applied sciences

MDPI

Review

Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research

Norziana Jamil [1,*], Qais Saif Qassim [2,*], Farah Aqilah Bohani [3], Muhamad Mansor [4] and Vigna Kumaran Ramachandaramurthy [4]

[1] College of Computing & Informatics, Institute of Energy Infrastructure, Universiti Tenaga Nasional, Kajang 43000, Selangor, Malaysia

[2] College of Technology, University of Technology and Applied Sciences-Ibri, Ibri 511, Oman

[3] Institute of Energy Infrastructure, Universiti Tenaga Nasional, Kajang 43000, Selangor, Malaysia; Farahaqilahb@gmail.com

[4] Institute of Power Engineering, Universiti Tenaga Nasional, Kajang 43000, Selangor, Malaysia; Muhamadm@uniten.edu.my (M.M.); Vigna@uniten.edu.my (V.K.R.)

* Correspondence: Norziana@uniten.edu.my (N.J.); qais.aljanabi@ibrict.edu.om (Q.S.Q.)

Abstract: The infrastructure of and processes involved in a microgrid electrical system require advanced technology to facilitate connection among its various components in order to provide the intelligence and automation that can benefit users. As a consequence, the microgrid has vulnerabilities that can expose it to a wide range of attacks. If they are not adequately addressed, these vulnerabilities may have a destructive impact on a country's critical infrastructure and economy. While the impact of exploiting vulnerabilities in them is understood, research on the cybersecurity of microgrids is inadequate. This paper provides a comprehensive review of microgrid cybersecurity. In particular, it (1) reviews the state-of-the-art microgrid electrical systems, communication protocols, standards, and vulnerabilities while highlighting prevalent solutions to cybersecurity-related issues in them; (2) provides recommendations to enhance the security of these systems by segregating layers of the microgrid, and (3) identifies the gap in research in the area, and suggests directions for future work to enhance the cybersecurity of microgrids.

Keywords: vulnerability assessment; microgrid; smart grid; SCADA

check for updates

Citation: Jamil, N.; Qassim, Q.S.; Bohani, F.A.; Mansor, M.; Ramachandaramurthy, V.K. Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. *Appl. Sci.* **2021**, *11*, 9812. https://doi.org/10.3390/app11219812

Academic Editors: Amjad Anvari-Moghaddam, Somayeh Asadi, Behnam Mohammadi-Ivatloo and Mohammad Shahidehpour

Received: 22 August 2021
Accepted: 8 October 2021
Published: 20 October 2021

1. Introduction

Various definitions of the microgrid and designs of its functional classification have been provided in the literature. In general, a microgrid is defined as a small-scale electrical distribution system that links numerous customers to numerous sources of generation and storage, and uses power electronic devices as a medium [1]. The concept of the microgrid dates back to 1882 in proposals by Thomas Edison, whose company built the first 50 direct current (DC) power plants [2].

A microgrid comprises elements such as energy storage, loads, and generation systems [3]. The generation system in a microgrid receives its sources from renewable energy and conventional energy sources (hybrid system). Other elements such as storage play an essential role in supplying electrical energy to the end users because the microgrid's reliability is improved through storage. Storage is also employed to overcome the problem of excess power generated from wind turbines and photovoltaic (PV) systems.

Microgrids can be divided into two operational systems: isolated and grid connected. An isolated microgrid can produce energy supply in a reliable condition in a small area, and can be used as a valuable testbed for suitable control function development. The use of grid-connected microgrids, on the other hand, is more widespread in supporting distribution networks that incorporate renewable energy sources (RES) and distributed generation (DG) units [4].

A microgrid system is a promising solution for handling power supply to loads with reliable power consumption. Some of the parameters to be considered in elements of the microgrid, such as the architecture of the communication system, protocols, and tools, are stability, reliability, and optimal operation [5].

Ensuring reliable communication among microgrids is not an easy task. Factors influencing the reliability of microgrid communication include the interface for communication among components, control requirements, resilience of the microgrid, its topology, geographical extension, and mode of operation, protection schemes for it, the technology of inverter-based distributed energy resources (DER), and reliability requirements [6].

Microgrid electrical systems were initially proposed to address energy supply issues in rural areas. Supplying energy to villages is costly and technically challenging because they are far from centralized electrical grid. The microgrid is an essential aspect in large-scale applications of the smart grid. It is a necessary part of a smart grid the main objective of which is to provide a reliable and safe means of electricity distribution by using intelligent and automated technologies.To maintain the reliability requirement, microgrid integrates various information and communication technologies in its legacy physical system. While the integration of operational (physical) technology and information technology provides more advancement and sophistication to the microgrid in terms of its operation, control, performance, connectivity and delivery, it opens up microgrid to a wider surface for cyber threats. As a result, the microgrid has security vulnerabilities i.e., the interconnectivity to the cyber system in microgrid brings more challenges to maintain resiliency as hackers might exploit vulnerabilities that lie in the physical system that has been long used without any patching or update for increasing protection being implemented. Some of the challenges or cyber threats to microgrid include false data injection [7], denial of service attack [8] and signal spoofing attack [9]. To the best of our knowledge, research on microgrid cybersecurity is inadequate. Vulnerabilities in microgrid and cyber-threats to them must be studied and understood thoroughly through a comprehensive and systematic literature review. This is the motivation of this paper.

The remainder of this paper is organised as follows: Section 2 provides a basic understanding of the components of a microgrid as well as such elements as microgrid architecture, communication systems and microgrid communication protocols. Section 3 then discusses the cybersecurity-related aspects of microgrids that include vulnerabilities and potential security issues to them. Finally, Section 4 discusses the challenges to microgrid security and the research opportunities that can be explored.

2. The Microgrid Architecture

To understand the threats posed to and vulnerabilities of microgrid electrical systems, this section provides a quick overview of the elements and components of a microgrid. A considerable number of studies have affirmed that the operation and data processing, transmission, and storage of microgrids must be secure to achieve reliable control [10,11]. The fundamental elements and components of a microgrid are discussed below.

The reference architecture of microgrid used in this research is given in [12]. To discuss the cybersecurity aspects of microgrid, the components of microgrid are categorized into four enclaves based on their functions: (i) distributed generation (DG) sources, (ii) energy storage, (iii) the distribution system and (iv) control and communication modules., as depicted in Figure 1.

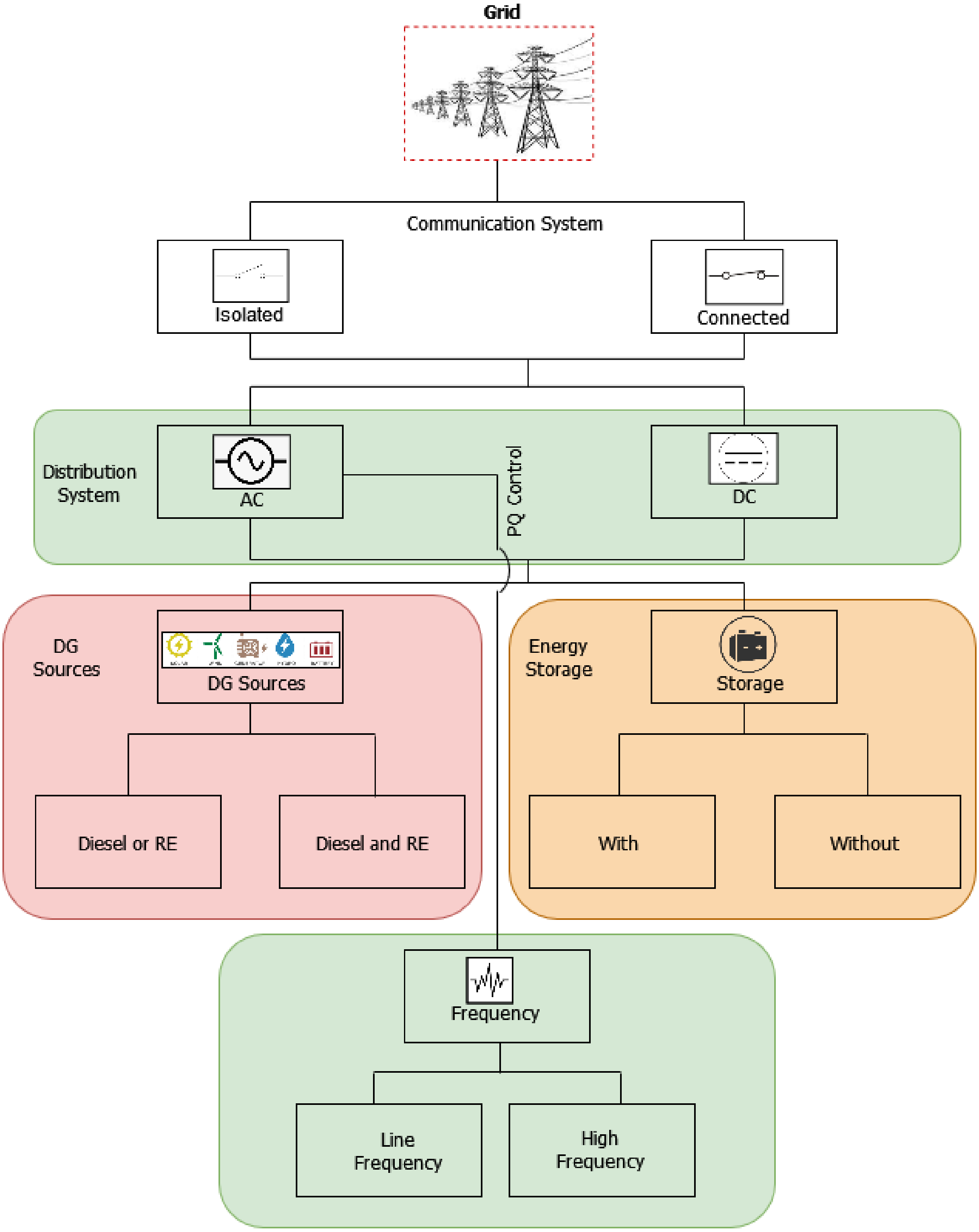

Figure 1. Microgrid architecture with enclaves.

The description of every enclave is given below:

(A) Enclave 1: DG sources
DG source refers to technologies that generate power such as:

- Generator
One of the sources of energy to a microgrid is the synchronous generator. Most of them are powered by natural gas or a diesel engine designed for stand-

alone or backup applications. A generator has two control algorithms, namely, an (1) exciter, which handles the voltage of the generator, and the (2) reactive power generator that is commonly used to minimise power loss and improve the voltage profile of power systems.

- Natural gas turbine
  The natural gas turbine is categorised based on the drive type, into single shaft and two shaft. The single-shaft light is generally used in microgrid systems as a distributed resource. To enhance the response speed, the governor control system uses an electronic control system. The gain and time are constantly monitored to achieve a reasonable response.
- Renewable energy source
  Renewable energy plays an essential role in maintaining the sustainability and survival of the microgrid. The prevalent sources of renewable energy are wind and photovoltaic. They are connected to the microgrid system through current-mode inverters, and can be operated at the maximum power point.

(B) Enclave 2: Energy storage
The reliability of the operations, power generation, and load stabilisation of the microgrid is ensured through a sophisticated storage management system, an indispensable element of the microgrid. Disturbances in power supply may occur in the grid due to variations in the load in terms of a mismatch between load generation and load time. Mechanical wear and failure of the battery are some other causes of a terminal voltage fault. Energy storage in microgrid architecture refers to devices that perform the following functions [12]:

(a) Balances the power in microgrid despite of load fluctuation and other transients.
(b) Provides ride-through capability and allows DGs to operate as dispatchable units during dynamic variations in intermittent energy sources.
(c) Provides the initial energy during the transition between grid connected or/from microgrid island.

Maintaining the stability of the microgrid is a challenging task because the system has various types of distributed generation, and demands for reactive and active power based on the needs of customers. Thus, the energy storage management system of the microgrid plays a vital role in stabilising its frequency and voltage for both the short and the long term [13]. The energy storage is connected to the grid through a micro-source, and absorbs power via the electronic converter. Subsequently, the energy storage exports power to the network in the island mode, enhancing the system's quality and stability [14]. The energy storage can be distributed via two applications: utilisation-scale and small-scale applications. Other than maintaining the management and control function of the storage device, the distributed energy storage system can help maintain maximal system safety, efficiency, and life. It also performs communication with the Supervisory Control and Data Acquisition (SCADA) system in larger management applications.

(C) Enclave 3: the distribution system
Distribution systems refers to transmission and distribution technologies, specifically line frequency AC, high frequency AC and DC technologies, whose main role is to transmit and distribute electricity in microgrid systems.

(D) Enclave 4: control and communication system
Control and communication system in microgrid architecture refers to technologies that handle the output data from microgrid and deliver them for further analysis by different applications, and microgrid controls and management. Two communication media, i.e., wired and wireless, support the communication technologies for power control and protection.
Microgrid controls and management includes:

- Microgrid Central Controller (MGCC)
  The MGCC facilitates communication between the Distribution Management System (DMS) and the microgrid to detect and control blackout procedures. The MGCC was also introduced to improve the voltage profile and handle tripping problems.
- Supervisory Control And Data Acquisition (SCADA)
  In a microgrid application, SCADA as a computer-based application plays an important role in acquiring data, and monitoring and controlling operations, including the adjustment of signal alarms. It also enhances the safety, reliability, and economic benefits of the microgrid, and reduces the burden on the dispatchers. Moreover, it employs the automation and modernisation of electrical power dispatch to improve the efficacy and level of information of the system [15].

2.1. Communication Protocols and Standards of Microgrid

To better understand microgrid communication protocols, research on the design of its communication network has focused on the interaction between several components of the microgrid for control and monitoring purposes. A review shows that numerous types of communication networks are used in microgrid systems, as depicted in Table 1. As standard communication protocols, the IEC 61850, Distributed Network Protocol 3.0 (DNP 3.0), Modbus, Profibus, Wi-Fi, and the TCP/IP are extensively used in microgrid operations [16–19]. We present a brief description of the commonly used communication protocols in microgrid electrical systems in the following subsections.

(A) IEC 61850
IEC 61850 is the most widely used standard of communication owing to its speed, excellent reliability, and security. The IEC 61850 standard is an international standard developed for substation automation. It is composed of three levels, namely, the process, bay, and substation. The IEC 61850 is built with different data attributes and functionalities to ensure interoperability, introducing some latencies in communication. This protocol is suitable to be applied in a microgrid, particularly in distribution automation [20].

(B) Modbus
As reported in [21], Modbus is widely used in microgrids due to its simplicity. It can be transmitted over the different physical networks of RS 485, RS 232, and the Ethernet TCP/IP. However, the Modbus protocol is inefficient for large-scale data transmission from/to the network. It has high latency, making it unsuitable for a communication system, especially one involving emergency control. Such microgrid architectures such as PrInCE Lab use hard-wired networks if long delays occur in communication [16].

(C) Distributed Network Protocol 3.0 (DNP3)
DNP3 is a power communication protocol originally developed by General Electric that was made public in 1993. Use in SCADA applications was the initial purpose for the design of DNP3. It is used mainly in the oil and gas, security, water infrastructure, and electrical industries in Asia, North America, South America, Australia, and South Africa [22]. The initial design of DNP3 comprises four layers: the transport, application, data link, and physical layers. Serial communication protocols such as the RS-232, RS-422, and RS-485 became the basis for designing the original physical layer. The DNP3 has been moved over to the TCP/IP layer to support current communication technologies. Therefore, it can be considered a three-layer network protocol that operates on the TCP/IP layer [22] in supporting end-to-end communication. Contrary to Modbus, the slave of DNP3 can produce feedback with unsolicited responses to the master. Single DNP3 messages can demonstrate time-stamped tasks and information on data quality and various data types [17].

Table 1. A summary of the advantages and limitations of microgrid communication protocols based on selected related works.

Study	Year	Media	Protocol	Advantages	Limitations
Korea- KEPRI Microgrid [18]	2014, 2017	Optical fiber	N.A.	High-speed communication, low latency time, high reliability	Cover short distances
Huatacondo [19]	2011	NA.	Modbus TCP/IP	Easy to implement, Low installation cost, Supported by different, communication links	High latency time
Am Steinweg [23]	2009	NA.	Modbus TCP/IP	Easy to implement, Low installation cost, Supported by different, communication links	High network delay; Low security level against cyber attacks
Kythnos [24]	2013, 2014	Power line	NA.	High speed communication, Adopts existing electrical, network, Low installation cost, High data transfer rate	Minimum security level, Data attenuation, Great amount of noise
Smart Polygeneration, Microgrid [22]	2013	NA.	IEC 61850	High reliability, High-speed communication, High security level, especially, against cyber attacks, High interoperability	Low redundancy level , High implementation cost, Requires change or upgrade of both, communication interface of already installed components and the existing IT network
DeMoTec [25]	2005	Ethernet	XLM-RPC	Improved reliability, Enhanced security level	High computational cost, High installation cost
Bornholm Island [24]	2014	Optical fiber	NA.	High-speed communication, Low latency time, High reliability	Cover short distances
NTUA [25]	2005	NA.	XLM	High operational flexibility, High readability	High load of communication challenges
BC Hydro [26]	2002, 2008	Telephone	NA.	Easy to be integrated	Low reliability, High implementation cost
University of Manchester, Microgrid [27]	2013	Power line	NA.	Adopts existing electrical, network, Low installation cost, High data transfer rate	Minimum security level, Data attenuation, Great amount of noise
Bronsbergen Holiday Park [27]	2013, 2009	GSM	NA.	High reliability, Cost effective	Limited transmission bandwidth
CESI Ricerca DER [28]	2013, 2009	Ethernet	NA.	High reliability	Low security level, High installation cost
CERTS [29]	2009, 2011, 2013	NA.	Modbus TCP/IP	Easy to implement, Low installation cost, Supported by different, communication links	High network delay, Low security level against cyber attacks
Sendai Project [24]	2014, 2014	GPS	NA.	Easy to integrate, Low installation cost, Global accessibility	Reduced accuracy, Low reliability due to battery life, Low security level, Low privacy.
Prince Lab [18]	2017	Ethernet	Modbus TCP/IP	Easy to implement, Low installation cost, Supported by different, communication links	High network delay, Low security level against cyber attacks, Involve partial upgrade and expansion of existing, IT network

DNP3 is to be replaced by IEC 61850 in substation communication. The general belief is that in future power systems, IEC 61850 has the potential for usage outside substation communication, although its use is presently limited within a power substation [30]. Due to the absence of any security mechanism in the initial design of DNP3 and IEC 61850, the microgrid network can easily intercept or falsify messages sent through them, resulting in either incorrect operation of power devices or information leakage. Two effective solutions were used as the basis for the design of the security functionality of DNP3 by [31]: (1) the introduction of security mechanisms to the DNP3 stack through the modification of the original protocol, and (2) the insertion of a security layer between the DNP3 protocol stack and the TCP/IP layer. The first solution offers suitable security solely for DNP3. Nonetheless, the protocol stack needs to be repeatedly modified while the communication systems in the power devices require upgrading. As such, the compatibility of legacy devices with smart grid devices can be more desirably achieved through the insertion of a security layer between the DNP3 and TCP/IP. This security layer aims to specifically assist the DNP3 protocol in attaining the primary security requirements for confidentiality and integrity. This is achieved through the interception of the DNP3 packets distributed to the TCP/IP layer by the security layer. The data are then encrypted, and the encrypted packets are then sent to the TCP/IP layer. All these are performed at the transmitter, the data packets are passed to the application layer (DNP3 layers) once the security layer has decrypted them. The confidentiality and integrity of DNP3 packets can be ensured through symmetric or asymmetric algorithms. In [32], for instance, MAC-based authentication was designed and implemented to function as an extension to the security of DNP3-based communication for distribution automation systems.

2.2. Cyberattacks on Microgrid

In general, the attack on and control over a system involves four steps: reconnaissance, scanning, exploitation, and maintaining access [33]. During reconnaissance, the attacker gathers information on the target. Scanning is the second step, where the attacker attempts to identify vulnerabilities in the system. These activities are intended to identify open ports and services that run on each port as well as their weaknesses. The exploitation involves the attacker attempting to compromise and gain complete control of the target. Before proceeding to maintain access, which is the final step, the administrative access enjoyed by the target needs to be achieved. Access is maintained by installing a hidden program in the system that enables the attacker(s) to return to the it in the future.

1. Reconnaissance
   Reconnaissance for attacks is carried out in the form of social engineering and traffic analysis. Social engineering (SE) relies on social skills and human interaction rather than technical skills. In this stage, the attacker uses communication and persuasion to win the trust of a legitimate user. This is done to obtain the user's credentials and confidential information, such as passwords or PIN numbers, to log on into a particular system. Some examples of popular techniques used in SE are phishing and password pilfering [33]. In a traffic analysis-based attack, the traffic is listened to and analysed to determine the device and hosts connected to the network, together with their IP addresses. In traffic analysis and social engineering, the compromise primarily involves confidential information.
2. Scanning
   Scanning is performed to identify live hosts and devices of the network. According to [33], there are four types of scans: those on ports, IPs, vulnerabilities, and services. Typically, an IP scan is conducted first to identify the hosts connected to the network together with their IP addresses. This is followed by the scanning of ports to identify an open port. Each host on the network is scanned. The attacker then performs a service scan to identify the system or service that operates behind each open port. For instance, if port 102 is detected as open on a system, the hacker can infer that this system is used for substation automation control or messaging. On the contrary, the phasor measurement unit (PMU) is the target system if port 4713 is open. Identifying vulnerabilities and

weaknesses related to each service on the target machine for further exploitation is the aim of the vulnerability scan, which is the final step of scanning.

The DNP3 and Modbus are two industrial protocols that are susceptible to scanning attacks. The Modbus/TCP is susceptible to an attack known as Modbus network scanning because it is designed for communication rather than security. In this attack, a benign message is sent to all devices connected to the network to collect information on them. An open Modbus/TCP is detected and slave IDs of the device together with their IP addresses are identified by Modscan, which is a SCADA Modbus network scanner [34]. Modscan scans the DNP3 protocol and determines the hosts: in particular, the slaves, their DNP3 addresses, and their corresponding master. It is thus clear that the target of these attacks is primarily confidential information on the smart grid.

3. Exploitation

   Exploitation features harmful activities to exploit the smart grid's vulnerable components and gain control of it. Popping the human–machine interface (HMI), Trojan horse, integrity violation, man-in-the-middle (MITM) attack, jamming the channel, privacy violation, worm, virus, replay attack, and DOS attack are examples of harmful activities. The infection attack on a particular system or device in a smart grid is performed using a program called the virus. On the contrary, a worm is a self-replicating program, and spreads by copying itself to infect other devices and systems by using the network. Another example involves a program that appears to carry out a legitimate task on the target system, yet operates a malicious code in the background; this is known as a Trojan horse. The attacker uses this form of malware to upload a worm or a virus to the target system [35]. The first cyberattack against a physical industrial control system was launched using Stuxnet.

4. Maintaining access

   Special forms of attack, including the backdoor, virus, and Trojan horse, are used in this final step to maintain permanent access to the target. The backdoor, which is an undetectable stealthy program, is installed on the target by the attacker for easier and faster use in the future. The successful embedding of a backdoor into the server of the SCADA control centre allows the attacker to launch several attacks against the power system that damage it. The security parameters of an IT network are classified based on their order of importance: confidentiality, integrity, accountability, and availability. However the order of precedence of the security parameters of a smart grid is as follows: availability, integrity, accountability, and confidentiality [36]. Thus, we can say that attacks that compromise the availability of smart grid systems are the most severe, while those targeting its confidentiality are the least severe. In addition to severity, the likelihood of each attack to be carried out is important. Although attacks based on Duqu and Stuxnet, for example, are highly destructive due to their ability to bypass all security boundaries and vandalise the industrial control system, they are complex and sophisticated. Hence, even though the severity of these viruses is high, they have a low likelihood of being launched.

   The HMI popping attack is an example of a highly severe. However, its execution does not demand outstanding experience in security and industrial control systems, or a high level of networking skill. The public availability of vulnerability documentation on devices enables the use of open-source tools, such as Metasploit and Meterpreter, or the so-called script-kiddies, by a hacker to launch an attack. Thus, this attack is considered to be highly severe as well as highly likely [35].

   Table 2 summarises common cyberattacks on microgrid based on the four steps identified above: reconnaissance, scanning, exploitation, and maintaining access. Each step includes the attack categories, examples, the component compromised in the smart grid due to each attack, the impact of each attack, and the appropriate countermeasures. It can be concluded that the use of secure network protocols, such as secure-DNP3, as well as the enabling of authentication and encryption mechanisms can help prevent most attacks.

Table 2. Cyber-attacks on microgrid, their impacts, and countermeasures.

Attacking Steps	Attack Categories	Attack Examples	Compromised Element	Compromised Security Parameters	Possible Countermeasures
Reconnaissance	Traffic analysis, Social Engineering	[35]	Modbus protocol, DNP3 Protocol	Confidentiality	Secure DNP3, PKI, TLS, SSL, Encryption, Authentication [35]
Scanning	Scanning IP, Port, Service, Vulnerabilities	Modbus network scanning [37], DNP3 network scanning [38]	Modbus Protocol, DNP3 Protocol	Confidentiality	IDS [39], SIEM, Automated security compliance checks
Exploitation	Virus, worms, Trojan Horse	Stuxnet, Duqu	SCADA PMU, Control device	Confidentiality Integrity Availability Accountability	DLP, SIEM, Anti-virus , IDS
	Denial of service (DoS)	Puppet attack, TSA	AMI, PMU, smart grid equipment GPS	Availability	SIEM, flow entropy, signal strength, sensing time measurement, transmission failure count, pushback, reconfiguration methods, IDS
	Privacy violation	[39]	Smart meters	Confidentiality	Secure DNP3, PKI, TLS, SSL, encryption, authentication
	Man-in-the-middle (MITM)	Intercept/alter, active eavesdropping attack	HMI, PLC, SCADA, AMI, DNP3	Confidentiality Integrity	Secure DNP3, PKI , TLS, SSL, encryption, authentication
	Replay attack	[35]	IED, SCADA, PLC, authentication scheme in AMI	Integrity	Secure DNP3, PKI , TLS, SSL, encryption, authentication
	Jamming channel	[40], MAS-SJ	PMU, CRN in WSGN	Availability	Anti-jamming [40]
	Popping the HMI	[35]	SCADA, EMS, substations	Confidentiality Integrity Availability Accountability	DLP, SIEM, Anti-virus, automated security compliance checks , IDS
	Masquerade attack	[35]	PLC	Confidentiality Integrity Availability Accountability	DLP, Secure DNP3, PKI , SIEM, TLS, SSL, encryption, authentication, IDS
	Integrity violation	[35]	Smart meter, RTU	Integrity Availability	DLP, Secure DNP3, PKI, SIEM, TLS, SSL, encryption, authentication, IDS
Maintaining access	Backdoor	[35]	SCADA	Confidentiality Integrity Availability Accountability	IDS, SIEM, Anti-virus

3. The Cybersecurity Aspects of Microgrid

Power systems featuring microgrids have been exposed to several cyberattacks with severe consequences, according to numerous industries and governmental bodies. These incidents can be examined to develop methods to respond to cyberattacks on the microgrid, such as methods to detect cyber-intrusion and mitigating its impact. This can be achieved through the identification and elimination of vulnerabilities in microgrid systems. In this section, we discuss the vulnerabilities and threats to microgrid.

3.1. Traditional Security Tools in Microgrid Systems

The microgrid is connected to the Internet through the control centre, which is the main component of these systems. It connects and links all distribution substations. DNP3, Modbus, and other Internet-enabled communication protocols carry out control commands and transfer status data from the various microgrid devices to the control centre. These Internet-enabled connections are vulnerable to several cyber-threats that disrupt power supply to the microgrid. Therefore, early solutions involved the use of traditional security tools, such as firewalls and intrusion detection systems, to secure these protocols.

To filter incoming network traffic, firewalls are installed in the router and the gateway to prevent unauthorised users from accessing the private network. Firewalls can inspect and discard suspicious packets by using such properties as their port numbers, IP address locations, and time delays. However, firewalls depend on a set of predefined rules that can turn into conflicts in many cases because hundreds of configurable rules are obtained in commercial-grade firewalls. However, this process can be complicated owing to the rare availability of information because the grid depends on a proprietary software platform. Moreover, perfect knowledge of cyber-assets is needed to develop accurate rules for firewalls [41].

Numerous identification-based approaches have been developed to address the issue of anomalies in firewall policies [41–43]. A high-level security policy has also been proposed by the American National Standards Institute (ANSI)/International Society for Automation (ISA) for best practices in mitigating threats in the control system. Another drawback of firewalls is that spoofed messages can bypass protections that contain filtering rules. In addition, the vulnerabilities in software allow for cyberattacks to be performed by the attackers. Firewalls may also be unusable in WANs owing to the high latency of communication among devices.

The cryptographic protection mechanism has become a critical issue in cybersecurity for building and developing data confidentiality and integrity. The power industry has developed various communication protocols and devices prior to implementing cybersecurity to protect data security. SCADA, the substation automation system (SAS), the phasor measurement unit (PMU), and DER, which use such protocols as Modbus and the DNP3 in a smart grid, have been applied, but cannot protect against cyberattacks [41]. High access to the network by many users in the WAN may increase security risks, especially when such protocols as DNP3 have been used. The authors of [42] proposed solutions for the MODBUS authentication framework. A secure frame format has also been proposed to overcome the drawbacks of DNP3 [43].

3.2. Vulnerabilities and Threats in Microgrid

A vulnerability is defined as weakness in the system, and threat can be defined as a potential to give harm to the system. Attackers exploit vulnerabilities in the system to attack it. This section presents a list of potential threats and threat agents to the microgrid in electrical systems.

3.2.1. Common Vulnerabilities in Microgrid

Although a combination of the cyber-system and the critical physical infrastructure can be beneficial, it creates several vulnerabilities that can lead to threats. Such vulnerabilities can expose a microgrid to physical system damage if they are not adequately addressed.

Cyber-physical vulnerabilities in a microgrid are inherited from the distributed power system. These vulnerabilities are developed by the following:

- **Wireless communication.** Such communication uses radio frequency, which makes it challenge to prevent physical access to users, especially in case of public access to the network. Although it has several advantages, it faces the risk of attacks, including interception and intrusion, that can be larger than in a wired network.
- **Heterogeneous communication technology.** Modern power systems are deployed through the use of various technologies. These technologies, which are either wired or wireless, create challenges for a robust and uniformed cybersecurity policy due to the need to protect the communication infrastructure.
- **Increased communication to external networks.** This occurs in a microgrid because communication to the external network helps maintain its performance and safety through continuous data exchange with the main operator. However, it exposes the created communication line to outsider threats.
- **Internet Exposure.** The exchange of data through the Internet plays an important role in providing ancillary services for the microgrid, including data on fuel prices and weather forecasts. This environment exposes the system to attacks through the Internet.
- **Increased system automation.** System automation improves the effectiveness and flexibility of operation by preventing the likelihood of human error. However, this creates new vulnerabilities, where the system has more access points, thus increasing the possibility of attacks.
- **Increased use of automation device and distributed control.** The possibility for a security breach is created through the heightened penetration of monitoring and control capabilities of the system. The boundaries of a microgrid have been extended and stretched in the digital era.
- **Cohabitation between legacy and new systems.** The sharing of a common infrastructure during contact between the microgrid controller and the operators of different distributions can introduce new vulnerabilities to the system.
- **Multiple independent systems.** Because the microgrid consists of such essential systems as computers, actuators, sensors, and emergency systems, it faces difficulty in guaranteeing uninterrupted communication, interfacing, and security between heterogeneous and independent systems.

All these vulnerabilities are considered weaknesses that can be exploited by one or more threats.

3.2.2. Threats against Microgrid

A threat model commonly used against the microgrid is the one developed by the European Union Agency for Network and Information Security (ENISA) [44]. This model features cybersecurity threats to ICT and non-IT assets, which are physical assets of the main operations of the system. Based on this model, the potential threats to microgrids can be categorised into the following:

- **Physical attacks occurring from intentional offensive actions.** These are targeted to perform distractions at the maximum level by gaining unauthorised access to assets of the microgrid and destroying them.
- **Eavesdropping.** This category of threats is realised by adjusting communication between parties without installing tools on the victim's side.
- **Nefarious Atrocious Activities.** This category is performed through cyberattacks or deliberate harmful activities which aims at system digital assets. Here, the attackers would use additional tools/software to attack the victim's software or IT infrastructure.

3.2.3. Potential Threat Agents against Microgrid

Several threat agents against microgrids have been identified:

- **Hostile threat agents.** Companies or organisations may be correlated to offensive tactics. These companies usually have a high capability of intelligence in technology or human beings.
- **Cyber-criminals.** This category is a hostile threat by nature, and targets financial gain at a high level of skill. This criminal act can be coordinated at a national, local, or international level.
- **Threat agents from the inside, including employees and third party.** The employees of a microgrid include the operational staff as well as contractors. Other, third parties, also help at the power facilities. All of these agents can access the private system of the microgrid and expose it to attacks on sensitive assets.
- **Hacktivists.** This type of threat is created by individuals who protest against political or social agendas, and promote their cause by hacking intelligence agencies, corporations, websites, and military institutions.
- **Capabilities of offensive cyber in nation-states.** This attack is considered a cyber-weapon. Nation states have high skill and expertise in malware, and use them to attack adversaries.
- **Terrorists.** Their activities have been expanded to include cyberattacks targeting critical infrastructure, including public health agencies, energy production facilities, and telecommunication infrastructures. This type of threat may have a severe impact on the government and society.
- **Cyber-fighters.** This is an emerging threat agent. It is composed of a group of patriotically motivated citizens who have the potential to initiate cyberattacks. There may be a conflict between their activities and those of other groups (e.g., hacktivists).
- **Insider Threat.** A cyberattack occurs when intruders use false system information to deceive the operators. Such operations cause the power system to become unstable. This situation obtains because insiders have knowledge of the power grid, especially its vulnerabilities. The detection and prevention of attacks initiated by insiders is challenging.

3.3. Security Issues in Microgrid

Understanding various threats and weaknesses that exist in the microgrid system helps us to present the potential security issues in microgrid using layered approach, as summarized in Table 3. In this section, we derive the attributes for every enclave and identify potential security issues in microgrid, following the guidelines by [45].

As resiliency is an important characteristic of a microgrid, introducing security solutions might introduce unwanted consequence that disturbs microgrid's resiliency. When considering security solutions for microgrid as a cyber physical system, a tool that gives a quantitative measure is needed so that the microgrid's resiliency can be quantified as per its definition.

CyPhyR [46] is a tool that measures microgrid's resiliency based on the cyber security exercises. The tool has two stages: (1) planning phase and (2) operational phase. The planning phase involves a study on impacts of various components in the microgrid towards microgrid's resiliency and the operational phase quantify the microgrid's resiliency based on the defined Cyber Impact Severity metric. Generally, the Common Vulnerability Scoring System (CVSS) [47] s used to measure technical vulnerabilities and provide the impact based on only qualitative measures such as high, medium, and low. It can be used to get a high level picture of microgrid systems security. There are also tools to measure the properties of network resiliency in general such as [48–51].

Table 3. Potential security issues for microgrid.

Enclave	Characteristic	Attributes	Potential Security Issues
DG sources	In terms of availability, most of DG sources such as solar and wind are geographical location dependent, it is not the case for diesel. DG sources such as solar, wind and hydro are uncontrollable. Diesel is controllable [12].	• Availability requirements. • Integrity requirements • Wireless media • Immature or proprietary protocols • Legacy end devices and systems • Patch and update management constraints for devices including scalability and communications • Environmental and physical access constraints	• **Hardware:** improper installation of DG devices or equipment, improper measurement, and command validation, battery operated devices, lack of security policy to device operation and maintenance. • **Software:** missing data protection, improper access control configuration, missing patches or software updates. • **Communication:** insecure communication protocol used, unstable communication link. • **Service:** improper configuration, implementation error.
Energy storage	1. Typical back up time ranges from 5 s to 30 min. 2. Losses at stand by ranges from very low to high. 3. Charging efficiency ranges from 75% to 95%.	• Confidentiality requirements • Privacy concerns • Availability requirements • Low bandwidth of communication channels. • Immature or proprietary protocols. • Real time operational requirements with low tolerance for latency problems. • Legacy communication • Legacy end-devices and systems protocol • Patch and update management constraints for devices including scalability and communications. • Limited power source for primary power • Autonomous control.	• **Hardware:** improper management of ES devices or equipment, improper or no device authentication. • **Software:** improper configuration for remote access and/or maintenance and update, software/firmware vulnerabilities, patching or update missing, no or unsupported malware detection, improper software configuration and access control, integrated circuits (ICs) vulnerability. • **Communication and Network:** use of insecure or less secure communication protocols. • **Service:** improper access configuration and management to cloud services, data privacy and data integrity, cloud data storage vulnerability
Distribution system	Three power electronics interfaces available for connecting the energy generated from the distributed sources to the distribution network.	• Inter organizational interactions • Availability requirements • Real time operational requirements with low tolerance for latency problems. • Legacy communication. • Legacy end devices and systems protocols.	• **Hardware:** improper configuration, Improper device management, inter-operability issue. • **Software:** improper configuration for remote access and/or maintenance and update, software/firmware vulnerabilities, patching or update missing, no or unsupported malware detection, improper software configuration and access control. • **Communication:** no resilient capability to switch between grid connection to stand alone mode.

Table 3. *Cont.*

Enclave	Characteristic	Attributes	Potential Security Issues
Communication system	• Ease of connection to difficult or unreachable areas. • Wired and wireless	• Confidentiality requirements • Privacy concerns • Integrity requirements • Availability requirements • Wireless media • Inter-organizational interactions • Key management for large number of devices • Unpredictability, variability, or diversity of interactions	• **Hardware:** improper configuration, Improper device management, inter-operability issue, battery operated devices, non-compliance to security standards devices, no device authentication. • **Software:** improper configuration for remote access and/or maintenance and update, software/firmware vulnerabilities, patching or update missing, no or unsupported malware detection, improper software configuration and access control, improper configuration of access control, use of non-standard cryptographic mechanisms. • **Communication/Network:** insecure network with weak or less secure communication protocol, instable wireless network, low bandwidth and speed, bi-directional characteristics.

3.4. Efforts and Initiatives for Smart Grid and Microgrid Security

The research in [52] proposed a baseline requirement and guidelines for data delivery in the implementation of a power grid system to ensure its reliability. The North American Electric Reliability Corporation, for example, has proposed the Critical Infrastructure Protection (CIP) standards, CIP-002 through CIP-009 [53], to provide a cybersecurity framework for the identification and protection of critical cyber-assets and support the reliable operation of the bulk electric system. Another example, the Achieve Energy Delivery System Cyber-Security, has been published by the Energy Sector Control Systems Working Group (ESCSWG) in a study conducted to improve cybersecurity in energy delivery systems [54]. In addition, the National Institute of Standards and Technology (NIST) has published cybersecurity guidelines for smart grid systems [45], in which important threat scenarios are mentioned for the cybersecurity of the microgrid.

In microgrid communication, the connection between internal and external networks, such as the enterprise network and the Internet, is widely exposed to cyber-threats. A cyberattack occurs through intrusion into power enclaves of the microgrid through the exploitation of vulnerabilities in the network, system, and/or application level by attackers to compromise critical operations. Researchers have chosen to follow such standards for specific microgrid architectures as NIST 800-53 [55] and IEC 62443 [56].

As they have an internal system design that does not focus on security, a majority of the systems depend on perimeter protection. Such a system is developed as part of a closed network. A drawbacks of the power network is that it is designed without the security of the IEC 61850. A security mechanism is thus needed for these protocols. However, this environment tends to have vulnerabilities that cyberattacks can exploit.

The IEC 62351 has been developed to enhance the IEC 61850 in terms of security [57]. However, this enhanced protocol does not include the cybersecurity of the microgrid communication network. Another secure framework that does not offer cybersecurity measures for microgrid-specific threats is the OLE for the Process Control Unified Architecture (OPC UA) [58]. This framework is a standard-based communication backbone that has advantages in case of a larger scale of cybersecurity threats. Examples of such threats include the sensitive control of network exposure, the complexities in achieving cybersecurity certification, and component integration legacy.

Microgrid systems are connected to external networks, such as enterprise networks and the Internet, which significantly increases the cyber-threats to them. Cyberattackers can attack microgrid power enclaves and compromise critical operations by exploiting vulnerabilities at the network, system, and/or application level. Most systems rely on perimeter protection, with internal systems designed with less security because they are intended to be part of a closed network.

The Secure Network of Assured Power Enclaves (SNAPE) architecture [59], which is based on the network separation strategy, was created for a large US Army base containing multiple power enclaves with secure communication. A microgrid system deployed based on the SNAPE architecture can contribute to the goals of energy security of the US Department of Defense. Network segregation is achieved by hardware devices that provide strong cryptographic separation. The segregation enables the isolation of control networks so that they can use lightweight cryptography to satisfy the requirements of low latency. This novel approach minimises the burden of cybersecurity certification by reducing the scope of certification to a subset of the microgrid network. In the SNAPE architecture, the OLE for the Process Control Unified Architecture (OPC UA) is used to implement the communication backbone. The OPC UA is backward-compatible with distributed control system protocols such as IEC 61850. It also provides authentication and authorisation services in the application layer.

Deploying IPv6-based networks leads to several gaps in security. If IPv6 and IPv4 are run simultaneously, IPv6 should be tunnelled over IPv4 or run independently. In the tunnelling mode, configuration problems can create security holes in the system [52]. If the two protocols are run in parallel, firewalls must be configured to filter IPv6 traffic, which is not very common. A typical firewall does not filter IPv6 traffic, and an attacker can leverage this unsecured channel to enter the system. Administrators must also use new (and better) ways to deploy, configure, and monitor networks. Essential tasks include troubleshooting networks, configuring firewalls, enforcing secure configurations, monitoring security logs, analysing real-time behaviour, and performing network audits. Most intrusion detection/prevention systems are still not very effective at handling IPv6 traffic, which increases the potential for attacks.

CERTSMicroGrid is a novel approach for integrating distributed energy resources in a microgrid to seamlessly island it from and them reconnect them to the power grid [60]. All distributed energy resources appear to be a single entity for coordination and control to the control centre. The traditional method involves integrating a small number of distributed energy sources and shut down the microgrid when problems arise (according to the IEEE P1547 standard). However, unlike the SNAPE architecture, the CERTS model does not explicitly focus on the cybersecurity of microgrids. The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) project was conducted by the US Department of Energy, Department of Defense, and Department of Homeland Security [61]. The goal was to provide secure control of on-base generation at military bases by building secure and robust microgrids that incorporate renewable energy sources.

Mueller [62] has discussed research undertaken according to the NSF ERC FREEDM project. The project has investigated challenges posed by the cyber-physical nature of microgrids, and has highlighted novel opportunities for providing selective power delivery during power outages. Mueller recognises the need to secure microgrids from cyberattacks. However, the FREEDM Project does not propose any security solutions. SNAPE stands out because it recognises the need to secure microgrids and presents a comprehensive cybersecurity architecture that adheres to industry standards, and satisfies the requirements of the microgrid.

4. Potential Future Work and Conclusions

ICT systems are the backbone of modern microgrids. Cybersecurity is essential for the stability and reliability of the microgrid. However, the integration of various technologies into microgrid also leads to more cyber security concerns.

Looking into the landscape and technology progress of microgrid, there are many potential R&D topic around microgrid security that can be summarized as in Table 4. A part of the motivation for these R&D topics is also originated from [45]:

Table 4. Potential R&D topics in microgrid security.

Level	Potential R&D Topic in Microgrid
Device/hardware level	• To investigate and improve cost effective higher tamper resistant and survivable device architectures. • Intrusion detection with embedded processors. • Device authentication.
System level	• To address security issues and challenges for scalable microgrid. • System architecture for real time security and bounded recovery considering legacy system integration. • Resiliency management and intelligent decision support. • To address issues in infrastructure interdependency. • Cross domain (power/electrical to cyber/digital) security event detection, analysis and response. • System segmentation and virtualization
Communication/Network level	• Secure protocol for inter-networking within microgrid to support resiliency. • IPV6 and 5G for microgrid security. • Architecture and issues of covert network channels in microgrid.

Table 4. *Cont.*

Level	Potential R&D Topic in Microgrid
Software and application level	• Resiliency of microgrid against (Distributed) Denial of Service (DOS) attacks. • Microgrid resiliency and security towards integration with cloud infrastructure. • Security design and verification tools. • Vulnerabilities and risk prediction in smart microgrid. • Intrusion detection without compromising microgrid availability requirements. • Cryptographic key management for data security in microgrid. • Advanced cryptography for microgrid security. • User authentication and access control.

With emerging focus on machine learning (ML) in many applications, their potential for microgrid security is worth exploring. This includes using ML for gathering threat intelligence, automated vulnerability assessment, and threat and risk prediction. Lightweight cryptographic algorithms and cryptographic protocols are other promising areas of research on microgrid security. This is part of solutions to vulnerabilities in the communication protocols of the microgrid. This paper has provided a comprehensive review of the components of a microgrid as well as related elements and cybersecurity aspects, and discussed the potential of research to address various vulnerabilities and potential threats in it. The understanding gleaned from the work here can help spur innovation in research on microgrid security.

Another technology that can be explored to address security issues in microgrid is blockchain. It is especially useful for authentication related issues and the development of blockchain platform for microgrid can be of significant contribution in commercialization.

To prevent unknown cyberattacks, potential vulnerabilities in cybersecurity can indicate research-related needs for enhancing the cybersecurity of a microgrid. Jamming attacks threaten wireless communication because the absence of mitigation approaches creates a weakness in the connectivity of components of the smart grid. GPS signals are vulnerable to spoofing attacks that may impact the time-based synchronisation requirements for PMU data. A standard to assess the performance of ADSs/IDSs is also not available. Although several detection systems have been proposed and tested for different sectors of a microgrid, they do not guarantee accurate detection in practice. Further research on coordinated cyberattacks is urgently needed. The response of operators should be considered in such work. In case of a cyberattack, an operator may be deceived by falsified data. Future work should also focus on investigating the performance of IEC 61850-based communication in microgrids in an energy storage system (ESS) for hardware systems by including a microgrid controller with a real-time digital simulator (RTDS). Further, the performance of systems developed for different communication technologies that can be used in small islands with a more diverse generation portfolio should be tested.

Finally, as the initiatives on smart grids are on the rise, it is well noted that there are lots of research rooms that should be explored for microgrid security. This paper has provided comprehensive coverage of microgrid components, its related elements, the cybersecurity aspects of microgrid and the potentials of research domains addressing various vulnerabilities and potential threats in the microgrid. The understanding will help in spurring innovation for microgrid security.

Author Contributions: N.J.: writing content, reviewing, editing and revising, Q.S.Q.: writing content, reviewing, editing and formatting; F.A.B.: writing-original draft, and resources; M.M. & V.K.R.: methodology, and investigation. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Long Term Research Grant Scheme (LRGS), sponsored by the Malaysia Ministry of Education, Grant Number: LRGS/1/2018/UNITEN/01/1/2.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hassan, M.; Abido, M.; Rahim, A. Optimal design of autonomous microgrid using particle swarm optimization. In Proceedings of the International Symposium on Power Electronics Power Electronics, Electrical Drives, Automation and Motion, Sorrento, Italy, 20–22 June 2012; pp. 152–157.
2. Abdulkarim, A.; Faruk, N.; Oloyode, A.; Olawoyin, L.A.; Popoola, S.I.; Abdullateef, A.; Ibrahim, O.; Surajudeen-Bakinde, N.; Abdelkader, S.; Morrow, J.D.; et al. State of the art in research on optimum design, reliability and control of renewable energy microgrids. *Elektr. J. Electr. Eng.* **2018**, *17*, 23–35. [CrossRef]
3. Villalón, A.; Rivera, M.; Salgueiro, Y.; Muñoz, J.; Dragičević, T.; Blaabjerg, F. Predictive control for microgrid applications: A review study. *Energies* **2020**, *13*, 2454. [CrossRef]
4. Leon, G. Smart Planning for Smart Grid AMI Mesh Networks. EDX Wireless. Available online: https://www.smartgrid.gov/files/documents/Smart_Planning_for_Smart_Grid_AMI_Mesh_Networks_201109.pdf (accessed on 2 November 2011).
5. Bani-Ahmed, A.; Weber, L.; Nasiri, A.; Hosseini, H. Microgrid communications: State of the art and future trends. In Proceedings of the 2014 International Conference on Renewable Energy Research and Application (ICRERA), Milwaukee, WI, USA, 19–22 October 2014; pp. 780–785.
6. Cagnano, A.; De Tuglie, E.; Mancarella, P. Microgrids: Overview and guidelines for practical implementations and operation. *Appl. Energy* **2020**, *258*, 114039. [CrossRef]
7. Nederland, N. *Privacy and Security of the Advanced Metering Infrastructure*; Technical Report; Chalmers University of Technology: Gothenburg, Sweden 2010.
8. Brown, B.; Singletary, B.; Willke, B.; Bennett, C.; Highfill, D.; Houseman, D.; Cleveland, F.; Lipson, H.; Ivers, J.; Gooding, J.; et al. AMI System Security Requirements. *AMI-SEC TF*. 2008. Available online: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf (accessed on 7 October 2021).
9. International Electrotechnical Commission. *Electricity Metering Data Exchange—The DLMS/COSEM Suite—Part 5-3: DLMS/COSEM Application Layer*; IEC 62056-5-3: 2016; Technical Report; International Electrotechnical Commission (IEC): Geneva, Switzerland, 2016.
10. Berrio, L.; Zuluaga, C. Concepts, standards and communication technologies in smart grid. In Proceedings of the 2012 IEEE 4th Colombian Workshop on Circuits and Systems (CWCAS), Barranquilla, Colombia, 1–2 November 2012; pp. 1–6.
11. Mariam, L.; Basu, M.; Conlon, M.F. Microgrid: Architecture, policy and future trends. *Renew. Sustain. Energy Rev.* **2016**, *64*, 477–489. [CrossRef]
12. Priyadharshini, N.; Gomathy, S.; Sabarimuthu, M. A review on microgrid architecture, cyber security threats and standards. *Mater. Today Proc.* **2020**. [CrossRef]
13. Zhao, J.; Wang, C.; Zhao, B.; Lin, F.; Zhou, Q.; Wang, Y. A review of active management for distribution networks: Current status and future development trends. *Electr. Power Components Syst.* **2014**, *42*, 280–293. [CrossRef]
14. Zhang, X.; Hao, M.; Liu, F.; Yu, C.; Zhao, W. Analysis and control of energy storage systems in microgrid. In Proceedings of the 2012 Second International Conference on Intelligent System Design and Engineering Application, Sanya, China, 6–7 January 2012; pp. 1375–1379.
15. Win, K.T.Z.; Tun, H.M. Design and implementation of SCADA system based power distribution for primary substation (control system). *Int. J. Electron. Comput. Sci. Eng* **2014**, *3*, 254–261.
16. Usman, A.; Shami, S.H. Evolution of communication technologies for smart grid applications. *Renew. Sustain. Energy Rev.* **2013**, *19*, 191–199. [CrossRef]
17. Segall, A. Distributed network protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 23–35. [CrossRef]
18. Cagnano, A.; De Tuglie, E.; Cicognani, L. Prince—Electrical Energy Systems Lab: A pilot project for smart microgrids. *Electr. Power Syst. Res.* **2017**, *148*, 10–17. [CrossRef]
19. Palma-Behnke, R.; Ortiz, D.; Reyes, L.; Jimenez-Estevez, G.; Garrido, N. A social SCADA approach for a renewable based microgrid—The Huatacondo project. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–7.
20. Chlela, M.; Joos, G.; Kassouf, M. Impact of cyber-attacks on islanded microgrid operation. In Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems, Waterloo, ON, Canada, 21–24 June 2016; pp. 1–5.
21. Martin-Martínez, F.; Sánchez-Miralles, A.; Rivier, M. A literature review of Microgrids: A functional layer based classification. *Renew. Sustain. Energy Rev.* **2016**, *62*, 1133–1153. [CrossRef]
22. Bracco, S.; Delfino, F.; Pampararo, F.; Robba, M.; Rossi, M. The University of Genoa smart polygeneration microgrid test-bed facility: The overall system, the technologies and the research challenges. *Renew. Sustain. Energy Rev.* **2013**, *18*, 442–459. [CrossRef]
23. Loix, T. *Distributed Generation—Micro Grids*; Alternative Energy: San Diego, CA, USA, 2009.
24. Qu, M. Microgrid Policy Review of Selected Major Countries, Regions, and organizations. 2012. Available online: https://escholarship.org/uc/item/51q0g9p8 (accessed on 7 October 2021).

25. Barnes, M.; Dimeas, A.; Engler, A.; Fitzer, C.; Hatziargyriou, N.; Jones, C.; Papathanassiou, S.; Vandenbergh, M. Microgrid laboratory facilities. In Proceedings of the 2005 International Conference on Future Power Systems, Amsterdam, The Netherlands, 18 November 2005; p. 6.
26. Katiraei, F.; Abbey, C.; Tang, S.; Gauthier, M. Planned islanding on rural feeders—Utility perspective. In Proceedings of the 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–6.
27. Kyriakarakos, G.; Piromalis, D.D.; Dounis, A.I.; Arvanitis, K.G.; Papadakis, G. Intelligent demand side energy management system for autonomous polygeneration microgrids. *Appl. Energy* **2013**, *103*, 39–51. [CrossRef]
28. Loix, T.; Leuven, K. The first micro grid in the Netherlands: Bronsbergen. *Retrieved Dec.* **2009**, *27*, 2012.
29. Eto, J.; Lasseter, R.; Schenkman, B.; Stevens, J.; Klapp, D.; VolkommeRr, H.; Linton, E.; Hurtado, H.; Roy, J. Overview of the CERTS microgrid laboratory test bed. In Proceedings of the 2009 CIGRE/IEEE PES Joint Symposium Integration of Wide-Scale Renewable Resources Into the Power Delivery System, Calgary, AB, Canada, 29–31 July 2009; p. 1.
30. Mohagheghi, S.; Stoupis, J.; Wang, Z. Communication protocols and networks for power systems-current status and future trends. In Proceedings of the 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–9.
31. Majdalawieh, M.; Parisi-Presicce, F.; Wijesekera, D. DNPSec: Distributed network protocol version 3 (DNP3) security framework. In *Advances in Computer, Information, and Systems Sciences, and Engineering*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 227–234.
32. Lim, I.; Hong, S.; Choi, M.; Lee, S.; Kim, T.; Lee, S.; Ha, B. Security protocols against cyber attacks in the distribution automation system. *IEEE Trans. Power Deliv.* **2009**, *25*, 448–455. [CrossRef]
33. Engebretson, P. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, 1st ed.; Syngress Publishing: Rockland, MA, USA, 2011.
34. Khelifa, B.; Abla, S. Security concerns in smart grids: Threats, vulnerabilities and countermeasures. In Proceedings of the 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC), Marrakech, Morocco, 10–13 December 2015; pp. 1–6. [CrossRef]
35. Knapp, E.D.; Samani, R. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*; Elsevier: Amsterdam, The Netherlands, 2013.
36. Gilchrist, G. Secure authentication for DNP3. In Proceedings of the 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–3.
37. Al-Dalky, R.; Abduljaleel, O.; Salah, K.; Otrok, H.; Al-Qutayri, M. A Modbus traffic generator for evaluating the security of SCADA ystems. In Proceedings of the 2014 9th International Symposium on Communication Systems, Networks Digital Sign (CSNDSP), Manchester, UK, 23–25 July 2014; pp. 809–814. [CrossRef]
38. Rodofile, N.R.; Radke, K.; Foo, E. DNP3 network scanning and reconnaissance for critical infrastructure. In Proceedings of the Australasian Computer Science Week Multiconference, Canberra, Australia, 2–5 February 2016.
39. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study. *IEEE Syst. J.* **2015**, *9*, 31–44. [CrossRef]
40. Reyes, H.; Kaabouch, N. Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic. *Int. J. Sci. Eng. Res.* **2013**, *4*, 1–7.
41. Shahzad, A.; Musa, S.; Aborujilah, A.; Irfan, M. Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. In Proceedings of the ICUIMC '14, Siem Reap, Cambodia, 9–11 January 2014.
42. Phan, R.C.W. Authenticated Modbus Protocol for Critical Infrastructure Protection. *IEEE Trans. Power Deliv.* **2012**, *27*, 1687–1689. [CrossRef]
43. Song, K.Y.; Yu, K.S.; Lim, D. Secure frame format for avoiding replay attack in Distributed Network Protocol (DNP3). In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 28–30 October 2015; pp. 344–349. [CrossRef]
44. Marinos, L. *ENISA Threat Taxonomy: A Tool for Structuring Threat Information*; ENISA: Heraklion, Greece, 2016.
45. Pritzker, P. *Guidelines for Smart Grid Cybersecurity, Volume 1—Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*; U.S. Department of Commerce: Washington, DC, USA, 2014.
46. Venkataramanan, V.; Hahn, A.; Srivastava, A. CyPhyR: A cyber-physical analysis tool for measuring and enabling resiliency in microgrids. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 313–321. [CrossRef]
47. Mell, P.; Scarfone, K.; Romanosky, S. Common vulnerability scoring system. *IEEE Secur. Priv.* **2006**, *4*, 85–89. [CrossRef]
48. Sterbenz, J.P.; Çetinkaya, E.K.; Hameed, M.A.; Jabbar, A.; Qian, S.; Rohrer, J.P. Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation. *Telecommun. Syst.* **2013**, *52*, 705–736. [CrossRef]
49. Francis, R.; Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 90–103. [CrossRef]
50. Zhao, K.; Kumar, A.; Harrison, T.P.; Yen, J. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. *IEEE Syst. J.* **2011**, *5*, 28–39. [CrossRef]
51. Pandit, A.; Crittenden, J.C. Index of network resilience (INR) for urban water distribution systems. *Nature* **2012**, *12*, 120–142.

52. Bakken, D.E.; Bose, A.; Hauser, C.H.; Whitehead, D.E.; Zweigle, G.C. Smart Generation and Transmission With Coherent, Real-Time Data. *Proc. IEEE* **2011**, *99*, 928–951. [CrossRef]
53. Lasseter, R.H.; Eto, J.H.; Schenkman, B.; Stevens, J.; Vollkommer, H.; Klapp, D.; Linton, E.; Hurtado, H.; Roy, J. CERTS microgrid laboratory test bed. *IEEE Trans. Power Deliv.* **2010**, *26*, 325–332. [CrossRef]
54. Mariam, L.; Basu, M.; Conlon, M.F. A review of existing microgrid architectures. *J. Eng.* **2013**, *2013*, 937614. [CrossRef]
55. Dempsey, K.L.; Witte, G.A.; Rike, D. Summary of NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. 2014. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02192014.pdf (accessed on 7 October 2021).
56. International Electrotechnical Commission. *IEC 62443: Industrial Communication Networks—Network and System Security*; IEC Central Office: Geneva, Switzerland, 2010.
57. International Electrotechnical Commission. *Power Systems Management and Associated Information Exchange—Data and Communications Security. Part 1: Communication Network and System Security—Introduction to Security Issues*; IEC Technical Specification; IEC Central Office: Geneva, Switzerland, 2007; p. 62351.
58. Andersson, R.; Sandelin, A.; Danko, C.G. A unified architecture of transcriptional regulatory elements. *Trends Genet.* **2015**, *31*, 426–433. [CrossRef]
59. Mohan, A.; Brainard, G.; Khurana, H.; Fischer, S. A cyber security architecture for microgrid deployments. In *International Conference on Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 245–259.
60. Lasseter, R.; Akhil, A.; Marnay, C.; Stephens, J.; Dagle, J.; Guttromsom, R.; Meliopoulous, A.S.; Yinger, R.; Eto, J. *Integration of distributed energy resources. The CERTS Microgrid Concept*; Technical Report; Lawrence Berkeley National Lab. (LBNL): Berkeley, CA, USA, 2002.
61. Stamp, J. The SPIDERS project-smart power infrastructure demonstration for energy reliability and security at US military facilities. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012.
62. Mueller, F. *Cyber-Physical Aspects of Energy Systems for the 21st Century: A Perspective from the Nsf Erc Freedm Project*; (moss. csc. ncsu. edu/mueller/ftp/pub/mueller/papers/cps09.pdf); Department of Computer Science, North Carolina State University: Raleigh, NC, USA, 2009.