention, and response mechanisms. Case studies and empirical evidence from the literature are

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

presented to illustrate the efficacy of these advanced SCADA applications [39].

Integration of Artificial Intelligence and Machine Learning

The utilization of artificial intelligence (AI) and machine learning (ML) in SCADA applications is a burgeoning area of research. This section reviews literature on the integration of AI and ML techniques to fortify power systems against cyber threats. It examines the potential benefits, challenges, and emerging trends in leveraging intelligent technologies for proactive cyber-security measures [40].

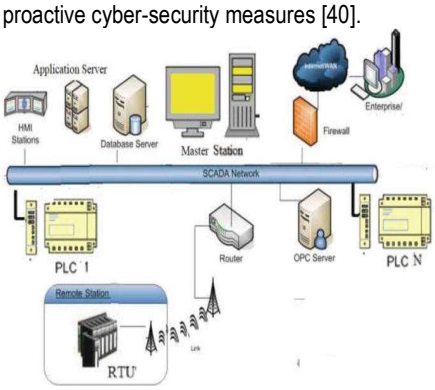

Figure 2.7: Architecture of a SCADA system, The Master Station refers to the servers and software responsible for communicating with Remote Terminal Units (RTUs), e.g PLCs [41]

In various sectors, the integration of AI and ML is driving unprecedented advancements. One prominent area is healthcare, where these technologies are being employed to analyse vast datasets, diagnose diseases, and personalize treatment plans. The ability of AI algorithms to discern patterns in medical data accelerates decision-making processes, leading to more efficient and accurate patient care [19].

Figure 2.8: AI Technology Landscape [42].

In the business landscape, AI and ML are reshaping customer experiences and operational efficiency. Chatbots, powered by AI, provide instant and personalized customer support, while machine learning algorithms analyse consumer behavior to predict trends and optimize inventory management. This integration streamlines processes, enhances decision-making, and ultimately contributes to the overall success of businesses [43].

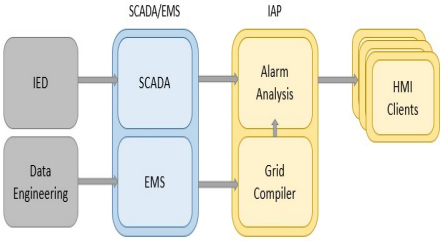

Figure 2.9: Configuration of SCADA and SMS [44]

In conclusion, the integration of Artificial Intelligence and Machine Learning is a paradigm shift that transcends traditional boundaries, redefining how we approach complex problems and unlocking new possibilities. As these technologies continue to evolve, their impact on various industries will undoubtedly shape the future, making our systems more intelligent, adaptive, and capable of addressing the challenges of a rapidly changing world [45]. The integration of Artificial Intelligence (AI) and Machine Learning (ML) presents a myriad of challenges that organizations and researchers must navigate to harness the full potential of these technologies.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

One significant challenge is the scarcity of skilled professionals in the field. The demand for AI and ML experts far exceeds the current supply, leading to a talent gap that hampers the seamless integration of these technologies into various industries [46]. The interpretability of AI and ML models is a challenge that impacts their acceptance and adoption. Many complex models operate as "black boxes," making it difficult for users to understand the rationale behind their decisions. Interpretable AI is crucial, especially in applications where accountability and transparency are essential, such as healthcare and finance. Security concerns form a substantial barrier to the integration of AI and ML. As these technologies become more integral to critical systems, they become attractive targets for malicious actors. Safeguarding AI and ML systems against adversarial attacks and ensuring their resilience to cyber threats is an ongoing challenge that requires constant vigilance and innovation in cyber-security [7].

The integration of AI and ML faces a spectrum of challenges, spanning from talent shortages and ethical considerations to interoperability issues and security concerns. Addressing these challenges requires a concerted effort from researchers, industry leaders, and policymakers to create a robust and ethical framework for the widespread adoption of AI and ML technologies.

Regulatory and Policy Implications

A comprehensive literature review would be incomplete without addressing the regulatory and policy landscape. The SCADA systems play a critical role in the efficient operation and management of power system networks. As these networks continue to evolve and become more complex, the regulatory and policy implications associated with SCADA technologies become increasingly significant [47].

One of the foremost considerations in the regulatory landscape is the need for robust cyber-security measures to safeguard SCADA systems from potential threats. Given the interconnected nature of power systems, a breach in the SCADA infrastructure could have far-reaching consequences, leading to disruptions in power supply, financial losses, and even compromise of national security. Regulatory frameworks must, therefore, be designed to enforce stringent cyber-security standards, fostering collaboration between government agencies, utilities, and technology providers to ensure the resilience of SCADA systems against cyber threats [26].

Moreover, as SCADA systems often involve the collection and analysis of vast amounts of sensitive data, privacy concerns come to the forefront of regulatory discussions. Policies must be formulated to govern the ethical and lawful use of data within SCADA networks, addressing issues such as data ownership, consent, and transparency. Striking the right balance between data access for operational efficiency and privacy protection is crucial to building public trust in the deployment of SCADA technologies.

METHODOLOGY

The method employed to review "Enhancing Resilience and Cyber-security in Power Systems through Advanced SCADA Applications: A Comprehensive Literature Review" involved a systematic and thorough examination of existing scholarly works within the field. The researchers began by conducting a comprehensive search of relevant databases, academic journals, and conference proceedings to identify key studies related to the enhancement of resilience and cyber-security in power systems through advanced SCADA applications. The inclusion criteria were carefully defined to ensure the selection of high-quality and relevant literature, and the researchers employed a rigorous screening process to filter out articles that did not meet the predetermined criteria.

After the initial literature selection, the researchers critically analysed and synthesized the chosen articles, identifying common themes, trends, and gaps in the existing knowledge..

CYBER THREAT LANDSCAPE ANALYSIS

The cyber threat landscape in the context of power systems has become

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

increasingly complex and sophisticated in recent years. This review presents a thorough analysis of the challenges and opportunities associated with securing power infrastructure against cyber threats. This section delves into the evolving nature of cyber threats targeting SCADA systems, which play a critical role in the operation and management of power grids [18].

The comprehensive review highlights the need for advanced SCADA applications as a key component in fortifying the resilience and cyber-security of power systems. As the energy sector becomes more interconnected and reliant on digital technologies, the vulnerabilities associated with SCADA systems have grown, making them attractive targets for malicious actors seeking to disrupt critical infrastructure. The review synthesizes existing research to identify the various attack vectors and tactics employed by cyber adversaries, shedding light on the potential consequences of a successful cyber-attack on power grids [48].

Furthermore, the analysis explores the current state of cyber-security measures implemented in SCADA systems and evaluates their effectiveness in mitigating cyber threats. The review also considers emerging technologies and innovative approaches that can be leveraged to enhance the security posture of power systems [11]. The integration of artificial intelligence, machine learning, and anomaly detection techniques is examined as a means to detect and respond to cyber threats in real-time, thereby bolstering the resilience of power infrastructure [42].

Table 4.1 show works of literature on different attacks on power systems. The table provides an overview of various works of literature that discuss different types of attacks on power systems, with a focus on enhancing resilience and cyber-security through advanced SCADA applications. Each entry includes the title of the work, the type of attack discussed, key findings, and the proposed solutions or mitigations.

Table 4.1 show works of literature on different attacks on power systems

Title	Type of Attack	Key Findings	Proposed Solutions/Mitigations
Microgrid Power Sharing Framework for Software Defined Networking and Cybersecurity Analysis [7]	Cyber-Physical Attacks	Comprehensive survey of cyber-physical attacks on power grids; highlights vulnerabilities	Use of advanced encryption, intrusion detection systems, and robust SCADA security
Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection [49]	Unsupervised Learning Methods for Cyber Detection	Reviews methods for detecting anomalies in smart grids, including machine learning techniques	Implementation of machine learning algorithms for real-time anomaly detection
Enhancing Cybersecurity of Power Systems using Machine Enhancing Cybersecurity of Power Systems using Machine Learning	Cyber Intrusions	Examines the role of machine learning in detecting and mitigating cyber intrusions in power systems	Development of adaptive machine learning models for continuous monitoring
A Security Assessment Model for Electrical Power Grid SCADA System [18]	Denial-of-Service Attacks	Analyses how denial-of-service (DoS) attacks can destabilize power systems	Deployment of redundant communication paths and DoS mitigation strategies
Research on Blockchain-Enabled Smart Grid for Anti-Theft Electricity Securing Peer-to-Peer Transactions in Modern Grids [50]	Data Integrity Attacks	Discusses the use of blockchain technology to ensure data integrity and secure transactions	Integration of blockchain for tamper-proof and transparent data management
Cyber-Security Risk Assessment for SCADA Systems in Power Networks [51]	Risk Assessment	Provides a framework for assessing cyber-security risks in SCADA systems	Comprehensive risk assessment and implementation of multi-layered security measures
Man-in-the-middle attacks and defence in a power system cyber-physical testbed [52]	Man-in-the-Middle Attacks	Investigates the impact of man-in-the-middle attacks	Use of advanced cryptographic protocols and

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

		and proposes mitigation techniques	secure communication channels
Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104 [26]	General Cyber Attacks	Reviews current resilience strategies against cyber attacks and suggests future research directions	Enhancement of SCADA resilience through diversified and redundant system design
Attacking IEC-60870-5-104 SCADA Systems [53]	Intrusion Detection	Surveys various intrusion detection systems tailored for SCADA networks	Development and deployment of specialized IDS tailored to SCADA environments
Security and Mitigation of Power grid and SCADA system against Cyber attacks [54]	Adaptive Security	Proposes an adaptive security framework that evolves based on threat intelligence	Implementation of adaptive and self-healing security mechanisms in SCADA systems

Table 4.1 highlights the diverse range of literature that addresses various types of cyber attacks on power systems. Each work contributes unique insights and proposed solutions, ranging from the application of advanced encryption and machine learning techniques to the integration of blockchain technology and adaptive security frameworks. By synthesizing these findings, the literature review aims to provide a comprehensive understanding of how advanced SCADA applications can enhance the resilience and cyber-security of power systems. This synthesis will guide future research and development efforts in creating robust, secure, and resilient power infrastructure.

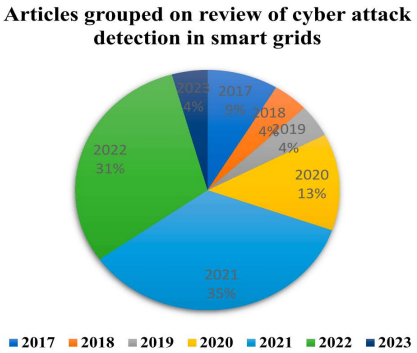

Figure 4.1 Year-wise publications with the search of cyber-attack reviews in various publications [49]

A comprehensive Cyber Threat Landscape Analysis of power system networks using SCADA is vital for maintaining the reliability and security of our modern energy infrastructure. As technology continues to advance, staying vigilant and proactive in addressing cyber threats is crucial to ensuring the uninterrupted and secure supply of electricity to communities worldwide [55].

Current Cyber Threat Landscape for Power Systems

The current cyber threat landscape for power systems, particularly those employing SCADA systems, is marked by a complex and evolving set of challenges [16]. SCADA systems play a critical role in managing and controlling various aspects of power generation, transmission, and distribution.

Figure 4.1: emerging Cyber-Security threat for 2030 [56]

The integration of Internet of Things (IoT) devices within power systems further complicates the threat landscape, creating additional points of entry for malicious actors. Threats such as distributed denial-of-service (DDoS) attacks could overwhelm SCADA systems, causing operational disruptions and potentially leading to widespread power

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

outages [16]. Furthermore, the interconnected nature of power grids makes them susceptible to cascading failures, where a compromise in one area could have a domino effect on the entire system [57].

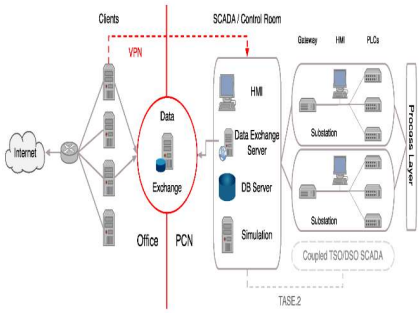

Figure 4.2: Configuration of SCAD/Control room [37]

As technology continues to advance, threat actors are likely to exploit emerging vulnerabilities in SCADA systems, necessitating constant vigilance and proactive cyber-security measures [33]. Power system operators and cyber-security professionals must collaborate to implement robust security protocols, conduct regular risk assessments, and stay informed about the latest threat intelligence to effectively safeguard critical infrastructure from the evolving cyber threat landscape. The consequences of a successful cyber-attack on power systems can be severe, not only causing economic losses but also posing significant risks to public safety and national security. Hence, a comprehensive and adaptive approach to cyber-security is essential to mitigate the ever-present and evolving cyber threats facing power systems that rely on SCADA [3], [34], [47].

Common Cyber-Attack Vectors Targeting SCADA Systems

In the realm of critical infrastructure, SCADA systems play a pivotal role in managing and controlling various industrial processes, particularly in power systems. However, the increasing integration of these systems with the digital landscape has exposed them to a myriad of cyber threats. Identifying common cyber-attack vectors targeting SCADA systems in power systems is crucial for enhancing their resilience and ensuring the uninterrupted supply of electricity [58].

Furthermore, vulnerabilities in network communication protocols pose a substantial risk. Many SCADA systems use legacy protocols that may lack robust security mechanisms. Exploiting these weaknesses, attackers can intercept and manipulate communication between devices, leading to unauthorized control over industrial processes or the injection of false data. Inadequate security practices and outdated software also contribute to the vulnerability of SCADA systems [26], [59]. Failure to apply security patches promptly or using outdated software versions can expose systems to known vulnerabilities, providing attackers with an entry point for exploitation.

Case Studies of Past Cyber Incidents to Extract Lessons Learned

Analysing case studies of past cyber incidents on power systems involving SCADA provides invaluable insights into the vulnerabilities and consequences associated with these critical infrastructures [60]. One notable case study involves the Stuxnet worm, a sophisticated cyber-weapon that specifically targeted SCADA systems controlling Iran's nuclear facilities. This incident highlighted the potential for malicious actors to exploit vulnerabilities in SCADA networks, leading to physical damage and disruption of critical operations.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

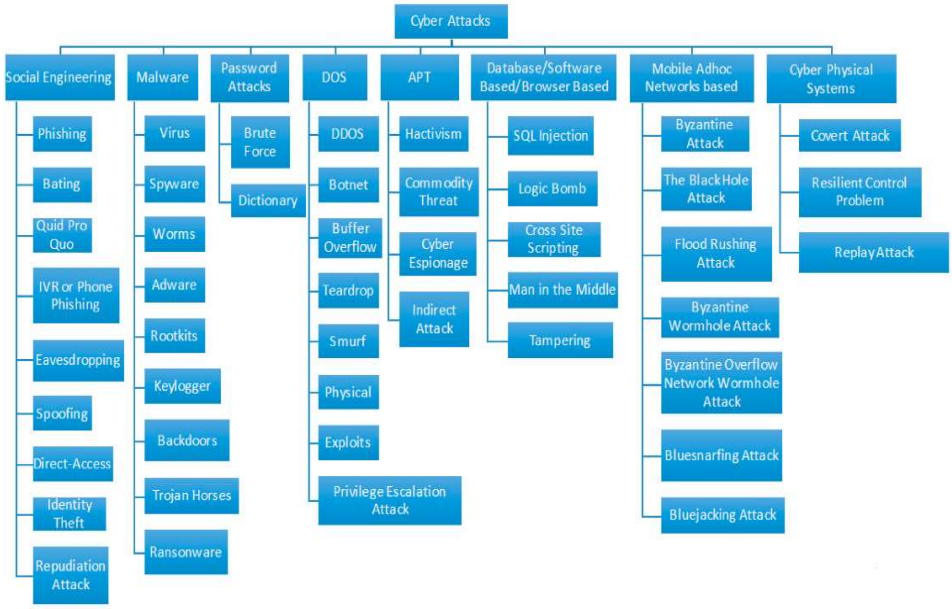

Figure 4.3: Types of cyber-attacks [61]

Determine the type of attack and establish a connection between it and the elements that preceded it, based on the analysis of case studies pertaining to that particular attack type. The authors looked at the attack types' quantitative and qualitative traits, such as the industry they targeted, the attack's financial intensity, its non-financial intensity effects, the number of affected consumers, and its effect on user loyalty and trust. We also looked into the major contributing factors to an attack, such as the organizational and cultural aspects, the security policies put in place, the business's adoption and investment in technology, the training and awareness of all stakeholders, including users, customers, and employees, and the cyber-security investments. Additionally, by assessing the co-occurrence and linking of components to create graphs of connected frequent rules seen throughout the case studies, the study examined the relationships between these factors [61].

ADVANCED SCADA APPLICATIONS

SCADA applications play a pivotal role in enhancing the efficiency, reliability, and security of power systems as mentioned earlier. SCADA systems have evolved from basic monitoring and control functions to sophisticated platforms that leverage advanced technologies to meet the growing demands of modern power grids. In the realm of power systems, these advanced SCADA applications bring about a myriad of benefits [31].

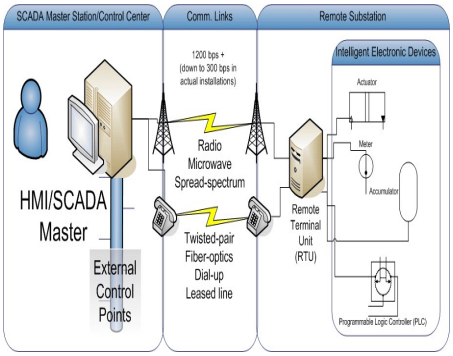

Figure 51: features of the SCADA [11]

One key aspect of advanced SCADA applications in power systems is their ability to facilitate real-time monitoring and control of diverse devices and components across the entire grid. Through a network of sensors, intelligent electronic devices (IEDs), and

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

communication infrastructure, SCADA systems gather and process data from various points within the power network. This real-time data acquisition allows operators to have an accurate and up-to-date understanding of the grid's status, enabling prompt decision-making and response to dynamic changes [62].

Moreover, advanced SCADA applications are instrumental in implementing advanced control strategies to optimize the operation of power systems. These strategies include automatic generation control, load shedding, and optimal power flow, among others. By leveraging advanced algorithms and predictive analytics, SCADA systems can dynamically adjust the operating parameters of generators, transformers, and other grid elements to maintain stability, enhance energy efficiency, and minimize losses [63].

The integration of advanced communication protocols and cyber-security features is another crucial dimension of SCADA applications in power systems [47]. As power grids become more interconnected and reliant on digital communication, ensuring the security and reliability of data transmission is paramount. Advanced SCADA systems employ robust encryption methods, firewalls, and intrusion detection systems to safeguard critical infrastructure from cyber threats, thereby bolstering the overall resilience of the power grid [26].

The advanced SCADA applications in power systems represent a paradigm shift in the way we monitor, control, and secure electrical grids [64]. Through real-time data acquisition, advanced control strategies, cyber-security measures, and support for renewable energy integration, these applications contribute significantly to the overall efficiency, reliability, and sustainability of modern power systems. As technology continues to advance, the role of SCADA in power systems is likely to evolve further, shaping the future landscape of energy management and grid operation [65].

Recent Developments in SCADA Technologies

In recent years, the SCADA has witnessed significant advancements, propelled by the integration of cutting-edge technologies, [4]. One of the most notable trends is the incorporation of Artificial Intelligence (AI) in anomaly detection within SCADA systems. AI-driven anomaly detection enhances the ability of SCADA systems to identify irregularities and potential threats by learning from historical data patterns [31]. This proactive approach not only improves the overall security posture of critical infrastructure but also allows for more efficient and timely responses to emerging issues.

The authors in Large PV power plants' predictive maintenance plans are dependent on accurate, consistent, and trustworthy data from the SCADA system. There is an identification of every required SCADA component that produces and transmits operational data. The suitability of standard SCADA communication protocols and topologies for big photovoltaic power plants is contrasted with their beneficial effects on the creation of predictive maintenance plans. In the context of predictive maintenance strategy, key performance indicators are established for creating actual operational trends, which are then compared to expected or designed operating trends. Redundancy instruments and techniques for mitigating cyberattack risks are offered to enhance the dependability and security of the SCADA system [34].

Mitigating Cyber Threats and Enhancing System Resilience in Power System Network

SCADA in mitigating cyber threats and enhancing system resilience is of paramount importance in today's interconnected and digitized industrial landscape. SCADA systems play a critical role in monitoring and controlling various industrial processes, from manufacturing to critical infrastructure such as power plants and water treatment facilities. As these systems become increasingly sophisticated, so do the challenges posed by cyber threats [18].

One key aspect of evaluating SCADA's effectiveness in addressing cyber threats lies in its ability to provide robust cyber-security measures. Advanced applications of SCADA should incorporate state-of-the-art encryption protocols, authentication mechanisms, and intrusion detection systems to safeguard against unauthorized access and

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

malicious activities. Regular vulnerability assessments and penetration testing are essential components of this assessment, ensuring that potential weaknesses are identified and addressed proactively [61].

Moreover, the integration of anomaly detection algorithms within SCADA systems is crucial for early detection of cyber threats. These algorithms analyse system behavior and network traffic patterns to identify deviations from normal operations, enabling rapid response to potential security incidents. The effectiveness of such advanced applications can be measured by their ability to not only detect anomalies but also autonomously respond to mitigate the impact of cyber threats, minimizing downtime and potential damage [66].

RESILIENCE STRATEGIES OF SCADA IN POWER SYSTEM NETWORKS

Resilience strategies play a crucial role in ensuring the robustness and reliability of SCADA systems in power system networks. SCADA systems are integral components of modern power grids, responsible for monitoring, controlling, and managing various aspects of the electrical infrastructure. As power systems face an increasing number of cyber threats, natural disasters, and other challenges, the development and implementation of effective resilience strategies for SCADA become paramount [14].

One key resilience strategy involves the integration of advanced cyber-security measures. As SCADA systems are vulnerable to cyber-attacks that can disrupt operations and compromise data integrity, implementing robust cyber-security protocols is essential. This includes regular security audits, the use of encryption technologies, and continuous monitoring for unusual activities. Additionally, the deployment of intrusion detection and prevention systems can help identify and mitigate potential threats before they escalate [31]. Another critical aspect of SCADA resilience is redundancy in both hardware and communication pathways. Redundancy ensures that if one component fails, there are backup systems in place to seamlessly take over operations. This can be achieved through the use of duplicate servers, communication channels, and data storage systems. Redundancy not only enhances the reliability of SCADA systems but also minimizes downtime in the event of a failure, contributing to the overall resilience of the power.

Various Strategies Employed to Enhance Resilience in Power Systems

Enhancing resilience in power systems is a multifaceted challenge that requires a comprehensive approach encompassing various strategies. One key strategy involves investing in advanced monitoring and control technologies. Implementing state-of-the-art sensors and communication systems enables real-time data collection and analysis, allowing operators to detect issues promptly and take corrective actions to prevent system failures. This proactive approach significantly contributes to the overall resilience of the power grid [26]. Diversification of energy sources is another crucial strategy to bolster the resilience of power systems. Relying on a mix of renewable energy, traditional power generation, and energy storage helps mitigate the impact of disruptions in any single source. This diversified portfolio enhances the system's ability to withstand fluctuations in supply and demand, as well as external shocks such as natural disasters or cyber-attacks [60].

Investments in grid modernization and infrastructure upgrades form a fundamental pillar in enhancing power system resilience. Upgrading aging components, integrating smart grid technologies, and reinforcing critical infrastructure ensure that the power grid can adapt to evolving challenges. The incorporation of advanced materials and construction techniques also contributes to the overall robustness of the system, making it more resilient to both expected and unexpected stressors.

Resilience frameworks, in the context of power systems, involve strategies and technologies designed to ensure the grid's ability to withstand and recover from disturbances, such as natural disasters, cyber-attacks, or equipment failures. Advanced SCADA applications contribute to resilience by offering predictive analytics that can anticipate

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

potential threats and vulnerabilities, allowing for proactive measures to be taken. This predictive capability empowers utilities to implement preventive maintenance, thereby reducing the risk of system failures and minimizing downtime [61].

Implementation of Advanced SCADA Applications has Improved System Resilience

The implementation of advanced Supervisory Control and Data Acquisition (SCADA) applications has proven instrumental in enhancing system resilience across various industries. One notable case study involves the integration of advanced SCADA systems in the energy sector. In this scenario, utilities have successfully utilized sophisticated SCADA applications to monitor and control their power generation, transmission, and distribution networks. These systems enable real-time data acquisition, analysis, and decision-making, contributing significantly to the reliability and resilience of the overall energy infrastructure [3]. Another compelling case study highlights the impact of advanced SCADA applications in the transportation industry. In the realm of smart transportation systems, SCADA technology has been employed to optimize traffic flow, manage public transportation networks, and enhance overall operational efficiency. By leveraging advanced data analytics and control capabilities, cities have witnessed a notable improvement in the resilience of their transportation systems, leading to reduced congestion, improved safety, and better response to unforeseen events [14].

Best Practices for Implementation of Cyber-Security in Power Systems through Advanced SCADA Applications

Implementing cyber-security in power systems through advanced SCADA applications is crucial for protecting critical infrastructure against evolving threats. A key practice involves conducting comprehensive risk assessments tailored to identify potential vulnerabilities and threats specific to SCADA systems. This enables the development of targeted security measures to mitigate risks effectively. Adopting a defence-in-depth strategy is essential, involving multiple layers of security controls such as firewalls, intrusion detection systems, and network segmentation. These measures create a robust security posture capable of withstanding diverse cyber threats. Regular training programs for personnel are also vital, equipping them with knowledge on current threats and effective response procedures to defend against social engineering and other attacks.

The Integration of Advanced SCADA Applications into Existing Power Systems.

Integrating advanced SCADA applications into existing power systems requires a systematic approach to ensure seamless operation, enhanced reliability, and improved efficiency. Implementing a set of best practices is essential to mitigate potential challenges and maximize the benefits of incorporating advanced SCADA technology. The following guidelines outline key considerations for a successful integration [4], [14], [29]

i. Comprehensive System Analysis:

Before integration, conduct a thorough analysis of the existing power system architecture. Identify critical components, communication protocols, and potential points of failure. Understanding the current state of the system is crucial for designing a seamless integration plan.

ii. Interoperability Standards:

Adhere to industry-standard communication protocols and interoperability standards to facilitate seamless integration with existing power system components. This ensures compatibility, reduces integration complexities, and allows for the incorporation of diverse SCADA applications.

iii. Cyber-security Measures:

Prioritize cyber-security throughout the integration process to safeguard against potential threats and vulnerabilities. Implement robust security protocols, encryption mechanisms, and access controls to protect sensitive data and maintain the integrity of the power system.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

Interoperability, Scalability, and Cost-Effectiveness of SCADA in Power Systems Networks

Interoperability, scalability, and cost-effectiveness are key factors influencing SCADA systems' effectiveness in power systems [45]. Interoperability ensures that diverse components from various vendors can communicate seamlessly, enhancing reliability and integrating new technologies smoothly. Scalability allows SCADA systems to adapt to power network expansions or modifications without compromising performance, ensuring robustness and responsiveness. Cost-effectiveness focuses on optimizing both initial and ongoing expenses, ensuring economic viability through efficient resource utilization and streamlined processes [22].

Regulatory Considerations

SCADA systems are crucial for the efficient and reliable operation of power systems, but they must comply with numerous regulatory considerations to safeguard critical infrastructure. Cyber-security is a key regulatory focus, with frameworks mandating measures to protect SCADA systems from cyber threats, ensuring compliance with industry standards and best practices [14]. Interoperability is also emphasized, guiding the development of SCADA systems to ensure seamless integration of diverse components from various vendors.

Existing Regulatory Frameworks Related to Cyber-Security in Power Systems.

Analyzing existing regulatory frameworks for cyber-security in power systems is crucial for ensuring the resilience and reliability of critical infrastructure. These frameworks, which vary across jurisdictions, often establish mandatory cyber-security standards for power utilities, outlining specific requirements for protecting critical assets. Compliance is monitored and enforced by regulatory authorities to ensure robust cyber-security measures. Information sharing and collaboration among stakeholders are also emphasized to foster a comprehensive understanding of emerging threats. Additionally, frameworks require regular risk and vulnerability assessments and mandate prompt incident reporting to enable swift, coordinated responses. As technology evolves, regulatory frameworks must adapt to integrate advanced technologies and address new cyber-security challenge.

Recommendations for Updating Regulations to Accommodate Advanced SCADA Technologies.

Given the rapid advancements in SCADA technologies, comprehensive regulatory updates are essential to ensure their relevance and effectiveness. Establishing a task force of industry experts, regulatory bodies, and technology innovators is recommended to identify gaps and outdated provisions in current SCADA regulations. Regulations should adopt flexible, technology-neutral language, focusing on performance-based standards to accommodate future innovations. Enhanced cyber-security measures, including encryption standards and regular vulnerability assessments, are crucial to mitigate cyber threats. Privacy protections must be emphasized, ensuring stringent data protection and transparency requirements. The updated regulations should balance data utilization for operational improvements with the safeguarding of individual privacy rights. These recommendations aim to create a collaborative, adaptable, and security-centric regulatory framework. By addressing these key areas, SCADA technologies can be integrated responsibly and effectively, mitigating risks and protecting privacy.

CHALLENGES AND FUTURE DIRECTIONS IMPLEMENTING ADVANCED SCADA APPLICATIONS

SCADA technologies are essential for managing power systems but face significant challenges, particularly in cyber-security and integrating renewable energy. As power systems become more interconnected, robust cyber-security measures are crucial to protect against threats. Integrating renewable energy sources like solar and wind introduces complexities that require advanced algorithms and real-time data analytics. Upgrading aging SCADA infrastructure to meet modern demands without disrupting operations is also

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

challenging. Embracing AI, machine learning, and edge computing, along with standardizing protocols, can enhance SCADA systems' adaptability, security, and efficiency.

CONCLUSION

SCADA technologies are crucial in power systems for monitoring, controlling, and managing infrastructure, significantly enhancing efficiency, reliability, and safety. They provide real-time monitoring for quick fault detection and enable remote control and automation, increasing system resilience.

Summary of key findings from the literature review.

The literature review on enhancing resilience and cyber-security in power systems through advanced SCADA applications reveals the critical importance of addressing evolving cyber threats. Advanced SCADA systems provide real-time monitoring and control, enabling prompt detection and response to cyber threats. Key measures include implementing intrusion detection, anomaly detection algorithms, and multi-layered defense strategies with encryption, access controls, and secure communication protocols.

SUGGESTIONS FOR FUTURE WORK

Enhancing resilience and cyber-security in power systems through advanced SCADA (Supervisory Control and Data Acquisition) applications is vital in today's interconnected energy infrastructure. Comprehensive strategies must address cyber threats to ensure robust power systems.

Continuous research and development are essential to stay ahead of emerging cyber threats. Collaboration among academia, industry experts, and government agencies is crucial to identify vulnerabilities and implement effective countermeasures, fortifying SCADA system resilience. Integrating artificial intelligence and machine learning technologies can significantly enhance cyber-security.

REFERENCE

[1] N. Society, O. F. Engineers, and M. Branch, "Transmission Company of Nigeria," no. June, 2011.

[2] K. Peddakapu, P. Srinivasarao, M. R. Mohamed, Y. Arya, and D. J. Krishna Kishore, "Stabilization of frequency in Multi-Microgrid system using barnacle mating Optimizer-based cascade controllers," *Sustain. Energy Technol. Assessments*, vol. 54, no. September, p. 102823, 2022, doi: 10.1016/j.seta.2022.102823.

[3] S. Angayarkanni, L. Aruna, R. Aswini, C. Deepa, and J. Kowsalya, "Plc and Scada Based Distribution and Substation Automation," *Int. Res. J. Eng. Technol.*, vol. 05, no. 03, pp. 3–6, 2018, [Online]. Available: www.irjet.net

[4] A. T. Jaiad, "Detecting the rate of growing electrical energy loads using," vol. 14, no. April 2022, pp. 2041–2048, 2023.

[5] R. B. Roy, "Application of SCADA for Controlling Electrical Power System Network," *UITS J.*, vol. 1, no. 2, pp. 85–97, 2003.

[6] "Transmission Company of Nigeria Scada / Ems".

[7] R. Perez, M. Rivera, P. Wheeler, G. Mirzaeva, E. E. Espinosa, and J. A. Rohten, "Microgrid Power Sharing Framework for Software Defined Networking and Cybersecurity Analysis," *IEEE Access*, vol. 10, no. August, pp. 111389–111405, 2022, doi: 10.1109/ACCESS.2022.3215434.

[8] S. Leonori, M. Paschero, F. M. Frattale Mascioli, and A. Rizzi, "Optimization strategies for Microgrid energy management systems by Genetic Algorithms," *Appl. Soft Comput. J.*, vol. 86, p. 105903, 2020, doi: 10.1016/j.asoc.2019.105903.

[9] P. Denholm *et al.*, "The challenges of achieving a 100% renewable electricity system in the United States," *Joule*, vol. 5, no. 6, pp. 1331–1352, 2021, doi: 10.1016/j.joule.2021.03.028.

[10] P. Maynard, K. McLaughlin, and B. Haberler, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," no.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

January, 2014, doi: 10.14236/ewic/ics-csr2014.5.

[11] Q. S. Qassim *et al.*, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *Int. J. Eng. Technol.*, vol. 7, no. 2.14 Special Issue 14, pp. 153–159, 2018, doi: 10.14419/ijet.v7i2.14.12816.

[12] P. György and T. Holczer, "Attacking IEC 60870-5-104 protocol," *CEUR Workshop Proc.*, vol. 2874, pp. 140–150, 2021.

[13] M. H. Elkholy, M. Elymany, H. Metwally, M. A. Farahat, T. Senjyu, and M. Elsayed Lotfy, "Design and implementation of a Real-time energy management system for an isolated Microgrid: Experimental validation," *Appl. Energy*, vol. 327, no. July, p. 120105, 2022, doi: 10.1016/j.apenergy.2022.120105.

[14] K. Mai, X. Qin, N. Ortiz Silva, and A. A. Cardenas, "IEC 60870-5-104 network characterization of a large-scale operational power grid," *Proc. - 2019 IEEE Symp. Secur. Priv. Work. SPW 2019*, pp. 236–241, 2019, doi: 10.1109/SPW.2019.00051.

[15] S. Sri, K. Kumar, G. Satheesh Kumar, and K. R. Sugavanam, "Intelligent Load Monitoring System of 11KV/440V Multi Distribution Transformers Using SCADA," *Int. J. Pure Appl. Math.*, vol. 119, no. 15, pp. 829–835, 2018.

[16] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016, doi: 10.1109/ACCESS.2016.2549047.

[17] R. L. Samson, T. F. Infante, R. D. S. Manzon, and M. John, "Strategical Application of Scada in Feeder 2 of an Electric Utility," vol. 6, no. 11, pp. 762–767, 2023.

[18] Q. Qassim, N. Jamil, M. Daud, N. Ja, and H. C. Hasan, "A Security Assessment Model for Electrical Power Grid SCADA System," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12S2, pp. 763–773, 2019, doi: 10.35940/ijitee.l1132.10812s219.

[19] J. L. Torres-Madroñero, C. Nieto-Londoño, and J. Sierra-Pérez, "Hybrid energy systems sizing for the colombian context: A genetic algorithm and particle swarm optimization approach," *Energies*, vol. 13, no. 21, pp. 1–30, 2020, doi: 10.3390/en13215648.

[20] G. Troops and O. Optimized, "Hybrid DC – AC Microgrid Energy Management System Using," *Energies*, vol. 15, no. 21, p. 8187, 2022, doi: https://doi.org/10.3390/en15218187.

[21] D. Prasad and C. Dhanamjayulu, "A Review of Control Techniques and Energy Storage for Inverter-Based Dynamic Voltage Restorer in Grid-Integrated Renewable Sources," *Math. Probl. Eng.*, vol. 2022, pp. 1–43, 2022, doi: 10.1155/2022/6389132.

[22] M. Behnert and T. Bruckner, "Causes and effects of historical transmission grid collapses and implications for the German power system," *Beiträge des Instituts für Infrastruktur und Ressourcenmanagement*, vol. No. 03/201, p. 19, 2018.

[23] A. Liu, J. Liu, and Q. Wu, "Improvement of VSG Transient Performance Based on Power Feedforward Decoupling Control," *IET Gener. Transm. &Distribution*, vol. 10, no. 10, pp. 1–27, 2022, doi: 10.1049/gtd2.12574.

[24] P. Roy *et al.*, "Techno-economic evaluation for hybrid renewable energy system: Application and merits," *Renew. Sustain. Energy Rev.*, vol. 42, no. 1, pp. 318–327, 2019, doi: 10.1016/j.rser.2015.12.223.

[25] A. Sabo *et al.*, "Artificial Intelligence-Based Power System Stabilizers for Frequency Stability Enhancement in Multi-Machine Power Systems," *IEEE Access*, vol. 9, pp. 166095–166116, 2021, doi:

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

10.1109/ACCESS.2021.3133285.

[26] L. Erdodi, P. Kaliyar, S. H. Houmb, A. Akbarzadeh, and A. J. Waltoft-Olsen, "Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104," in *ACM International Conference Proceeding Series*, 2022, pp. 1–10. doi: 10.1145/3538969.3544475.

[27] N. S. V. Rao, C. Y. T. Ma, F. He, D. K. Y. Yau, and J. Zhuang, "Cyber-physical correlation effects in defense games for large discrete infrastructures," *Games*, vol. 9, no. 3, pp. 1–24, 2018, doi: 10.3390/g9030052.

[28] C. Prochaska and A. Zouboulis, "A mini-review of urban wastewater treatment in Greece: History, development and future challenges," *Sustain.*, vol. 12, no. 15, 2020, doi: 10.3390/su12156133.

[29] C.-I. Toma, M. Popescu, M. D. Constantinescu, and I. C. Popa, "Application of Electrical Substation, Ring Topology versus Star Topology," *Ann. Univ. Craiova Electr. Eng. Ser.*, vol. 46, no. 46, pp. 63–68, 2022, doi: 10.52846/aucee.2022.10.

[30] A. Adewuyi, "Challenges and prospects of renewable energy in Nigeria: A case of bioethanol and biodiesel production," *Energy Reports*, vol. 6, no. xxxx, pp. 77–88, 2020, doi: 10.1016/j.egyr.2019.12.002.

[31] A. B. Abdulsalam, H. A. J. Alsaadi, and Z. Hamodat, "Control And Management of Solar PV Grid Using Scada System," *HORA 2022 - 4th Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc.*, no. June 2022, pp. 9–11, 2022, doi: 10.1109/HORA55278.2022.9799994.

[32] A. M. Zaw and H. M. Tun, "Design and Implementation of SCADA System Based Power Distribution for Primary Substation (Monitoring System)," *Int. J. Sience, Eng. Technol. Res.*, vol. 3, no. 5, pp. 1542–1546, 2014.

[33] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSI Trans. ICT*, vol. 1, no. 2, pp. 135–141, 2013, doi: 10.1007/s40012-013-0013-5.

[34] M. E. Master *et al.*, "Technische Hochschule Ingolstadt Faculty of Mechanical Engineering Master of Science in Renewable Energy Systems Master ' s Thesis Comparison of SCADA Systems and Their Effect on Predictive Maintenance Strategies in Large PV Power Plants," Technische Hochschule Ingolstadt Faculty, 2023. [Online]. Available: https://www.thi.de/en/

[35] H. Karimipour and V. Dinavahi, "Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack," *IEEE Access*, vol. 6, no. December 2017, pp. 2984–2995, 2017, doi: 10.1109/ACCESS.2017.2786584.

[36] H. Hui, Y. Chen, S. Yang, H. Zhang, and T. Jiang, "Coordination control of distributed generators and load resources for frequency restoration in isolated urban microgrids," *Appl. Energy*, vol. 327, no. March, p. 120116, 2022, doi: 10.1016/j.apenergy.2022.120116.

[37] Y. Xu, "A review of cyber security risks of power systems: from static to dynamic false data attacks," *Prot. Control Mod. Power Syst.*, vol. 5, no. 1, 2020, doi: 10.1186/s41601-020-00164-w.

[38] K. E. Hemsley, R. E. Fisher, Kevin E. Hemsley;, and Dr. Ronald E. Fisher, "History of Industrial Control System Cyber Incidents," *INL/CON-18-44411-Revision-2*, no. December, pp. 1–37, 2018, [Online]. Available: https://www.osti.gov/servlets/purl/1505628

[39] A. Shamshad, M. T. Riaz, A. Raza, and M. A. Khan, *An Intelligent Automation of Power Transformer using PLC and SCADA at Substation*,

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

vol. 1, no. 1. Association for Computing Machinery, 2023. doi: 10.1145/3593434.3594242.

[40] T. Zhou, J. Sun, H. Quan, D. Zou, and Q. Peng, "Oscillation Source Location of Ultra-low Frequency Oscillations Based on Random Forest Algorithm," *Proc. Int. Conf. Cyber-Physical Soc. Intell. ICCSI 2022*, pp. 460–465, 2022, doi: 10.1109/ICCSI55536.2022.9970595.

[41] C. A. Buckner *et al.*, "Combining Supervisory Control and Data Acquisition (SCADA) with Artificial Intelligence (AI) as a Video Management System," *Intech*, vol. 11, no. tourism, p. 13, 2016, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics

[42] A. Panda, A. K. Dauda, H. Chua, R. R. Tan, and K. B. Aviso, "Recent advances in the integration of renewable energy sources and storage facilities with hybrid power systems," *Clean. Eng. Technol.*, vol. 12, no. January, p. 100598, 2023, doi: 10.1016/j.clet.2023.100598.

[43] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, 2017, doi: 10.1145/3098954.3103166.

[44] N. Baranović, P. Andersson, I. Ivanković, K. Žubrinić-Kostović, D. Peharda, and J. E. Larsson, "Experiences from intelligent alarm processing and decision support tools in smart grid transmission control centers," *CIGRE Sess. 46*, vol. 2016-Augus, no. August, 2016.

[45] P. Sarajcev, A. Kunac, G. Petrovic, and M. Despalatovic, "Artificial Intelligence Techniques for Power System Transient Stability Assessment," *Energies*, vol. 15, no. 2, 2022, doi: 10.3390/en15020507.

[46] M. S. Shahriar *et al.*, "Stability improvement of the PSS-connected power system network with ensemble machine learning tool," *Energy Reports*, vol. 8, pp. 11122–11138, 2022, doi: 10.1016/j.egyr.2022.08.225.

[47] K. Chauhan, A. Bhut, J. Brahmbhatt, and S. Dalia, "Substation Automation Using Plc and," *J. Emerg. Technol. Innov. Res.*, vol. 5, no. 11, pp. 923–930, 2018.

[48] A. Amir, H. Shareef, and F. Awwad, "Energy Management in a Standalone Microgrid: A Split-Horizon Dual-Stage Dispatch Strategy," *Energies*, vol. 16, no. 8, 2023, doi: 10.3390/en16083400.

[49] S. J. Pinto and P. Siano, "Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection," 2023.

[50] F. Almutairy, "Enhancing Cybersecurity of Power Systems using Machine Enhancing Cybersecurity of Power Systems using Machine Learning," 2022.

[51] A. Kpoze, J. Degila, A. Ahouandjinou, P. Houngue, H. Soude, and S. F. Wamba, "Cybersecurity Risk Assessment for Beninese Power Grid SCADA system," *Proc. - 2023 IEEE Int. Conf. Cryptogr. Informatics, Cybersecurity Cryptogr. Cybersecurity Roles, Prospect. Challenges, ICoCICs 2023*, no. August, pp. 320–326, 2023, doi: 10.1109/ICoCICs58778.2023.10277307.

[52] P. Wlazlo *et al.*, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Physical Syst. Theory Appl.*, vol. 6, no. 3, pp. 164–177, 2021, doi: 10.1049/cps2.12014.

[53] P. Radoglou-grammatikis, P. Sarigiannidis, and I. Giannoulakis, "Attacking IEC-60870-5-104 SCADA Systems," 2019, doi: 10.1109/services.2019.00022.The.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna

[54] C. Korzeniowski and D. Morano, "Security and Mitigation of Powergrid and SCADA system against Cyber attacks," no. May, 2020.

[55] A. Fayyad, A. Abdel Gawad, S. Saleh, and A. Alenany, "IoT based Fourth Generation SCADA System for High Voltage Networks Fault Diagnosis based on BSDT-ANN," *Egypt. Int. J. Eng. Sci. Technol.*, vol. 41, no. 3, pp. 75–91, 2023, doi: 10.21608/eijest.2022.144314.1161.

[56] T. Kovanen, V. Nuojua, and M. Lehto, "Cyber threat landscape in energy sector," *Proc. 13th Int. Conf. Cyber Warf. Secur. ICCWS 2018*, vol. 2018-March, no. December, pp. 353–361, 2018.

[57] S. H. C. Cherukuri, B. Saravanan, and G. Arunkumar, "Experimental evaluation of the performance of virtual storage units in hybrid micro grids," *Int. J. Electr. Power Energy Syst.*, vol. 114, no. February 2019, p. 105379, 2020, doi: 10.1016/j.ijepes.2019.105379.

[58] O. D. T. Odou, R. Bhandari, and R. Adamou, "Hybrid off-grid renewable power system for sustainable rural electrification in Benin," *Renew. Energy*, vol. 145, pp. 1266–1279, 2020, doi: 10.1016/j.renene.2019.06.032.

[59] A. S. Alghamdi, "Optimal Power Flow of Hybrid Wind/Solar/Thermal Energy Integrated Power Systems Considering Costs and Emissions via a Novel and Efficient Search Optimization Algorithm," *Appl. Sci.*, vol. 13, no. 8, 2023, doi: 10.3390/app13084760.

[60] L. Salazar, N. Ortiz, X. Qin, and A. A. Cardenas, "Towards a High-Fidelity Network Emulation of IEC 104 SCADA Systems," *CPSIOTSEC 2020 - Proc. 2020 Jt. Work. CPS IoT Secur. Priv.*, pp. 3–12, 2020, doi: 10.1145/3411498.3419969.

[61] F. Quader and V. P. Janeja, "Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies," *J. Cybersecurity Priv.*, vol. 1, no. 4, pp. 638–659, 2021, doi: 10.3390/jcp1040032.

[62] A. M. Ewais, A. M. Elnoby, T. H. Mohamed, M. M. Mahmoud, Y. Qudaih, and A. M. Hassan, "Adaptive frequency control in smart microgrid using controlled loads supported by real-time implementation," *PLoS One*, vol. 18, no. 4, p. e0283561, 2023, doi: 10.1371/journal.pone.0283561.

[63] T. Z. Ang, M. Salem, M. Kamarol, H. S. Das, M. A. Nazari, and N. Prabaharan, "A comprehensive study of renewable energy sources: Classifications, challenges and suggestions," *Energy Strateg. Rev.*, vol. 43, no. August, p. 100939, 2022, doi: 10.1016/j.esr.2022.100939.

[64] D. E. A. Mansour, *Energy storage technologies in mvdc microgrids*. Elsevier Inc., 2019. doi: 10.1016/B978-0-12-814560-9.00010-0.

[65] A. V. Kumar, S. Sharma, and A. Verma, "Optimal sizing and multi-energy management strategy for PV-biofuel-based off-grid systems," *IET Smart Grid*, vol. 3, no. 1, pp. 83–97, Feb. 2020, doi: 10.1049/iet-stg.2019.0178.

[66] C. H. Hariprasad, "Optimum Restructuring of Radial Distribution Network with Integration of DG and DSTATCOM using Artificial Fish Swarm Optimization Technique," in *Optimum Restructuring of Radial Distribution Network with Integration of DG and DSTATCOM using Artificial Fish Swarm Optimization Technique*, IEEE, 2022, pp. 4–6.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Technology, Kaduna