energies

MDPI

Review

Digital Transformation of Microgrids: A Review of Design, Operation, Optimization, and Cybersecurity

Erdal Irmak [1], Ersan Kabalci [2,*] and Yasin Kabalci [3]

[1] Electrical and Electronics Engineering, Faculty of Technology, Gazi University, Ankara 06560, Turkey; erdal@gazi.edu.tr
[2] Electrical and Electronics Engineering Department, Nevsehir Haci Bektas Veli University, Nevsehir 50300, Turkey
[3] Electrical and Electronics Engineering Department, University of Nigde Omer Halisdemir, Nigde 51240, Turkey; yasinkabalci@ohu.edu.tr
* Correspondence: kabalci@nevsehir.edu.tr

Abstract: This paper provides a comprehensive review of the future digitalization of microgrids to meet the increasing energy demand. It begins with an overview of the background of microgrids, including their components and configurations, control and management strategies, and optimization techniques. It then discusses the key digital technologies that can be used to improve the performance of microgrids, including distributed energy resources management systems, the Internet of Things, big data analytics, blockchain technology, artificial intelligence, digital twin technology, cloud computing, and augmented reality. The paper also highlights the importance of cybersecurity in microgrids, identifying the potential security vulnerabilities and threats to microgrid cybersecurity, as well as strategies for addressing these challenges. Finally, the paper discusses the barriers and challenges regarding the digitalization of microgrids, including technical complexity, high implementation costs, regulatory barriers, data privacy and security concerns, lack of standardization, interoperability issues, limited technical expertise, and integration with the main grid. Overall, this paper demonstrates the significant potential for digital technologies to transform the future of microgrids. By leveraging advanced technologies and implementing effective cybersecurity measures, microgrids can become more efficient, reliable, and resilient, enabling them to meet the growing demand for energy and contribute to a sustainable energy future.

Keywords: microgrids; digitalization; optimization; cybersecurity; renewable energy sources; IoT

check for updates

Citation: Irmak, E.; Kabalci, E.; Kabalci, Y. Digital Transformation of Microgrids: A Review of Design, Operation, Optimization, and Cybersecurity. *Energies* **2023**, *16*, 4590. https://doi.org/10.3390/en16124590

Academic Editor: J. C. Hernandez

Received: 12 May 2023
Revised: 21 May 2023
Accepted: 5 June 2023
Published: 8 June 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The demand for clean and sustainable energy sources is increasing at a rapid pace, and microgrids (MGs) have emerged as a promising solution for achieving energy resilience, efficiency, and security. As a general definition, a microgrid is a localized power system that integrates renewable energy resources, energy storage systems, and loads to operate autonomously or in parallel with the main grid [1–3]. Thanks to these features, MGs offer many benefits, such as improved reliability, reduced carbon emissions, and lower energy costs. However, their design, operation, and management can be complex and challenging. Moreover, the emergence of new digital technologies and the growing demand for decentralized energy systems have led to the digitalization of MGs [4–6].

MGs can be classified based on their operating mode, connectivity, and ownership. For instance, MGs can operate in grid-connected or islanded mode, depending on whether they are connected to the main grid or not. They can also be classified as customer-owned, utility-owned, or third-party-owned, depending on who owns and operates the microgrid. Although the concept of MGs dates back to the early 20th century, when isolated communities in rural areas began using diesel generators to generate electricity, the modern microgrid concept emerged in the 1990s, when the U.S. Department of Energy funded

a series of research projects aimed at developing advanced microgrid technologies [7,8]. Since then, MGs have gained significant attention, and many research projects and pilot programs have been conducted worldwide to explore their potential benefits, challenges, design, and operational procedures.

The design and operation of MGs depend on various factors, such as the local energy resources, load profiles, and customer requirements. The components of a typical microgrid include energy sources, energy storage systems, power electronics, and control systems. The configuration of a microgrid depends on its size, location, and operating mode. For instance, islanded MGs may require more energy storage systems and backup generators than grid-connected MGs [9,10]. Therefore, control and management strategies are critical for the efficient operation of MGs. Various control strategies, such as droop control, frequency control, and voltage control, can be used to maintain the stability and reliability of MGs [11–16]. Optimization techniques, such as economic dispatch and unit commitment, can be used to minimize the operational cost of MGs [17–19]. Microgrid stability and resilience are essential for ensuring uninterrupted power supply to critical loads during grid disturbances or equipment failures. Therefore, various stability and resilience analysis methods have been developed to evaluate the performance of MGs under different operating conditions.

The digitalization of MGs has opened new possibilities for the management and control of these systems. The integration of digital technologies such as distributed energy resources management systems (DERMSs), microgrid energy management systems (MEMSs), Internet of Things (IoT) devices, big data analytics, blockchain technology, artificial intelligence (AI), digital twin technology, cloud computing, and augmented reality have enabled the optimization of MGs' performance and the enhancement of their resilience and stability [20–25]. DERMSs and MEMSs have emerged as essential tools for the efficient management of MGs. DERMSs allows for the integration of distributed energy resources such as wind turbines and solar panels into the grid, while MEMSs enable the optimization of microgrid operations, including load balancing, energy storage management, and demand response. IoT devices are also playing a crucial role in the digitalization of MGs [21]. These devices provide real-time data on energy consumption, production, and storage, enabling better decision making and enhanced control. Big data analytics can process and analyze the massive amounts of data collected by IoT devices, providing insights into the performance of MGs and identifying areas for improvement.

Blockchain technology offers a secure and transparent method for managing transactions in MGs, ensuring that energy transactions are executed efficiently and securely. AI is being used to optimize microgrid performance, reduce costs, and enhance grid stability. Digital twin technology enables the creation of a virtual replica of a microgrid, which can be used for simulation and testing purposes, enhancing the design and operation of MGs [22]. Cloud computing provides a platform for the integration of various digital technologies, enabling the efficient management of MGs. Augmented reality is also being explored as a tool for enhancing the visualization and monitoring of MGs.

As MGs become more digitalized, the threat of cyberattacks also increases. Cybersecurity is, therefore, a critical concern for the operation and management of MGs. Threats to microgrid cybersecurity include unauthorized access to microgrid systems, data breaches, and malicious attacks on microgrid control systems [26,27]. Vulnerability assessments and risk analysis are essential tools for identifying potential cybersecurity threats and vulnerabilities in microgrid systems. Cybersecurity strategies such as access control, data encryption, and firewalls can be implemented to protect MGs from cyberattacks. Incident response and recovery plans should also be emplaced to ensure a quick response in case of a cyberattack.

Despite the potential benefits of digitalization, there are still several barriers and challenges to its implementation in MGs. One of the primary challenges is the high cost of implementing digital technologies in MGs. Additionally, the lack of standardization and interoperability between different digital technologies can make their integration challenging. The complexity of digital technologies can also make their implementation

and management difficult [28–30]. Finally, there are concerns regarding the security and privacy of data collected by digital technologies in MGs.

In conclusion, the digitalization of MGs offers significant opportunities for enhancing their performance, resilience, and stability. With this motivation, this paper provides a comprehensive review of the current state of knowledge on the design, operation, and digitalization of MGs. The selected scientific databases, including IEEE Xplore, ScienceDirect, Elsevier, MDPI, ACM Digital Library, Web of Science, Scopus, and Google Scholar, were utilized to access a diverse range of scholarly articles, conference papers, theses, and other academic resources. The paper begins by providing an overview of the background of MGs, including their definition, historical development, benefits, and challenges. Subsequently, the paper delves into the design and operation of MGs, including their components, configurations, control and management strategies, optimization techniques, stability, and resilience. The paper then explores the digitalization of MGs, examining the role of advanced technologies in enhancing the performance of MGs, and cybersecurity issues that may arise in the process. Finally, the paper identifies barriers and challenges in the digitalization of MGs and outlines future directions for research in this area. Overall, this paper provides valuable insights for researchers, policymakers, and practitioners interested in the future of MGs and the role of advanced technologies in their digitalization.

2. Background of Microgrids

The immense and complicated electric power system is controlled by the power system organizations. Sharing a variety of renewable sources will continue to be the primary feature of utility grids, as has been in the past. The increased use of renewable energy sources (RESs) achieves global participation in electricity generation, and decreasing the dependency. The integration of RESs is becoming more important toward the distribution network due to the technological advancements and environmental concerns. MGs are small-scale local power systems that function inside larger distribution networks. MGs are gaining popularity because of their capacity to decrease environmental impact, increase energy stability efficiency, provide ride-through capability provided by energy storage, and to reduce consequences of sudden grid outages. RESs such as the wind, solar energy, and hydro are cost-effective in meeting their share of the energy requirement. In terms of power supply, microgrid technology offers significant possibilities in distant communities by improving local energy security.

This technology plays a crucial role in enhancing energy security by minimizing the reliance on energy imports. The integration of renewable energy MGs with the utility grid eliminates the need for extra measures to regulate frequency. However, MGs face significant challenges, such as stability, bidirectional power flows, modeling, low inertia, the impact of load perturbations, and uncertainty. It is worth noting that the application of distributed generators (DGs) within MGs can sometimes create more issues than they resolve. MGs are advanced energy grids that incorporate renewable energy generation and storage technologies to ensure sufficient energy supply for meeting regional demand [1].

The MG system as a regulated power supply infrastructure utilizes the grid to connect various components such as loads, DG, energy storage devices, and power electronic converters. Unlike the traditional grid structure, the MG system operates independently as a standalone system. The external grid is linked to the MGs as a single control unit, responsible for self-regulation, protection, and management while meeting customer requirements for power quality and supply reliability. The MG system can either be connected to the grid or function as an isolated island. In practical terms, an MG represents a specific location where the management system oversees and controls the connection between DGs and loads, forming a smaller distribution grid. In this scenario, the regulation and control of DGs are achieved by the management system, which adjusts network structure or load capacity based on data collected, ensuring stability, adaptability, and reliability in the power supply of the distribution system. Additionally, RESs can be integrated into the MG system to reduce grid redundancy, resulting in higher economic benefits compared to traditional

systems. This effectively guarantees the resilience of the power supply. In the case of a problem or security issue occurring in the grid, it solely impacts the MG system based on its location, without affecting the utility grid.

There are two major ways that MGs are operated; the first is known as normal mode or grid-connected mode, and the second is known as islanded mode. In normal mode operation, power flows in both directions. By operating the MG in an islanded mode, isolation switches can prevent difficulties such as voltage dips, frequency drift, and other power quality issues. MGs can guarantee high power quality supply and easy switching between islanded and normal operation modes by using advanced control algorithms, as well as reducing or preventing the impact on key loads when the grid system fails [31].

MGs play a significant role in integrating DG, RES, and energy storage systems (ESSs). The development of infrastructure has been driven by the increasing penetration of RESs, enabling end users to generate, store, control, and manage a portion of their electricity needs. This paradigm shift allows end users to become "prosumers", acting as both consumers and producers of electricity for the grid. Different types of MGs, including DC and AC systems, as well as hybrid configurations, have been proposed for various applications. Islanded MGs find applications in sectors such as transportation, automotive, shipping, and rural regions, providing localized energy generation. Power electronic converters, specifically voltage source inverters (VSIs), often serve as interfaces between prime movers and MGs, allowing parallel connection to these converters. To ensure efficient power sharing without the need for extensive communication, the droop control method is frequently employed to eliminate circulating currents among the converters. This method involves simulating virtual inertias by adjusting the frequency and amplitude of each module based on proportional deductions from the output average active and reactive powers, utilizing control loops known as P-ω and Q-V droops.

While the droop control approach offers high reliability and flexibility, it has certain limitations that restrict its usability. For instance, traditional droop control is not suitable for interconnected systems sharing nonlinear loads, as it fails to account for harmonic currents and balance active and reactive power. Consequently, current-sharing methods that minimize circulating distortion power by addressing harmonic content have been proposed. These methods involve trade-offs by adjusting voltage to enhance current sharing accuracy. Recently, novel control loops incorporating output virtual reactors or resistors have been integrated into the droop approach, allowing for harmonic current content sharing through adjustments in output impedance [32–34].

Several research studies examine the control of individual MGs, where the different proposed control approaches such as predictive control, neural-network-based control, the sliding mode control, and H∞ control are the most widely used robust control methods [35–39]. However, MG control has gained greater attention recently due to increased interest in the community MG concept. According to the literature survey, the community MG control approach can be classified as master–slave [40–42], peer-to-peer (P2P) [43,44], and hierarchical control [34,42,45–47]. This section discusses the overall definition and classification of the MG concept as it evolved over time. Following that, the benefits provided by MGs as well as the challenges in the MG evaluation are thoroughly discussed.

2.1. Historical Development of Microgrids

Microgrid systems have a rich historical development that dates back to the early 20th century. This part explores the evolution of microgrid technology from its inception to the establishment of early isolated systems. The Pearl Street Station, constructed by Thomas Edison in 1882 in New York City, can be regarded as an early form of a centralized power station and a precursor to MGs. The station utilized direct current (DC) generators to provide electricity to customers within a limited radius. While not technically a microgrid, the Pearl Street Station laid the foundation for the development of localized energy systems. As electrification expanded to remote areas, isolated microgrid systems emerged as a solution to provide electricity to communities and industries beyond the reach of centralized

grids. These isolated systems typically included a local power generation source, often based on fossil fuels, and a distribution network serving a specific area. Examples of early isolated MGs include systems established in remote mining operations, rural communities, and islands. Early microgrid systems faced several challenges and limitations. Limited generation capacity was a significant constraint, often relying on diesel generators or small-scale hydroelectric plants. Fuel availability and transportation logistics posed challenges in remote locations. Moreover, the lack of interconnectivity between MGs and the main grid limited their ability to share excess energy or receive backup power during outages. These limitations emphasized the need for technological advancements and grid interconnection to unlock the full potential of MGs [8,48].

The background of MGs is closely tied to the evolution of the electric power industry. In the early days of electrification, power systems were small and isolated, serving specific communities or industrial sites. As the industry grew, power systems became larger and more interconnected, leading to the development of centralized power plants and transmission grids. This model of power generation and distribution has been the dominant paradigm for most of the 20th century, but it has also presented a number of challenges. One of the primary challenges of centralized power systems is their vulnerability to disruptions. If a transmission line or substation is down, it can cause a widespread outage that affects thousands or even millions of people. In addition, centralized power systems are often inefficient, with significant energy losses during transmission and distribution. Furthermore, centralized power systems are often heavily reliant on fossil fuels, which can have significant environmental impacts.

The creation of isolated microgrid systems in remote areas was driven by various motivations, including geographical limitations and the desire for energy self-sufficiency. Many remote areas, such as islands, mountainous regions, and sparsely populated rural communities, faced significant challenges in accessing electricity from centralized grids due to their geographical location. Extending transmission lines from distant power plants to these areas was often economically and technically impractical. As a result, establishing isolated microgrid systems became a viable solution to meet the energy needs of these communities. By generating electricity locally and distributing it within a limited radius, isolated MGs could overcome the geographical limitations and provide reliable power to the inhabitants.

Another motivation for creating isolated microgrid systems was the desire for energy self-sufficiency. In some cases, communities or industries sought to reduce their dependence on external energy sources, such as imported fuels or the main power grid. Establishing MGs allowed them to generate electricity locally using available resources, which could be renewable or conventional, and have greater control over their energy supply. By becoming self-sufficient, these communities could enhance their energy security and reduce vulnerability to disruptions in the centralized grid. Isolated MGs often provided a cost-effective solution for meeting the energy needs of remote areas. Building a smaller-scale generation and distribution system tailored to the local demand was more economical than extending long transmission lines. Additionally, isolated MGs offered increased reliability compared to the centralized grid. Since the distribution network was shorter, the risk of widespread outages due to faults or failures in the main grid was minimized. This aspect was particularly important in areas prone to natural disasters or with challenging terrain, where restoring power from a distant grid could be time-consuming and costly. In some cases, the motivation behind isolated MGs stemmed from environmental concerns. Remote communities or environmentally conscious industries aimed to reduce their carbon footprint and minimize reliance on fossil fuels. By establishing MGs with RESs, such as solar, wind, or small-scale hydroelectric systems, these entities could generate clean energy locally and contribute to sustainability goals. Isolated MGs provided a platform for integrating and maximizing the utilization of renewable resources in areas where centralized grid expansion was not feasible. In summary, the motivations behind the creation of isolated MG systems included overcoming geographical limitations, achieving energy self-sufficiency,

addressing cost and reliability considerations, and embracing environmental sustainability. These motivations drove the early development of microgrid technology and paved the way for subsequent advancements and the interconnected microgrid networks that are seen today [49–58].

MGs offer a potential solution to the challenges mentioned earlier by enabling localized and decentralized electricity generation and distribution. They can operate independently or in conjunction with the main grid and can incorporate various RESs such as solar, wind, and biomass. This enhances their resilience to disruptions and improves overall power supply efficiency and reliability.

The Consortium for Electric Reliability Technology Solutions (CERTS) initiative in the United States and the MGS project in Europe were pioneering efforts in studying and implementing microgrid systems. CERTS, established in 1999, is widely recognized as the originator of the modern grid-connected microgrid concept. Its proposal focused on developing MGs that could integrate multiple distributed energy resources (DERs) while presenting themselves as typical consumers or small generators to the existing network. The emphasis was on seamless and automatic islanding and grid reconnection, utilizing passive control schemes such as reactive power, voltage, and active power–frequency relationships. The goal was to minimize reliance on centralized controllers and high-speed communications, creating a flexible "plug-and-play" system that could accommodate the addition or removal of DERs without extensive redesign. This approach aimed to reduce initial system costs and provide cogeneration facilities with the flexibility to be located near thermal loads. The CERTS microgrid concept has been successfully tested and implemented in real-world microgrid applications. While initially focused on improving reliability rather than directly lowering greenhouse gas emissions, CERTS MGs can incorporate renewable microgeneration sources.

Similarly, the MGS project in the European Union addressed technical challenges such as safe islanding and reconnection procedures, energy management, control techniques for both islanded and interconnected modes, protection devices, and communication protocols. Ongoing research and development continue to explore and refine these issues in the field of MGs [8].

MGs have the ability to provide new economic and social benefits in addition to their technical advantages. They can help local communities and businesses become more autonomous in their energy needs, as well as stimulate the development of new energy generation and distribution business models. Overall, the history of MGs indicates an increasing awareness of the need for more localized and decentralized methods to energy generation and distribution. Microgrid development and deployment are part of a larger movement toward a more sustainable, resilient, and cooperative energy system.

2.2. Definition and Classification of MGs

An MG can be defined as a network consisting of various power generation sources and loads that operate either in isolation (island mode) or in interconnection with the utility grid (grid-connected mode) through integration of these sources. The connection and disconnection of the microgrid to the utility grid are determined based on technical and financial considerations. DERs form a crucial part of MGs, encompassing independently regulated power generation sources that work together to establish an efficient and flexible grid infrastructure. Even if some sources are temporarily disconnected from the generation cycle, the operational perspective of an MG ensures its sustainability. ESSs and power converters connected to the utility grid play a role in managing excess generation within the microgrid. MGs can have installed power capacities ranging from a few kilowatts to multiple megawatts (MW). The primary objective of microgrid installations is to provide power to consumers in remote areas and critical industrial and military facilities. Factors such as the scarcity of fossil fuels, power quality issues, resiliency and flexibility challenges in existing grid infrastructure, and network architecture degradation have stimulated advancements in grid technology and spurred research in MGs. Properly implemented

MGs serve as critical infrastructures that enhance the reliability and resilience of the utility grid by providing a backup system against grid disturbances. Key components of MGs include isolation and protection devices at the point of common coupling (PCC), DERs encompassing various power generation technologies, and RESs such as wind power, solar photovoltaics, fuel cells, biomass, and CHP plants [59–61].

The MGs are categorized into five types: industrial, community, campus, the military, and remote MGs. Industrial MGs are specifically designed to meet the energy needs of industrial facilities, such as manufacturing plants, refineries, mining sites, and data centers. These MGs often operate in conjunction with the main grid but have the capability to disconnect and operate independently during grid outages. Industrial MGs prioritize reliability, cost-effectiveness, and power quality to ensure uninterrupted operations. They may incorporate a combination of onsite generation, energy storage, and advanced control systems to optimize energy usage and minimize disruptions. The community MGs serve a specific community or neighborhood, providing localized power generation, distribution, and resilience. They are typically designed to integrate RESs, such as solar and wind, and may include energy storage systems. Community MGs prioritize energy resilience, allowing them to operate independently during grid outages and provide critical services, such as emergency shelters, medical facilities, and community centers, with electricity. These MGs often promote energy efficiency, local energy production, and community engagement in energy management.

The campus MGs are designed to serve large institutions or campuses, such as universities, military bases, industrial complexes, and business parks. They provide reliable and efficient energy supply to multiple buildings and facilities within a localized area. Campus MGs often incorporate diverse energy sources, including renewable energy, CHP systems, and energy storage. They can optimize energy usage, reduce carbon emissions, and enable better control and management of energy resources. Campus MGs may also act as living laboratories for research and development of advanced energy technologies and systems. Military MGs are deployed in military bases and installations to ensure secure and reliable energy supply for critical operations. These MGs enhance the energy resilience and independence of military facilities, reducing reliance on vulnerable and extended transmission and distribution lines. Military MGs often integrate RESs, energy storage, and advanced control systems to enhance operational capabilities, reduce fuel consumption, and improve energy security. They play a vital role in supporting mission-critical operations, emergency response, and disaster recovery efforts.

Remote MGs are deployed in isolated or remote areas that lack access to the main utility grid. These MGs provide energy independence to communities, facilities, and infrastructure in remote locations. Remote MGs typically rely on a combination of RESs, such as solar, wind, and hydro, along with energy storage systems and backup generators. They enable reliable and sustainable electricity supply in off-grid areas, supporting essential services such as lighting, communication, healthcare, education, and water pumping. Remote MGs can significantly improve the quality of life and economic opportunities for remote communities. These different types of MGs cater to specific needs and priorities based on their intended application and location. Each type has unique challenges and considerations in terms of design, operation, and integration with existing infrastructure [60,62].

The microgrid architecture consists of power sources, such as DERs and RESs, equipped with microgrid controllers, as well as the assets that ensure utility connections. Intelligent-power electronic devices are essential for controlling the power conversion processes between MGs and generation sources. A microgrid control infrastructure is established with centralized and distributed controllers. The central controllers are connected to the microgrid central controller (MGCC), which improves and enhances the operation of the microgrid. The MGCC determines power demand, optimization conditions, and load capacities while considering auxiliary services of the distribution system. Control signals are sent to controllable field loads and microgrid controllers to implement the defined optimization and operating scenarios. If needed, noncritical and flexible loads can be

disconnected from the grid. Real-time measurements of active and reactive power are performed. MG controllers interact with central and load controllers in the overall distributed control strategy, aiming to supply maximum available electricity to the grid while considering market conditions. This technique is enhanced to address MGCC issues in systems with numerous DG sources and locally made decisions. Figure 1 illustrates a generic representation of the control techniques applied to a microgrid configured with various source and load types. In this scenario, the microgrid concept is managed by a microsource control system (MCS) where load controllers (LCs) handle controllable loads defined by load models. Each microgrid infrastructure is connected to a central controller (CC) through a distribution management system (DMS) or distribution system operator (DSO). These controllers handle medium-voltage (MV) and low-voltage (LV) controls in architectures with multiple MGs. The MGs consist of several layers and control loops, similar to typical utility grids. This hierarchical control scheme addresses fundamental infrastructure and dynamic interface requirements while enabling integration through central and distributed control systems [60,63,64].

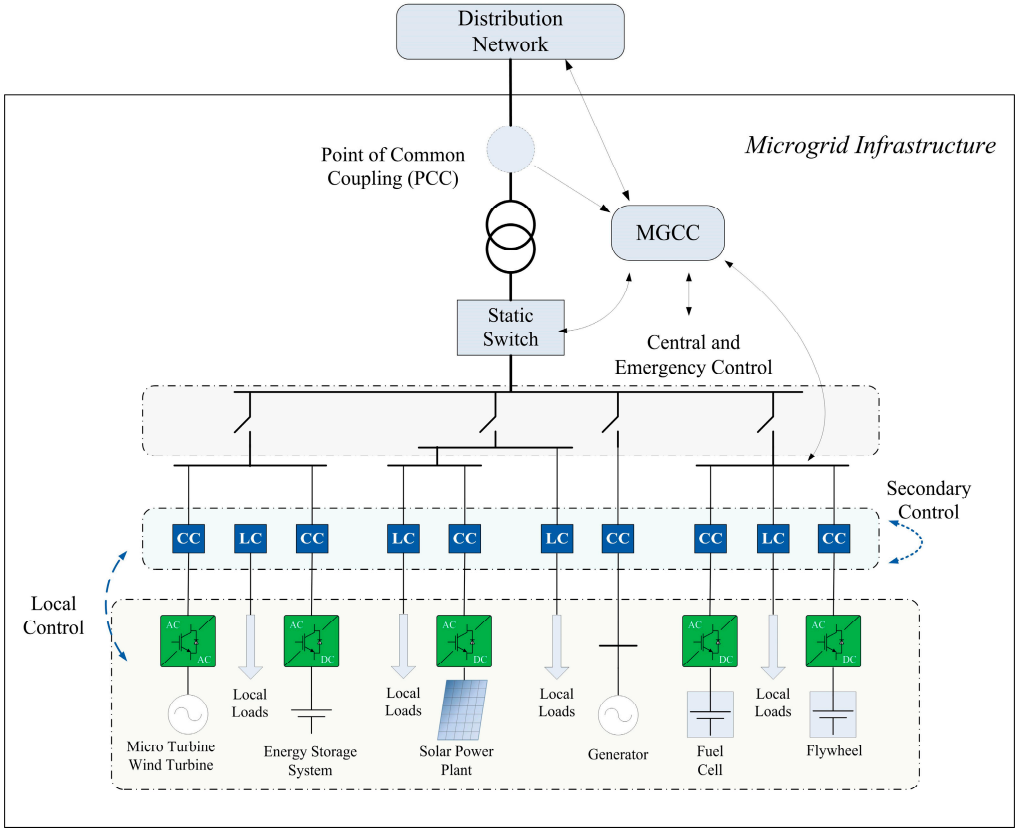

Figure 1. The block diagram of a detailed microgrid architecture with controller infrastructures.

To integrate DGs and RESs within a microgrid infrastructure, various control systems are implemented. The local control section includes primary control systems such as voltage and current control loops. The secondary control is responsible for regulating frequency and mean voltage deviations that occur due to load or source fluctuations. It also manages local auxiliary services. The central and emergency control layer handles protection and emergency control protocols to ensure the reliability of the microgrid. Emergency control techniques estimate faults by implementing protective and regulatory measures.

The coordination between distribution networks and MGs is established through the general control, which ensures the efficient operation of MGs. The general control infrastructure, as depicted in Figure 1, manages power flow control and acts as the interface between the MGCC and the distribution network. This control interface ensures the

distribution of power at the desired levels by controlling the entire microgrid infrastructure. Communication channels are required between the different control layers depicted in the schematic diagram of the microgrid in Figure 1. The secondary and emergency controllers function as central controllers (CCs), while the local controllers within the MGs are referred to as distributed controllers. The general control processes may take minutes to an hour to complete. The general controller sends control signals to the central level controllers and other controllers connected to the distribution systems. Furthermore, the CC has the ability to quickly coordinate the actions of local and secondary controllers (SCs) within the microgrid. The SC mechanism can respond to system faults or command requests within seconds. Local controller (LC) systems are intended to function autonomously and in accordance with specified event timetables [47,65–67]. The detailed introduction of LCs, SCs, general controllers, and central and emergency controllers are presented under MG control sections in the paper.

Microgrid architectures are typically implemented in three types: AC, DC, and hybrid topologies. These architectures are based on the concept of integrating various microsources and loads into a single entity, which can be seen as a dispatchable prosumer within the power system. AC MGs gained recognition as a crucial component for integrating DGs and ESSs while providing power autonomy from the utility grid. This led to significant advancements in AC microgrid research over the past decade. The use of power electronics in MGs can be traced back to the control of parallel inverters in uninterruptible power supplies (UPSs). Alongside the development of AC MGs, there have been advancements in DC MGs. In 2004, Ito et al. reported one of the earliest research prototypes of a DC microgrid with a capacity of 10 kW. They highlighted the advantages of simpler control and superior efficiency and reliability compared to their AC counterparts. These developments in AC and DC MGs have contributed to the dynamic progress in microgrid research, enabling the integration of DGs and storage systems while enhancing efficiency and reliability in power systems [68]. Subsequently, further research and studies expanded on the concept of DC MGs, demonstrating their versatility in various applications such as telecommunications systems, data centers [69], distributed RESs, ESSs, and residential uses [70]. DC MGs have emerged as a distinct research field, particularly with the proliferation of consumer electronics, integration of RES, and the growth of the electric vehicle (EV) market along with its associated charging infrastructure.

In an AC microgrid, RESs and loads are connected to a single AC bus. However, AC MGs face challenges in terms of control and operation, which have been identified as their main drawback. Overall, the development of DC MGs has offered promising alternatives and solutions to address the limitations of AC MGs, opening up new possibilities for efficient and effective energy management in various applications and sectors.

Additionally, Figure 1 illustrates a typical AC microgrid structure where both AC and DC resources are connected to the AC busbar and integrated with the utility grid through a static switch. AC MGs can be classified into three types based on the distribution system architecture: single-phase, three-phase three-wire, and three-phase four-wire. In contrast, DC MGs offer several advantages over AC MGs in terms of reliability and efficiency. They can be connected to various distribution energy resources and exhibit robust stability against external factors. DC MGs utilize simpler power electronic devices and control methods, making their management and operation easier, particularly in coordinating ESSs within the infrastructure. Unlike AC MGs, DC MGs are not affected by issues related to reactive power or frequency control, such as circulating reactive currents or harmonic distortions. Synchronizing DC MGs with the main AC grid only requires voltage magnitude adjustments, whereas AC MGs need to consider voltage magnitude, frequency, and phase shift between each PCC. Furthermore, when integrating different DG sources, DC MGs demonstrate relatively higher energy efficiency due to shorter transmission distances and more effective utilization of ESSs. However, one drawback of DC MGs is their higher capital cost, despite offering lower operating costs and occupying smaller physical space compared to AC MGs [1,8,64].

Figure 2 illustrates the structure of a hybrid microgrid including PV power plants, wind turbines, and fuel cell stack. In such an MG infrastructure, DERs are integrated over the islanded DC and AC busbars, as seen in the figure. The power flow between islanded subgrids of MG and the utility grid is managed via the interface of power electronic converters, which can manage bidirectional power flow. The direction of power flow between load and sources is determined using generation potential of DERs. If there is excess generation capacity, energy storage devices such as fuel cell stacks or batteries are charged. Hybrid MGs are built with the intention of increasing network efficiency overall. As a result, they have been designed to minimize conversion stages, boost reliability, minimize the number of interfacing devices, and lower energy costs. The various literature has reported on a lot of research on the use, safety, and stability of DC, AC, and hybrid MGs [1,59,71–78]. MGs provide increased reliability and flexibility to the utility grid during fault conditions and grid problems. They can continue operating even when the utility grid is down, thanks to their ability to generate power at close proximity to loads. MGs reduce the demand on the grid and utilize their ESSs as a feedback system to support the utility grid. However, the reliability of the microgrid can be a concern for the utility grid if the microgrid protection is not properly ensured. Common protection devices such as fuses, reclosers, and circuit breakers, which are typically installed at the distribution level, may not provide adequate protection for the microgrid. This is due to the significant difference in short-circuit capacity between the utility grid and the microgrid or any DG source within the microgrid. Coordinating and arranging protection devices becomes challenging due to this capacity inequality.

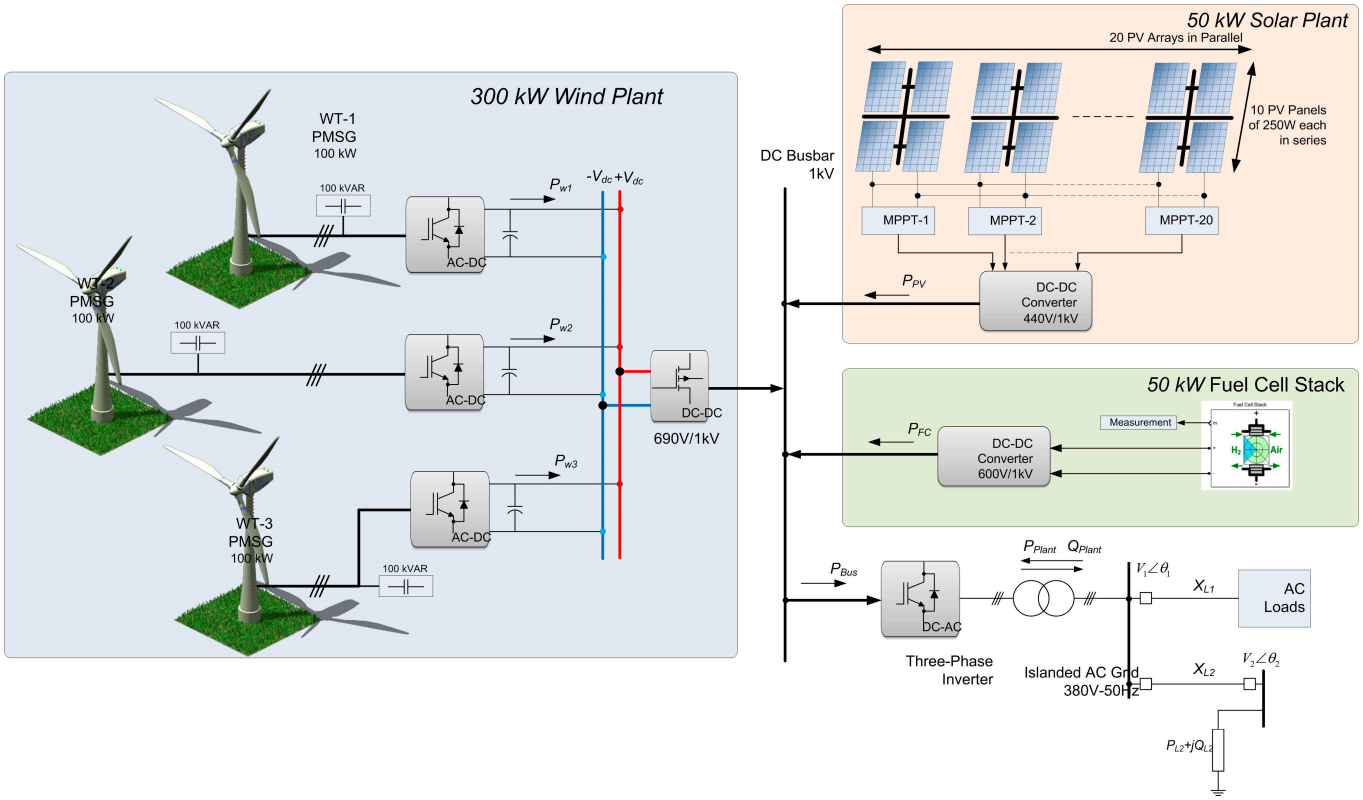

Figure 2. Schematic diagram of a hybrid microgrid.

Microgrid protection research has gained more attention, and various novel techniques have been developed and improved. To ensure commercial and industrial use, MGs should undergo testing and verification based on safety recommendations. Currently available directional overcurrent, distance, and differential relays used in transmission and distribution networks are being utilized in MGs. Although these relays were not specifically developed

for MGs, they offer more sensitive protection infrastructures to handle challenging short-circuit levels in MGs. Despite the differences in fault characteristics and configurations between MGs and utility grids, it is expected that these relays will operate successfully in microgrid protection, similar to their performance in the main grid infrastructure [60,79].

2.3. Benefits and Challenges of MGs

One of the key benefits of MGs is their ability to improve the reliability and resilience of the energy system. This section elaborates on how MGs achieve enhanced reliability and resilience through various mechanisms. MGs mitigate the risk of a single point of failure by distributing energy generation and storage across multiple sources. In traditional centralized grids, a disruption in one location can lead to widespread blackouts. In contrast, MGs can isolate specific areas and continue to provide electricity even if the main grid experiences an outage. This capability is particularly valuable in critical infrastructure facilities such as hospitals, military bases, and data centers, where uninterrupted power supply is essential. MGs have the ability to operate in "island mode" during emergencies or when intentionally disconnected from the utility grid. By leveraging local generation and storage resources, MGs can continue to provide electricity to connected loads even if the main grid fails. This grid independence enables MGs to support crucial services during natural disasters, severe weather events, or other disruptions. The ability to isolate and operate independently enhances the resilience of the energy system and reduces dependence on external sources. Islanding refers to the ability of an MG to operate autonomously and independently from the main power grid. MGs are mainly designed to detect disruptions in the utility grid, such as power outages or faults, and swiftly disconnect from the grid to operate in island mode. When disconnected, the MG relies on its local energy resources, including generation and storage, to meet the energy needs of connected loads. The ability to seamlessly transition into islanding mode ensures a continuous power supply to critical loads during grid disturbances [31,63,80,81].

Islanding provides an additional layer of resilience and reliability to the energy system. In the event of a major grid failure or natural disaster, MGs can continue to function independently, supplying electricity to critical facilities such as hospitals, emergency response centers, or water treatment plants. By isolating from the main grid, MGs are less vulnerable to widespread outages caused by cascading failures or external disturbances, ensuring the continuity of essential services. Islanding enables MGs to have greater control over their energy management. When operating independently, MGs can optimize the use of available energy resources based on local demand, renewable energy generation, and storage capacity. This flexibility allows MGs to prioritize renewable energy utilization, reduce reliance on fossil fuels, and optimize energy generation and consumption patterns without the constraints imposed by the main grid. Once the main grid is restored, MGs can seamlessly transition from island mode back to grid-connected operation. The reconnection process involves synchronization with the utility grid's voltage and frequency levels to ensure a smooth and safe transition. The ability to synchronize and seamlessly reconnect to the main grid allows MGs to benefit from grid-supplied electricity, import or export surplus energy, and participate in grid services such as ancillary services or demand response programs. Islanding enhances energy security and independence by reducing reliance on the main grid. MGs can deploy local energy resources, including renewable energy generation and energy storage, to meet their energy needs. This reduces vulnerability to external disruptions such as fuel supply interruptions, grid failures, or geopolitical factors that may affect centralized energy systems. By diversifying energy sources and promoting local generation, MGs contribute to a more resilient and self-sufficient energy infrastructure. Islanding is particularly valuable in remote or off-grid areas where extending the main grid is logistically or economically challenging. MGs can be deployed in such locations, providing reliable and sustainable energy access to communities, industries, and infrastructure. By establishing self-contained energy systems, MGs enable remote areas to develop independently and foster economic growth without relying on centralized grids [50,63,82].

MGs enable rapid response to changes in demand and supply conditions. With advanced control systems and real-time monitoring, MGs can quickly adjust the generation, storage, and consumption patterns to match the load requirements. This load-balancing capability improves the overall reliability of the system by avoiding overloads, reducing voltage fluctuations, and minimizing the risk of cascading failures. MGs often incorporate diverse energy sources, including renewable energy technologies such as solar, wind, and biomass, as well as conventional generation sources such as natural gas or diesel generators. This diversity provides redundancy in the energy supply, ensuring that even if one energy source is temporarily unavailable, others can compensate. It reduces reliance on a single source of fuel or technology, thereby enhancing the overall reliability and resilience of the microgrid. Enhanced fault detection and self-healing features are other benefits provided by the MGs. MGs employ advanced monitoring and control systems that enable rapid fault detection and self-healing capabilities. Through real-time monitoring, anomalies and faults can be quickly identified, allowing for swift corrective actions. Intelligent control algorithms and automation mechanisms enable the MG to reconfigure itself, isolate faulty sections, and reroute electricity flow to ensure continuous power supply to critical loads. MGs with decentralized generation and energy storage resources can maintain stable voltage and frequency levels, even during fluctuations in the main grid. This stability is crucial for sensitive equipment, industrial processes, and electronics. By avoiding voltage sags, surges, and frequency deviations, MGs provide a reliable and high-quality power supply.

MGs enhance reliability and resilience by reducing single points of failure, enabling islanding and grid independence, providing fast response and load balancing, incorporating diverse energy sources, implementing fault detection and self-healing mechanisms, and maintaining voltage and frequency stability. These features make MGs well suited for critical infrastructure, remote areas, and environments prone to disruptions, thereby ensuring a reliable and robust energy supply [46,74,83,84].

In addition to their technical benefits, MGs offer numerous cost savings and economic benefits that make them an attractive energy solution. The various ways MGs contribute to cost savings and deliver economic advantages are also briefly described. MGs enable energy cost savings through several mechanisms. First, by generating electricity locally, MGs avoid transmission and distribution losses associated with long-distance power delivery in centralized grids. This results in higher overall energy efficiency and reduced energy losses, leading to cost savings. Additionally, MGs can leverage RESs, such as solar and wind, which have lower operating and fuel costs compared to conventional fossil-fuel-based generation. As renewable energy costs continue to decline, MGs become more financially viable and offer greater long-term savings. On the other hand, MGs facilitate demand response programs that allow customers to adjust their energy consumption patterns based on price signals or grid conditions. This flexibility helps optimize energy usage during peak demand periods, when electricity prices are typically higher. By implementing load management strategies, MGs can shift energy consumption to off-peak hours or curtail noncritical loads, resulting in cost savings for both microgrid operators and consumers. Additionally, MGs can participate in demand response programs and earn financial incentives for providing load-reduction services to the grid.

In cases where the existing grid infrastructure is aging or inadequate to meet increasing demand, MGs offer an alternative that can avoid or defer costly infrastructure upgrades. Instead of investing in costly transmission and distribution infrastructure expansion, MGs can be deployed to supply to local energy needs. This reduces the burden on the central grid and the associated capital expenditure, offering significant cost savings. MGs with excess generation capacity can participate in energy trading or sell surplus energy back to the main grid. Through power purchase agreements (PPAs), MGs can enter into contracts to supply electricity to neighboring entities or utilities, generating additional revenue streams. In certain jurisdictions, MGs can also participate in electricity markets and earn revenue through the sale of energy and grid services, such as frequency regulation or capacity support. Microgrid deployment and operation create employment opportunities

ranging from construction and installation to ongoing maintenance and management. This contributes to local economic development by stimulating job growth and generating income for the community. Moreover, MGs can attract new businesses and industries to an area by offering reliable, sustainable, and cost-effective energy solutions, thereby fostering economic growth and revitalization [85–88].

In conclusion, MGs offer various cost savings and economic benefits, including reduced energy costs, demand response capabilities, avoidance of infrastructure upgrades, revenue generation through energy trading, enhanced energy resilience, job creation, local economic development, and the provision of grid support services. These economic advantages make MGs an attractive investment and energy solution for a wide range of stakeholders, including businesses, communities, and governments.

3. Design and Operation of Microgrids

The design and operation of MGs involve multiple components, including power sources, storage systems, control systems, and management strategies. Additionally, the optimization of MGs is critical in achieving efficient and cost-effective energy production and delivery. This part of the paper focuses on the components and configurations of MGs, the control and management strategies used to operate them, the optimization techniques used to improve their efficiency, and the stability and resilience of MGs in the face of various challenges.

3.1. Components and Configurations of MGs

A microgrid consists of several components that work together to provide a complete and reliable power supply to the consumers. Although it can be further detailed, the four basic components of a microgrid are illustrated in Figure 3.

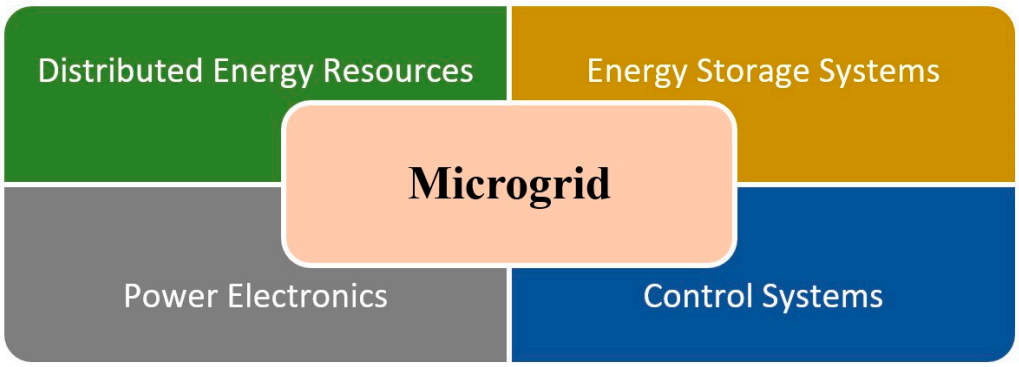

Figure 3. Four basic components of a microgrid.

Distributed Energy Resources (DERs): DERs are the primary source of energy in MGs. They include RESs such as solar panels, wind turbines, and hydroelectric generators, as well as nonrenewable sources such as diesel generators. These resources provide the power required to meet the energy demands of the microgrid. As MGs continue to grow, managing these resources has become a complex task [21,89].
Energy Storage Systems (ESSs): ESSs are used to store energy generated by DERs during off-peak hours or when there is an excess supply of energy. The stored energy can be used during peak hours or when the DERs are unable to generate enough power. ESSs are typically batteries or flywheels that can store energy in the form of electrical or mechanical energy, respectively [3,28].
Power Electronics: Power electronics are used to manage the flow of energy between the DERs, ESSs, and loads. They include inverters, converters, and controllers that convert DC to AC power, and regulate the voltage and frequency of the power supply [90]. Power electronics are critical in ensuring that the microgrid operates efficiently and safely.

Control Systems: Control systems are used to monitor and control the operation of the microgrid. They include software and hardware systems that manage the flow of energy and ensure that the microgrid operates within safe and reliable limits [3,11,16].

MGs can be configured in several ways, depending on their size, the types of DERs used, and the energy demands of the consumers. Here are the most common configurations of MGs:

Grid-Connected Microgrids: Grid-connected MGs are connected to the main grid and operate in parallel with it. In this configuration, the microgrid can either import or export power to the main grid, depending on the energy demand and supply [9,91]. Grid-connected MGs provide backup power during power outages and reduce the energy demand on the main grid.

Islanded Microgrids: Islanded MGs operate independently of the main grid and rely solely on their own DERs and ESSs to meet the energy demands of the consumers. Islanded MGs are typically used in remote areas where there is no access to the main grid [92,93].

Hybrid Microgrids: Hybrid MGs combine renewable and non-RESs to provide a reliable and flexible power supply. They typically use RESs such as solar panels and wind turbines as the primary source of energy and nonrenewable sources such as diesel generators as a backup [15,94].

The advantages and disadvantages of each type of microgrid can vary depending on the specific implementation and the needs of the community it serves. Factors such as the availability of renewable energy resources, the reliability of the main power grid, and the cost of infrastructure investment can all play a role in determining the most suitable type of microgrid for a particular community. Table 1 compares the different types of MGs, focusing on their basic advantages and disadvantages.

Table 1. A general comparison table among different types of microgrids.

Type	Advantages	Disadvantages
Grid-Connected Microgrid	Can provide backup power during power outages. Can help reduce strain on the main power grid during peak hours. Can be more cost-effective than islanded microgrids, as it leverages the existing grid infrastructure.	Requires a reliable connection to the main power grid. May not be able to operate independently for extended periods of time. May not be able to provide power to remote areas without additional infrastructure investment.
Islanded Microgrid	Can operate completely independently from the main power grid, providing power in remote areas. Can provide a reliable source of power during disasters. Can potentially be more reliable than grid-connected microgrids, as it is not dependent on the main power grid.	Requires significant upfront investment in infrastructure. May be less cost-effective than grid-connected microgrids, as it requires its own infrastructure. May be less reliable than grid-connected microgrids if backup power sources are not available.
Hybrid Microgrid	Can provide backup power during power outages. Can operate independently from the main power grid for extended periods of time. Can be more reliable than grid-connected microgrids, as it has backup power sources. Can be more cost-effective than islanded microgrids, as it leverages both grid infrastructure and its own infrastructure.	Requires a reliable connection to the main power grid. May be more complex and expensive to operate than other types of microgrids. Requires additional infrastructure investment compared to grid-connected microgrids.

3.2. Control and Management Strategies for MGs

The control and management of MGs is a challenging task that requires careful planning and coordination. As shown in Figure 4, control and management strategies of MGs can be classified into three main categories: centralized, decentralized, and hybrid [95].

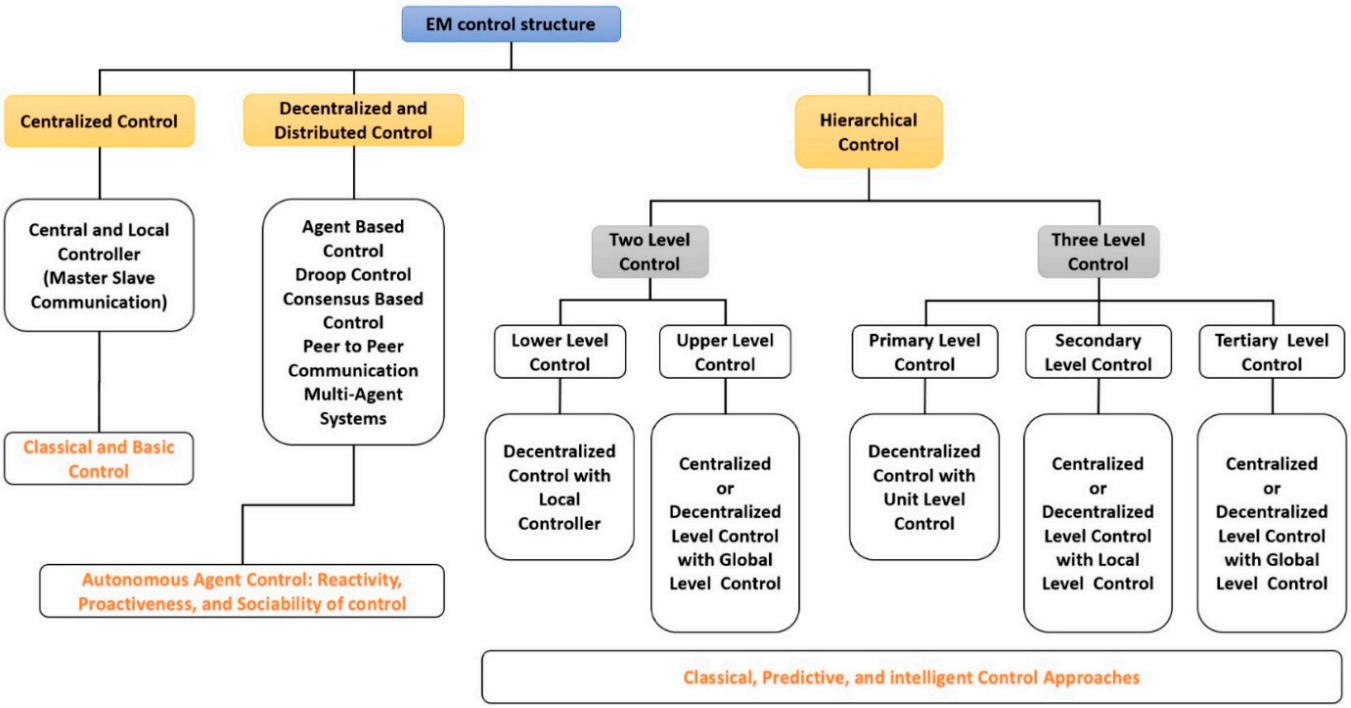

Figure 4. Control and management strategies of microgrids [95].

Centralized control is the most common approach to microgrid control and management [7,96]. It involves a central control system that monitors and controls all the DERs within the microgrid. The central control system uses sophisticated algorithms to optimize the operation of the DERs, taking into account the available resources, load demand, and energy storage capacity. Centralized control is particularly useful for MGs with a large number of DERs, as it allows for efficient management of the system [3,15].

Decentralized control involves the distribution of control across multiple entities, with each DER having its own control system. This approach is particularly useful for MGs with a small number of DERs, as it allows for greater flexibility and resilience in the event of a failure in one of the DERs [95,97]. Decentralized control also reduces the need for complex communication and coordination between DERs, as each unit operates independently.

Hybrid control combines elements of centralized and decentralized control to achieve the benefits of both approaches. This approach is particularly useful for MGs with a moderate number of DERs, as it allows for efficient management of the system while also providing flexibility and resilience. Hybrid control can be achieved through the use of multiple control systems that operate in parallel or through the use of a hierarchical control structure [52,98].

The control and management of MGs are essential to ensure their efficient and reliable operation. Centralized, decentralized, and hybrid control and management strategies can be used, depending on the size and complexity of the microgrid. Table 2 presents a comparison table between centralized control, decentralized control, and hybrid control. The comparison parameters in this table include the control method, level of system optimization, communication and coordination requirements, and control system infrastructure and management cost. Centralized control provides efficient management of the system and optimization of DERs operation. However, the communication and coordination issues can

lead to a single point of failure, and the infrastructure and management costs can be higher. Decentralized control offers flexibility in the system, resilience, and reduced communication and coordination issues. However, there is a lack of system-wide optimization and difficulty in scaling up due to the number of controllers required. Hybrid control balances the advantages of centralized and decentralized control, providing efficient management of the system, flexibility, and resilience. However, the design and implementation of control systems can be complex, and the cost can be higher.

Table 2. A general comparison table among control strategies for microgrids.

Strategy	Advantages	Disadvantages	Microgrid Size
Centralized Control	Efficient management of the system, optimization of DERs operation. Ability to take into account a wide range of variables and constraints for optimal system performance.	Communication and coordination issues, leading to a single point of failure. Higher infrastructure and management costs.	Large microgrids with a high number of DERs.
Decentralized Control	Flexibility in the system, resilience, and reduced communication and coordination issues. Ability to continue operating if parts of the system fail.	Lack of system-wide optimization, and the possibility of suboptimal performance overall. Difficulty in scaling up due to the number of controllers that would be required.	Small microgrids with a low number of DERs.
Hybrid Control	Efficient management of the system, flexibility, and resilience. Ability to balance the advantages of centralized and decentralized control Better ability to respond to sudden changes in the system.	Complexity in designing and implementing control systems, and higher cost.	Moderate-sized microgrids with a moderate number of DERs.

As seen from Table 2, the choice of control strategy for a microgrid depends on various factors, such as the size, complexity, and specific needs of the microgrid. Future research in this field should focus on developing more advanced algorithms and control systems, adopting standardized communication protocols and architectures, and integrating MGs with the larger power grid. The successful implementation of these strategies can provide cost-effective, reliable, and sustainable energy to communities around the world.

3.3. Optimization Techniques for Microgrids

There are several optimization techniques used in MGs to improve their performance, efficiency, and reliability. Although there may be additional advantages and disadvantages for each technique depending on the specific application and system requirements, Table 3 compares the most prominent pros and cons of the commonly used optimization.

Table 3. The most prominent pros and cons of the commonly used optimization techniques.

Optimization Technique/Method	▲ Pros	▼ Cons
Economic Dispatch	Minimizes the cost of meeting the load demand.	Does not consider long-term system planning.
Power Flow Analysis	Improves the voltage and frequency stability, reduces losses, and maximizes the use of renewable energy resources.	Requires detailed modeling of the microgrid.

Table 3. *Cont.*

Optimization Technique/Method	▲ Pros	▼ Cons
Energy Management Systems	Optimizes the use of energy resources, including storage, generation, and load, to meet demand and minimize energy costs.	Requires sophisticated software and hardware.
Load Shedding	Helps prevent blackouts and improves the microgrid's reliability.	Can result in inconvenience and discomfort for customers.
Demand Response	Stabilizes the microgrid and prevents blackouts.	Requires incentives for customers to participate.
Stochastic Optimization	Optimizes the performance of the microgrid under uncertain conditions.	Requires extensive computational resources.
Model Predictive Control	Predicts the future behavior of the system and optimizes the control actions accordingly.	Can be computationally expensive.
Fuzzy Logic Control	Optimizes the operation of the microgrid by defining rules that describe the relationship between inputs and outputs.	Limited ability to handle complex systems.
Mixed-Integer Linear Programming	Optimizes the operation of the microgrid using both continuous and integer variables.	Can be computationally expensive for large-scale systems.
Genetic Algorithms	Optimizes the operation of the microgrid through a process of selection, mutation, and crossover.	Requires a large number of potential solutions to be evaluated.
Artificial Neural Networks	Optimizes the operation of the microgrid by learning from historical data.	Requires extensive data to train the network.
Particle Swarm Optimization	Optimizes the operation of the microgrid by "swarming" around the search space.	Can be sensitive to the initial conditions and parameters.
Reinforcement Learning	Optimizes the operation of the microgrid through trial and error.	Requires a large number of iterations to converge.
Multiobjective Optimization	Optimizes multiple conflicting objectives simultaneously.	Can be computationally expensive for complex systems.

Economic Dispatch: This technique optimizes the operation of DERs in a microgrid to minimize the cost of meeting the load demand. It involves determining the optimal power output of each DER in the microgrid while taking into account operational constraints such as capacity, ramp rates, and minimum and maximum power output [19,97].
Power Flow Analysis: Power flow analysis is a mathematical technique used to calculate the flow of power through a microgrid network. By modeling the microgrid's power flow, engineers can optimize the microgrid's voltage and frequency stability, reduce losses, and maximize the use of renewable energy resources [99].
Energy Management Systems: Energy management systems (EMSs) are software programs that manage and control the operation of a microgrid [92,100,101]. They optimize the use of energy resources, including storage, generation, and load, to meet demand and minimize energy costs.
Load Shedding: Load shedding is a technique used to reduce demand in a microgrid during peak periods or emergencies. It involves disconnecting noncritical loads from the microgrid to balance the demand and supply of energy resources. By reducing demand, load shedding can help prevent blackouts and improve the microgrid's reliability [102,103].
Demand Response: Demand response involves incentivizing microgrid customers to reduce their energy consumption during peak periods or when the microgrid is experiencing high

demand [89,104]. By reducing demand, demand response can help stabilize the microgrid and prevent blackouts.
Stochastic Optimization: Stochastic optimization is a technique used to optimize the performance of a microgrid under uncertain conditions. It involves modeling the probability of different outcomes and optimizing the system's operation to maximize expected value [105,106].
Model Predictive Control: Model predictive control (MPC) is a technique used to optimize the operation of a microgrid by predicting the future behavior of the system and optimizing the control actions accordingly. MPC uses mathematical models of the microgrid and predictive algorithms to optimize the system's operation [107,108].
Fuzzy Logic Control: Fuzzy logic control is a technique used to optimize the operation of a microgrid by defining rules that describe the relationship between inputs and outputs [109]. It involves using linguistic variables to define control rules that can be used to optimize the operation of the system.
Mixed-Integer Linear Programming: This technique is used to optimize the operation of a microgrid by formulating an optimization problem with both continuous and integer variables. The objective function and constraints are then expressed as linear equations, and an optimal solution is obtained using linear programming techniques [110,111].
Genetic Algorithms: Genetic algorithms are a type of evolutionary algorithm used to optimize the operation of a microgrid. They involve creating a population of potential solutions and iteratively improving them through a process of selection, mutation, and crossover [100].
Artificial Neural Networks: Artificial neural networks (ANNs) are used in MGs to optimize the operation of the system by learning from historical data. ANNs are trained on data from the microgrid to develop a model of the system's behavior [2,94], which can then be used to predict future performance and optimize the operation of the system.
Particle Swarm Optimization: Particle swarm optimization (PSO) is an optimization technique inspired by the collective behavior of swarms of birds or insects [16,18]. It involves creating a population of potential solutions that "swarm" around the search space, with each individual adjusting its position based on its own experience and the experience of other individuals.
Reinforcement Learning: Reinforcement learning is a machine learning technique used to optimize the operation of a microgrid by learning through trial and error [102,112]. The microgrid is modeled as an agent interacting with an environment, with the objective of maximizing a reward signal. The agent learns from experience, adjusting its actions based on the feedback it receives.
Multiobjective Optimization: Multiobjective optimization is used in MGs to optimize multiple conflicting objectives simultaneously. The optimization problem is formulated as a multiobjective function, and the solution space is searched to identify the optimal trade-off between the objectives [113–115].

This section discussed a selection of commonly used optimization techniques in MGs. The optimal choice of optimization technique depends on the specific requirements of the microgrid and the nature of the optimization problem being addressed. For instance, if the goal is to minimize costs, economic dispatch or mixed-integer linear programming may be a suitable choice, whereas if the goal is to optimize performance under uncertain conditions, stochastic optimization or reinforcement learning may be more appropriate. Ultimately, the choice of optimization technique should be guided by a thorough understanding of the microgrid's characteristics and objectives.

4. Digitalization of MGs

The use of digital technologies in electric power systems has been evolving over several decades, and there have been several milestones in this journey. Table 4 presents some key milestones in the history of digital technologies in electric power systems.

Table 4. Key milestones in the history of digital technologies in electric power systems.

Years	Milestones
1970s	The development of supervisory control and data acquisition (SCADA) systems enables remote monitoring and control of power system components.
1980s	The introduction of microprocessor-based digital relays improves the accuracy and reliability of power system measurements and monitoring. The development of phasor measurement units (PMUs) enables real-time monitoring and analysis of power system dynamics.
1990s	The introduction of digital protective relays replaces traditional electromechanical relays, leading to better accuracy, faster response times, and more advanced fault detection and diagnosis.
2000s	The use of digital communication technologies such as fiber-optic cables and wireless networks facilitates the integration of DERs such as solar panels and wind turbines into the power grid. The development of synchro phasors enables the measurement and visualization of power system dynamics in real time, leading to improved situational awareness and enhanced stability. The adoption of smart grid technologies enables the integration of advanced sensors, communication networks, and automation systems, leading to greater efficiency, reliability, and sustainability of the power grid.
2010s	The advent of big data analytics, machine learning, and artificial intelligence (AI) enables advanced data processing and predictive modeling, leading to improved forecasting, fault detection, and outage management. The development of cloud computing platforms enables the processing and storage of large amounts of data generated by the power system, leading to improved data analytics and decision making. The introduction of virtual power plants (VPPs) enables the aggregation and management of DERs, leading to more efficient and flexible energy management.
2020s	The use of digital twins, which are virtual replicas of physical assets, in the power system has the potential to improve asset management, maintenance, and planning, leading to improved reliability and cost-effectiveness. The development of blockchain technology and distributed ledger systems has the potential to revolutionize the way energy transactions are managed, enabling secure and efficient peer-to-peer energy trading and billing. The deployment of 5G wireless networks has the potential to enable the integration of more advanced communication and automation systems in the power grid, leading to greater efficiency, reliability, and sustainability.

In parallel to advances in electric power systems, the digitalization of MGs has enabled the integration of various digital technologies, such as DERMSs, MEMSs, IoT devices, big data analytics, blockchain technology, AI, digital twin technology, cloud computing, and augmented reality, allowing for the optimization of microgrid performance and the enhancement of their resilience and stability.

Additionally, one technological trend that aligns with several of these paradigms is open-source technology, encompassing both hardware and software components that are freely available for modification and distribution. Open-source technology offers several advantages in the context of microgrid development and digitalization. Firstly, it fosters collaboration and knowledge sharing within the microgrid community, enabling researchers, practitioners, and developers to exchange ideas, best practices, and innovative solutions. This collaborative environment promotes the rapid advancement of microgrid technologies. Moreover, open-source hardware and software tools provide cost-effective options for implementing and maintaining microgrids [116]. By reducing the financial barriers associated with proprietary systems, open-source technology makes microgrid solutions more accessible and affordable. This affordability factor is especially significant in developing regions and remote communities, where the adoption of microgrids can greatly impact energy access and sustainability goals. To this end, supervisory and remote monitoring systems are improved with the hardware and software technologies enabling IoT-based communication mediums in RESs such as wind and solar PV systems, and in battery ESSs [116–118].

4.1. Distributed Energy Resources Management Systems

In recent years, the deployment of MGs has become increasingly popular due to the need for more reliable and resilient energy systems, particularly in areas with high renewable energy penetration. As the amount of DERs connected to MGs continues to grow, managing these resources has become a complex task [119–121]. To address this challenge, DERMSs have emerged as an innovative solution that provides a centralized platform for controlling and optimizing the operation of microgrid DERs [99,122]. Firstly, it is important to understand the components of DERMSs. DERMSs are essentially software platforms that enable the integration, control, and coordination of various DERs within a microgrid. DERs include solar photovoltaic (PV) systems, wind turbines, ESSs, electric vehicles (EVs), and demand response (DR) systems. The DERMS platform communicates with each of these components, collecting data on their status and performance and using this information to optimize the overall operation of the microgrid [90,123,124].

One of the key benefits of a DERMS is that it allows for real-time control and optimization of the microgrid, which can significantly improve its reliability and efficiency. For example, the DERMS can use advanced algorithms to forecast energy demand and supply, and adjust the output of DERs accordingly. This ensures that the microgrid is always supplying the appropriate amount of energy to meet demand, while minimizing wastage and reducing the need for energy storage. Another advantage of a DERMS is that it enables the integration of RESs into MGs [89,97,120]. RESs, such as solar and wind, are variable in nature, which makes it difficult to predict their output. DERMSs can monitor the output of RESs and adjust the output of other DERs accordingly to maintain grid stability.

However, implementing DERMSs for MGs comes with its own set of challenges. One of the main challenges is the need for data communication and interoperability between different components of the microgrid. This requires standardization of communication protocols and interfaces, which can be a complex and time-consuming process. Additionally, the implementation of DERMSs requires a significant investment in infrastructure and technology, which can be a barrier to adoption [99,122,125,126]. Furthermore, ensuring the security of critical energy infrastructure is crucial, and the integration of distributed energy resources (DERs) is a vital aspect of achieving a more secure and resilient electric grid. As seen from Figure 5, the electric grid consists of interconnected machines, expertly managed by professional operators, and DERs connected at the grid edge must conform to the power system's reliability, safety, and security operations requirements [127].

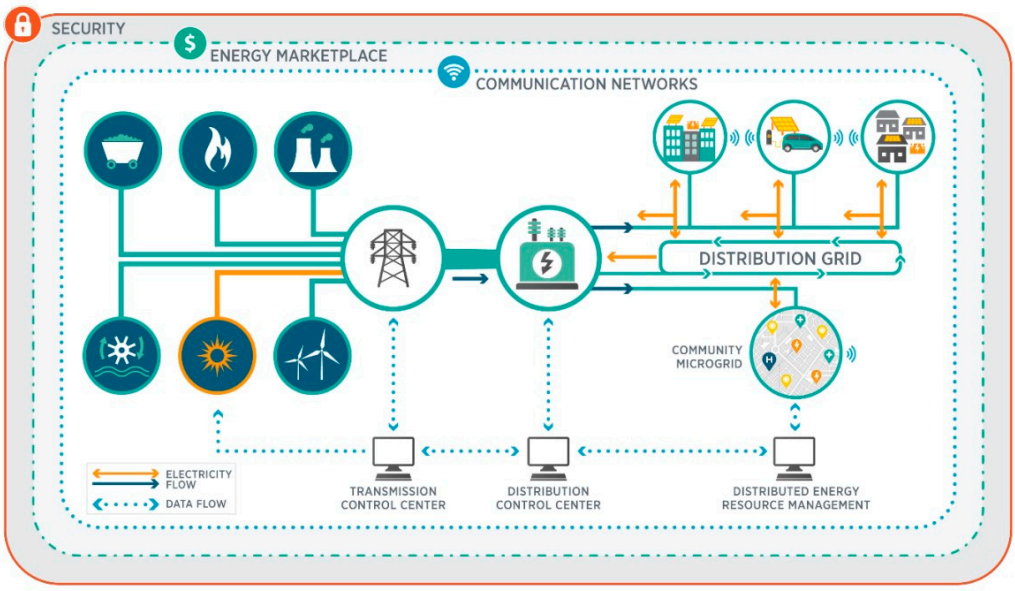

Figure 5. Interconnection of a DERM to the grid and security requirement [127].

It is important to implement measured defenses that consider tiered requirements to balance the risk of compromise with the potential impact, making it a critical industry concern. In conclusion, DERMSs are an innovative solution for managing the operation of microgrid DERs and represent a promising technology that can help accelerate the transition to a more sustainable energy system. Table 5 presents a summarized assessment of DERMSs.

Table 5. A summarized assessment of DERMSs.

Characteristics	Description
Definition	A software platform that manages and optimizes the integration and operation of DERs in a power system.
Key Components	Communication interfaces to DERs, data acquisition and storage, analytics and decision-making algorithms, control and dispatch functions, human-machine interface.
Types of DERs managed	Photovoltaic systems, wind turbines, battery energy storage systems, electric vehicles, combined heat and power systems, fuel cells.
Benefits	Increased reliability and resiliency, improved energy efficiency, lower energy costs, reduced greenhouse gas emissions, improved grid stability and flexibility, integration of RESs, improved visibility and control over DER assets, enhanced customer engagement and satisfaction.
Challenges	Limited interoperability and standardization among DERs, cost and complexity of integration, security and privacy concerns, regulatory and policy barriers, limited awareness and education among stakeholders.
Market Outlook	Expected to grow significantly in the coming years, driven by factors such as the increasing penetration of renewable energy, rising demand for energy management solutions, and advancements in software technology. According to a report by Markets and Markets, the DERMS market is projected to reach USD 750 million by 2026, up from an estimated USD 286 million in 2021 [128].
Leading Vendors	Schneider Electric, Siemens, ABB, General Electric, Honeywell, Sensus, Landis+Gyr, Opus One Solutions, Smarter Grid Solutions, Spirae.

Currently, DERMSs focus on enabling efficient management, control, and optimization of diverse distributed energy resources such as solar panels, wind turbines, energy storage systems, electric vehicles, and demand response technologies. They aim to facilitate grid stability, reliability, and flexibility while maximizing the utilization of distributed energy resources. DERMSs leverage advanced technologies such as data analytics, artificial intelligence, and real-time monitoring to enable better forecasting, coordination, and decision making. These systems enable active management of distributed energy resources, enabling utilities and grid operators to respond to dynamic conditions, optimize energy flows, and ensure grid stability. Furthermore, DERMSs are also being integrated with other smart grid technologies, such as advanced metering infrastructure and grid automation, to enhance their capabilities and enable seamless integration of distributed energy resources into the existing power grid. In this context, some of the most frequently used systems in DERMSs include EMSs, SCADA systems, distributed energy resource aggregators, advanced metering infrastructure systems, energy storage management systems, and demand response management systems. It is important to note that the specific systems used in DERMSs can vary depending on the scale, complexity, and requirements of the distributed energy resources being managed. The choice of systems also depends on the preferences and technological capabilities of utilities, grid operators, and energy service providers.

4.2. Microgrid Energy Management Systems

MEMSs are computerized systems that allow for the efficient and reliable operation of MGs. MGs are localized power systems that can operate independently of the tradi-

tional power grid, typically powered by RESs such as solar and wind [1,129,130]. The management of these systems can be complex, as they require coordination between different energy sources and energy storage systems. MEMSs are designed to help with this complexity by monitoring and controlling the microgrid's energy flows, optimizing energy use, and ensuring energy security. Figure 6 illustrates the structure of a sample microgrid energy management system [131].

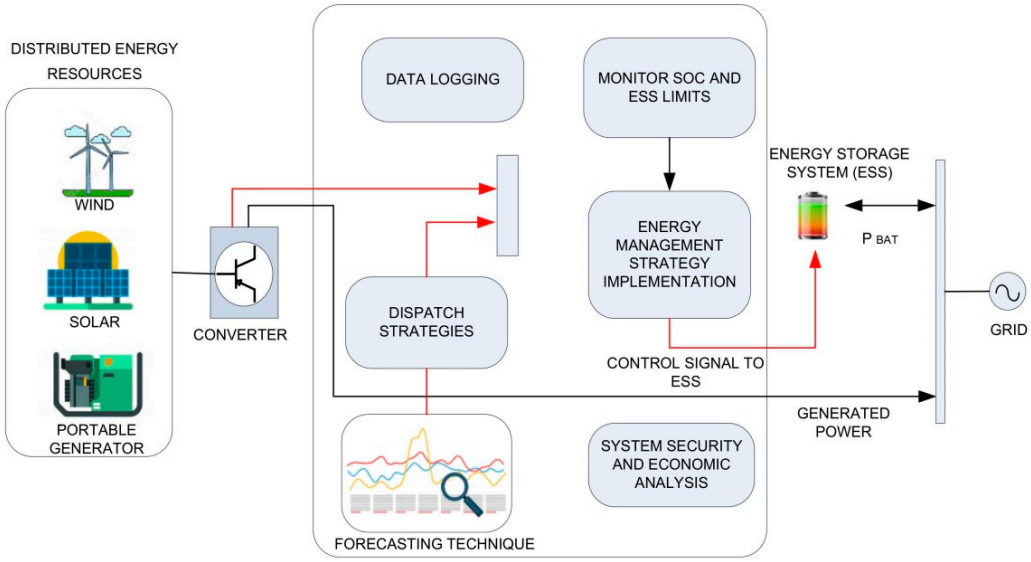

Figure 6. Structure of a sample microgrid energy management [131].

The components of MEMSs can vary depending on the specific design and implementation. However, some common components typically found in an MEMS can be listed as follows:

Power Generation Units: These components encompass various energy sources, such as solar panels, wind turbines, or fuel-based generators, that generate electricity within the microgrid.

Energy Storage Systems (ESSs): Batteries or other storage devices used to store excess energy generated by the microgrid or to provide backup power during high-demand periods or outages.

Load Controllers: Devices or software that manage and control the electricity consumption of different loads within the microgrid, ensuring efficient utilization of energy resources.

Grid Interface: The interface between the microgrid and the utility grid, enabling bidirectional energy flow and coordination with the larger grid system.

Communication Infrastructure: The network infrastructure and protocols that facilitate real-time communication and data exchange between various components of the microgrid.

Sensors and Monitoring Devices: These devices measure and collect data on energy generation, consumption, storage levels, and other relevant parameters within the microgrid.

Control Algorithms: Software algorithms that analyze real-time data and make decisions to optimize energy flow, load balancing, and grid stability.

Human–Machine Interface (HMI): The user interface through which operators or users interact with the MEMS, allowing for monitoring, control, and visualization of the system's performance.

One of the primary functions of MEMSs is to monitor the energy inputs and outputs of a microgrid [91,132]. This includes measuring the production and consumption of energy, as well as tracking the state of energy storage systems. By continuously monitoring the system, MEMSs can identify areas where energy efficiency can be improved, such as reducing energy waste or adjusting the balance of energy inputs. This information

can also be used to predict future energy use and help to optimize the operation of the microgrid [92,100,133].

Another important feature of MEMSs is their ability to control the energy flows within a microgrid. This includes coordinating the use of different energy sources, such as solar, wind, and diesel generators, to ensure a stable and reliable power supply. MEMSs can also manage the energy storage systems within a microgrid, ensuring that energy is stored and used efficiently [134,135]. By regulating the energy flows, MEMSs can help to avoid power outages and ensure that the microgrid remains operational even during periods of high demand.

MEMSs also play a critical role in ensuring the security of energy supply within a microgrid. They can monitor the health of the system, identify any faults or issues, and take corrective action to prevent system failures. MEMSs can also coordinate with other systems, such as local utility companies, to ensure that the microgrid has access to backup power supplies if needed. This helps to ensure that the microgrid can continue to provide energy even during emergencies or disasters [109,136].

The benefits of MEMSs are numerous, including improved energy efficiency, increased reliability and security of energy supply, and greater control over energy costs. By optimizing the use of RESs, MEMSs can help to reduce greenhouse gas emissions and contribute to a more sustainable energy future. MEMSs can also help to reduce energy costs for consumers by optimizing energy use and reducing waste [101].

However, the implementation of MEMSs can also present challenges. The integration of different energy sources and storage systems can be complex, and the software used to manage the system must be carefully designed and tested [137]. Additionally, an MEMS must be able to communicate with other systems, such as the local utility company or other MGs, to ensure a reliable energy supply. The cost of implementing MEMSs can also be a barrier for some communities, although the long-term benefits may outweigh the initial investment.

In conclusion, MEMSs are critical to the efficient and reliable operation of MGs. They help to optimize energy use, coordinate different energy sources and storage systems, and ensure the security of energy supply. While there are challenges associated with their implementation, the benefits of MEMSs are numerous, including increased energy efficiency, reliability, and sustainability. As the use of MGs continues to grow, the importance of MEMSs will only continue to increase, making them a vital component of the energy landscape. Table 6 highlights the key features and characteristics of MEMSs briefly

The current state of MEMSs involves the integration of advanced control algorithms, real-time monitoring, and energy management strategies to ensure efficient and reliable operation of microgrids. These systems aim to balance energy supply and demand, optimize the use of renewable energy resources, and enable seamless integration of distributed energy resources. MEMSs leverage technologies such as data analytics, artificial intelligence, and predictive modeling to make informed decisions regarding energy generation, storage, and consumption. They enable dynamic control of microgrid components, allowing for optimal dispatch of energy sources, load management, and grid stability. Furthermore, MEMSs are evolving to incorporate grid-edge intelligence and advanced communication systems, enabling enhanced coordination and interaction between microgrids and the larger utility grid. This integration facilitates bidirectional energy flow, demand response, and grid support services.

Table 6. Key features and characteristics of MEMSs.

Feature/Characteristics	Description
Definition	Computerized systems that enable efficient and reliable operation of MGs, which are localized power systems that can operate independently of the traditional power grid, typically powered by RESs such as solar and wind.
Energy Monitoring	Continuous monitoring of energy inputs and outputs of a microgrid, including production and consumption of energy, and tracking the state of energy storage systems.
Energy Efficiency Optimization	Identification of areas where energy efficiency can be improved, such as reducing energy waste or adjusting the balance of energy inputs. Prediction of future energy use and optimization of microgrid operation.
Energy Flow Control	Coordination of energy sources to ensure a stable and reliable power supply. Management of energy storage systems to ensure efficient storage and use of energy. Regulation of energy flows to avoid power outages and ensure microgrid operation during high-demand periods.
Energy Security	Monitoring of system health, identification of faults/issues, and corrective action to prevent system failures. Coordination with other systems (local utility companies) to ensure access to backup power supplies during emergencies/disasters.
Benefits	Improved energy efficiency, increased reliability and security of energy supply, greater control over energy costs. Reduction of greenhouse gas emissions and contribution to a more sustainable energy future. Reduction of energy costs for consumers by optimizing energy use and reducing waste.
Challenges	Complex integration of different energy sources and storage systems. Careful design and testing of software used to manage the system. Need for communication with other systems to ensure reliable energy supply. Cost of implementing MEMSs may be a barrier for some communities.
Importance	MEMS are critical to the efficient and reliable operation of MGs. They help to optimize energy use, coordinate different energy sources and storage systems, and ensure the security of energy supply.

4.3. Internet of Things (IoT)

The IoT has emerged as a game-changing technology that is revolutionizing various industries, including the energy sector. In particular, IoT applications have become increasingly relevant in MGs [138–140]. MGs can offer a range of benefits, such as improved energy access, reliability, and cost-effectiveness. The integration of IoT devices in MGs can further enhance these benefits, by enabling real-time monitoring, analysis, and optimization of energy systems.

One of the most significant advantages of IoT in MGs is improved energy efficiency. IoT sensors and controllers can collect real-time data on energy consumption, production, and distribution, which can be analyzed and used to optimize microgrid operations [73]. For example, IoT devices can detect when energy consumption is at its peak and adjust the power supply accordingly, reducing the risk of overloading and minimizing energy waste. Additionally, IoT-enabled MGs can integrate RESs by managing their fluctuating output and ensuring their efficient use. By using IoT technology in MGs, energy providers can improve their energy management, reduce energy waste, and reduce costs, leading to a more sustainable and cost-effective energy system. Another benefit of IoT in MGs is improved reliability and resilience. IoT sensors can detect faults or anomalies in the system, enabling quick identification and resolution of potential issues. This is particularly important in MGs, which rely on localized power generation and distribution, and are more vulnerable to disruptions and failures than the main grid. By using IoT technology, MGs can improve their monitoring and maintenance processes, reducing the risk of downtime and power outages. Additionally, IoT-enabled MGs can incorporate energy storage systems which can store surplus energy for later use and provide backup power during outages. By

leveraging IoT technology in MGs, energy providers can improve energy reliability and resilience, leading to a more stable and secure energy system.

In conclusion, IoT applications have become an indispensable tool for microgrid technology, offering numerous benefits to energy providers and consumers alike. By collecting and analyzing real-time data, IoT devices can optimize microgrid operations, integrate RESs, and improve energy access and reliability. As the world moves towards a more sustainable and decentralized energy system, the role of IoT in MGs is expected to grow, driving innovation and progress in the energy sector. However, the adoption of IoT technology in MGs also poses several challenges, such as data privacy and security, interoperability, and regulatory issues. Energy providers need to address these challenges to ensure the safe and effective deployment of IoT in MGs.

One of the major challenges of IoT in MGs is data privacy and security [138,141]. IoT devices collect and transmit sensitive information, such as energy consumption patterns and user behavior, which can be exploited by cybercriminals if not adequately secured. Energy providers need to implement robust security measures, such as encryption, authentication, and access control, to protect IoT devices and data from unauthorized access and cyberattacks. Additionally, they need to ensure compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR), to protect users' privacy rights. Another challenge of IoT in MGs is interoperability. IoT devices and systems are often developed by different vendors and operate on different protocols and standards, which can hinder their integration and interoperability. Energy providers need to ensure that IoT devices in MGs can communicate and exchange data seamlessly, regardless of their origin and technology. This requires the adoption of open standards and protocols, such as the OpenADR and IEEE 2030.5, that facilitate the integration and interoperability of IoT devices and systems. Furthermore, regulatory issues can also impede the adoption of IoT in MGs [140]. Regulations governing the energy sector may not always be compatible with the deployment of IoT-enabled MGs, which can create legal and administrative barriers. Energy providers need to work closely with policymakers and regulators to ensure that regulations support the deployment of IoT in MGs and foster innovation and competition in the energy sector.

A general SWOT analysis for IoT-enabled MGs is presented in Table 7. To address these weaknesses and capitalize on the opportunities, energy providers and stakeholders must collaborate to overcome the challenges of IoT-enabled MGs. For instance, they could invest in research and development to develop standardized and interoperable IoT devices and systems, which can facilitate integration and scalability. Additionally, they can develop robust data privacy and security protocols to ensure that sensitive information collected by IoT devices is protected from cyberattacks and unauthorized access. To address the high deployment and maintenance costs, stakeholders can develop new business models and financing options to enable more affordable and accessible microgrid systems. This can include partnerships with local communities, governments, and nongovernmental organizations (NGOs) to provide financing options and incentives for microgrid deployment, particularly in remote and underserved areas. By providing access to clean and affordable energy, IoT-enabled MGs can help bridge the energy access gap and enhance the quality of life for many people around the world.

In conclusion, IoT applications in MGs have the potential to transform the energy sector by improving efficiency, reliability, and sustainability. However, stakeholders must address the challenges posed by data privacy and security, interoperability, and regulatory issues to realize the full potential of IoT-enabled MGs. By collaborating and investing in research and development, stakeholders can develop standardized and interoperable IoT devices and systems, while also ensuring data privacy and security. As the world continues to face environmental, social, and economic challenges, IoT-enabled MGs can offer a viable and scalable solution to address these challenges and pave the way towards a more sustainable and equitable energy future.

Table 7. A general SWOT analysis for IoT-enabled MGs.

Strengths	• Increased efficiency and reliability of MGs through real-time monitoring and control of energy generation and consumption. • Facilitation of renewable energy integration, enabling MGs to operate on cleaner sources of energy. • Improved energy access and affordability, particularly in remote or underserved areas. • Better prediction and management of energy demand and supply, reducing energy waste and costs. • Increased resilience and flexibility of MGs to respond to power outages and natural disasters through the use of DERs and intelligent control systems.
Weaknesses	• High deployment and maintenance costs of IoT-enabled microgrid systems. • Dependence on a stable and secure internet connection to ensure reliable communication and operation of IoT devices. • Lack of standardization and interoperability of IoT devices and systems, making integration and scalability challenging. • Potential data privacy and security risks, especially with the collection and transmission of sensitive information. • Regulatory and policy barriers that may hinder the deployment of IoT-enabled MGs in certain areas.
Opportunities	• Growing demand for cleaner and more sustainable energy solutions, creating opportunities for the deployment of IoT-enabled MGs. • Advances in IoT technology, including artificial intelligence and machine learning, could enhance the performance and efficiency of MGs. • Collaboration with other industries, such as the telecommunications and technology sectors, to develop new IoT-enabled solutions for MGs. • Partnerships with governments and NGOs to deploy IoT-enabled MGs in remote and underserved areas, providing access to clean and affordable energy. • Opportunities to monetize data collected by IoT devices through new business models, such as energy trading and demand response programs.
Threats	• Competition from traditional centralized energy systems and other emerging technologies, such as blockchain and peer-to-peer energy trading platforms. • Resistance from stakeholders, such as utilities and regulators, who may perceive IoT-enabled MGs as a threat to their existing business models and revenue streams. • Legal and regulatory barriers that could limit the deployment of IoT-enabled MGs in certain regions or countries. • Rapidly evolving IoT technology, which may render existing systems and devices obsolete or require frequent upgrades and maintenance. • Cybersecurity risks and potential breaches of sensitive information, leading to reputational damage and financial losses.

4.4. Big Data Analytics

Big data analytics refers to the process of examining and analyzing large datasets to uncover hidden patterns, unknown correlations, market trends, customer preferences, and other valuable information that can help businesses make more informed decisions. In the context of MGs, big data analytics involves collecting, processing, and analyzing vast amounts of data generated by various components of the microgrid, including smart meters, sensors, and RESs [142–144]. By combining digitalization and big data analytics, it is possible to create a highly optimized and efficient microgrid that can adapt to changing energy demands and supply conditions. Therefore, big data analytics can play a crucial role in optimizing the performance and efficiency of the grid. The data collected can be used to optimize the performance of the microgrid, improve energy efficiency, reduce operational costs, and enhance the reliability and resiliency of the microgrid. For example, by analyzing the data collected from smart meters, it is possible to identify patterns of energy consumption and make adjustments to the microgrid's operations to reduce energy wastage. Similarly, by analyzing the data generated by sensors, it is possible to identify

potential faults or problems in the system before they cause significant disruptions. As shown in Figure 7, smart grids can manage energy efficiently and dynamically with the use of big data analytics.

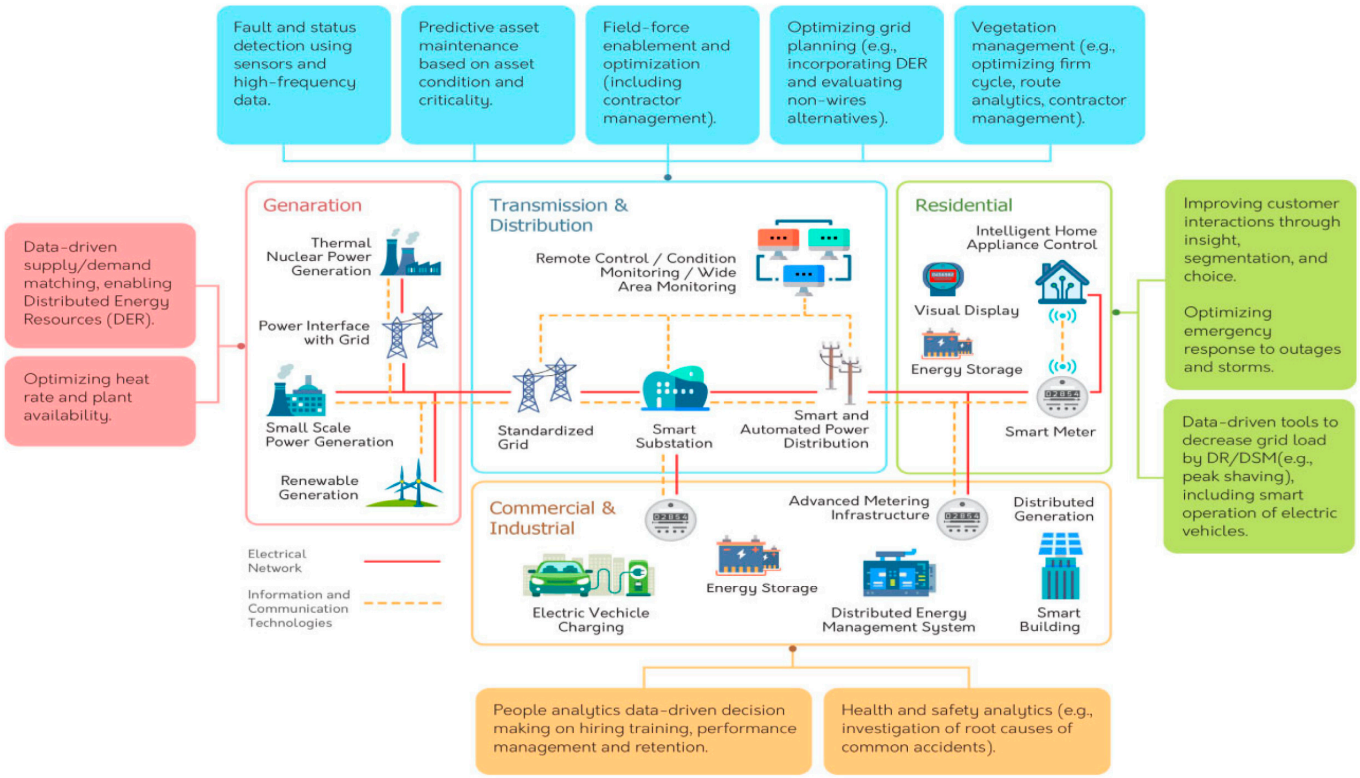

Figure 7. Big data analytics development model with improved grid visualization [143].

When the smart grid and big data are combined, it is possible to optimize power generation in power plants, improve customer interaction, improve emergency response to outages in domestic coverage, plan and optimize transmission and smart distribution from the transmission and distribution sides, and efficiently involve DERs and electric vehicles from the commercial side. The following are some of the ways in which big data analytics can be beneficial in the digitalization of MGs [145–149]:

Improved Energy Efficiency: Big data analytics enables microgrid operators to monitor and analyze the energy consumption patterns of the grid. This can help them identify areas where energy usage can be optimized, leading to improved energy efficiency and reduced costs.

Enhanced Grid Reliability: By analyzing data on energy generation and consumption, microgrid operators can identify potential issues and take proactive measures to prevent equipment failures. This can help to improve the overall reliability of the microgrid and reduce downtime.

Cost Savings: Big data analytics can help microgrid operators identify areas where energy usage can be optimized, leading to cost savings for both the operators and consumers. Additionally, by identifying potential equipment failures before they occur, proactive maintenance can be performed, reducing repair and replacement costs.

Increased Sustainability: MGs are typically composed of RESs such as solar panels and wind turbines. By analyzing data on energy generation and consumption, microgrid operators can ensure that the energy being generated is being used efficiently and effectively, leading to increased sustainability.

Demand Response: Big data analytics enables microgrid operators to predict when demand response will be required and adjust energy consumption accordingly. This can help to reduce peak demand, improve grid stability, and reduce energy costs for consumers.

Improved Decision Making: Big data analytics provides microgrid operators with valuable insights into the grid's performance. This can help them make informed decisions about energy management, maintenance, and grid optimization, leading to improved overall performance and reliability.

Scalability: As MGs continue to grow and expand, big data analytics can help to ensure that the grid remains efficient and effective. By analyzing data on energy generation, consumption, and storage, microgrid operators can identify areas where additional capacity may be required and take proactive measures to address the issue.

Overall, the benefits of big data analytics in MGs are numerous and significant. As the adoption of MGs continues to grow, the importance of big data analytics in this context will only continue to increase. However, there are several challenges regarding big data analytics in MGs. One of the significant challenges of big data analytics in MGs is the collection and integration of data from various sources [150]. MGs use a combination of DERs such as solar panels, wind turbines, and batteries, making data collection and integration complex [146]. The data collected from these sources may be in different formats and may require preprocessing before analysis. In addition, data quality is crucial in big data analytics, as it can affect the accuracy and reliability of the analysis. In MGs, data quality can be affected by data errors, missing data, and data incompleteness. Poor data quality can lead to inaccurate predictions and inefficient energy management. Another significant challenge of big data analytics in MGs is data security and privacy [145]. MGs collect sensitive information related to energy usage patterns, which must be kept secure to prevent data breaches and unauthorized access. As MGs grow in size and complexity, the scalability of big data analytics becomes a significant challenge. Big data analytics requires a considerable amount of computing power and storage, which may be difficult to scale up as the microgrid expands [144].

On the other hand, potential solutions for these challenges can be sorted out. Standardization of data collection and integration processes can help overcome the challenge of data collection and integration. The use of standardized data formats and protocols can simplify the integration of data from various sources, making data analysis more efficient. To address the challenge of data quality, microgrid operators can implement data quality assurance techniques such as data cleansing, data validation, and data enrichment. These techniques can help ensure that data are accurate, complete, and consistent, improving the quality of data analysis. To address the challenge of data security and privacy, microgrid operators can implement data security measures such as encryption, access controls, and intrusion detection systems. These measures can help protect sensitive data and prevent unauthorized access. Cloud computing can provide a scalable and cost-effective solution to the scalability challenge of big data analytics. Cloud-based big data analytics platforms can provide on-demand computing resources, enabling microgrid operators to scale up their analytics capabilities as the microgrid expands. By addressing these challenges, microgrid operators can effectively implement big data analytics and achieve the full potential of MGs in enhancing energy sustainability and resilience.

4.5. Blockchain Technology

The integration of blockchain technology into MGs is a recent development that holds significant potential for transforming the energy sector. Blockchain technology, on the other hand, is a decentralized system that allows for secure, transparent, and tamper-proof transactions. The combination of these two technologies can enhance the efficiency, security, and transparency of MGs, enabling them to better meet the energy needs of communities. This section explores the use of blockchain technology in MGs, its benefits, challenges, and future prospects.

Blockchain technology is a decentralized, distributed ledger system that is designed to record transactions in a secure and transparent manner. The technology allows participants to maintain a shared and immutable record of transactions without the need for a central authority or intermediary [25,151,152]. In a blockchain network, transactions are verified

and recorded by a network of nodes or computers, which work together to maintain the integrity of the ledger. Each block in the chain contains a record of several transactions, along with a cryptographic hash of the previous block in the chain, which creates an unbreakable chain of blocks. This creates a tamper-proof and transparent record of transactions that is available to all participants in the network. Blockchain technology was first introduced as the underlying technology for the cryptocurrency Bitcoin. However, the technology has since been applied to a wide range of applications beyond cryptocurrency, including supply chain management, identity verification, and decentralized finance [25,151]. The potential of blockchain technology lies in its ability to provide a secure, transparent, and decentralized record of transactions that can be used across a variety of industries and applications.

The layers of a blockchain can be divided into three main layers entitled network layer, consensus layer, and application layer. The network layer is the lowest layer in the architecture and is responsible for managing the communication between nodes in the network. This layer includes protocols such as TCP/IP and HTTP, which enable the transmission of data between nodes. The network layer also includes P2P protocols, which enable nodes to connect to each other and share data in a decentralized manner. The consensus layer is responsible for validating transactions and adding them to the blockchain. This layer includes the consensus mechanism, which is a set of rules that determine how transactions are validated and added to the blockchain. There are various types of consensus mechanisms, such as proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS). The application layer is the top layer in the architecture and is responsible for providing a user interface and enabling the development of decentralized applications (dApps). This layer includes smart contracts, which are self-executing contracts that are encoded on the blockchain. Smart contracts enable the automation of various processes, such as payments, asset transfers, and identity verification. The application layer also includes various tools and libraries that developers can use to build and deploy dApps on the blockchain. Each layer of the blockchain architecture has its unique functionalities and components, but they work together to create a secure and transparent record of transactions on the blockchain. The network layer enables the transmission of data between nodes, the consensus layer ensures the integrity of the transactions, and the application layer enables the development of decentralized applications that can interact with the blockchain.

The Integration of blockchain technology into MGs can enhance their efficiency, security, and transparency [151,153–155]. One application of blockchain in MGs is P2P energy trading. P2P energy trading allows consumers to buy and sell energy directly from each other, without the need for intermediaries such as utilities or retailers. The technology can enable P2P energy trading by providing a secure and transparent platform for buyers and sellers to transact without the need for a central authority. Additionally, the use of smart contracts can automate the trading process, ensuring that transactions are executed only when certain conditions are met. Another remarkable application of this technology is the management of energy data. MGs generate vast amounts of data, including energy production, consumption, and storage. The use of blockchain technology can enable the secure and transparent sharing of energy data between different stakeholders, such as consumers, producers, and grid operators. This can improve the management of MGs, allowing for more efficient energy usage and greater system resilience.

The integration of this technology into MGs can offer several benefits [25,151,154,155]. Firstly, it can enhance the security of MGs by providing a tamper-proof and transparent platform for transactions. The decentralized nature of the technology ensures that there is no single point of failure or control, making it virtually impossible for malicious actors to manipulate or hack the system. Additionally, the use of smart contracts can automate the trading process, ensuring that transactions are executed only when certain conditions are met, further enhancing the security of the system. Secondly, the use of this technology can enhance the efficiency of MGs by enabling P2P energy trading. P2P energy trading allows consumers to buy and sell energy directly from each other, without the need for

intermediaries such as utilities or retailers. This can reduce transaction costs, increase competition, and promote the use of RESs, such as solar and wind. Additionally, the use of smart contracts can automate the trading process, ensuring that transactions are executed only when certain conditions are met, such as the availability of energy and the price of energy. Thirdly, the use of blockchain can enhance the transparency of MGs by providing a transparent and auditable platform for transactions. The decentralized nature of blockchain ensures that all transactions are recorded on a transparent and immutable ledger, providing stakeholders with a clear and auditable record of all transactions. This can improve the management of MGs, allowing for more efficient energy usage and greater system resilience.

Despite its potential benefits, the integration of blockchain into MGs also poses several challenges. One of the major challenges is scalability. MGs are often small-scale systems that generate and consume limited amounts of energy. However, as the number of participants in P2P energy trading increases, the system may become congested, leading to slow transaction times and high transaction costs. Additionally, the use of blockchain requires significant computing power and storage, which may be a challenge for small-scale MGs. Another challenge is the interoperability of different blockchain platforms. There are several platforms available, each with its unique features and capabilities. However, the lack of standardization and interoperability among different blockchain platforms can create barriers to the adoption of the technology in MGs. Therefore, the development of new standards and protocols is required to ensure compatibility among different blockchain platforms.

In spite of the explained challenges, integrating blockchain with MGs holds significant potential for transforming the energy sector. The use of this technology can enhance the efficiency, security, and transparency of MGs, enabling them to better meet the energy needs of communities. Additionally, it can promote the adoption of RESs, such as solar and wind, by enabling P2P energy trading. In the future, the adoption is expected to increase as the technology becomes more mature and the regulatory environment becomes more supportive. Additionally, the development of new standards and protocols may facilitate the interoperability of different blockchain platforms, enabling greater collaboration and innovation in the energy sector.

4.6. Artificial Intelligence (AI)

In MGs, managing and optimizing power flow is a complex task that can benefit from advanced control and optimization strategies, as illustrated in Figure 8. AI algorithms, capable of analyzing large datasets and adapting to changing conditions, are well-suited for this purpose. By leveraging big data, AI tools have demonstrated their value in optimizing power systems, improving decision making, and overall efficiency. Additionally, they contribute to increased power processing, enhanced condition monitoring, and optimized supply chain management, ultimately leading to improved accuracy and efficiency in modern energy systems.. An important issue in microgrid operation is predicting the energy generation and demand patterns accurately [156,157]. This is critical for managing the energy storage systems and ensuring reliable and cost-effective power supply. AI techniques, such as machine learning (ML) and deep learning (DL), have shown promising results in predicting energy demand and generation patterns accurately. ML algorithms can analyze historical data from the microgrid and identify patterns in energy demand and generation. These patterns can then be used to predict future energy demand and generation with a high degree of accuracy. DL algorithms, on the other hand, can analyze vast amounts of data and identify complex patterns that may not be apparent to human analysts. This allows for more accurate predictions of energy demand and generation, leading to improved microgrid operation [156,158,159].

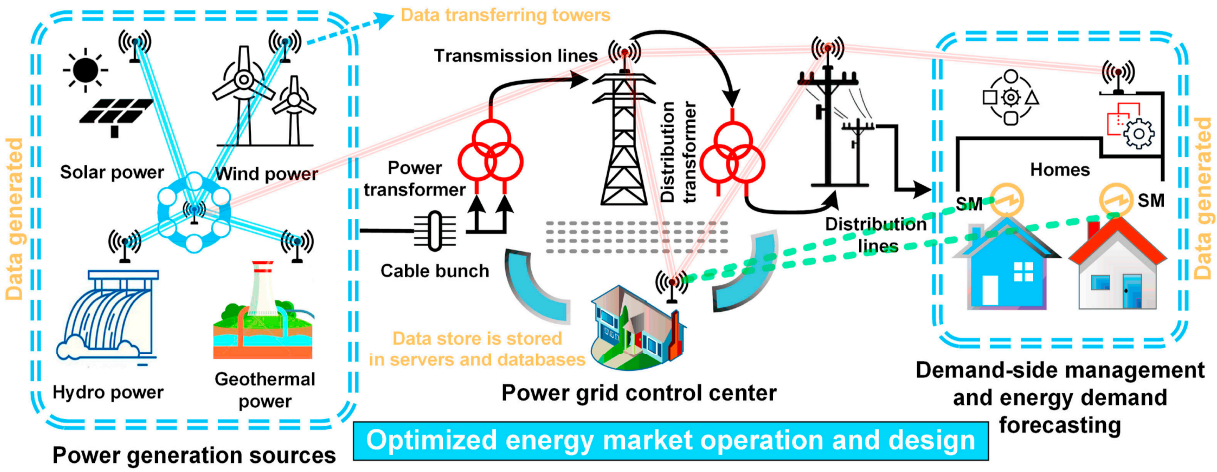

Figure 8. Interaction of AI control algorithms with power grid components [160].

Optimizing the operation of MGs is crucial for maximizing the use of RESs and minimizing energy costs. AI algorithms can optimize various aspects of microgrid operation, including energy storage, energy generation, and energy consumption [161,162]. One of the most significant challenges in microgrid operation is managing the energy storage systems. These algorithms can optimize the operation of energy storage systems by predicting energy demand and generation patterns and adjusting the energy storage systems' charging and discharging schedules accordingly. This can lead to more efficient use of energy storage systems and reduced energy costs. In addition, the algorithms can enhance the energy generation side by forecasting renewable energy generation components and setting the power output of energy sources properly. This can maximize the use of RESs and reduce reliance on traditional energy sources, leading to reduced energy costs and increased energy independence. Furthermore, they can manage energy consumption in a similar manner. This can reduce energy costs and ensure that energy consumption is aligned with renewable energy generation.

One of the AI applications in MGs is control, where they can handle various aspects of microgrid operation [159]. A significant challenge in microgrid control is managing the power flows among the various energy sources. AI algorithms can optimize power flows by foreseeing energy demand and generation plans and adjusting the power output of energy sources and storage systems accordingly. This can ensure a reliable and cost-effective power supply while minimizing the reliance on traditional energy sources. These approaches can also control the operation of energy storage systems by adjusting the charging and discharging schedules to ensure that the energy storage systems are operating efficiently. This can extend the lifespan of energy storage systems and reduce energy costs [162]. In addition, the algorithms can control energy consumption by adjusting energy consumption schedules based on energy demand and generation plans. This can ensure that energy consumption is aligned with renewable energy generation and reduces energy costs. Another critical application of AI in MGs is fault detection and diagnosis. MGs are vulnerable to faults, such as equipment failures or disturbances in the power supply. AI algorithms can monitor the system and detect these faults early, allowing for prompt diagnosis and repair. This can minimize the downtime of the microgrid and prevent damage to equipment [156]. In addition to these benefits, the use of AI in MGs can also help to reduce greenhouse gas emissions and promote sustainability. By optimizing the use of RESs and reducing the reliance on non-RESs, MGs can help to mitigate the effects of climate change.

Despite the potential benefits of AI in MGs, there are also some challenges and limitations. One of the main challenges is the availability and quality of data. These algorithms require large amounts of data to make accurate predictions and decisions. In MGs, data may be limited, and the quality of the data may be poor, which can directly affect the

accuracy of the algorithms. Another challenge is the complexity of microgrid systems. They can be composed of various energy sources, storage systems, and loads, which can make it difficult to develop and implement AI algorithms that can optimize the overall system performance. Furthermore, the implementation of algorithms requires specialized expertise, which may not be readily available. Moreover, the use of AI in MGs raises concerns about cybersecurity. As MGs become more reliant on digital technologies, they become more vulnerable to cyberattacks. AI algorithms may also be vulnerable to attacks, which could compromise the reliability and safety of the microgrid. Therefore, it is crucial to ensure that adequate cybersecurity measures are in place to protect the microgrid from cyberthreats. Another limitation of them is the potential for bias. AI algorithms are only as unbiased as the data they are trained on. If the data used to train the algorithm are biased, the algorithm will produce biased results. This could result in unfair or discriminatory decision making, which could be problematic, particularly in areas such as energy access and affordability. Nonetheless, with careful consideration of the challenges and limitations, AI can be a valuable tool for improving the efficiency, reliability, and sustainability of MGs.

4.7. Digital Twin Technology

Digital twin technology is a powerful tool that has recently gained popularity in the energy industry, particularly in MGs. A digital twin is a virtual replica of a physical asset, process, or system, which can be used to model and optimize its performance in real time [163–165]. In the context of MGs, digital twin technology can provide insights into the grid's behavior, enable predictive maintenance, and optimize energy management strategies.

Digital twin technology is a software-based technology that enables the creation of a virtual replica of a physical asset or system. The technology uses data collected from sensors, machines, and other sources to create a digital model that can be used to simulate the behavior of the physical asset or system. Digital twins can be used in various industries, including manufacturing, aerospace, and healthcare, to optimize performance and reduce maintenance costs [166–168]. In the energy industry, digital twin technology is particularly useful in MGs, which are small-scale electricity grids that can operate independently or in conjunction with the main power grid. Digital twins can be used to model the behavior of MGs, enabling operators to optimize energy management strategies, predict and prevent system failures, and reduce downtime. They can provide various important services in MGs, some of which are system design and optimization, control and monitoring, predictive maintenance, resiliency and reliability, energy management, and demand response. A general overview of the important digital twinning services in MGs is provided in Figure 9 [6].

One of the most significant benefits of digital twin technology in MGs is the ability to optimize energy management strategies [169–171]. By creating a digital twin of the microgrid, operators can simulate different scenarios and test various energy management strategies to determine the most efficient and cost-effective approach. For example, they can use the digital twin to test the impact of different energy storage systems [172,173] or RESs [104,174] on the microgrid's overall performance.

Another benefit of digital twin technology is predictive maintenance [175–178]. By analyzing data from sensors and other sources, operators can identify potential system failures before they occur, enabling them to take corrective action before any damage occurs. This can help to reduce maintenance costs and downtime, ensuring the microgrid operates at peak efficiency.

Digital twin technology can also improve the overall reliability of MGs [179–181]. By simulating different scenarios, operators can identify potential system weaknesses and vulnerabilities, enabling them to implement corrective measures to improve the system's overall resilience. This can help to ensure that the microgrid remains operational during power outages or other disruptions.

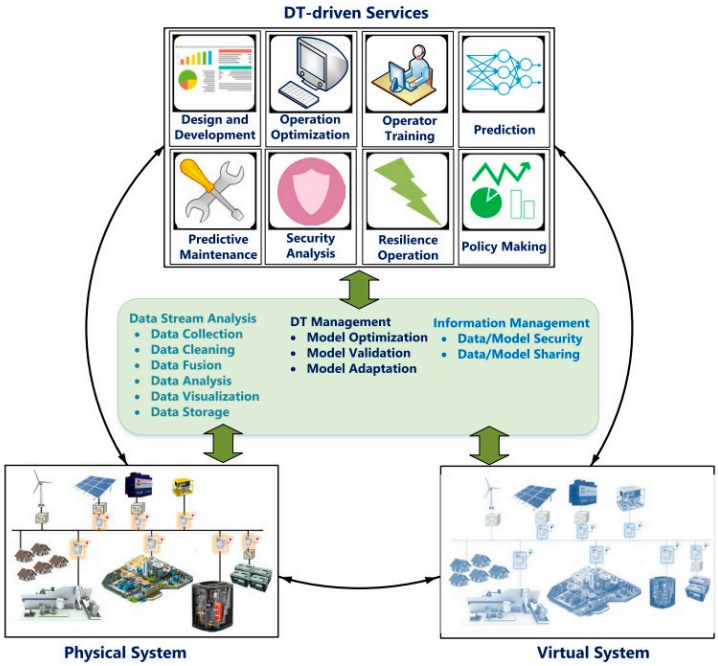

Figure 9. A general overview of the important digital twinning services in MGs [6].

In conclusion, digital twin technology is a powerful tool that can provide significant benefits to microgrid operators. By creating a virtual replica of the microgrid, operators can optimize energy management strategies, predict and prevent system failures, and improve overall reliability. As the energy industry continues to evolve, it is likely that digital twin technology will become an increasingly important tool for microgrid operators, enabling them to stay ahead of the curve and ensure that their systems operate at peak efficiency. Table 8 presents some key concepts for the use of digital twin technology in MGs.

Table 8. Key concepts for the use of digital twin technology in MGs.

Key Concept	Explanation
Optimization of energy management strategies	Digital twins enable simulation of scenarios and testing of energy management strategies in MGs to optimize energy usage, reduce costs, and increase efficiency.
Predictive maintenance	Digital twins can prevent system failures and reduce maintenance costs and downtime by enabling operators to identify potential issues through analysis of data from sensors and other sources.
Improved reliability	Digital twins can improve the overall resilience of MGs by identifying potential weaknesses and enabling operators to implement corrective measures to ensure operational continuity during power outages or other disruptions.
Real-time monitoring	Digital twins can provide real-time monitoring of microgrid performance, allowing operators to detect issues promptly and prevent system failures to ensure peak efficiency.
Cost savings	Optimizing energy management strategies and implementing predictive maintenance measures can lower maintenance and downtime costs for microgrid operators.
Increased efficiency	Digital twins can help to optimize energy usage, reduce waste, and increase efficiency, resulting in lower costs and improved performance.
Better planning	Digital twins enable simulation of scenarios and testing of energy management strategies to prepare for future developments and ensure operational continuity in changing conditions.

4.8. Cloud Computing

The digitalization of MGs has become an increasingly important trend in the modern energy industry. Cloud computing (CC), a technology that allows users to access a shared pool of computing resources over the internet, has emerged as a key enabler of this trend. This section provides an overview of CC, its components, applications, and its impact on the digitalization of MGs.

CC is a technology that allows users to access computing resources such as processing power, storage, and software over the internet, without having to invest in and manage their own information technology (IT) infrastructure. The CC is based on a model where resources are provided as a service, and users pay only for what they use, similar to a utility model. CC consists of several components that are used to enable the delivery of on-demand computing resources, such as storage, processing power, and applications, over the internet. In the context of MGs, these components can include [182,183]:

Infrastructure as a Service (IaaS): IaaS provides the computing infrastructure needed to support microgrid operations, such as servers, storage, and networking equipment. This infrastructure is typically provided by cloud service providers, who offer scalable and flexible resources that can be adjusted to meet the needs of microgrid operators.

Platform as a Service (PaaS): PaaS provides the platform needed to build and deploy applications that can be used to manage and optimize microgrid operations. This can include tools for data analytics, machine learning, and automation, which can be used to optimize the performance of microgrid components and to predict future energy needs.

Software as a Service (SaaS): SaaS provides software applications that can be used to manage and monitor microgrid operations, such as energy management systems, demand response platforms, and energy trading platforms. These applications are typically provided by cloud service providers, who offer them on a subscription basis, and can be accessed through a web browser or mobile app.

Cloud Storage: Cloud storage provides the storage resources needed to store and manage the large amounts of data generated by microgrid operations. These data can include energy usage data, weather data, and other operational data, which can be used to optimize microgrid performance and to make accurate predictions about future energy needs.

Cloud Security: Cloud security provides the security measures needed to protect the data and infrastructure used to support microgrid operations. This can include measures such as access control, encryption, and monitoring, which can be used to prevent unauthorized access and ensure the integrity of microgrid operations.

The CC can provide several applications that can be used to manage and optimize microgrid operations. These applications can include energy management systems, demand response platforms, energy trading platforms, and predictive analytics [23,184–186]. Energy management systems can be used to optimize the operation of microgrid components, such as energy storage and RESs, to meet energy demand and minimize energy costs. Demand response platforms can be used to reduce energy consumption during periods of high energy demand, by incentivizing consumers to reduce their energy usage [184,185]. Energy trading platforms can be used to facilitate the buying and selling of energy between microgrid operators, energy providers, and consumers [23]. Predictive analytics can be used to make accurate predictions about future energy demand and supply, which can help to optimize microgrid operations and improve energy efficiency [186]. The impact of the CC on MGs has been significant. It can increase the efficiency of MGs by providing the computing resources needed to optimize energy production, storage, and consumption, as illustrated in Figure 10 [23,182,186]. This can result in lower energy costs, improved reliability, and reduced greenhouse gas emissions.

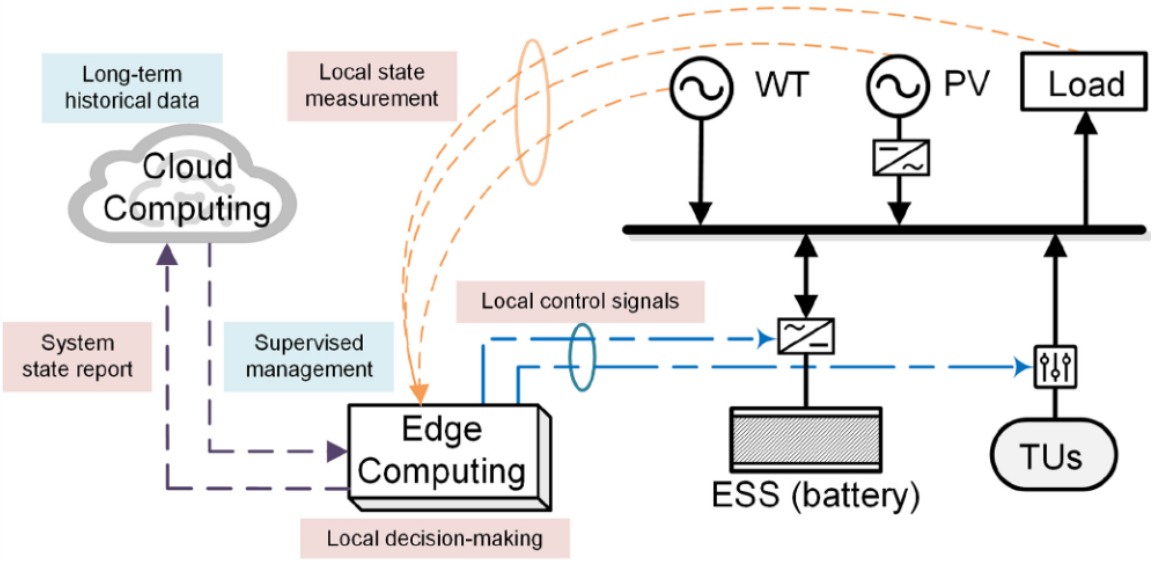

Figure 10. The illustration of the use of CC and its computational resources [186].

The CC can also improve the resiliency of MGs by providing backup power and redundancy, and by enabling remote monitoring and control of microgrid components. This can help to minimize the impact of power outages and other disruptions, and can ensure that critical infrastructure and services remain operational during emergencies. It can enhance the flexibility of MGs by enabling real-time monitoring of energy usage and automatic adjustment of energy production and consumption based on changing conditions. This can help to reduce energy waste and to optimize the use of RESs such as solar and wind power.

The CC can also enable more advanced data analytics in MGs, by providing the computing resources needed to analyze large amounts of data in real time [186]. This can help to identify patterns and trends in energy usage, and to make more accurate predictions about future energy needs. This method can also enable greater collaboration between microgrid operators, energy providers, and other stakeholders. Cloud-based platforms can provide a secure and transparent marketplace for energy trading, and can enable peer-to-peer energy trading between consumers. This can help to promote sustainability, and to build more resilient and efficient energy systems.

Overall, the integration of the CC in MGs has the potential to revolutionize the way we generate, store, and consume energy. By providing the computing resources needed to optimize energy production, storage, and consumption, the CC can help to reduce energy costs, improve reliability, and promote sustainability. As the demand for RESs continues to increase, and as the need for more resilient and efficient energy systems becomes more pressing, the CC is likely to play an increasingly important role in the management and optimization of microgrid operations. However, to fully realize the potential of the CC in MGs, it will be important to address the challenges associated with its use and to ensure that the computing infrastructure is reliable, resilient, and secure.

4.9. Augmented Reality

Augmented reality (AR) is a rapidly growing technology that has found numerous applications in different fields. One area where AR can have a significant impact is in MGs. As defined before, a microgrid is a small-scale power grid that can operate independently or in conjunction with a larger power grid. The integration of AR technology into MGs can provide a range of benefits, such as improved efficiency, reliability, and safety [187,188]. This section provides an overview of AR technology and its potential applications in MGs.

AR technology is a computer-generated overlay that enhances the real-world environment with additional information. This technology works by overlaying digital information

on top of real-world objects or environments. AR can be used in different ways, such as displaying text, images, or videos in a real-world environment. AR technology can be used on various devices, including smartphones, tablets, smart glasses, and head-mounted displays. The technology works by using a camera to capture the real-world environment and display the digital overlay on the device's screen [189]. AR technology can provide several benefits in MGs. The following are some of the potential applications of AR in MGs [190–194]:

Remote Monitoring and Maintenance: AR technology can be used to remotely monitor and maintain microgrid equipment. With AR, maintenance technicians can view a digital overlay of the equipment's components and identify issues without having to be physically present. This can save time and money while also reducing the risk of accidents.

Training and Education: AR technology can be used to provide training and education to microgrid operators and technicians. By overlaying digital information on top of the real-world environment, AR can provide a more immersive and interactive learning experience. AR can also be used to simulate different scenarios, allowing operators and technicians to practice and develop their skills in a safe and controlled environment. An example picture for virtual training is shown in Figure 11. While Figure 11a shows the virtual training environment, Figure 11b depicts the real-life counterpart of the same environment. In that instance, the operator must deal with an energized transformer while in a small place. The workforce can receive interactive training with real-time feedback, imitating difficulties and random cases, without endangering their safety, by mimicking this dangerous task.

(**a**) (**b**)

Figure 11. Virtual training example of a microgrid operator: (**a**) virtual environment; (**b**) real environment [195].

Fault Detection and Diagnosis: AR technology can be used to detect and diagnose faults in microgrid systems. By overlaying digital information on top of the real-world environment, AR can help operators and technicians identify the root cause of a fault quickly. This can lead to faster repairs and reduced downtime.

Optimization of Microgrid Operations: AR technology can be used to optimize microgrid operations. By overlaying digital information on top of the real-world environment, AR can provide real-time information about the microgrid's performance. This information can be used to optimize the microgrid's operation, leading to improved efficiency and reduced costs.

While AR technology has several potential applications in MGs, there are also several challenges and limitations to its use [187,188,191]. The challenges and limitations of AR in MGs can be summarized as follows. AR technology can be expensive, and implementing it in a microgrid system may not be cost-effective for smaller systems. The cost of AR hardware and software can be a significant barrier to adoption. In addition, it can be complex and require specialized knowledge to operate effectively. Operators and technicians may require training to use AR effectively, and the technology may not be accessible to all users.

AR technology relies on data and connectivity to operate effectively. As such, there may be concerns about data security and privacy when using AR technology in a microgrid system. Moreover, AR technology relies on hardware, and the limitations of that hardware can impact its effectiveness. For example, low-quality cameras may not capture the real-world environment effectively, resulting in inaccurate overlays.

As AR technology continues to develop, there are several directions in which it could be applied in MGs. Some potential future direction examples for AR in MGs can be given. For instance, integrating AR technology with AI could enhance its capabilities significantly [192]. By using AI algorithms to analyze data from the microgrid, AR could provide real-time insights and recommendations for optimizing the microgrid's performance. In addition, wearable AR devices, such as smart glasses or head-mounted displays, could enhance the use of AR technology in MGs. These devices provide a more hands-free and immersive experience, allowing operators and technicians to interact with the digital overlay more effectively [190,193,194]. Another expected example is that the AR technology could be used to facilitate energy trading in MGs. By overlaying real-time information about energy supply and demand, AR could help microgrid operators make more informed decisions about energy trading, leading to improved efficiency and cost savings. Moreover, AR technology could also be used to engage consumers in microgrid systems. By overlaying digital information on top of real-world energy usage, consumers could gain a better understanding of their energy usage and how it impacts the microgrid system as a whole.

While there are challenges and limitations to its use, ongoing developments in AR technology could help overcome these barriers. As AR technology continues to evolve, its applications in MGs could expand, providing a range of benefits for operators, technicians, and consumers alike.

5. Cybersecurity in MGs

As MGs continue to grow in popularity as a means of providing reliable and sustainable energy to communities and businesses, the issue of cybersecurity becomes increasingly important. With the use of digital technology and communication systems, MGs are vulnerable to cyberattacks that can compromise their operation and even cause physical damage. As a result, it is essential to consider cybersecurity as a critical aspect of microgrid design, implementation, and operation. Therefore, this part of the paper explores the potential cybersecurity risks associated with MGs and discusses the strategies and technologies that can be used to mitigate these risks.

5.1. Security Vulnerabilities in MGs

Cybersecurity vulnerabilities in MGs are similar to those found in large-scale energy grids. However, due to the unique characteristics of MGs, they require different attention. MGs are mainly based on RESs. Therefore, the devices used for energy generation, storage, and distribution are manufactured by different vendors and are not compatible with each other [196,197]. This can lead to cybersecurity vulnerabilities in MGs as cyberattackers may exploit the weaknesses of these devices.

The vulnerabilities of MGs are generally caused by factors such as inadequate security measures, lack of software and hardware updates, weak authentication, incorrect configuration, faulty software coding, and improperly separated networks [198]. Cybersecurity vulnerabilities allow a cyberattacker to take control of devices, gain unauthorized access to systems, install malware, and monitor network traffic. This can cause interruptions in the energy production and distribution processes of MGs and create security risks for individuals [199]. Table 9 provides a brief description of the categories and explanations of significant vulnerabilities encountered in MGs.

Table 9. Some significant vulnerabilities encountered in MGs.

Vulnerability Type	Description	Potential Consequences
Attacks on field devices	Field devices are vulnerable due to limited memory and processing resources, which can be exploited by attackers.	Attackers can overwrite memory sections of field devices with incorrect values, leading to device crashes or malfunctions.
Backdoor or malware loaded onto command-and-control network	Malware/backdoors can be installed on the command-and-control network, providing attackers with covert access to devices or assets on the system.	Attackers can gain unauthorized access to the network and compromise the security of devices or assets.
Attacks on databases	Database attacks can impact system security and data collection from the field.	Attackers can update device values through the database, which may not be reflected in the human–machine interface (HMI), or affect the collection of data from the field.
Devices with few or no security features	Microgrid devices may lack basic security mechanisms, such as authentication or encryption.	Attackers can send control messages that disable grid devices, which are executed as there is no way to verify their validity.
Misconfigurations of assets	Default configurations, misconfigured assets, and using default passwords can undermine system security.	Assets that are not enabled to authenticate, or use default or hardcoded credentials, can compromise security.
Unsatisfactory cybersecurity procedures and training for personnel	Uneducated personnel can compromise network security by disregarding security policies and practices.	Personnel can unintentionally or intentionally disable security features or install new software that impacts the security profile of the information system.
Incorrect configured network	Networks that are not completely separated from the corporate network can become vulnerable to attackers.	An attacker can exploit a security vulnerability in the microgrid information system by sending a phishing email with a malicious attachment.
Incorrect or nonexistent patches	Incorrect or nonexistent patches can leave software and hardware vulnerable to attacks, compromising microgrid system security and reliability.	The patching process can create a risk for the system's accessibility, affecting the security and reliability of the microgrid system.
Unsafe coding techniques	Inappropriate authentication, access control, and error checking can negatively impact system security.	An attacker can bypass authentication mechanisms that use device serial numbers or 16-bit authentication keys.
Failure to use microgrid-specific security technologies	The absence of a security technology aimed at detecting security vulnerabilities in MGs makes these systems vulnerable to attackers.	The system becomes vulnerable to attackers due to the absence of a security technology aimed at detecting security vulnerabilities in MGs.
Security vulnerabilities in microgrid-specific protocols	The communication protocols used in MGs are designed with little emphasis on security, making them more vulnerable to attacks.	Microgrid-specific protocols are more vulnerable to well-known attacks due to their lack of emphasis on security.
Unauthorized personnel access	Failure to monitor or restrict physical access to the microgrid network may result in unrestricted access to all assets in the network.	Failure to monitor or restrict physical access to the microgrid network.

5.2. Threats to Microgrid Cybersecurity

MGs and smart grids, as complex cyberphysical systems, are vulnerable to various types of cyberattacks that can cause severe disruptions to energy generation, distribution, and consumption. To better understand these risks, it is essential to develop a systematic

taxonomy of cyberattacks on smart grids based on their themes and characteristics [200,201]. Such a taxonomy can provide a useful framework for classifying and analyzing different types of cyberattacks, identifying common patterns and vulnerabilities, and designing effective countermeasures. A remarkable and up-to-date thematic taxonomy of cyberattacks to smart grids, which can also be considered for MGs, is presented by Ding et al., as illustrated in Figure 12 [202].

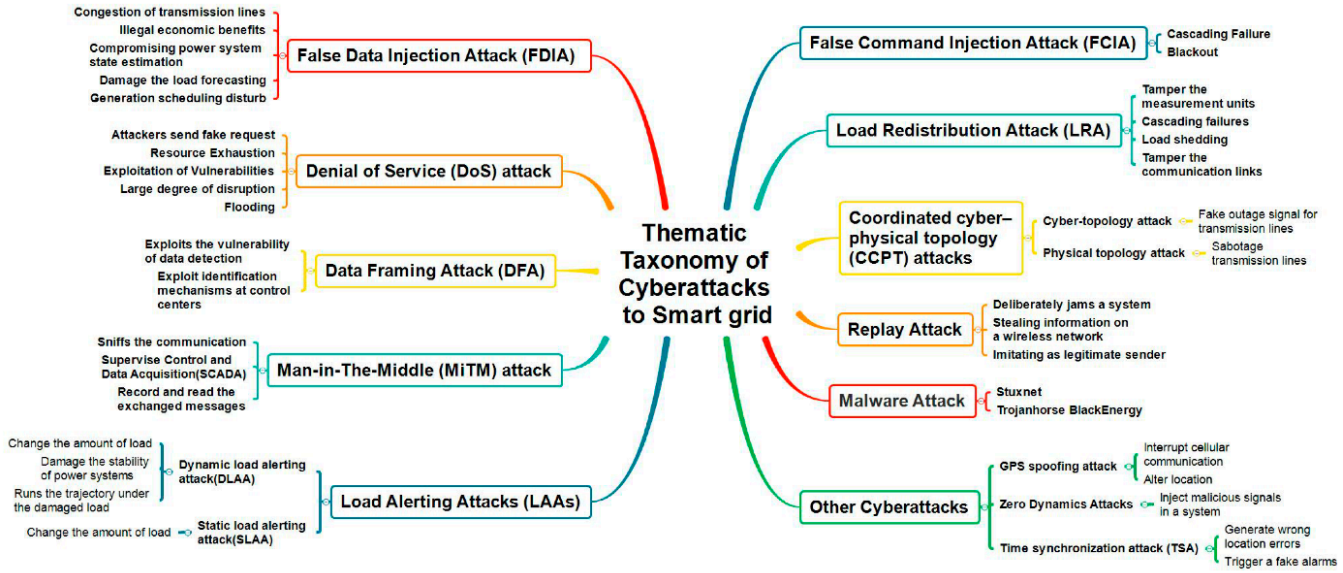

Figure 12. A thematic taxonomy of cyberattacks to smart grids [202].

As illustrated in Figure 12, cyberattacks on smart and microgrids has mainly focused on various attack methods such as false data injection attacks, denial of service attacks, data framing attacks, man-in-the-middle attacks, load altering attacks, false command injection attacks, load redistribution attacks, coordinated cyberphysical topology attacks, and replay attacks. These attacks exploit different vulnerabilities in power grids and have varying intentions and strategies. Moreover, the integration of information systems into power physical systems has resulted in severe threats such as malware attacks [202]. It is crucial to analyze and understand these cyberattacks on MGs to develop effective countermeasures against potential threats. Therefore, some of the most significant of attacks are outlined below:

False Data Injection Attack: False data injection (FDI) can have serious consequences by affecting the operation of MGs. FDI attacks cause incorrect processing or decision making in the system by providing misleading or erroneous data to the network users [203,204]. This can lead to faulty load distribution, device failures, or system crashes. Typically, an attacker injects false data into network devices starting from a point where the attacker can access the network system. By using fake data, the attacker can deceive the network devices and cause them to perform incorrect operations. For example, an attacker can change traffic density data by sending false signals to a traffic sensor and create traffic flow in the wrong direction [205]. False data injection attacks have been increasingly observed in recent years. To protect against these attacks, security vulnerabilities of microgrid systems need to be identified, and security measures need to be taken [206,207]. Additionally, designing network devices for authentication and accuracy checks can reduce the impact of attacks.

Denial of Service (DoS): The cybersecurity infrastructure in MGs should be designed to ensure access to energy, related information, and communication structures. In this context, a DoS attack targets power availability by reliably and timely affecting access to microgrid services [93,208]. Despite its simplicity, an effective DoS attack can cause significant disruption. A DoS attack can be carried out by overloading the device or chan-

nel with data, manipulating vulnerabilities or abnormalities in protocols and systems, or both. DoS attacks can also be generated by a large number of compromised information assets that have been turned into zombies, known as distributed denial of service (DDoS) attacks [209,210]. Therefore, a DoS attack on a microgrid can be carried out against the accessibility of traditional power usage, preventing control over communication, computation, and information systems, endangering data integrity, and causing power outages. If the microgrid is connected to the internet, DoS attacks can cause significant power outages and have extremely harmful consequences. MGs contain a variety of measurement devices, such as smart meters, smart devices, data collectors, phase measurement units, remote terminal units, smart electronic devices, and programmable logic controllers (PLCs). These devices are sensitive to DoS attacks due to their use of internet standard protocols [211]. For instance, PLCs, integral components of automation systems within microgrids, are responsible for controlling and monitoring various processes. However, their connection to the internet and utilization of standard protocols can introduce vulnerabilities. DoS attacks, for example, can disrupt the operation of PLCs by overwhelming them with a high volume of malicious requests, rendering them unresponsive or causing system malfunctions. It is crucial for microgrid operators and cybersecurity professionals to be aware of these vulnerabilities and implement robust security measures to mitigate potential risks. This may include implementing intrusion detection systems, access controls, secure network architectures, regular patching and updates, and ongoing monitoring and incident response protocols. By addressing these vulnerabilities, microgrids can enhance their resilience against cyberthreats and ensure the secure operation of their automation systems.

Data Framing Attacks: These are a type of cyberattack that targets communication networks. In this type of attack, the attackers attempt to deceive the devices in the network by sending fake messages that mimic the network traffic [212,213]. These fake messages are used to distort or alter the data as they are transmitted between the devices in the network. Attackers may also send fake messages to cut off a data stream or to cause damage to a specific device. This type of attack is especially dangerous for many industrial protocols because these protocols are typically designed without security measures and use plain text for communication between devices in the network. Attackers can exploit the weak points in the communication algorithms of network devices by manipulating data through techniques such as modifying the values stored in the devices' memory, sending fake messages, or using other methods to disrupt or disable devices [214]. This type of attack can cause devices in the network to malfunction or even suffer physical damage [215].

Man-in-the Middle Attacks: One of the most significant threats faced by MGs is the man-in-the-middle (MitM) attack. The MitM attack is a type of cyberattack where the attacker intercepts communication between two parties to steal or alter data [216,217]. In the context of MGs, MitM attacks can cause significant disruptions to the energy supply chain, leading to power outages, equipment damage, and even safety hazards. The MitM attack in MGs typically involves an attacker gaining access to the communication network used to control and manage the grid's various components. The attacker may use various methods to gain access, such as social engineering, phishing attacks, or exploiting vulnerabilities in the network infrastructure. Once the attacker gains access, they can intercept communication between the various components of the microgrid and manipulate data to their advantage [218,219]. For instance, the attacker can intercept communication between the microgrid's control system and the energy storage system and modify the power flow to create an overload, which can damage the equipment or cause a power outage. Similarly, the attacker can manipulate the data from the RESs to make them appear unreliable, which can cause the microgrid to switch to a more expensive and less sustainable energy source. MitM attacks in MGs can also pose a significant threat to the privacy and confidentiality of the energy data [220]. For example, the attacker can intercept communication between the smart meters and the microgrid's control system to gain access to the energy usage data of individual consumers. These data can be used for various purposes, such as identity theft or targeted advertising, leading to significant financial losses and privacy violations.

Concludingly, the three main objectives of MiTM attacks are (1) to interrupt or modify measurements; (2) to alter smart meter data; and (3) to manipulate network traffic by the attacker. This attack technique relies on the Address Resolution Protocol (ARP) poisoning approach, and attack detection can be performed using packet evaluation techniques [221].

Load Manipulation Attacks: These attacks aim to modify power usage of targeted loads or even to overload them. For instance, the method of load manipulation can be employed indirectly by publishing incorrect price information to customers in terms of demand response management techniques. Power loads must be protected to prevent overloading and to manage them cost-effectively [222].

Malicious Command Injection Attack: In power grids, phase shifting transformers or phase shifters are used to control the flow of electricity. Phase shifters are used to prevent the accumulation of electrical density in transmission lines and to apply contract-based regulations. In an automatic power grid system, phase shifting commands are transmitted through the SCADA system. This situation can make the system vulnerable to cyberattacks in terms of both harmless and malicious commands being sent from the phase shifters. Malicious commands can cause serious damage, power outages, and disrupt cross-network interactions [223].

Load Redistribution Attacks: These attacks are related to the distribution or routing of energy sources on a microgrid. This type of attack is carried out when a device with low security levels changes the flow of energy on the grid by sending fake data packets or using a predetermined strategy [224,225]. Attackers can artificially increase energy consumption in a specific area of the grid, causing energy sources in that area to rapidly deplete. This can create a balancing issue across the entire grid, requiring other areas to be fed from different energy sources [226]. Load redistribution attacks also allow individuals with access to energy sources to manipulate energy consumption by redirecting energy sources from one area to another. This can cause power outages in specific areas of the grid and harm electricity consumers in the affected region. The best way to counter these types of attacks is to implement appropriate mechanisms for controlling the distribution and routing of energy sources on the grid and monitoring them securely. Additionally, it is important to take appropriate security measures on each device to ensure the security of each component of the grid [102].

Coordinated Cyberphysical Topology Attacks: Coordinated cyberphysical topology attacks (CCPT) are more dangerous for MGs than either physical topology attacks or cybertopology attacks alone [227,228]. CCPT attacks are divided into two categories: physical topology attacks and cybertopology attacks. In a physical topology attack, the attacker cuts the transmission line, while in a cybertopology attack, the attacker deceives the control center, hides the outage signal in the cyberlayer, and creates a false outage signal for another transmission line [229]. As a result, the most important goal of a coordinated topology attack is to overload the critical line by deceiving the control center into making incorrect dispatches [230].

Replay Attack: A replay attack can be carried out by intercepting information in a communication network and then mimicking a legitimate sender by distributing the intercepted information to reproduce the original information [231,232]. This type of attack relies on past data and makes it difficult for the control center to detect the attack. As a result, the attack can cause disruption in the power flow and lead to time delays at different frequencies. From the attacker's point of view, a replay attack can intentionally disrupt the system and various processes completely [233].

Malware Attacks: Malware is software designed to harm or disrupt computer systems, and it can be introduced into a microgrid's system through email attachments, software updates, or infected USB drives. Once installed, malware can spread throughout the system, causing significant damage [234,235]. Some types of malwares, such as ransomware, can encrypt the microgrid's data and demand payment for their release, causing significant financial losses. Cyberattacks on microgrid systems can be carried out through the use of malicious software such as BlackEnergy, Stuxnet Trojan horses, or WannaCry ransomware.

In December 2015, a cyberattack targeted the electricity grid in Ivano-Frankivsk, Ukraine, resulting in a power outage and directly affecting 80,000 people. It was determined that this cyberattack was created using phishing emails and the BlackEnergy Trojan horse [236]. This attack method was observed to have the ability to delete certain types of data, damage hard disks, and control systems.

Insider Attacks: This could involve a rogue employee, contractor, or supplier who has access to the microgrid's systems and deliberately causes harm [27]. Such an attack could be motivated by financial gain, personal animosity, or ideological beliefs. Insider attacks can be challenging to detect, as the attacker may already have authorized access to the system.

Phishing Attacks: Phishing is another major threat to microgrid cybersecurity. Phishing is a type of social engineering attack that uses deceptive emails or other means to trick users into divulging sensitive information, such as passwords or other login credentials. Once attackers have this information, they can use it to gain unauthorized access to the microgrid system. To protect against phishing, microgrid operators should train employees to recognize and avoid phishing scams, and should implement multifactor authentication to prevent unauthorized access to critical systems [27].

Ransomware Attacks: Ransomware is a type of malware that prevents users from accessing their own data or computer systems until a ransom is paid to the attacker [237]. In recent years, ransomware has become a significant threat to the security of MGs. MGs are small-scale power grids that can operate independently or in conjunction with the main power grid. They typically use DERs such as solar panels and battery storage to generate and manage power. Ransomware attacks on MGs can cause significant disruptions to power supply and create safety hazards [238,239], and they can take various forms, including locking access to control systems or preventing the delivery of electricity to customers. Attackers may also demand payment in cryptocurrency, making it difficult to track the flow of funds and apprehend the perpetrators. The consequences of a successful ransomware attack can be severe, with potential risks to human life and property. For example, an attacker could disrupt the supply of power to critical infrastructure, such as hospitals or emergency services, causing life-threatening situations. In addition, an attack on a microgrid could lead to a wider power outage affecting a larger population.

Advanced Persistent Threats: Advanced persistent threats (APTs) are a significant concern in the context of MGs as these critical infrastructures are vulnerable to cyberattacks due to their interconnected nature and the increased use of digital technologies in microgrid management systems [112]. APTs are sophisticated and stealthy cyberattacks that are often orchestrated by state-sponsored actors, organized criminal groups, or hacker collectives [240]. Unlike traditional cyberattacks that are aimed at exploiting vulnerabilities in software or hardware systems, APTs are designed to remain undetected for extended periods to collect sensitive data, steal intellectual property, or disrupt critical infrastructure. In the context of MGs, APTs can be devastating as they can compromise the integrity of the system, disrupt operations, and cause physical damage to the infrastructure [241,242]. For example, an APT targeting the control system of a microgrid can lead to unauthorized access, data theft, and even physical damage to the equipment. Moreover, an APT can also be used to launch a ransomware attack, where the attacker encrypts the critical data and demands a ransom payment in exchange for the decryption key.

SQL Injection Attacks: These attacks can pose a significant threat to the cybersecurity of the system. MGs often use web applications and interfaces to monitor and control the system, and these interfaces are potential targets for SQL injection attacks. An SQL injection attack works by inserting malicious code into a web application's input field, which is then executed by the database server [243,244]. This code can be used to bypass authentication, retrieve sensitive data, or modify the contents of the database. In the context of MGs, a successful SQL injection attack could allow an attacker to gain control of the system, modify power flow, or even shut down the microgrid entirely [245].

Zero-day Attacks: Zero-day exploits, also known as zero-day vulnerabilities, refer to previously unknown software vulnerabilities that hackers can exploit to launch attacks. These types of attacks are particularly concerning for MGs, as they can target critical infrastructure and cause significant damage to the system [246,247]. Zero-day exploits are a type of cyberthreat that is difficult to defend against, as the system administrators may be unaware of the vulnerability and unable to apply a patch or update to fix it. They are a growing concern in the energy sector, and MGs are not immune to these types of attacks. In fact, as MGs become more prevalent, the likelihood of being targeted by zero-day exploits increases. This is because MGs often rely on outdated software and hardware, which can contain vulnerabilities that are not yet known to system administrators. Hackers can exploit these vulnerabilities to gain access to the microgrid system and launch attacks that can disrupt operations, cause damage to equipment, and potentially harm people [247,248].

Physical Attacks: Physical attacks on MGs are also a significant threat to cybersecurity. These attacks could include vandalism, theft, or sabotage of the microgrid's hardware or infrastructure [249,250]. Physical attacks can be challenging to prevent, as they often require significant security measures and resources.

5.3. Strategies for Cybersecurity in MGs

MGs are small energy networks that usually provide electricity to a few consumers. These grids are important in terms of the use of RESs and energy efficiency. However, MGs are vulnerable to cyberattacks and can be manipulated by malicious actors who have access to the grid if cybersecurity measures are not taken.

Some of the crucial strategies that should be applied to ensure the security of MGs are listed below [251,252]:

Encryption of communication channels: In MGs, communication between different devices is often carried out wirelessly. Therefore, encryption of communication channels is very important. Encrypting data traffic between wireless communication devices significantly reduces the risks of unauthorized access and data theft.

Access control: In MGs, communication between devices and systems often has an open structure, which can facilitate cyberattackers' access to the system. Therefore, access control is important. Access control includes techniques such as authentication, authorization, and access control, and provides system access only to authenticated users and devices.

Device updates and patches: Devices in MGs, in addition to current software and hardware patches, should also be updated periodically to minimize cybersecurity vulnerabilities. Simultaneously performing these updates on all devices and systems helps make the system more secure.

Threat detection and response: Malware and other cyberthreats can spread quickly in MGs and cause serious damage. Therefore, an automatic threat detection and response system capable of detecting and monitoring threats and taking necessary measures should be established in MGs.

Network security: MGs can be protected with network security measures. Network security includes technologies such as firewalls, network monitoring systems, network access control, and similar measures, which help prevent malicious actors from accessing and damaging the network.

Identification and protection of weak points: Weak points in MGs can be a target for attackers. Therefore, identifying and protecting weak points is important in preventing attacks. This can include regular updates and patch installations, identifying and closing security vulnerabilities, encryption, and similar measures.

Personnel training: Personnel working in MGs should be trained on cybersecurity issues. This ensures that personnel are informed about secure practices and are knowledgeable about detecting and preventing cyberattacks.

Password management: Using strong and unique passwords is important in protecting MGs from cyberattacks. Passwords should be changed regularly and stored securely.

Emergency planning: MGs' emergency plans should include contingency plans for a cyberattack or natural disaster. These plans should be regularly updated and tested to ensure their effectiveness in a crisis.
Physical security: Physical security is of great importance in MGs. Physical security involves the physical protection of devices, systems, and other hardware. Therefore, it is important to properly place devices, use mechanisms that ensure physical access control, and employ mechanisms that ensure the security of devices.

5.4. Vulnerability Assessment and Risk Analysis

Vulnerability assessment and risk analysis are two related but distinct processes that are often used in the field of cybersecurity to identify potential threats and vulnerabilities in computer systems, networks, and other digital assets.

Vulnerability assessment involves the systematic examination of a system or network to identify vulnerabilities that could be exploited by attackers. This can involve both automated and manual techniques, such as scanning for open ports, analyzing software configurations, and testing for known vulnerabilities in specific applications. Risk analysis, on the other hand, involves a more comprehensive examination of the potential impact of a security breach, including the likelihood of an attack occurring and the potential consequences for the organization. This can involve evaluating the value of assets that could be compromised, the cost of remediation, and the potential impact on reputation, financial stability, and legal liability [253,254].

Performing a vulnerability assessment in a microgrid involves several important steps to ensure that the microgrid system is secure and resilient. This process includes identifying the assets and infrastructure that need to be assessed, identifying potential threats, analyzing vulnerabilities, evaluating the likelihood and impact of an attack, developing and implementing mitigation strategies, and continuously monitoring and updating the microgrid system to ensure ongoing security and resilience. By following these steps, a vulnerability assessment can identify potential threats and vulnerabilities, assess the impact of an attack, and develop and implement effective mitigation strategies to protect the microgrid system. Figure 13 illustrates some of the main and crucial steps to perform a vulnerability assessment in a microgrid.

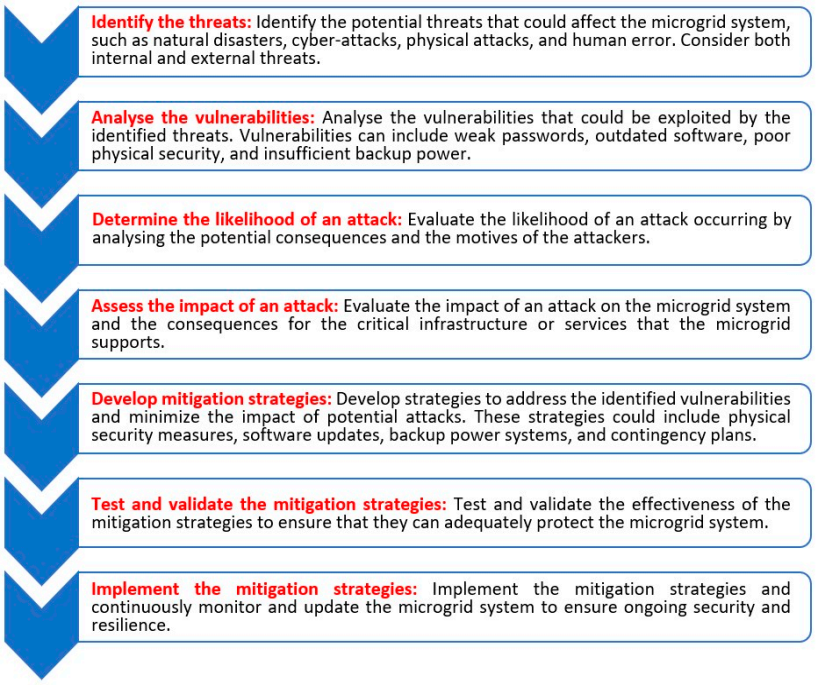

Figure 13. Crucial steps to perform a vulnerability assessment in a microgrid.

In addition to vulnerability assessment, to ensure the safe and reliable operation of MGs, it is essential to perform a comprehensive risk analysis that identifies potential hazards, assesses their likelihood and impact, prioritizes risks, develops appropriate risk mitigation strategies, and monitors the effectiveness of the risk management process over time [103,255]. As illustrated in Figure 14, the main and crucial steps to perform a risk analysis in a microgrid includes hazard identification, likelihood assessment, impact assessment, risk prioritization, risk tolerance determination, evaluation of existing controls, development of risk mitigation strategies, implementation of risk mitigation measures, and monitoring and review. By following these steps, organizations can effectively manage risk in their MGs and ensure the continuity of critical services even in the face of unexpected events.

Figure 14. Crucial steps to perform a risk analysis in a microgrid.

6. Barriers and Challenges in Digitalization of MGs

The digitalization of MGs refers to the integration of advanced communication, monitoring, and control technologies into the microgrid infrastructure to optimize energy management and improve reliability. However, despite the benefits of digitalization, there are still several barriers and challenges that hinder its implementation. Various barriers and challenges to digitalization of MGs and possible solutions to overcome these obstacles are summarized below:

Technical complexity: The digitalization of MGs involves the integration of various technologies such as sensors, communication systems, and advanced control algorithms. The complexity of integrating these technologies can pose a significant challenge, especially for small-scale MGs that have limited resources and technical expertise [96,256,257]. The technical complexity of microgrid digitalization requires specialized knowledge and expertise, making it difficult for small-scale MGs to invest in such systems.

High implementation costs: Digitalizing a microgrid requires significant upfront investment, which can be a barrier to its implementation, particularly for small and medium-sized enterprises (SMEs) [258,259]. The cost of digitalization includes the installation of communication infrastructure, software, hardware, and sensors. The high cost of digitalization is a significant challenge, especially for MGs with limited resources and financing options.

Regulatory barriers: MGs are subject to various regulatory frameworks, which can be challenging to navigate, especially when it comes to digitalization. Regulatory barriers may include strict technical and safety standards, grid interconnection rules, and permitting processes that can delay the implementation of digitalization projects [260–262]. The regulatory barriers can be challenging for small-scale MGs to meet, especially when they lack the financial and technical resources to comply.

Data privacy and security concerns: The digitalization of MGs involves the collection and processing of sensitive data, such as energy consumption patterns, personal information, and grid performance data. Ensuring data privacy and security is critical, and any breach can have severe consequences. The data privacy and security concerns are a significant challenge, especially when MGs lack the resources to invest in advanced cybersecurity measures [26,263,264].

Lack of standardization: The lack of standardization in digitalization technologies can pose a significant challenge to the implementation of microgrid digitalization projects. There are several different communication protocols, control algorithms, and hardware systems used in microgrid digitalization, which can make interoperability and data exchange difficult [265–267].

Interoperability issues: The integration of various technologies in microgrid digitalization can lead to interoperability issues [268–270]. Interoperability refers to the ability of different systems to work together seamlessly. Limited interoperability can be a significant barrier to the successful implementation of microgrid digitalization, leading to data silos, communication breakdowns, and inefficient energy management. In recent years, protocols such as MQTT (Message Queuing Telemetry Transport) and OPC-UA (OPC Unified Architecture) have gained prominence in the context of IoT and Industry 4.0, respectively. These protocols offer standardized communication frameworks that facilitate the exchange of data and enable interoperability among different components and devices. In the context of microgrids, the application of protocols such as MQTT and OPC-UA can significantly enhance interoperability. By utilizing these prevalent communication protocols, microgrid systems can achieve seamless data sharing, efficient energy management, and improved coordination among various devices and subsystems. Moreover, the adoption of such standardized protocols can address data silos and communication breakdowns, ensuring a more robust and integrated microgrid infrastructure.

Limited technical expertise: Microgrid digitalization requires specialized technical expertise in areas such as communication systems, control algorithms, and cybersecurity [271,272]. However, there is a shortage of professionals with the necessary skills and knowledge to implement and maintain microgrid digitalization projects.

Integration with the main grid: MGs are typically designed to operate in isolation from the main grid, but they can also be connected to it [94,269,273]. The integration of MGs with the main grid requires complex control algorithms to ensure the stability and reliability of both systems.

As clearly outlined above and also presented in Table 10, there are several barriers and challenges to the digitalization of MGs. To overcome these barriers and challenges, various solutions can be employed, including providing training and support to enhance technical expertise, utilizing cost-effective technologies and financing options, working with regulatory bodies to establish clear guidelines, investing in advanced cybersecurity measures, developing common standards for hardware and software systems, establishing a common communication protocol and interface, investing in education and training programs to develop expertise, and developing sophisticated control algorithms to ensure integration. By addressing these barriers and challenges, the digitalization of MGs can be successfully implemented, leading to optimized energy management and improved reliability, which are critical for the transition to sustainable energy sources.

Table 10. Main barriers and challenges to the digitalization of MGs.

Barrier/Challenge	Description	Possible Solution
Technical complexity	Integration of multiple technologies can pose a challenge	Provide training and support to enhance technical expertise
High implementation costs	Upfront investment in infrastructure and systems	Utilize cost-effective technologies and financing options
Regulatory barriers	Navigating complex regulatory frameworks	Work with regulatory bodies to establish clear guidelines
Data privacy and security	Ensuring protection of sensitive data	Invest in advanced cybersecurity measures
Lack of standardization	Lack of standardization in digitalization technologies	Develop common standards for hardware and software systems
Interoperability issues	Limited interoperability of different systems	Establish a common communication protocol and interface
Limited technical expertise	Shortage of skilled professionals in microgrid digitalization	Invest in education and training programs to develop expertise
Integration with the main grid	Complex control algorithms to ensure stability and reliability	Develop sophisticated control algorithms to ensure integration

7. Conclusions

This paper provides a comprehensive overview of the future digitalization of MGs that are a promising solution for ensuring reliable, secure, and sustainable energy supply to both urban and rural communities. The paper presented the background and design of MGs, as well as their control, management, and optimization techniques. Moreover, the paper discussed the various digital technologies that are transforming the way MGs are designed, operated, and managed. These technologies have the potential to revolutionize the way MGs operate and improve their efficiency, reliability, and sustainability.

However, the paper also highlighted the various challenges and barriers that hinder the digitalization of MGs. These challenges must be addressed to fully realize the potential benefits of digitalization in MGs. Furthermore, the paper emphasized the importance of cybersecurity in MGs. The increasing dependence on digital technologies has made MGs vulnerable to various cyberattacks, and, thus, cybersecurity strategies must be implemented.

In conclusion, this paper provides a comprehensive overview of the future digitalization of MGs and yields several significant outcomes as follows:

Overview of future digitalization: The paper presented an in-depth understanding of the role of digitalization in MGs, showcasing their potential as a reliable, secure, and sustainable energy supply solution for urban and rural communities. The outcomes emphasize the importance of adopting digital technologies in transforming the design, operation, and management of MGs.

Analysis of digital technologies: The paper explored various digital technologies reshaping MGs, including distributed energy resources management systems, microgrid energy management systems, Internet of Things (IoT), big data analytics, blockchain technology, artificial intelligence (AI), digital twin technology, cloud computing, and augmented reality. These outcomes highlight how these technologies can revolutionize MG operations, enhancing their efficiency, reliability, and sustainability.

Identification of challenges and barriers: The paper shed light on the challenges and barriers hindering the digitalization of MGs. These include technical complexity, high implementation costs, regulatory barriers, data privacy and security concerns, lack of standardization, interoperability issues, limited technical expertise, and integration with the main grid. The outcomes underscore the importance of addressing these obstacles to fully harness the benefits of digitalization in MGs.

Emphasis on cybersecurity: The paper emphasized the significance of cybersecurity in MGs due to their increasing reliance on digital technologies. The outcomes emphasize the implementation of robust cybersecurity strategies, such as encryption of communication channels, access control, device updates and patches, threat detection and response mechanisms, network security, identification and protection of weak points, personnel training, password management, emergency planning, and physical security. These measures ensure the resilience and protection of MGs against cyberthreats.

Need for further research and development: The paper highlights that the digitalization of MGs is a rapidly evolving field that necessitates ongoing research and development efforts. The outcomes stress the importance of continuously integrating and advancing digital technologies while simultaneously addressing the challenges and barriers. The paper encourages future studies to explore innovative solutions, strategies, and frameworks to propel the digital transformation of MGs.

The outcomes of this paper have significant implications for the future digitalization of MGs, highlighting the potential benefits of adopting digital technologies in MG design, operation, and management. Emphasizing the crucial role of these technologies in ensuring reliable, secure, and sustainable energy supply to urban and rural communities, the paper underscores their importance in the digitalization process. By demonstrating how digital technologies such as DERMSs, MEMs, IoT, big data analytics, blockchain technology, AI, digital twin technology, cloud computing, and augmented reality can revolutionize MG operations, the paper provides valuable insights for policymakers, energy planners, and industry stakeholders.

Furthermore, the paper makes substantial contributions by offering a comprehensive overview of the future digitalization of MGs. It synthesizes and consolidates diverse research and developments in this rapidly evolving field, and addresses the challenges and barriers hindering MG digitalization, including technical complexities, regulatory constraints, and cybersecurity concerns. Additionally, it identifies gaps and areas for future investigation, providing valuable insights for further research in the field.

Overall, these contributions and implications contribute to the advancement of knowledge and understanding in the digitalization of MGs, guiding future endeavors and promoting the implementation of effective strategies.

Funding: This research received no external funding.

Data Availability Statement: Data sharing not applicable.

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

References

1. Shahgholian, G. A Brief Review on Microgrids: Operation, Applications, Modeling, and Control. *Int. Trans. Electr. Energy Syst.* **2021**, *31*, e12885. [CrossRef]
2. Al Sumarmad, K.A.; Sulaiman, N.; Wahab, N.I.A.; Hizam, H. Energy Management and Voltage Control in Microgrids Using Artificial Neural Networks, PID, and Fuzzy Logic Controllers. *Energies* **2022**, *15*, 303. [CrossRef]
3. Chaudhary, G.; Lamb, J.J.; Burheim, O.S.; Austbø, B. Review of Energy Storage and Energy Management System Control Strategies in Microgrids. *Energies* **2021**, *14*, 4929. [CrossRef]
4. Céspedes, R.; Lónez, C. Remote Microgrids Digitization: Design and Implementation for Sustainability. In Proceedings of the 2021 IEEE PES Innovative Smart Grid Technologies Conference—Latin America (ISGT Latin America), Lima, Peru, 15–17 September 2021; pp. 1–5.
5. Celanovic, N.F. Digitalization of Microgrids and Electrical Distribution Networks. Available online: https://info.typhoon-hil.com/blog/microgrid-digitalization (accessed on 6 April 2023).
6. Bazmohammadi, N.; Madary, A.; Vasquez, J.C.; Mohammadi, H.B.; Khan, B.; Wu, Y.; Guerrero, J.M. Microgrid Digital Twins: Concepts, Applications, and Future Trends. *IEEE Access* **2022**, *10*, 2284–2302. [CrossRef]
7. Abbasi, M.; Abbasi, E.; Li, L.; Aguilera, R.P.; Lu, D.; Wang, F. Review on the Microgrid Concept, Structures, Components, Communication Systems, and Control Methods. *Energies* **2023**, *16*, 484. [CrossRef]
8. Hirsch, A.; Parag, Y.; Guerrero, J. Microgrids: A Review of Technologies, Key Drivers, and Outstanding Issues. *Renew. Sustain. Energy Rev.* **2018**, *90*, 402–411. [CrossRef]

9. Ali, M.; Vasquez, J.C.; Guerrero, J.M.; Guan, Y.; Golestan, S.; De La Cruz, J.; Koondhar, M.A.; Khan, B. A Comparison of Grid-Connected Local Hospital Loads with Typical Backup Systems and Renewable Energy System Based Ad Hoc Microgrids for Enhancing the Resilience of the System. *Energies* **2023**, *16*, 1918. [CrossRef]
10. Lagrange, A.; de Simón-Martín, M.; González-Martínez, A.; Bracco, S.; Rosales-Asensio, E. Sustainable Microgrids with Energy Storage as a Means to Increase Power Resilience in Critical Facilities: An Application to a Hospital. *Int. J. Electr. Power Energy Syst.* **2020**, *119*, 105865. [CrossRef]
11. Gao, F.; Kang, R.; Cao, J.; Yang, T. Primary and Secondary Control in DC Microgrids: A Review. *J. Mod. Power Syst. Clean Energy* **2019**, *7*, 227–242. [CrossRef]
12. Voltage and Frequency Control in Renewable-Rich Power Grids—IEEE Smart Grid. Available online: https://smartgrid.ieee.org/resources/webinars/bulk-generation/voltage-and-frequency-control-in-renewable-rich-power-grids (accessed on 6 April 2023).
13. Lan, Z.; Wang, J.; Zeng, J.; He, D.; Xiao, F.; Jiang, F. Constant Frequency Control Strategy of Microgrids by Coordinating Energy Router and Energy Storage System. *Math. Probl. Eng.* **2020**, *2020*, e4976529. [CrossRef]
14. Erdocia, J.; Urtasun, A.; Marroyo, L. Conductance-Frequency Droop Control to Ensure Transient Stability of Inverter-Based Stand-Alone Microgrids. *Int. J. Electr. Power Energy Syst.* **2023**, *144*, 108562. [CrossRef]
15. Malik, S.M.; Ai, X.; Sun, Y.; Zhengqi, C.; Shupeng, Z. Voltage and Frequency Control Strategies of Hybrid AC/DC Microgrid: A Review. *IET Gener. Transm. Distrib.* **2017**, *11*, 303–313. [CrossRef]
16. Yang, Z.; Wang, C.; Han, J.; Yang, F.; Shen, Y.; Min, H.; Hu, W.; Song, H. Analysis of Voltage Control Strategies for DC Microgrid with Multiple Types of Energy Storage Systems. *Electronics* **2023**, *12*, 1661. [CrossRef]
17. Thirunavukkarasu, G.S.; Seyedmahmoudian, M.; Jamei, E.; Horan, B.; Mekhilef, S.; Stojcevski, A. Role of Optimization Techniques in Microgrid Energy Management Systems—A Review. *Energy Strategy Rev.* **2022**, *43*, 100899. [CrossRef]
18. Phommixay, S.; Doumbia, M.L.; Lupien St-Pierre, D. Review on the Cost Optimization of Microgrids via Particle Swarm Optimization. *Int. J. Energy Environ. Eng.* **2020**, *11*, 73–89. [CrossRef]
19. Alvarado-Barrios, L.; Rodríguez del Nozal, A.; Tapia, A.; Martínez-Ramos, J.L.; Reina, D.G. An Evolutionary Computational Approach for the Problem of Unit Commitment and Economic Dispatch in Microgrids under Several Operation Modes. *Energies* **2019**, *12*, 2143. [CrossRef]
20. Blockchain Technology in Distributed Energy Domain. *FutureBridge*. 2021. Available online: https://www.futurebridge.com/blog/blockchain-technology-in-distributed-energy-domain (accessed on 4 June 2023).
21. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.R.; Chopra, S.S. Distributed Energy Resources and the Application of AI, IoT, and Blockchain in Smart Grids. *Energies* **2020**, *13*, 5739. [CrossRef]
22. Danilczyk, W.; Sun, Y.; He, H. ANGEL: An Intelligent Digital Twin Framework for Microgrid Security. In Proceedings of the 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 13–15 October 2019; pp. 1–6.
23. Rosero, D.G.; Díaz, N.L.; Trujillo, C.L. Cloud and Machine Learning Experiments Applied to the Energy Management in a Microgrid Cluster. *Appl. Energy* **2021**, *304*, 117770. [CrossRef]
24. Chandak, S.; Rout, P.K. The Implementation Framework of a Microgrid: A Review. *Int. J. Energy Res.* **2021**, *45*, 3523–3547. [CrossRef]
25. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.M. Towards Collective Energy Community: Potential Roles of Microgrid and Blockchain to Go beyond P2P Energy Trading. *Appl. Energy* **2022**, *314*, 119003. [CrossRef]
26. Ramotsoela, D.T.; Hancke, G.P.; Abu-Mahfouz, A.M. Practical Challenges of Attack Detection in Microgrids Using Machine Learning. *J. Sens. Actuator Netw.* **2023**, *12*, 7. [CrossRef]
27. 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. [CrossRef]
28. Choudhury, S. A Comprehensive Review on Issues, Investigations, Control and Protection Trends, Technical Challenges and Future Directions for Microgrid Technology. *Int. Trans. Electr. Energy Syst.* **2020**, *30*, e12446. [CrossRef]
29. Ghobakhloo, M. Determinants of Information and Digital Technology Implementation for Smart Manufacturing. *Int. J. Prod. Res.* **2020**, *58*, 2384–2405. [CrossRef]
30. Zaki, M. Digital Transformation: Harnessing Digital Technologies for the next Generation of Services. *J. Serv. Mark.* **2019**, *33*, 429–435. [CrossRef]
31. Lei, B.; Ren, Y.; Luan, H.; Dong, R.; Wang, X.; Liao, J.; Fang, S.; Gao, K. A Review of Optimization for System Reliability of Microgrid. *Mathematics* **2023**, *11*, 822. [CrossRef]
32. Ahmad, S.; Shafiullah, M.; Ahmed, C.B.; Alowaifeer, M. A Review of Microgrid Energy Management and Control Strategies. *IEEE Access* **2023**, *11*, 21729–21757. [CrossRef]
33. Eid, B.M.; Rahim, N.A.; Selvaraj, J.; El Khateb, A.H. Control Methods and Objectives for Electronically Coupled Distributed Energy Resources in Microgrids: A Review. *IEEE Syst. J.* **2016**, *10*, 446–458. [CrossRef]
34. Guerrero, J.M.; Vasquez, J.C.; Matas, J.; de Vicuna, L.G.; Castilla, M. Hierarchical Control of Droop-Controlled AC and DC Microgrids—A General Approach Toward Standardization. *IEEE Trans. Ind. Electron.* **2011**, *58*, 158–172. [CrossRef]
35. Salehi, R.; Vahidi, B.; Farokhnia, N.; Abedi, M. Harmonic Elimination and Optimization of Stepped Voltage of Multilevel Inverter by Bacterial Foraging Algorithm. *J. Electr. Eng. Technol.* **2010**, *5*, 545–551. [CrossRef]
36. Salehi, N.; Martinez-Garcia, H.; Velasco-Quesada, G.; Guerrero, J.M. A Comprehensive Review of Control Strategies and Optimization Methods for Individual and Community Microgrids. *IEEE Access* **2022**, *10*, 15935–15955. [CrossRef]

37. Wang, R.; Wang, P.; Xiao, G. *Intelligent Microgrid Management and EV Control Under Uncertainties in Smart Grid*; Springer Singapore: Singapore, 2018; ISBN 978-981-10-4249-2.
38. Yu, Z.; Ai, Q.; Gong, J.; Piao, L. A Novel Secondary Control for Microgrid Based on Synergetic Control of Multi-Agent System. *Energies* **2016**, *9*, 243. [CrossRef]
39. Kaur, A.; Kaushal, J.; Basak, P. A Review on Microgrid Central Controller. *Renew. Sustain. Energy Rev.* **2016**, *55*, 338–345. [CrossRef]
40. Ding, T.; Lin, Y.; Bie, Z.; Chen, C. A Resilient Microgrid Formation Strategy for Load Restoration Considering Master-Slave Distributed Generators and Topology Reconfiguration. *Appl. Energy* **2017**, *199*, 205–216. [CrossRef]
41. Saad, N.H.; El-Sattar, A.A.; Mansour, A.E.-A.M. A Novel Control Strategy for Grid Connected Hybrid Renewable Energy Systems Using Improved Particle Swarm Optimization. *Ain Shams Eng. J.* **2018**, *9*, 2195–2214. [CrossRef]
42. Hu, J.; Shan, Y.; Cheng, K.W.; Islam, S. Overview of Power Converter Control in Microgrids—Challenges, Advances, and Future Trends. *IEEE Trans. Power Electron.* **2022**, *37*, 9907–9922. [CrossRef]
43. Werth, A.; Andre, A.; Kawamoto, D.; Morita, T.; Tajima, S.; Tokoro, M.; Yanagidaira, D.; Tanaka, K. Peer-to-Peer Control System for DC Microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 3667–3675. [CrossRef]
44. Long, C.; Wu, J.; Zhou, Y.; Jenkins, N. Peer-to-Peer Energy Sharing through a Two-Stage Aggregated Battery Control in a Community Microgrid. *Appl. Energy* **2018**, *226*, 261–276. [CrossRef]
45. Adineh, B.; Keypour, R.; Davari, P.; Blaabjerg, F. Review of Harmonic Mitigation Methods in Microgrid: From a Hierarchical Control Perspective. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 3044–3060. [CrossRef]
46. Ahmed, M.; Meegahapola, L.; Vahidnia, A.; Datta, M. Stability and Control Aspects of Microgrid Architectures—A Comprehensive Review. *IEEE Access* **2020**, *8*, 144730–144766. [CrossRef]
47. Chen, M.; Xiao, X. Hierarchical Frequency Control Strategy of Hybrid Droop/VSG-Based Islanded Microgrids. *Electr. Power Syst. Res.* **2018**, *155*, 131–143. [CrossRef]
48. Wan Abdullah, W.A.; Ahmad, A.Z. Voltage and Active Power Management Control of PV Source Distributed Generations under Unbalanced Voltage of Non-Islanded Microgrid. *J. Phys. Conf. Ser.* **2022**, *2319*, 012003. [CrossRef]
49. Ma, Q.; Huang, X.; Wang, F.; Xu, C.; Babaei, R.; Ahmadian, H. Optimal Sizing and Feasibility Analysis of Grid-Isolated Renewable Hybrid Microgrids: Effects of Energy Management Controllers. *Energy* **2022**, *240*, 122503. [CrossRef]
50. Tran, Q.T.; Davies, K.; Sepasi, S. Isolation Microgrid Design for Remote Areas with the Integration of Renewable Energy: A Case Study of Con Dao Island in Vietnam. *Clean Technol.* **2021**, *3*, 804–820. [CrossRef]
51. Rodriguez, M.; Arcos–Aviles, D.; Martinez, W. Fuzzy Logic-Based Energy Management for Isolated Microgrid Using Meta-Heuristic Optimization Algorithms. *Appl. Energy* **2023**, *335*, 120771. [CrossRef]
52. Jain, D.; Saxena, D. Comprehensive Review on Control Schemes and Stability Investigation of Hybrid AC-DC Microgrid. *Electr. Power Syst. Res.* **2023**, *218*, 109182. [CrossRef]
53. Modu, B.; Abdullah, M.P.; Sanusi, M.A.; Hamza, M.F. DC-Based Microgrid: Topologies, Control Schemes, and Implementations. *Alex. Eng. J.* **2023**, *70*, 61–92. [CrossRef]
54. Abd-el-Motaleb, A.M.; Hamilton, D. Modelling and Sensitivity Analysis of Isolated Microgrids. *Renew. Sustain. Energy Rev.* **2015**, *47*, 416–426. [CrossRef]
55. Polleux, L.; Guerassimoff, G.; Marmorat, J.-P.; Sandoval-Moreno, J.; Schuhler, T. An Overview of the Challenges of Solar Power Integration in Isolated Industrial Microgrids with Reliability Constraints. *Renew. Sustain. Energy Rev.* **2022**, *155*, 111955. [CrossRef]
56. Bintoudi, A.D.; Demoulias, C. Optimal Isolated Microgrid Topology Design for Resilient Applications. *Appl. Energy* **2023**, *338*, 120909. [CrossRef]
57. Hanzaei, S.H.; Korki, M.; Zhang, X.-M. Distributed Cooperative Voltage Mode Control for DC-Isolated Microgrids Powered by Renewable Energy Sources. *Int. J. Electr. Power Energy Syst.* **2023**, *152*, 109175. [CrossRef]
58. Hui, H.; Chen, Y.; Yang, S.; Zhang, H.; Jiang, T. Coordination Control of Distributed Generators and Load Resources for Frequency Restoration in Isolated Urban Microgrids. *Appl. Energy* **2022**, *327*, 120116. [CrossRef]
59. Kabalcı, E. An Islanded Hybrid Microgrid Design with Decentralized DC and AC Subgrid Controllers. *Energy* **2018**, *153*, 185–199. [CrossRef]
60. Mahdavi Tabatabaei, N.; Kabalci, E.; Bizon, N. (Eds.) *Microgrid Architectures, Control and Protection Methods*; Power Systems; Springer International Publishing: Cham, Switzerland, 2020; ISBN 978-3-030-23722-6.
61. Maitra, A.; Pratt, A.; Hubert, T.; Wang, D.; Prabakar, K.; Handa, R.; Baggu, M.; McGranaghan, M. Microgrid Controllers: Expanding Their Role and Evaluating Their Performance. *IEEE Power Energy Mag.* **2017**, *15*, 41–49. [CrossRef]
62. *IEEE Standard for the Specification of Microgrid Controllers*; IEEE: New York, NY, USA, 2017.
63. Hatziargyriou, N. *Microgrid: Architectures and Control*; John Wiley and Sons Ltd.: Noida, India, 2014; ISBN 978-1-118-72064-6.
64. Hamidieh, M.; Ghassemi, M. Microgrids and Resilience: A Review. *IEEE Access* **2022**, *10*, 106059–106080. [CrossRef]
65. Ma, X.; Yang, P.; Dong, H.; Yang, J.; Zhao, Y. Secondary Control Strategy of Islanded Micro-Grid Based on Multi-Agent Consistency. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6.
66. Xiao, J.; Wang, P.; Setyawan, L. Hierarchical Control of Hybrid Energy Storage System in DC Microgrids. *IEEE Trans. Ind. Electron.* **2015**, *62*, 4915–4924. [CrossRef]
67. Wang, J.; Jin, C.; Wang, P. A Uniform Control Strategy for the Interlinking Converter in Hierarchical Controlled Hybrid AC/DC Microgrids. *IEEE Trans. Ind. Electron.* **2018**, *65*, 6188–6197. [CrossRef]

68. Ito, Y.; Zhongqing, Y.; Akagi, H. DC Microgrid Based Distribution Power Generation System. In Proceedings of the 4th International Power Electronics and Motion Control Conference IPEMC 2004, Xi'an, China, 14–16 August 2004; Volume 3, pp. 1740–1745.
69. Kwasinski, A.; Krein, P.T. A Microgrid-Based Telecom Power System Using Modular Multiple-Input DC-DC Converters. In Proceedings of the INTELEC 05—Twenty-Seventh International Telecommunications Conference, Berlin, Germany, 18–22 September 2005; pp. 515–520.
70. Kakigano, H.; Miura, Y.; Ise, T. Low-Voltage Bipolar-Type DC Microgrid for Super High Quality Distribution. *IEEE Trans. Power Electron.* **2010**, *25*, 3066–3075. [CrossRef]
71. Li, Z.; Zang, C.; Zeng, P.; Yu, H.; Li, S. Fully Distributed Hierarchical Control of Parallel Grid-Supporting Inverters in Islanded AC Microgrids. *IEEE Trans. Ind. Inform.* **2018**, *14*, 679–690. [CrossRef]
72. Kiehbadroudinezhad, M.; Merabet, A.; Abo-Khalil, A.G.; Salameh, T.; Ghenai, C. Intelligent and Optimized Microgrids for Future Supply Power from Renewable Energy Resources: A Review. *Energies* **2022**, *15*, 3359. [CrossRef]
73. Aljafari, B.; Vasantharaj, S.; Indragandhi, V.; Vaibhav, R. Optimization of DC, AC, and Hybrid AC/DC Microgrid-Based IoT Systems: A Review. *Energies* **2022**, *15*, 6813. [CrossRef]
74. Mannini, R.; Eynard, J.; Grieu, S. A Survey of Recent Advances in the Smart Management of Microgrids and Networked Microgrids. *Energies* **2022**, *15*, 7009. [CrossRef]
75. Dragicevic, T.; Lu, X.; Vasquez, J.C.; Guerrero, J.M. DC Microgrids—Part II: A Review of Power Architectures, Applications, and Standardization Issues. *IEEE Trans. Power Electron.* **2016**, *31*, 3528–3549. [CrossRef]
76. Sahoo, S.K.; Sinha, A.K.; Kishore, N.K. Control Techniques in AC, DC, and Hybrid AC–DC Microgrid: A Review. *IEEE J. Emerg. Sel. Top. Power Electron.* **2018**, *6*, 738–759. [CrossRef]
77. Beheshtaein, S.; Cuzner, R.M.; Forouzesh, M.; Savaghebi, M.; Guerrero, J.M. DC Microgrid Protection: A Comprehensive Review. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, 1. [CrossRef]
78. Pamulapati, T.; Cavus, M.; Odigwe, I.; Allahham, A.; Walker, S.; Giaouris, D. A Review of Microgrid Energy Management Strategies from the Energy Trilemma Perspective. *Energies* **2022**, *16*, 289. [CrossRef]
79. Hooshyar, A.; Iravani, R. Microgrid Protection. *Proc. IEEE* **2017**, *105*, 1332–1353. [CrossRef]
80. Bayrak, G.; Kabalci, E. Implementation of a New Remote Islanding Detection Method for Wind–Solar Hybrid Power Plants. *Renew. Sustain. Energy Rev.* **2016**, *58*, 1–15. [CrossRef]
81. Li, C.; Cao, C.; Cao, Y.; Kuang, Y.; Zeng, L.; Fang, B. A Review of Islanding Detection Methods for Microgrid. *Renew. Sustain. Energy Rev.* **2014**, *35*, 211–220. [CrossRef]
82. Abdulrazzaq Oraibi, W.; Mohammadi-Ivatloo, B.; Hosseini, S.H.; Abapour, M. Multi Microgrid Framework for Resilience Enhancement Considering Mobile Energy Storage Systems and Parking Lots. *Appl. Sci.* **2023**, *13*, 1285. [CrossRef]
83. Khan, S.S.; Wen, H. A Comprehensive Review of Fault Diagnosis and Tolerant Control in DC-DC Converters for DC Microgrids. *IEEE Access* **2021**, *9*, 80100–80127. [CrossRef]
84. Alam, M.N.; Chakrabarti, S.; Ghosh, A. Networked Microgrids: State-of-the-Art and Future Perspectives. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1238–1250. [CrossRef]
85. Arkhangelski, J.; Siano, P.; Mahamadou, A.-T.; Lefebvre, G. Evaluating the Economic Benefits of a Smart-Community Microgrid with Centralized Electrical Storage and Photovoltaic Systems. *Energies* **2020**, *13*, 1764. [CrossRef]
86. Jiang, W.; Wang, X.; Huang, H.; Zhang, D.; Ghadimi, N. Optimal Economic Scheduling of Microgrids Considering Renewable Energy Sources Based on Energy Hub Model Using Demand Response and Improved Water Wave Optimization Algorithm. *J. Energy Storage* **2022**, *55*, 105311. [CrossRef]
87. Huang, S.; Abedinia, O. Investigation in Economic Analysis of Microgrids Based on Renewable Energy Uncertainty and Demand Response in the Electricity Market. *Energy* **2021**, *225*, 120247. [CrossRef]
88. Arunachalam, R.K.; Chandrasekaran, K.; Rusu, E.; Ravichandran, N.; Fayek, H.H. Economic Feasibility of a Hybrid Microgrid System for a Distributed Substation. *Sustainability* **2023**, *15*, 3133. [CrossRef]
89. Wolsink, M. Distributed Energy Systems as Common Goods: Socio-Political Acceptance of Renewables in Intelligent Microgrids. *Renew. Sustain. Energy Rev.* **2020**, *127*, 109841. [CrossRef]
90. Sandelic, M.; Peyghami, S.; Sangwongwanich, A.; Blaabjerg, F. Reliability Aspects in Microgrid Design and Planning: Status and Power Electronics-Induced Challenges. *Renew. Sustain. Energy Rev.* **2022**, *159*, 112127. [CrossRef]
91. Bordons, C.; Garcia-Torres, F.; Ridao, M.A. Interconnection of Microgrids. In *Model Predictive Control of Microgrids*; Bordons, C., Garcia-Torres, F., Ridao, M.A., Eds.; Advances in Industrial Control; Springer International Publishing: Cham, Switzerland, 2020; pp. 191–225, ISBN 978-3-030-24570-2.
92. Raya-Armenta, J.M.; Bazmohammadi, N.; Avina-Cervantes, J.G.; Sáez, D.; Vasquez, J.C.; Guerrero, J.M. Energy Management System Optimization in Islanded Microgrids: An Overview and Future Trends. *Renew. Sustain. Energy Rev.* **2021**, *149*, 111327. [CrossRef]
93. Hu, S.; Ge, X.; Chen, X.; Yue, D. Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial-of-Service Attacks. *IEEE Trans. Smart Grid* **2023**, *14*, 690–700. [CrossRef]
94. Talaat, M.; Elkholy, M.H.; Alblawi, A.; Said, T. Artificial Intelligence Applications for Microgrids Integration and Management of Hybrid Renewable Energy Sources. *Artif. Intell. Rev.* **2023**. [CrossRef]

95. Elmouatamid, A.; Ouladsine, R.; Bakhouya, M.; El Kamoun, N.; Khaidar, M.; Zine-Dine, K. Review of Control and Energy Management Approaches in Micro-Grid Systems. *Energies* **2021**, *14*, 168. [CrossRef]
96. Ishaq, S.; Khan, I.; Rahman, S.; Hussain, T.; Iqbal, A.; Elavarasan, R.M. A Review on Recent Developments in Control and Optimization of Micro Grids. *Energy Rep.* **2022**, *8*, 4085–4103. [CrossRef]
97. Rangu, S.K.; Lolla, P.R.; Dhenuvakonda, K.R.; Singh, A.R. Recent Trends in Power Management Strategies for Optimal Operation of Distributed Energy Resources in Microgrids: A Comprehensive Review. *Int. J. Energy Res.* **2020**, *44*, 9889–9911. [CrossRef]
98. Rajesh, P.; Shajin, F.H.; Rajani, B.; Sharma, D. An Optimal Hybrid Control Scheme to Achieve Power Quality Enhancement in Micro Grid Connected System. *Int. J. Numer. Model. Electron. Netw. Devices Fields* **2022**, *35*, e3019. [CrossRef]
99. Bilakanti, N.; Gurung, N.; Chen, H.; Kothandaraman, S.R. Priority-Based Management Algorithm in Distributed Energy Resource Management Systems. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 351–356.
100. Shakir, M.; Biletskiy, Y. Forecasting and Optimisation for Microgrid in Home Energy Management Systems. *IET Gener. Transm. Distrib.* **2020**, *14*, 3458–3468. [CrossRef]
101. Ali, S.A.; Hussain, A.; Haider, W.; Rehman, H.U.; Kazmi, S.A.A. Optimal Energy Management System of Isolated Multi-Microgrids with Local Energy Transactive Market with Indigenous PV-, Wind-, and Biomass-Based Resources. *Energies* **2023**, *16*, 1667. [CrossRef]
102. Lei, J.; Gao, S.; Shi, J.; Wei, X.; Dong, M.; Wang, W.; Han, Z. A Reinforcement Learning Approach for Defending Against Multiscenario Load Redistribution Attacks. *IEEE Trans. Smart Grid* **2022**, *13*, 3711–3722. [CrossRef]
103. Peng, H.; Su, M.; Li, S.; Li, C. Static Security Risk Assessment for Islanded Hybrid AC/DC Microgrid. *IEEE Access* **2019**, *7*, 37545–37554. [CrossRef]
104. Li, Q.; Cui, Z.; Cai, Y.; Su, Y.; Wang, B. Renewable-Based Microgrids' Energy Management Using Smart Deep Learning Techniques: Realistic Digital Twin Case. *Sol. Energy* **2023**, *250*, 128–138. [CrossRef]
105. Abunima, H.; Park, W.-H.; Glick, M.B.; Kim, Y.-S. Two-Stage Stochastic Optimization for Operating a Renewable-Based Microgrid. *Appl. Energy* **2022**, *325*, 119848. [CrossRef]
106. Cheng, Z.; Jia, D.; Li, Z.; Xu, S.; Si, J. Multi-Time-Scale Energy Management for Microgrid Using Expected-Scenario-Oriented Stochastic Optimization. *Sustain. Energy Grids Netw.* **2022**, *30*, 100670. [CrossRef]
107. Kamal, F.; Chowdhury, B. Model Predictive Control and Optimization of Networked Microgrids. *Int. J. Electr. Power Energy Syst.* **2022**, *138*, 107804. [CrossRef]
108. Konneh, K.V.; Adewuyi, O.B.; Lotfy, M.E.; Sun, Y.; Senjyu, T. Application Strategies of Model Predictive Control for the Design and Operations of Renewable Energy-Based Microgrid: A Survey. *Electronics* **2022**, *11*, 554. [CrossRef]
109. Afzal, M.Z.; Aurangzeb, M.; Iqbal, S.; Rehman, A.u.; Kotb, H.; AboRas, K.M.; Elgamli, E.; Shouran, M. A Resilience-Oriented Bidirectional ANFIS Framework for Networked Microgrid Management. *Processes* **2022**, *10*, 2724. [CrossRef]
110. Faghiri, M.; Samizadeh, S.; Nikoofard, A.; Khosravy, M.; Senjyu, T. Mixed-Integer Linear Programming for Decentralized Multi-Carrier Optimal Energy Management of a Micro-Grid. *Appl. Sci.* **2022**, *12*, 3262. [CrossRef]
111. Mirbarati, S.H.; Heidari, N.; Nikoofard, A.; Danish, M.S.S.; Khosravy, M. Techno-Economic-Environmental Energy Management of a Micro-Grid: A Mixed-Integer Linear Programming Approach. *Sustainability* **2022**, *14*, 15036. [CrossRef]
112. Ning, B.; Xiao, L. Defense Against Advanced Persistent Threats in Smart Grids: A Reinforcement Learning Approach. In Proceedings of the 2021 40th Chinese Control Conference (CCC), Shanghai, China, 26–28 July 2021; pp. 8598–8603.
113. Lian, Y.; Li, Y.; Zhao, Y.; Yu, C.; Zhao, T.; Wu, L. Robust Multi-Objective Optimization for Islanded Data Center Microgrid Operations. *Appl. Energy* **2023**, *330*, 120344. [CrossRef]
114. Aziz, H.; Tabrizian, M.; Ansarian, M.; Ahmarinejad, A. A Three-Stage Multi-Objective Optimization Framework for Day-Ahead Interaction between Microgrids in Active Distribution Networks Considering Flexible Loads and Energy Storage Systems. *J. Energy Storage* **2022**, *52*, 104739. [CrossRef]
115. Lakhina, U.; Badruddin, N.; Elamvazuthi, I.; Jangra, A.; Huy, T.H.B.; Guerrero, J.M. An Enhanced Multi-Objective Optimizer for Stochastic Generation Optimization in Islanded Renewable Energy Microgrids. *Mathematics* **2023**, *11*, 2079. [CrossRef]
116. Silva, F.M.Q.; El Kattel, M.B.; Pires, I.A.; Maia, T.A.C. Development of a Supervisory System Using Open-Source for a Power Micro-Grid Composed of a Photovoltaic (PV) Plant Connected to a Battery Energy Storage System and Loads. *Energies* **2022**, *15*, 8324. [CrossRef]
117. González, I.; Calderón, A.J.; Folgado, F.J. IoT Real Time System for Monitoring Lithium-Ion Battery Long-Term Operation in Microgrids. *J. Energy Storage* **2022**, *51*, 104596. [CrossRef]
118. Li, S.; Patnaik, S.; Li, J. IoT-Based Technologies for Wind Energy Microgrids Management and Control. *Electronics* **2023**, *12*, 1540. [CrossRef]
119. Mendonca, T.; Bottrell, N.; Green, T. Incorporating Ancillary Service Costs in Distributed Energy Resources Management Systems. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, 29 September–2 October 2019; pp. 1–5.
120. Strezoski, L. Distributed Energy Resource Management Systems—DERMS: State of the Art and How to Move Forward. *WIREs Energy Environ.* **2023**, *12*, e460. [CrossRef]
121. Reilly, J.T. From Microgrids to Aggregators of Distributed Energy Resources. The Microgrid Controller and Distributed Energy Management Systems. *Electr. J.* **2019**, *32*, 30–34. [CrossRef]

122. Poudel, S.; Keene, S.J.; Kini, R.L.; Hanif, S.; Bass, R.B.; Kolln, J.T. Modeling Environment for Testing a Distributed Energy Resource Management System (DERMS) Using GridAPPS-D Platform. *IEEE Access* **2022**, *10*, 77383–77395. [CrossRef]
123. Hosseinzadeh, N.; Al Maashri, A.; Tarhuni, N.; Elhaffar, A.; Al-Hinai, A. A Real-Time Monitoring Platform for Distributed Energy Resources in a Microgrid—Pilot Study in Oman. *Electronics* **2021**, *10*, 1803. [CrossRef]
124. Ali, S.; Zheng, Z.; Aillerie, M.; Sawicki, J.-P.; Péra, M.-C.; Hissel, D. A Review of DC Microgrid Energy Management Systems Dedicated to Residential Applications. *Energies* **2021**, *14*, 4308. [CrossRef]
125. Johnson, J.; Fox, B.; Kaur, K.; Anandan, J. Evaluation of Interoperable Distributed Energy Resources to IEEE 1547.1 Using SunSpec Modbus, IEEE 1815, and IEEE 2030.5. *IEEE Access* **2021**, *9*, 142129–142146. [CrossRef]
126. Razavi, S.-E.; Rahimi, E.; Javadi, M.S.; Nezhad, A.E.; Lotfi, M.; Shafie-khah, M.; Catalão, J.P.S. Impact of Distributed Generation on Protection and Voltage Regulation of Distribution Systems: A Review. *Renew. Sustain. Energy Rev.* **2019**, *105*, 157–167. [CrossRef]
127. U.S. Department of Energy. *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*; U.S. Department of Energy: Washington, DC, USA, 2022.
128. Distributed Energy Resource Management System Market Growth Drivers and Opportunities. Available online: https://www.marketsandmarkets.com/Market-Reports/distributed-energy-resource-management-system-market-256436187.html (accessed on 13 April 2023).
129. Saeed, M.H.; Fangzong, W.; Kalwar, B.A.; Iqbal, S. A Review on Microgrids' Challenges & Perspectives. *IEEE Access* **2021**, *9*, 166502–166517. [CrossRef]
130. Baidya, S.; Nandi, C. A Comprehensive Review on DC Microgrid Protection Schemes. *Electr. Power Syst. Res.* **2022**, *210*, 108051. [CrossRef]
131. Battula, A.R.; Vuddanti, S.; Salkuti, S.R. Review of Energy Management System Approaches in Microgrids. *Energies* **2021**, *14*, 5459. [CrossRef]
132. Sirviö, K.; Kauhaniemi, K.; Ali Memon, A.; Laaksonen, H.; Kumpulainen, L. Functional Analysis of the Microgrid Concept Applied to Case Studies of the Sundom Smart Grid. *Energies* **2020**, *13*, 4223. [CrossRef]
133. Gust, G.; Brandt, T.; Mashayekh, S.; Heleno, M.; DeForest, N.; Stadler, M.; Neumann, D. Strategies for Microgrid Operation under Real-World Conditions. *Eur. J. Oper. Res.* **2021**, *292*, 339–352. [CrossRef]
134. Wang, C.; Fu, S.; Zhang, L.; Jiang, Y.; Shu, Y. Optimal Control of Source–Load–Storage Energy in DC Microgrid Based on the Virtual Energy Storage System. *Energy Rep.* **2023**, *9*, 621–630. [CrossRef]
135. Arunkumar, A.P.; Kuppusamy, S.; Muthusamy, S.; Pandiyan, S.; Panchal, H.; Nagaiyan, P. An Extensive Review on Energy Management System for Microgrids. *Energy Sources Part Recovery Util. Environ. Eff.* **2022**, *44*, 4203–4228. [CrossRef]
136. Younesi, A.; Shayeghi, H.; Wang, Z.; Siano, P.; Mehrizi-Sani, A.; Safari, A. Trends in Modern Power Systems Resilience: State-of-the-Art Review. *Renew. Sustain. Energy Rev.* **2022**, *162*, 112397. [CrossRef]
137. Sinsel, S.R.; Riemke, R.L.; Hoffmann, V.H. Challenges and Solution Technologies for the Integration of Variable Renewable Energy Sources—A Review. *Renew. Energy* **2020**, *145*, 2271–2285. [CrossRef]
138. Kabalci, Y.; Kabalci, E.; Padmanaban, S.; Holm-Nielsen, J.B.; Blaabjerg, F. Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments. *Electronics* **2019**, *8*, 972. [CrossRef]
139. Sedhom, B.E.; El-Saadawi, M.M.; El Moursi, M.S.; Hassan, M.A.; Eladl, A.A. IoT-Based Optimal Demand Side Management and Control Scheme for Smart Microgrid. *Int. J. Electr. Power Energy Syst.* **2021**, *127*, 106674. [CrossRef]
140. Kabalci, E.; Kabalci, Y. Internet of Things for Smart Grid Applications. In *From Smart Grid to Internet of Energy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 249–307, ISBN 978-0-12-819710-3.
141. Kondoro, A.; Ben Dhaou, I.; Tenhunen, H.; Mvungi, N. Real Time Performance Analysis of Secure IoT Protocols for Microgrid Communication. *Future Gener. Comput. Syst.* **2021**, *116*, 1–12. [CrossRef]
142. Guerrero-Prado, J.S.; Alfonso-Morales, W.; Caicedo-Bravo, E.; Zayas-Pérez, B.; Espinosa-Reza, A. The Power of Big Data and Data Analytics for AMI Data: A Case Study. *Sensors* **2020**, *20*, 3289. [CrossRef]
143. Ponnusamy, V.K.; Kasinathan, P.; Madurai Elavarasan, R.; Ramanathan, V.; Anandan, R.K.; Subramaniam, U.; Ghosh, A.; Hossain, E. A Comprehensive Review on Sustainable Aspects of Big Data Analytics for the Smart Grid. *Sustainability* **2021**, *13*, 13322. [CrossRef]
144. Kezunovic, M.; Pinson, P.; Obradovic, Z.; Grijalva, S.; Hong, T.; Bessa, R. Big Data Analytics for Future Electricity Grids. *Electr. Power Syst. Res.* **2020**, *189*, 106788. [CrossRef]
145. Arif, A.; Javaid, N.; Aldegheishem, A.; Alrajeh, N. Big Data Analytics for Identifying Electricity Theft Using Machine Learning Approaches in Microgrids for Smart Communities. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6316. [CrossRef]
146. Oprea, S.-V.; Bâra, A.; Tudorică, B.G.; Călinoiu, M.I.; Botezatu, M.A. Insights into Demand-Side Management with Big Data Analytics in Electricity Consumers' Behaviour. *Comput. Electr. Eng.* **2021**, *89*, 106902. [CrossRef]
147. Dhanalakshmi, J.; Ayyanathan, N. A Systematic Review of Big Data in Energy Analytics Using Energy Computing Techniques. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6647. [CrossRef]
148. Gupta, R.; Al-Ali, A.R.; Zualkernan, I.A.; Das, S.K. Big Data Energy Management, Analytics and Visualization for Residential Areas. *IEEE Access* **2020**, *8*, 156153–156164. [CrossRef]
149. Jeong, B.-C.; Shin, D.-H.; Im, J.-B.; Park, J.-Y.; Kim, Y.-J. Implementation of Optimal Two-Stage Scheduling of Energy Storage System Based on Big-Data-Driven Forecasting—An Actual Case Study in a Campus Microgrid. *Energies* **2019**, *12*, 1124. [CrossRef]

150. Guerrero-Prado, J.S.; Alfonso-Morales, W.; Caicedo-Bravo, E.F. A Data Analytics/Big Data Framework for Advanced Metering Infrastructure Data. *Sensors* **2021**, *21*, 5650. [CrossRef]
151. Umar, A.; Kumar, D.; Ghose, T. Blockchain-Based Decentralized Energy Intra-Trading with Battery Storage Flexibility in a Community Microgrid System. *Appl. Energy* **2022**, *322*, 119544. [CrossRef]
152. Chen, Z.; Guo, W.; Zhao, R.; Liu, Y.; Xie, H. Deep Learning Optimization of Microgrid Economic Dispatch and Wireless Power Transmission Using Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 2050031. [CrossRef]
153. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H.H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access* **2021**, *9*, 29429–29440. [CrossRef]
154. Tsao, Y.-C.; Vu, T.-L. A Decentralized Microgrid Considering Blockchain Adoption and Credit Risk. *J. Oper. Res. Soc.* **2022**, *73*, 2116–2128. [CrossRef]
155. Aloqaily, M.; Bouachir, O.; Özkasap, Ö.; Ali, F.S. SynergyGrids: Blockchain-Supported Distributed Microgrid Energy Trading. *Peer-to-Peer Netw. Appl.* **2022**, *15*, 884–900. [CrossRef]
156. Zulu, M.L.T.; Carpanen, R.P.; Tiako, R. A Comprehensive Review: Study of Artificial Intelligence Optimization Technique Applications in a Hybrid Microgrid at Times of Fault Outbreaks. *Energies* **2023**, *16*, 1786. [CrossRef]
157. Sabzehgar, R.; Amirhosseini, D.Z.; Rasouli, M. Solar Power Forecast for a Residential Smart Microgrid Based on Numerical Weather Predictions Using Artificial Intelligence Methods. *J. Build. Eng.* **2020**, *32*, 101629. [CrossRef]
158. Nakabi, T.A.; Toivanen, P. Deep Reinforcement Learning for Energy Management in a Microgrid with Flexible Demand. *Sustain. Energy Grids Netw.* **2021**, *25*, 100413. [CrossRef]
159. Mbuwir, B.V.; Geysen, D.; Spiessens, F.; Deconinck, G. Reinforcement Learning for Control of Flexibility Providers in a Residential Microgrid. *IET Smart Grid* **2020**, *3*, 98–107. [CrossRef]
160. Ahmad, T.; Zhang, D.; Huang, C.; Zhang, H.; Dai, N.; Song, Y.; Chen, H. Artificial Intelligence in Sustainable Energy Industry: Status Quo, Challenges and Opportunities. *J. Clean. Prod.* **2021**, *289*, 125834. [CrossRef]
161. Mahendravarman, I.; Elankurisil, S.A.; Venkateshkumar, M.; Ragavendiran, A.; Chin, N. Artificial Intelligent Controller-Based Power Quality Improvement for Microgrid Integration of Photovoltaic System Using New Cascade Multilevel Inverter. *Soft Comput.* **2020**, *24*, 18909–18926. [CrossRef]
162. Nair, D.R.; Nair, M.G.; Thakur, T. A Smart Microgrid System with Artificial Intelligence for Power-Sharing and Power Quality Improvement. *Energies* **2022**, *15*, 5409. [CrossRef]
163. Jafari, M.; Kavousi-Fard, A.; Chen, T.; Karimi, M. A Review on Digital Twin Technology in Smart Grid, Transportation System and Smart City: Challenges and Future. *IEEE Access* **2023**, *11*, 17471–17484. [CrossRef]
164. Khalyasmaa, A.I.; Stepanova, A.I.; Eroshenko, S.A.; Matrenin, P.V. Review of the Digital Twin Technology Applications for Electrical Equipment Lifecycle Management. *Mathematics* **2023**, *11*, 1315. [CrossRef]
165. Reniers, J.M.; Howey, D.A. Digital Twin of a MWh-Scale Grid Battery System for Efficiency and Degradation Analysis. *Appl. Energy* **2023**, *336*, 120774. [CrossRef]
166. Can, O.; Turkmen, A. Digital Twin and Manufacturing. In *Digital Twin Driven Intelligent Systems and Emerging Metaverse*; Karaarslan, E., Aydin, Ö., Cali, Ü., Challenger, M., Eds.; Springer Nature: Singapore, 2023; pp. 175–194, ISBN 978-981-9902-52-1.
167. Attaran, M.; Celik, B.G. Digital Twin: Benefits, Use Cases, Challenges, and Opportunities. *Decis. Anal. J.* **2023**, *6*, 100165. [CrossRef]
168. Singh, M.; Srivastava, R.; Fuenmayor, E.; Kuts, V.; Qiao, Y.; Murray, N.; Devine, D. Applications of Digital Twin across Industries: A Review. *Appl. Sci.* **2022**, *12*, 5727. [CrossRef]
169. Nasirahmadi, A.; Hensel, O. Toward the Next Generation of Digitalization in Agriculture Based on Digital Twin Paradigm. *Sensors* **2022**, *22*, 498. [CrossRef]
170. Agostinelli, S.; Cumo, F.; Nezhad, M.M.; Orsini, G.; Piras, G. Renewable Energy System Controlled by Open-Source Tools and Digital Twin Model: Zero Energy Port Area in Italy. *Energies* **2022**, *15*, 1817. [CrossRef]
171. Bortolini, R.; Rodrigues, R.; Alavi, H.; Vecchia, L.F.D.; Forcada, N. Digital Twins' Applications for Building Energy Efficiency: A Review. *Energies* **2022**, *15*, 7002. [CrossRef]
172. Kharlamova, N.; Træholt, C.; Hashemi, S. A Digital Twin of Battery Energy Storage Systems Providing Frequency Regulation. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25–28 April 2022; pp. 1–7.
173. Söderäng, E.; Hautala, S.; Mikulski, M.; Storm, X.; Niemi, S. Development of a Digital Twin for Real-Time Simulation of a Combustion Engine-Based Power Plant with Battery Storage and Grid Coupling. *Energy Convers. Manag.* **2022**, *266*, 115793. [CrossRef]
174. Steindl, G.; Stagl, M.; Kasper, L.; Kastner, W.; Hofmann, R. Generic Digital Twin Architecture for Industrial Energy Systems. *Appl. Sci.* **2020**, *10*, 8903. [CrossRef]
175. Falekas, G.; Karlis, A. Digital Twin in Electrical Machine Control and Predictive Maintenance: State-of-the-Art and Future Prospects. *Energies* **2021**, *14*, 5933. [CrossRef]
176. van Dinter, R.; Tekinerdogan, B.; Catal, C. Predictive Maintenance Using Digital Twins: A Systematic Literature Review. *Inf. Softw. Technol.* **2022**, *151*, 107008. [CrossRef]
177. Hosamo, H.H.; Svennevig, P.R.; Svidt, K.; Han, D.; Nielsen, H.K. A Digital Twin Predictive Maintenance Framework of Air Handling Units Based on Automatic Fault Detection and Diagnostics. *Energy Build.* **2022**, *261*, 111988. [CrossRef]

178. You, Y.; Chen, C.; Hu, F.; Liu, Y.; Ji, Z. Advances of Digital Twins for Predictive Maintenance. *Procedia Comput. Sci.* **2022**, *200*, 1471–1480. [CrossRef]
179. Jamieson, M.R.; Hong, Q.; Han, J.; Paladhi, S.; Booth, C. Digital Twin-Based Real-Time Assessment of Resilience in Microgrids. In Proceedings of the 11th International Conference on Renewable Power Generation—Meeting Net Zero Carbon (RPG 2022), London, UK, 22–23 September 2022; pp. 213–217. [CrossRef]
180. Hong, Y.-Y.; Apolinario, G.F.D.G. Ancillary Services and Risk Assessment of Networked Microgrids Using Digital Twin. *IEEE Trans. Power Syst.* **2022**, 1–15. [CrossRef]
181. Saad, A.; Faddel, S.; Mohammed, O. IoT-Based Digital Twin for Energy Cyber-Physical Systems: Design and Implementation. *Energies* **2020**, *13*, 4762. [CrossRef]
182. Rosero, D.G.; Sanabria, E.; Díaz, N.L.; Trujillo, C.L.; Luna, A.; Andrade, F. Full-Deployed Energy Management System Tested in a Microgrid Cluster. *Appl. Energy* **2023**, *334*, 120674. [CrossRef]
183. Zheng, X.; Wu, H.; Ye, Q. A Cloud Fog Intelligent Approach Based on Modified Algorithm in Application of Reinforced Smart Microgrid Management. *Sustain. Cities Soc.* **2022**, *76*, 103455. [CrossRef]
184. Benblidia, M.A.; Brik, B.; Esseghir, M.; Merghem-Boulahia, L. Power Allocation and Energy Cost Minimization in Cloud Data Centers Microgrids: A Two-Stage Optimization Approach. *IEEE Access* **2022**, *10*, 66213–66226. [CrossRef]
185. Benblidia, M.A.; Brik, B.; Esseghir, M.; Merghem-Boulahia, L. A Renewable Energy-Aware Power Allocation for Cloud Data Centers: A Game Theory Approach. *Comput. Commun.* **2021**, *179*, 102–111. [CrossRef]
186. Dong, W.; Yang, Q.; Li, W.; Zomaya, A.Y. Machine-Learning-Based Real-Time Economic Dispatch in Islanding Microgrids in a Cloud-Edge Computing Environment. *IEEE Internet Things J.* **2021**, *8*, 13703–13711. [CrossRef]
187. Olabi, A.G.; Abdelkareem, M.A.; Jouhara, H. Energy Digitalization: Main Categories, Applications, Merits, and Barriers. *Energy* **2023**, *271*, 126899. [CrossRef]
188. Heymann, F.; Milojevic, T.; Covatariu, A.; Verma, P. Digitalization in Decarbonizing Electricity Systems—Phenomena, Regional Aspects, Stakeholders, Use Cases, Challenges and Policy Options. *Energy* **2023**, *262*, 125521. [CrossRef]
189. Xiong, J.; Hsiang, E.-L.; He, Z.; Zhan, T.; Wu, S.-T. Augmented Reality and Virtual Reality Displays: Emerging Technologies and Future Perspectives. *Light Sci. Appl.* **2021**, *10*, 216. [CrossRef]
190. Teodoro, P.; Mattioli, L.; Cyrino, G.; Cardoso, A.; Lamounier, E.; Zorcot, E.; Ramos, D. Training Routine for Electrical Power Station Operators Using Virtual Reality. In *Perspectives and Trends in Education and Technology*; Mesquita, A., Abreu, A., Carvalho, J.V., de Mello, C.H.P., Eds.; Smart Innovation, Systems and Technologies; Springer Nature Singapore: Singapore, 2023; Volume 320, pp. 387–398, ISBN 978-981-19658-4-5.
191. Sattarpanah Karganroudi, S.; Silva, R.E.; Chahdi El Ouazani, Y.; Aminzadeh, A.; Dimitrova, M.; Ibrahim, H. A Novel Assembly Process Guidance Using Augmented Reality for a Standalone Hybrid Energy System. *Int. J. Adv. Manuf. Technol.* **2022**, *122*, 3425–3445. [CrossRef]
192. Zheng, S.; Zhang, M.; Zhou, H. Application of Augmented Reality Technology and Artificial Intelligence Satellite Communication Equipment in Power Grid Emergency Training. *J. Phys. Conf. Ser.* **2021**, *2074*, 012093. [CrossRef]
193. Pan, Q.; Zhang, M.; Zhou, H. Application of Augmented Reality (AR) Technology in Power Grid Emergency Training. *J. Phys. Conf. Ser.* **2021**, *2074*, 012095. [CrossRef]
194. Bi, M.; Zhang, M.; Zhou, H. Application of Augmented Reality (AR) Technology in Low-Voltage Line Interruption Training and Power Grid Emergency Training. *J. Phys. Conf. Ser.* **2021**, *2074*, 012094. [CrossRef]
195. Fernandes, S.V.; João, D.V.; Cardoso, B.B.; Martins, M.A.I.; Carvalho, E.G. Digital Twin Concept Developing on an Electrical Distribution System—An Application Case. *Energies* **2022**, *15*, 2836. [CrossRef]
196. Dileep, G. A Survey on Smart Grid Technologies and Applications. *Renew. Energy* **2020**, *146*, 2589–2625. [CrossRef]
197. Kimani, K.; Oduol, V.; Langat, K. Cyber Security Challenges for IoT-Based Smart Grid Networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
198. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015; p. NIST SP 800-82r2, Appendix C.
199. Veitch, C.; Henry, J.; Richardson, B.; Hart, D. *Microgrid Cyber Security Reference Architecture*; Sandia National Lab.: Albuquerque, NM, USA, 2013; pp. SAND2013–5472, 1090210, 460305. [CrossRef]
200. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive Survey and Taxonomies of False Data Injection Attacks in Smart Grids: Attack Models, Targets, and Impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
201. Reda, H.T.; Anwar, A.; Mahmood, A.N.; Tari, Z. A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids. *ACM Comput. Surv.* **2023**. [CrossRef]
202. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
203. Cao, G.; Gu, W.; Lou, G.; Sheng, W.; Liu, K. Distributed Synchronous Detection for False Data Injection Attack in Cyber-Physical Microgrids. *Int. J. Electr. Power Energy Syst.* **2022**, *137*, 107788. [CrossRef]
204. Giraldo, J.; Hariri, M.E.; Parvania, M. Decentralized Moving Target Defense for Microgrid Protection Against False-Data Injection Attacks. *IEEE Trans. Smart Grid* **2022**, *13*, 3700–3710. [CrossRef]
205. Koduru, S.S.; Machina, V.s.P.; Madichetty, S. Cyber-Attacks in Cyber Physical Microgrid Systems: A Comprehensive Review. *Electr. Electron. Eng.* **2023**, 2023040691. [CrossRef]

206. Tan, S.; Xie, P.; Guerrero, J.M.; Vasquez, J.C. False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters. *Appl. Energy* **2022**, *310*, 118425. [CrossRef]
207. Barzegari, Y.; Zarei, J.; Razavi-Far, R.; Saif, M.; Palade, V. Resilient Consensus Control Design for DC Microgrids against False Data Injection Attacks Using a Distributed Bank of Sliding Mode Observers. *Sensors* **2022**, *22*, 2644. [CrossRef]
208. Chen, X.; Zhou, J.; Shi, M.; Chen, Y.; Wen, J. Distributed Resilient Control against Denial of Service Attacks in DC Microgrids with Constant Power Load. *Renew. Sustain. Energy Rev.* **2022**, *153*, 111792. [CrossRef]
209. Chen, X.; Hu, C.; Tian, E.; Peng, C. Event-Based Fuzzy Resilient Control of Nonlinear DC Microgrids under Denial-of-Service Attacks. *ISA Trans.* **2022**, *127*, 206–215. [CrossRef]
210. Jamali, M.; Baghaee, H.R.; Sadabadi, M.S.; Gharehpetian, G.B.; Anvari-Moghaddam, A. Distributed Cooperative Event-Triggered Control of Cyber-Physical AC Microgrids Subject to Denial-of-Service Attacks. *IEEE Trans. Smart Grid* **2023**, 1. [CrossRef]
211. Kumar, V.; Mohanty, S.R. Chapter 1—Denial-of-Service Attack Resilient Control for Cyber Physical Microgrid System. In *Microgrid Cyberphysical Systems*; Subudhi, B., Ray, P.K., Eds.; Elsevier: Amsterdam, The Netherlands, 2022; pp. 1–27, ISBN 978-0-323-99910-6.
212. Zuo, S.; Beg, O.A.; Lewis, F.L.; Davoudi, A. Resilient Networked AC Microgrids Under Unbounded Cyber Attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 3785–3794. [CrossRef]
213. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3–19. [CrossRef]
214. Jiao, W.; Li, V.O.K. Support Vector Machine Detection of Data Framing Attack in Smart Grid. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–5.
215. Ramakrishna, R.; Scaglione, A. Detection of False Data Injection Attack Using Graph Signal Processing for the Power Grid. In Proceedings of the 2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Ottawa, ON, Canada, 11–14 November 2019; pp. 1–5.
216. Ma, M.; Lahmadi, A.; Chrisment, I. Detecting a Stealthy Attack in Distributed Control for Microgrids Using Machine Learning Algorithms. In Proceedings of the 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Tampere, Finland, 10–12 June 2020; Volume 1, pp. 143–148.
217. Karanfil, M.; Rebbah, D.E.; Ghafouri, M.; Kassouf, M.; Debbabi, M.; Hanna, A. Security Monitoring of the Microgrid Using IEC 62351-7 Network and System Management. In Proceedings of the 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, USA, 24–28 April 2022; pp. 1–5.
218. Naderi, E.; Asrari, A. Experimental Validation of a Remedial Action via Hardware-in-the-Loop System Against Cyberattacks Targeting a Lab-Scale PV/Wind Microgrid. *IEEE Trans. Smart Grid* **2023**, 1. [CrossRef]
219. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids. *IEEE Trans. Power Electron.* **2021**, *36*, 2522–2532. [CrossRef]
220. Fritz, J.J.; Sagisi, J.; James, J.; Leger, A.S.; King, K.; Duncan, K.J. Simulation of Man in the Middle Attack On Smart Grid Testbed. In Proceedings of the 2019 SoutheastCon, Huntsville, AL, USA, 11–14 April 2019; pp. 1–6.
221. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-Middle Attacks and Defence in a Power System Cyber-Physical Testbed. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 164–177. [CrossRef]
222. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872. [CrossRef]
223. Chakrabarty, S.; Sikdar, B. Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems. *IEEE Trans. Power Syst.* **2021**, *36*, 271–280. [CrossRef]
224. Choeum, D.; Choi, D.-H. Vulnerability Assessment of Conservation Voltage Reduction to Load Redistribution Attack in Unbalanced Active Distribution Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 473–483. [CrossRef]
225. Zhang, Z.J.; Bloch, M.; Saeedifard, M. Load Redistribution Attacks in Multi-Terminal DC Grids. In Proceedings of the 2022 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA, 9–13 October 2022; pp. 1–7.
226. Pinceti, A.; Sankar, L.; Kosut, O. Detection and Localization of Load Redistribution Attacks on Large-Scale Systems. *J. Mod. Power Syst. Clean Energy* **2022**, *10*, 361–370. [CrossRef]
227. He, H.; Huang, S.; Liu, Y.; Zhang, T. A Tri-Level Optimization Model for Power Grid Defense with the Consideration of Post-Allocated DGs against Coordinated Cyber-Physical Attacks. *Int. J. Electr. Power Energy Syst.* **2021**, *130*, 106903. [CrossRef]
228. Poursmaeil, B.; Ravadanegh, S.N. Robust Defense Strategy Against Cyber Physical Attacks In Networked Microgrids. In Proceedings of the 2019 International Power System Conference (PSC), Tehran, Iran, 9–11 December 2019; pp. 709–715.
229. Qin, C.; Zhong, C.; Sun, B.; Jin, X.; Zeng, Y. A Tri-Level Optimal Defense Method against Coordinated Cyber-Physical Attacks Considering Full Substation Topology. *Appl. Energy* **2023**, *339*, 120961. [CrossRef]
230. Zhang, J.; Sankar, L. Physical System Consequences of Unobservable State-and-Topology Cyber-Physical Attacks. *IEEE Trans. Smart Grid* **2016**, *7*, 2016–2025. [CrossRef]
231. Na, G.; Eun, Y. A Probing Signal-Based Replay Attack Detection Method Avoiding Control Performance Degradation. *Int. J. Control Autom. Syst.* **2022**, *20*, 3637–3649. [CrossRef]
232. Naha, A.; Teixeira, A.; Ahlén, A.; Dey, S. Sequential Detection of Replay Attacks. *IEEE Trans. Autom. Control* **2023**, *68*, 1941–1948. [CrossRef]

233. Abdelwahab, A.; Lucia, W.; Youssef, A. Set-Theoretic Control for Active Detection of Replay Attacks with Applications to Smart Grid. In Proceedings of the 2020 IEEE Conference on Control Technology and Applications (CCTA), Montreal, QC, Canada, 24–26 August 2020; pp. 1004–1009.
234. Alsokhiry, F.; Annuk, A.; Kabanen, T.; Mohamed, M.A. A Malware Attack Enabled an Online Energy Strategy for Dynamic Wireless EVs within Transportation Systems. *Mathematics* **2022**, *10*, 4691. [CrossRef]
235. Xu, S.; Tu, H.; Xia, Y. Resilience Enhancement of Renewable Cyber–Physical Power System against Malware Attacks. *Reliab. Eng. Syst. Saf.* **2023**, *229*, 108830. [CrossRef]
236. BlackEnergy APT Attacks in Ukraine. Available online: https://www.kaspersky.com/resource-center/threats/blackenergy (accessed on 19 April 2023).
237. Karanfil, M.; Rebbah, D.E.; Debbabi, M.; Kassouf, M.; Ghafouri, M.; Youssef, E.-N.S.; Hanna, A. Detection of Microgrid Cyberattacks Using Network and System Management. *IEEE Trans. Smart Grid* **2022**, 1. [CrossRef]
238. Czekster, R.M.; Avritzer, A.; Menasché, D.S. Aging and Rejuvenation Models of Load Changing Attacks in Micro-Grids. In Proceedings of the 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Wuhan, China, 25–28 October 2021; pp. 17–24.
239. Khalil, S.M.; Bahsi, H.; Dola, H.O.; Korõtko, T.; McLaughlin, K.; Kotkas, V. Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. *Comput. Secur.* **2023**, *124*, 102950. [CrossRef]
240. Tian, W.; Du, M.; Ji, X.; Liu, G.; Dai, Y.; Han, Z. Honeypot Detection Strategy Against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game. *IEEE Internet Things J.* **2021**, *8*, 17372–17381. [CrossRef]
241. Tian, W.; Ji, X.; Liu, W.; Liu, G.; Zhai, J.; Dai, Y.; Huang, S. Prospect Theoretic Study of Honeypot Defense Against Advanced Persistent Threats in Power Grid. *IEEE Access* **2020**, *8*, 64075–64085. [CrossRef]
242. Park, K.; Ahn, B.; Kim, J.; Won, D.; Noh, Y.; Choi, J.; Kim, T. An Advanced Persistent Threat (APT)-Style Cyberattack Testbed for Distributed Energy Resources (DER). In Proceedings of the 2021 IEEE Design Methodologies Conference (DMC), Bath, UK, 14–15 July 2021; pp. 1–5.
243. Sheng, J. Research on SQL Injection Attack and Defense Technology of Power Dispatching Data Network: Based on Data Mining. *Mob. Inf. Syst.* **2022**, *2022*, e6207275. [CrossRef]
244. Gaggero, G.B.; Caviglia, R.; Armellin, A.; Rossi, M.; Girdinio, P.; Marchese, M. Detecting Cyberattacks on Electrical Storage Systems through Neural Network Based Anomaly Detection Algorithm. *Sensors* **2022**, *22*, 3933. [CrossRef] [PubMed]
245. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.B.M.; Habib, A.K.M.A.; Aman, A.H.M.; Hossain, M.A. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, e9065768. [CrossRef]
246. Liu, M.; Zhao, C.; Zhang, Z.; Deng, R.; Cheng, P.; Chen, J. Converter-Based Moving Target Defense Against Deception Attacks in DC Microgrids. *IEEE Trans. Smart Grid* **2022**, *13*, 3984–3996. [CrossRef]
247. Takiddin, A.; Rath, S.; Ismail, M.; Sahoo, S. Data-Driven Detection of Stealth Cyber-Attacks in DC Microgrids. *IEEE Syst. J.* **2022**, *16*, 6097–6106. [CrossRef]
248. Salehghaffari, H.; Khodaparastan, M. Dynamic Attacks Against Inverter-Based Microgrids. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; pp. 1–5.
249. Kawoosa, A.I.; Prashar, D. Cyber and Theft Attacks on Smart Electric Metering Systems: An Overview of Defenses. In *Smart Electrical Grid System*; CRC Press: Boca Raton, FL, USA, 2022; ISBN 978-1-00-324227-7.
250. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. [CrossRef]
251. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
252. Gunduz, M.Z.; Das, R. Cyber-Security on Smart Grid: Threats and Potential Solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
253. Luo, J.; Li, H.; Wang, S. A Quantitative Approach and Simplified Generic Transient Motor Startup Power Models for Microgrids Security Assessment. *Sustain. Cities Soc.* **2022**, *83*, 103998. [CrossRef]
254. Mishra, S.; Anderson, K.; Miller, B.; Boyer, K.; Warren, A. Microgrid Resilience: A Holistic Approach for Assessing Threats, Identifying Vulnerabilities, and Designing Corresponding Mitigation Strategies. *Appl. Energy* **2020**, *264*, 114726. [CrossRef]
255. Colorado, P.J.; Suppioni, V.P.; Filho, A.J.S.; Salles, M.B.C.; Grilo-Pavani, A.P. Security Assessment for the Islanding Transition of Microgrids. *IEEE Access* **2022**, *10*, 17189–17200. [CrossRef]
256. Shahzad, S.; Abbasi, M.A.; Ali, H.; Iqbal, M.; Munir, R.; Kilic, H. Possibilities, Challenges, and Future Opportunities of Microgrids: A Review. *Sustainability* **2023**, *15*, 6366. [CrossRef]
257. Khan, R.; Islam, N.; Das, S.K.; Muyeen, S.M.; Moyeen, S.I.; Ali, M.F.; Tasneem, Z.; Islam, M.R.; Saha, D.K.; Badal, M.F.R.; et al. Energy Sustainability–Survey on Technology and Control of Microgrid, Smart Grid and Virtual Power Plant. *IEEE Access* **2021**, *9*, 104663–104694. [CrossRef]
258. Rupeika-Apoga, R.; Petrovska, K. Barriers to Sustainable Digital Transformation in Micro-, Small-, and Medium-Sized Enterprises. *Sustainability* **2022**, *14*, 13558. [CrossRef]
259. Fritzsche, K.; Shuttleworth, L.; Brand, B.; Blechinger, P. *Exploring the Nexus of Mini-Grids and Digital Technologies. Potentials, Challenges and Options for Sustainable Energy Accessin Sub-Saharan Africa*; Institute for Advanced Sustainability Studies (IASS): Potsdam, Germany, 2019; p. 27. [CrossRef]

260. Norouzi, F.; Hoppe, T.; Elizondo, L.R.; Bauer, P. A Review of Socio-Technical Barriers to Smart Microgrid Development. *Renew. Sustain. Energy Rev.* **2022**, *167*, 112674. [CrossRef]
261. Martins, M.A.I.; Fernandes, R.; Heldwein, M.L. Proposals for Regulatory Framework Modifications for Microgrid Insertion–The Brazil Use Case. *IEEE Access* **2020**, *8*, 94852–94870. [CrossRef]
262. Brown, M.A.; Zhou, S.; Ahmadi, M. Smart Grid Governance: An International Review of Evolving Policy Issues and Innovations. *WIREs Energy Environ.* **2018**, *7*, e290. [CrossRef]
263. Manimuthu, A.; Ramesh, R. Privacy and Data Security for Grid-Connected Home Area Network Using Internet of Things. *IET Netw.* **2018**, *7*, 445–452. [CrossRef]
264. Wang, J.; Gao, F.; Zhou, Y.; Guo, Q.; Tan, C.-W.; Song, J.; Wang, Y. Data Sharing in Energy Systems. *Adv. Appl. Energy* **2023**, *10*, 100132. [CrossRef]
265. Reddy, G.P.; Kumar, Y.V.P.; Chakravarthi, M.K. Communication Technologies for Interoperable Smart Microgrids in Urban Energy Community: A Broad Review of the State of the Art, Challenges, and Research Perspectives. *Sensors* **2022**, *22*, 5881. [CrossRef] [PubMed]
266. Taveras Cruz, A.J.; Aybar-Mejía, M.; Díaz Roque, Y.; Coste Ramírez, K.; Durán, J.G.; Rosario Weeks, D.; Mariano-Hernández, D.; Hernández-Callejo, L. Implications of 5G Technology in the Management of Power Microgrids: A Review of the Literature. *Energies* **2023**, *16*, 2020. [CrossRef]
267. Idries, A.; Krogstie, J.; Rajasekharan, J. Challenges in Platforming and Digitizing Decentralized Energy Services. *Energy Inform.* **2022**, *5*, 8. [CrossRef]
268. Anees, T.; Habib, Q.; Al-Shamayleh, A.S.; Khalil, W.; Obaidat, M.A.; Akhunzada, A. The Integration of WoT and Edge Computing: Issues and Challenges. *Sustainability* **2023**, *15*, 5983. [CrossRef]
269. Kim, J.-S.; So, S.M.; Kim, J.-T.; Cho, J.-W.; Park, H.-J.; Jufri, F.H.; Jung, J. Microgrids Platform: A Design and Implementation of Common Platform for Seamless Microgrids Operation. *Electr. Power Syst. Res.* **2019**, *167*, 21–38. [CrossRef]
270. Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C. Digitalization and Decentralization Driving Transactive Energy Internet: Key Technologies and Infrastructures. *Int. J. Electr. Power Energy Syst.* **2021**, *126*, 106593. [CrossRef]
271. Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid Cyber-Security: Review and Challenges toward Resilience. *Appl. Sci.* **2020**, *10*, 5649. [CrossRef]
272. Mondejar, M.E.; Avtar, R.; Diaz, H.L.B.; Dubey, R.K.; Esteban, J.; Gómez-Morales, A.; Hallam, B.; Mbungu, N.T.; Okolo, C.C.; Prasad, K.A.; et al. Digitalization to Achieve Sustainable Development Goals: Steps towards a Smart Green Planet. *Sci. Total Environ.* **2021**, *794*, 148539. [CrossRef] [PubMed]
273. Thakar, S.; A.s., V.; Doolla, S. System Reconfiguration in Microgrids. *Sustain. Energy Grids Netw.* **2019**, *17*, 100191. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.